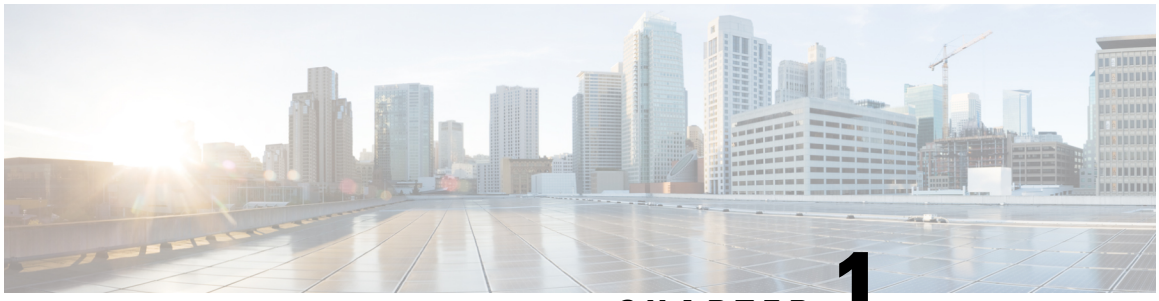
Cisco Crosswork Infrastructure 4.0 and Applications Administration Guide

First Published: 2021-04-19

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 you begin using the Cisco Crosswork applications, you are recommended to be familiar with the following basic concepts and complete the planning and information-gathering steps:

- **User Accounts** : Cisco recommends as a best practice that you create separate accounts for all of your users, so that there is an audit record of user activity on the system. Prepare a list of the people who will use the Crosswork application. Decide on their user names and preliminary passwords, and create user profiles for them.
- **User Roles**: Cisco recommends that you use role-based access control to confine users to just the software functions needed to perform their job duties. By default, every new user you create has full administrative privileges. Unless you want to extend the same privileges to every user, you will need to plan a system of user roles, create them, and assign them to the user profiles you create.
- **Credential Profiles**: For Cisco Crosswork to be able to access a device or to interact with a provider, it must be able to present credentials. Rather than entering credentials each time they are needed, you can instead create credential profiles to securely store this information. The platform supports unique credentials for each type of access protocol, and allows you to bundle multiple protocols and their corresponding credentials in a single profile. Devices that use the same credentials can share a credential profile. For example, if all of your routers in a particular building share a single SSH user ID and password, you can create a single credential profile to allow Cisco Crosswork to access and manage them.

  Before creating a credential profile, you must gather access credentials and supported protocols that you will use to monitor and manage your devices. For providers, this always includes user IDs, passwords, and connection protocols. For devices, it includes user IDs, passwords, and additional data such as the SNMP v2 read and write community strings, and SNMPv3 auth and privilege types. You will use these to create credential profiles.
- **Tags**: Tags are simple text strings you can attach to devices to help group them. Cisco Crosswork comes with a short list of ready-made tags used to group network devices. You can create your own tags and use them to identify, find, and group devices for a variety of purposes.

Plan a preliminary list of custom tags to create when setting up the system, so that you can use them to group your devices when you first onboard them. You need not have a complete list of tags at first, as you can always add more later, but please note that all the tags you do plan to use must be in place before you need them; you cannot create them "on the fly".

- **Providers**: Cisco Crosswork applications rely on external services such as Cisco Network Services Orchestrator (NSO) or SR-PCE for various tasks like configuration changes, segment routing path computation, and so on. In order to manage the access and reuse of information between Crosswork applications, a Provider (such as NSO and SR-PCE) need to be configured for each external service. The provider family determines the type of service that provider supplies to Cisco Crosswork, and the parameters unique to that service, which must be configured. The parameters needed to configure a provider depend on what Crosswork application is used. It is important to review and gather each Crosswork application requirement, before configuring a Provider. For more information, see Provider Dependency, on page 116 and About Provider Families, on page 115.
  - Cisco Network Services Orchestrator (Cisco NSO) is the default provider used in every Cisco Crosswork application installation, so you will need to gather the Cisco NSO IP address or host name, port and protocol, and the credentials to be used to communicate with it (which you will need to add as a credential profile). You will need to do the same for any other providers you may plan to use. For more information, see Add Cisco NSO Providers, on page 120.
  - If you plan to use Crosswork Optimization Engine, a Cisco SR-PCE provider, at minimum, must be defined in order to discover devices and to distribute policy configuration to devices. You should determine the auto-onboarding mode and device profile you will use (if you auto-onboard devices). For more information, see Add Cisco SR-PCE Providers, on page 122.
- **Devices**: You can onboard devices using the UI, a CSV file, an API, SR-PCE discovery, or ZTP. The way a device is onboarded determines the type of information needed to configure a device in Crosswork. Also, Crosswork can forward device configuration to NSO which can change how you provision an NSO provider. For more information, see Add Devices to the Inventory, on page 145.
- **External Data Destination(s)**: Cisco Crosswork functions as the controller for the Cisco Crosswork Data Gateway. Operators who plan to have Cisco Crosswork Data Gateway forward data to other data destinations, need to know about the format required by those destinations and other connection requirements. This is covered in detail in Manage Cisco Crosswork Data Gateways, on page 15.
- If you plan to use Crosswork Change Automation and Health Insights, **KPI (Key Performance Indicators) Profile(s)** are used to monitor the health of the network. You can establish unique performance criteria based on the way a device or devices are used in the network. KPIs can be grouped to form a KPI Profile. It is helpful if you to have a good idea of the data you plan to monitor and the performance targets that you want to establish as you setup Health Insights.

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 Cisco Crosswork application that you are using with the help of 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 file name.

Setup Workflow

The first step in getting started with Cisco Crosswork 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, enrolled Cisco Crosswork Data Gateway and created Cisco Crosswork Data Gateway pools as explained in *Cisco Crosswork Infrastructure 4.0 and Applications 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 Cisco Crosswork

Step	Action
1. Ensure that your devices are configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: Telemetry Prerequisites for New Devices, on page 146 Sample Configuration for Cisco NSO Devices, on page 147
2. Create credential profiles.	Follow the steps in Create Credential Profiles, on page 108
3. Add the provider(s).	Follow the steps in About Adding Providers, on page 117
4. Validate communications with the provider(s).	Check on the provider's reachability using the steps in Get Provider Details, on page 137
5. Import or create tags.	To import them: Import Tags, on page 141 To create them: Create Tags, on page 141
6. Onboard devices using the method you prefer.	See Add Devices to the Inventory, on page 145 **Note** (Optional) To update device attributes (such as mapping a device to NSO, replacing the Loopback IP address with the management IP address, adding geographical coordinates, setting the Local Provider to your NSO server, and so on) export the CSV file, make and save modifications, and import it back to the device inventory.
7. Attach devices to Cisco Crosswork Data Gateway pool to manage them.	Review the **Data Gateways** pane (see Overview of Cisco Crosswork Data Gateway, on page 15). The operational state of the Cisco Crosswork Data Gateway pool to which you want to attach devices must be **Up**. Follow the steps in Attach a Device to Cisco Crosswork Data Gateway Pool, on page 35
8. Validate Cisco Crosswork communications with devices.	Review the **Devices** window (see Manage Network Devices, on page 153). All the devices you have onboarded should be reachable. Click to investigate any device whose **Reachability State** is marked as (unreachable), (degraded), or (unknown).

Step	Action
9. (Optional) Create additional user accounts and user roles.	Follow the steps in Manage Users, on page 230 and Create User Roles, on page 233.
10. (Optional) Import or create additional credential profiles and providers.	To import providers: Import Providers, on page 136 To create providers: Add Providers Through the UI, on page 118
11. (Optional) Group your devices logically as per your requirement.	Follow the steps in Create and Modify Device Groups, on page 161.
12. (Optional) Set display preferences for your topology.	Follow the steps in Define Map Display Settings, on page 213 and Define Color Thresholds for Link Bandwidth Utilization, on page 214.

Log In and Log Out

The Cisco Crosswork user interface is browser based. See the <insert-xref to Install Guide> for supported browser versions.

Step 1 Open a web browser and enter:

`https://<Crosswork_Management_VIP_adddress>:30603/`

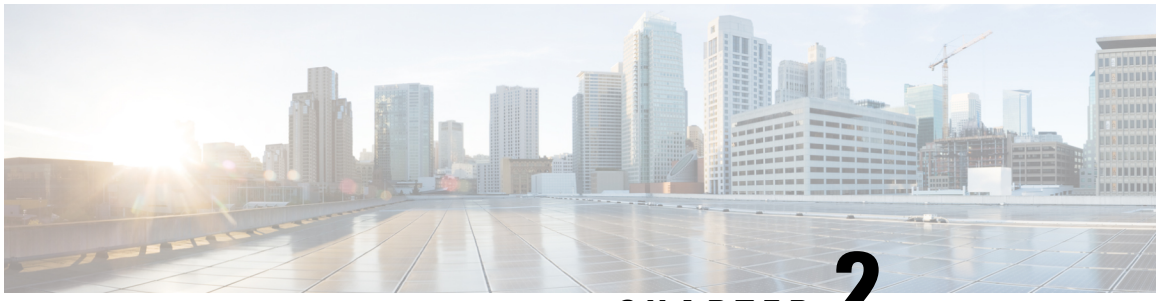
When you access Cisco Crosswork from your browser for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the server. After you do this, the browser accepts the Cisco Crosswork server as a trusted site in all subsequent logins.

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

Note The default administrator user name and password is **admin**. This account is created automatically at installation (see Administrative Users Created During Installation, on page 231). 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 accounts with appropriate privileges and their own credentials and use only those accounts for all subsequent user logins.

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 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, available, and extensible manner.

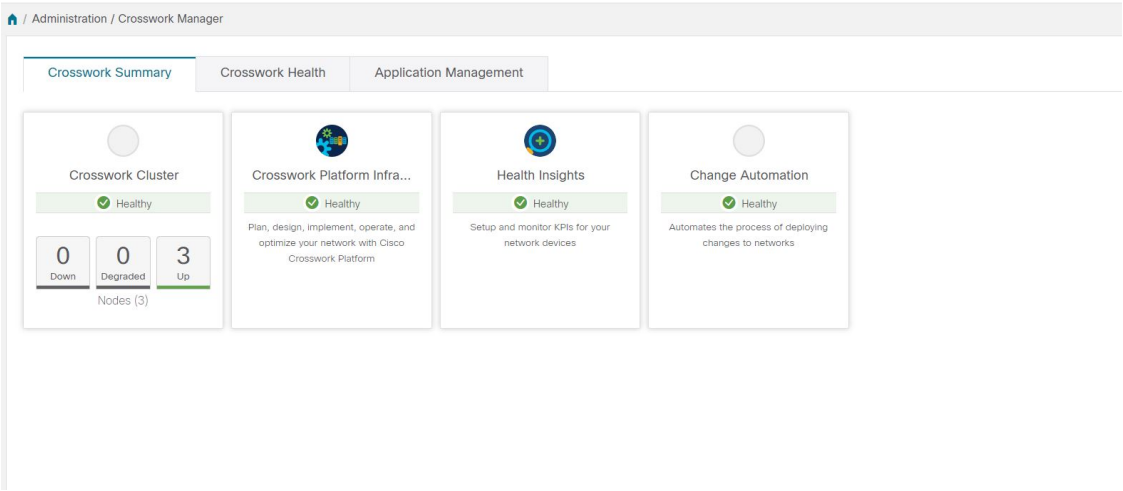
For the 4.0 release, a single cluster consists of a minimum of three nodes, all operating in a hybrid configuration. These three hybrid nodes are mandatory for all Cisco Crosswork deployments. If you have more demanding scale requirements, you can add up to three more nodes, all operating in a worker configuration.

As a Cisco Crosswork administrator, you have full access to all cluster configuration and monitoring functions.

Check Cluster Health

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

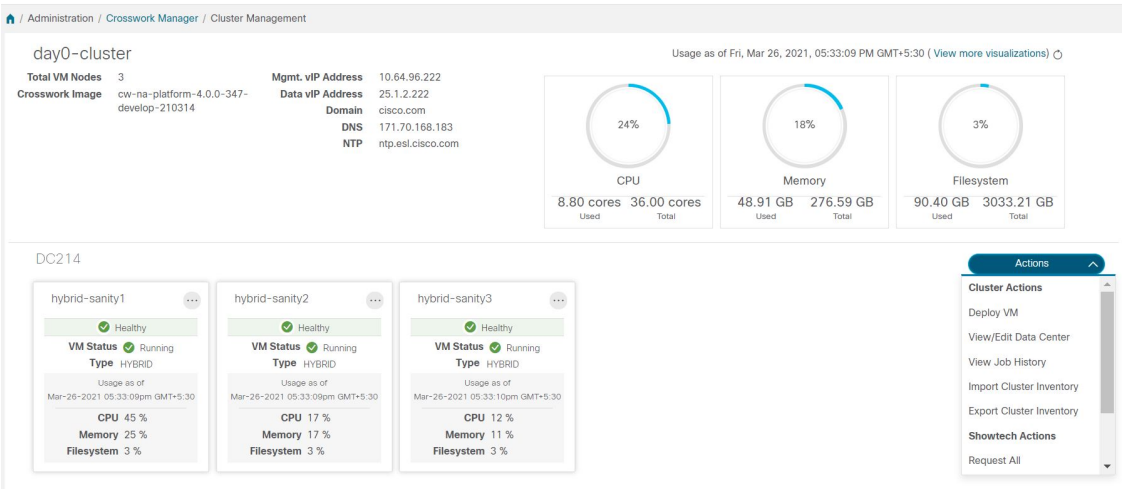
Figure 1: Crosswork Manager Window



The **Crosswork Manager** window gives you summary information about the status of the cluster nodes, the Platform Infrastructure, and the applications you have installed.

For details on the nodes in the cluster: On the **Crosswork Summary** tab, click the **Crosswork Cluster** tile. Cisco Crosswork displays a **Cluster Management** window like the one shown in the following figure.

Figure 2: Cluster Management Window

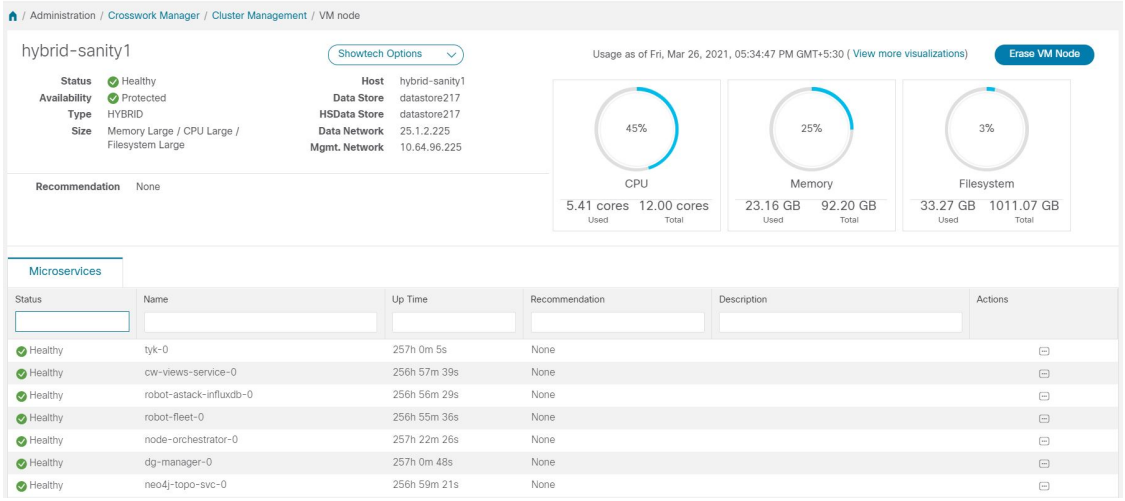


The top section of the window shows the total resources that the cluster is using. The bottom section breaks down the resource utilization by node, with a separate detail tile for each node. The window shows other details, including the IP addresses in use, whether each node is a hybrid or worker, and so on.

Note Click the **View more visualizations** link to Visually Monitor System Functions in Real Time, on page 243.

To see details for a single node: On the tile for the node, click ⋯ and choose **View Details**. The VM Node window displays the node details and the list of microservices running on the node.

Figure 3: VM Node Details Window



To restart a microservice, click  under the **Action** column, and choose **Restart**.

For information on how to use the **Crosswork Health** tab, see Monitor Platform Infrastructure and Application Health, on page 242.

Deploy New Cluster Nodes

After the cluster installer forms the Cisco Crosswork cluster, you may find you need more nodes to meet your requirements. The following steps show how to deploy a new node.

Before you begin

Before you begin, you must know:

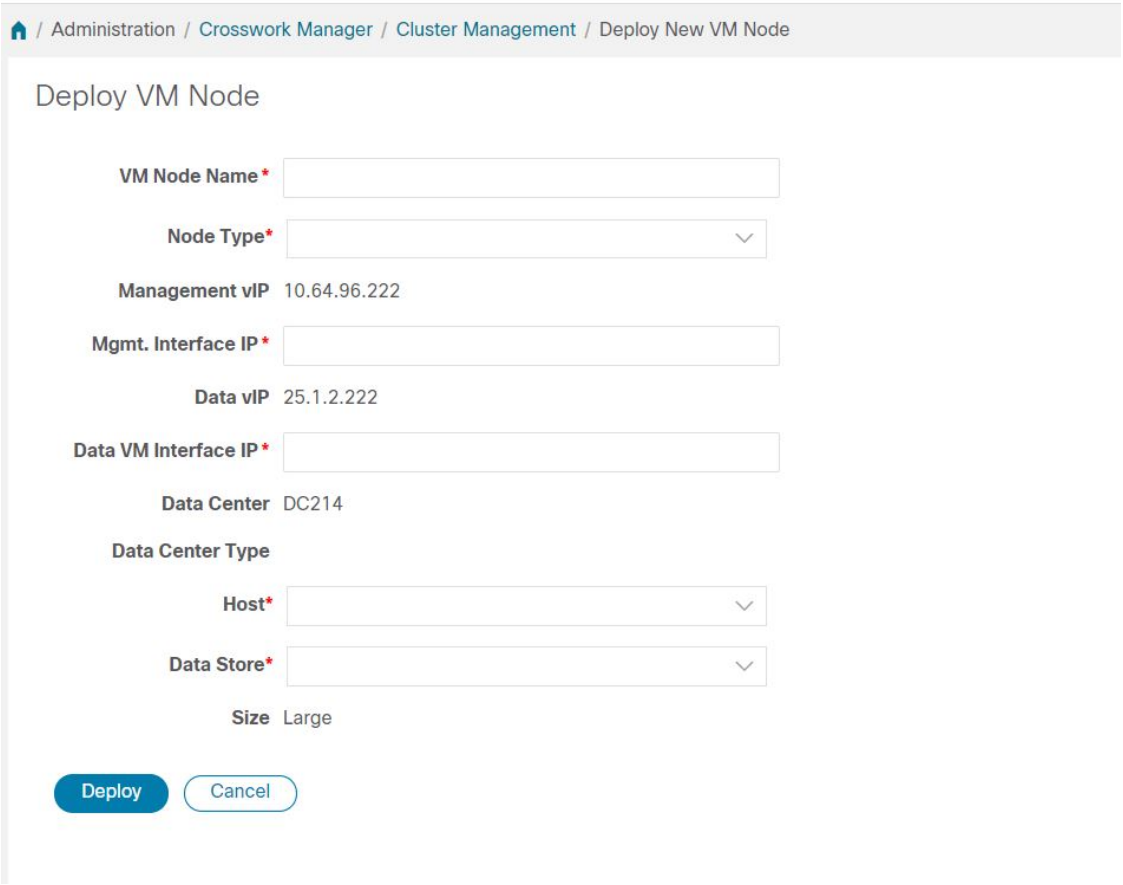
- Details about the Cisco Crosswork network configuration, such as the management IP address.
- Details about the VMware host where you are deploying the new node, such as the data store and data VM interface IP address.
- The type of node you want to add. Your cluster can have a minimum of three hybrid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

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

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

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

Figure 4: 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 added the VM node using Cisco Crosswork APIs: On the newly added VM node tile, click ··· and choose **Deploy** to complete the operation.

View and Edit Data Center Credentials

You can deploy the Cisco Crosswork platform in a data center under either VMware vCenter or Cisco CSP management. The following steps show how to view and edit the credentials for the data center.

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

Step 2 On the **Crosswork Summary** tab, click the **Crosswork Cluster** 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.

View Cluster Job History

Use the Job History window to track the status of cluster 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 **Crosswork Cluster** 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.

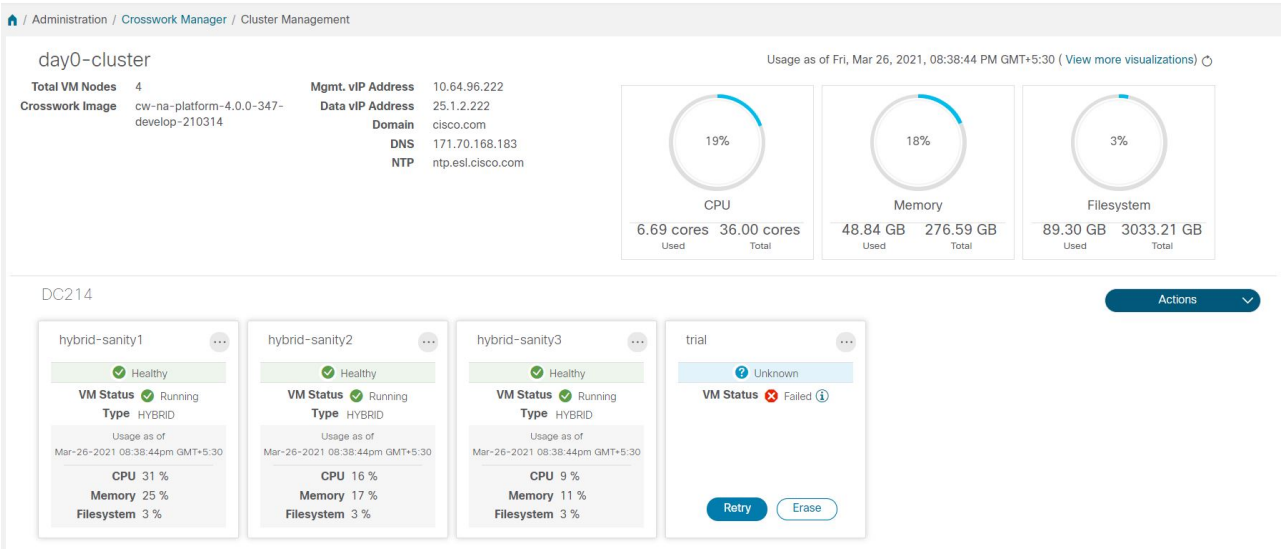
Retry Failed Nodes

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 **Crosswork Cluster** tile to display the **Cluster Management** window.

Figure 5: Cluster Management Window: Failed VM Deployment



Step 3 Click **Retry** on the failed node tile to display the **Deploy New VM 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 your 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 three hybrid nodes is faulty, erase it immediately. Then replace it by deploying a new hybrid node.
- You can have from one to three worker nodes. While you can erase all of them without consequences, we recommend that you erase and replace them one at a time.
- If one hybrid node is faulty, along with one or more worker nodes and applications, try the "Clean System Reboot" procedure described in Cluster System Recovery, on page 12.

  If more than one hybrid node is faulty, follow the "Redeploy and Recover" procedure described in Cluster System Recovery, on page 12.
- If you are still having trouble after taking these steps, contact the Cisco Customer Experience team for assistance.

Erasing a node is a disruptive action and can block some processes until the action is completed. To minimize disruption, try to conduct this activity during a maintenance window only.

Note While removing a Hybrid or Worker node, the Cisco Crosswork UI may become unreachable for 1-2 minutes, due to the location of the `cw-ui` pod in the removed node.

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

Step 2 On the **Crosswork Summary** tab, click the **Crosswork Cluster** 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.

Import Cluster Inventory

Cisco Crosswork uses a cluster inventory file to deploy or replace nodes in your cluster. If your cluster was a manual install, you must import the cluster inventory file to Cisco Crosswork manually.

Note Importing the cluster inventory file is a **required** operation for manually-installed clusters. "Manually installed" means clusters that are created without the help of the cluster installer. You cannot deploy or remove VM nodes until you complete this operation. Cisco Crosswork disables the options to deploy or remove a VM until you import the missing cluster inventory file.

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

Step 2 On the **Crosswork Summary** tab, click the **Crosswork Cluster** 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.

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

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

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 **Crosswork Cluster** 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.

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 nodes in the cluster, and the microservices running on each of the nodes.

Cisco Crosswork 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.

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

Step 2 On the **Crosswork Summary** tab, click the **Crosswork Cluster** 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 the  under the **Actions** column. Then select the showtech option that you want to perform.

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

Cluster System Recovery

When System Recovery Is Needed

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 re-distribute 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, first examine the alarm. Then check on the health of the individual node, application, or service identified in the alarm. You can use the features described in Check Cluster Health, on page 5 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 re-add) 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.

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

If you instantiated your Cisco Crosswork nodes using Cisco CSP 5000, the process in both cases is similar to the process for VMware. See the CSP 5000 documentation at https://www.cisco.com/c/en/us/support/switches/cloud-services-platform-5000/series.html#~tab-documents.

Clean System Reboot (VMware)

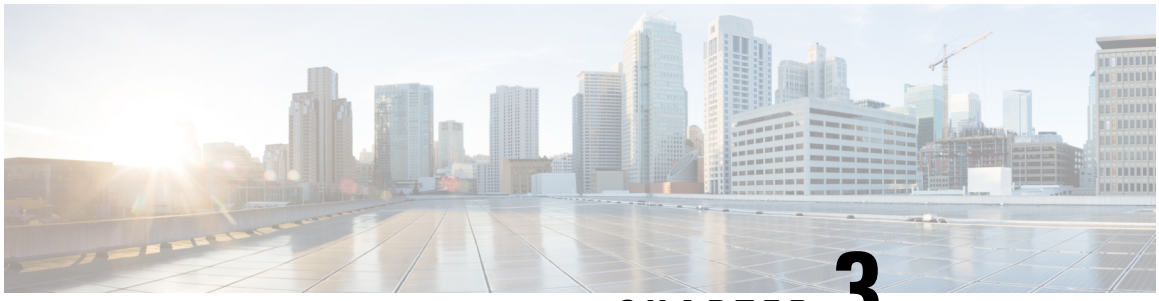
Follow these steps to perform a clean system reboot:

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**.
2. Repeat Step 1 for each of the remaining VMs, until you are sure they are all shut down.
3. Power up the VM hosting the first of your hybrid nodes:
   a. Log in to the VMware vSphere Web Client.
   b. In the **Navigator** pane, right-click the VM that you want to power up.
   c. Choose **Power** > **Power Up**.
   d. Wait for the VM status to change to **On**, then wait another 30 seconds before continuing.
4. Repeat Step 3 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.

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 Cisco Crosswork Backup and Restore, on page 99.

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 the *Cisco Crosswork Platform 4.0 and Applications Installation Guide*.
4. Recover the system state to the newly deployed cluster, as explained in Restore After a Disaster, on page 101.



CHAPTER 3

Manage Cisco Crosswork Data Gateways

This section contains the following topics:

Overview of Cisco Crosswork Data Gateway

When Cisco Crosswork Data Gateway and Cisco Crosswork Platform (also referred to as Cisco Crosswork in this guide) are deployed together, Cisco Crosswork acts as the controller application for the Cisco Crosswork Data Gateway instance. You can use the Cisco Crosswork UI to manage Cisco Crosswork Data Gateway no matter if they are forwarding data to Cisco Crosswork or other compatible data destination (external gRPC or Kafka servers). The number of Cisco Crosswork Data Gateways you need depends on the number of devices being supported, the amount of data being processed and your network architecture.

Once you install a Cisco Crosswork Data Gateway VM, it identifies itself to Cisco Crosswork and enrolls itself automatically. Newly enrolled Cisco Crosswork Data Gateway VMs will have the Operational Status as "Degraded" until enrollment is completed. Cisco Crosswork Data Gateway VMs that have the Role as "Unassigned" need to be assigned to a Crosswork Data Gateway pool before they can used. A pool can consist of one or more Cisco Crosswork Data Gateway VMs with an option to enable HA configuration.

Once you assign a Cisco Crosswork Data Gateway VM to a pool, a virtual Cisco Crosswork Data Gateway gets created automatically and is visible under **Data Gateways** tab. You can then attach or detach devices to the pool, create external data destinations and run collection jobs to forward data to the preferred data destination.

Cisco Crosswork includes MIB files and device model definitions for many Cisco products and provides the ability to load custom software packages in order to add data collection capability for currently unsupported devices.

Cisco Crosswork Data Gateway features can be accessed the Cisco Crosswork main menu. To open Cisco Crosswork Data Gateway management view, choose **Administration** > **Data Gateway Management** from the left navigation bar.

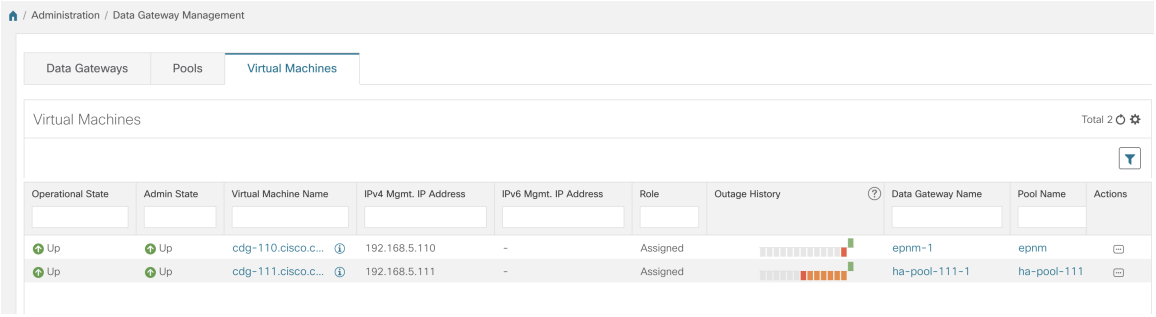
Data Gateway Management page has three tabs:

- Data Gateways: Displays details of the virtual Cisco Crosswork Data Gateway instances.
- Pools: Manage Cisco Crosswork Data Gateway pools.
- Virtual Machines: Manage physical Cisco Crosswork Data Gateway VMs.

Manage Cisco Crosswork Data Gateway VMs

When a Cisco Crosswork Data Gateway auto-enrolls with Cisco Crosswork, it shows up on the **Virtual Machines** page.

Note It can take up to 5 mins for the Operational state to become UP after the initial deployment.



The **Virtual Machines** page provides the following details about Cisco Crosswork Data Gateway VMs:

Field	Description
Operational State	Operational state of the Cisco Crosswork Data Gateway VM. The Cisco Crosswork Data Gateway has following operational states: • Unknown: The initial state when the Cisco Crosswork Data Gateway is enrolled. • Up: When Cisco Crosswork Data Gateway is enrolled with Cisco Crosswork and is running. • Error: When Cisco Crosswork Data Gateway is not reachable from Cisco Crosswork. • Degraded: When there is a disconnect between Cisco Crosswork collectors and Cisco Crosswork.
Admin State	Administrative state of the Cisco Crosswork Data Gateway VM.

Field	Description
Virtual Machine Name	Name of the Cisco Crosswork Data Gateway VM. Clicking the info icon next to the name displays the enrollment details of each VM. This includes details such as, the • Pool name • VM name • Management IP (eth0) with related MAC address • eth1 IP (north bound/vNIC1) with related MAC address • eth2 (south bound/vNIC2) with only the MAC address **Note** The eth2 IP (south bound) is assigned to the Crosswork Data Gateway VM during pool creation. Hence, it will not be displayed as part of enrollment details for each VM.
IPv4 Mgmt.IP Address	Management IPv4 address of the Cisco Crosswork Data Gateway VM.
IPv6 Mgmt.IP Address	Management IPv6 address of the Cisco Crosswork Data Gateway VM.
Role	Shows the role of the Cisco Crosswork Data Gateway VM. It could be either: • Assigned: when Cisco Crosswork Data Gateway VM is assigned to a pool. • Unassigned: when Cisco Crosswork Data Gateway VM is not assigned to any pool. • Spare: when Cisco Crosswork Data Gateway VM is part of a pool but is in standby mode

Field	Description
Outage History	Outage history of the Cisco Crosswork Data Gateway VM over the period of 14 days. Each tile represents the consolidated status of the corresponding Cisco Crosswork Data Gateway for a day. If the Cisco Crosswork Data Gateway was in error state at any time during that day, the tile will be the color representing Error. If the Data Gateway was not in Error but was in Degraded State anytime of the day, the tile will be the color for Degraded state. Finally, if the DG was neither Error nor Degraded but only UP, then the tile will be the color representing OK.
Data Gateway Name	Name of the virtual Cisco Crosswork Data Gateway associated with the Cisco Crosswork Data Gateway VM (if any).
Pool Name	Name of the pool to which the Cisco Crosswork Data Gateway has been assigned (if any).
High Availability Status	High availability status of the Cisco Crosswork Data Gateway VM. It could be either: • Protected • Limited protection • None Planned • Not Protected
Actions	Provides the following options: • Change administration state • Delete Cisco Crosswork Data Gateway VM

Change the Administration State of Cisco Crosswork Data Gateway VM

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

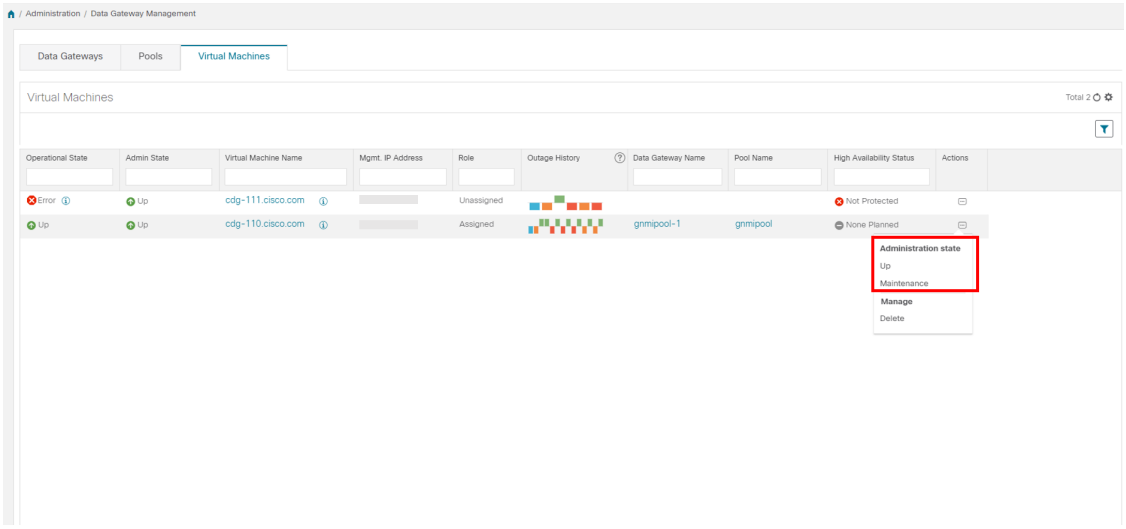
Note If the maintenance activities are affecting the communication between Crosswork and Crosswork Data Gateway, the collection is interrupted and resumes when the communication is restored. Similarly if the maintenance activities are affecting the communication between Crosswork Data Gateway and external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

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

Follow the steps below to change the administration state of a Crosswork Data Gateway VM:

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

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



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

Delete Cisco Crosswork Data Gateway VM from Cisco Crosswork

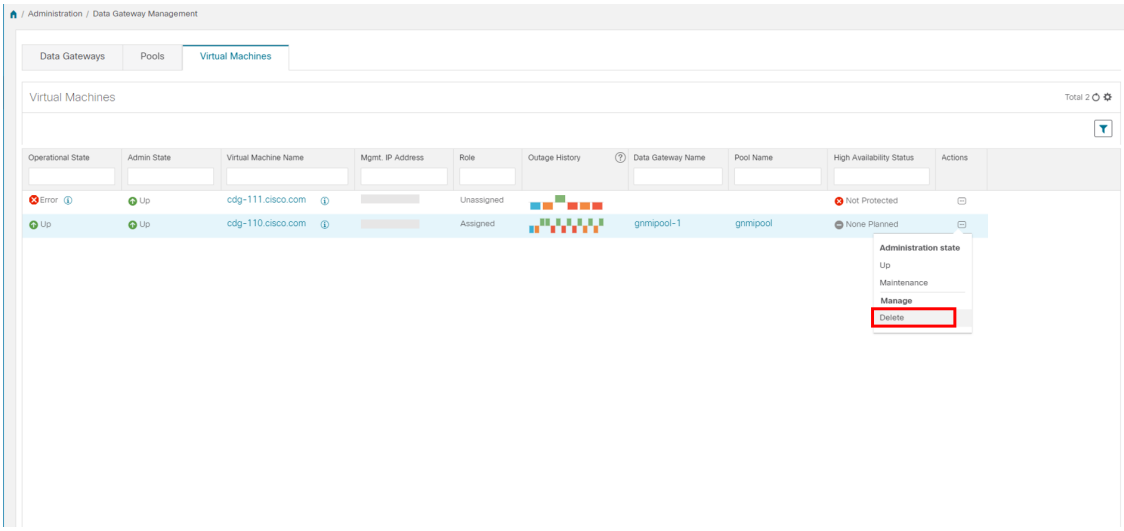
Follow the steps below to delete a Cisco Crosswork Data Gateway VM from Cisco Crosswork:

Before you begin

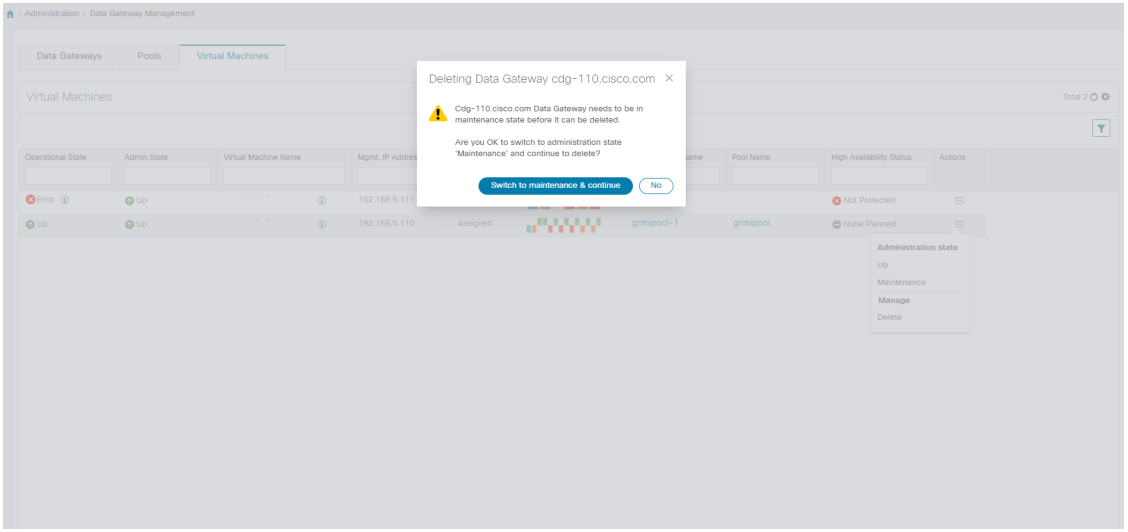
It is recommended that you move the attached devices to another data gateway to not lose any jobs corresponding to these devices. If you detach the devices from Cisco Crosswork Data Gateway VM, then the corresponding jobs are deleted.

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

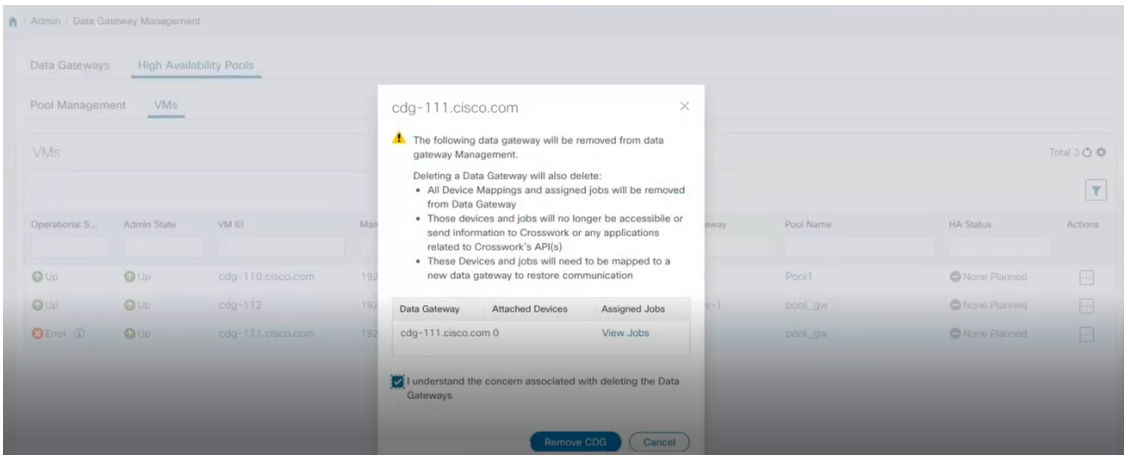
Step 2 For the Crosswork Data Gateway that you want to delete, click ⋯ under **Actions** column and click **Delete**.



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



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



Re-deploy/Re-enroll a Crosswork Data Gateway VM

Re-install a Crosswork Data Gateway VM

If a Crosswork Data Gateway VM has gone down and can no longer be used, then delete the old VM and install a new one. For details on how to install a new Crosswork Data Gateway VM, refer to Section: *Install Cisco Crosswork Data Gateway* in the *Cisco Crosswork Infrastructure 4.0 and Applications Installation Guide*.

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

Re-enroll a Crosswork Data Gateway

If a Crosswork Data Gateway VM was already enrolled with Cisco Crosswork and Cisco Crosswork was re-installed, re-enroll the existing Crosswork Data Gateway VM with these steps:

1. Delete the existing Crosswork Data Gateway enrollment from Cisco Crosswork.
2. Login to the Crosswork Data Gateway VM. From the **Main Menu** in the Interactive Console, select **Troubleshooting** > **0 Re-enroll Data Gateway**.

Troubleshoot Cisco Crosswork Data Gateway from Crosswork UI

Crosswork UI provides the following options to troubleshoot Cisco Crosswork Data Gateway:

- Download showtech Logs, on page 22
- Reboot Cisco Crosswork Data Gateway VM, on page 23

Download showtech Logs

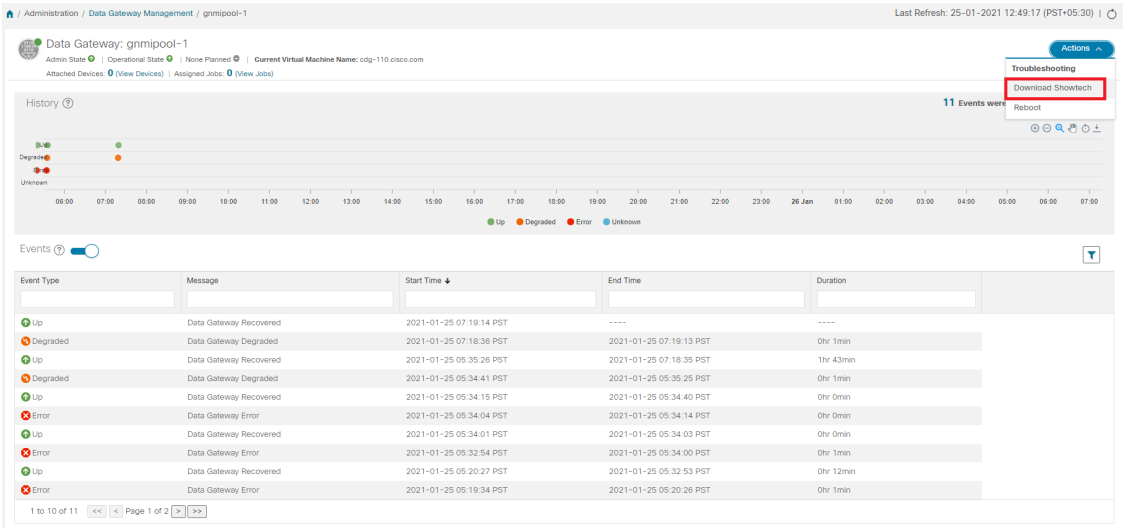
Follow the steps to download showtech logs from Cisco Crosswork UI:

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

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

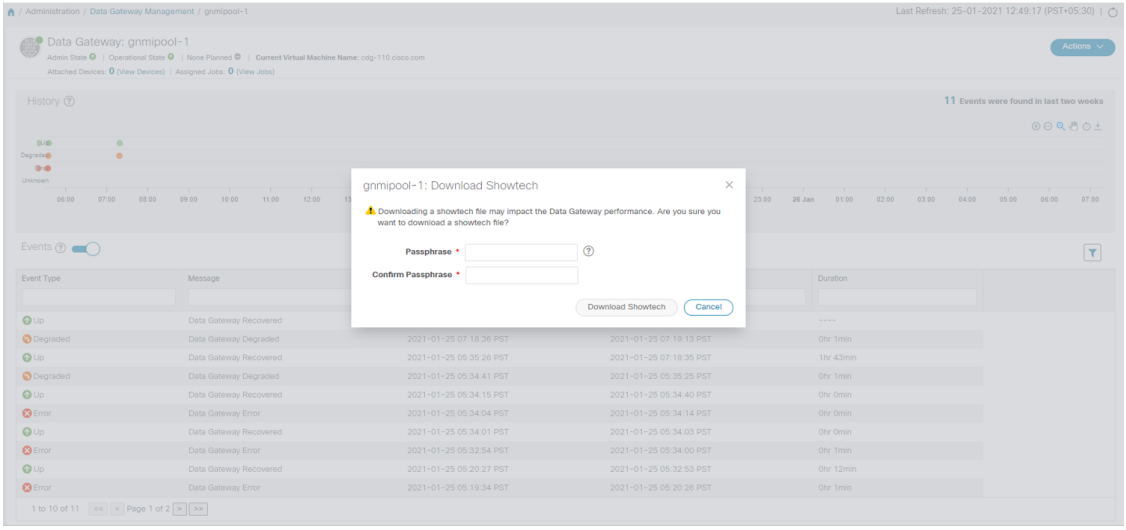
Step 2 Click the Crosswork Data Gateway name for which you want to download showtech.

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



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.



Step 5 Click **Download Showtech**. The showtech file downloads in 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 decrpyt 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 that are 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:<encrypt string>
```

Reboot Cisco Crosswork Data Gateway VM

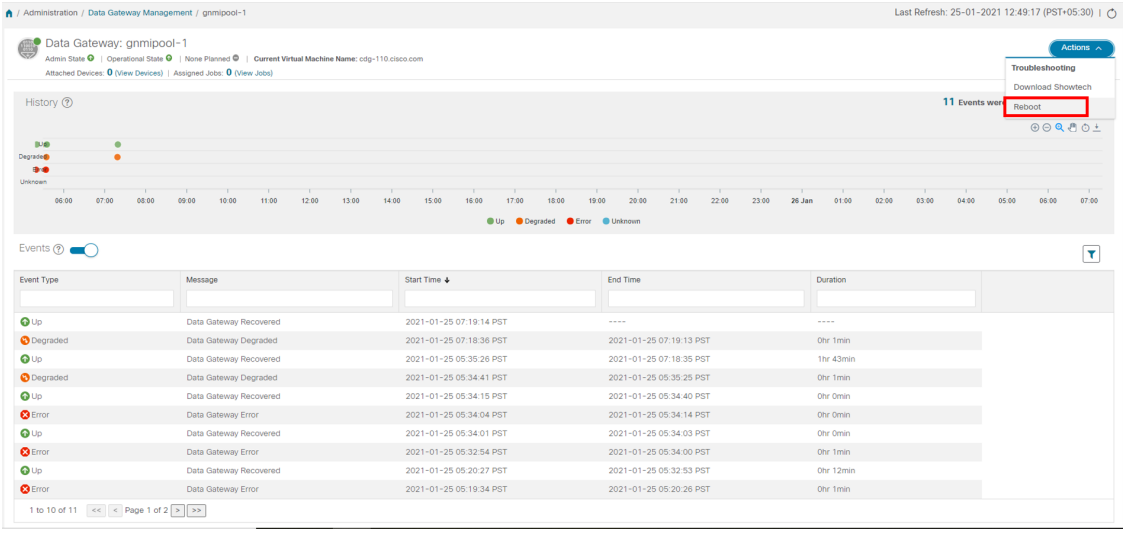
Follow the steps to reboot a Crosswork Data Gateway from Cisco Crosswork UI:

Note Rebooting the Cisco Crosswork Data Gateway pauses its functionality until it's up again.

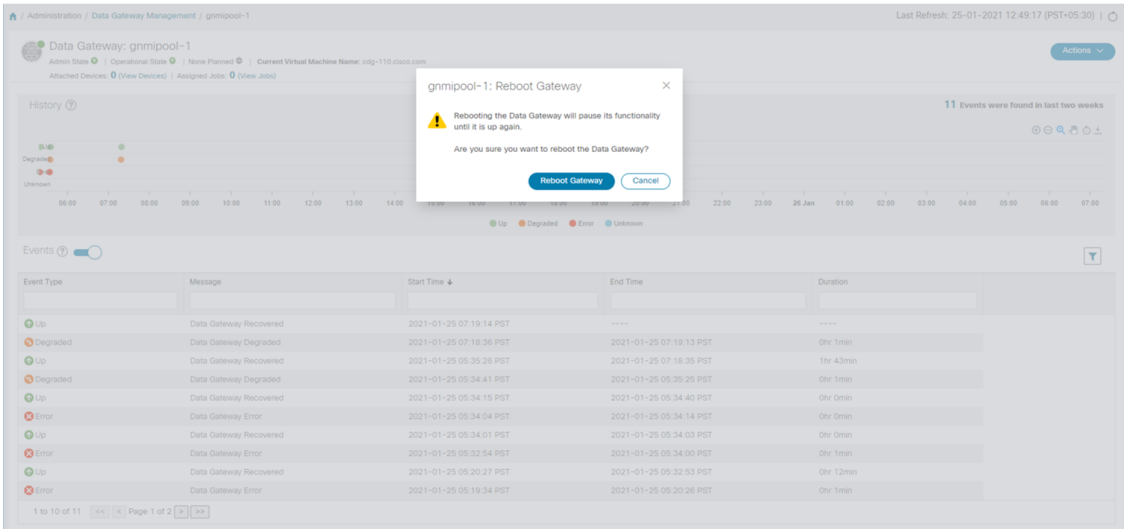
Step 1 Go to **Administration** > **Data Gateway Management** > **Data Gateways**.

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

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



Step 4 Click on **Reboot Gateway**.



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

Manage Cisco Crosswork Data Gateway Pools

A Cisco Crosswork Data Gateway pool ensures that your devices are managed and collections occur with minimal to no disruption.

You can use the Cisco Crosswork UI to create and configure pool(s) of Cisco Crosswork Data Gateway VMs. For information on how to create a pool, see Section: *Create a Cisco Crosswork Data Gateway Pool* in the *Cisco Crosswork Infrastructure 4.0 and Applications Installation Guide*.

Once you install a Cisco Crosswork Data Gateway VM and assign it to a to a pool, a virtual Cisco Crosswork Data Gateway gets created automatically and is visible under **Data Gateways** tab. You can then attach or detach devices to it and run collection jobs.

Note You cannot attach or detach devices to your physical Cisco Crosswork Data Gateway VM. They can only be attached or detached to a virtual Crosswork Data Gateway.

If a Cisco Crosswork Data Gateway VM goes down, Cisco Crosswork automatically replaces that VM with a spare VM from the pool. Devices and any existing collection jobs are auto-assigned from the failed VM to the spare VM. Once the VM that went down is repaired, it becomes a spare VM in the pool.

A pool has following states:

- **Protected**: All VMs are UP and there is at least one spare VM in the pool.
- **Not Protected**: All the spare VMs are DOWN and there are none available to replace a VM that is in use.
- **Limited Protection**: Some spare VMs are DOWN, but there is still at least one standby that is UP.
- **None Planned**: No spare VMs were added to the pool during pool creation.

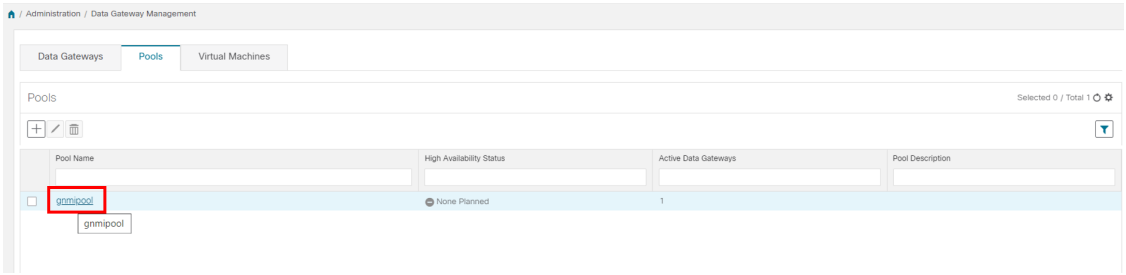
The pools can be managed from the **Pools** Tab. It can be accessed via **Administration** > **Data Gateway Management** > **Pools**.

View Pool Details

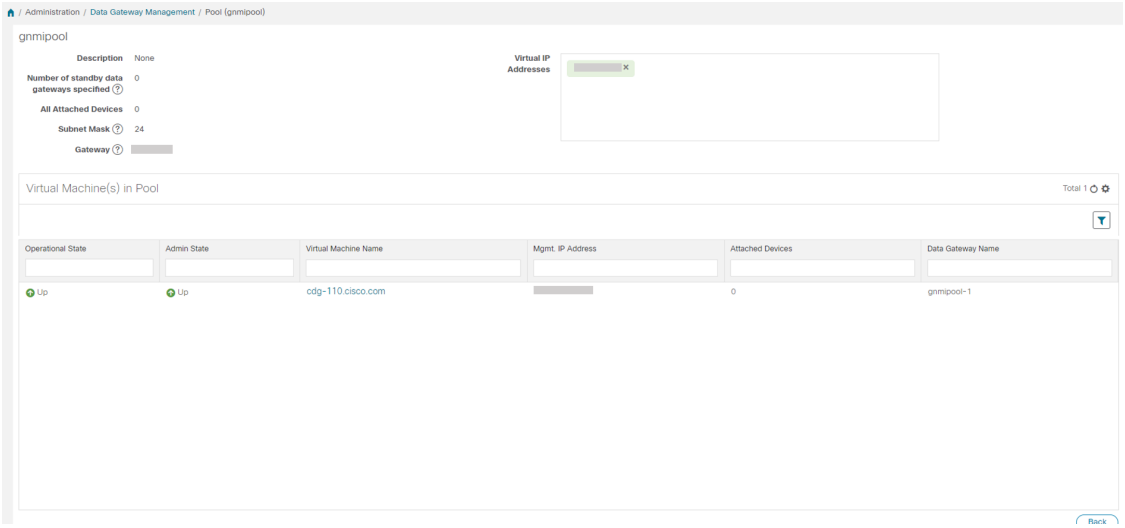
Follow the steps to view pool details:

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

Step 2 Click the pool name whose details you want to view.



The pool details page opens where you can view the details of the pool.



Note If more than one Crosswork Data Gateways in a pool have same Southbound IP address, for example, CDG2 (Active) as well as CDG1 (Standby) have exact same Southbound IP address. Then, reboot the standby Crosswork Data Gateway (CDG1 in this example), so that it will loose its southbound IP address once it comes up.

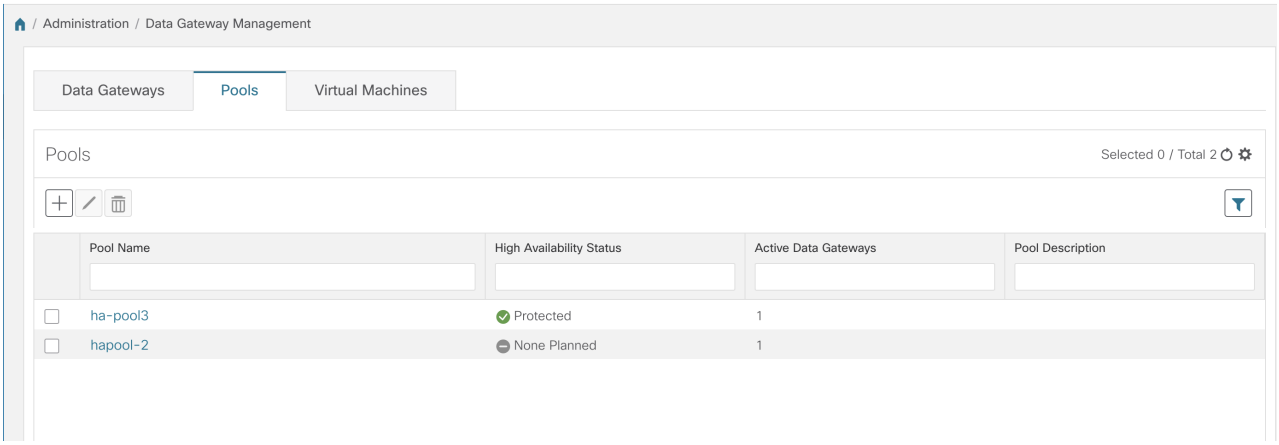
This happens in case of a failover scenario: CDG1 was active and CDG2 was standby. CDG1 had southbound IP address IP1. CDG1 went down, so Cisco Crosswork made CDG2 as new active and programmed same IP1 as southbound IP on CDG2.

CDG1 later restores connectivity as a standby, but it kept the same IP1 as southbound IP address. Therefore, resulting in both CDG1 and CDG2 having same IP1 as southbound IPs.

Edit a Cisco Crosswork Data Gateway Pool

Follow the steps to edit a Cisco Crosswork Data Gateway pool:

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

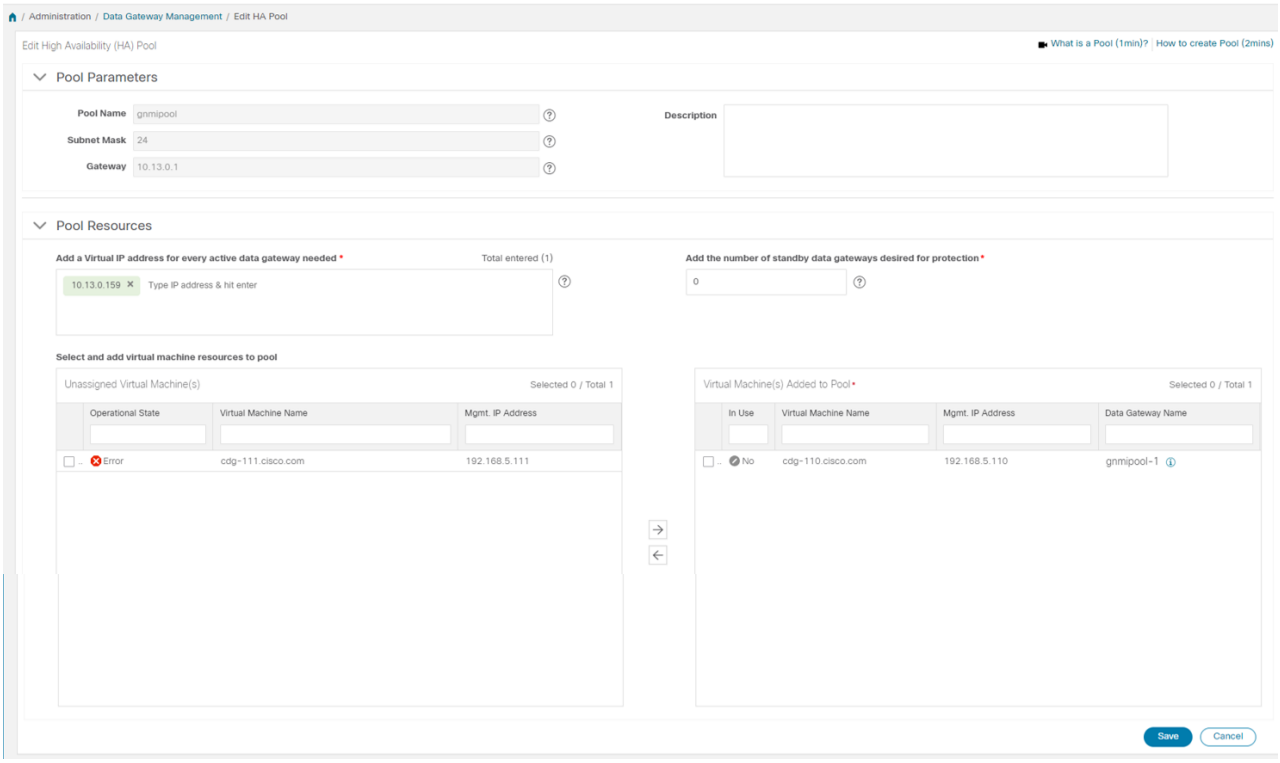


Step 2 From the list displayed in this page, select the pool which you wish to edit.

Step 3 Click button to open **Edit High Availability (HA) Pool** page.

Step 4 In the **Pool Resources** pane, modify the values for the following parameters:

Note You cannot edit the parameters in the **Pool Parameters** pane. If you need to make changes to these parameters, you must create a new pool with the desired values and then move the Cisco Crosswork Data Gateway VMs to that pool.



- **Add a Virtual IP address for every active data gateway needed**: A virtual IP address for every active Cisco Crosswork Data Gateway VM.

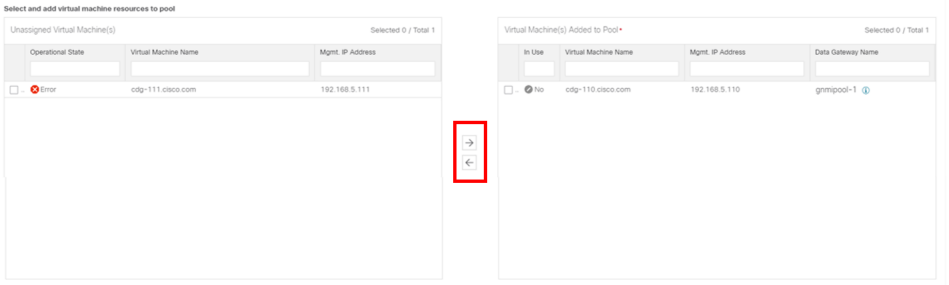
  Note Enter either IPv4 or IPv6 addresses. Combination is not allowed.

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

Step 5 Add or remove Cisco Crosswork Data Gateway VMs from the pool.

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

- To add a VM to the pool, select VMs from the **Unassigned Virtual Machine(s)** on the left and click right arrow to move these to the **Virtual Machine(s) Added to Pool**.
- To remove a VM from the pool, select VMs from the **Virtual Machine(s) Added to Pool** on the right and click left arrow to move these to the **Unassigned Virtual Machine(s)**.



Note A virtual Cisco Crosswork Data Gateway can be taken out of the pool only if all devices have been unmapped from it. Once virtual Cisco Crosswork Data Gateway is removed, the Crosswork Data Gateway VM that was backing the virtual Crosswork Data Gateway becomes a spare automatically.

Step 6 Click **Save**.

Delete a Crosswork Data Gateway Pool

Follow the steps to delete a pool:

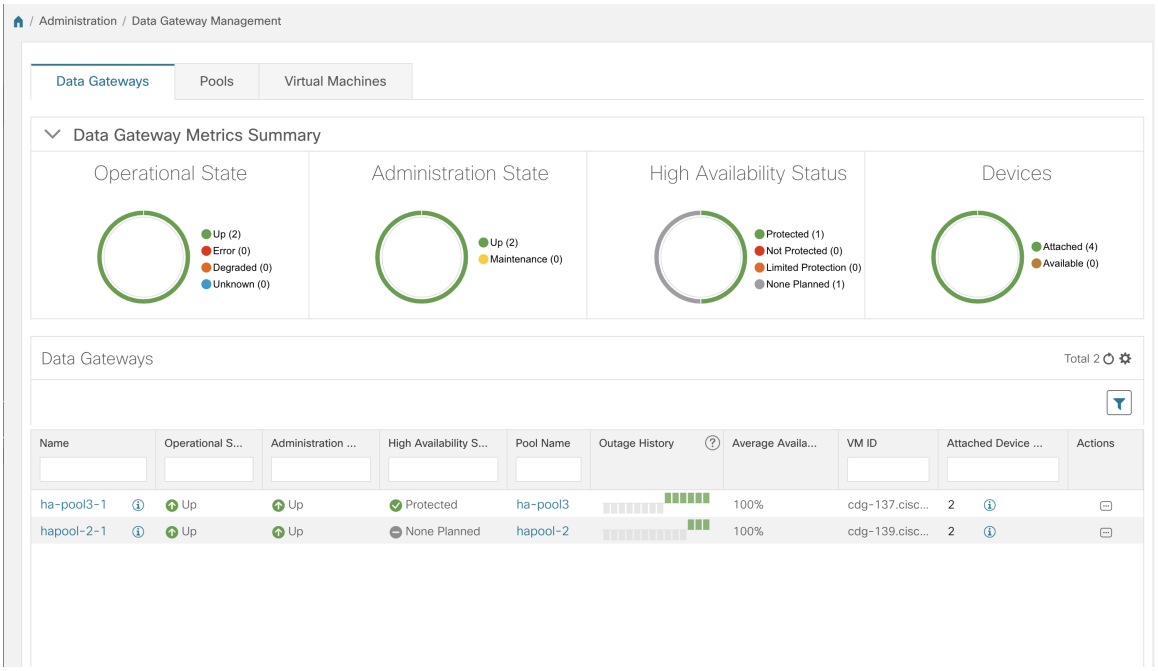
Step 1 From the main menu, choose **Administration** > **Data Gateway Management** and click **Pools** tab.

Step 2 Select the pool you want to delete and click button.

Step 3 Click **Delete** in the **Delete High Availability (HA) Pool** dialog box.

Manage Cisco Crosswork Data Gateway

The **Data Gateways** tab provides the following information:



Data Gateway Metrics Summary Pane

Summarizes the overall metrics of all Cisco Crosswork Data Gateway pools currently enrolled with Cisco Crosswork.

Item	Description
Operational State Tile	Shows the number of Cisco Crosswork Data Gateway in each operational state i.e., Up, Error, Degraded, and Unknown.
Administration State Tile	Shows the number of Cisco Crosswork Data Gateways in each adminstration state i.e., Up and Maintenance.
High Availability Status Tile	Shows the high availability status of the Cisco Crosswork Data Gateways.
Devices Tile	Shows the number of devices that are currently attached to a Cisco Crosswork Data Gateway and number of available devices.

Data Gateways Pane

Displays the following details for all Cisco Crosswork Data Gateway pools listed here.

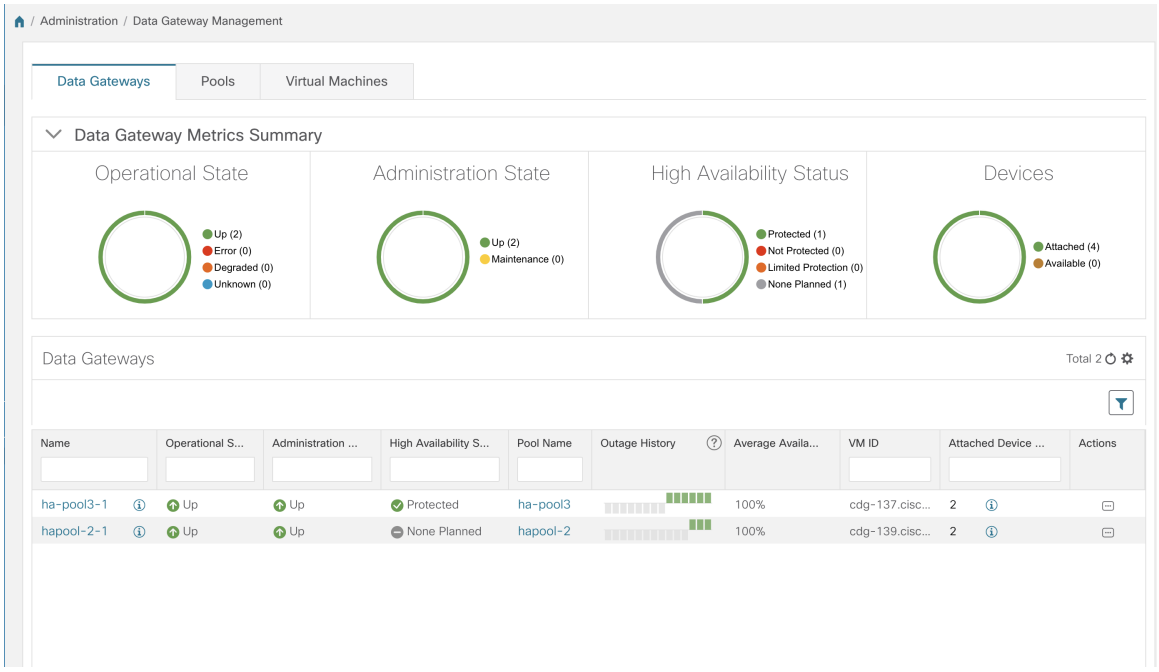
Item	Description
Name	Name of the Cisco Crosswork Data Gateway pool

Item	Description
Operational State	Operational state of the Cisco Crosswork Data Gateway VM that is currently associated with the Cisco Crosswork Data Gateway pool. • **Up**: The Cisco Crosswork Data Gateway VM is operational and all individual components are "OK". • **Error**: The Cisco Crosswork Data Gateway VM is either unreachable or all of its components are in Error state. • **Degraded**: The Cisco Crosswork Data Gateway VM is reachable but one or more of its components are in a state other than OK. • **Unknown**: The Cisco Crosswork Data Gateway's operational state is unknown as it has enrolled itself with Cisco Crosswork, but hasn't established a session yet.
Administration State	Adminstration state of the Cisco Crosswork Data Gateway VM. • **Up**: The VM is administratively up. • **Maintenance**: The Crosswork Data Gateway VM has been set to "Maintenance" mode by the user. There is no impact new or running jobs.
High Availability Status	A Cisco Crosswork Data Gateway can be in one of these states: • **Protected**: All VMs are UP and there is at least one spare in the pool. • **Not Protected**: All the spare VMs are DOWN and there are none available to replace a VM that is in use • **Limited Protection**: Some spare VMs are DOWN, but there is still at least one standby that is UP • **None Planned**: No spare VMs were added to the pool during pool creation

Item	Description
Pool Name	Name of the pool with which the Cisco Crosswork Data Gateway VM is associated.
Outage History	Shows past status changes of Cisco Crosswork Data Gateway VMs over a period of 14 days. Each tile represents the consolidated status of the corresponding Cisco Crosswork Data Gateway for a day. If the Cisco Crosswork Data Gateway was in error state at any time during that day, the tile will be the color representing Error. If the Data Gateway was not in Error but was in Degraded State anytime of the day, the tile will be the color for Degraded state. Finally, if the DG was neither Error nor Degraded but only UP, then the tile will be the color representing OK.
Average Availability	Value indicating the health of the Cisco Crosswork Data Gateway VM. This percentage is calculated as the time for which the Cisco Crosswork Data Gateway VM was available over the past 14 days or the time from when it was enrolled if less than 14 days. A higher average is an indication of good health.
VM ID	VM ID of the associated Cisco Crosswork Data Gateway VM.
Attached Device Count	Number of devices attached to the Cisco Crosswork Data Gateway pool.
Unique Identifier	Unique identifier of the Cisco Crosswork Data Gateway VM.
Actions	Allows you to manage devices associated with the Cisco Crosswork Data Gateway pool. • Attach a Device to Cisco Crosswork Data Gateway Pool • Detach a Device from Cisco Crosswork Data Gateway Pool • Move Devices between Cisco Crosswork Data Gateway Pools

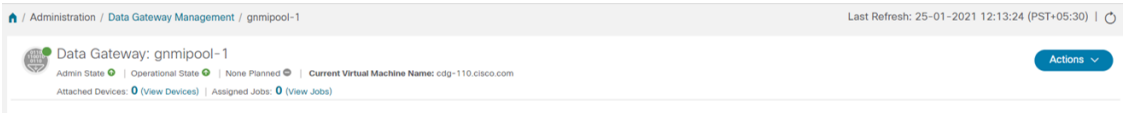
View Cisco Crosswork Data Gateway Details

To view details of a Cisco Crosswork Data Gateway, in the **Data Gateways** pane, click the Cisco Crosswork Data Gateway name. For example,



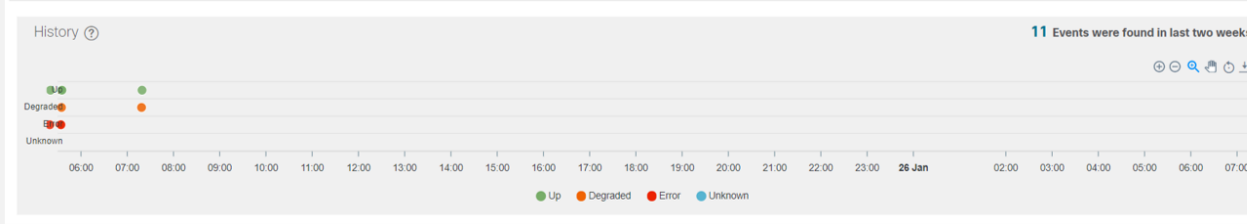
The Cisco Crosswork Data Gateway details page opens that shows the following details:

1. General Cisco Crosswork Data Gateway Details



- Name
- Admin state
- Operational state
- High availability state
- Current virtual machine name
- Attached devices (Click **View Devices** to see all attached devices.)
- Assigned jobs (Click **View Jobs** to see all associated jobs.)
- Actions (Provides troubleshooting options. See Troubleshoot Cisco Crosswork Data Gateway from Crosswork UI, on page 21.)

2. History



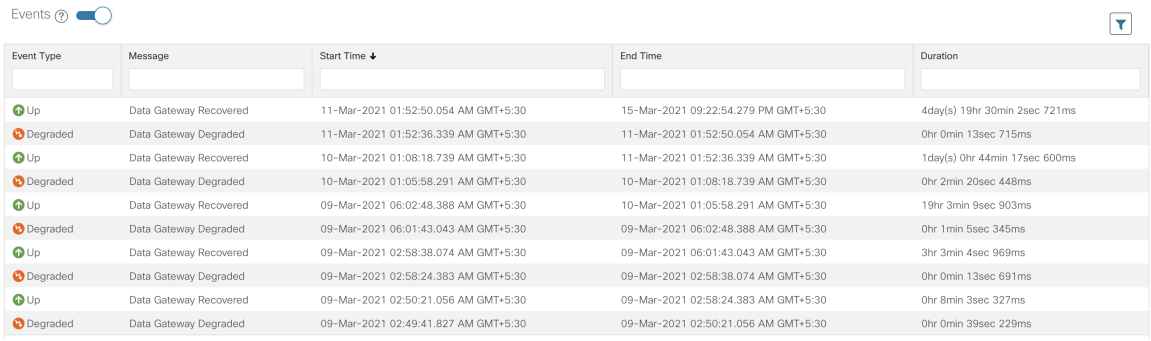
Shows the outage history of the Cisco Crosswork Data Gateway over 14 days. Cisco Crosswork maintains a list of all Cisco Crosswork Data Gateway transition state changes over the last 14 days. It includes information such as the timestamp, outage time and clear time.

Note In outage history, the operation state change data of a Cisco Crosswork Data Gateway for past 14 days and the current or latest state change event will have the current time as “end time” and “duration” in **Events** table as Cisco Crosswork cannot anticipate it. But, the end time is required for plotting the graph. Hence, the change can be seen in **Events** table only. See Events.

It also provides the following options that are available in the top right corner of the **History** pane.

- Zoom in
- Zoom out
- Selection zoom
- Panning
- Reset Zoom
- Download SVG and PNG of the history chart

3. Events



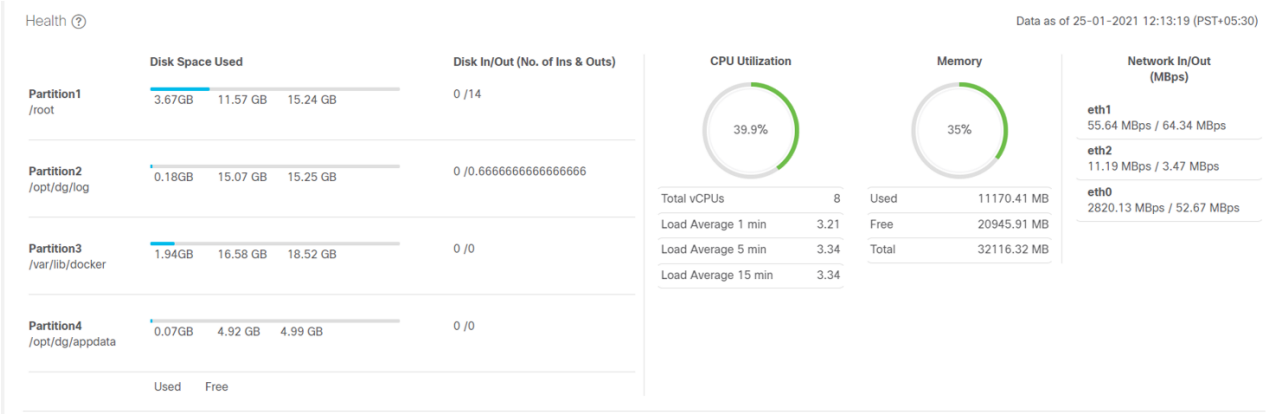
Event Type	Message	Start Time ↓	End Time	Duration
Up	Data Gateway Recovered	11-Mar-2021 01:52:50.054 AM GMT+5:30	15-Mar-2021 09:22:54.279 PM GMT+5:30	4day(s) 19hr 30min 2sec 721ms
Degraded	Data Gateway Degraded	11-Mar-2021 01:52:36.339 AM GMT+5:30	11-Mar-2021 01:52:50.054 AM GMT+5:30	0hr 0min 13sec 715ms
Up	Data Gateway Recovered	10-Mar-2021 01:08:18.739 AM GMT+5:30	11-Mar-2021 01:52:36.339 AM GMT+5:30	1day(s) 0hr 44min 17sec 600ms
Degraded	Data Gateway Degraded	10-Mar-2021 01:05:58.291 AM GMT+5:30	10-Mar-2021 01:08:18.739 AM GMT+5:30	0hr 2min 20sec 448ms
Up	Data Gateway Recovered	09-Mar-2021 06:02:48.388 AM GMT+5:30	10-Mar-2021 01:05:58.291 AM GMT+5:30	19hr 3min 9sec 903ms
Degraded	Data Gateway Degraded	09-Mar-2021 06:01:43.043 AM GMT+5:30	09-Mar-2021 06:02:48.388 AM GMT+5:30	0hr 1min 5sec 345ms
Up	Data Gateway Recovered	09-Mar-2021 02:58:38.074 AM GMT+5:30	09-Mar-2021 06:01:43.043 AM GMT+5:30	3hr 3min 4sec 969ms
Degraded	Data Gateway Degraded	09-Mar-2021 02:58:24.383 AM GMT+5:30	09-Mar-2021 02:58:38.074 AM GMT+5:30	0hr 0min 13sec 691ms
Up	Data Gateway Recovered	09-Mar-2021 02:50:21.056 AM GMT+5:30	09-Mar-2021 02:58:24.383 AM GMT+5:30	0hr 8min 3sec 327ms
Degraded	Data Gateway Degraded	09-Mar-2021 02:49:41.827 AM GMT+5:30	09-Mar-2021 02:50:21.056 AM GMT+5:30	0hr 0min 39sec 229ms

The **Events** table shows the following details for Cisco Crosswork Data Gateway events:

- Event Type
- Message indicating the reason for the status change
- Start Time
- End Time

- Duration

4. Health



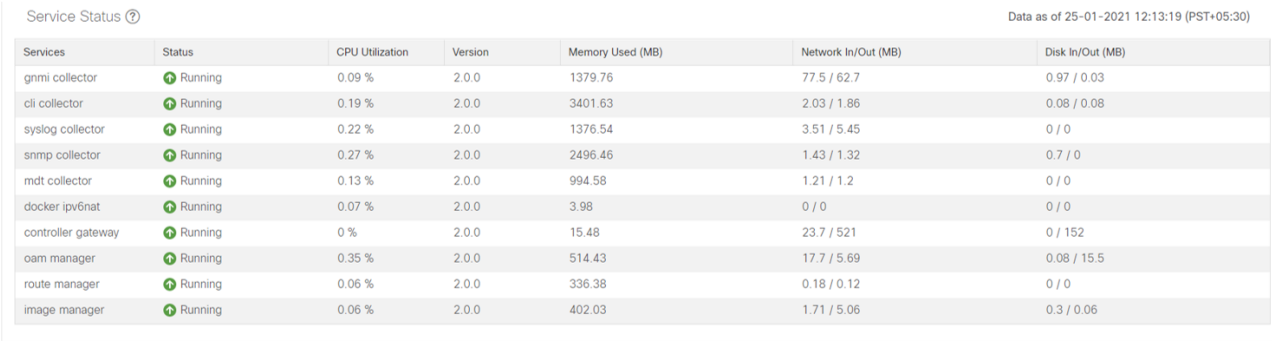
Shows the health information of the Cisco Crosswork Data Gateway. The timestamp in the top right corner is the timestamp when the last health data was collected. If the Cisco Crosswork Data Gateway is in a Error state or if the data is stale for any reason, the the timestamp label highlights that the data is old.

- Disk Space Used: Amount of the disk space used and available for different partitions.
- Disk In/Out: Number of read/write or input/output operations involving a disk for the partitions.

  This is a cumulative counter, not a delta time series.
- CPU Utilization: Amount of actively used CPU and total number of vCPUs.
- Memory: Amount of used, available, and total memory.
- Network In/Out: The amount of data sent/received in MB for NIC interfaces - eth1, eth2, and eth0.

  This is a cumulative counter, not a delta time series.

5. Service Status



Services	Status	CPU Utilization	Version	Memory Used (MB)	Network In/Out (MB)	Disk In/Out (MB)
gnmi collector	Running	0.09 %	2.0.0	1379.76	77.5 / 62.7	0.97 / 0.03
cli collector	Running	0.19 %	2.0.0	3401.63	2.03 / 1.86	0.08 / 0.08
syslog collector	Running	0.22 %	2.0.0	1376.54	3.51 / 5.45	0 / 0
snmp collector	Running	0.27 %	2.0.0	2496.46	1.43 / 1.32	0.7 / 0
mdt collector	Running	0.13 %	2.0.0	994.58	1.21 / 1.2	0 / 0
docker ipv6nat	Running	0.07 %	2.0.0	3.98	0 / 0	0 / 0
controller gateway	Running	0 %	2.0.0	15.48	23.7 / 521	0 / 152
oam manager	Running	0.35 %	2.0.0	514.43	17.7 / 5.69	0.08 / 15.5
route manager	Running	0.06 %	2.0.0	336.38	0.18 / 0.12	0 / 0
image manager	Running	0.06 %	2.0.0	402.03	1.71 / 5.06	0.3 / 0.06

Cisco Crosswork Data Gateway comprises of various containerized services running on an Ubuntu VM. Its overall health depends on health of each containerized service. Cisco Crosswork also displays the health information of these individual container services running on the Cisco Crosswork Data Gateway and their resource consumption:

Note The resource consumption data displayed here is from docker statistics. This is higher than the actual resource consumed by the containerized service.

- Service: Name of the service
- Service Status: Status of the service i.e., Running, Degraded, or Error.
- CPU Utilization: Percentage of actively utilized CPU by the service.

  CPU utilization is reported against maximum of 800% (8vCPUs) for Standard Profiles and 1600% (16vCPUs) for Extended Profiles.
- Version: Version of the service deployed.
- Memory Used: Amount of memory being used by the service in MB.
- Network In/Out: The amount of data sent/received in MB by the service over its interface.

  This is a cumulative counter, not a delta time series.
- Disk In/Out: Number of read/write or input/output operations that the service has done involving a disk.

  This is a cumulative counter, not a delta time series.

Attach a Device to Cisco Crosswork Data Gateway Pool

For optimal performance, it is recommended that attaching devices to a Cisco Crosswork Data Gateway pool should be done in batches of 300 devices or fewer.

Note A device can be attached to only one Cisco Crosswork Data Gateway pool.

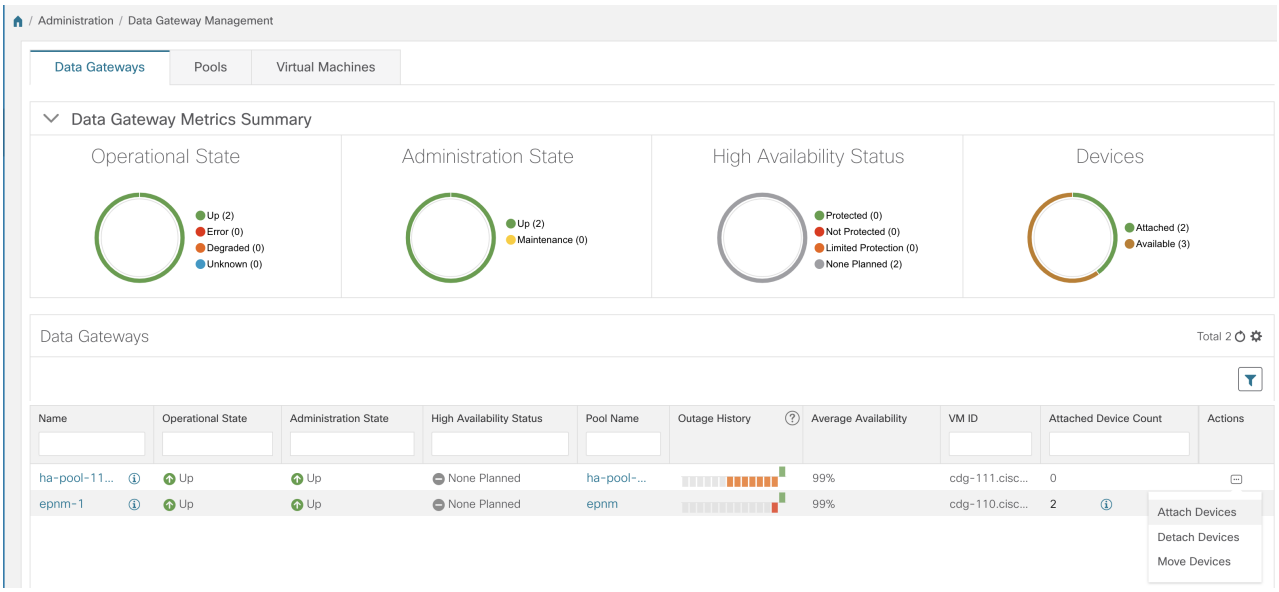
Follow the steps below to attach device(s) to a Cisco Crosswork Data Gateway pool:

Before you begin

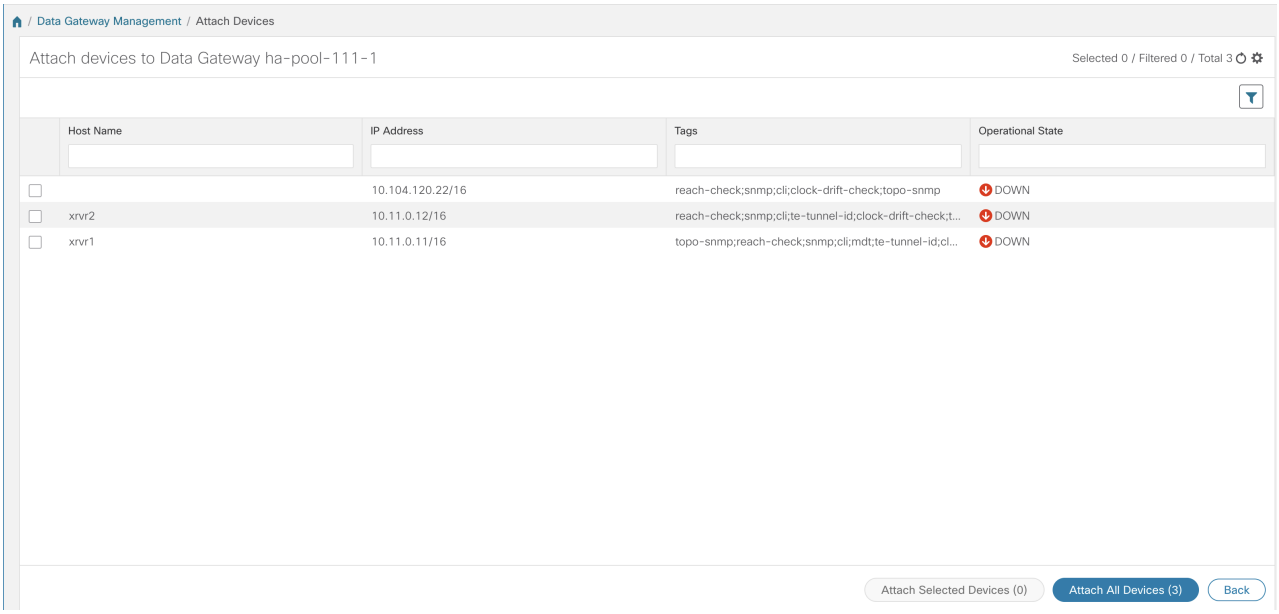
Ensure that both the Admin state and Operational state of the Cisco Crosswork Data Gateway to which you want to attach devices is UP. Only then proceed with attaching devices.

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

Step 2 For the Cisco Crosswork Data Gateway pool to which you want to attach devices, under **Actions** column, click ··· and select **Attach Devices**.



The **Attach Devices** window opens showing all the devices available for attaching.



Step 3 To attach all the devices, click **Attach All Devices**. Otherwise, select the devices you want to attach and click **Attach Selected Devices**.

Step 4 In **Confirm - Attach Devices** dialog box, click **Attach**.

To verify if the devices were attached to the VM, check the **Attached Device Count** under the **Data Gateways** pane. Click on the *i* icon next to the attached device count to see the list of all devices attached to the selected Cisco Crosswork Data Gateway pool.

Detach a Device from Cisco Crosswork Data Gateway Pool

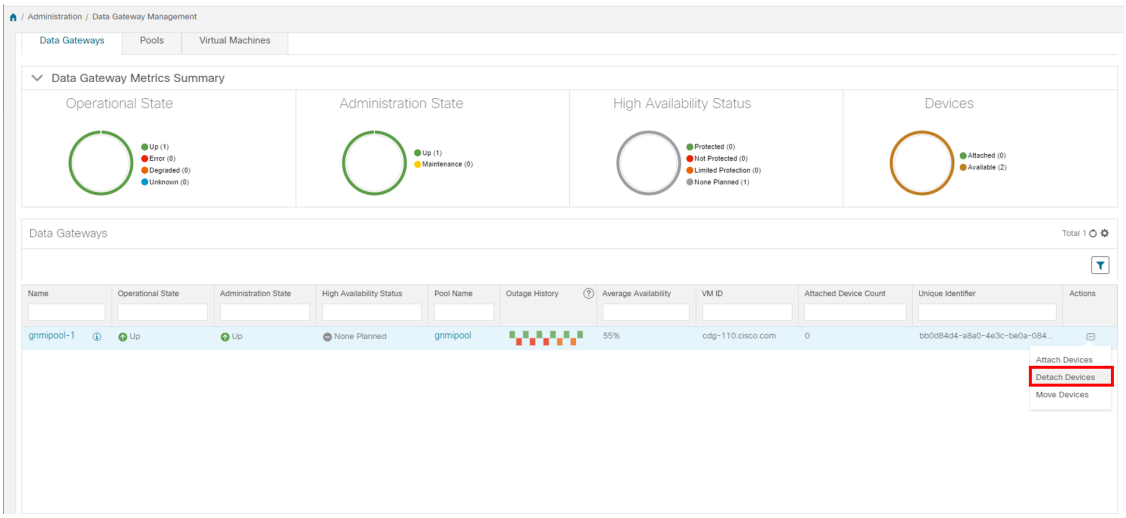
Follow the steps below to detach a device from a Crosswork Data Gateway:

Before you begin

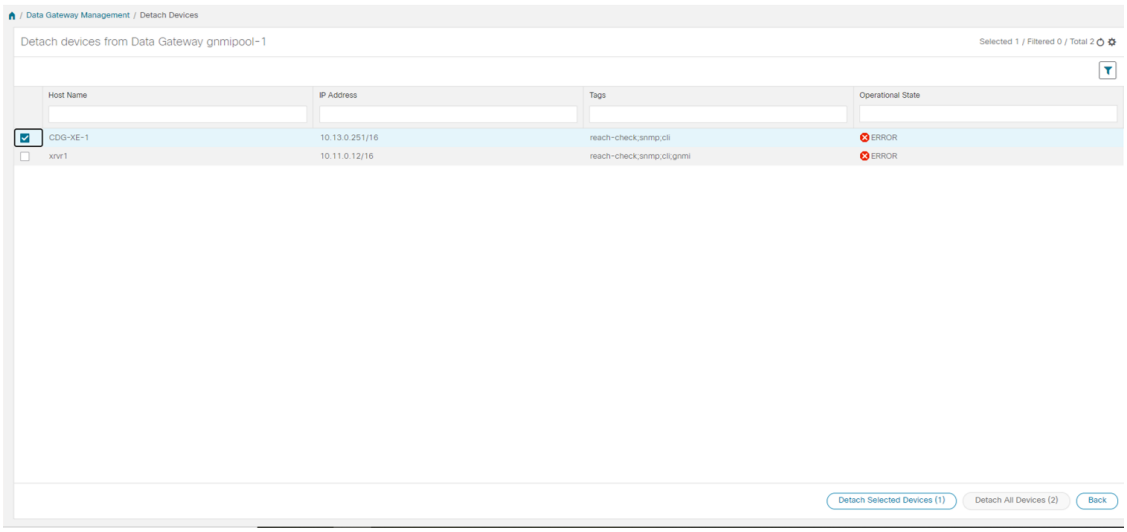
If you do not want to lose the jobs submitted for the device you wish to delete, it is reccomended that you move the device to another Cisco Data Gateway. Detaching the device from Cisco Crosswork Data Gateway will delete the jobs corresponding to the device.

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

Step 2 For the Crosswork Data Gateway from which you want to detach devices, under **Actions** column, click ··· and select **Detach Devices**.



The **Detach Devices** window opens showing all attached devices.



Step 3 To detach all the devices click **Detach All Devices**. Otherwise, select the devices you want to detach and click **Detach Selected Devices**.

Step 4 In **Confirm - Detach Devices** dialog box, click **Detach**.

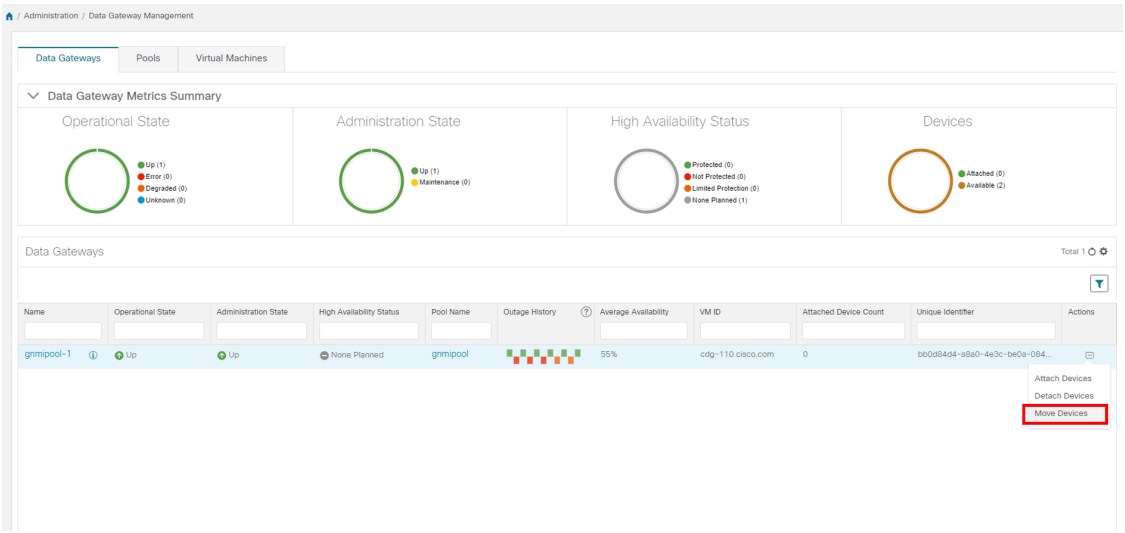
Move Devices between Cisco Crosswork Data Gateway Pools

It is highly recommended that you move devices between Data Gateways belonging to the same pool although you can move devices from a Data Gateway to any Data Gateway.

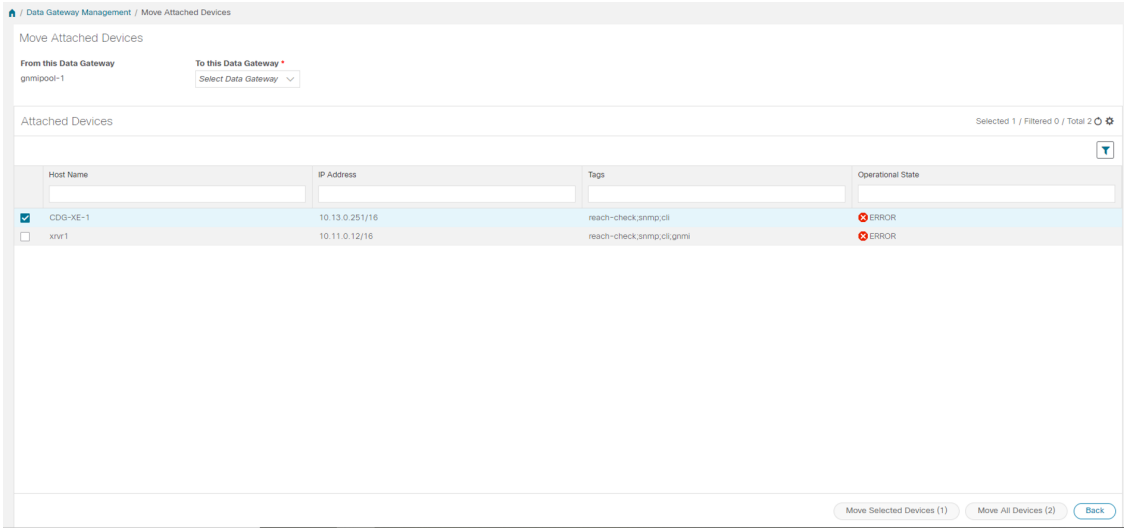
Follow the steps to move devices from one Crosswork Data Gateway to another:

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

Step 2 For the Crosswork Data Gateway from which you want to move devices, under **Actions** column, click ⋯ and select **Move Devices** .



The **Move Attached Devices** window opens showing all the devices available for moving.



Step 3 From the **To this Data Gateway** dropdown, select the data gateway to which you want to move the devices.

Step 4 To move all the devices, click **Move All Devices**. Otherwise, select the devices you want to move and click **Move Selected Devices**.

Step 5 In **Confirm - Move Devices** dialog box, click **Move**.

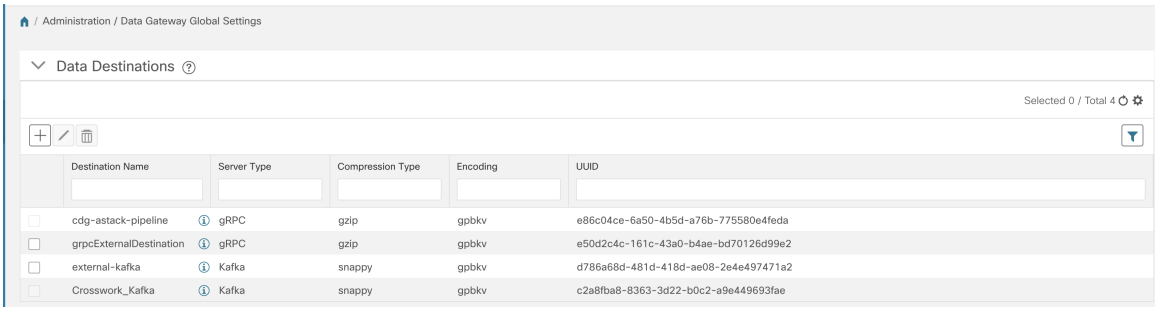
Manage Data Destinations

Cisco Crosswork allows you to create external data destinations that can be used by collection jobs to deposit data.

In Cisco Crosswork UI, from the **Data Destinations** pane, you can add a new data destination, update the settings configured for an existing data destination, and delete a data destination.

It can be accessed by going to **Administration** > **Data Gateway Global Settings**. This table shows approved data destinations that can be used by the collection jobs to deposit their data. Kafka or gRPC servers can be added as new data destinations for REST API created collection jobs.

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



Data Destination pane displays the following details of the data destinations:

Field	Description
Destination Name	Name of the data destination.
Server Type	Server type of the data destination i.e., external Kafka or gRPC server.
Compression Type	Compression type being used for the data destination.
Encoding	Encoding type being used for the data destination.
UUID	Unique identifier for the data destination. This ID is automatically generated by Cisco Crosswork when an external data destination is created and is a required parameter for collection job creation.

It also allows you to do the following:

- Add/Edit a Data Destination, on page 40
- View Data Destination Details, on page 45
- Delete a Data Destination, on page 45

Add/Edit a Data Destination

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

Note

- 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 place .
- You can secure the communication channel between Cisco Crosswork and the specified data destination i.e., either Crosswork Kafka or external Kafka. **Step 6** of the below procedure explain how to do that.

  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 will need 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.

- Create the Kafka topics prior to submitting the job to Cisco Crosswork. Depending on external Kafka and how topics are managed in that external Kafka, Cisco Crosswork logs may show the exception listed when and if the topic does not exist at the time of dispatching the collected data to that specific external Kafka / topic. This could be either due to the topic is not yet created or topic got deleted prior to the completion of the requested collection job and dispatching the collected data.

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

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:

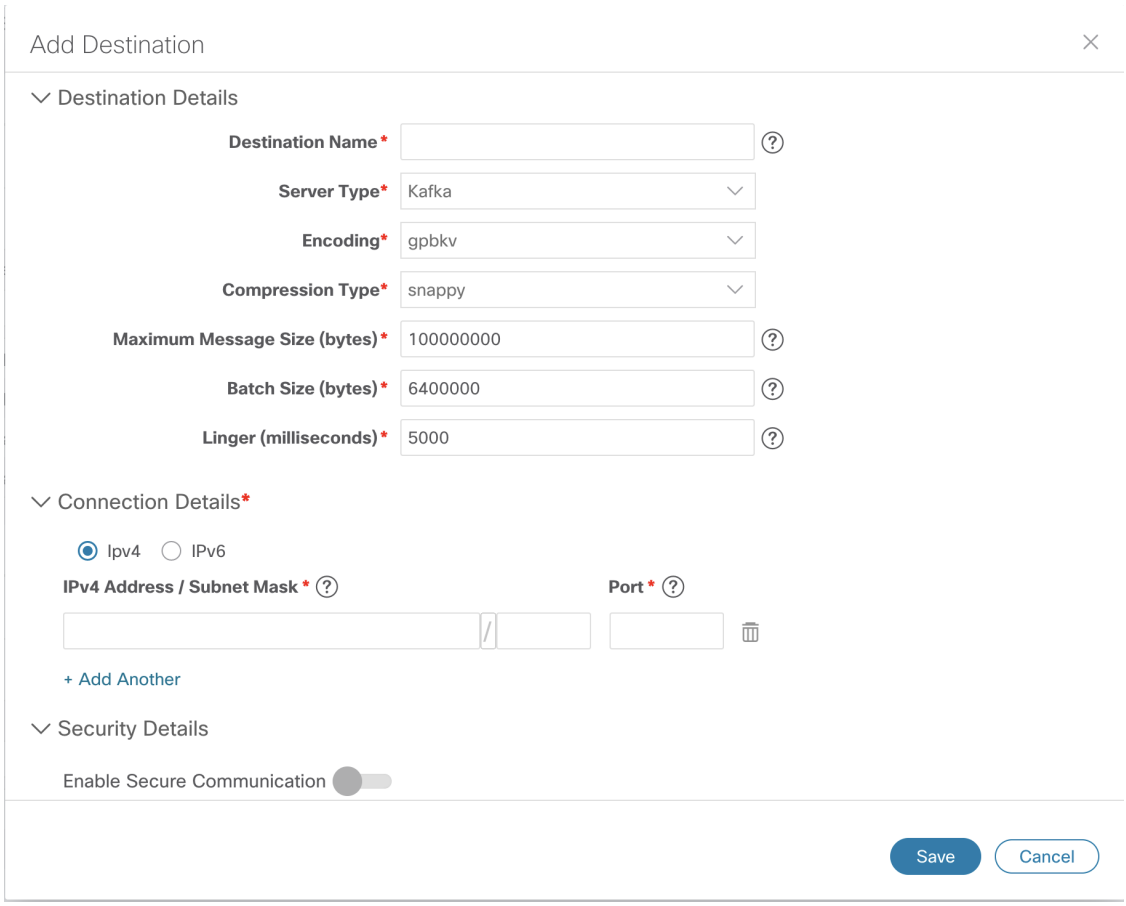
  Note Refer your Kafka documentation for description and usage of these properties as this explanation is out of scope of this document.

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

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

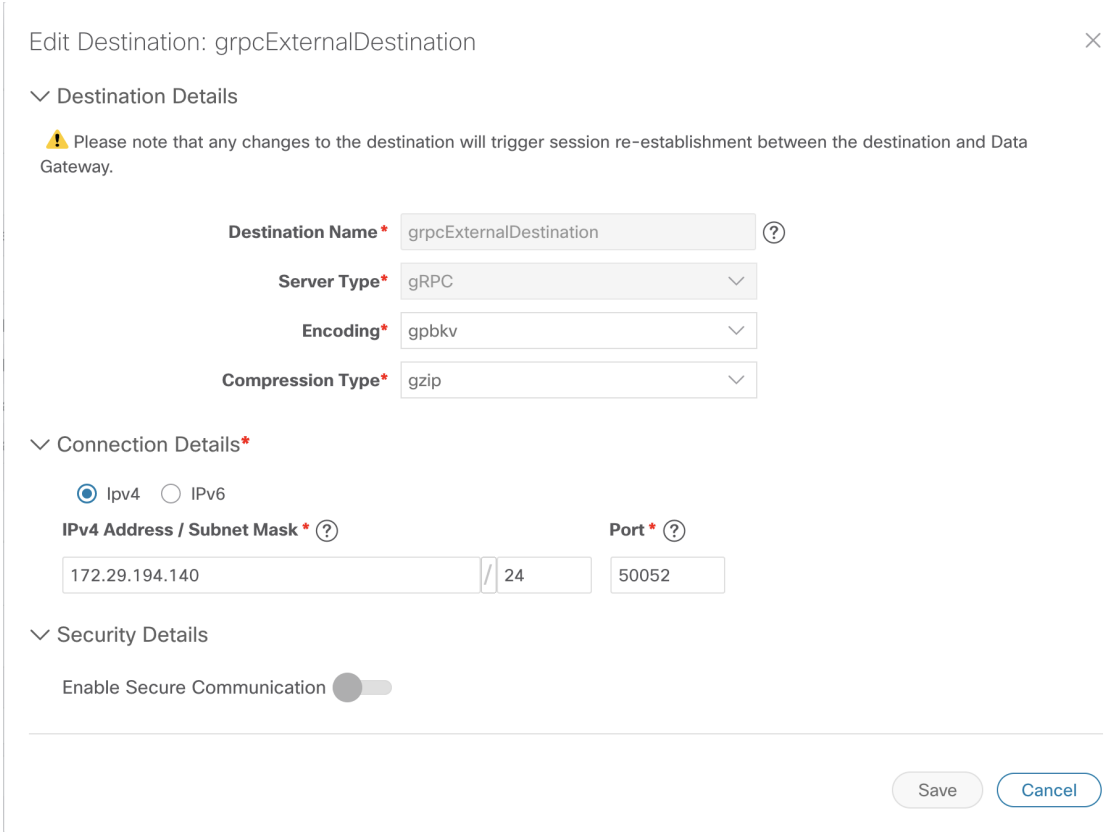
Step 1 From the main menu, choose **Administration** > **Data Gateway Global Settings**.

Step 2 From **Data Destinations** pane, click + button. The **Add Destination** page opens.



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

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



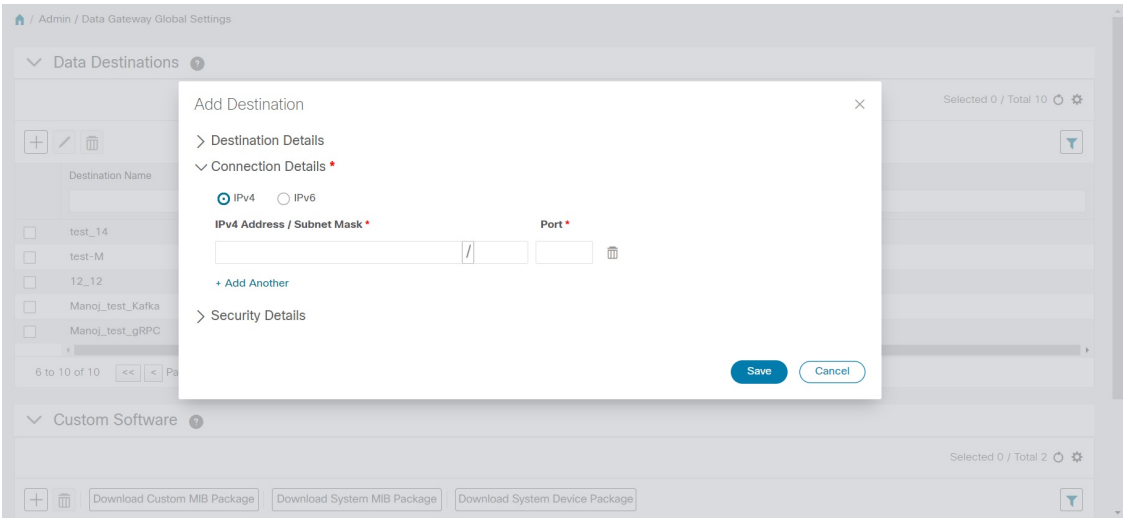
Step 3 Enter or modify the values for the following parameters:

Field	Value
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.
Server Type	From the drop down, select the server type of your data destination (Kafka/gRPC).
Encoding	From the drop down, select the encoding (json/gpbkv).
Compression Type	From the drop down, select the compression type: Compression types supported for Kafka are snappy, gzip, lz4, zstd, and none) **Note** zstd compression type is supported only for Kafka 2.0 or higher. Compression types supported for gRPC are snappy, gzip, and deflate.

Field	Value
Maximum Message Size (bytes) (Kafka-only)	Enter the maximum message size in bytes. • **Default Value**: 100000000 bytes/ 30 MB • **Min**: 1000000 bytes/1 MB • **Max**: 100000000 bytes/ 30 MB
Batch Size (bytes) (Kafka-only)	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
Linger (milliseconds) (Kafka-only)	Enter the required linger time in milliseconds. • **Default Value**: 5000 ms • **Min**: 0 ms • **Max**: 5000 ms

For telemetry based collection, it is recommended to use the destination settings of **Batch size** as 16384 bytes and **linger** as 500 ms, for optimal results.

Step 4 Select a protocol from the **Connection Details** options. IPv4 and IPv6 are supported.



Step 5 Complete the **Connection Details** fields as described in the following table. The fields displayed will vary with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
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.
IPv6	Enter the required **IPv6 Address/ Subnet Mask**, and **Port**. You can add multiple IPv6 addresses by clicking **+ Add Another**. IPv6 subnet mask ranges from 1 to 128 and port range from 1024 to 65535.

Step 6 (Optional) To connect securely to the data destination, enable the **Enable Secure Communication** option under **Security Details**.

Step 7 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 217 for more information.

Note If you do not add the certificate for the data destination after enabling the **Enable Secure Communication** option, Cisco Crosswork still connects to the destination in non-secure mode for any collection jobs.

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. Cisco Crosswork displays the details as 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 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**.

Step 2 Select the Data destination(s) you want to delete and click button.

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

Manage Custom Software Packages

Cisco Crosswork allows you to add MIB files, device model definitions by means of custom software packages.

Device packages enable Crosswork to retrieve CLI and SNMP data and convert it into XML for third-party devices.

You can add three types of custom software packages:

1. **CLI Device Package**: You may want to use CLI-based KPIs to monitor device health indicator 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.

   Note Before migrating to Cisco Crosswork 4.0, ensure that you back up CLI Device Package. See Migrate CLI Device Packages, on page 49.

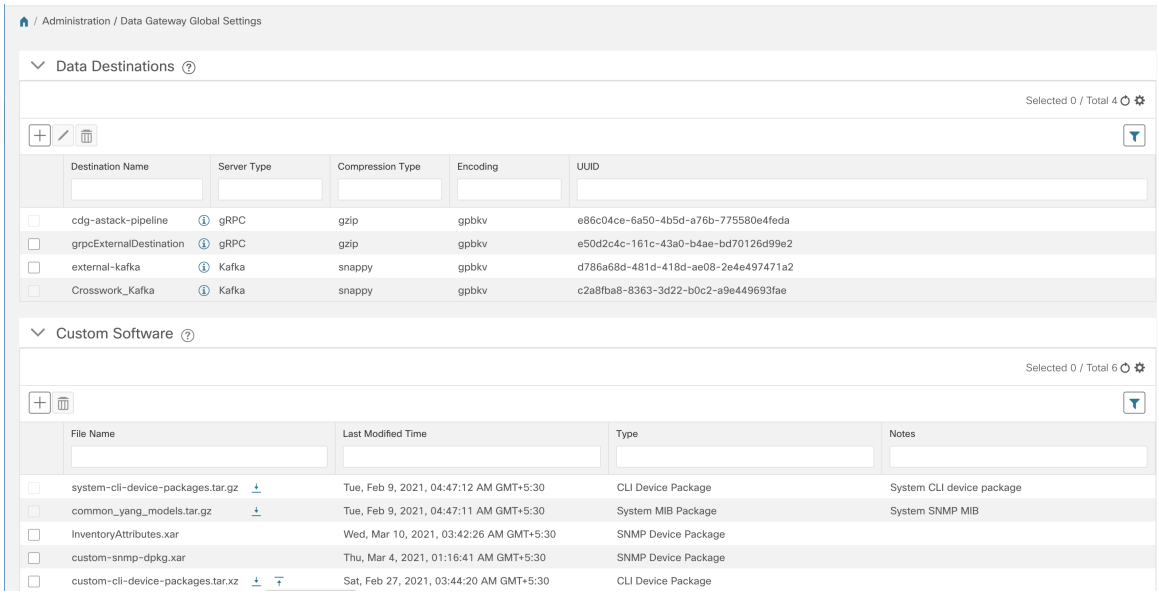
2. **Custom MIB Packages**: Custom MIBs and device packages can be specific to third-party devices or be used to filter the collected data or format it differently for Cisco devices. These are editable by the user. All custom SNMP MIB packages along with YANG models should be included in file custom-mib-packages.tar.xz.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

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

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

System Device and MIB Packages are bundled in the Crosswork software and are automatically downloaded to the system instances. These are *not* modifiable by the user. Custom Device Packages can be uploaded by the user, for example, when required for interfacing with third-party devices.

The Customer software pane can be accessed via **Adminstration** > **Data Gateway Global Settings**.



Custom Software pane displays the following details for the available custom software packages:

Field	Description
File Name	Name of the custom software package.
Last Modified Time	Time when the file was last (re)uploaded.
Type	Type of the custom software package.
Notes	Notes related to the custom software package entered by the user while importing the package.

It also allows you to perform the following operations:

- Add a Custom Software Package, on page 47
- Download Custom Software Packages, on page 47
- Delete a Custom Software Package, on page 49

Download Custom Software Packages

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

Add a Custom Software Package

The scope of the usage of this feature is limited to Crosswork Change Automation and Health Insights only.

1. You can upload one or more xar file in a single device package tar.gz file.
2. When uploading new MIBs as a part of Custom MIB Package, it's required that those new MIBs files are loadable within collectors along with existing System MIB files i.e., all dependencies in the files get

resolved properly. An offline tool and procedure are available for you to ensure that new MIBs can be uploaded properly.

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

3. Cisco Crosswork 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 software package TAR file has just the device package folders and none of the parent folder or hierarchy of folders as part of the TAR file. If not imported properly, Cisco Crosswork throws exceptions when executing the job with custom device package.
5. Cisco Crosswork does not validate the files being uploaded other than checking the file extension.
6. To update the existing Custom CLI Device Package, click the upload icon next to the File name in the table

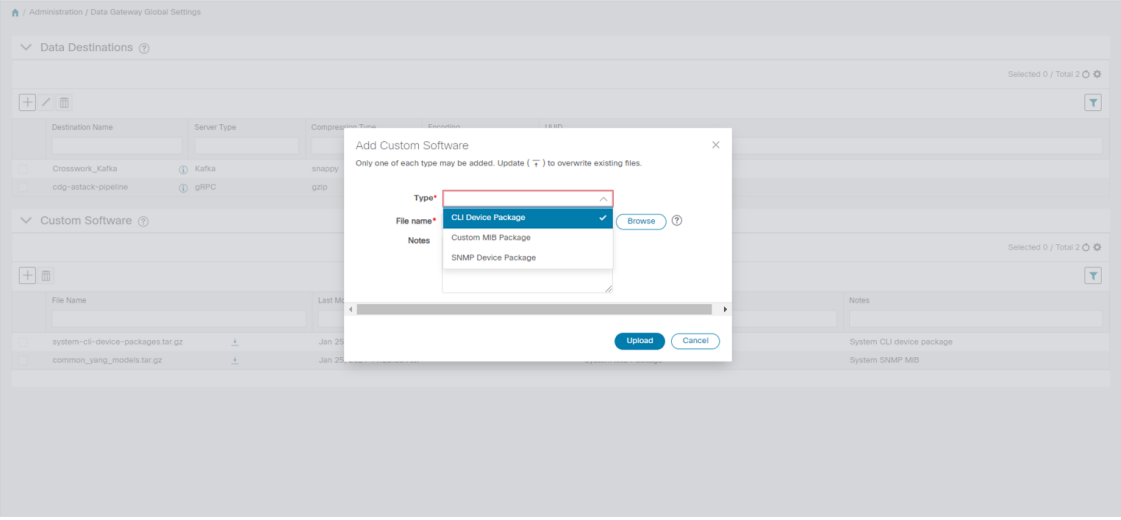
Follow these steps to upload a custom software package:

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

Step 2 In **Custom Software** pane, click ⊞ button.

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

Step 3 In the **Add Custom Software** pop up, select the type of custom software package you want to import from the **Type** dropdown.



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

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

Step 6 Click **Upload**.

What to do next

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

Delete a Custom Software Package

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

Follow the steps to delete a custom software package:

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

Step 2 From the **Custom Software** pane, select the custom package you want to delete and click button.

Step 3 In the **Delete Custom Software** pop up, click **Delete** to confirm.

Migrate CLI Device Packages

Back up CLI Device Packages

To take a back up of the existing CLI device packages:

1. Download the CLI device package (.xar files) to your local machine.
2. Delete the CLI Device Package from Cisco Crosswork.

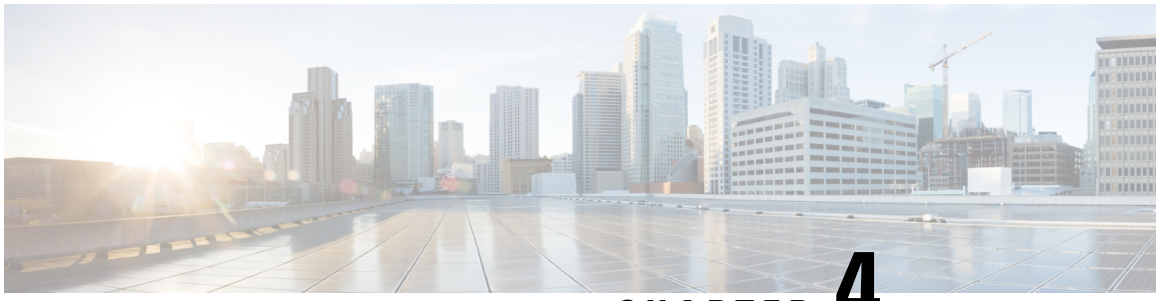
Restore CLI Device Package

After migrating to Cisco Crosswork 4.0, follow these steps to restore the CLI Device Packages before starting any collection jobs. To do this:

1. Create the `custom-cli-device-packages.tar.xz` file from the .xar files you had backed up before migration in the following format:

```
custom-cli-device-package
├── xar
│   ├── function1.xar
│   └── function2.xar
└── yang
├── supported_yang-1.yang
├── supported_yang-2.yang
└── supported_yang-3.yang
```

2. Add the `custom-cli-device-packages.tar.xz` file in **Administration > Data Gateway Global Settings > Custom Packages** pane. Refer to the Section: Add a Custom Software Package, on page 47.



CHAPTER 4

Manage Collection Jobs

This section contains the following topics:

About Collection Jobs

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

You can collect more than one type of data at a time by using separate collection jobs.

For each collection job you create, Cisco Crosswork Data Gateway executes the collection request and deposits the collected data in the preferred data destination(s).

Cisco Crosswork Data Gateway lets you create following types of collection jobs:

- CLI Collection Job, on page 52
- SNMP Collection Job, on page 53
- MDT Collection Job, on page 61
- gNMI Collection Job, on page 62
- Syslog Collection Job, on page 70

Note

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

Smart Licensing for Active Collection Jobs

To be able to create collection jobs that can forward data to third-party destinations, ensure that the following Smart Licensing requirements are met:

1. From the main menu, go to **Administration > Application Management > Smart License** and select the Cisco Crosswork application.
2. 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 you have not exceeded the device count in the external collection jobs

In the Evaluation period (**Registration Status** is Unregistered and the **License Authorization Status** is **Evaluation mode**), you will be able to create collection jobs until the evaluation period expires. After this, you must register with Cisco Smart Software Manager (CSSM) to use licensed features. See Section: Manage Licenses, on page 225 for more information.

If you do not register with Cisco Smart Software Manager (CSSM) after the Evaluation period has expired, you will not be able to create collection jobs. However, you can still view and delete any collection jobs.

CLI Collection Job

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

Note

- The initial status for all the collection jobs in the UI is Unknown. Upon receiving a CLI collection job, Cisco Crosswork Data Gateway performs basic validations on it. If the collection job is valid, its status changes to Successful, else it changes to Failed.
- Device should not have any banner configuration for CLI collection to work properly. Please refer to device documentation on how to turn this off.
- The value of **Cadence** is in seconds. It should be set either to 0 to indicate the sensor configured to be collected only once.

  OR

  It should be >= 60 (i.e. at least 1 minute) up to 2764800 seconds (i.e. at most 32 days) max, indicating how frequently configured sensor data should be collected.
- When collection from a device is skipped due to previous execution still in progress, Cisco Crosswork Data Gateway raises a warning log. No alert is generated for this scenario.

Following is a sample of CLI collection job. For more information, see API documentation on Cisco DevNet.

```
{
  "collection_job": {
    "application_context": {
```

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

SNMP Collection Job

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

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

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

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

The device packages can be imported into the Crosswork Data Gateway VM as described in Section Add a Custom Software Package, on page 47.

The following SNMP versions are supported:

- SNMPv1
- SNMPv2c
- SNMPv3

The table below lists supported privacy protocols and the value that needs to be given in the collection payload for SNMP and SNMP Trap collection jobs:

Protocol	SNMP Collection Payload	SNMP Trap Collection Payload
aes	AES	N/A
des56	DES	N/A
3des	3DES	N/A
aes 128	AES128	N/A
aes 192	AES192 or CiscoAES192(Cisco specific)	N/A
aes 256	AES256 or CiscoAES256(Cisco specific)	N/A

Note

- The initial status for all the collection jobs in the UI is Unknown. Upon receiving a SNMP collection job, Cisco Crosswork Data Gateway performs basic validations on it. If the collection job is valid, its status changes to Successful, else it changes to Failed.
- The value of **Cadence** is in seconds. It should be set either to 0 to indicate the sensor configured to be collected only once.

  OR

  It should be >= 60 (i.e. at least 1 minute) up to 2764800 seconds (i.e. at most 32 days) max, indicating how frequently configured sensor data should be collected.
- When collection from a device is skipped due to previous execution still in progress, Cisco Crosswork Data Gateway raises a warning log. No alert is generated for this scenario.
- For SNMP v1/v2c, if the device details (such as host or community string) are incorrect in the payload, Cisco Crosswork Data Gateway ignores the traps received from the device and logs a WARN message.
- Only SNMPv1 and SNMPv2c versions are supported for SNMP traps
- In case of SNMP v3, if the device details (such as auth, priv, and security name details) are incorrect in the payload, Cisco Crosswork Data Gateway filters it out and hence, does not receive the trap. Thus, no WARN message is logged.

Sample Configurations on Device:

Table 2:

Version	Command	To...
V1	`snmp-server group <group_name> v1` `snmp-server user <user_name> <group_name> v1`	Define the SNMP version, user/user group details.

	`snmp-server host <host_ip> traps <community_string> udp-port 1062`
	For example,
	`snmp-server host a.b.c.d traps test udp-port 1062`
		Define the destination to which trap data must be forwarded.

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

Version	Command	To...

V3	`snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name>`
	
	`snmp-server view <user_name> 1.3 included`
		Define the SNMP version, user/user group details.

	`snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password>`
	
	`snmp-server host <host_IP> traps version 3 priv <user_name> udp-port 1062`
		Define the destination to which trap data must be forwarded.

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

The SNMP Collector supports the following operations:

- SCALAR
- TABLE
- MIB_WALK
- TRAP
- DEVICE_PACKAGE

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 very high. It's not recommended to use **snmpRequestTimeoutMillis** unless you are absolutely certain that your device response time is very high.

The value for snmpRequestTimeoutMillis should be specified in milliseconds:

Default value is 1500 milliseconds

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 are handled in a similar manner. Trap listeners listen on a port and then dispatch data to recipients (based on their topic of interest).

Cisco Crosswork Data Gateway supports three types of 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 notifications (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)

Note

- Device should have been pre-configured by the traps.
- Cisco Crosswork Data Gateway listens on UDP port 1062 for Traps.
- 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 89

On receiving a trap, Cisco Crosswork Data Gateway does the following validations:

1. Check if any collection job is created for the device.
2. Checks the trap version and community string.
3. For SNMP v3, validates for user auth and priv protocol and credentials.

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

Cisco Crosswork Data Gateway supports the following YANG paths:

sensor path	purpose
snmp-trap-raw-oper:traps/data	To get all the traps pushed from the device without any filter.
IF-MIB:notifications	To get all the IF-MIB notifications (ex: linkUp, linkDown, etc.)
ISIS-MIB:notifications	To get all the ISIS-MIB notifications.

sensor path	purpose
SNMPv2-MIB:notifications	To get all the snmpV2 Mib notifications.

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

As per the current implementation, in case of an SNMP Trap collection job, all traps are sent to the specified data destination even if the SNMP Trap OID is not provided in the sensor path.

Note It is also recommended to selectively enable on the device only those traps that are needed by Crosswork.

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).

Below are some sample values and a sample payload:

- 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).

Note

- MDT collector retains the collection ID that comes as part of the telemetry proto for the device. This behavior is different from CLI and SNMP collectors which compute the collection ID based on the sequence number of the collection.
- MDT collection jobs require some configuration to be done on the device. This configuration is automatically taken care of by NSO. Ensure that NSO is integrated and properly working
- If there is some change (delete/update) in existing MDT jobs between backup and restore operations, Cisco Crosswork does not replay the jobs for config update on the devices as it involves Provider(NSO). You have to restore configs on provider/devices. Cisco Crosswork will just restore 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 95

It supports data collection for the following transport mode:

- MDT TCP Dial-out Mode

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"
   }
  }
}
```

gNMI Collection Job

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

For sample device configuration, see Sample Device Configuration - gNMI, on page 64.

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

If 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/Dispatch cadence is not supported in gNMI collector.

Cisco Crosswork Data Gateway supports all types of stream-based subscriptions:

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

Note

- Cisco 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 payload. This is a known protobuf behavior.

  For boolean default value will be 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:

```
{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "device_group": "gnmi"
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
```

```
            "gnmi_sensor": {
                 "path":{
                    "origin":"",
                    "elem":[
                       {
                          "name":"interfaces"
                       },
                       {
                          "name":"interface",
                           "key":{
                             "name":"GigabitEthernet0/0/0/4"
                          }
                       }
                    ]
                 },
                 "mode" : "SAMPLE"
            }
          },
          "cadence_in_millisec": "30000"
        }
      ],
      "sensor_output_configs": [
        {
          "sensor_data": {
            "gnmi_sensor": {
                 "path":{
                    "origin":"",
                    "elem":[
                       {
                          "name":"interfaces"
                       },
                       {
                          "name":"interface",
                           "key":{
                             "name":"GigabitEthernet0/0/0/4"
                          }
                       }
                    ]
                 },
                 "mode" : "SAMPLE"
            }
          },
          "destination": {
            "context_id": "topic_gnmi",
            "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
          }
        }
      ],
      "application_context": {
        "context_id": "gnmi_test_context",
        "application_id": "gnmi"
      },
      "collection_mode": {
        "lifetime_type": "APPLICATION_MANAGED",
        "collector_type": "GNMI_COLLECTOR"
      }
    }
}
```

Sample Device Configuration - gNMI

Cisco IOS XR devices

1. Enable gRPC over an HTTP/2 connection.

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

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

2. Set the session parameters.

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

where:

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

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

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

Cisco IOS XE Devices

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

Certs and trustpoint are only required for secure gNMI servers.

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

Device certificates

Certs and trustpoint are only required for secure gNMI servers.

Creating Certs with OpenSSL on Linux

The following example shows how to create Certs with OpenSSL on a Linux machine:

```
# Setting up a CA
openssl genrsa -out rootCA.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=rootCA -x509 -new -nodes -key rootCA.key -sha256 -out
rootCA.pem

# Setting up device cert and key
openssl genrsa -out device.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=<hostnameFQDN> -new -key device.key -out device.csr
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
device.crt -sha256
# Encrpyt device key - needed for input to IOS
openssl rsa -des3 -in device.key -out device.des3.key -passout pass:<password - remember
this for later>

# Setting up client cert and key
openssl genrsa -out client.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=gnmi_client -new -key client.key -out client.csr
openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
client.crt -sha256
```

Installing Certs on a Cisco IOS XR Device

To install certs on Cisco IOS XR, replace files in the following path:

1. Login into XR machine.
2. Type run command on terminal prompt.

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

   ```
   cd /misc/config/grpc
   ```
4. Replace the content of the following files:
   - replace contents of ems.pem with device.crt
   - replace contents of ems.key with device.key
   - replace contents of ca.cert with rootCA.pem

Installing Certs on a Cisco IOS XE Device

The following example shows how to install certs 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#
```

Enable Secure gNMI communication between Device and Crosswork Data Gateway

Secure gNMI set up workflow:

1. Upload the trust chain to the Crosswork Certificate Management UI in Cisco Crosswork. See Configure gNMI Certificate, on page 67.
2. Update device configuration with secure gNMI port details from Cisco Crosswork UI. See Device Configuration from Cisco Crosswork UI, on page 69

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. For sample device configuration to configure trust point on devices, see Sample Device Configuration - gNMI, on page 64.

Note You can upload only one gNMI Certificate to Crosswork.

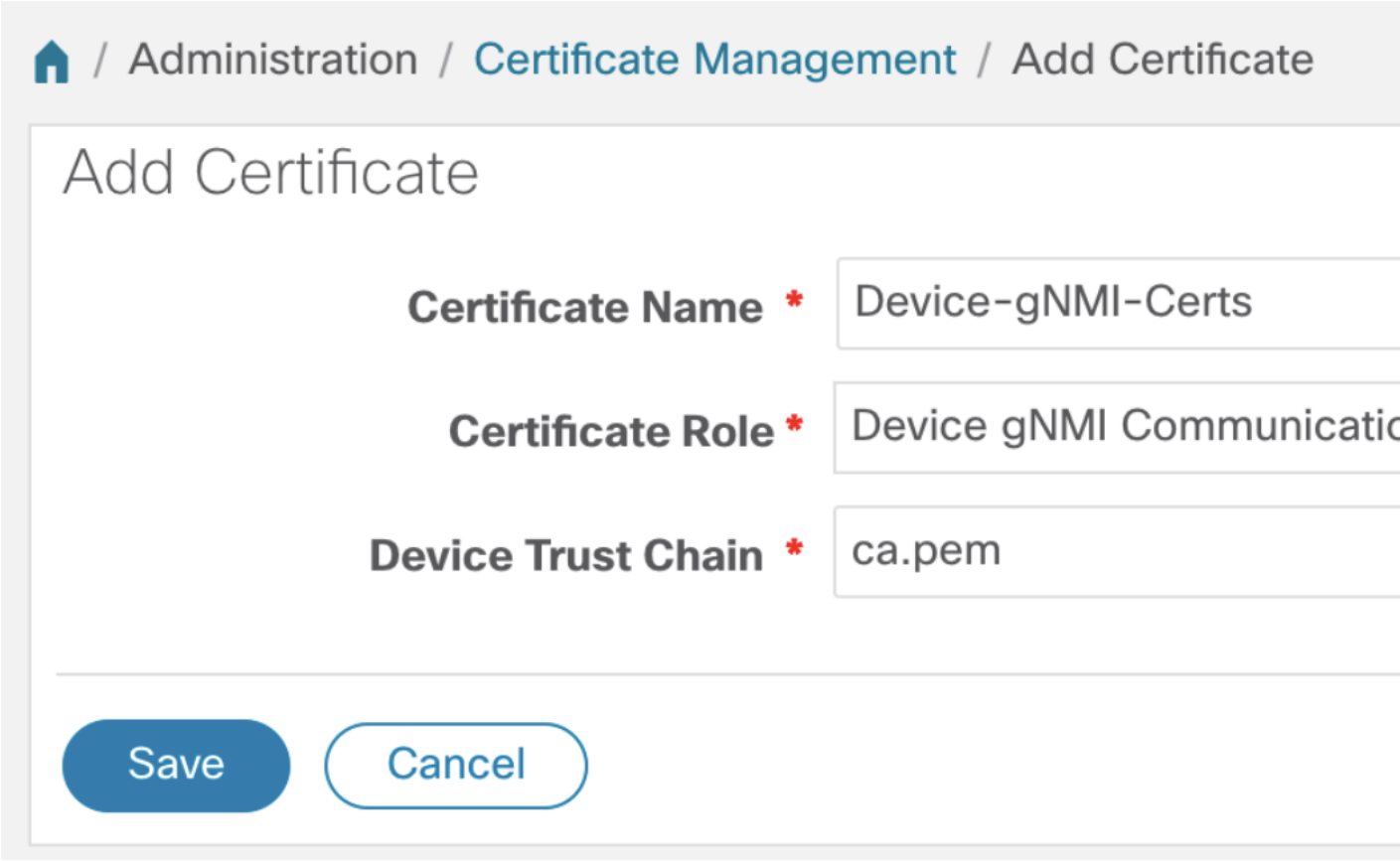
To configure the gNMI Certificate:

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

Step 2 Click the + icon to add certificate.

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

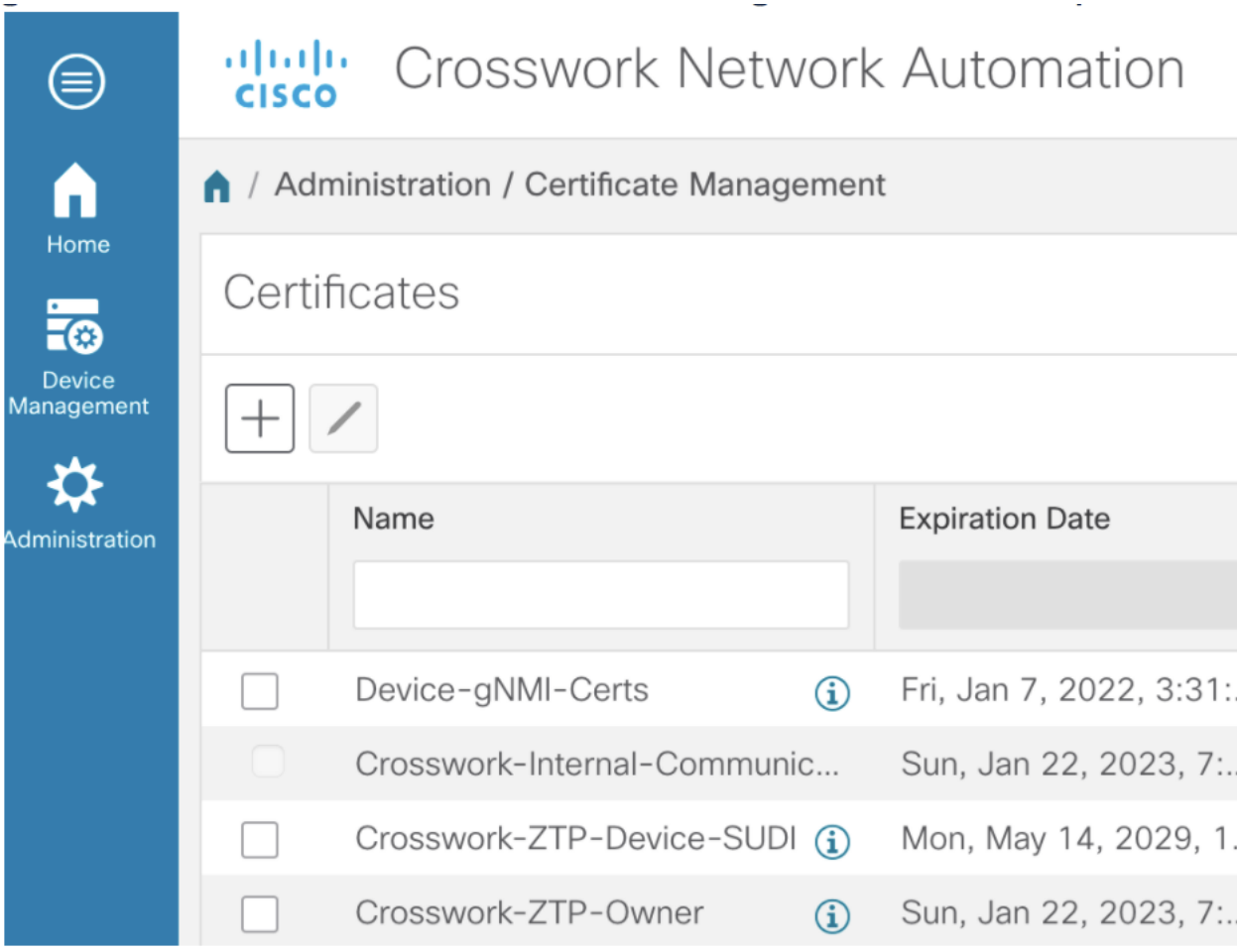
- **Device Certificate Name** - Enter a name for the certificate.
- **Certificate Role** - Select **Device gNMI Communication.**
- **Device Trust Chain** - Browse your local file system to the location of the .pem file and select the file.



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 is listed in the configured certificates once it has been added successfully.

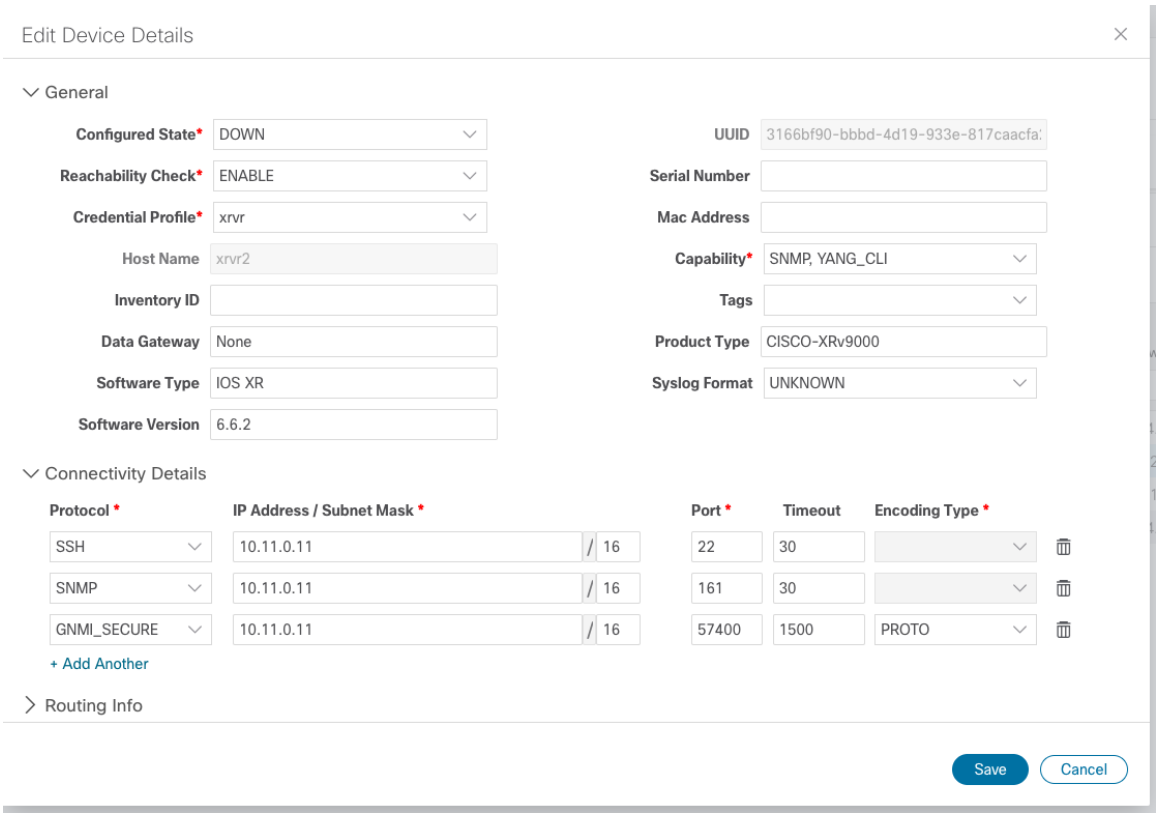


Device Configuration from Cisco Crosswork UI

Once you have configured the gNMI certificate in the Crosswork UI, update the device with secure protocol details.

1. From the Cisco Crosswork UI, navigate to **Device Management > Network Devices**
2. Select the device and click **Edit** to update the **Protocol** field with the details as:

   Protocol for secure communication : **GNMI_SECURE Port**.



Syslog Collection Job

Cisco Crosswork Data Gateway supports Syslog-based events collection from devices. Following Syslog formats are supported:

- RFC5424 syslog format
- RFC3164 syslog format

Note Syslog must be configured on devices before you can submit Syslog collection jobs. Please refer to the platform-specific documentation.

For sample device configuration, see Configure Syslog in RFC3164/RFC5424 format, on page 71.

Following is a sample Syslog collection payload:

```
{
  "collection_job": {
      "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c6f25a33-92e6-468a-ba0d-15490f1ce787"
          ]
        }
      }
```

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

Based on the facilities and severities mentioned in the payload, matching Syslog events will be sent to the specified destination. All other non-matching syslog events will be dropped.

Configure Syslog in RFC3164/RFC5424 format

This section lists sample configuration to configure syslog in the RFC3164 or RFC5424 format on the device. The same configuration can also be used for non-secure syslog configuration on the device.

Configure RFC3164 Syslog format

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

For Cisco IOS XR devices:

```
logging  <server 1> 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>
```

For Cisco IOS XE Devices:

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host 172.29.194.174 transport tcp port 9898 session-id string <sessionidstring> -->
 To use TCP channel
OR
logging host 172.29.194.174 transport udp port 9514 session-id string <sessionidstring>
---> To use UDP channel
OR
logging host <cdg ip> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
```

Configure RFC5424 Syslog format

For Cisco IOS XR devices:

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

For Cisco IOS XE Devices:

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host 172.29.194.174 transport tcp port 9898 session-id string <sessionidstring> -->
 To use TCP channel
OR
logging host 172.29.194.174 transport udp port 9514 session-id string <sessionidstring>
---> To use UDP channel
OR
logging host <cdg ip> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```

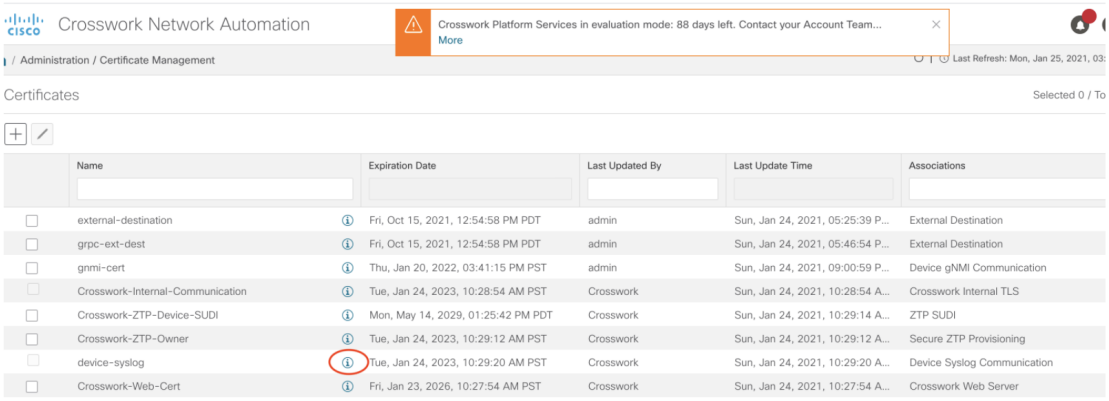
Configure Secure Syslog on Device

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

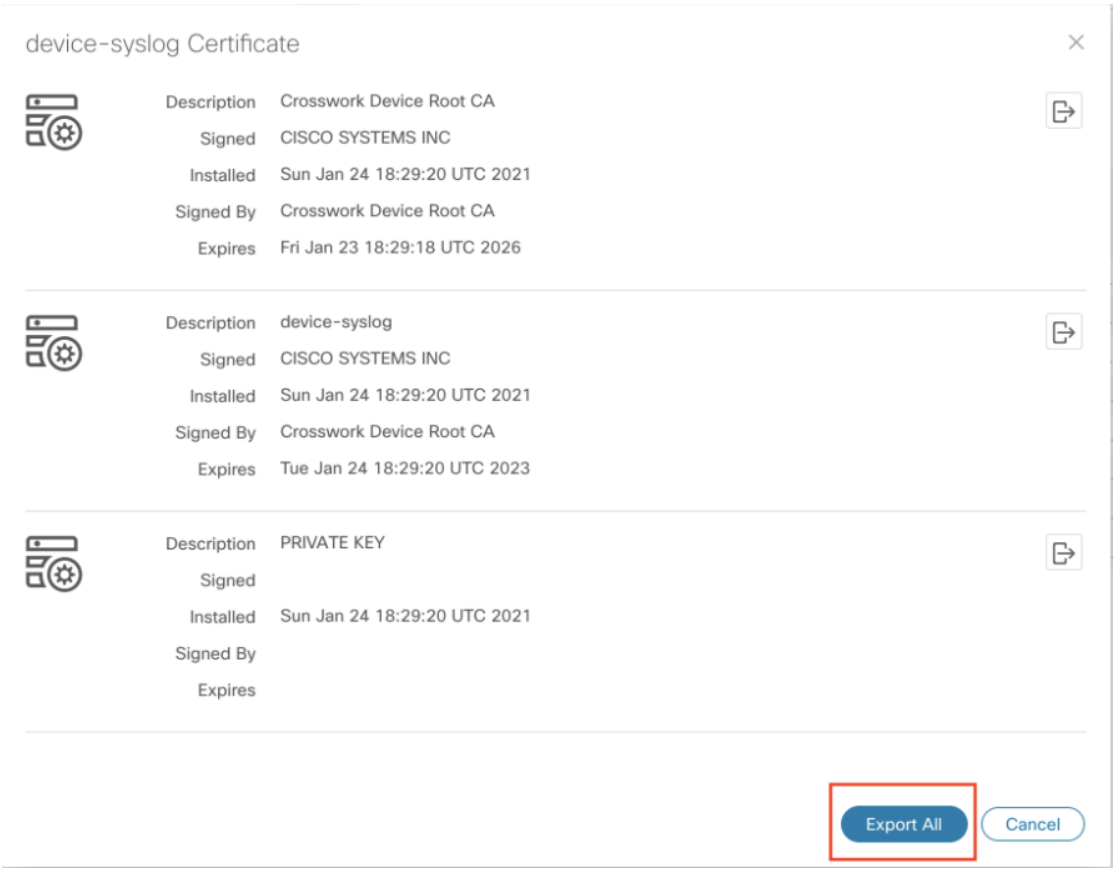
1. Download the Crosswork trust chain from the Certificate Management UI page in Cisco Crosswork.
2. Configure devices with the Crosswork trust chain for syslog configuration.

Download Syslog Certificates

1. In the Cisco Crosswork UI, go to **Administration > Certificate Management**
2. Click *i* in the '**device-syslog**' row as shown in the image below



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



The following files are downloaded to your system.

Syslog Configuration on Device

Sample XR Device Configuration to enable TLS

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


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

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

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

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


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

-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIRAKhqHQXcJzQzeQK6U2wn8PIwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.....................................................................
.....................................................................
5lBk617z6cxFER5c+/PmJFhcreisTxXg1aJbFdnB5C8f+0uUIdLghykQ/zaZGuBn
AAB70c9r9OeKGJWzvv1e2U8HH1pdQ/nd
-----END CERTIFICATE-----

Read 1560 bytes as CA certificate
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
                CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
```

```
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
  SHA1 Fingerprint:
               B06F2BFDE95413A8D08A01EE3511BC3D42F01E59

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


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


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

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

Sample XE Device Configuration to enable TLS

```
csr8kv(config)#crypto pki trustpoint syslog-root
csr8kv(ca-trustpoint)#enrollment terminal
```

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

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

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

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

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


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

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

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

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

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

Syslog Collection Job Output

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

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

Following is the sample output for each of the options:

1. **UNKNOWN** - Syslog Collection Job output contains the syslog event 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, by default this is considered as **UNKNOWN**.

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 event from the device.

Note The syslog collector will parse the syslog event(best effort parsing) as per the following Java RegEx pattern:

RFC5424

"^<(?<pri>\\d+)>(?<version>\\d{1,3})\\s*(?<date>(([0-9]{4}\\s+
9T:.Z-]+))\\s*(?<host>\\S+)\\s*(?<processname>\\S+)\\s*(?<pr
<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 event and the RFC3164 best-effort parsed syslog event from the device.

Note The syslog collector will parse the syslog event(best effort parsing) as per the following Java RegEx pattern:

RFC3164

"^(<(?<pri>\\d+)>[:]*\\s*)?(?<date>(*[a-zA-Z]{3}\\s+\\d+\\s
[a-zA-Z]{3}\\s+\\d+\\s+\\d+:\\d+:\\d+[.]*[\\d{3}\\s+]+[[a-zA-Z
<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 the syslog events as received from device.

Create a Collection Job

Follow the steps to create a collection job:

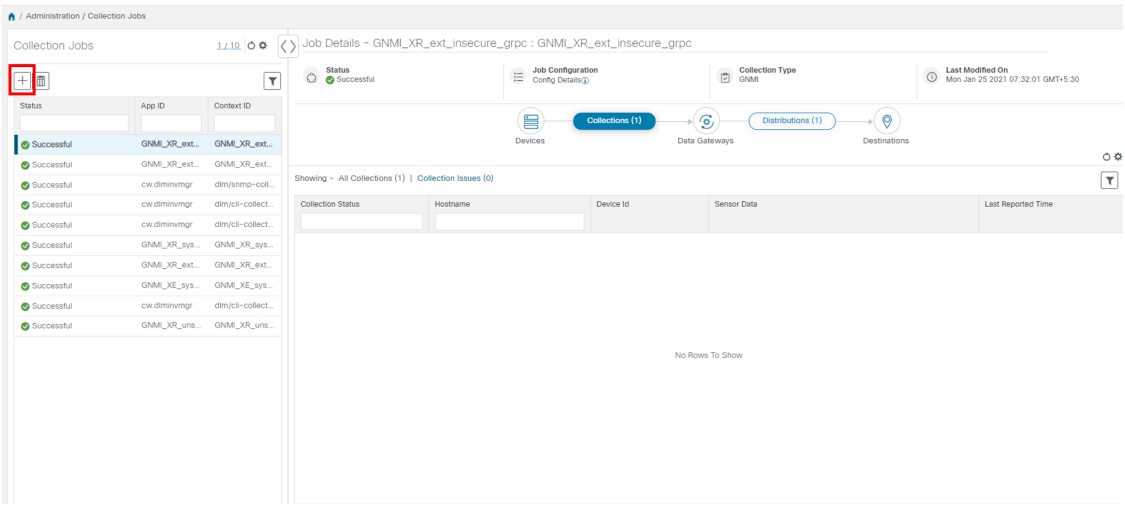
Note Collection jobs created through the Cisco Crosswork UI page can only be published once.

Before you begin

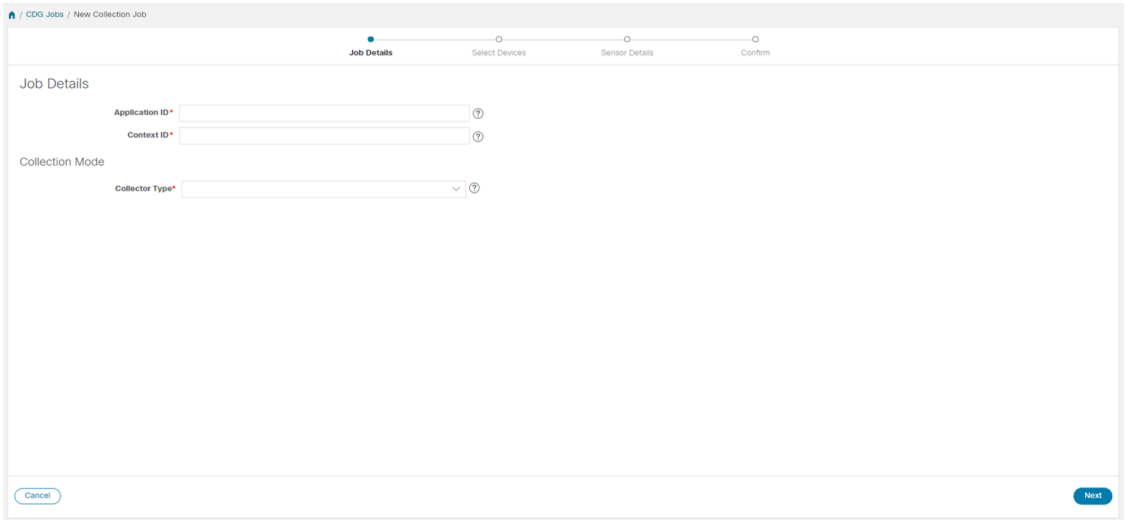
Ensure that a data destination is created (and active) to deposit the collected data. Also, have details of the sensor path and MIB that you plan to collect data from.

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

Step 2 In the **Collection Jobs** pane on the left hand side, click + button.



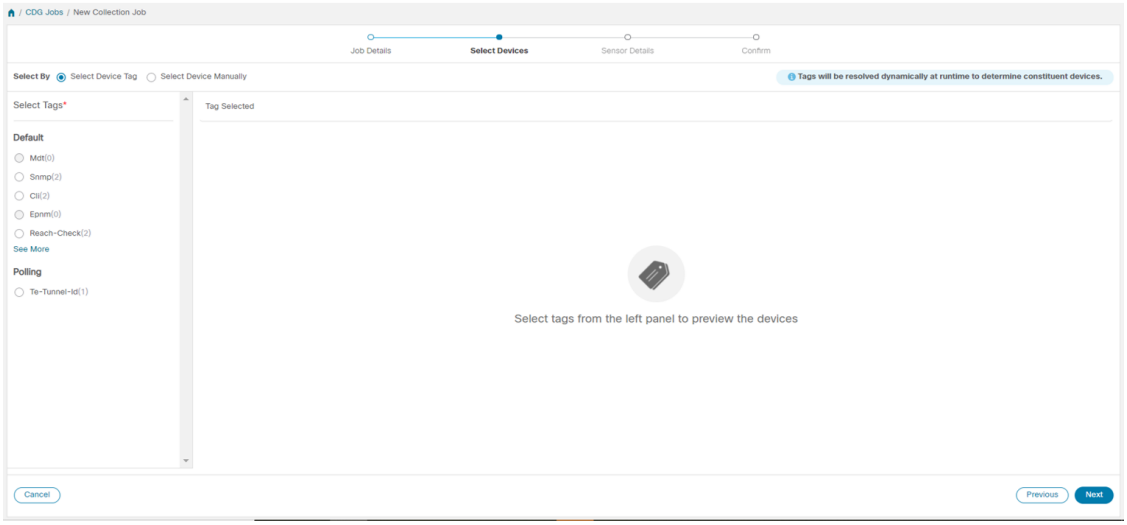
Step 3 In the **Job details** page, enter values for the following fields:



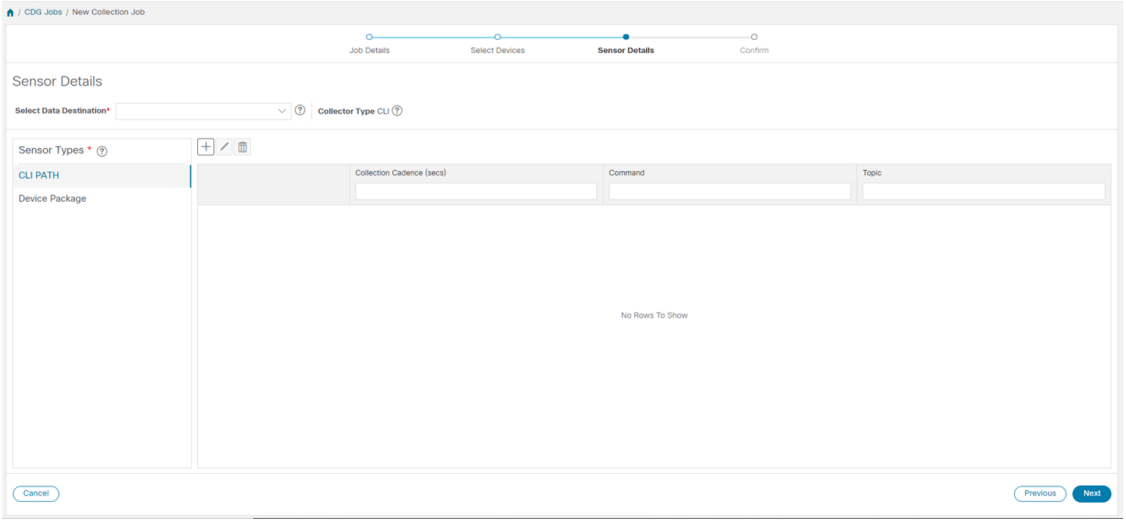
- Application ID: A unique identifier for the application.
- Context: A unique identifier to identify your application subscription across all collection jobs.
- Collector Type: Select the type of collection - CLI or SNMP.

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**.

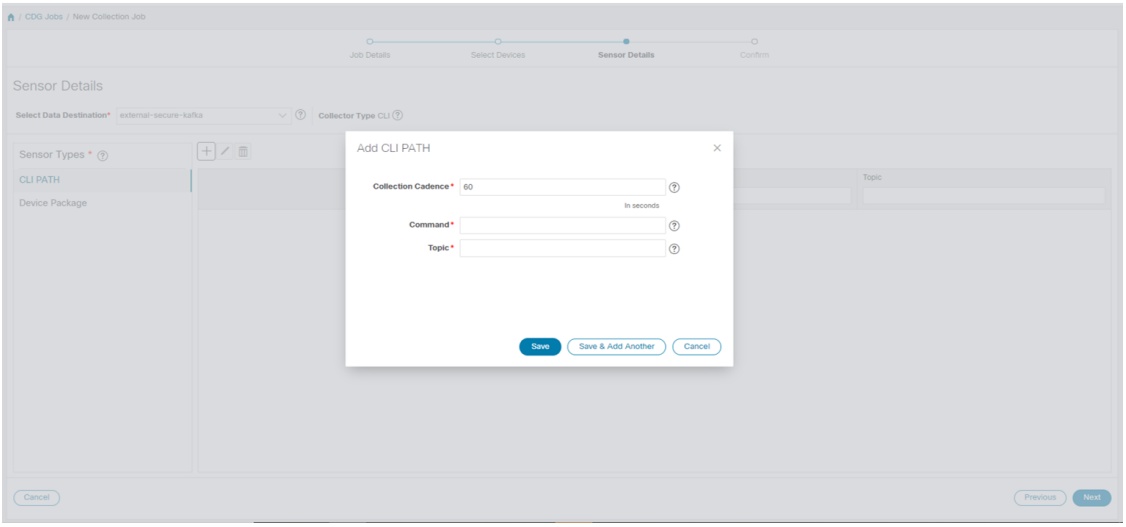


Step 5 (Applicable only for CLI collection) Enter the following sensor details:



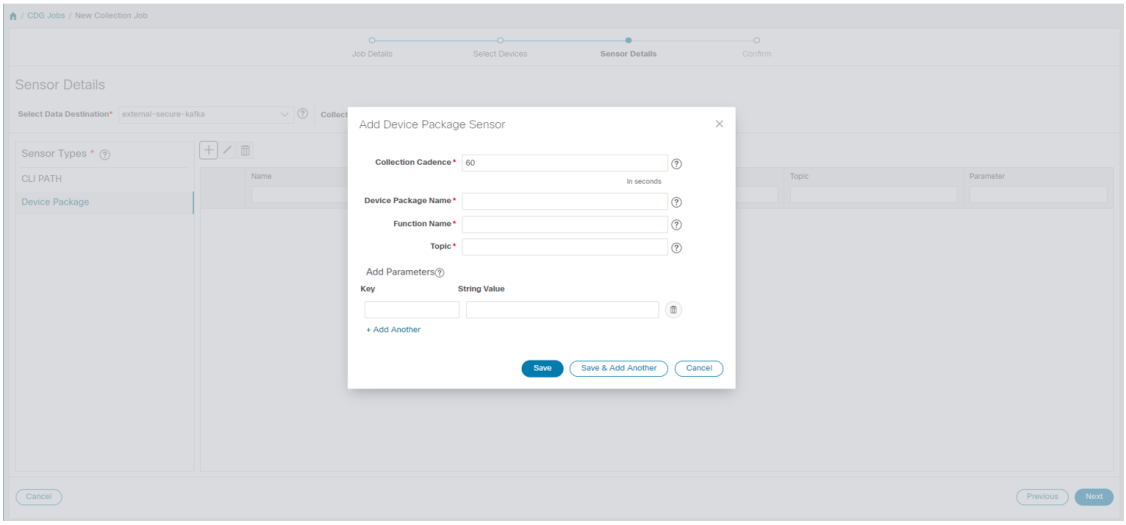
- Select data destination from **Select Data Destination** drop-down.
- Select sensor type from **Sensor Types** pane on the left.

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



- Collection Cadence: Push or poll cadence in seconds.
- Command: CLI command
- 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:

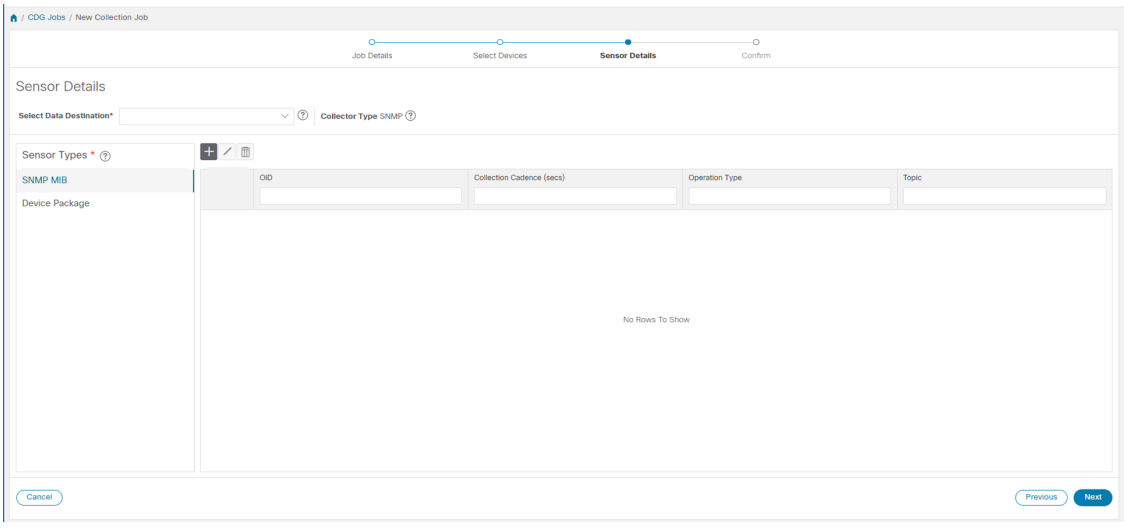


- Collection cadence: Push or poll cadence in seconds.
- Device Package Name: Custom XDE device package ID used while creating device package.
- Function name: Function name within custom XDE device package.
- Topic: Topic associated with the output destination.

Enter Key and String value for the paramters.

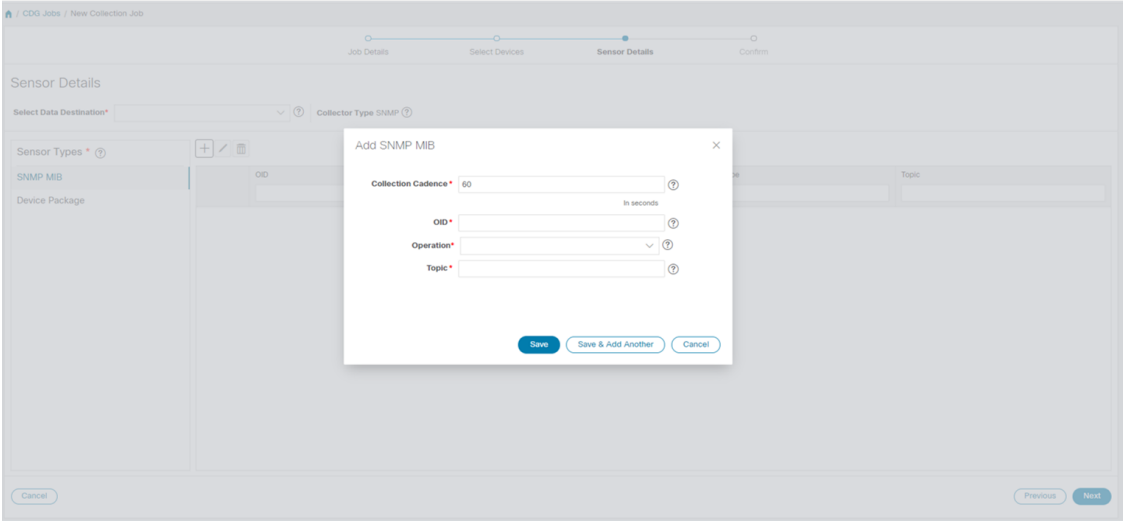
Click **Save**.

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



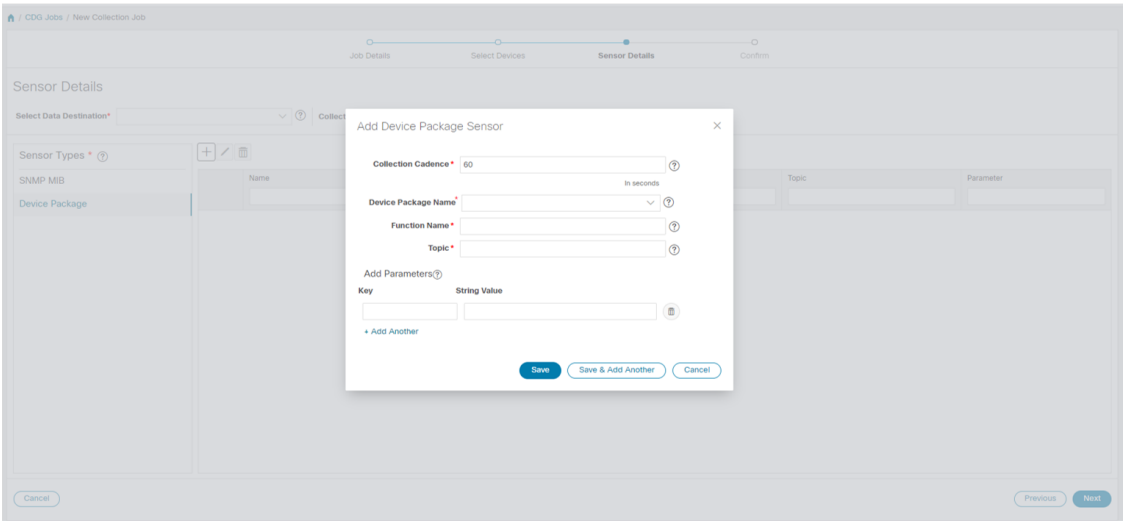
- Select data destination from **Select Data Destination** drop-down.
- Select sensor type from **Sensor Types** pane on the left.

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



- 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:



- 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 paramters.

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
```

Reboot the Kafka VM to fix this issue.

Delete a Collection Job

System and Crosswork Change Automation and Health Insights collection jobs should not be deleted as it will cause issues. Only external collection jobs can be deleted from the **Collection Jobs** page.

Follow the steps to delete a collection job:

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

Step 2 In the **Collection Jobs** pane on the left hand side, select the collection job you want to delete.

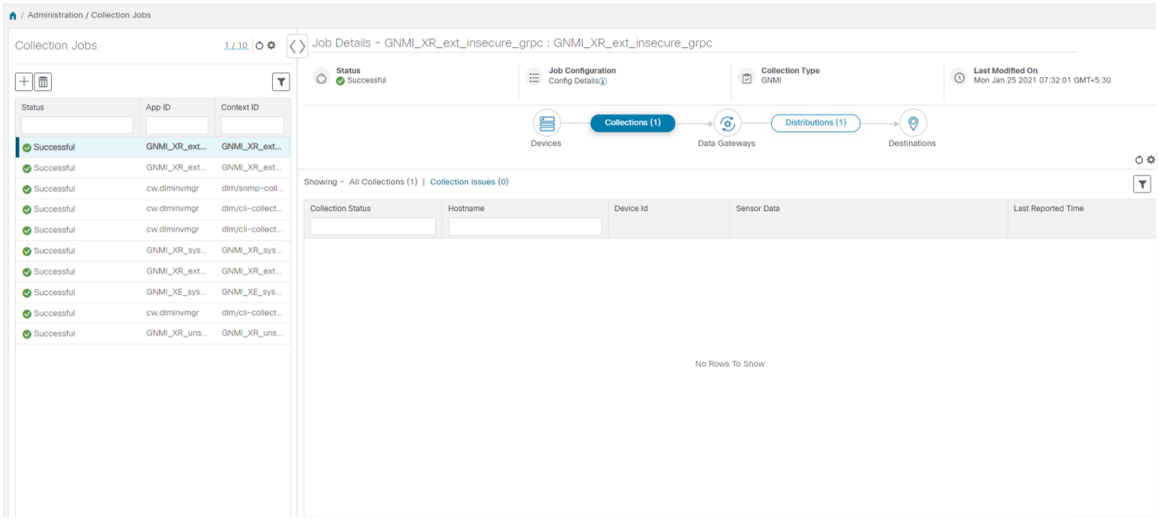
Step 3 Click delete button.

Step 4 Click **Delete** button when prompted.

Monitoring Collection Jobs

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

From the Cisco Crosswork main menu, choose **Administration** > **Collection Jobs**.



The **Collection Jobs** pane shows the list of all active collection jobs along with their Status, App ID, and Context ID.

The **Job Details** pane shows the details of a particular job selected in the **Collection Jobs** pane.

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

- Application name and context associated with the collection job.
- Status of the collection job.

Note

- Once a device is mapped to a Cisco Crosswork Data Gateway, the status of all the associated collection jobs is set to 'Unknown'. A job could have staus as 'Unknown' for either of the following reasons:
  - Cisco Crosswork Data Gateway has not yet reported its status.
  - Loss of connection between Cisco Crosswork Data Gateway and Crosswork.
  - Cisco Crosswork Data Gateway received the collection job, but actual collection is still pending.
- 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.
- Health Insights - KPI jobs must be enabled only on devices mapped to an extended Crosswork Data Gateway VM. Health Insights - KPI jobs that are enabled on devices mapped to standard Crosswork Data Gateway VM will have the job status as Degraded and the collection status as Failed.

- Job configuration of the collection job that you pass in the REST API request. Click icon next to **Config Details** to view the job configuration. Cisco Crosswork lets you view configuration in two modes:
  - View Mode
  - Text Mode
- Collection type
- Time and date of last modification of the collection job.
- Collections (x): x refers to requested input collections that span device by sensor paths. The corresponding **(y) Issues** is the count of input collections that are in UNKNOWN or FAILED state.
- Distributions (x): x refers to requested output collections that span device by sensor paths. The corresponding **(y) Issues** is the count of output collections that are in UNKNOWN or FAILED state.

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

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

Note

- `Create Failed` error means out of N devices, some devices failed to setup. However, the collection would happen on the devices that were successfully setup. You can identify the device(s) causing this error by using `Control Status` API.
- If job creation failed on a particular device because of NSO errors, after fixing NSO errors , you have to manually change the administration state of the device first to "Down" and then "Up". However, doing so resets the collection on the device.

Note

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

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

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 3: 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
ALARM-MIB.mib	CISCO-LWAPP-LOCAL-AUTH-MIB.mib	IANAifType-MIB.mib
APS-MIB.mib	CISCO-LWAPP- MDNS-MIB.mib	IEEE8021-CFM-MIB.mib
ATM-FORUM-MIB.mib	CISCO-LWAPP-MESH-BATTERY-MIB.mib	IEEE8021-PAE-MIB.mib
ATM-FORUM- TC-MIB.mib	CISCO-LWAPP-MESH-LINKTEST-MIB.mib	IEEE8021-TC-MIB.mib
ATM-MIB.mib	CISCO-LWAPP-MOBILITY-EXT-MIB.mib	IEEE802171-CFM- MIB.mib
ATM-TC-MIB.mib	CISCO-LWAPP-MOBILITY-MIB.mib	IEEE8023-LAG-MIB.mib
ATM2-MIB.mib	CISCO-LWAPP-NETFLOW-MIB.mib	IEEE802dot11-MIB.mib
BGP4-MIB.mib	CISCO-LWAPP- REAP-MIB.mib	IF-INVERTED-STACK-MIB.mib
BRIDGE-MIB.mib	CISCO-LWAPP- RF-MIB.mib	IF-MIB.mib
CISCO-AAA- SERVER-MIB.mib	CISCO-LWAPP- SI-MIB.mib	IGMP-STD-MIB.mib
CISCO-AAA- SESSION-MIB.mib	CISCO-LWAPP- TC-MIB.mib	INET-ADDRESS-MIB.mib
CISCO-AAL5-MIB.mib	CISCO-LWAPP-TRUSTSEC-MIB.mib	INT-SERV-MIB.mib
CISCO-ACCESS-ENVMON-MIB.mib	CISCO-LWAPP- TSM-MIB.mib	INTEGRATED-SERVICES -MIB.mib
CISCO-ATM-EXT -MIB.mib	CISCO-LWAPP- WLAN-MIB.mib	IP-FORWARD-MIB.mib
CISCO-ATM-PVCTRAP-EXTN-MIB.mib	CISCO-LWAPP-WLAN -SECURITY-MIB.mib	IP-MIB.mib
CISCO-ATM- QOS-MIB.mib	CISCO-MEDIA-GATEWAY-MIB.mib	IPMCAST-MIB.mib
CISCO-AUTH-FRAMEWORK-MIB.mib	CISCO-MOTION-MIB.mib	IPMROUTE-MIB.mib
CISCO-BGP-POLICY -ACCOUNTING-MIB.mib	CISCO-MPLS-LSR -EXT-STD-MIB.mib	IPMROUTE-STD -MIB.mib
CISCO-BGP4-MIB.mib	CISCO-MPLS-TC -EXT-STD-MIB.mib	IPV6-FLOW-LABEL -MIB.mib

CISCO-BULK-FILE -MIB.mib	CISCO-MPLS-TE-STD -EXT-MIB.mib	IPV6-ICMP-MIB.mib
CISCO-CBP-TARGET -MIB.mib	CISCO-NAC-TC -MIB.mib	IPV6-MIB.mib
CISCO-CBP-TARGET -TC-MIB.mib	CISCO-NBAR-PROTOCOL -DISCOVERY-MIB.mib	IPV6-MLD-MIB.mib
CISCO-CBP-TC-MIB.mib	CISCO-NETSYNC -MIB.mib	IPV6-TC.mib
CISCO-CCME-MIB.mib	CISCO-NTP-MIB.mib	IPV6-TCP-MIB.mib
CISCO-CDP-MIB.mib	CISCO-OSPF- MIB.mib	IPV6-UDP-MIB.mib
CISCO-CEF-MIB.mib	CISCO-OSPF- TRAP-MIB.mib	ISDN-MIB.mib
CISCO-CEF-TC.mib	CISCO-OTN-IF-MIB.mib	ISIS-MIB.mib
CISCO-CLASS-BASED -QOS-MIB.mib	CISCO-PAE-MIB.mib	ITU-ALARM-MIB.mib
CISCO-CONFIG- COPY-MIB.mib	CISCO-PAGP-MIB.mib	ITU-ALARM-TC- MIB.mib
CISCO-CONFIG- MAN-MIB.mib	CISCO-PIM-MIB.mib	L2TP-MIB.mib
CISCO-CONTENT-ENGINE-MIB.mib	CISCO-PING-MIB.mib	LANGTAG-TC-MIB.mib
CISCO-CONTEXT-MAPPING-MIB.mib	CISCO-POLICY-GROUP -MIB.mib	LLDP-EXT-DOT1 -MIB.mib
CISCO-DATA -COLLECTION-MIB.mib	CISCO-POWER-ETHERNET-EXT-MIB.mib	LLDP-EXT-DOT3 -MIB.mib
CISCO-DEVICE-EXCEPTION -REPORTING-MIB.mib	CISCO-PRIVATE -VLAN-MIB.mib	LLDP-MIB.mib
CISCO-DIAL- CONTROL-MIB.mib	CISCO-PROCESS-MIB.mib	MAU-MIB.mib
CISCO-DOT11-ASSOCIATION-MIB.mib	CISCO-PRODUCTS- MIB.mib	MGMD-STD-MIB.mib
CISCO-DOT11-HT- PHY-MIB.mib	CISCO-PTP-MIB.mib	MPLS-FTN-STD- MIB.mib
CISCO-DOT11-IF-MIB.mib	CISCO-RADIUS- EXT-MIB.mib	MPLS-L3VPN-STD- MIB.mib
CISCO-DOT11-SSID-SECURITY-MIB.mib	CISCO-RF-MIB.mib	MPLS-LDP-ATM-STD-MIB.mib
CISCO-DOT3- OAM-MIB.mib	CISCO-RF-SUPPLEMENTAL -MIB.mib	MPLS-LDP-FRAME -RELAY-STD-MIB.mib
CISCO-DS3-MIB.mib	CISCO-RTTMON-TC -MIB.mib	MPLS-LDP-GENERIC-STD-MIB.mib
CISCO-DYNAMIC-TEMPLATE-MIB.mib	CISCO-SELECTIVE-VRF-DOWNLOAD-MIB.mib	MPLS-LDP-MIB.mib
CISCO-DYNAMIC -TEMPLATE-TC-MIB.mib	CISCO-SESS-BORDER-CTRLR -CALL-STATS-MIB.mib	MPLS-LDP-STD-MIB.mib

CISCO-EIGRP-MIB.mib	CISCO-SESS-BORDER-CTRLR-EVENT-MIB.mib	MPLS-LSR-MIB.mib
CISCO-EMBEDDED-EVENT-MGR-MIB.mib	CISCO-SESS-BORDER-CTRLR-STATS-MIB.mib	MPLS-LSR-STD-MIB.mib
CISCO-ENHANCED-IMAGE-MIB.mib	CISCO-SMI.mib	MPLS-TC-MIB.mib
CISCO-ENHANCED-MEMPOOL-MIB.mib	CISCO-SONET-MIB.mib	MPLS-TC-STD-MIB.mib
CISCO-ENTITY-ASSET -MIB.mib	CISCO-ST-TC.mib	MPLS-TE-MIB.mib
CISCO-ENTITY-EXT -MIB.mib	CISCO-STACKWISE- MIB.mib	MPLS-TE-STD-MIB.mib
CISCO-ENTITY-FRU-CONTROL-MIB.mib	CISCO-STP-EXTENSIONS -MIB.mib	MPLS-VPN-MIB.mib
CISCO-ENTITY- QFP-MIB.mib	CISCO-SUBSCRIBER -IDENTITY-TC-MIB.mib	MSDP-MIB.mib
CISCO-ENTITY-REDUNDANCY-MIB.mib	CISCO-SUBSCRIBER-SESSION-MIB.mib	NET-SNMP-AGENT -MIB.mib
CISCO-ENTITY-REDUNDANCY-TC-MIB.mib	CISCO-SUBSCRIBER-SESSION-TC-MIB.mib	NET-SNMP-EXAMPLES -MIB.mib
CISCO-ENTITY- SENSOR-MIB.mib	CISCO-SYSLOG-MIB.mib	NET-SNMP-MIB.mib
CISCO-ENTITY-VENDORTYPE-OID-MIB.mib	CISCO-SYSTEM-EXT- MIB.mib	NET-SNMP-TC.mib
CISCO-ENVMON-MIB.mib	CISCO-SYSTEM-MIB.mib	NHRP-MIB.mib
CISCO-EPM-NOTIFICATION-MIB.mib	CISCO-TAP2-MIB.mib	NOTIFICATION-LOG-MIB.mib
CISCO-ETHER-CFM- MIB.mib	CISCO-TC.mib	OLD-CISCO-CHASSIS-MIB.mib
CISCO-ETHERLIKE- EXT-MIB.mib	CISCO-TCP-MIB.mib	OLD-CISCO-INTERFACES -MIB.mib
CISCO-FABRIC- C12K-MIB.mib	CISCO-TEMP-LWAPP -DHCP-MIB.mib	OLD-CISCO-SYS- MIB.mib
CISCO-FIREWALL -TC.mib	CISCO-TRUSTSEC -SXP-MIB.mib	OLD-CISCO-SYSTEM -MIB.mib
CISCO-FLASH-MIB.mib	CISCO-TRUSTSEC -TC-MIB.mib	OPT-IF-MIB.mib
CISCO-FRAME- RELAY-MIB.mib	CISCO-UBE-MIB.mib	OSPF-MIB.mib
CISCO-FTP-CLIENT -MIB.mib	CISCO-UNIFIED-COMPUTING-ADAPTOR -MIB.mib	OSPF-TRAP-MIB.mib
CISCO-HSRP-EXT -MIB.mib	CISCO-UNIFIED-COMPUTING-COMPUTE -MIB.mib	OSPFV3-MIB.mib

CISCO-HSRP-MIB.mib	CISCO-UNIFIED-COMPUTING-ETHER -MIB.mib	P-BRIDGE-MIB.mib
CISCO-IETF-ATM2 -PVCTRAP-MIB.mib	CISCO-UNIFIED-COMPUTING-FC- MIB.mib	PIM-MIB.mib
CISCO-IETF-BFD -MIB.mib	CISCO-UNIFIED-COMPUTING-MEMORY -MIB.mib	PIM-STD-MIB.mib
CISCO-IETF-FRR -MIB.mib	CISCO-UNIFIED- COMPUTING -MIB.mib	POWER-ETHERNET -MIB.mib
CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED-COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED-COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED-COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS-TE-EXT-STD-03- MIB.mib	CISCO-VLAN-IFTABLE-RELATIONSHIP -MIB.mib	PTOPO-MIB.mib
CISCO-IETF-MPLS-TE-P2MP-STD-MIB.mib	CISCO-VLAN-MEMBERSHIP-MIB.mib	PerfHist-TC-MIB.mib
CISCO-IETF-MSDP -MIB.mib	CISCO-VOICE-COMMON -DIAL-CONTROL-MIB.mib	Q-BRIDGE-MIB.mib
CISCO-IETF-PIM-EXT -MIB.mib	CISCO-VOICE-DIAL -CONTROL-MIB.mib	RADIUS-ACC-CLIENT -MIB.mib
CISCO-IETF-PIM -MIB.mib	CISCO-VOICE-DNIS -MIB.mib	RADIUS-AUTH-CLIENT -MIB.mib
CISCO-IETF-PW- ATM-MIB.mib	CISCO-VPDN-MGMT -MIB.mib	RFC-1212.mib
CISCO-IETF-PW- ENET-MIB.mib	CISCO-VTP-MIB.mib	RFC-1215.mib
CISCO-IETF-PW-MIB.mib	CISCO-WIRELESS-NOTIFICATION-MIB.mib	RFC1155-SMI.mib
CISCO-IETF-PW- MPLS-MIB.mib	CISCOSB-DEVICEPARAMS -MIB.mib	RFC1213-MIB.mib
CISCO-IETF-PW -TC-MIB.mib	CISCOSB- HWENVIROMENT.mib	RFC1315-MIB.mib
CISCO-IETF-PW -TDM-MIB.mib	CISCOSB-MIB.mib	RFC1398-MIB.mib
CISCO-IETF-VPLS -BGP-EXT-MIB.mib	CISCOSB-Physicaldescription -MIB.mib	RIPv2-MIB.mib
CISCO-IETF-VPLS -GENERIC-MIB.mib	DIAL-CONTROL-MIB.mib	RMON-MIB.mib
CISCO-IETF-VPLS- LDP-MIB.mib	DIFFSERV-DSCP-TC.mib	RMON2-MIB.mib

CISCO-IF-EXTENSION -MIB.mib	DIFFSERV-MIB.mib	RSTP-MIB.mib
CISCO-IGMP-FILTER -MIB.mib	DISMAN-NSLOOKUP -MIB.mib	RSVP-MIB.mib
CISCO-IMAGE-LICENSE -MGMT-MIB.mib	DISMAN-PING-MIB.mib	SMON-MIB.mib
CISCO-IMAGE-MIB.mib	DISMAN-SCHEDULE -MIB.mib	SNA-SDLC-MIB.mib
CISCO-IMAGE-TC.mib	DISMAN-SCRIPT-MIB.mib	SNMP-COMMUNITY -MIB.mib
CISCO-IP-LOCAL- POOL-MIB.mib	DISMAN-TRACEROUTE -MIB.mib	SNMP-FRAMEWORK -MIB.mib
CISCO-IP-TAP-MIB.mib	DOT3-OAM-MIB.mib	SNMP-MPD-MIB.mib
CISCO-IP-URPF-MIB.mib	DRAFT-MSDP-MIB.mib	SNMP-NOTIFICATION -MIB.mib
CISCO-IPMROUTE- MIB.mib	DS0-MIB.mib	SNMP-PROXY-MIB.mib
CISCO-IPSEC-FLOW -MONITOR-MIB.mib	DS1-MIB.mib	SNMP-REPEATER -MIB.mib
CISCO-IPSEC-MIB.mib	DS3-MIB.mib	SNMP-TARGET-MIB.mib
CISCO-IPSEC-POLICY -MAP-MIB.mib	ENTITY-MIB.mib	SNMP-USER-BASED -SM-MIB.mib
CISCO-IPSLA-AUTOMEASURE-MIB.mib	ENTITY-SENSOR-MIB.mib	SNMP-USM-AES -MIB.mib
CISCO-IPSLA- ECHO-MIB.mib	ENTITY-STATE-MIB.mib	SNMP-USM-DH-OBJECTS-MIB.mib
CISCO-IPSLA- JITTER-MIB.mib	ENTITY-STATE- TC-MIB.mib	SNMP-VIEW-BASED-ACM-MIB.mib
CISCO-IPSLA- TC-MIB.mib	ESO-CONSORTIUM -MIB.mib	SNMPv2-CONF.mib
CISCO-ISDN-MIB.mib	ETHER-WIS.mib	SNMPv2-MIB.mib
CISCO-LICENSE- MGMT-MIB.mib	EtherLike-MIB.mib	SNMPv2-SMI.mib
CISCO-LOCAL-AUTH-USER-MIB.mib	FDDI-SMT73-MIB.mib	SNMPv2-TC-v1.mib
CISCO-LWAPP- AAA-MIB.mib	FR-MFR-MIB.mib	SNMPv2-TC.mib
CISCO-LWAPP- AP-MIB.mib	FRAME-RELAY -DTE-MIB.mib	SNMPv2-TM.mib
CISCO-LWAPP- CCX-RM-MIB.mib	FRNETSERV- MIB.mib	SONET-MIB.mib
CISCO-LWAPP- CDP-MIB.mib	GMPLS-LSR- STD-MIB.mib	SYSAPPL-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-CAPABILITY.mib	GMPLS-TC-STD- MIB.mib	TCP-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-MIB.mib	GMPLS-TE-STD-MIB.mib	TOKEN-RING-RMON -MIB.mib

CISCO-LWAPP-DHCP -MIB.mib	HC-PerfHist-TC-MIB.mib	TOKENRING-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.mib	HC-RMON-MIB.mib	TRANSPORT-ADDRESS -MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CCX-TC-MIB.mib	HCNUM-TC.mib	TUNNEL-MIB.mib
CISCO-LWAPP-DOT11 -LDAP-MIB.mib	HOST-RESOURCES -MIB.mib	UDP-MIB.mib
CISCO-LWAPP- DOT11-MIB.mib	HOST-RESOURCES -TYPES.mib	VPN-TC-STD-MIB.mib
CISCO-LWAPP -DOWNLOAD-MIB.mib	IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib	VRRP-MIB.mib
CISCO-LWAPP- IDS-MIB.mib	IANA-GMPLS-TC-MIB.mib	

List of Pre-loaded YANG Modules for MDT Collection

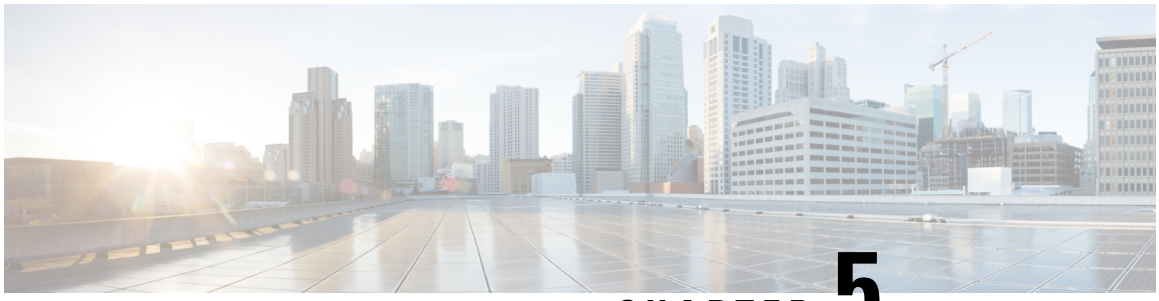
This section lists the YANG modules that the Cisco Crosswork Data Gateway supports for MDT collection on Cisco IOS XR devices.

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
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
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



CHAPTER 5

Manage Backups

This section contains the following topics:

Manage Cisco Crosswork Backup and Restore

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

Note If you want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in Backup Cisco Crosswork with Cisco NSO, on page 103 instead of the instructions here.

When you create backups for the Cisco Crosswork cluster, or restore the cluster from a backup, follow these guidelines:

- During your first login, configure a destination SCP server to store backup files. This configuration is a one-time activity. You can't take a backup or initiate a restore operation until you complete this task.
- We recommend that you perform backup or restore operations during a scheduled maintenance window only. Users shouldn’t attempt to access Cisco Crosswork while these operations are running. Backups will take the system offline for about 10 minutes, but restore operations can be lengthy. Both will pause other applications until they are complete. These pauses can affect data-collection jobs.
- When performing a normal restore, Cisco Crosswork applications and data are restored to the same version as when you took the backup. When performing a *disaster* restore, you must use the same Cisco Crosswork software image that you used when creating the backup. You can’t perform a disaster restore using a backup created using a different version of the software.
- Use the dashboard to monitor progress of the backup or restore process, until the process completes. If you attempt to use the Cisco Crosswork system during the process, you may see incorrect content or errors, since various services pause and restart frequently.

- You can run only one backup or restore operation at a given time.
- Both the Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.
- Don't attempt to move or rename any of the backup tarballs Cisco Crosswork creates on the backup server. To save space on your backup server, you may delete older backups, but they will still appear in the job list in this version.

Before you begin

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 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 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) Click **Backup** to display the **Backup** dialog box with the destination server details prefilled.
b) Provide a relevant name for the backup in the **Job Name** field.
c) If you want Cisco Crosswork to take the backup despite application or microservice issues, check the **Force** check box.
d) Be sure to uncheck the **Backup NSO** checkbox.

   If you want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in Backup Cisco Crosswork with Cisco NSO, on page 103 instead of the instructions here

e) (Optional) Click **Verify Backup** to verify that Cisco Crosswork has enough free resources to complete the backup. If the check is successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.
f) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list.
g) 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** table 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.

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

a) Select the required backup file from the **Backup Restore Job Sets** table. The page displays the job list on the left, with details for the selected job on the right side.
b) Click **Restore** to display the **Restore** dialog box with the destination server details prefilled.

c) Provide a relevant name in the **Job Name** field.
d) If you want Cisco Crosswork to take the backup despite application or microservice issues, check the **Force** check box.
e) (Optional) Click **Verify Restore** to verify that Cisco Crosswork has enough free resources to complete the restore. If the check is successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.
f) Click **Start Restore** to start the restore operation. Cisco Crosswork 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.

Restore After a Disaster

A disaster recovery is a restore operation that you use after a natural or human-caused disaster has destroyed a Cisco Crosswork cluster. You will need to deploy a new cluster first, following the instructions in the *Cisco Crosswork Platform and Applications Installation Guide*.

If your cluster only has one malfunctioning hybrid node, or one or more worker nodes, don't perform a disaster recovery. Instead, use cluster management features to redeploy these nodes, or replace them with new nodes, as explained in Manage the Crosswork Cluster, on page 5 chapter.

If you have more than one malfunctioning hybrid node, the system will not be in a functional state. Even if you replace or reboot the failed hybrid nodes, there is no guarantee that the system will recover correctly even if you replace or reboot the failed hybrid nodes. In this case, you can deploy a new cluster, and then recover the entire system using a recent backup taken from the old cluster. For more information, see the Manage the Crosswork Cluster, on page 5 chapter.

When conducting a disaster recovery, note the following:

- The new Cisco Crosswork cluster to which you restore the backup must use the same IP addresses as the one where you took the backup. This guideline is important, as internal certificates use the IP addresses of the original cluster.
- The new cluster must have the same number and types of nodes as the cluster where you took the backup.
- The new cluster must use the same Cisco Crosswork software image that you used when creating the backup. You can’t restore the cluster using a backup that was created using a different version of the software.
- Keep your backups current, so that you can recover the true state of your system as it existed before the disaster. The restore operation restores all applications that are installed at the time the backup was made. If you have installed more applications or patches since your last backup, take another backup.
- If the disaster recovery fails, contact Cisco Customer Experience.

To perform a disaster recovery:

Before you begin

Get from the SCP backup server the full name of the backup file you want to use in your disaster recovery. This file is normally the most recent backup file you have made. Cisco Crosswork backup filenames have the following format:

`backup_JobName_CWVersion_TimeStamp.tar.gz`

Where:

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

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

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

Step 2 Click **Disaster Restore** to display the **Disaster Restore** dialog box with the destination server details pre-filled.

Step 3 Enter the backup filename in the **Backup File Name** field.

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

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

Resolve Missing SR-TE Policies and RSVP-TE Tunnels

The information in this topic is applicable only when Cisco Crosswork Optimization Engine is installed.

The Configuration Database contains all SR-TE policies and RSVP-TE tunnels of which Cisco Crosswork is aware. Cisco Crosswork updates the Configuration Database whenever you provision, modify or delete an SR-TE policy or RSVP-TE tunnel. You can use the Configuration Database CLI tool to do the following:

- Read and write CSV files to the Configuration Database.
- Populate SR-TE policy and RSVP-TE tunnel information from the Configuration Database to create a CSV file.

The Configuration Database CLI tool is especially useful when trying to recover missing SR-TE policies and RSVP-TE tunnels after a restore operation. For example, the `--dump-missing` option produces a CSV file which lists the SR-TE policies and RSVP-TE tunnels that are missing. Use this CSV file to determine which SR-TE policies and RSVP-TE tunnels are missing. Then load them back into the topology using the `--load` option. See the CLI tool help for more information.

Step 1 Enter the **optima-pce-dispatcher** container:

```
kubectl exec -it optima-pce-dispatcher-XXXXXXX-XXXX bash
```

Step 2 You can run the following commands:

a) Show CLI tool help text.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --help
```

b) Save all SR-TE policies and RSVP-TE tunnels that are in the Configuration Database to a CSV file.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --dump /<PathToFile>/dump_file.csv
```

c) Load the contents from the provided CSV file and write policies to the Configuration Database.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --load /<PathToFile>/load_file.csv
```

Note This command overwrites any duplicate SR-TE policies or RSVP-TE tunnels that it finds, and adds only valid TE tunnels to the Configuration Database. Duplicate SR-TE policies have the same combination of headend, endpoint, and color. Duplicate RSVP-TE tunnels have the same combination of headend and tunnel name.

d) After the CSV load completes, synchronize the Cisco Crosswork Optimization Engine UI with the Configuration Database by restarting Optimization Engine, as follows:

1. From the main menu, select **Administration** > > **Crosswork Manager** > **Crosswork Health** > **Optimization Engine**.
2. Select **optima-ui-service** > > **Action** > **Restart**. Restart takes approximately five minutes.

e) After the restart, compare SR-TE policies and RSVP-TE tunnels that are currently in the topology with the Configuration Database contents. Save the missing SR policies and RSVP-TE tunnels to a CSV file. You can then use this CSV file and the following command to load the missing policies into the Configuration Database:

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py -dump-missing /<PathToFile>/dump_file.cs
```

Backup Cisco Crosswork with Cisco NSO

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

Before you begin

Before you begin, be sure:

- 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.

Also ensure that the NSO provider, the Cisco Crosswork credential profile that is associated with the NSO provider, and the NSO server meet the following prerequisites:

- The NSO provider configuration includes an SSH connection. If you don't enable SSH on the provider, Cisco Crosswork displays a warning alarm. Cisco Crosswork creates a backup for its own data, but not for NSO.
- The NSO provider's credential profile contains the user ID and password of a user with `sudo` privileges on the NSO server.

- 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 NSO server has Python version 3.x installed, and the user in the credential profile for the NSO provider can execute `python3` 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 requirements means that all or part of the backup job will fail.

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 Cisco Crosswork and Cisco NSO backups:**

a) Click **Backup** to display the **Backup** dialog box with the destination server details prefilled.
b) Provide a relevant name for the backup in the **Job Name** field.
c) If you want Cisco Crosswork to take the backup despite application or microservice issues, check the **Force** check box.
d) Be sure to leave the **Backup NSO** check box checked.
e) (Optional) Click **Verify Backup** to verify that Cisco Crosswork has enough free resources to complete the backup. If the check is successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.
f) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list.
g) 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 the job set you want.

The **Job Details** table 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.

Restore with Cisco NSO

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

- We recommend that you perform restore operations during a scheduled maintenance window only. Users shouldn't attempt to access Cisco Crosswork or Cisco NSO while these operations are running. Cisco Crosswork restore operations are lengthy, and will pause other Cisco Crosswork applications until they are complete. Cisco NSO must be stopped completely during restores.
- You can run both a Cisco Crosswork and a Cisco NSO restore operation at the same time.

Before you begin

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

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

Where:

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

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

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 Cisco 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.gz
```

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

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

Step 3 Un-tar the Cisco NSO backup file in the destination folder. You will see Cisco NSO files being extracted to a folder structure under `/nso/`*`ProviderName/`*, where `/nso/`*`ProviderName/`* is the name of the Cisco NSO provider as configured in Cisco Crosswork. In the following example, the Cisco NSO provider is named `nso121`:

```
tar -xvsf 468c4715-ea09-4c2b-905e-98999d.tar.gz
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 Cisco NSO backup file. In the example in the previous step, the file name is highlighted.

Step 5 Log in to Cisco NSO as a user with root privileges and access the command line. Then copy or move the generated Cisco NSO backup file from the SCP server to the specified restore path location of the Cisco 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 Cisco NSO restore operations only while NSO is not running. At the Cisco NSO cluster command line, run the following command to stop Cisco 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 Cisco NSO backup file. For example:

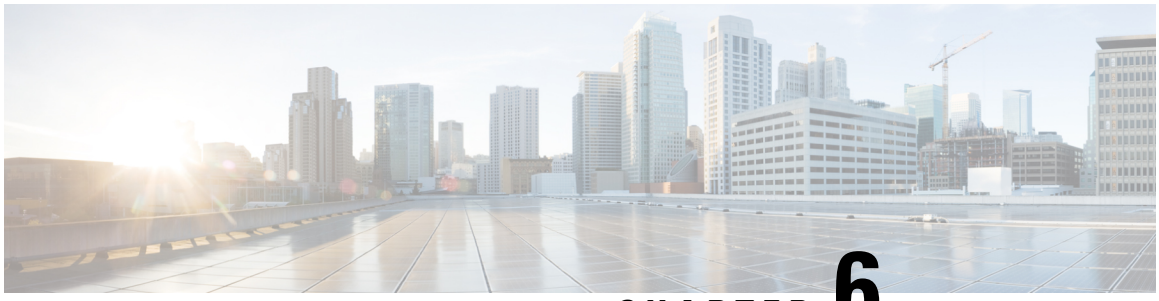
```
#ncs-backup --restore ncs-5.4.2@backup_Wed_nso121.backup.gz
```

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

Step 8 Once the restore completes, restart Cisco 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 Cisco Crosswork and Cisco NSO clusters from backups, re-add the Cisco NSO provider to Cisco Crosswork.



CHAPTER 6

Prepare Infrastructure for Device Management

This section contains the following topics:

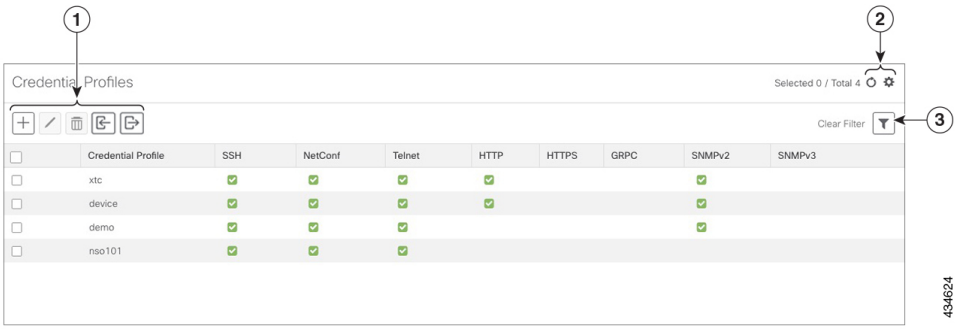
Manage Credential Profiles

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 6: Credentials Profile window



Item	Description
1	Click  to add a credential profile. See Create Credential Profiles, on page 108.
	Click  to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 112.
	Click  to delete the selected credential profile. See Delete Credential Profiles, on page 113.
	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 110.
	Click  to export credential profiles to a CSV file. See Export Credential Profiles, on page 112.
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 110.

When creating device credential profiles that contain SNMP credentials, Cisco recommends that the profile contain credentials for the version of SNMP actually 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 112).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see Import Credential Profiles, on page 110).

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 112 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 will vary 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**.

Connectivity Type	Fields
SNMPv3	Choose the required **Security Level** and enter the **User Name**. If you chose the NO_AUTH_NO_PRIV **Security Level** of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional. 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**. Only the following SNMPv3 Privacy Types are supported • CFB_AES_128 • CBC_DES_56 The following Privacy Types are not supported: • AES192 • AES256 • 3DES

Step 6 (Optional) Click **+ Add Another** and repeat the above 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 112 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`**

Field	Entries	Required or Optional
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**
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	Valid values are **CFB_AES_128** or **CBC_DES_56** The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	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 112).

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 112 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 112).

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 113 and Edit Providers, on page 138).

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 Network Devices>).
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**.

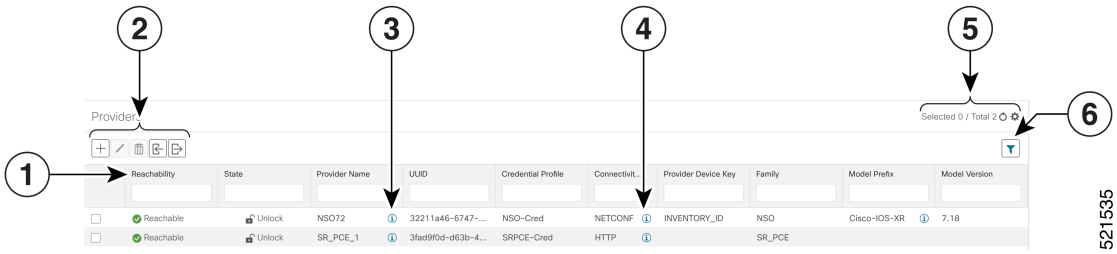
Manage Providers

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 readding 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 7: Providers Window



Item	Description
1	The icon shown next to the provider in this column indicates the provider's **Reachability**. See Reachability and Operational State, on page 155.
2	Click to add a provider. See About Adding Providers, on page 117.
	Click to edit the settings for the selected provider. See Edit Providers, on page 138.
	Click to delete the selected provider. See Delete Providers, on page 138.
	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 136.
	Click to export a provider to a CSV file. See Export Providers, on page 139.
3	Click next to the provider in the **Provider Name** column to open the **Properties for** 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).
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 4: 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 120.
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 122.
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 133 .
Syslog Storage	Instances of storage servers (remote or on the Cisco Crosswork application VM itself) where you want store syslogs and other data retrieved from devices by KPIs and Playbooks. See Add Syslog Storage Providers, on page 134.
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 135

Provider Dependency

This section explains the provider configurations required for each Cisco Crosswork application and for Cisco Crosswork Network Controller (CNC).

Cisco Crosswork Network Controller is an integrated solution that combines Cisco Crosswork Active Topology (CAT) and Cisco Crosswork Optimization Engine (COE). You can also optionally integrate CNC with Cisco Crosswork Change Automation (NCA), Cisco Crosswork Health Insights (HI) and Cisco Crosswork Zero Touch Provisioning (ZTP).

Table 5: Provider Dependency matrix

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider	Cisco WAE Provider	Syslog Storage Provider	Alert Provider
Cisco Crosswork Network Controller (CNC) solution (combination of CAT & COE)	Mandatory Required protocols are HTTPS and NETCONF. Provider property key **forward** must be set as *true*.	Mandatory Required protocol is HTTP.	Optional	Optional	Optional

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider	Cisco WAE Provider	Syslog Storage Provider	Alert Provider
Cisco Crosswork Optimization Engine (COE)	Optional	Mandatory Required protocol is HTTP.	Optional	Optional	Optional
Cisco Crosswork Change Automation (NCA)	Mandatory Required protocol is NETCONF. Provider property key **forward** must be set as *true*.	Optional	Optional	Optional	Optional
Cisco Crosswork Health Insights (HI)	Mandatory Required protocol is NETCONF. Provider property key **forward** must be set as *true*.	Optional	Optional	Optional	Optional
Cisco Crosswork Zero Touch Provisioning (ZTP)	Optional	Optional	Optional	Optional	Optional

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 118. 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 136. 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 108.
- 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 6: 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: **MyWAE**. 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**.
*** Device Key**	Select the method that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way the Cisco Crosswork application maps the device in its own inventory to the device as it is stored in the Cisco NSO provider. Choices are: • **NODE_IP**—Use this value if the device identifier Cisco NSO uses is the IP address. • **INVENTORY_ID**—Use this value if the device identifier Cisco NSO uses is the inventory ID. • **HOST_NAME**—If Cisco NSO uses the device hostname as the device identifier, this value must match the hostname that is specified for the device in the inventory. Note that the **Device Key** is only required for the Cisco NSO provider. It is not needed for other providers.
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.
*** IP Address/ Subnet Mask**	Enter the IP address (IPv4 or IPv6) and subnet mask of the provider's server.

Field	Description
*** 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-interface`** and **`eth1`** respectively. This is most often necessary when creating the SR-PCE provider, as its management interface may reside on the data network instead of the management network.
Property Value	Enter the value to assign to the property key. To add more special properties for this provider, click ⊕ at the end of any key/value pair in the **Provider Properties** section. To delete a key/value pair you have entered, click ⊗ shown next to that pair.

Add Cisco NSO Providers

The Cisco Network Services Orchestrator (Cisco NSO) provider supplies the following functionality:

- Network services and device configuration services to Cisco Crosswork applications.
- Device management and configuration maintenance services.
- When using Crosswork Optimization Engine or the Cisco Crosswork Network Controller Automation solution:
  - Provisioning of SR-TE policies and RSVP-TE tunnels. The Cisco NSO core function pack provides SR-TE policy provisioning capability. The RSVP-TE sample function pack provides a starting point for RSVP tunnel provisioning, to be extended per customer needs.
  - Provisioning of Layer 2 and Layer 3 services running over SR-TE (ODN or preferred path). Cisco NSO provides sample function packs for provisioning of these services, allowing the services to be instantiated "as-is" or extended to meet specific needs using the APIs.

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.

Follow the steps below to add a Cisco NSO provider through the UI. 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 136).

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see Create Credential Profiles, on page 108).
- 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.

Note You can find the Cisco NSO and NED versions using the `version` and `package-version` commands, as shown in the below examples:

```
nso@nso-virtual-machine:~$ ncs --version
5.2.03
```

```
admin@ncs> show packages package  package-version
NAME                              PACKAGE VERSION
-----------------------------------------------
cisco-iosxr-cli-7.13                 7.13.9
```

- Know the Cisco NSO server IP address and hostname. 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 147.

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`**.
- **Device Key:** The device key is generally used as the default method of identifying devices if no attribute is set on the device itself. Select **Node IP** as the method that Cisco NSO uses to identify devices uniquely. This will serve as the way the Cisco Crosswork applications maps the device to Cisco NSO. Choices are: **`NONE`**, **`NODE_IP`**, **`INVENTORY_ID`**, or **`HOST_NAME`**. When using the Cisco Crosswork Network Controller solution, use **`HOST_NAME`**.
- Under Connection Type(s), **Protocol**: Select the protocol that Cisco Crosswork applications will use to connect to the provider. **`NETCONF`** is usually preferred.Enable both **`HTTPS`** (required when using the Cisco Crosswork Network Controller solution) and **`NETCONF`** (required when applications communicate to NSO as a southbound access) protocols.
- **IP Address/Subnet Mask**: Enter the IP address and subnet mask of the Cisco NSO server.
- **Port**:
  - For Netconf: Enter the port to use to connect to the Cisco NSO server. The default is **`2022`**.
  - 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**) from the drop-down list and enter its associated NED driver version. 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.

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.

Step 4 Under Provider Properties, enter a **Property Key** of **`forward`** and a **Property Value** of **`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. In cases where multiple providers are configured, only one provider (specifically an NSO provider) must have this property configured.

Step 5 When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

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 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:

- Create a credential profile for the Cisco SR-PCE provider (see Create Credential Profiles, on page 108). 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:

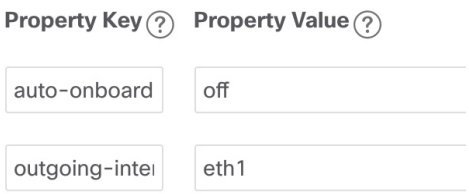
a) Required fields:

- **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**.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) 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 Cisco Crosswork Inventory Management database.
auto-onboard	**unmanaged** If this option is enabled, all devices that Cisco Crosswork discovers will be registered in the Cisco Crosswork 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.
auto-onboard	**managed** This option is only available for IPv4 deployments. If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork 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 (Router ID). The devices will be added with the credential profile associated with the device-profile key in the SR-PCE provider configuration. **Note** If you enable this option for an IPv6 deployment, devices will still register as **unmanaged** in the inventory.

Property Key	Value
`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`** or **`unmanaged`**.
`outgoing-interface`	`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.

Figure 8: Provider Property Key and Value Example



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 Cisco Crosswork. This avoids Cisco Crosswork from rediscovering and adding the device back.
- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork. However, doing so will not allow Cisco Crosswork 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 137). 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 three Cisco SR-PCE HA pairs (total of six SR-PCEs) to ensure high availability (HA). Each HA pair of Cisco SR-PCE providers must have matching configurations, supporting the same network topology.

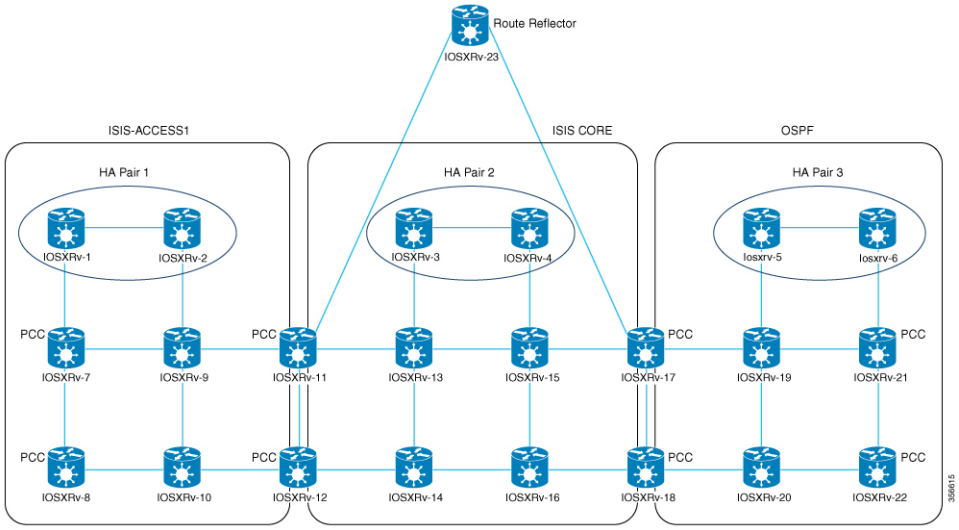
In HA, if the primary SR-PCE becomes unreachable, Cisco Crosswork Optimization Engine uses the secondary SR-PCE to discover the network topology. If this pair fails, then the next HA pair takes over and so forth. The network topology will continue to be updated correctly and you can view SR-PCE connectivity 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). In the figure below, 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 9: 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 rest 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.
- After an SR-PCE reloads, do the following:
  1. Execute the following command:

     ```
     # process restart pce_server
     ```

  2. From the UI, navigate to **Administration** > **Manage Provider Access**, remove and then add the provider again.
- 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 Cisco 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 136).

Before you begin

You will need to:

- Create a credential profile for the Cisco WAE provider (see Create Credential Profiles, on page 108). 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 136).

Before you begin

You will need to:

- Create a credential profile for the storage provider (see Create Credential Profiles, on page 108). 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 136).

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 108). 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.

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 139).

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.

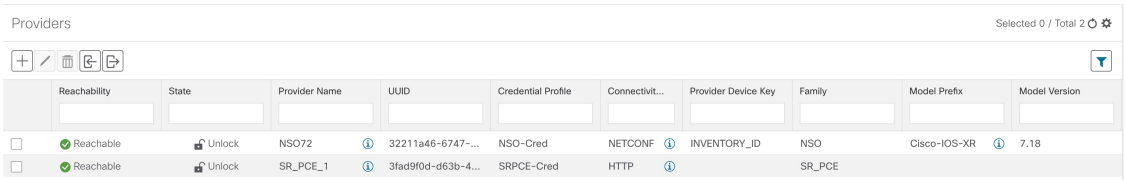
Step 6 Resolve any errors reported during the import and check provider details to confirm connection.

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, device key, and more, as shown in the figure below.

Figure 10: Providers Window



Step 2 The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols. For more information, see Reachability and Operational State, on page 155.

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 125. 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 122 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 139).

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 139).

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.

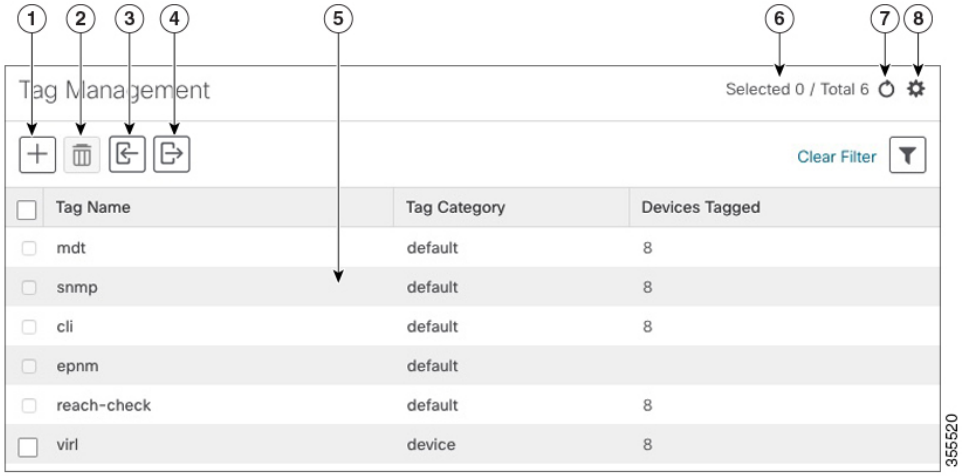
To open this window, choose **Administration** > **Tags**.

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 11: Tag Management Window



Item	Description
1	Click to create new device tags. See Create Tags, on page 141.
2	Click to delete currently selected device tags. See Delete Tags, on page 143.
3	Click to import the device tags defined in a CSV file into the Cisco Crosswork application. See Import Tags, on page 141. 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 143.
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 141.

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 142.

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 143).

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 142.

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).

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 143).

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

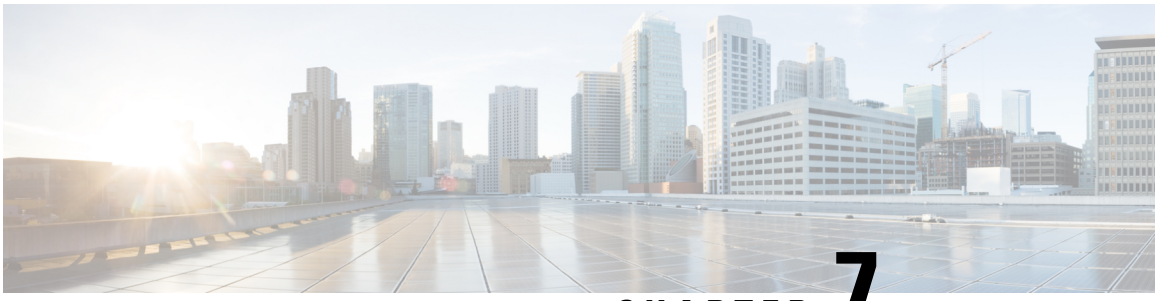
You can quickly export tags and tag categories to a CSV file. This will allow you to keep backup copies of your tags. You can also edit the CSV file as needed, and re-import it to overwrite existing tags. Note that you will need to re-associate devices and tags in some cases.

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 7

Onboard and Manage 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 Telemetry Prerequisites for New Devices, on page 146 and Sample Configuration for Cisco NSO Devices, on page 147.

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 is time-consuming and error-prone, as you must create and format all of the data yourself beforehand (including not only devices, but also the providers, credential profiles and tags), and then ensure all of these items are properly associated with the devices after the CSV import. 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 117.
   - Create corresponding credential profiles for all of the devices and providers listed in the CSV file. See Create Credential Profiles, on page 108.
   - Create tags for use in grouping the new devices. See Create Tags, on page 141.
   - 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 UI, on page 148.
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 122.
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 Zero Touch Provisioning, on page 165.

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 Cisco Crosswork Data Gateway interface, then it must be on the Cisco Crosswork Data Gateway's southbound network. This is because Cisco Crosswork Data Gateway implements 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.

Telemetry Prerequisites for New Devices

Before onboarding new devices, you must ensure that the devices are configured to collect and transmit telemetry data successfully with Cisco Crosswork. The following sections provide sample configurations for several telemetry options, including SNMP, NETCONF, SSH and Telnet. Use them as a guide to configuring the devices you plan to manage.

Note Only SNMPv2 and SNMPv3 (NoAuth/NoPriv) traps are supported.

Pre-Onboarding Device Configuration

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.

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
 exec-timeout 0 0
 width 107
 length 37
 absolute-timeout 0
```

```
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
 server <NTPServerIPAddress>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

SNMPv3 Pre-Onboarding Device Configuration

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>
```

Sample Configuration for Cisco NSO Devices

If you plan to use Cisco Network Services Orchestrator (Cisco NSO) as a provider to configure devices managed by Cisco Crosswork, be 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
set devices device RouterSFO address 198.18.1.12 port 830
```

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 UI

Follow the steps below to add devices one by one, using the UI. Under normal circumstances, you will want to use this method only when adding a few devices.

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 Click ⊞.

Step 3 Enter 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 7: Add New Device Window (*=Required)

Field	Description
*** Administration State**	The management state of the device. Options are • **UNMANAGED**—Crosswork 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 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 UI 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 host name 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 with the Inventory ID used as the device name.

Field	Description
Software Type	Software type of the device.
Software Version	Software version of the device.
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**, and **GNMI**. The capabilities 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.
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 will contain syslog events as received from 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 RFC5424 format. Refer to Section: Syslog Collection Job Output, on page 76 for more details.
Connectivity Details	
Protocol	The connectivity protocols used by the device. Choices are: **SSH**, **SNMP**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **GNMI**, and **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.
*** 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 **`PROTO`** and **`JSON IETF`**. Based on device capability, only one encoding format is supported at a time in a device.
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 Cisco Crosswork with the **TE Router ID** field populated.
Streaming Telemetry Config	
Vrf	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.

Field	Description
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.
Location All location fields are optional, with the exception of **Longitude** and **Latitude**, which are required for the geographical view of your network topology.	
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, in feet or meters, 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.
Provider Name	Provider name used for topology computation. Choose a provider from the list.
Credential	The Credential profile used for the provider. This field is read-only and is auto-populated based on the provider you select.
Device Key	This field is read-only and is auto-populated based on the provider you select.

Add Devices By Import From CSV File

Complete the steps below to create a CSV file that specifies multiple devices and then import it into Crosswork.

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 and device key 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

- While importing large number of devices via a CSV file, value for the **TE Router ID** field should be populated.
- Importing large number of devices with incorrect CSV values using a Firefox browser may render the window unusable. If this happens, login to Cisco Crosswork in a new tab or window, and onboard devices with correct CSV values.

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

- Confirm that the TE router ID value for each device is populated. This value is used to uniquely identify the device in the topology which is learned from SR-PCE. Without a valid TE router ID for each device, the topology will not be displayed.
- After importing a device or onboarding a device, the TE Router ID should not be changed. If it is necessary to change the TE Router ID of a device after it has been imported then then do the following:
  1. The device should be removed from Crosswork.
  2. All SR-PCE Providers should be removed.
  3. Onboard the device again with the new TE Router ID.
  4. Add the SR-PCE providers again.

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 UI, on page 148.

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 devices or providers via UI using a CSV file, user 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.

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 Cisco Crosswork Data Gateway instance.

Export Device Information to a CSV File

When you export the device list, all device information is exported 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.

The exported device CSV file will contain only the name of the credential profile for each device, not the credentials themselves.

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.

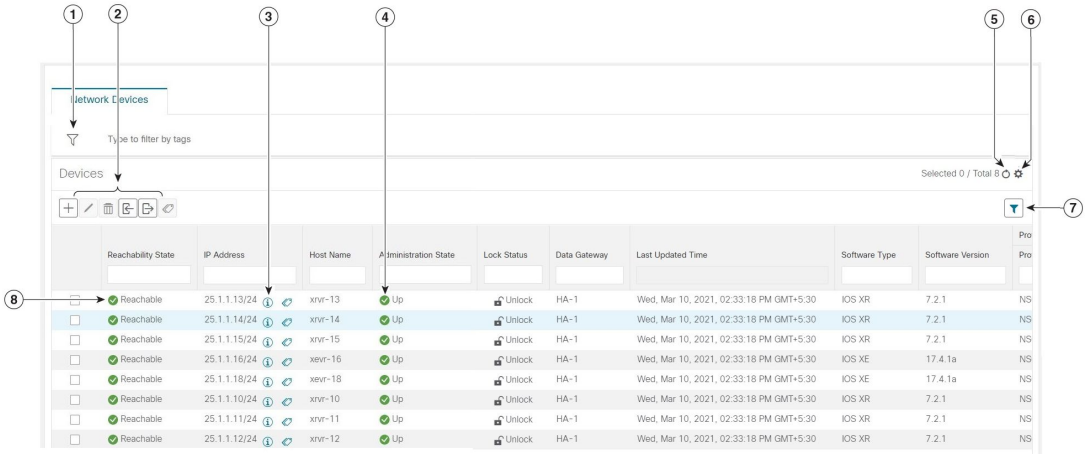
Step 3 Check the check boxes for the devices you want to export. Check the check box at the top of the column to select all the devices for export.

Step 4 Click the  . 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

Manage Network Devices

Cisco Crosswork's **Network Devices** window gives you a consolidated list of all your devices and their status. To view the **Network Devices** window, select **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

Figure 12: Network Devices Window



Item	Description
1	The **Filter by tags** field lets you filter the devices by the tags applied to them. Type the name of the tag that has been applied to the device that you are trying to find.
2	Click the to add a new device to the device inventory.
	Click the to edit the information for the currently selected devices. .
	Click the to delete the currently selected devices.
	Click the to import new devices and update existing devices, using 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.
	Click the to export information for selected devices to a CSV file.
	Click the to modify tags applied to the selected devices. See .
3	Click the to open the **Device Details** pop-up window, where you can view important information for the selected device.
4	Icons in the **Administration State** column show whether a device is operational or not.
5	Click the to refresh the Devices list.
6	Click the to select which columns to display in the Devices list.
7	Click to set filter criteria on one or more columns in the Devices list.
	Click the **Clear Filter** link to clear any filter criteria you may have set.
8	Icons in the **Reachability State** column show whether a device is reachable or not.

Reachability and Operational State

Cisco Crosswork computes the Reachability State of the providers it uses and devices it manages, as well as the Operational State of reachable managed devices. It indicates these states using the icons in the following table.

Table 8: Reachability and Operational State Icons

This Icon...	Indicates...
Reachability State icons show whether a device or a provider is reachable or not	
	Reachable: The device or provider can be reached by all configured protocols configured for it.
	Reachability Degraded: The device or provider can be reached by at least one protocol, but is not reachable by one or more of the other protocols configured for it.
	Unreachable: The device or provider cannot be reached by reachable by any protocol configured for it.
	Reachability Unknown: Cisco Crosswork cannot determine if the device is reachable, degraded, or unreachable . This state can also occur if the device is not connected to Cisco Crosswork Data Gateway.
Operational State icons show whether a device is operational or not.	
	The device is operational and under management, and all individual protocols are "OK" (also known as "up").
	The device is not operational ("down"). The same icon is used when the device has been set "administratively down" by an operator.
	The device's operational or configuration state is unknown.
	The device's operational or configuration state is degraded.

This Icon...	Indicates...
	The device's operational or configuration state is in an error condition. It is either not up, or unreachable, or both, due to errors encountered while attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of recent errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available in the Network Topology application).
	The device's operational state is currently being checked.
	The device is being deleted.
	The device is unmanaged.

The Reachability State of a device is computed as follows:

1. Reachability is always computed for each device as long as the device's configured state (as configured by users) is UP. It is not computed if the device is administratively DOWN or UNMANAGED.
2. Reachability state is always either REACHABLE, UNREACHABLE, or UNKNOWN.
   - The Reachability state is REACHABLE if there is at least one route to the device via at least one protocol AND the device is discoverable.
   - The Reachability state is UNREACHABLE if there are no routes to the device via one protocol OR the device does not respond.
   - The Reachability state is UNKNOWN if the device is UNMANAGED.

The Operational State of a device is computed as follows:

1. Operational state is always computed for each device as long as the device's configured state (as configured by users) is UP. It is not computed if the device is administratively DOWN or UNMANAGED.
2. Operational state is always OK or ERROR.
3. For a device to be Operational=OK, the device must be REACHABLE and discoverable. Any other Reachability state is ERROR.
4. For XR or XE devices only, Operational=OK also requires that Clock Drift difference between the Crosswork host and device clocks is <=the default Drift Value, currently 2 minutes.

Note Some timezone settings are known to result in Clock Drift errors when no clock drift actually exists. To work around this issue set your devices to use UTC time.

Filter Network Devices by Tags

By creating a tag and assigning it to a particular device, you can easily provide additional information that might be of interest to other users, such as the device's physical location and its administrator's email ID. You can also use tags to find and group devices with the same or similar tags in any window that lists devices.

To filter devices by tags:

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 In the **Type to filter by tags** bar at the top of the user interface, type all or part of the name of a tag.

The **Type to filter by Tags** bar has a type-ahead feature: As you start typing, the field shows a drop-down list of tags that match all the characters you have typed so far. To force the drop-down list to display all available tags, type *****.

Step 3 Choose the name of the tag you want to add to the filter. The filter appears in the **Type to filter by tags** filter bar. The table or map shows only the devices with that tag.

Step 4 If you want to filter on more than one tag:

a) Repeat Steps 2 and 3 for each additional tag you want to set as part of the filter.

b) When you have selected all the tags you want, click **Apply Filters**. The table or map shows only the devices with tags that match **all** the tags in your filter.

Step 5 To clear all tag filters, click the **Clear Filters** link. To remove a tag from a filter containing multiple tags, click the **X** icon next to that tag's name in the filter.

Get More Information About a Device

Whenever you select **Device Management** > **Network Devices** and display the list of devices under the **Network Devices** tab, you can click the next to any listed device to get more information about that device. Clicking this icon opens the **Details for DeviceName** pop-up window, as shown in the following example:

Figure 13: Details for DeviceName Window

Expand the **Connectivity Details** area at the top of the pop-up window (if it is not already expanded). This area shows the reachability status for all transport types.

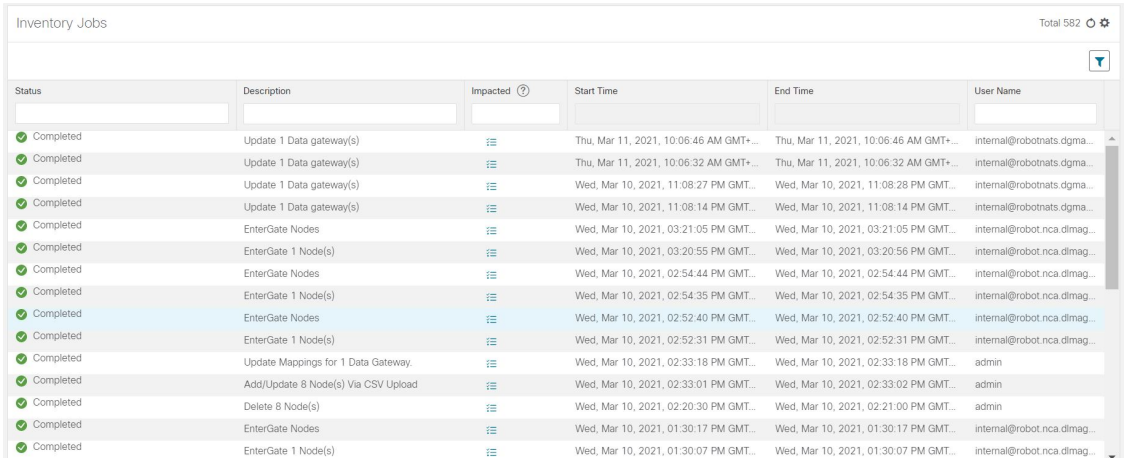
Expand and collapse the other areas of the pop-up window, as needed. Click the ✕ to close the window.

View Device Job History

Cisco Crosswork collects and stores information about device-related jobs. Follow the steps below to track all create, update and delete activities.

Step 1 From the main menu, choose **Device Management** > **Inventory Jobs**. The **Inventory Jobs** window opens displaying a log of all device-related jobs, like the one shown below.

Figure 14: Inventory Jobs window



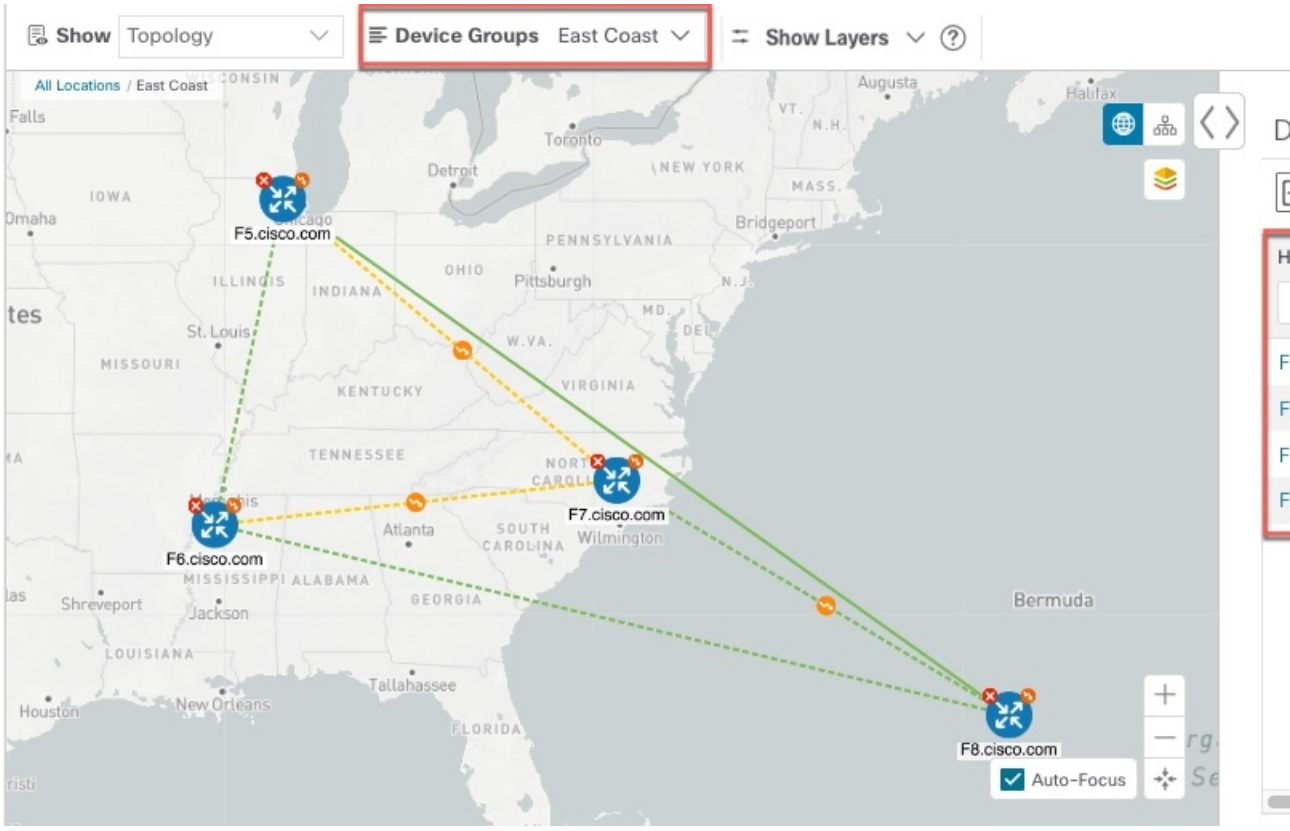
The jobs display in descending order of creation time. The most recent job is shown first. To sort the data in the table, click a column heading. Click the column heading again to toggle between ascending and descending sort order.

Step 2 The **Status** column shows the types of states: completed, failed, running, partial, and warning. For any failed or partial job, click the shown next to the error for more information.

Use Device Groups to Filter Your Topology View

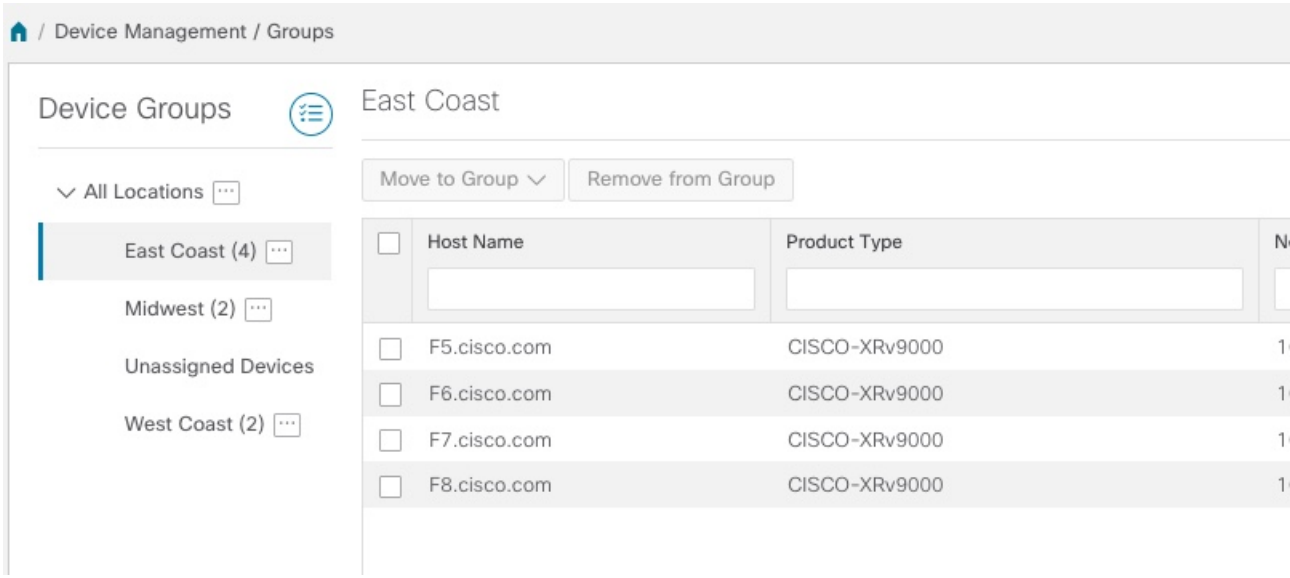
To help you identify, find, and group devices for a variety of purposes, you can create device groups. Device Groups allow you to visualize and zoom in on data specific to that device group. It reduces the clutter on your screen and allows you to focus on data that is most important to you. For example, as shown in the following figure, we see that the East Coast device group has been selected and is zoomed in on the Topology map. Also note that only the devices belonging to the East Coast device group are listed in the Devices table.

Figure 15: Device Group Selection on Topology Map



The **Device Groups** window (**Device Management** > **Groups**) allows you to create and manage device groups. By default, all devices initially appear in the **Unassigned Devices** group.

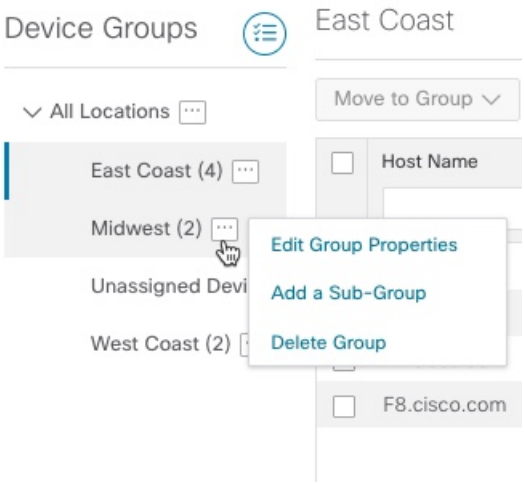
Figure 16: Device Groups Window



Create and Modify Device Groups

Step 1 From the main menu choose **Device Management** > **Groups**.

Step 2 From the Device Groups tree, click ⋯ next to a group.



Step 3 Choose to add, delete, or edit (rename or move) a group. If you delete a group, all devices that belong to that group are moved to the Unassigned Devices group.

Note Devices can belong to only one device group.

Step 4 Click **Save**.

Enable 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 hostname. Any newly added or discovered devices that matches the rule will be placed in the group.

Note Dynamic rules do not apply to devices that already belong in groups. You must move them to Unassigned Devices if you want to include them as part of the devices that the dynamic rule will consider.

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** > **Groups**.

Step 2 Click ☰.

Step 3 Click **Show more details and examples** to help you fill out the required Host Name and Group Name fields.

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 Check the **Enable Rule** checkbox. After the rule is enabled, the system checks devices every minute and will either create or assign them into groups.

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 corresponding group hierarchy.

Step 8 To move newly created Unassigned groups to the correct group, do the following:

a) Select **…** next to All Locations and click **Add a Sub-Group**.
b) Enter the New Group details and click **Save**.
c) Select **…** next to the unassigned created dynamic group and select **Edit Group Properties**.
d) Click **Change Parent Group** and select the appropriate group.

Edit Devices

Complete the following procedure to update a device's information.

Before editing any device, it is always good practice to export a CSV backup of the devices you want to change.

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 (Optional) Filter the list of devices by filtering specific columns.

Step 3 Check the check box of the device you want to change, then click the .

Step 4 Edit the values configured for the device, as needed.

Note In addition to the existing fields, you can also view the **Data Gateway** configured for the selected device. This field is read-only.

Step 5 Click **Save**. The Save button remains dimmed until all required fields are completed.

Step 6 Resolve any errors and confirm device reachability.

Delete Devices

Complete the following procedure to delete devices.

Before you begin

- If you set the autoonboard **managed** or **unmanaged** options for an SR-PCE provider, set autoonboard for one or more SR-PCEs to **off**.
- Confirm that the device is disconnected and powered off before deleting the device.

- If devices are mapped to Cisco NSO with MDT capability, and telemetry configuration is pushed, then those configurations will be removed from the device.
- If autoonboard isn't set to **off**, and it's still functional and connected to the network, the device will be rediscovered as unmanaged when it's deleted.

Step 1 Export a backup CSV file containing the devices that you plan to delete.

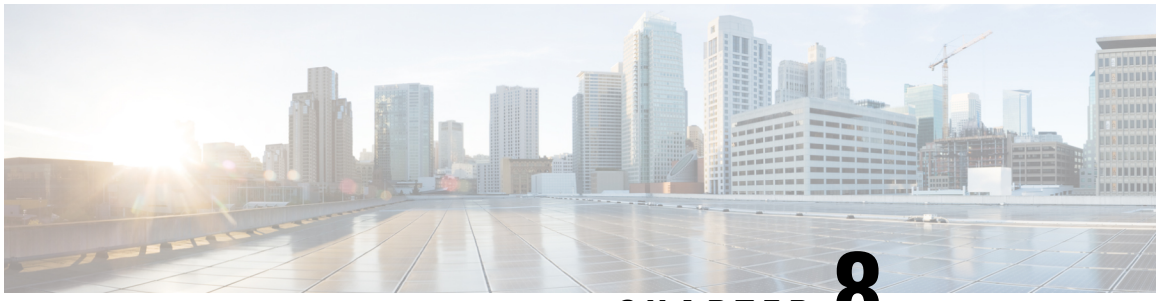
Step 2 From the main menu, choose **Device Management** > **Network Devices**.

Step 3 (Optional) In the **Devices** window, filter the list of devices by entering text in the **Search** field or filtering specific columns.

Step 4 Check the check boxes for the devices you want to delete.

Step 5 Click the  .

Step 6 In the confirmation dialog box, click **Delete**.



CHAPTER 8

Zero Touch Provisioning

This section contains the following topics:

Zero Touch Provisioning Concepts

The Cisco Crosswork Zero Touch Provisioning (ZTP) application allows you to provision networking devices remotely. You can ship factory-fresh devices to a branch office or remote site. Local operators can cable these devices to the network without installing an image or configuring them. To use ZTP, you first establish an entry for each device in the DHCP server and in the ZTP application. You can then activate ZTP processing by connecting the device to the network and powering it on or reloading it. ZTP downloads and applies a certified image and one or more configurations to the device automatically (you can also apply configurations only). Once configured, ZTP on boards the new device to the Cisco Crosswork device inventory. You can then use other Cisco Crosswork applications to monitor and manage the device.

Cisco Crosswork ZTP uses the following basic terms and concepts:

- **Classic ZTP**: A process to download and apply software and configuration files to devices. It uses iPXE firmware and HTTP to boot the device and perform downloads. It's not suitable for use over public networks.
- **Secure ZTP**: A secured process to download and apply software images and configuration files to devices. It uses secure transport protocols and certificates to verify devices and perform downloads.
- **Evaluation License Countdown**: Licenses for devices onboarded using ZTP have an evaluation period, normally 90 days. Cisco Crosswork displays a countdown banner throughout the evaluation period. Try to purchase a pool of licenses by the time the evaluation period expires. After expiration, Cisco Crosswork displays a warning banner and blocks onboarding of new devices until you apply purchased licenses.
- **Image file**: A binary software image file, used to install the network operating system on a device. For Cisco devices, these files are the supported versions of Cisco IOS-XR images. When configured to do so, the Classic ZTP process downloads the image from Cisco Crosswork and installs it using the open-source boot firmware iPXE. If you must install SMUs, ZTP applies them as part of configuration processing.
- **Configuration file**: A file used to set the operating parameters of the newly imaged or reimaged device. The file can be a Python script, Linux shell script, or a sequence of Cisco IOS CLI commands stored as

ASCII text. The ZTP process downloads the configuration file to the newly imaged device, which then executes it. ZTP processing requires configuration files.

- **Credential profile**: Collections of passwords and community strings that are used to access devices via SNMP, SSH, HTTP, and other network protocols. Cisco Crosswork uses credential profiles to access your devices, automating device access. All credential profiles store passwords and community strings in encrypted format.
- **Bootfile name**: The explicit path to and name of a software image that is stored in the ZTP repository. For each device you plan to onboard using ZTP, specify the bootfile name as part of the device configuration in DHCP.
- **HTTPS/TLS**: Hypertext Transport Protocol Secure (HTTPS) is a secure form of the HTTP protocol. It wraps an encrypted layer around HTTP. This layer is the Transport Layer Security (TLS) (formerly Secure Sockets Layer, or SSL).
- **iPXE**: The open-source boot firmware iPXE is the popular implementation of the Preboot eXecution Environment (PXE) client firmware and bootloader. iPXE allows devices without built-in PXE support to boot from the network. The iPXE boot process is part of Classic ZTP processing, and isn't part of Secure ZTP processing. However, on-site technicians can still force iPXE boot and then begin Secure ZTP processing.
- **Owner certificate**: The CA-signed end-entity certificate for your organization, which binds a public key to your organization. You install owner certificates on your devices.
- **Ownership Voucher**: Nonceless audit vouchers that verify that devices onboarded with ZTP are bootstrapping into a domain your organization owns. Cisco supplies OVs in response to requests from your organization.
- **PDC**: A Pinned Domain Certificate (PDC) is the CA- or self-signed domain certificate of your organization. The public key of the PDC pins the PDC to the DNS network domain assigned to your organization. The PDC helps your devices verify that images and configurations that are downloaded and applied during ZTP processing come from within your organization.
- **SUDI**: The Secure Unique Device Identifier (SUDI) is a certificate with an associated key pair. The SUDI contains the product identifier and serial number. Cisco inserts the SUDI and key pair in the device hardware Trust Anchor module (TAm) during manufacturing, giving the device an immutable identity. During Secure ZTP processing, the back-end system challenges the device to validate its identity. The router responds using its SUDI-based identity. This exchange, and the TAm encryption services, permit the back-end system to provide encrypted image and configuration files. Only the specific router can open these encrypted files, ensuring confidentiality in transit over public networks.
- **SUDI Root CA Certificates**: A root authority certificate for SUDIs, issued and signed by a Certificate Authority (CA), used to authenticate subordinate SUDI certificates.
- **UUID**: The Universal Unique Identifier (UUID) uniquely identifies an image file that is uploaded to Cisco Crosswork. You can use the UUID of the software image file in the DHCP bootfile URL. UUIDs are not required for configuration files.
- **ZTP asset**: ZTP requires access to several types of files and information in order to onboard new devices. We refer to these files and information collectively as "ZTP assets." You load these assets as part of ZTP setup, before initiating ZTP processing.
- **ZTP profile**: A Cisco Crosswork storage construct that combines (normally) one image and one configuration into a single unit. Cisco Crosswork uses ZTP profiles to automate imaging and configuration processes. Using ZTP profiles is optional, but we recommended them. They are an easy way to organize

ZTP images and configurations around device families, classes, and roles, and help maintain consistent ZTP use.

- **ZTP repository**: The location where Cisco Crosswork stores ZTP image and configuration files.

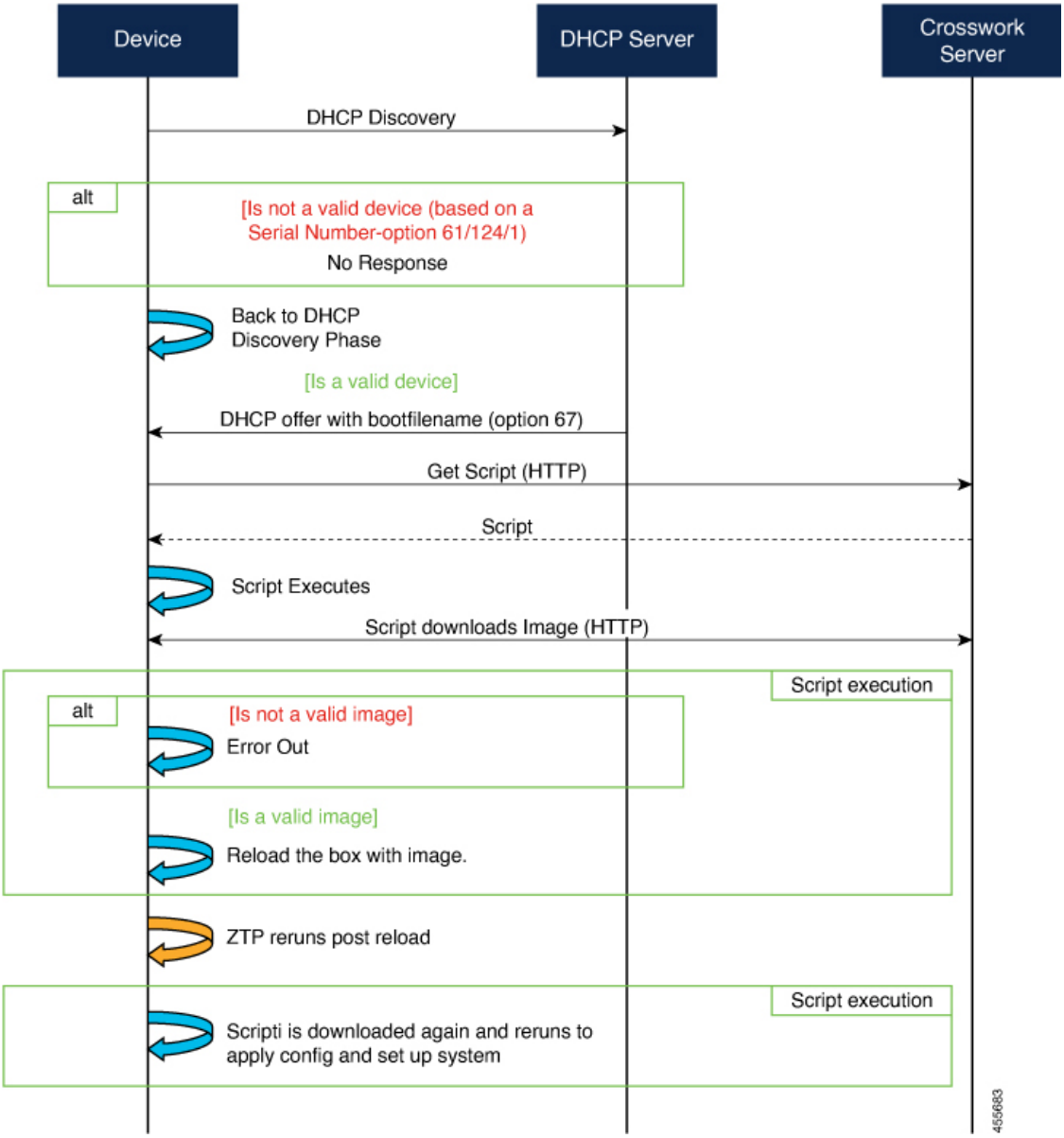
ZTP Processing Logic

Cisco Crosswork ZTP processing differs depending on whether you choose to implement Classic ZTP or Secure ZTP.

Classic ZTP Logic

The following illustration shows the processing logic that Classic ZTP uses to provision and onboard devices. The DHCP server verifies the device identity based on the device serial number, then offers downloads of the boot file and image. Once ZTP images the device, the device downloads the configuration file and executes it.

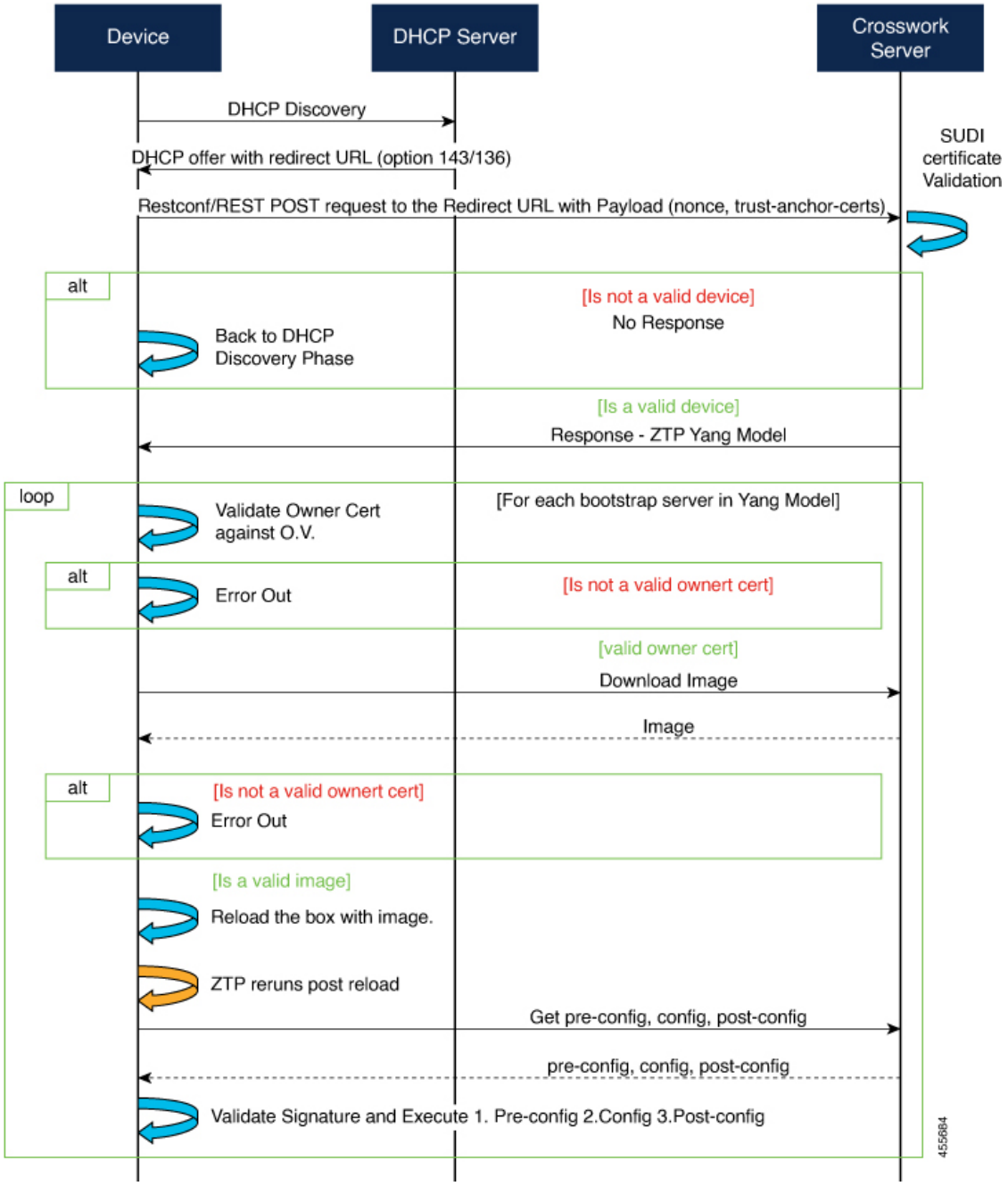
Figure 17: Classic ZTP Processing Logic



Secure ZTP Logic

The following illustration shows the process logic that Secure ZTP uses to provision and onboard devices. The device and the ZTP bootstrap server authenticate each other using the Secure Unique Device Identifier (SUDI) on the device and server certificates over TLS/HTTPS. Over a secure HTTPS channel, the bootstrap server lets the device download signed image and configuration artifacts. These artifacts must adhere to the RFC 8572 YANG schema. Once the device installs the new image (if any) and reloads, the device downloads configuration scripts and executes them.

Figure 18: Secure ZTP Processing Logic



ZTP State Transitions

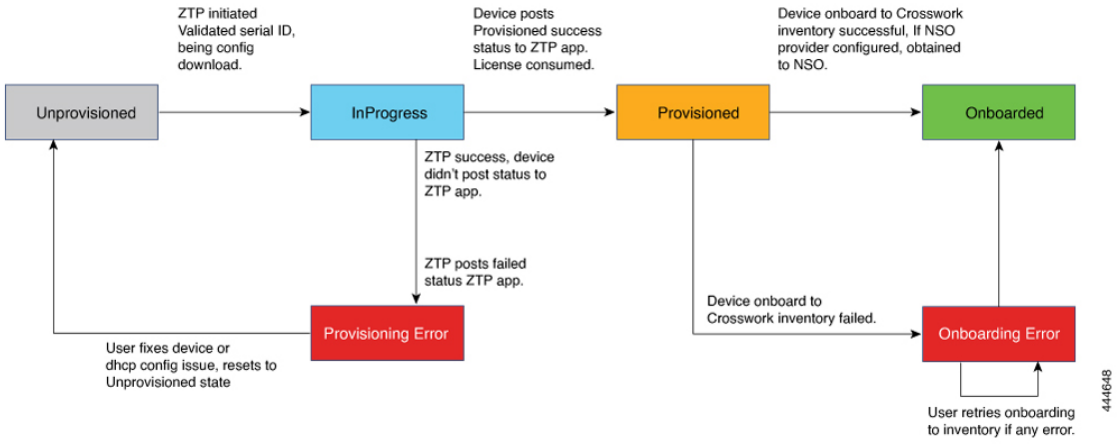
Once initiated by a device reset or reload, the ZTP process proceeds automatically. Cisco Crosswork also updates the Zero Touch Devices window with status messages showing which stage of the process each device has reached. The states and their transitions differ between Classic and Secure ZTP, as explained in the next two sections.

The configuration scripts you use with ZTP must report device state changes to Cisco Crosswork using Cisco API calls. Failure to do so means Cisco Crosswork can't register state changes when they occur, resulting in failed provisioning and onboarding. To see examples of these calls, select **Device Management** > **ZTP Configuration Files**, then click **Download Sample Script**.

Classic ZTP State Transitions

The following figure shows the state changes for Classic ZTP processing.

Figure 19: Classic ZTP Device State Transitions



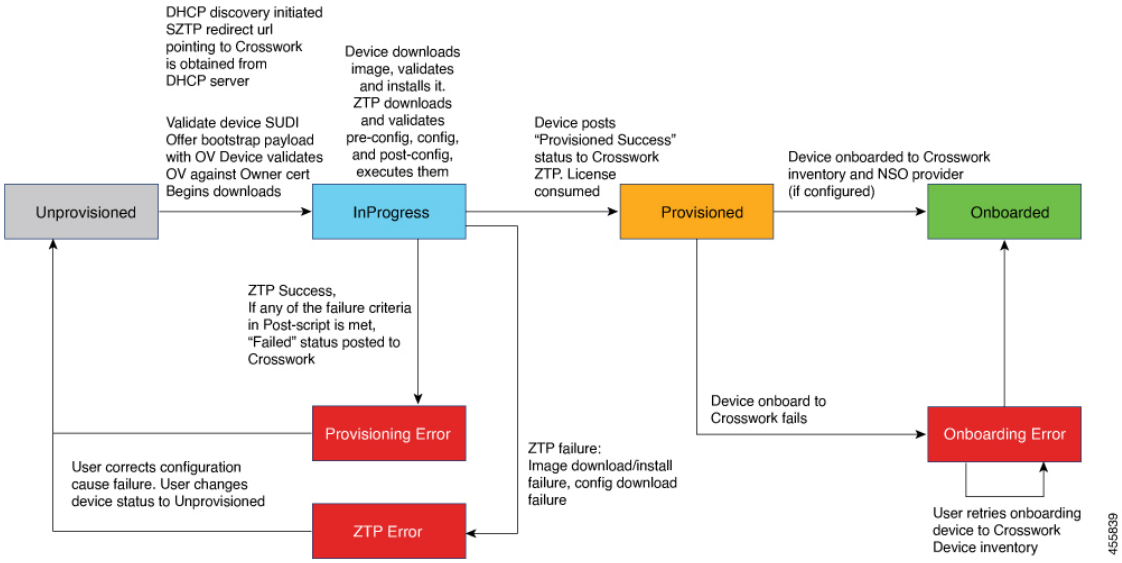
Classic ZTP device entries start out in the **Unprovisioned** state. After you initiate ZTP, devices transition to the **InProgress** state, when they connect to the network and start downloading image and configuration files. The device remains in the **InProgress** state until it reports either that it ran into a **Provisioning Error** or that it's **Provisioned**. If provisioning is successful, the device transitions to the **Provisioned** state. Once provisioned, Cisco Crosswork onboards the device. If Cisco NSO is a Cisco Crosswork provider, Cisco NSO also onboards the device. If onboarding is successful, the device state changes to **Onboarded**. It's now part of inventory and you can monitor and manage it like any other Cisco Crosswork network device.

Classic ZTP is successful when the device loads its image and/or configuration code successfully, connects with Cisco Crosswork, and reports a **Provisioned** status. This status change causes one license to be counted for that device serial number. Because the license is tied to the serial number, later transition to the **Onboarded** state, or any further ZTP processing, doesn't affect the license count.

Secure ZTP State Transitions

The following figure shows the state changes for Secure ZTP processing.

Figure 20: Secure ZTP State Transitions



Secure ZTP device entries start out in the **Unprovisioned** state. After you initiate ZTP, the device and the bootstrap server validate each other and the payload. The two use the device SUDI, ownership vouchers and device owner certificates to validate over HTTP/TLS. After validation, the device entry transitions to the **InProgress** state, when it connects to the network and starts downloading image and configuration files. The device remains in the **InProgress** state until it posts a **Provisioning Error**, **ZTP Error** or **Provisioned** status to Cisco Crosswork. If the provisioning is successful, the device transitions to the **Provisioned** state. Once provisioned, Cisco Crosswork onboards the device. If Cisco NSO is a Cisco Crosswork provider, Cisco NSO also onboards the device. If onboarding is successful, the device state changes to **Onboarded**. It's now part of inventory and you can monitor and manage it like any other Cisco Crosswork network device.

If any of the validation steps fail, Secure ZTP posts a **Provisioning Error**. If the image or configuration code fails verification or installation, Secure ZTP posts a **ZTP Error** instead. Like Classic ZTP, Secure ZTP is successful when the device loads its image and/or configuration code successfully, connects with Cisco Crosswork, and posts a **Provisioned** status. License consumption is the same as in Classic ZTP.

ZTP and Evaluation Licenses

All licenses start with an evaluation period of 90 days. When the evaluation period expires, Cisco Crosswork displays a banner warning users that evaluation licenses have expired. While ZTP displays this banner, it blocks some operations, including configuration downloads. When your organization enrolls in smart licensing and applies licenses to some of the onboarded devices, ZTP removes the block. ZTP displays the warning banner until you license all your onboarded devices.

Your onboarded ZTP devices are always associated with either:

- A serial number, or
- The values of the Option 82 location ID attributes (remote ID and circuit ID).

Serial numbers and location IDs form an "allowed" list. ZTP uses this list when deciding to onboard a device and assign it a license. If you delete an onboarded ZTP device from inventory, and then onboard it again later, use the same serial number or location ID. If you use a different serial number or location ID, you may consume

an extra license. The current release provides no workaround for this scenario. In any case, you can't have two different ZTP devices with the same serial number or location ID active at the same time.

Platform Support for ZTP

This topic details Cisco Crosswork Zero Touch Provisioning support for Cisco and third-party software and devices.

Platform Support for Classic ZTP

The following platforms support Classic ZTP:

- **Software**: Cisco IOS-XR versions 6.6.3, 7.0.1, 7.0.2, 7.0.12, and 7.3.1 or later.
- **Hardware**:
  - Cisco Network Convergence Systems (NCS) 540 Series Routers
  - Cisco NCS 1000-1004 Series Routers
  - Cisco NCS 5500 Series Routers
  - Cisco NCS 8000 and 8800 Series Routers (Spitfire fixed mode)

Classic ZTP doesn't support third-party devices or software.

Platform Support for Secure ZTP

The following platforms support Secure ZTP:

- **Software**: Cisco IOS-XR version 7.3.1 or later.

  You can upgrade from IOS-XR 6.6.3 to 7.3.1 as a single image installation.
- **Hardware**:
  - Cisco Network Convergence Systems (NCS) 540 Series Routers
  - Cisco NCS 1000-1004 Series Routers
  - Cisco NCS 5500 Series Routers
  - Cisco NCS 8000 and 8800 Series Routers (Spitfire fixed mode)

Secure ZTP supports provisioning for third-party devices only if the third-party devices:

- Are 100-percent compliant with the Secure ZTP RFC 8572(https://tools.ietf.org/html/rfc8572).
- Match Cisco format guidelines for serial numbers in device certificates and ownership vouchers. For details, see the following section, "Guidelines for Third-Party Device Certificates and Ownership Vouchers."

Guidelines for Third-Party Device Certificates and Ownership Vouchers

Secure ZTP processing for any device starts with a successful HTTPS/TLS handshake between the device and Cisco Crosswork. After the handshake, Secure ZTP must extract a serial number from the device certificate.

Secure ZTP then validates the extracted serial number against its internal "allowed" list of serial numbers. You create the allowed list by uploading device serial numbers to Cisco Crosswork. A similar serial-number validation step occurs later, when validating downloads using ownership vouchers.

Unlike Cisco IOS-XR devices, the format of the serial number in third-party vendors' device certificates is not standardized across vendors. Typically, a third-party vendor's device certificate has a `Subject` field or section. The `Subject` contains multiple key-value pairs that the vendor decides upon. One of the key-values pairs is usually a `serialNumber` key. This key's value contains the actual device serial number as a string, which is preceded by the string `SN:`. For example: Let's suppose that the third-party device certificate's `Subject` section contains the following key and value: `serialNumber = PID:NCS-5501 SN:FOC2331R0CW`. Secure ZTP will take the value after the `SN:` string and match that to one of the serial numbers in the allowed list.

If the third-party vendor's device certificate has a different format, validation failures can occur. The degree of failure depends on the degree of difference. The vendor certificate may not match this format at all. The certificate's `Subject` field may not contain a `serialNumber` key with a value that contains the `SN:` string. In this case, Secure ZTP processing falls back to using the whole string value of the `serialNumber` key (if present) as the device serial number. It will then try to match that value to one in the allowed list of serial numbers. These two methods – string matching and the fallback – are the only means Secure ZTP has for determining the third-party device's serial number. If the vendor certificate differs from this expectation sufficiently, Secure ZTP may be unable to validate the device at all.

Secure ZTP has similar format expectations for ownership vouchers. Cisco tools generate ownership vouchers with filenames in the format *`SerialNumber`*`.vcj`, where *`SerialNumber`* is the device's serial number. Secure ZTP extracts the serial number from the filename and then attempts to match it to one in the allowed list. For multivendor support, we assume that third-party vendor tools generate OV files in the same format. If this expectation isn't met, validation failures are likely.

ZTP Implementation Decisions

ZTP offers a range of implementation choices and cost vs. benefit tradeoffs worth considering in advance:

- **When to Use Classic ZTP**: Classic ZTP is easier to implement than Secure ZTP. It needs no PDC, owner certificates, or ownership vouchers. It’s less subject to processing errors, as device and server verification is less stringent and setup is less complex. It’s your only choice if your Cisco devices run IOS XR versions earlier than 7.3.1, as Secure ZTP doesn’t support them. Although Classic ZTP new includes a device serial-number check, it remains insecure at the transport layer. It's not recommended if routes to your remote devices cross a metro or otherwise unsecured network.
- **When to Use Secure ZTP**: Use Secure ZTP when you must traverse public networks and you have devices that support Secure ZTP. The additional security that it provides requires a more complex setup than Classic ZTP. This complexity can make processing error-prone if you’re new to the setup tasks. Secure ZTP setup also requires a certificates and ownership vouchers from the device manufacturer. Use it if your devices are from third-party manufacturers, as Classic ZTP doesn't support third-party hardware. Third-party devices and their software must be 100-percent compliant with RFCs 8572 and 8366. Device certificates for third-party devices must contain the device serial number. Third-party ownership vouchers must be in a format that uses the device serial number as the filename. Cisco can’t guarantee Secure ZTP compatibility with all third-party devices. For more details on third-party device support, see Platform Support for ZTP, on page 172.
- **Use ZTP With Imaged Devices**: There’s no need to specify a software image when you use Classic or Secure ZTP. This feature allows you the option of shipping to your remote location one or more devices on which you have already installed a software image. You can then connect to these devices and trigger ZTP processing remotely. Depending on how you set up things, you can apply:

- A configuration only
- One or more images or SMUs, with more configurations.

All licenses start with an evaluation period of 90 days. When the evaluation period expires, Cisco Crosswork displays a banner warning users that evaluation licenses have expired. While ZTP displays this banner, it blocks some operations, including configuration downloads. When your organization enrolls in smart licensing and applies licenses to some of the onboarded devices, ZTP removes the block. ZTP displays the warning banner until you license all your onboarded devices.

Secure ZTP offers more flexibility with preimaged devices because it offers preconfiguration, day-zero, and postconfiguration script execution capability. But both ZTP modes can chain configuration files that load images, SMUs and configurations.

In both cases, the result is to onboard the device. Once onboarded to Cisco Crosswork, you can't use ZTP to configure the device.

- **Organize Configurations**: Keep your configurations as consistent as possible across devices. Consistency makes solving problems easier. It minimizes the amount of extra configuration you must perform to bring new devices online. It also reduces the number of "special" things to keep in mind when it comes time to reconfigure or upgrade your devices. Start by ensuring that all devices from the same device family and with similar roles have the same or similar basic configurations.

  How you define the role that a device plays depends on your organization, its operational practices, and the complexity of your network environment. For example: Suppose that your organization is a financial services enterprise. It has three types of branches: Sidewalk ATMs, retail branches open during standard business hours, and private trading offices. You could define three sets of basic profiles covering all the devices at each type of branch. You can map your configuration files to each of these profiles.

  Another method of enforcing consistency is to develop basic script configurations for similar types of devices, then use the script logic to call other scripts. If you're using Classic ZTP, the script is in the specified configuration file. That script downloads the basic configuration, then downloads other scripts depending on the branch type. If using Secure ZTP, you have even more flexibility, as you can specify preconfiguration and postconfiguration scripts in addition to the main or day-zero configuration script.

ZTP Setup Workflow

Zero touch provisioning requires you to complete the following setup tasks first, before you can trigger ZTP boot and configuration:

1. Make sure that your environment meets ZTP prerequisites for security, provider configuration, and device connectivity.
2. Assemble the assets ZTP needs for processing. These assets include:
   - The software image to install.
   - The configurations to apply.
   - Credentials to access the device.
   - Device serial numbers.

   If you're using Secure ZTP, these assets also include device owner certificates, the PDC, and ownership vouchers.

3. Load into Cisco Crosswork the ZTP assets you have assembled.
4. Create credential profiles using the credential assets that you assembled.
5. Prepare ZTP device entry files. These files create the Cisco Crosswork device entries that ZTP uses to onboard the devices to the Cisco Crosswork device inventory. If you have many devices to onboard, create the entries in bulk by importing a CSV file. If you have only a few devices to onboard, it's more convenient to prepare these entries one by one, using the Cisco Crosswork UI.

The remaining topics in this section discuss how to perform each of these tasks.

Meet ZTP Prerequisites

For compatibility with ZTP, your Cisco Crosswork installation must meet the following prerequisites:

- If you're using Classic ZTP to onboard any device, ensure that Cisco Crosswork and the devices are in a secure network domain.
- If you want ZTP to onboard your devices to Cisco NSO, configure NSO as a Cisco Crosswork provider. Be sure to set the NSO provider property key to `forward` and the property value to `true`.
- The Cisco Crosswork cluster must be reachable from the devices, and the cluster from the devices, over either an out-of-band management network or an in-band data network. For a general indication of the scope of these requirements, see the network diagrams in the "Network Requirements" section of the *Cisco Crosswork Infrastructure 4.0 and Applications Installation Guide*. Enabling this kind of access may require you to add static routes and change firewall configurations.

Assemble ZTP Assets

Both Classic and Secure ZTP require that you collect the following ZTP assets:

- **Software images**: The installable operating system software, such as Cisco IOS-XR, that enables the network device to function. Cisco distributes images as TAR, ISO, or RPM files. Each image file represents a single release of the given network OS for a given device platform or family. Upload image files to Cisco Crosswork one at a time, and enter each the MD5 checksum for each software image file. Cisco Crosswork uses the MD5 checksum to validate the integrity of the file. Be sure to record the checksum when you download device images from Cisco or any third-party manufacturer. You can also generate your own MD5 checksum for an image you want to upload.
- **Software Maintenance Updates (SMUs)**: Cisco software packages that provide point fixes for one or more critical issues in a given software release. Cisco distributes SMUs in nonbootable format with a readme.txt file explaining the associated issues. Cisco rolls SMU contents into the next maintenance release of a software image. Apply SMUs using configuration files, not during software image download. Upload SMUs to Cisco Crosswork one at a time.

  Cisco customers with current devices and valid support contracts can find and download Cisco software images and SMUs using the Cisco Support & Downloads page.
- **Configurations**: ZTP uses configuration files to configure the features of the installed software image on a given device, including upgrading the software using SMUs. Configuration files can be Linux shell scripts (SH), Python scripts (PY), or device operating system CLI commands stored in an ASCII text file (TXT). Your organization or consultants create configurations. Upload configuration files to Cisco Crosswork one at a time. Your custom configuration code can use replaceable parameters and must use

Cisco Crosswork API calls to complete many tasks. In particular, the code must use API calls to notify the Cisco Crosswork server when the device transitions from one ZTP state to another. For examples of how to use these parameters and API calls, see the sample ZTP configuration file. You can download the sample ZTP configuration file from Cisco Crosswork by selecting **Device Management** > **ZTP Configuration Files**, then clicking **Download Sample Script**. For more details, see the following sections, "Default Replaceable Parameters" and "Create Custom Replaceable Parameters". Secure ZTP allows you to load pre-, post-, and day-zero configuration files.

- **Credentials**: The user names and passwords that Cisco Crosswork uses to access a device and control it. You load them as credential profiles, and Cisco Crosswork stores them in encrypted form. You can create credential profiles one at a time using the GUI, or load them in bulk by downloading and modifying a credential profile CSV file.
- **Serial numbers**: The serial numbers of the devices you plan to onboard using ZTP. Enter serial numbers for each device you're planning to onboard using either Classic or Secure ZTP. Load serial numbers in bulk, by importing a CSV file, before creating device entries. If you're planning to use Secure ZTP, submit the serial numbers to Cisco when requesting ownership vouchers.

If you plan to use Secure ZTP, assemble the following extra ZTP assets:

- **Owner certificates**: Load both the owner certificates and the owner key to Cisco Crosswork, so it can generate leaf certificates for each of your devices.
- **Pinned Domain Certificate (PDC)**: Load the PDC to Cisco Crosswork along with your owner certificates. You also submit the PDC to Cisco when requesting ownership vouchers.
- **Ownership vouchers (OVs)**: Load your OVs with the other certificates. Submit your PDC and device serial numbers when you request OVs from Cisco or third party manufacturers. Cisco returns the OVs to you when they are ready, as one or more VCJ files in a Tarball. This exchange takes place using a secure method agreed upon by you and your Cisco account team. If you're using vouchers for third-party devices, the VCJ files the manufacturer supplies must follow the naming convention `serial.vcj`, where `serial` is the serial number of the corresponding device. Cisco Crosswork requires this file naming convention in order to map the ownership voucher to the device.
- **SUDI Root CA certificates**: Load SUDI Root CA certificates at the same time as other certificates and OVs. Cisco SUDI root certificates are available for customer download at the Cisco PKI: Policies, Certificates, and Documents page (https://www.cisco.com/security/pki/policies/index.html).

Some organizations maintain libraries of approved assets. If your organization has a library like this, ensure that these assets are easily accessible from your client machine. Doing so makes it easier for you to complete ZTP setup.

Default Replaceable Parameters

The following table lists the default replaceable parameters you can use in your custom configuration files. At runtime, for each of these placeholders, Cisco Crosswork substitutes the appropriate values for each device. For an example of the use of these placeholders, download the sample configuration script from Cisco Crosswork as explained in the preceding section of this topic.

Table 9: Default Parameters in ZTP Configuration Files

Cisco Crosswork substitutes this placeholder...	...using the value from the...
{$HOSTNAME}	Host name of the device as specified in the ZTP device entry.
{$IP_ADDRESS}	IP address of the device, as assigned by DHCP.
{$SSH_USERNAME}	The value of the **User Name** field in the credential profile (when the **Connectivity Type** is **SSH**).
{$SSH_PASSWORD}	The value of the **Password** field in the credential profile (when the **Connectivity Type** is **SSH**).
{$SSH_ENPASSWORD}	The value of the **Enable Password** field in the credential profile (when the **Connectivity Type** is **SSH**)
{$SNMP_READ_COM}	The value of the **Read Community** field in the credential profile (when the **Connectivity Type** is **SNMPv2**).
{$SNMP_WRITE_COM}	The value of the **Write Community** field in the credential profile (when the **Connectivity Type** is **SNMPv2**).
{$SNMP_SEC_LEVEL}	The value of the **Security Level** field in the credential profile (when the **Connectivity Type** is **SNMPv3**).
{$SNMP_USERNAME}	The value of the **User Name** field in the credential profile (when the **Connectivity Type** is either **SNMPv2** or **SNMPv3**).
{$SNMP_AUTH_TYPE}	The value of the **User Name** field in the credential profile (when the **Connectivity Type** is **SNMPv3** and **Security Level** is **AUTH_NO_PRIV**) or **AUTH_PRIV**).
{$SNMP_AUTH_PASS}	The value of the **User Name** field in the credential profile (when the **Connectivity Type** is **SNMPv3** and **Security Level** is **AUTH_NO_PRIV** or **AUTH_PRIV**).
{$SNMP_PRIV_TYPE}	The value of the **User Name** field in the credential profile (when the **Connectivity Type** is **SNMPv3** and **Security Level** is **AUTH_PRIV**).
{$SNMP_PRIV_PASS}	The value of the **Priv Password** field in the credential profile (when the **Connectivity Type** is **SNMPv3** and **Security Level** is **AUTH_PRIV**).

Custom Replaceable Parameters

You can create your own replaceable parameters in configuration files, as shown in the following example.

```
!
hostname {$name}
username {$ssh_name}
 group root-lr
 group cisco-support
 secret {$ssh_pwd}
!
```

```
tpa
 vrf default
 !
!
call-home
 service active
 contact smart-licensing
 profile CiscoTAC-1
  active
  destination transport-method http
 !
!

interface loopback1
 ipv4 address {$ip1}
interface loopback2
 ipv4 address {$ip2}
```

Load ZTP Assets

Before creating credential profiles, upload the ZTP assets you assembled.

Both Classic and Secure ZTP require you to load:

- Software images
- SMUs
- Configuration files
- Device serial numbers

Secure ZTP requires you to load:

- Pinned domain certificate
- Ownership certificates
- Ownership Vouchers

You may use a mapped network drive to upload software images, SMUs, and configuration files.

Cisco Crosswork checks for duplicate serial numbers and merges them into single entries automatically. Cisco Crosswork also associates all uploaded ownership vouchers with existing serial numbers automatically.

You can upload images, configuration files, and serial numbers in any order. Load the certificates and ownership vouchers only after loading serial numbers.

Step 1 Upload images and SMUs:

a) From the main menu, select **Device Management** > **Software Images** and then click  .

b) Enter the required image or SMU file information and then click **Add**.

You must enter the MD5 checksum for the file.

You can also click **Browse** to select the ISO, TAR, or RPM file.

c) Click and repeat step 1b until you have loaded all the image and SMU files.

Step 2 Upload configuration files and scripts:

a) From the main menu, select **Device Management** > **Configuration Files** and then click the +.
b) Enter the required configuration file information and then click **Add**. You can click **Browse** to select the PY, SH, or TXT configuration file.
c) Click + and repeat step 2b until you have loaded all the configuration files. If you're implementing Secure ZTP, include your pre-, post-, and main or day-zero configuration files.

Step 3 Upload device serial numbers:

a) From the main menu, select **Device Management** > **Serial Number and Voucher**, then click **Add Serial Number**.
b) Click **Upload CSV**, then click the **serialnumber.csv** link to download the sampleSerialnumber.csv file.
c) Using your choice of CSV file editor, enter into the template the serial numbers for all the devices you plan to onboard using ZTP. Save the updated CSV file template under a new name.
d) Select **Add Serial Number** again. Click **Browse** to select the updated CSV file, then click **Add Serial Number** to import the serial numbers.

Step 4 Continue with the following steps if you plan to implement Secure ZTP.

Step 5 Upload your pinned domain certificate, owner certificates, and SUDI Root CA certificates:

a) From the main menu, select **Administration** > **Certificate Management**, then click +.
b) In **Certificate Name**, enter a name for this certification grouping.
c) In **Certificate Role**, select **Secure ZTP Provisioning**.
d) Click **Browse** to select the **Pinned Domain CA Certificate**, **Owner Certificate**, and **Owner Key**files.
e) Click **Save**.

Step 6 Upload ownership vouchers:

a) From the main menu, select **Device Management** > **Serial Number and Voucher**, then click **Add Voucher**.
b) Click **Browse** to select the Cisco-supplied VCJ file (or, if there's more than one voucher, the TARball containing the ownership vouchers) . Then click **Upload**.

If you're uploading vouchers for third-party devices, the uploaded VCJ file or files in the TARball must follow the naming convention `serial.vcj`. In this convention, `serial` is the serial number of the corresponding device. Cisco Crosswork requires naming in order to map the ownership voucher to the device.

Create Credential Profiles for ZTP

Cisco Crosswork ZTP requires credential profiles in order to access and configure your devices. The following steps show how to add them in bulk using a CSV file. To add credential profiles one by one, select **Device Management** > **Credential Profiles**, then click the +.

It's good practice to create SNMP credential profiles only for the version of SNMP enabled on the device. For example: If only SNMPv2 is enabled in the device configuration, don't include SNMPv3 credentials in the profile.

Step 1 From the main menu, choose **Device Management** > **Credential Profiles**.

Step 2 Click the ⎘.

Step 3 Click the **Download sample 'Credential template (*.csv)' file** link and save the CSV file template locally.

Step 4 Open the CSV template using your preferred editor. Begin adding rows to the file, one row for each credential profile you want to create.

As you do, observe these guidelines:

- If the **Password** column for any credential profile is blank, you can't import the CSV file. If you wish, you can enter the actual passwords in these fields. Cisco Crosswork stores them in encrypted form. If you choose this method, be sure to destroy the CSV file immediately after upload. We recommend using asterisks to fill the **Password** column in the CSV file and then importing it. After successful import, you can use the Cisco Crosswork GUI to edit each profile and enter the actual passwords, as explained in the following steps.
- Use a semicolon to separate multiple entries in the same field.
- When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. The first entry in one column will map to the first entry in the next column, and so on. For example: Suppose you enter in **Password Type** this list of password types: **`ROBOT_USERPASS_SSH;ROBOT_USERPASS_TELNET;ROBOT_USERPASS_NETCONF`**. You then enter in the **User Name** column **`Tom;Dick;Harry;`** and in the **Password** column **`root;MyPass;Turtledove;`**. The order of entry in these three columns determines the resulting mapping between the values you entered:
  - ROBOT_USERPASS_SSH: Tom : root
  - ROBOT_USERPASS_NETCONF: Dick : MyPass
  - ROBOT_USERPASS_TELNET: Harry : Turtledove
- Be sure to delete sample data rows before saving the file. You can ignore the column header row.

Step 5 When you're finished, save the CSV file to a new name.

Step 6 If necessary, choose **Device Management** > **Credential Profiles** again, then click the .

Step 7 Click **Browse** to navigate to the CSV file and select it.

Step 8 With the CSV file selected, click **Import**.

Step 9 When the import is complete:

a) From the left-hand side of the **Credential Profiles** window, select the profile you want to update, and click .
b) Enter the passwords and community strings for the credential profile and then click **Save**.
c) Repeat these steps as needed until you have entered all passwords and community strings.

Create ZTP Profiles

Cisco Crosswork uses ZTP profiles to automate imaging and configuration processes. While ZTP profiles are optional, we strongly recommend creating them, as they can help simplify the ZTP imaging and configuration process. Use ZTP profiles to help organize defined sets of image and configuration files you can apply to devices in a particular class or device family.

If you're implementing Classic ZTP, each ZTP profile can have only one image file and one configuration file associated with it. Secure ZTP allows you to specify pre-, post-, and main or day-zero configuration files.

ZTP profiles don't require that you specify an image file.

You can create as many ZTP profiles as you like. We recommend that you create only one ZTP profile for each device family, use case, or network role.

Step 1 From the main menu, choose **Device Management** > **Zero Touch Profiles**.

Step 2 Click **+ New Profile**.

Step 3 Enter the required values for the new ZTP profile. You don't need to specify a software image for the profile.

Step 4 If you're implementing Secure ZTP: Adjust the **Enable Secure ZTP** slider and enter the names of the pre- and post-configuration files.

Step 5 Click **Save** to create the new ZTP profile.

Prepare ZTP Device Entry Files

Cisco Crosswork uses ZTP device entries to let you specify in advance the IP addresses, protocols, and other information for the devices you want to provision. Cisco Crosswork populates these imported entries with more information once ZTP processing completes successfully.

You can create ZTP device entries in bulk by importing a device-entry CSV file.

The following topics explain how to download a template for a device entry CSV file. They also explain how to create properly formatted ZTP device entries.

We recommend that you experiment with the device entry CSV file format until you get used to it. Add only one or two device entries in a copy of the template, then import it. You can then see if you get the results you want.

You can also create ZTP device entries one by one, using the Cisco Crosswork UI, as explained in the next topic.

Download and Edit the ZTP Device Entry Template

1. From the main menu, choose **Device Management** > **Devices**.
2. Click the **Zero Touch Devices** tab.
3. Click the  .
4. Click the **Download 'devices import' template (.csv)** link and then **Save** it to a local storage resource. Click **Cancel** to clear the dialog box.
5. Open the CSV template with the application of your choice and save it to a new name. In each row, create an entry for each of the devices you plan to onboard using ZTP. Refer to the next topic section for help on the values to enter in each column.

ZTP Device Entry CSV Template Reference

The following table explains how to use the columns in the template. We mark columns that require entries with an asterisk (*) next to the column name.

The four "Connectivity" columns allow multiple entries, so you can specify multiple connectivity protocols for a single device. If you use this option, use semicolons between entries, and enter the values in the next three columns in the same order. For example: Suppose you enter `SSH;NETCONF;` in the **Connectivity Protocol** column. If you enter `23;830;` in the **Connectivity Port** column, the entries in the two columns map like this:

- SSH: 22
- NETCONF: 830

Table 10: ZTP Device Entry Template Column Reference

Column	Usage
UUID	Cisco Crosswork assigns a random UUID unless you elect to generate and enter it yourself. Enter the 128-bit universally unique identifier assigned to the device.
Host Name *	Enter the host name you want to assign to the device.
Serial Number *	Enter the device serial number. You can enter up to three serial numbers for the same device. These must be the same serial number for each device that you loaded into Cisco Crosswork previously. ZTP requires a serial number entry for all normal deployments. If you're using DHCP option 82 to implement a relay agent, you can leave this field blank, but you must specify a Remote Id and Circuit ID to identify the device.
MAC Address	Enter the device MAC address.
IP Address	Enter the device IP address (IPv4 or IPv6), along with its subnet mask in slash notation.
Credential Profile *	Enter the name of the credential profile you want Cisco Crosswork to use to access and configure the device. Required only if you want to use a credential profile.
OS Platform *	Enter the OS platform for the device. For example: IOS-XR.
Version *	Enter the OS platform version for the device software image. The platform version should be the same version as the ones specified for the image and configuration files you use to provision it. Currently, ZTP supports IOS-XR versions 6.6.3, 7.0.1, 7.0.2 and 7.0.12. Required only if you don't specify a ZTP profile in the Profile Name column.
Device Family *	Enter the device family for the device. The device family must match the device family in the image and configuration files ZTP uses to provision it. Required only if you don't specify a ZTP profile in the Profile Name column.
Image ID	Enter the Cisco Crosswork-assigned ID for the software image file you want to install on the device.
Config ID *	Enter the Cisco Crosswork-assigned ID for the configuration file you want to use when configuring the device.

Column	Usage
Profile Name	Enter the name of the ZTP profile you want to use to provision this device.
Configuration Attributes	Enter the values you want Cisco Crosswork to use for the replaceable parameters in the configuration file for the device. If you're using Secure ZTP, you can include pre-, post-, and day-zero configuration file parameters.
Connectivity Protocol	The connectivity protocols needed to monitor the device or to support Cisco Crosswork applications and features. Choices are: **SSH**, **SNMPv2**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **GRPC**, and **SNMPv3**.
Connectivity IP Address *	Enter the IP address (IPv4 or IPv6) and subnet mask for the connectivity protocol. Required only if you chose to set up a connectivity protocol.
Connectivity Port *	Enter the port used for this connectivity protocol. Each protocol maps to a port. Be sure to enter the port number that maps to the protocol you chose. Specify at least one port and protocol for every device, except if you want to: • Set the status of the onboarded device set as unmanaged or down. • Disable Cisco Crosswork reachability checks for the onboarded device. You may need to specify more than one protocol and port per device. The number of protocols and ports you specify depends on how you have configured Cisco Crosswork and the Crosswork applications you're using. See the table in the following section, "Crosswork Connectivity Protocol Requirements".
Connectivity Timeout	Enter the elapsed time (in seconds) before an attempt to communicate using this protocol times out. The default value is 30 seconds; the recommended timeout value is 60 seconds.
Provider Name	Enter the name of the provider to which you want to onboard the new ZTP devices. The name you enter must match exactly the name of the provider managing the device.
Provider Type	The type of provider. For example: NSO.
Provider Node ID	The IP address or URL of the main node of the provider.
Inventory ID	Enter the inventory ID you want to assign to the device.
Secure ZTP Enabled	Enter TRUE if you want to provision the device using Secure ZTP, or FALSE if not.

Column	Usage
PreConfig ID	Enter the Cisco Crosswork ID of the configuration script you want to run before running the associated configuration file.
PostConfig ID	Enter the Cisco Crosswork ID of the configuration script you want to run immediately after running the associated configuration file.
Location Enabled	Enter TRUE if you plan to identify the device using a location ID. Enter FALSE if you plan to identify it by serial number. If you enter TRUE, enter a Remote ID and a Circuit ID in the corresponding columns. If you enter FALSE, enter a Serial Number in the corresponding column.
Remote ID *	If implementing Secure ZTP and using option 82: Identify the name of the remote host acting as the bootstrap server. If you're using DHCP option 82 to implement a relay agent, this entry is required. You must enter a combination of the device RemoteID and CircuitID. If you're not using option 82, you can leave this field blank but you must specify the device serial number.
Circuit ID *	If implementing Secure ZTP and using option 82: Identify the interface or VLAN on which the bootstrap server receives requests. If you're using DHCP option 82 to implement a relay agent, this entry is required. You must enter a combination of the device RemoteID and CircuitID. If you're not using option 82, you can leave this field blank but you must specify the device serial number.
routingInfo.globalospfrouterid	If implementing OSPF on the device: Enter the OSPF Router ID for the device.
routingInfo.globalisissystemid	If implementing IS-IS on the device: Enter the IS-IS System ID for the device.
routingInfo.teRouterid	If implementing Traffic Engineering on the device: Enter the TE router ID for the device.

Crosswork Connectivity Protocol Requirements

Cisco Crosswork features and applications require you to enable a range of connectivity protocols for each device. The following table identifies these requirements for each supported connectivity protocol.

Table 11: Connectivity Protocol Requirements for Applications and Features

Protocol	Port	Application	Feature
GRPC	9090	• Cisco Crosswork Network Controller (CNC) • Cisco Crosswork Change Automation and Health Insights (CAHI) • Cisco Crosswork Optimization Engine (COE)	• Cisco Crosswork API communication
HTTP	80	• Cisco Crosswork Network Controller (CNC) • Cisco Crosswork Change Automation and Health Insights (CAHI) • Cisco Crosswork Optimization Engine (COE)	• Onboarding of NSO provider with all three applications
HTTPS	443	• Cisco Crosswork Network Controller (CNC)	• Onboarding of NSO provider
NETCONF	830	• Cisco Crosswork Network Controller (CNC) • Cisco Crosswork Change Automation and Health Insights (CAHI) • Cisco Crosswork Optimization Engine	• Onboarding of NSO provider with all 3 applications
SNMPv2	161	• Cisco Crosswork Network Controller (CNC) • Cisco Crosswork Change Automation and Health Insights (CAHI) • Cisco Crosswork Optimization Engine	• SNMPv2 data collection

Protocol	Port	Application	Feature
SNMPv3	161	• Cisco Crosswork Network Controller (CNC) • Cisco Crosswork Change Automation and Health Insights (CAHI) • Cisco Crosswork Optimization Engine	• SNMPv3 data collection
SSH	22	• Cisco Crosswork Network Controller (CNC) • Cisco Crosswork Change Automation and Health Insights (CAHI) • Cisco Crosswork Optimization Engine	• CLI data collection, SSH access to devices

Prepare Single ZTP Device Entries

If you have only a few devices to onboard using ZTP, you may find it easier to create the device entries one by one. Use the ZTP user interface and the following instructions to create single ZTP device entries.

Step 1 From the main menu, choose **Device Management** > **Devices**.

Step 2 Click the **Zero Touch Devices** tab.

Step 3 Click  .

Step 4 Enter values for the new ZTP device entry.

After ZTP onboards your devices, Cisco Crosswork may display more attributes.

Step 5 Click **Save**.

ZTP Provisioning Workflow

Once you complete ZTP setup, you can provision your devices and maintain them, as follows:

1. Set up DHCP so that Cisco Crosswork can download image and configuration software securely after you trigger ZTP processing.
2. Upload to Cisco Crosswork the ZTP device entry CSV file you created. Importing the file creates the device entries that ZTP populates during onboarding. If you're onboarding only a few ZTP devices, create device entries using the ZTP user interface instead.
3. Trigger ZTP processing by power-cycling or performing a CLI reboot for each device.

4. Complete the information for the onboarded devices. Edit them and supply (for example) geographical location information that ZTP couldn't discover during provisioning.

After completing this core workflow, you can perform ongoing maintenance of your ZTP devices using the advice and methods in the following topics:

- Update ZTP devices with additional information.
- Reconfigure your ZTP devices after onboarding, using other applications or by deleting and reonboarding the devices.
- Retire or replace ZTP devices without consuming more device licenses.
- Perform housekeeping on the ZTP assets you used to onboard your devices.
- Troubleshoot issues with ZTP processing and devices.

The remaining topics in this section discuss how to perform each of these tasks.

Upload ZTP Device Entries

The following steps explain how to create multiple ZTP device entries by importing your previously prepared ZTP device entry CSV file.

Imported ZTP device entries always appear in the **Zero Touch Devices** tab with their **Status** set to **`Unprovisioned`**. They remain **`Unprovisioned`** until you trigger ZTP processing.

Step 1 From the main menu, choose **Device Management** > **Devices**.

Step 2 Click the **Zero Touch Devices** tab.

Step 3 Click **Import Devices**.

Step 4 Click **Browse** to navigate to the ZTP device entry CSV file you created and then select it.

Step 5 With the CSV file selected, click **Import**.

Set Up DHCP for Crosswork ZTP

Before triggering ZTP processing, update your DHCP configuration file with information that identifies your ZTP devices and the software applied to them. This information permits Cisco Crosswork and DHCP to identify the ZTP devices and respond to requests for network connection and file downloads.

The following topics provide examples showing how to update DHCP server configurations to meet this requirement. The examples in these topics assume the DHCP context settings shown in the following figure. The figure shows example settings for the Internet Systems Consortium DHCP server. The line enabling the `sztp-redirect` option is required for Secure ZTP only. Leave it out if you're using Classic ZTP.

Figure 21: Secure ZTP DHCP Context

```
#
authoritative;

default-lease-time 7200;
max-lease-time 7200;
# Next line is needed for Secure ZTP only;
```

```
option sztp-redirect code 143 = text;

subnet 192.168.100.0 netmask 255.255.255.0 {
  option routers 192.168.100.1;
  option domain-name "cisco.com";
  option domain-name-servers 171.70.168.183;
  option subnet-mask 255.255.255.0;
  range 192.168.100.105 192.168.100.195;
}
```

DHCP Setup for Classic ZTP

We strongly recommend that you use Classic ZTP to provision devices over secure network domains only.

Cisco devices supported by Classic ZTP allow iPXE software image downloads via HTTP only. These same devices support download of configuration files via either HTTP or HTTPS. These options require entry of DHCP bootfile URLs in the DHCP server configuration for your organization.

If you want to use HTTP for both image and configuration file downloads, these URLs must specify the HTTP protocol and port 30604. For help, see the examples in figures 1 and 2.

If you want to use HTTPS for configuration file downloads only, the URL must specify the HTTPS protocol and port 30603. Specify the -k option before the HTTPS protocol in the URL. For help, see the examples in figures 3 and 4.

ZTP permits use of DHCP option 82 for configuration downloads. Option 82, also known as the DHCP Relay Agent Information Option, helps protect your devices from attacks using IP and MAC spoofing or DHCP address starvation. Option 82 allows you to specify an intermediary, or relay, router located between the device you're onboarding and the DHCP server resolving device requests. To use this option, specify a location ID. The location ID consists of a circuit ID (interface or VLAN ID) and remote ID (host name). Specify these values as parameters of the configuration download URL, as shown in the examples in figures 2 and 4. For more information about option 82, see RFC 3046 (http://tools.ietf.org/html/rfc3046).

When following these examples:

- Be sure to replace <*CW_HOST_IP*> with the IP address of your Cisco Crosswork server.
- Replace <*IMAGE_UUID*> with the UUID of the software image file in the ZTP repository. For help with using bootfile names and UUIDs, see the later section of this topic, "Copy Bootfile Names and UUIDs for DHCP Setup".
- Configuration files do not require UUIDs.

Figure 22: Classic ZTP DHCP Setup, Using HTTP

```
host cztp1 {
 hardware ethernet 00:a7:42:86:54:f1;
  if exists user-class and option user-class = "iPXE" {
    filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";

  } else if exists user-class and option user-class ="exr-config" {
     filename = "http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file";
  }
}
```

Figure 23: Classic ZTP DHCP Setup, Using HTTP and Option 82

```
host cztp2 {
 hardware ethernet 00:a7:42:86:54:f2;
  if exists user-class and option user-class = "iPXE" {
    filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";
```

```
  } else if exists user-class and option user-class ="exr-config" {
     filename =
"http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file?circuitid=Gig001&remoteid=MAR1";
  }
}
```

Figure 24: Classic ZTP DHCP Setup, Using HTTPS

```
host cztp3 {
 hardware ethernet 00:a7:42:86:54:f3;
  if exists user-class and option user-class = "iPXE" {
    filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";

  } else if exists user-class and option user-class ="exr-config" {
     filename = "-k https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/file";
  }
}
```

Figure 25: Classic ZTP DHCP Setup, Using HTTPS and Option 82

```
host cztp4 {
 hardware ethernet 00:a7:42:86:54:f4;
  if exists user-class and option user-class = "iPXE" {
    filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";

  } else if exists user-class and option user-class ="exr-config" {
     filename = "-k
https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/file?circuitid=Gig001&remoteid=MAR1";
  }
}
```

DHCP Setup for Secure ZTP

Secure ZTP allows you to provision devices over both secure and insecure network domains. Use HTTPS for the configuration file download, and specify `option sztp-redirect` for configuration artifacts. Add a remote ID and circuit ID if you want to use option 82. The remote ID identifies the remote host acting as the bootstrap server, and the circuit ID identifies the interface or VLAN on the remote host. See the examples in figures 5 and 6. For help with using bootfile names and UUIDs, see the following section, "Copy Bootfile Names and UUIDs for DHCP Setup".

Figure 26: Secure ZTP DHCP Setup, Using HTTPS

```
host sztp1 {
 hardware ethernet 00:a7:42:86:54:f4;
  if exists user-class and option user-class = "iPXE" {
    filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";

  } else {
     option sztp-redirect
"https://<CW_HOST_IP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";

  }
}
```

Figure 27: Secure ZTP DHCP Setup, Using HTTPS and Option 82

```
host sztp2 {
 hardware ethernet 00:a7:42:86:54:f5;
  if exists user-class and option user-class = "iPXE" {
    filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";

  } else if exists user-class and option user-class ="exr-config" {
```

```
    option sztp-redirect
"https://<CW_HOST_IP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data?circuitid=Gig001&remoteid=MAR1";

  }
}
```

Copy Bootfile Names and UUIDs for DHCP Setup

When modifying your DHCP server configuration file, specify the bootfile name and UUID for each software image. You can quickly copy both to your clipboard directly from the list of software images that you have already uploaded to Cisco Crosswork. No UUID is required for configuration files.

To copy software image bootfile names and UUIDs:

1. From the main menu, choose **Device Management** > **Software Images**.
2. If you want to copy:
   - The bootfile name and UUID of the software image: Click the ⧉ in the **Image/SMU Name** column.
   - Only the UUID of the software image: Click the ⧉ in the **Image UUID** column.

   Cisco Crosswork copies the bootfile name and/or UUID to your clipboard. You can now paste it into your DHCP host entry.

   When using the copied file path to create DHCP host entries, replace the *IP* variable with the IP address and port of your Cisco Crosswork server.

Generic Internet Systems Consortium (ISC) DHCP Setup Examples

The following figures show examples of the type of host entries you would make for a Classic ZTP and for a Secure ZTP device in the `/etc/dhcp/dhcp.conf` configuration file of an Internet Systems Consortium (ISC) DHCP server.

Other third-party DHCP servers differ in overall implementation, but many use options and formats similar to these ISC examples.

Be sure to reload or restart the ISC DHCP server once you have finished creating these new entries.

Figure 28: Classic ZTP ISC IPv4 DHCP Configuration Example

```
host NCS5k-1
{
    option dhcp-client-identifier "FOC2302R09H";
    hardware ethernet 00:cc:fc:bb:be:6a;
    fixed-address 105.1.1.16;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/
           <IMAGE_UUID>
    } else if exists user-class and option user-class = "exr-config" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file";
    }
}
```

Figure 29: Classic ZTP ISC IPv6 DHCP Configuration Example

```
host 5501
{
    host-identifier option dhcp6.client-id
```

```
00:02:00:00:00:09:46:4f:43:32:33:30:38:52:30:53:33:00;
    fixed-address6 fc00:15:2::36;
    if exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) = "iPXE" {
     option dhcp6.bootfile-url "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/

        <IMAGE_UUID>";
    } else {if exists dhcp6.user-class and substring(option dhcp6.user-class, 0, 10) =
"exr-config" {
      option dhcp6.bootfile-url
"http://<CW_HOST_IP>:30604/crosswork/crosswork/configsvc/v1/file";
    }
}
```

Figure 30: Secure ZTP ISC IPv4 DHCP Configuration Example

```
authoritative;
option sztp-redirect code 143 = text;

default-lease-time 7200;
max-lease-time 7200;

subnet 105.1.1.0 netmask 255.255.255.0 {
  option routers 105.1.1.254;
  option domain-name "cisco.com";
  option domain-name-servers 171.70.168.183;
  option subnet-mask 255.255.255.0;
  range 105.1.1.40 105.1.1.140;
  if exists user-class and option user-class = "iPXE" {
         filename =
"http://105.1.2.100:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-db2fb355-de5b-4c13-8290-346c4daaa577";

      } else {
option sztp-redirect
"https://105.1.2.100:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";

  }

}
```

Figure 31: Secure ZTP ISC IPv6 DHCP Configuration Example

```
default-lease-time 2592000;
preferred-lifetime 604800;
option dhcp-renewal-time 3600;
option dhcp6.user-class code 15 = string;
option dhcp6.bootfile-url code 59 = string;
option dhcp-rebinding-time 7200;
allow leasequery;
option dhcp6.name-servers 3ffe:501:ffff:100:200:ff:fe00:3f3e;
option dhcp6.domain-search "cisco.com";
option sztp-redirect code 136 = text;

option dhcp6.info-refresh-time 21600;
subnet6 fc00::/64 {
 range6 fc00::10:10:101 fc00::10:10:105;
}
 host CW14-NCS {

      host-identifier option dhcp6.client-id
00:02:00:00:00:09:46:4f:43:32:32:32:31:52:31:39:4e:00;
      fixed-address6 fc00::10:10:100;
      if exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) = "iPXE" {
  option dhcp6.bootfile-url
"http://[fc00::10:11:97]:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-db2fb355-de5b-4c13-8290-346c4daaa577";
```

```
      } else {
option sztp-redirect
"https://[fc00::10:11:20]:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";

 }

 }
```

The following table describes each line in the IPv4 ISC DHCP device entry examples given, and the source of the values used. The descriptions apply to both Classic ZTP and Secure ZTP for IPv4. Descriptions for the entries in the IPv6 example are identical, but adapted for the IPv6 addressing scheme.

Table 12: ISC IPv4 DHCP Configuration Host Entries and Values

IPv4 Entry	Description
`host NCS5k-1`	The device entry host name. The host name can be the same as the actual assigned host name, but need not be.
`option dhcp-client-identifier`	The unique ID of the device entry. The value `"FOC2302R09H"` shown in the Classic ZTP and IPv4 example is the serial number of the device. You can find the serial number on the device chassis. If you don't have physical access to the device, the IOS-XR `show inventory` command provides the serial number.
`hardware ethernet 00:cc:fc:bb:be:6a`	The MAC address of the Ethernet NIC port on the device. This address is the address on which you trigger the ZTP process. The address can be a management or data port, as long as it's reachable from Cisco Crosswork.
`fixed-address 105.1.1.16`	The IP address to be assigned to the device during configuration. The example is for a static IP, but you can also use standard DHCP IP pool assignment commands.
`option user-class = "iPXE"` and `filename =`	This line checks that the incoming ZTP request contains the `"iPXE"` option. Classic ZTP uses this option to image the device. If the request includes this option, then the device downloads the image file matching the UUID and path specified in the `filename =` parameter.
For Classic ZTP: `option user-class = "exr-config"` and `ffl filename =` For Secure ZTP: `option sztp-redirect code 143=text`	This line checks that the incoming ZTP request contains the `"exr-config"` option. ZTP uses this option to configure the device. If the request includes this option, then the device downloads the configuration file matching the path specified in the `filename =` parameter.

Classic ZTP DHCP Setup Scripts for Cisco Prime Network Registrar (CPNR)

Following are two sets of scripts that allow you to add ZTP device, image and configuration file entries to the CPNR DHCP server configuration file. There's one set of three scripts for IPv4, and a separate set of five scripts for IPv6. To use these scripts:

1. Copy and paste the contents of the scripts into local text files with the names given here.
2. Modify the device, image, and configuration entries in the `ztp-v4-setup-vi-nrcmd.txt` script, or the `ztp-v6-setup-vi-nrcmd.txt` script, to fit your needs, as explained in the script comments.

3. Copy the script files you want to use to the root folder of your local CPNR server.
4. Execute the scripts on the CPNR server using the following command:

   ```
   [root@cpnr-local ~]#/opt/nwreg2/local/usrbin/nrcmd -N username -P password
   <ztp-IPVersion-setup-via-nrcmd.txt
   ```

   Where:

   - *username* is the name of a user ID with administrator privileges on the CPNR server.
   - *password* is the password for the corresponding CPNR admin user ID.
   - *IPVersion* is either `v4` for the IPv4 version of the scripts, or `v6` for the IPv6 version of the scripts.

Note The following scripts are for use with Classic ZTP only. You can't use them with Secure ZTP.

Figure 32: IPv4 Script 1 of 3: ztp-v4-setup-vi-nrcmd.txt

```
#
# Create the scope
#
scope ztp-ncs-5501-mgmt create 192.0.20.0/24

# Add the dynamic range
scope ztp-ncs-5501-mgmt addrange 200 225

# Default the routers option. Note: No need to do subnet-mask. It is automatically provided.
scope-policy ztp-ncs-5501-mgmt setoption routers 10.10.10.1

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-script\")) (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
```

```
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ####
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0cb"


client <device-1-serial-num>-script create
client-policy <device-1-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"
client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
0)"

### Device-2 Settings ####
client <device-2-serial-num>--iso create
client-policy <device-2-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0cb"


client <device-2-serial-num>-script create
client-policy <device-2-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1640deb-8252-47b6-aab1-a843c0c7757b"
client-policy <device-2-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
0)"

#
# Create more as needed using the above as models.
# Note: For those that need option 67 (boot file), you can use:
#   client-policy <name> setoption boot-file "<file-url>"
#
# The next line is optional. Uncomment it if you want to log what the script is doing.
# dhcp set log-settings=+incoming-packet-detail,outgoing-packet-detail,client-detail

# Assure that the server is up-to-date with this configuration
dhcp reload
```

Figure 33: IPv4 Script 2 of 3: ztp-v4-setup-vi-nrcmd.txt

```
#
# Create the scope
#
scope ztp-ncs-5501-mgmt create 192.0.20.0/24

# Add the dynamic range
scope ztp-ncs-5501-mgmt addrange 200 225

# Default the routers option. Note: No need to do subnet-mask. It is automatically provided.
scope-policy ztp-ncs-5501-mgmt setoption routers 10.10.10.1

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
```

```
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-script\")) (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ####
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0cb"


client <device-1-serial-num>-script create
client-policy <device-1-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"
client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
0)"

### Device-2 Settings ####
client <device-2-serial-num>--iso create
client-policy <device-2-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0cb"


client <device-2-serial-num>-script create
client-policy <device-2-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1640deb-8252-47b6-aab1-a843c0c7757b"
client-policy <device-2-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
0)"
```

```
#
# Create more as needed using the above as models.
# Note: For those that need option 67 (boot file), you can use:
#   client-policy <name> setoption boot-file "<file-url>"
#
# The next line is optional. Uncomment it if you want to log what the script is doing.
# dhcp set log-settings=+incoming-packet-detail,outgoing-packet-detail,client-detail

# Assure that the server is up-to-date with this configuration
dhcp reload
```

Figure 34: IPv4 Script 3 of 3: ztp-v4-client-class-expr.txt

```
(or
   (if (equal (as-string (request get-blob option 77)) "iPXE") "ztp-iso")
   (if (equal (as-string (request get-blob option 77)) "exr-config") "ztp-script")
   "ztp-none"
)
```

Figure 35: IPv6 Script 1 of 5: ztp-v6-setup-vi-nrcmd.txt

```
#
# create prefix for mgmt
prefix prefix-for-mgmt create 2001:DB8:10e:201a::/64
#
# Set the client classing expression and enable use
# of client-class
#
dhcp set v6-client-class-lookup-id=@ztp-v6-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct
# client details depending on whether an iso or script is requested
# by the client.
#
client-class ztp-iso create
client-class ztp-iso set v6-client-lookup-id=@ztp-v6-iso-lookup-expr.txt
#
client-class ztp-script create
client-class ztp-script set v6-client-lookup-id=@ztp-v6-script-lookup-expr.txt
client-class-policy ztp-script set v6-reply-options=17
#
# Delete option set (may not exist and ok if fails)
#
option-set dhcp6-cisco-custom delete
#
import option-set ztp-v6-options.txt
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create action=exclude
#
# Create a default client that will prevent service to
# unknown clients.
#
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their mac-address.
```

```
# One has "-iso" added to the end that will be used when the client's
# request does not include the "exr-config" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request does include "exr-config" in option 77.
#
client <device-serial-no>-iso create
# Set the vendor options using blob format as option definitions are for different data
client-policy <device-serial-no>-iso setV6VendorOption 17 dhcp6-cisco-custom "(1 exr-config)(2
 0)"
# Escape the [ and ] as nrcmd (which uses tcl interpreter) will otherwise fail command
client-policy <device-serial-no>-iso setv6option bootfile-url
   "http://\[cw-ipv6-address\]:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-aec596

      a1-7847-4254-966a-2456aa5"
#
client <device-serial-no>-script create
# Set the vendor options using blob format as option definitions are for different data
client-policy <device-serial-no>-script setV6VendorOption 17 dhcp6-cisco-custom "(1
exr-config)(2 0)"
# Escape the [ and ] as nrcmd (which uses tcl interpreter) will otherwise fail command
client-policy <device-serial-no>-script setv6option bootfile-url
   "http://\[cw-ipv6-address\]:30604/crosswork/configsvc/v1/configs/device/files/8eb6b7e1
      -bd54-40bb-84e0-89f11a60128b"
#

# Assure the server is up-to-date with this configuration
dhcp reload
```

Figure 36: IPv6 Script 2 of 5: ztp-v6-client-class-expr.txt

```
(or (try (if (equal (as-string (request get option 15)) "exr-config") "ztp-script"))
    (try (if (equal (as-string (request get option 15)) "iPXE") "ztp-iso"))
   "ztp-none"
)
```

Figure 37: IPv6 Script 3 of 5: ztp-v6-iso-lookup-expr.txt

```
(let (id)
  (setq id (request get option 1))
  (or
# First try extracting the serial number from DUID
      (try (if (equali (substring id 0 6) 00:02:00:00:00:09)
                (concat (as-string (substring id 6 128)) "-script")
           )
      )
# If that fails, use normal client-id (DUID) lookup
     (concat (to-string id) "-iso")

  )
)
```

Figure 38: IPv6 Script 4 of 5: ztp-v6-script-lookup-expr.txt

```
(let (id)
  (setq id (request get option 1))
  (or
# First try extracting the serial number from DUID
      (try (if (equali (substring id 0 6) 00:02:00:00:00:09)
                (concat (as-string (substring id 6 128)) "-script")
           )
      )
```

```
# If that fails, use normal client-id (DUID) lookup
     (concat (to-string id) "-script")
  )
)
```

Figure 39: IPv6 Script 5 of 5: ztp-v6-options.txt

```
# Option Definition Set Export/Import Utility
# Version: 1
#
{
  ( name = dhcp6-cisco-custom )
  ( desc = Cisco Systems, Inc. )
  ( vendor-option-enterprise-id = 9 )
  ( id-range = 2 )
  ( option-list = [
    {
      ( name = cisco-17 )
      ( id = 17 )
      ( base-type = AT_VENDOR_OPTS )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
      ( option-list = [
        {
          ( name = clientID )
          ( id = 1 )
          ( base-type = AT_NSTRING )
          ( sepstr = , )
          ( desc = ZTP - clientID )
        }
        {
          ( name = authCode )
          ( id = 2 )
          ( base-type = AT_INT8 )
          ( sepstr = , )
          ( desc = ZTP - authCode )
        }
        {
          ( id = 3 )
          ( name = md5sum )
          ( base-type = AT_NSTRING )
          ( desc = ZTP - md5sum )
        }
        {
          ( name = cnr-leasequery )
          ( id = 13 )
          ( base-type = AT_BLOB )
          ( flags = AF_IMMUTABLE )
          ( sepstr = , )
          ( option-list = [
            {
              ( name = oro )
              ( id = 1 )
              ( base-type = AT_SHORT )
              ( flags = AF_IMMUTABLE )
              ( repeat = ZERO_OR_MORE )
              ( sepstr = , )
            }
            {
              ( name = dhcp-state )
              ( id = 2 )
              ( base-type = AT_INT8 )
              ( flags = AF_IMMUTABLE )
              ( sepstr = , )
```

```
}
{
  ( name = data-source )
  ( id = 3 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = start-time-of-state )
  ( id = 4 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = base-time )
  ( id = 5 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = query-start-time )
  ( id = 6 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = query-end-time )
  ( id = 7 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-class-name )
  ( id = 8 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = partner-last-transaction-time )
  ( id = 9 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-creation-time )
  ( id = 10 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = limitation-id )
  ( id = 11 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
```

```
{
  ( name = binding-start-time )
  ( id = 12 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-end-time )
  ( id = 13 )
  ( base-type = AT_STIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = fwd-dns-config-name )
  ( id = 14 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = rev-dns-config-name )
  ( id = 15 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = lookup-key )
  ( id = 16 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = user-defined-data )
  ( id = 17 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = prefix-name )
  ( id = 18 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = failover-state-serial-number )
  ( id = 19 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reservation-key )
  ( id = 20 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
```

```
      ( name = failover-partner-lifetime )
      ( id = 21 )
      ( base-type = AT_STIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = failover-next-partner-lifetime )
      ( id = 22 )
      ( base-type = AT_STIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = failover-expiration-time )
      ( id = 23 )
      ( base-type = AT_STIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = client-oro )
      ( id = 24 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( repeat = ZERO_OR_MORE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = failover )
  ( id = 21 )
  ( base-type = AT_BLOB )
  ( flags = AF_NO_CONFIG_OPTION,AF_SUPPORTS_ENCAP_OPTION,AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = server-state )
      ( id = 1 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = server-flags )
      ( id = 2 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = binding-status )
      ( id = 3 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = binding-flags )
      ( id = 4 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
```

```
}
{
  ( name = start-time-of-state )
  ( id = 5 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = state-expiration-time )
  ( id = 6 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = failover-expiration-time )
  ( id = 7 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = bndupd-serial )
  ( id = 8 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = bndack-serial )
  ( id = 9 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-flags )
  ( id = 10 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = vpn-id )
  ( id = 11 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = lookup-key )
  ( id = 12 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = type )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
```

```
    {
      ( name = data )
      ( id = 0 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = user-defined-data )
  ( id = 13 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reconfigure-data )
  ( id = 14 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = time )
      ( id = 0 )
      ( base-type = AT_DATE )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = key )
      ( id = 0 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = requested-fqdn )
  ( id = 15 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = flags )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = domain-name )
      ( id = 0 )
      ( base-type = AT_DNSNAME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = forward-dnsupdate )
```

```
  ( id = 16 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reverse-dnsupdate )
  ( id = 17 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = partner-raw-cltt )
  ( id = 18 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-class )
  ( id = 19 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = status-code )
  ( id = 20 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = status-code )
      ( id = 0 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = status-message )
      ( id = 0 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = dns-info )
  ( id = 21 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = flags )
      ( id = 0 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
```

```
      ( name = host-label-count )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = name-number )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = base-time )
  ( id = 22 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = relationship-name )
  ( id = 23 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = protocol-version )
  ( id = 24 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = mclt )
  ( id = 25 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = dns-removal-info )
  ( id = 26 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = host-name )
      ( id = 1 )
      ( base-type = AT_RDNSNAME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = zone-name )
      ( id = 2 )
      ( base-type = AT_DNSNAME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
```

```
    {
      ( name = flags )
      ( id = 3 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = forward-dnsupdate )
      ( id = 4 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = reverse-dnsupdate )
      ( id = 5 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = max-unacked-bndupd )
  ( id = 27 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = receive-timer )
  ( id = 28 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = hash-bucket-assignment )
  ( id = 29 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = partner-down-time )
  ( id = 30 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = next-partner-lifetime )
  ( id = 31 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = next-partner-lifetime-sent )
  ( id = 32 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
```

```
                }
                {
                  ( name = client-oro )
                  ( id = 33 )
                  ( base-type = AT_SHORT )
                  ( flags = AF_IMMUTABLE )
                  ( repeat = ZERO_OR_MORE )
                  ( sepstr = , )
                }
                {
                  ( name = requested-prefix-length )
                  ( id = 34 )
                  ( base-type = AT_INT8 )
                  ( flags = AF_IMMUTABLE )
                  ( sepstr = , )
                }
              ] )
            }
          ] )
        }
      ] )
    }
```

Trigger ZTP Device Bootstrap

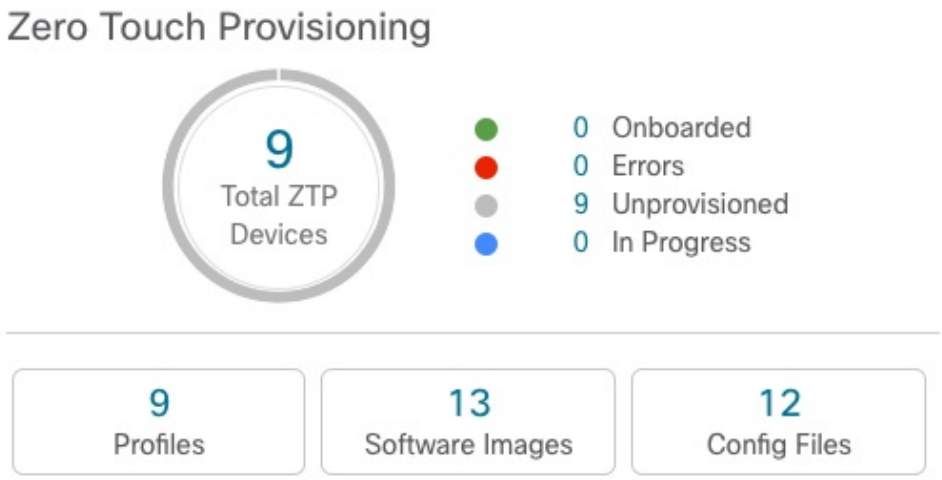
With device entries imported to Cisco Crosswork and DHCP configured, you can initiate ZTP processing by rebooting each of the devices.

Step 1 Initiate ZTP processing using one of the following options:

- Power-cycle the device to restart it.
- Using a pin, press the chassis reset button at the back of the device. Press for 15 seconds, or until the power light on the device starts flashing.
- For a previously imaged device: Connect to it via Telnet, then issue a **ztp initiate** command.

Repeat this step as needed for each of the devices you plan to provision during this session. You need not restart all the devices you have uploaded as device entries in a single session.

Step 2 Monitor ZTP progress using the Zero Touch Provisioning status tile shown in the following figure. To view the tile, click the **Home** icon on the main menu.



The tile provides a summary view of your current ZTP processing status. It gives a count of all the ZTP profiles, images, and configuration files currently in use. The tile also shows the number of devices in each of the possible ZTP processing states.

Complete Onboarded ZTP Device Information

ZTP devices, once onboarded, are automatically part of the shared Cisco Crosswork device inventory. You can edit them like any other device. The following steps explain two ways to add information to devices onboarded using ZTP.

Before editing any device, it's always good practice to export a CSV backup of the devices you want to change. You can do this using the export function described in Step 2.

Before you begin

Some information needed for a complete device inventory record is either not necessary or not available via automation. For example: Geographical data, indicating that a device is located in a building at a given address, or at a set of GPS coordinates. Location data like this is a requirement for most organizations with active networks, and can only be added by a human operator.

Still other kinds of inventory information are useful when you use other applications to manage your network. For example: Cisco Crosswork tags make it easier to apply Cisco Crosswork Health Insights KPIs to particular devices. Similarly, associating an SRE policy with devices makes it easier to use Cisco Crosswork Network Controller or Cisco Crosswork Optimization Engine. Some Cisco Crosswork providers, such as Cisco NSO, base convenient functions on this kind of extended device information. All of it needs update from humans.

You can add this kind of information using functions in the other Cisco Crosswork applications and providers. For more information on this topic, see the user documentation for the application. You can also add much of it using Cisco Crosswork ZTP.

Step 1 To update the inventory record for a ZTP device:

a) From the main menu, choose **Device Management** > **Network Devices**.

b) Click the **ZTP Devices** tab.
c) Select the device you want to change, then click the  .
d) Change the value of the **Status** field to **`Unprovisioned`**.
e) Edit the other values configured for the device, as needed.
f) Click **Save**.

Step 2 To update the inventory records for devices in bulk, including devices onboarded using ZTP:

a) From the main menu, choose **Device Management** > **Devices**.
b) Click  . Save the CSV file.
c) Open the CSV template with the application of your choice and edit the device information you want to add or update. It's a good idea to delete rows for devices you don't want to update.
d) When you're finished, save the edited CSV file.
e) If needed: Choose **Device Management** > **Devices**, then click the **Zero Touch Devices** tab.
f) Click  .
g) Click **Browse** to navigate to the CSV file you created and then select it.
h) With the CSV file selected, click **Import**.

Reconfigure Onboarded ZTP Devices

The purpose of Cisco Crosswork ZTP is to onboard new devices quickly and easily, without requiring you to locate experts on site with the new devices. ZTP performs imaging and configuration as part of that task, and can run scripts as part of device configuration. But it's not designed as an all-purpose device configuration utility, and shouldn't be used in that way.

If you need to reconfigure a device onboarded using ZTP, use:

- A Cisco Crosswork Change Automation Playbook, which allows you to roll out configuration changes to devices on demand.
- The configuration change functions of Cisco Network Services Orchestrator (Cisco NSO), or any of the other Cisco Crosswork providers you're using.
- A direct connection to the device and the device OS command line interface.

If you can't use any of these methods, the best approach is to delete the device. You can onboard the device again, this time with the correct configuration.

To delete a ZTP device, select **Device Management** > **Devices** > **Zero Touch Devices**, select the device in the table, then click  .

Retire or Replace Devices Onboarded With ZTP

Sometimes you must retire a Cisco device that was onboarded using ZTP. Device licenses are associated with the device serial number that you entered at the time of onboarding. ZTP permits association of a single device with up to three different serial numbers. You can use this fact to remove a failed or obsolete device from your network and from Cisco Crosswork inventory. You can replace it later without consuming an extra license.

This rule applies not only to devices with a chassis, but also to line cards and other pluggable device modules. Each of these modules has its own serial number. If you need to RMA a module, associate the old license with the serial number of the new module. But first remove the old line card and its serial number from inventory, as explained in the following steps.

1. Select **Device Management** > **Devices** > **Zero Touch Devices**.
2. Find the old device in the table and make a record of its serial number.
3. Select the device and then click the to delete it.

   After you delete the device, Cisco Crosswork will still count the license associated with this serial number as consumed. Track this license as part of any new or RMA replacement device purchase, so you can return the license for the old device to active use.

   Cisco Crosswork won't allow two active devices with the same license. You must delete the old device before you can onboard a new or replacement device.
4. When it's time to onboard the new device:
   a. When you create a ZTP device entry for the new device, enter both the new and old serial numbers.
   b. If you're using Secure ZTP: Submit both the old and new device serial numbers with the Ownership Voucher request for the new device. Cisco associates the old and new serial numbers with the in-use license in the regenerated Ownership Voucher.
   c. Onboard the new device as you would any other ZTP device. Only the old device license is consumed.

ZTP Asset Housekeeping

Once you have completed onboarding your devices with ZTP, you can delete offline copies of some of the ZTP assets you assembled. Retain others, depending on the policies and best practices of your organization. We recommend:

- **ZTP profiles**: Usually, it's safe to delete ZTP profiles after onboarding is complete. To delete a ZTP profile, select **Device Management** > **Zero Touch Profiles** . On the tile representing the ZTP profile you want to delete, click the ••• and then select **Delete** from the dropdown menu.
- **ZTP device entry CSV file**: You may want to retain an offline copy of this file for use as a template. This file can be handy if, say, you have many branch offices sharing the same network architecture and device types. Otherwise, you can simply delete it from the file system. You can download the CSV file template at any time. You may find it more useful to export a backup CSV file containing all the data for your ZTP devices, including data you entered after onboarding. To export a CSV device backup, select **Device Management** > **Devices** > **Zero Touch Devices** . Then click the and save the CSV file.
- **Software images and SMUs**: Save the production versions of these files offline, and delete older ones per the policies of your organization. Don't delete the uploaded image files from Cisco Crosswork if you plan to use them to image more devices of the same family. To delete obsolete images, select **Device Management** > **Software Images**, select the file in the table, then click the .
- **Configuration files**: You need not retain configurations you already uploaded to Cisco Crosswork, but the policy of your organization may differ. Don't delete uploaded configuration files if you plan to configure more devices of the same family using ZTP. When configurations change, you can easily

update the stored version. Prepare the new configuration file or script, select **Device Management** > **Configuration Files**, select the file in the table, and then click the . You can then browse to the new script file you created, and copy/paste the new configuration. If a configuration becomes obsolete, delete it: Select **Device Management** > **Configuration Files**, select the file in the table, then click the .

- **Credential profiles**: You can delete an imported credential profile CSV file immediately. Don't delete the uploaded credential profiles. When user names and passwords change, update the credential profiles: Select **Device Management** > **Credentials**, select the credential profile in the table, then click the .

Troubleshoot ZTP Issues

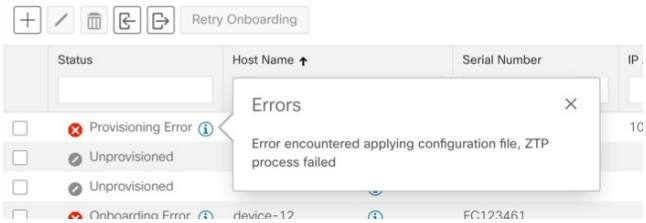
Cisco Crosswork ZTP provisioning and onboarding happen quickly and automatically, but errors and problems do occur. The following topics discuss how to remedy common problems.

Third-party devices that conform 100 percent to the Secure ZTP RFC are the only third-party devices you can onboard using Cisco Crosswork ZTP.

Inspect Status Errors

The **Status** column in the Zero Touch Devices window displays the next to every device entry whose ZTP processing finished with a **`Provisioning Error`**, **`Onboarding Error`** or (for Secure ZTP only) **`ZTP Error`**. Click on the icon to display a popup window with information about the error, as in the following example. When you're finished viewing the popup window, click to close it.

Figure 40: Provisioning Error Popup Window



Errors while uploading image files

Make sure that the MD5 checksum for the file is correct. If the file information is correct, image uploads can still fail due to slow network connections. If you're running into this problem, retry the upload.

Uploaded images and configuration files aren't in the drop-down menu when creating ZTP device entries or ZTP profiles

The drop-down menu selects images and configuration files based on the device family and release number you specify in your device entry or ZTP profile. Make sure that the file information matches the information for the device entry or profile you're using.

Errors during import of devices

If devices in inventory have the same serial numbers as the devices you're importing, check that the devices are in the **`Unprovisioned`** state before import. All the devices imported using CSV files have their status set to **`Unprovisioned`** on import. Before import, make sure the configurations, images, and ZTP profiles

mentioned in the CSV file exist. You can edit device image and configuration files by exporting a device CSV file and reimporting it with changes. If you use this edit method, make sure the CSV file has the correct UUIDs before import.

Image file download fails

Check that there's network connectivity between Cisco Crosswork and the device. Make sure that the device is getting its IP address from the DHCP server. Ensure that the UUID of the software image given in the configuration file of the DHCP server is correct. If you must correct the image UUID specified in the configuration file, make sure you restart the DHCP server before initiating ZTP processing again.

Configuration file download fails

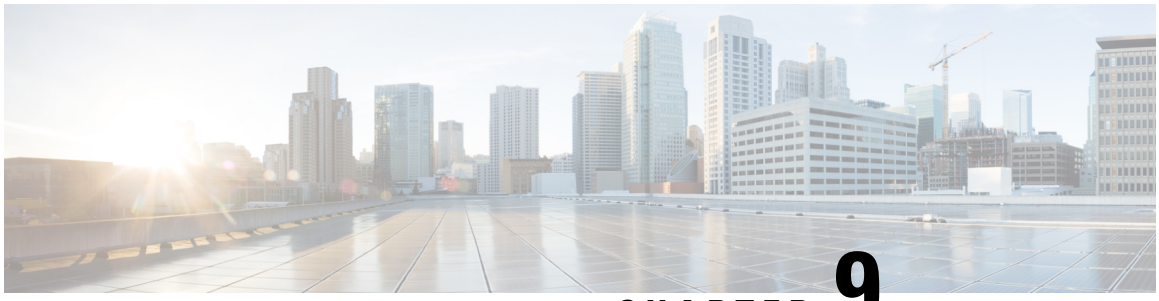
Check that there's network connectivity between Cisco Crosswork and the device. Make sure that the device is getting its IP address from the DHCP server. Ensure that the UUID of the software image given in the DHCP server configuration file is correct. If you must correct the image UUID specified in the DHCP configuration file, make sure you restart the DHCP server before reinitiating ZTP processing. Make sure that the device serial number matches the serial number on the chassis of the device. Ensure that the status of the device is either **`Unprovisioned`** or **`In Progress`** before initiating ZTP processing. Configuration downloads continue to fail as long as the device is in any other state.

Device state is showing Onboarded and not Provisioned

`Provisioned` is an intermediate state in ZTP processing. When the device state changes to **`Provisioned`**, Cisco Crosswork attempts to onboard the device immediately. The status changes to **`Onboarded`** or **`Onboarding Error`** after.

Onboarding Error

The default Cisco Crosswork device life-cycle management (DLM) policy for identifying devices uniquely is the IP address. If you import a new device with an IP address that matches an existing device, the device status changes to **`Provisioned`**, then to **`Onboarding Error`**. If the IP address of the new device is blank, you get the same result. These same issues apply if your installation uses an OSPF ID, ISIS ID, or other DLM policy for determining device IDs. Onboarding can only succeed when you fill all the DLM policy fields with unique, nonblank values. If onboarding fails, inspect the popup error message, update the corresponding fields and retry onboarding.



CHAPTER 9

Set Up Maps

This section contains the following topics:

Define Map Display Settings

The network topology can be displayed on a logical map or a geographical map (geo map), where the devices and links are shown in their geographic context. The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. The geo map shows single devices, device clusters, links, and tunnels, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude).

The logical map is automatically rendered with no intervention required. The geographical map is rendered by default using map tiles from an external map provider (Mapbox). Internet access is required when using an external map provider. If there is no Internet access, you can download map files from Cisco.com and upload them into the system. These map files will be accessed internally in order to render the geo map. See Use Internal Maps Offline for Geographical Map Display, on page 213.

When setting up maps, administrators can also define display settings, for example, colors representing changes in link bandwidth utilization.

To set up your maps and define display settings, see:

- Use Internal Maps Offline for Geographical Map Display, on page 213
- Define Color Thresholds for Link Bandwidth Utilization, on page 214

Use Internal Maps Offline for Geographical Map Display

Note The option to work offline using internal maps is not available for the Topology View in the Network Automation dashboard. The Network Automation menu is present if the Cisco Crosswork Change Automation application is installed.

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-4.0.0-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 Visualization Settings, 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.

Define Color Thresholds for Link Bandwidth Utilization

Link bandwidth utilization can be visualized and monitored in the logical and geographical maps. Links are colored based on the percentage of total bandwidth currently utilized on the link. Following is the default set of bandwidth utilization thresholds (percentage ranges) and corresponding color indicators. These color thresholds can be customized by administrators.

- Green—0–25% usage
- Yellow—25–50% usage
- Orange—50–75% usage
- Red—75–100% usage

To define color thresholds for link bandwidth utilization:

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

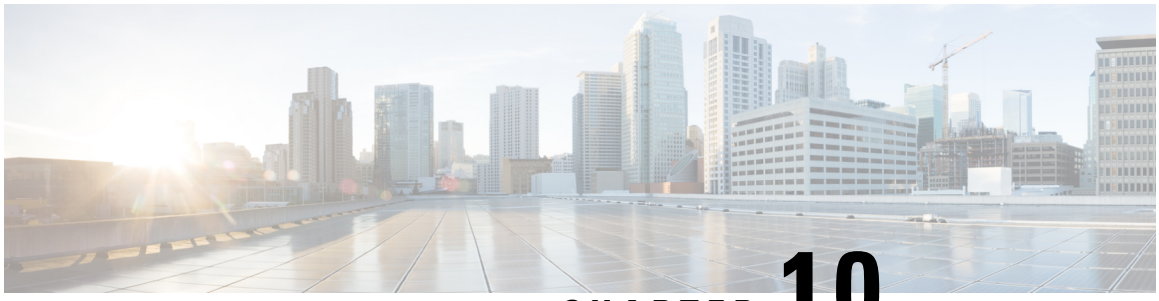
Step 2 Under Visualization Settings, click the **Bandwidth Utilization** option.

Step 3 In the **Polling Interval** field, enter a whole number from 5 to 60 (minutes) to specify how often links will be polled for bandwidth utilization. By default, link bandwidth is polled every 5 minutes.

Step 4 In the **Link Coloring Thresholds** area, define the criteria for coloring the links. Each row defines a color and the bandwidth percentage range that the color will represent. Note that:

- 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, 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.

Step 5 Click **Save**.



CHAPTER 10

Manage System Access and Security

This section contains the following topics:

Manage Certificates

What is a Certificate?

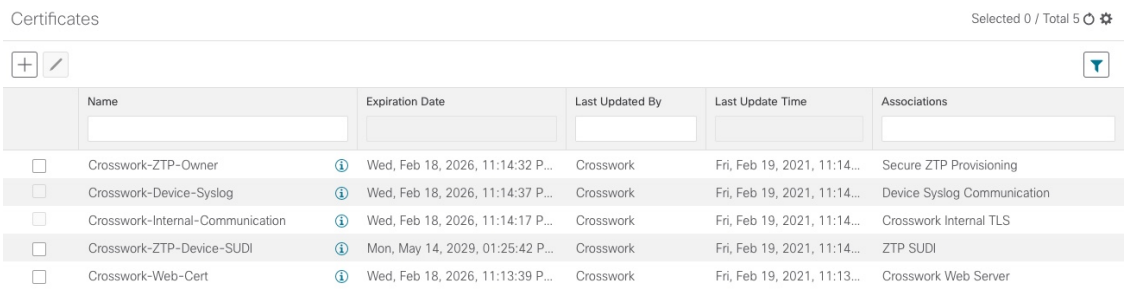
A certificate is an electronic document that identifies an individual, a server, a company, or another entity, and associates that entity with a public key. When a certificate is created with a public key, a matching private key is also generated. In TLS, the public key is used to encrypt data being 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 237 and HTTPS, on page 237.

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 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.

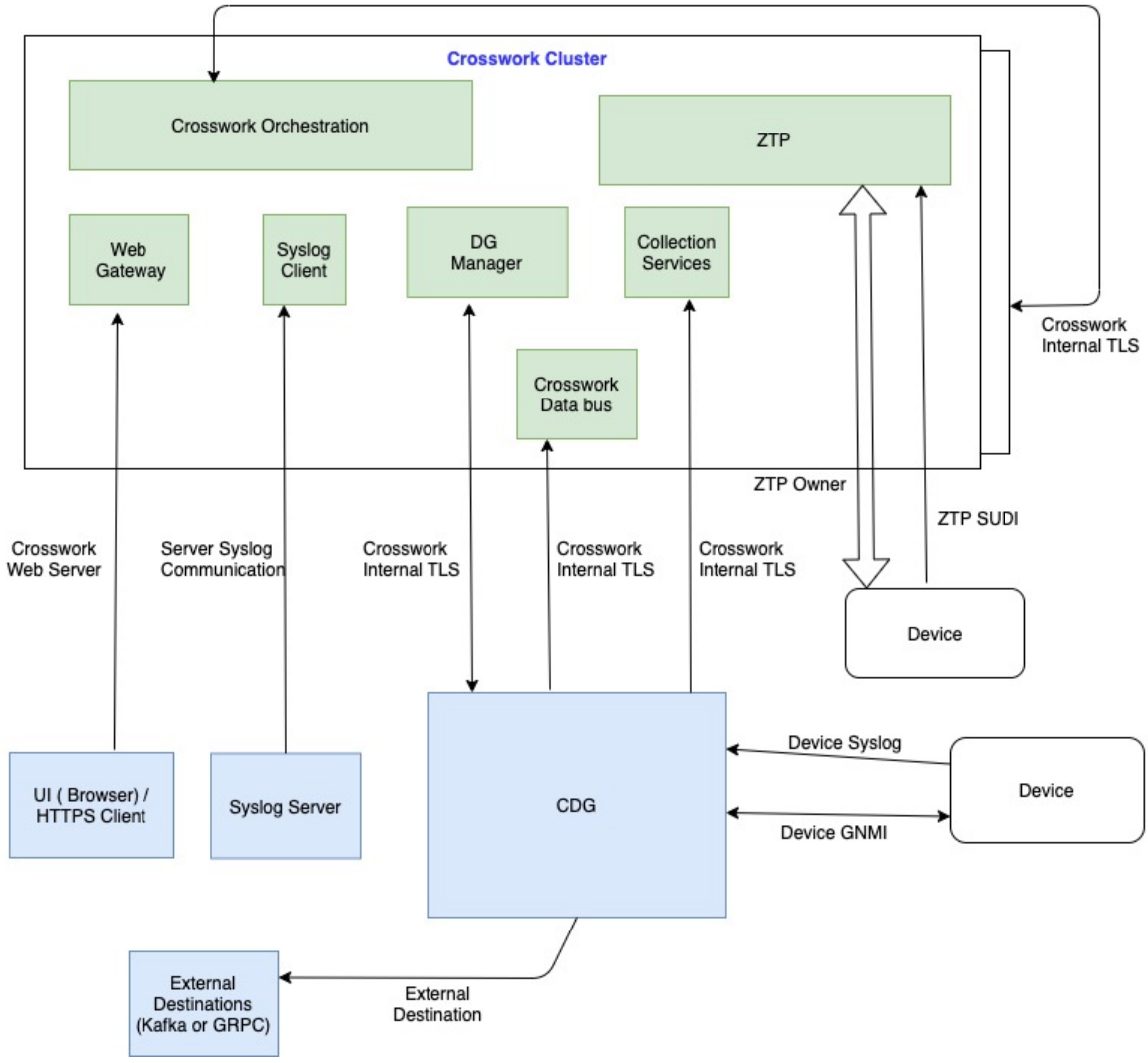
Figure 41: Certificate Management UI



Certificate Types and Usage

The following figure shows how Crosswork uses certificates for various communication channels.

Figure 42: 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 certificatess) and are created by Crosswork during initialization. They are used for interprocess communications between Crosswork and CDG as well as communication between internal Crosswork components. • Allows mutual and server authentication.	CW	• CDG • CW	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.	CW Web Server	User Browser or API Client	• Upload • Download	5 years	30 day - 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.	CW ZTP	Device	• Upload • Download	100 days	30 day - 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.	CW ZTP	Device	• Upload • Download	5	30 day - User defined
Device Syslog	CW-Device-Syslog	• Generated and provided by Crosswork. • Provides Syslog telemetry communications between devices and CDG. • Allows server authentication.	CDG	Device	Download	5 years	—
Device gNMI Communication	—	Provides GNMI telemetry communications between devices and CDG.	CDG	Device	• Upload • Download	Not Applicable	30 day - User defined

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Server Syslog	Not Applicable	• Allows syslog events and logs from Crosswork to an external Syslog server. • Allows server authentication.	External Syslog Server	Crosswork	• Upload **Note** You can upload multiple certificates associated with different servers. • Download	—	30 - User defined
External Destination	—	Exports telemetry data from CDG to external destinations (Kafka or GRPC).	External Destinations (Kafka or GRPC)	CDG	• Upload **Note** You can upload multiple certificates associated with different destinations. • Download	—	30 - User defined

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 the trust chain and an intermediate certificate and key

The intermediate certificate and key is used either by Crosswork or by the user to generate end-entity certificates for servers or devices. For example, the Crosswork Web Server Role allows a user to download the trust-chain, and an intermediate certificate and key. This intermediate certificate and key is used internally by Crosswork to generate the web server certificate.

Upload New Certificates

You can add certificates for the following roles:

- **External Destination**—Certificates uploaded for this role are used to secure communication between CDG and external destinations like Kafka servers. To enable mutual authentication, the user uploads a **CA Certificate Trustchain** that will be common to both CDG 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 server**, and optionally **Passphrase** (if one was used for generating the intermediate key). Crosswork will internally create a client certificate using this intermediate key for

the CDGs that will connect to the external destination. The destination (for example: Kafka) server certificate trust needs to be derived from the same root CA certificate.

- **Syslog Server 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.
- **Devices gNMI communication**—The user uploads a bundle of trust chains used by CDG 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 67.

If you prefer to upload your own ZTP (Zero Touch Provisioning Concepts, on page 165) and web certificates (instead of using the default certificates provided within Cisco Crosswork), use the Edit function (see Edit Certificates.

Before you begin

- For information on certificate types and usage, see Certificate Types and Usage, on page 218.
- 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/Edit a Data Destination, on page 40.

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 Manage Certificates, on page 217.

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 intermediate certificate and intermediate key. The Passphrase field is optional and is used to create the intermediate key (if applicable).

Step 6 Click **Save**.

Edit Certificates

You can edit a certificate to add or remove connection destinations, upload, and replace expired or misconfigured certificates. User provided certificates and ZTP 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/Edit a Data Destination, on page 40). 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  .

Step 3 Update the necessary options.

Note For information about ZTP certificates, see the following:

- Assemble ZTP Assets, on page 175
- Load ZTP Assets, on page 178

Note Update CW Web Server certificates with an intermediate CA certificate and intermediate key because the Certificate Management UI requires them to create a new web certificate. While editing 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.

Upon successful validation, the Certificate Management UI logs out automatically and applies the certificate to the Web Gateway.

Step 4 Click **Save**.

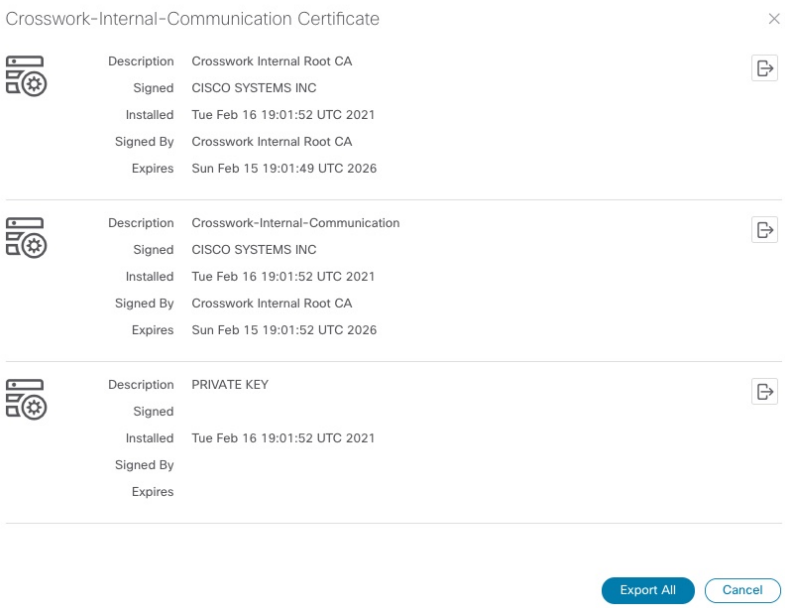
Download Certificates

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 43: 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**.

Manage Licenses

Smart Licensing is a software based end-to-end license platform that comprises several tools and processes that authorizes customers to use Cisco products. Smart Licensing provides a software inventory management system that provides Customers, Cisco, and selected Partners with information about Software Ownership and Software Utilization.

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 more information, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html

From the main menu, select **Administration** > **Smart Licensing Registration** to display the **Smart Software Licensing** window. Using this window, you can register your Cisco Crosswork application, edit the transport settings, renew the license, and de-register your application.

Prerequisites for Smart Licensing Registration

You should have:

- A Cisco Smart Account.
- Purchased licenses for the Cisco Crosswork application.

Configure Transport Settings

You can configure the transport settings to decide how Cisco Crosswork communicates with the Cisco servers.

- **Direct**: The application directly connects with Cisco Smart Software Manager (CSSM).
- **Transport Gateway**: The application communicates via a Transport Gateway or CSSM on-prem, which replicates the cloud-based user experience but keeps all communication on premises.

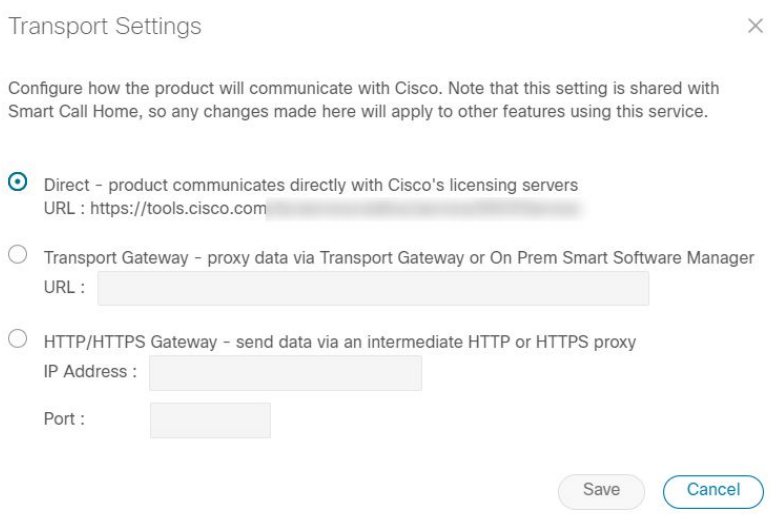
Note For more information on the CSSM on-prem option, see the Smart Software Manager guide.

- **HTTP/HTTPS Gateway**: The application connects via an intermediate proxy server. This is applicable only for Direct mode.

Note Transport Settings cannot be changed while the Cisco Crosswork is in Registered mode. You have to de-register to change them.

Step 1 In the **Smart Software Licensing** window, the Transport Settings display the current transport mode selected. To modify, click **View/Edit**.

The **Transport Settings** dialog box is displayed.



Step 2 Select the relevant transport mode and make relevant entries in the fields provided.

Step 3 Click **Save**.

Register Cisco Crosswork Application

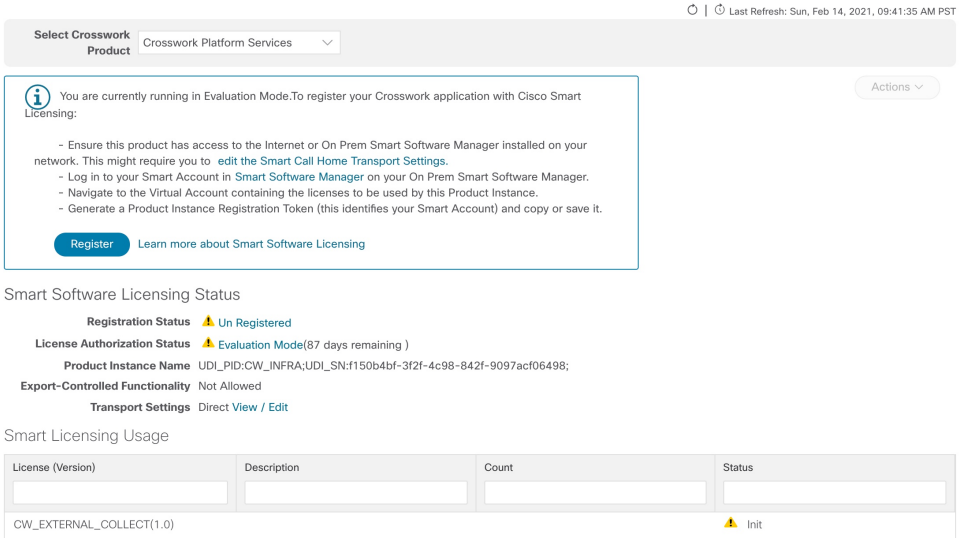
To enable licensed features, the Cisco Crosswork application must be registered to CSSM using a registration ID token. Once registered, an Identity Certificate is saved securely in the Smart Account and used for all ongoing communications. The certificate is valid for one year and will be renewed automatically 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.

Step 1 From the main menu, select **Administration** > **Smart Licensing Registration** to display the **Smart Software Licensing** window. The registration status

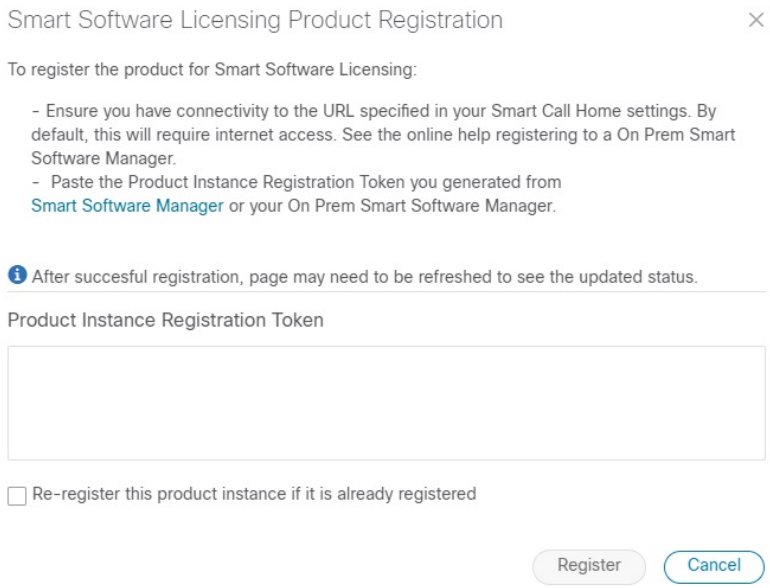
The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 44: Smart Software Licensing Unregistered Example



Step 2 In the **Smart Software Licensing** window, click **Register**.

The **Smart Software Licensing Product Registration** dialog box is displayed.



Step 3 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 4 (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** checkbox.

Note After a backup restore or disaster restore operation, you must manually re-register the Cisco Crosswork VM to CSSM. This is applicable in case of a Cisco Crosswork VM that has been already registered while taking the backup which is used in the restore operations.

Step 5 Click **Register**. It may take a few minutes to process the registration. If successful, the 'Product Registration completed successfully' message is displayed.

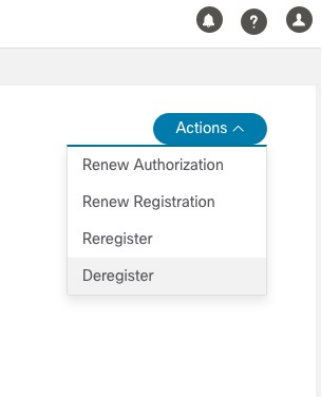
The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Note
- If you encounter a communication timeout error during registration, click **OK** in the error dialog box and the application will reattempt the registration.
- In some cases, after successful registration, the page may need to be refreshed manually to see the updated status.

Manually Perform Licensing Actions

The renewal of registration and authorization are automatically enabled for Cisco Crosswork, 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** window, click **Actions** drop-down button and select the relevant option for the following quick actions.



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 229.

Step 2 The selected action is executed successfully.

License Authorization Statuses

Based on the registration status of your Cisco Crosswork application, you can see the following License Authorization Statuses.

Table 13: 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.

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 233).

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.
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**.

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 Cisco Crosswork data to help their work as system architects or planners.

The following table describes some sample custom user roles you should consider creating:

Table 14: 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

Local users with administrator privileges can create new users as needed (see Manage Users, on page 230).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

The local **admin** role enables access to all functionality. It is created during installation and cannot be changed or deleted. However, its privileges can be assigned to new local users. Only local users can create or update user roles; TACACS users cannot.

Follow the steps below to create a new user role.

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 **admin** table 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 Define the user role's privilege settings:

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 234).

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 230). Later, you can edit the roles themselves to give users the privileges you want (see Edit User Roles, on page 234).

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 In the **Roles** table, click on an existing role to select it. The **Admin** table 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.

Set Up User Authentication (TACACS+ and LDAP)

In addition to supporting local users, Cisco Crosswork supports TACACS+ and LDAP users through integration with the TACACS+ and LDAP servers. The integration process has the following steps:

- Configure the TACACS+ and LDAP server.
- Create the roles that are referenced by the TACACS+ and LDAP users.

Note If you try to login to Cisco Crosswork as a TACACS+ or LDAP user before creating the required user roles, you will get an 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. After the roles are created, you can logout and login back as a TACACS+ or LDAP user.

Manage TACACS Servers

Step 1 From the main menu, select **Administration** > **AAA** > **TACACS+ Servers** tab. From this window, you can add, edit settings, and delete a new TACACS+ server.

Step 2 To add a new TACACS+ server:

a) Click + and enter the required TACACS+ server details.
b) Click **Add**.
c) Click **Save Server Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Note You cannot change the value for the **Shared Secret** parameter.

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.

Manage LDAP Servers

Crosswork supports the use of LDAP servers to authenticate users. Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

Like TACACS+ server, you can specify a unique priority value to assign precedence in the authentication request.

Note

- 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 TACACS+ changes and submit them in a single session.
- As 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. For more information, see Create User Roles, on page 233.

Step 1 From the main menu, select **Administration** > **AAA** > **LDAP Servers** tab. Using this window, you can add, edit settings, and delete a new LDAP server.

Step 2 To add a new LDAP server:

a) Click and enter the required LDAP server details.

b) Click **Add**.

c) Click **Save Server Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Note You cannot change the value for the **Shared Secret** parameter.

Step 3 To edit a LDAP server:

a) Click the checkbox next to the LDAP server and click .

b) After making changes, click **Update**.

Step 4 To delete a LDAP server:

a) Click the checkbox next to the LDAP server 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, youYou 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 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 your Cisco representative.

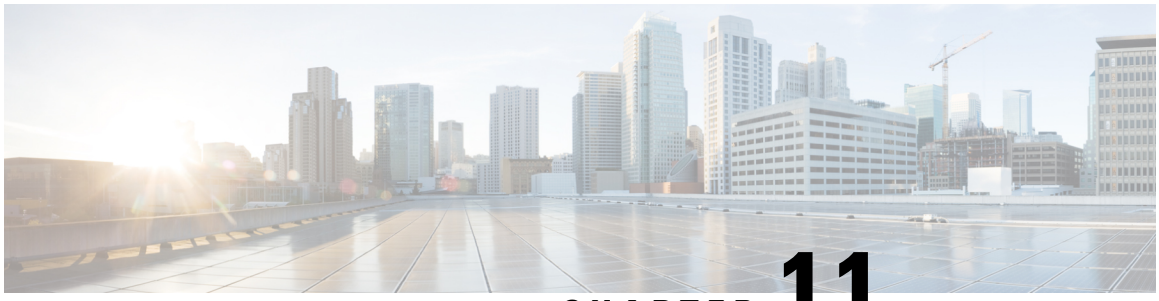
Step 3 If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork to operate.

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 your storage vendor and your Cisco representative.

- If you are using internal storage, contact your 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 your Cisco representative for more information.



CHAPTER 11

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.

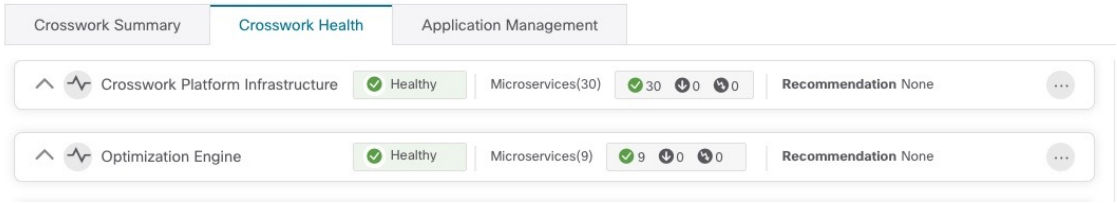
Monitor Cluster Health

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 **Crosswork Cluster** 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 Check Cluster Health, on page 5.

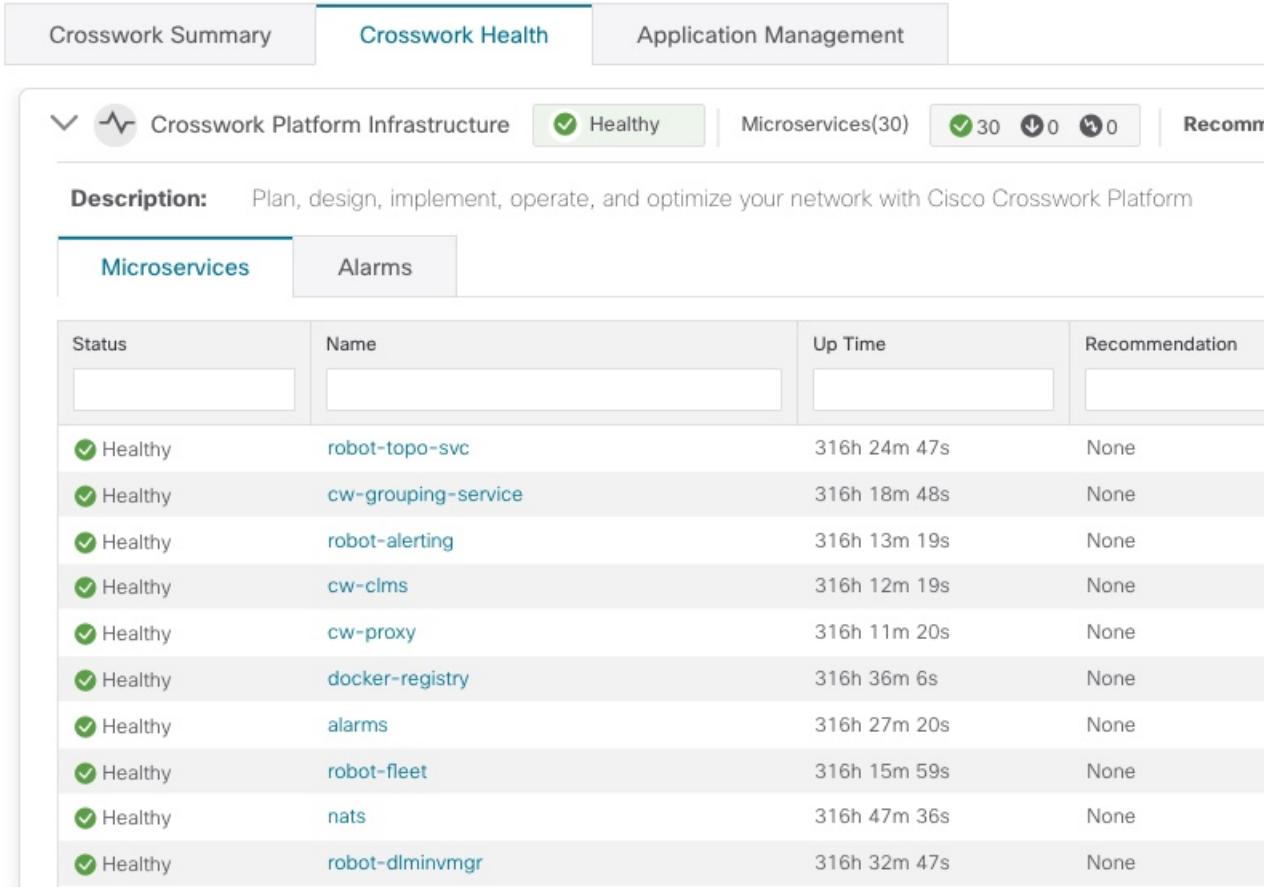
In addition to accessing Crosswork Cluster health, you can click on the **Cisco Crosswork Platform Infrastructure** and application tiles to view more details such as microservices and alarms.

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.



Within this window, expand an application row to view Microservice and Alarm information.



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.

From the **Alarms** tab:

- Click the alarm description to drill down on alarm details.
- Acknowledge, change status, and add notes to alarms.

You can also download *all* of a Cisco Crosswork application or Cisco Crosswork Platform Showtech service logs and perform installation-related operations from the **Application Details** window. Click ··· to open the **Application Details** window.

Visually Monitor System Functions in Real Time

You can monitor the health of Cisco Crosswork and any of its functions in real time, using a set of monitoring dashboards you can access from the **Crosswork Manager** window.

Cisco Crosswork 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 Cisco Crosswork 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 whichCisco Crosswork applications are installed.

Table 15: 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, Cisco Crosswork maintains a maximum of 24 hours of collected metric data.

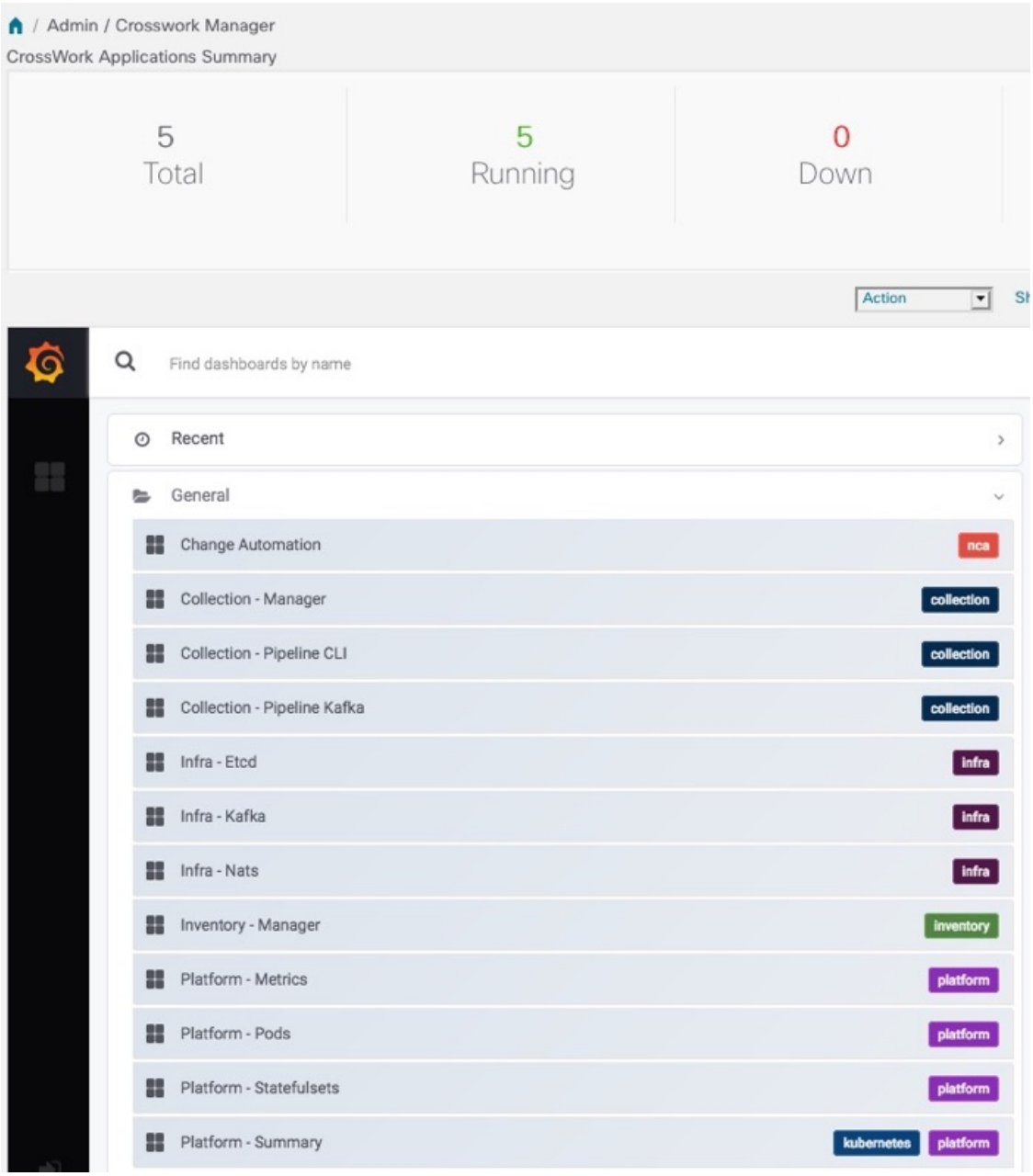
Grafana is an open-source visualization tool. The following provides general information about how to use the Cisco Crosswork implementation of Grafana. For more information about Grafana itself, see https://grafana.com and http://docs.grafana.org

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

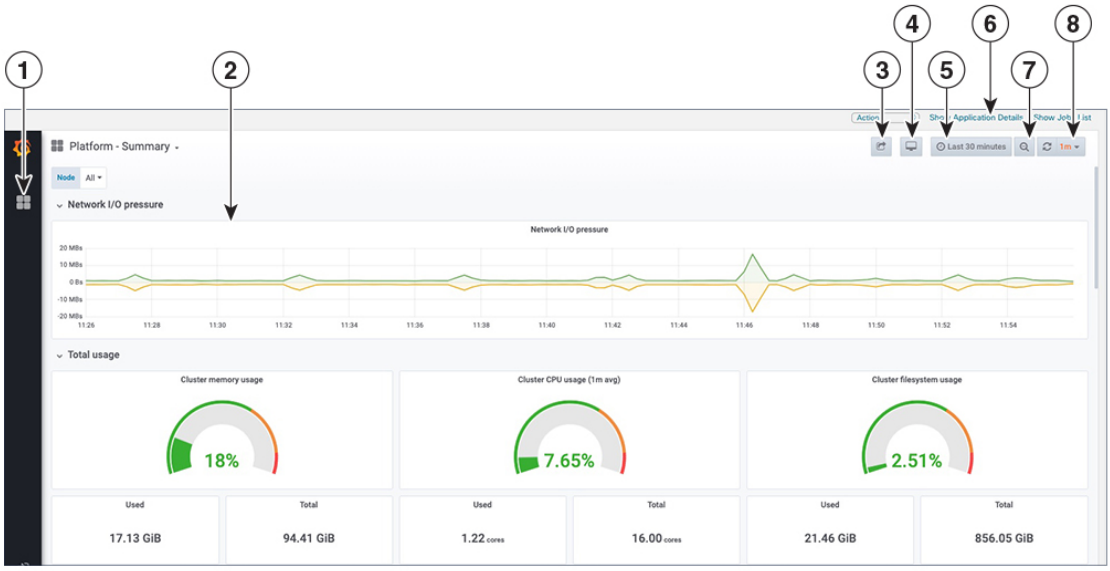
Step 2 At the top right, click **View more visualizations**.

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 **Today so far** or **Last three hours**. You can choose predefined refresh rates from **Off** to **2 Days**. When you have finished making changes, click **Apply**. When making selections, remember only 24 hours of data is stored. If you select time ranges or refresh rates beyond that limit, the dashboard may be blank.
6	**Zoom Out icon**: Click this icon to reset a zoomed time series graph back to the unzoomed state.
7	**Refresh icon**: Immediately or choose time interval to refresh the data shown.

View System and Network Alarms

You can view alarms by navigating to one of the following:

- From the main Crosswork window, click  .
- From the main menu, choose **Administration** > **Alarms**.
- For application specific alarms, choose **Administration** > **Crosswork Manager** > **Crosswork Health** tab. Expand one of the applications and select the **Alarms** tab.

From the **Alarms** window:

- Click the alarm description to drill down on alarm details.
- Acknowledge, change status, and add notes to alarms.

System Events

To help an operator troubleshoot issues, Crosswork Infrastructure has a Syslog feature which forwards system related events to an external server (see Configure a Syslog Server, on page 257). 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 and sample events or actions within that category.

Table 16: 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 17: 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 18: 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 19: 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 20: Adding an Application—Success

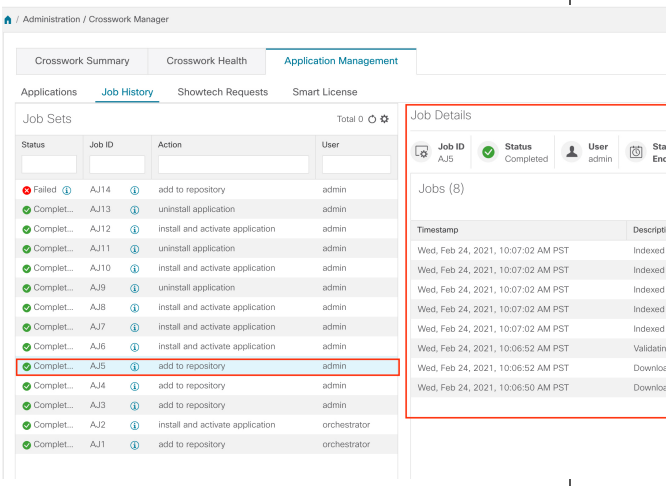
Severity	Information
Description	This event occurs when an application is added successfully.
Alarm	
Syslog Message	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* CLUSTER-CLUSTER - 627b2140-a906-4a96-b59b-1af22f2af9f6 CLUSTER-99 'job_type=INSTALL_AND_ACTIVATE_APPLICATION,manager=app_manager: ,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 21: Adding an Application—Failure

Severity	Information

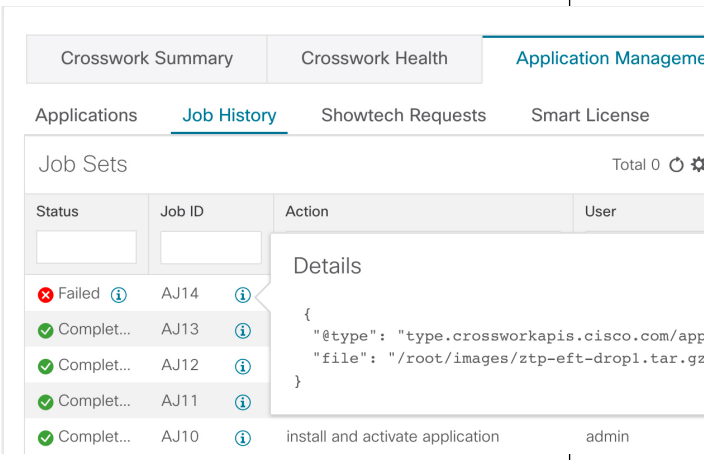
Description	This event occurs when an application cannot be added.
Sample Alarm	
Sample Syslog Message	None
Recommendation	After fixing the error, try adding the application again.

Table 22: 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 23: 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 24: 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 25: 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 26: 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 27: 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 28: 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 29: 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 30: 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 31: 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 32: 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.

Table 33: 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 34: 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 35: 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.

Check System Health Example

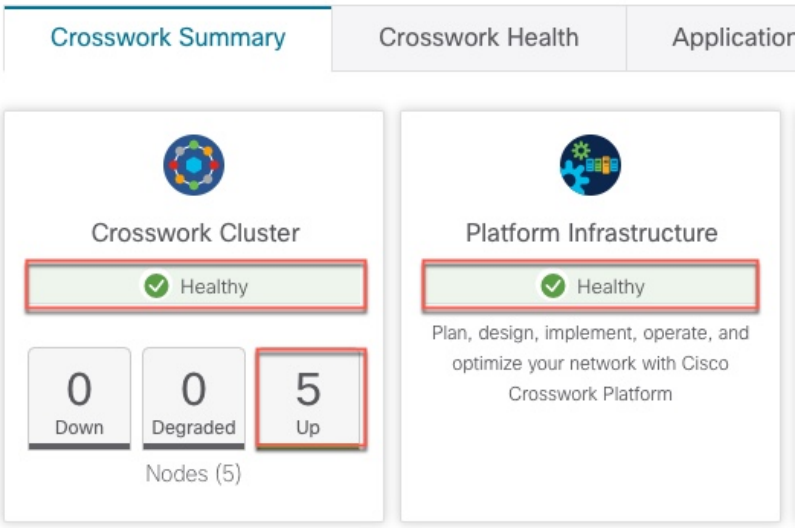
In this example, we navigate through the various windows and what areas should be checked for a healthy Crosswork system.

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 45: Crosswork Summary

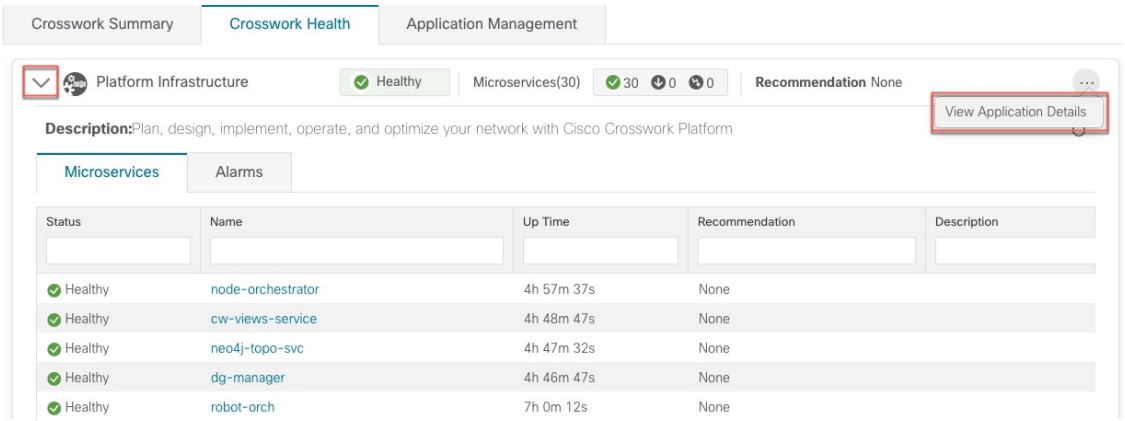


Step 2 Check and view detailed information about the microservices that are running as part of the Crosswork Platform Infrastructure.

a) Click the **Crosswork Health** tab.

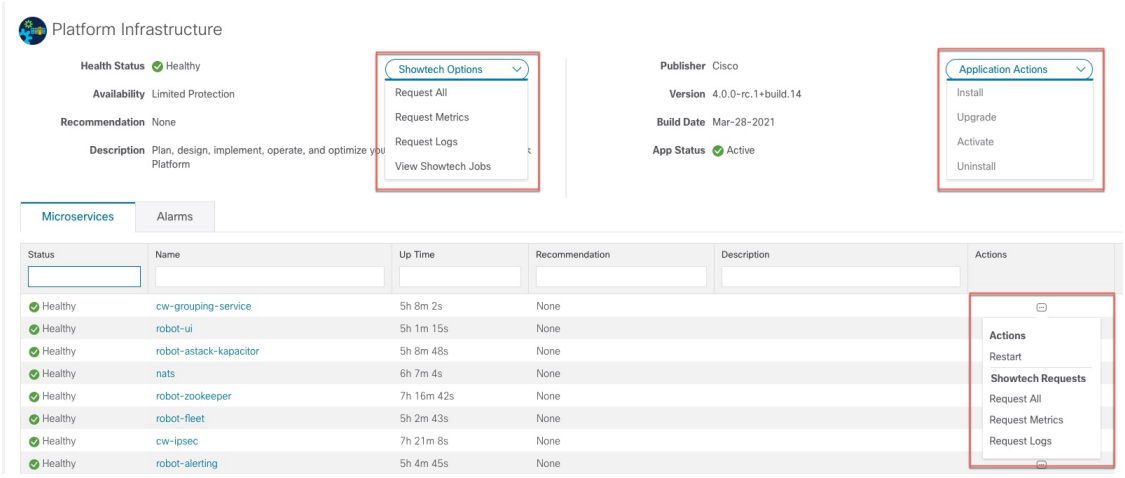
b) Expand the Crosswork Platform Infrastructure row, click ⋯, and select **Application Details**.

Figure 46: 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.

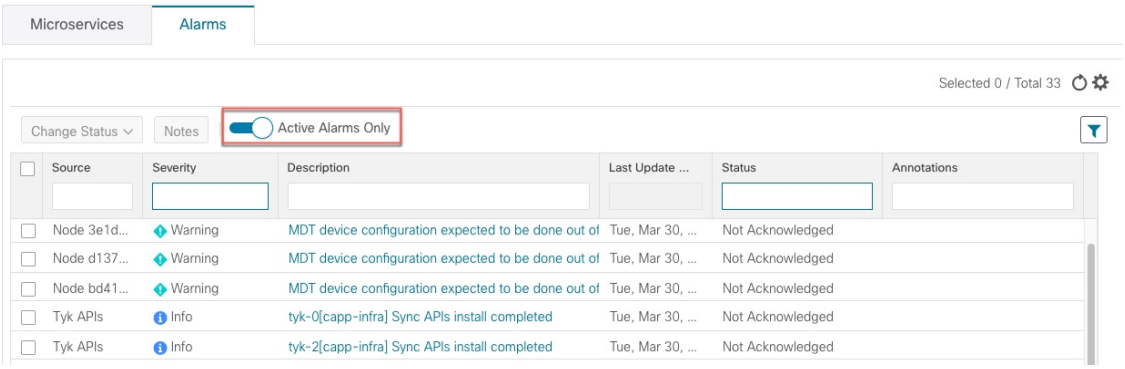
Figure 47: Application Details



Step 3 Check and view alarms 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 48: 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.

Configure a Syslog Server

Crosswork allows external syslog consumers to:

- Register on Crosswork and receive system events as syslogs.
- Define and filter which kind of events should be forwarded as a syslog, per consumer.
- Define the rate of which syslogs are forwarded to the consumer.

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** tab.

Step 2 Click +.

Step 3 Enter Syslog configuration 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 syslog. For example: **(EventSeverity<2 or EventSeverity>=5) and OriginAppId=capp-infra and EventCategory=1**

The expression will send 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.

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 242.

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 36: 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.
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.

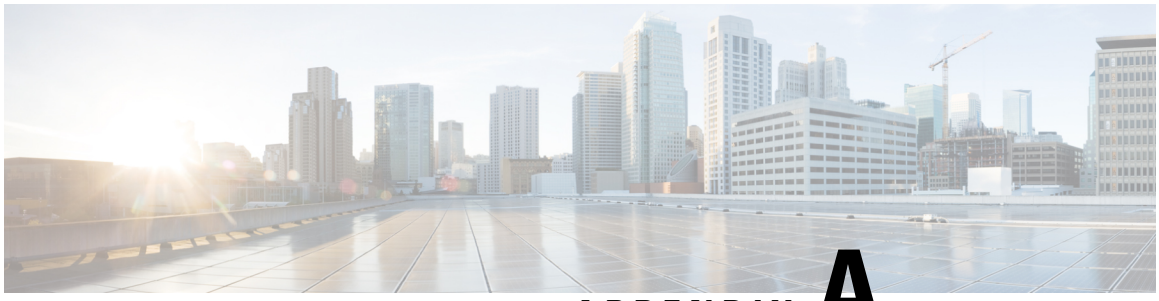
Audit Log Location

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`**.



APPENDIX A

Configure Crosswork Data Gateway VM

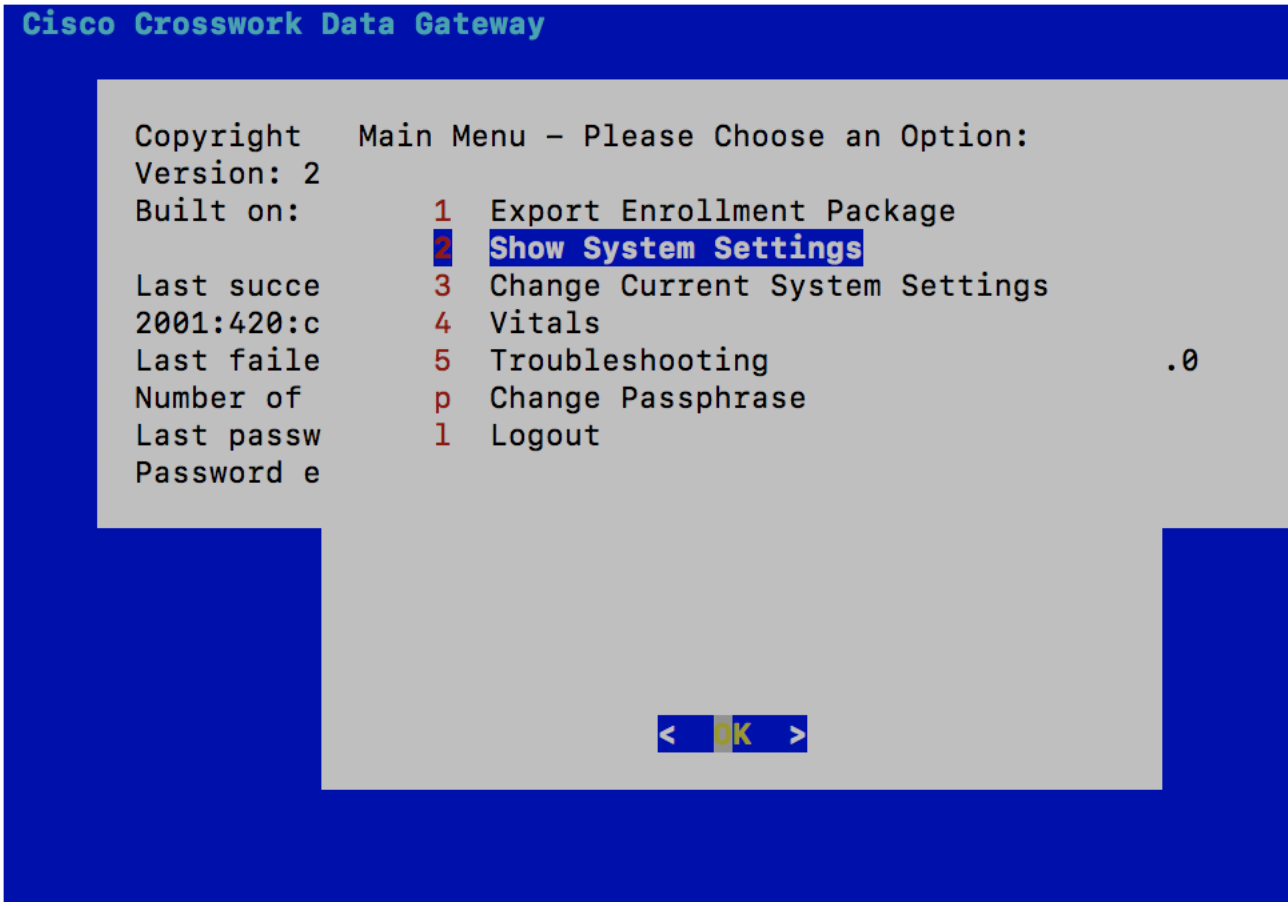
A Cisco Crosswork Data Gateway instance is created as a standalone VM and can be geographically separate from the controller application (the controller application could be Cisco Crosswork Infrastructure or Crosswork Cloud). This VM is capable of connecting to the controller application which will enable 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 adminstrator. See Table Table 37: Permissions Per Role, on page 263.



The Main Menu presents the following options:

1. Export Enrollment Package
2. Show System Settings
3. Change Current System Settings
4. Vitals
5. Troubleshooting

- **p.** Change Passphrase
- **l.** Logout

Manage Crosswork Data Gateway Users

This section contains the following topics:

Supported User Roles

Cisco Crosswork Data Gateway supports only two users with the following user roles:

- **Administrator**: One default **dg-admin** user with administrator role is created when Cisco Crosswork Data Gateway is brought up for the first time. This user cannot be deleted and has both read and write privileges such as start/shut down Cisco Crosswork Data Gateway, register an application, apply authentication certificates, configure server settings, and perform kernel upgrade.
- **Operator**: The **dg-oper** user is also created by default during the initial VM bring up. Operator can review the state/health of the Cisco Crosswork Data Gateway, retrieve health/error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.

Note

- Both users' credentials are configured during Cisco Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

Table 37: Permissions Per Role

Permissions	Administrator	Operator
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 vNIC2 MTU Configure Timezone Configure Password Requirements	✓	×
Vitals		
Docker Containers Docker Images Controller Reachability NTP Reachability Route Table ARP Table Network Connections Disk Space Usage Linux services	✓	✓
Troubleshooting		
Ping a Host	✓	✓
Traceroute to a Host	✓	✓
NTP Status	✓	✓
System Uptime	✓	✓
Run show-tech	✓	✓
Remove All Collectors and Reboot VM	✓	×
Reboot VM	✓	×
Test SSH Connection	✓	✓
Export auditd logs	✓	✓
Re-enroll Data Gateway	✓	✓
Enable TAC Shell Access	✓	×

Permissions	Administrator	Operator
Change Passphrase	✓	✓

Change Password

Both adminstrator 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 **p Change Passphrase** and click **OK**.

Step 2 Input 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:

- vNIC Addresses
- NTP
- DNS
- Proxy
- UUID
- Syslog
- Certificates
- First Boot Provisioning Log
- Timezone

Follow these steps to view the current system settings:

Step 1 From the Main Menu, select **2 Show System Settings**, as shown in the following figure:

Step 2 Click **OK**. The **Show Current System Settings** menu opens.

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.

Setting Option	Description
3 DNS	Displays DNS server details.
4 Proxy	Displays proxy server details (if any configured).
5 UUID	Displays the system UUID.
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.

Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

- NTP
- DNS
- Control proxy
- Static routes
- Syslog
- SSH keys
- Certificate
- vNIC2 MTU
- Timezone
- Password requirements

Note

- Crosswork Data Gateway system settings can only be configured by the administrator.

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 276. 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 273. 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 **1 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 **2 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 **3 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.

Note 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/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/IPv6 subnet in CIDR format.

Step 6 Click **OK** to save the settings.

Configure Syslog

Note For any Syslog server configuration with IPv4/IPv6 support for different linux distributions, please refer your system administrator and configuration guides.

Follow the steps to configure Syslog:

Step 1 From the **Change Current System Settings** Menu, select **5 Configure Syslog**.

Step 2 Enter the new values for the following syslog attributes:.

- Server address: IPv4 or IPv6 address of a syslog server accessible from the management interface. If you are using an IPv6 addres, it must be surrounded by square brackets ([1::1]).
- Port: Port number of the syslog server
- Protocol: Use UDP, TCP, or RELP when sending syslog.
- 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 3 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 certficate file
- Proxy certificate file

Step 1 From the **Change Current System Settings** Menu, select **7 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 **8 Configure vNIC1 MTU**.

Step 2 Enter vNIC2 MTU value.

Step 3 Click **OK** to save the settings.

Configure Timezone

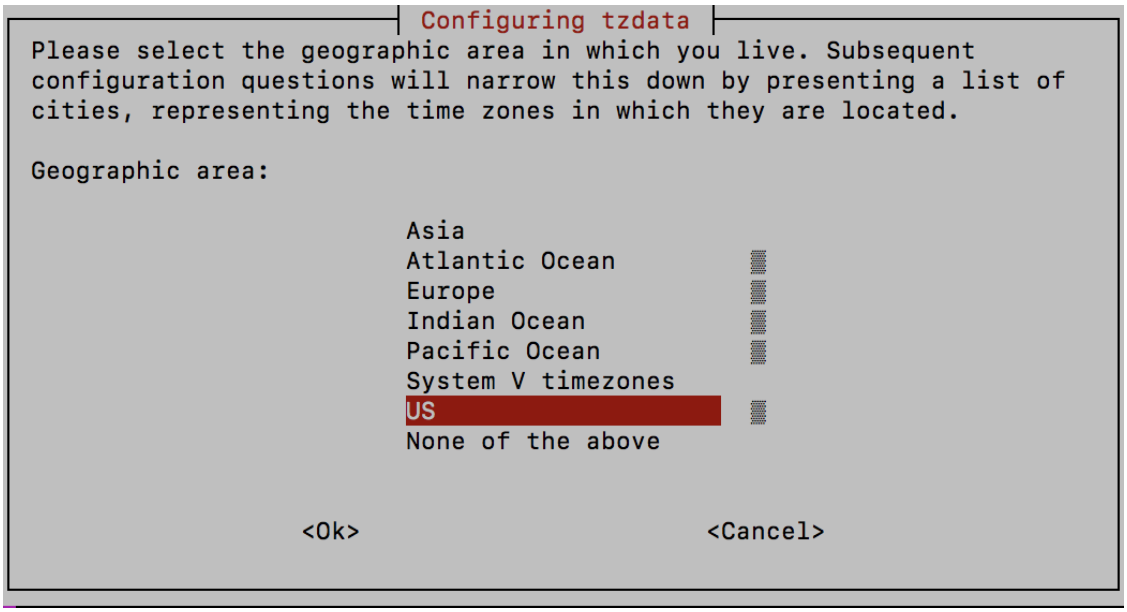
The Crosswork Data Gateway first launches with default timezone as UTC.

Follow the steps to configure timezone:

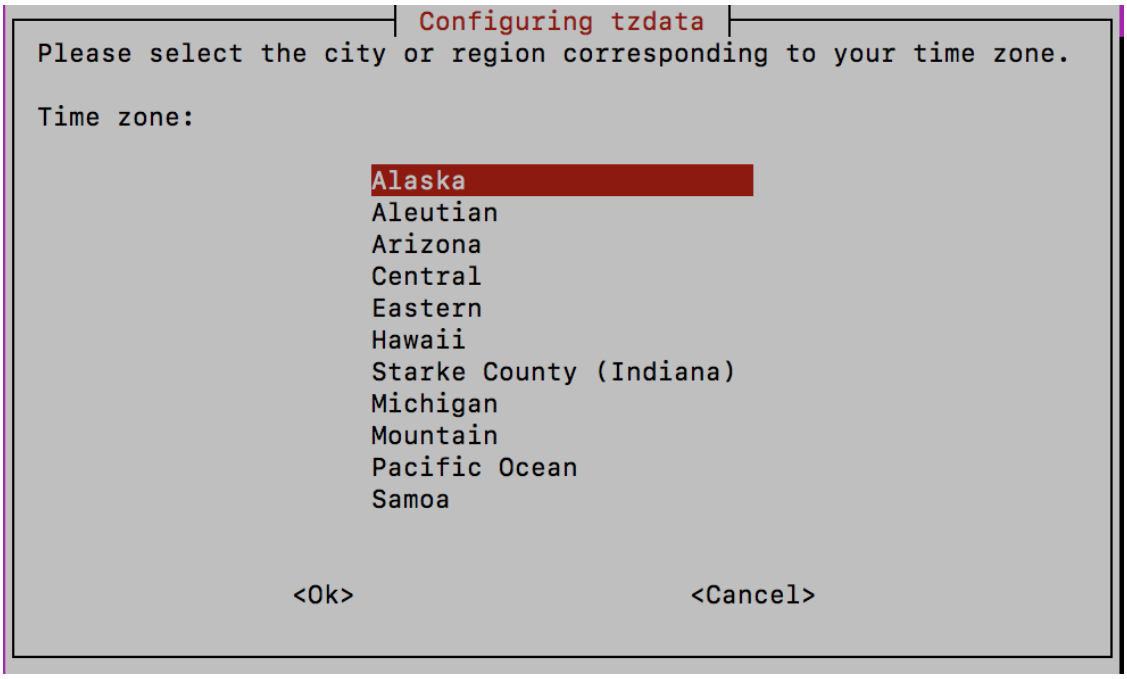
Step 1 In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.

Step 2 Select **9 Configure Timezone**.

Step 3 Select the geographic area in which you live.



Step 4 Select the city or region corresponding to your timezone.



Step 5 Select **OK** to save the settings.

Step 6 Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone.

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 **0 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.

View Crosswork Data Gateway Vitals

Follow these steps to view Cisco Crosswork Data Gateway vitals:

Step 1 From the Main Menu, select **4 Vitals**.

Step 2 From the **Show VM Vitals** menu, select the vital you want to view.

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

Vital	Description
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.
Linux Services	Displays the status of the following linux services: • NTP • SSH • Syslog • Docker • Cisco Crosswork Data Gateway Infrastructure containers.

Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu as shown in the following figure:

Note The following figure shows the Troubleshooting Menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table Table 37: Permissions Per Role, on page 263.

The **Troubleshooting** menu that provides you the following options:

- Ping a Host, on page 275
- Traceroute to a Host, on page 275
- Check NTP Status, on page 275
- Check System Uptime, on page 276

- Run show-tech, on page 276
- Reboot Crosswork Data Gateway VM, on page 277
- Test SSH Connection, on page 276
- Export auditd Logs, on page 277
- Enable TAC Shell Access, on page 277

Ping a Host

Crosswork Data Gateway provides you ping utility that can be used to check reachability to any IP address.

Step 1 From **Troubleshooting** menu, select **1 Ping a Host**.

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 **Traceroute to a Host** option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Crosswork Data Gateway to reach the controller application.

Step 1 From **Troubleshooting** menu, select **2 Traceroute to a Host**.

Step 2 Enter the traceroute destination.

Step 3 Click **OK**.

Check NTP Status

Use this option to check the status of the NTP server.

Step 1 From **Troubleshooting** menu, select **3 NTP Status**.

Step 2 Click **OK**. The cdg displays the NTP server status.

Check System Uptime

Follow the steps to check system uptime since last reboot.

Step 1 From **Troubleshooting** menu, select **4 System Uptime**.

Step 2 Click **OK**. The Crosswork Data Gateway displays the system uptime.

Run show-tech

Crosswork Data Gateway provides the option **show_tech** 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 **5 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**.

Test SSH Connection

This operation attempts an SSH connection with full debugging enabled on the client side.

1. From **Troubleshooting** menu, select **8 Test SSH**.
2. Enter the following details:
   - Port
   - Host
   - Username
   - Passphrase
3. Click **OK**.

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 remove all the collectors (functional images) 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.

Export auditd Logs

Follow the steps to export auditd logs:

Step 1 From **Troubleshooting**, select **9 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 **0 Re-enroll Data Gateway**.

Step 2 Click **Yes** in the below dialog box.

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 **5 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 Log in as the **dg-tac** user Via SSH using the following command:

```
ssh dg-tac@<DG hostname or IP>
```

Step 8 Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. The Cisco engineer must sign this token using the SWIMS Aberto tool.

Step 9 Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt. 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.

Step 10 Once the troubleshooting is complete, log out of the TAC shell.