



## **Cisco Crosswork Network Controller 6.0 Administration Guide**

**First Published:** 2023-11-30

**Last Modified:** 2024-02-16

### **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



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

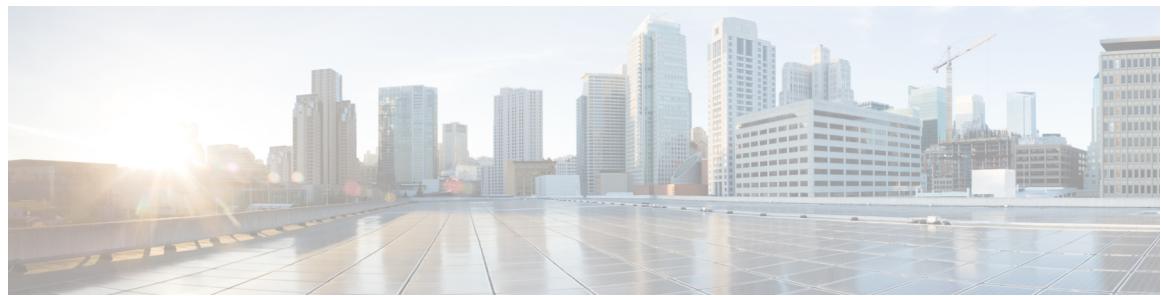
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2024 Cisco Systems, Inc. All rights reserved.





## CONTENTS

---

---

### CHAPTER 1

#### **Get Up and Running (Post-Installation)** 1

- Before You Begin 1
  - Setup Workflow 3
  - Log In and Log Out 4
- 

### CHAPTER 2

#### **Manage the Crosswork Cluster** 7

- Cluster Management Overview 7
  - Check Cluster Health 8
  - Import Cluster Inventory 9
  - Deploy New Cluster Nodes 10
  - Rebalance Cluster Resources 12
  - View and Edit Data Center Credentials 16
  - View Job History 17
  - Export Cluster Inventory 17
  - Retry Failed Nodes 17
  - Erase Nodes 18
  - Manage Maintenance Mode Settings 19
  - Cluster System Recovery 20
  - Collect Cluster Logs and Metrics 23
- 

### CHAPTER 3

#### **Cisco Crosswork Data Gateway** 25

- Overview of Cisco Crosswork Data Gateway 25
- Set Up Crosswork Data Gateway to Collect Data 32
  - Crosswork Data Gateway High Availability with Pools 32
  - Create a Cisco Crosswork Data Gateway Pool 34
  - Perform a Manual Failover 38

Attach Devices to a Crosswork Data Gateway	39
Manage Crosswork Data Gateway Post-Setup	40
Monitor Crosswork Data Gateway Health	40
Viewing Crosswork Data Gateway Alarms	43
Manage a Crosswork Data Gateway Pool	44
Manage Cisco Crosswork Data Gateway Device Assignments	46
Maintain Crosswork Data Gateway Instances	48
Change the Administration State of Cisco Crosswork Data Gateway Instance	48
Delete Crosswork Data Gateway Instance from Cisco Crosswork	49
Redeploy a Crosswork Data Gateway Instance	51
Configure Crosswork Data Gateway Global Settings	51
Create and Manage External Data Destinations	52
Licensing Requirements for External Collection Jobs	52
Add or Edit a Data Destination	53
Delete a Data Destination	58
Manage Device Packages	59
Custom Package	59
System Device Package	61
Configure Crosswork Data Gateway Global Parameters	61
Allocate Crosswork Data Gateway Resources	63
Manage Crosswork Data Gateway Collection Jobs	66
Types of Collection Jobs	67
CLI Collection Job	68
SNMP Collection Job	69
MDT Collection Job	76
Syslog Collection Job	78
gNMI Collection Job	87
Create a Collection Job from Cisco Crosswork UI	98
Monitor Collection Jobs	104
Delete a Collection Job	107
Troubleshoot Crosswork Data Gateway	108
Check Connectivity to the Destination	108
Download Service Metrics	109
Download Showtech Logs	109

Reboot Cisco Crosswork Data Gateway VM	111
Change Log Level of Crosswork Data Gateway Components	112
Network Load Balancer Displays Incorrect Health Status for Active Crosswork Data Gateway	113
Collection Job Status on the Collection Jobs Page is in the DEGRADED State	114
Data Gateway continues to collect data regardless of a change to the SNMPv3 Engine ID	114

---

**CHAPTER 4****Manage Backups** **115**

Backup and Restore Overview	115
Manage Cisco Crosswork Backup and Restore	116
Restore Cisco Crosswork After a Disaster	119
Crosswork Data Gateway Disaster Recovery Scenarios	120
Crosswork Data Gateway Disaster Recovery with High Availability	120
Crosswork Data Gateway Disaster Recovery without High Availability	122
Resolve SR-TE Policies and RSVP-TE Tunnels	124
Backup Cisco Crosswork with Cisco NSO	124
Restore Cisco Crosswork with Cisco NSO	125
Migrate Data Using Backup and Restore	127

---

**CHAPTER 5****Set Up and Use Your Topology Map for Network Visualization** **131**

Overview of the Topology Map	131
Use Internal Maps Offline for Geographical Map Display	135
Use Device Groups to Filter your Topology Map	135
Create Device Groups Individually	136
Create Rules for Dynamic Device Grouping	136
Modify Device Groups	137
Delete Device Groups	137
Move Devices from One Group to Another	137
Import Multiple Device Groups	138
Export Multiple Device Groups	139
View Device Details from the Topology Map	139
View Basic Device Details	139
View All Device Details	140
Identify Device Routing Details	141
Identify the Links on a Device	142

Get Details About Topology Links	143
View Link Details	143
View Link Interface Metrics	146
Link States and Discovery Methods	147
Protocols Used for Topology Services	147
Enable or Disable Topology Link Discovery	148
Import and Export Geographical Data	150
Import Geographical Data to Keyhole Markup Language (KML) Format	150
Export Geographical Data to Keyhole Markup Language (KML) Format	151
Customize your Map for your Needs	151
Show or Hide Device State	152
Define the Device Label Type	152
Differentiate Aggregated Links from Single Links	153
Differentiate all Down Links by Color	154
Show Link Utilization by Color	155
Troubleshoot your Topology Map	156
Rebuild the Topology	156
Find Missing L2 Links	157
Missing L3 Links	158
Error Record in Alarm/Events Report of Topology Services	159

---

**CHAPTER 6****Prepare Infrastructure for Device Management** 161

Manage Credential Profiles	161
Create Credential Profiles	162
Import Credential Profiles	164
Edit Credential Profiles	166
Export Credential Profiles	167
Delete Credential Profiles	167
Change the Credential Profile for Multiple Devices	168
Manage Providers	168
About Provider Families	170
Provider Dependency	170
About Adding Providers	171
Add Providers Through the UI	172

Add Cisco NSO Providers	174
Enable Layered Service Architecture (LSA)	176
NSO LSA Setup Recovery	177
View Installed NSO Function Packs	178
Add Cisco SR-PCE Providers	178
Cisco SR-PCE Reachability Issues	182
Multiple Cisco SR-PCE HA Pairs	183
SR-PCE Configuration Examples	187
Path Computation Client (PCC) Support	190
Add Cisco WAE Providers	190
Add Syslog Storage Providers	191
Add an Alert Provider	193
Add Proxy Providers	194
Import Providers	195
Get Provider Details	196
Edit Providers	197
Delete Providers	198
Export Providers	199
Manage Tags	199
Create Tags	201
Import Tags	201
Apply or Remove Device Tags	202
Delete Tags	203
Export Tags	203

---

**CHAPTER 7**

<b>Onboard and Manage Devices</b>	<b>205</b>
Add Devices to the Inventory	205
Telemetry Prerequisites for New Devices	206
Sample Configuration for Cisco NSO Devices	211
Add Devices through the UI	211
Add Devices by Importing from CSV File	216
Export Device Information to a CSV File	218
Manage Network Devices	218
Device State	219

Filter Network Devices by Tags	221
Get More Information About a Device	222
View Device Job History	222
Edit Devices	223
Delete Devices	224
Work With Device Alerts	225
View Alert Details	227
Acknowledge Alarms	228
Clear Alarms	229
Annotate Alarms	229
Work With Saved Alert Views	230
Export Alerts	231
Customize Alerting Devices	232
Customize Alarm Auto Clear	232
Customize Instructive Text for Alarms	233
Customize Alert Cleanup	234
Customize Alarm Severity	235

---

**CHAPTER 8**

<b>Zero Touch Provisioning</b>	<b>237</b>
Zero Touch Provisioning Concepts	237
Platform Support for ZTP	239
ZTP Implementation Decisions	240
ZTP Processing Logic	242
ZTP and Evaluation Licenses	246
ZTP Setup Workflow	246
Meet ZTP Prerequisites	247
Assemble and Load ZTP Assets	248
Find and Load Software Images	249
Prepare and Load Configuration Files	250
Load ZTP Assets	261
Find and Load SMUs	263
Create Credential Profiles for ZTP	264
Find and Load Device Serial Numbers	265
Update the PDC, Owner Certificates, and Owner Key	266

Load Ownership Vouchers	268
Prepare and Load the SUDI Root Certificate	269
Create ZTP Profiles	270
Prepare ZTP Device Entry Files	271
Prepare Single ZTP Device Entries	276
ZTP Provisioning Workflow	277
Upload ZTP Device Entries	278
Set Up DHCP for Crosswork ZTP	278
Set Up DHCP for Classic ZTP	278
Set Up DHCP for Secure ZTP	282
Set Up DHCP and TFTP for PnP ZTP	283
Classic ZTP DHCP Setup Scripts for Cisco Prime Network Registrar (CPNR)	284
Trigger ZTP Device Bootstrap	299
Complete Onboarded ZTP Device Information	301
Reconfigure Onboarded ZTP Devices	302
Retire or Replace Devices Onboarded With ZTP	302
ZTP Asset Housekeeping	303
Troubleshoot ZTP Issues	304
Diagnose ZTP Issues Using the Alarms Window	304
Diagnose ZTP Issues Using the Status Column	304
Diagnose ZTP Issues Using Error Logs	305
Troubleshoot Common ZTP Issues	306
Troubleshoot Classic ZTP Issues	309
Troubleshoot PnP ZTP Issues	309
Troubleshoot ZTP: Alarms and Events Reference	310

---

**CHAPTER 9****Manage System Access and Security** **321**

Manage Certificates	321
Certificate Types and Usage	322
Add a New Certificate	326
Edit Certificates	328
Download Certificates	331
Renew Certificates	331
Manage Licenses	334

Configure Transport Settings	335
Register Cisco Crosswork Application via Token	336
Manually Perform Licensing Actions	338
Register Cisco Crosswork Applications via Offline Reservation	339
Update Offline Reservation	340
Disable Offline Reservation	341
License Authorization Statuses	342
Authorization Status Response	342
Manage Users	344
Administrative Users Created During Installation	346
User Roles, Functional Categories and Permissions	346
Create User Roles	347
Clone User Roles	348
Edit User Roles	349
Delete User Roles	349
Global API Permissions	349
Manage Active Sessions	361
Manage Device Access Groups	362
Create Device Access Groups	363
Edit Device Access Groups	364
Assign Task permissions	364
Associate a User with a Device Access Group	365
Configure NSO Servers	366
Configure Standalone NSO	366
Configure LSA NSO	371
Set Up User Authentication (TACACS+, LDAP, and RADIUS)	373
Manage TACACS+ Servers	374
Manage LDAP Servers	379
Manage RADIUS Servers	384
Configure AAA Settings	385
Enable Single Sign-on (SSO)	386
Security Hardening Overview	388
Authentication Throttling	388
Core Security Concepts	388

HTTPS	388
X.509 Certificates	389
1-Way SSL Authentication	389
Disable Insecure Ports and Services	390
Harden Your Storage	391
Configure System Settings	391
Configure a Syslog Server	391
Syslog Events	392
Configure a Trap Server	393
Configure the Interface Data Collection	394
Set the Pre-Login Disclaimer	395
Manage File Server Settings	396

---

**CHAPTER 10****Manage System Health** 397

Monitor System and Application Health	397
Monitor Cluster Health	397
Monitor Platform Infrastructure and Application Health	398
Visually Monitor System Functions in Real Time	399
Check System Health Example	402
View System and Network Alarms	404
System Events	405
Sample Day 0, Day 1, and Day 2 Events	406
Enable Trap Handling	414
Collect Audit Information	414
View Audit Log	416

---

**APPENDIX A****Configure Crosswork Data Gateway Instance** 419

Use the Interactive Console	419
Manage Crosswork Data Gateway Users	420
Supported User Roles	420
Change Passphrase	423
View Current System Settings	423
Change Current System Settings	425
Configure NTP	427

Configure DNS	428
Configure Control Proxy	428
Configure Static Routes	429
Add Static Routes	429
Delete Static Routes	429
Configure Syslog	429
Create New SSH Keys	430
Import Certificate	431
Configure vNIC2 MTU	431
Configure Timezone of the Crosswork Data Gateway VM	432
Configure Password Requirements	433
Configure Simultaneous Login Limits	434
Configure Idle Timeout	435
Configure Remote Auditd Server	435
Configure Login Frequency	435
Configure Interface Address	436
View Crosswork Data Gateway Vitals	439
Troubleshooting Crosswork Data Gateway VM	442
Run Diagnostic Commands	442
Ping a Host	443
Traceroute to a Host	443
Command Options to Troubleshoot	444
Download tcpdump	444
Run a Controller Session Test	445
Run show-tech	447
Reboot Crosswork Data Gateway VM	447
Shutdown the Crosswork Data Gateway VM	448
Export auditd Logs	448
Re-enroll Crosswork Data Gateway	448
Remove Rotated Log Files	449
Enable TAC Shell Access	449

---

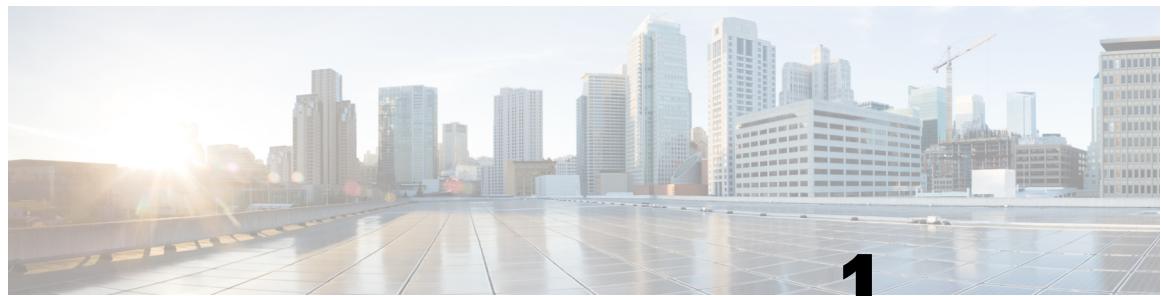
**APPENDIX C**      **List of Pre-loaded YANG Modules for MDT Collection**      **459**

---

**APPENDIX D**      **Cisco EPM Notification MIB**      **463**

    Cisco EPM Notification MIB      **463**





# CHAPTER 1

## Get Up and Running (Post-Installation)

---

This section contains the following topics:

- [Before You Begin, on page 1](#)
- [Setup Workflow, on page 3](#)
- [Log In and Log Out, on page 4](#)

## 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 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.
- **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. Crosswork also supports integration with many TACACS+ and LDAP servers to allow you to centrally manage user roles and accounts. See [Set Up User Authentication \(TACACS+, LDAP, and RADIUS\), on page 373](#) for more details.
- **Device-Access Groups:** Device-access groups (DAGs) are groups of devices that are used to define device access for users. Users associated with the DAGs are allowed to make configuration changes and provision services on the devices that belong to those DAGs. When a user is created, they must be assigned both a DAG (at least one) and a role. See [Manage Device Access Groups, on page 362](#) for more details.
- **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 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 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. For other type of providers (NSO, SR-PCE, Storage, Alert, and WAE), this always includes user IDs, passwords, and connection protocols. 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. Otherwise, you will need to manually go back and add them where you wish to use them. See [Create Tags, on page 201](#) for more details.

- **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) needs 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 the type of Crosswork application is used. It is important to review and gather each Crosswork application requirement, before configuring a Provider. For more information, see [About Provider Families, on page 170](#) and [Provider Dependency, on page 170](#).

- Cisco Network Services Orchestrator (Cisco NSO) is used by many Crosswork Applications to make changes to device configurations and to provision services on devices. To add Cisco NSO as a provider you will need the IP address and credentials used to communicate. See [Add Cisco NSO Providers, on page 174](#) for more details.



#### Note

Additional steps are needed when using Cisco NSO in LSA mode. See [Enable Layered Service Architecture \(LSA\), on page 176](#) for more details.

- If you plan to use Crosswork Optimization Engine, at least one Cisco SR-PCE provider, at minimum, must be defined in order to discover devices and to distribute policy configuration to devices. Additional SR-PCEs can be used for more complex network topologies and redundancy. You can either add devices to the system yourself (see [Add Devices to the Inventory, on page 205](#) for more details) or auto-onboard them via the SR-PCE discovery (see [Add Cisco SR-PCE Providers, on page 178](#) for more details). While you can change the configuration at any time it is ideal to decide which process you will use before you get too far into the deployment and configuration of Crosswork.
- **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 205](#).
- **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 [Cisco Crosswork Data Gateway, on page 25](#).

- **Labels:** Labels are used with Crosswork Change Automation to restrict which users are able to execute a playbook. For example, while you may want lower-level operators to be able to run check playbooks you may use labels to prevent them from running more complex or impactful playbooks that make changes to network device configuration.
- If you plan to use Crosswork 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 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.
- If you plan to install the Crosswork Service Health application, you should review the samples provided to determine if they are adequate for monitoring devices in your network.

Note that you can capture the devices, credential profiles, tags, and providers lists in spreadsheet form, convert the spreadsheet to CSV format, and then upload them in bulk to the 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 Cisco Crosswork Applications and Crosswork Data Gateway. For the installation instructions, please refer to the latest version of [Cisco Crosswork Network Controller 6.0 Installation Guide](#).

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

**Table 1: Tasks to Complete to Get Started with Cisco Crosswork**

Step	Action
1. Ensure that your devices are configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: <a href="#">Telemetry Prerequisites for New Devices, on page 206</a> <a href="#">Sample Configuration for Cisco NSO Devices, on page 211</a>
2. (Optional) If the set-up is a Cisco NSO LSA deployment, enable LSA.	Follow the steps in <a href="#">Enable Layered Service Architecture (LSA), on page 176</a>
3. Create credential profiles.	Follow the steps in <a href="#">Create Credential Profiles, on page 162</a>
4. Add the provider(s).	Follow the steps in <a href="#">About Adding Providers, on page 171</a>
5. Validate communications with the provider(s).	Check on the provider's reachability using the steps in <a href="#">Get Provider Details, on page 196</a>

Step	Action
6. Import or create tags.	To import them: <a href="#">Import Tags, on page 201</a> To create them: <a href="#">Create Tags, on page 201</a>
7. Onboard devices using the method you prefer.	See <a href="#">Add Devices to the Inventory, on page 205</a>
8. Setup Crosswork Data Gateway	Follow the steps in <a href="#">Set Up Crosswork Data Gateway to Collect Data, on page 32</a> .
9. Validate Cisco Crosswork communications with devices.	Review the <b>Devices</b> window (see <a href="#">Manage Network Devices, on page 218</a> ). All the devices you have onboarded should be reachable.  Click  to investigate any device whose <b>Reachability State</b> is marked as  (unreachable),  (degraded), or  (unknown).
10. (Optional) Enable source IP for auditing.	If you want to log the user's IP address for auditing and accounting, see <a href="#">Configure AAA Settings, on page 385</a> .
11. (Optional) Create additional user accounts and user roles.	Follow the steps in <a href="#">Manage Users, on page 344</a> and <a href="#">Create User Roles, on page 347</a> .
12. (Optional) Import or create additional credential profiles and providers.	To import providers: <a href="#">Import Providers, on page 195</a> To create providers: <a href="#">Add Providers Through the UI, on page 172</a>
13. (Optional) Group your devices logically as per your requirement.	Follow the steps in <a href="#">Use Device Groups to Filter your Topology Map, on page 135</a> .
14. (Optional) Set display preferences for your topology.	Follow the steps in <a href="#">Use Internal Maps Offline for Geographical Map Display, on page 135</a> and <a href="#">Show Link Utilization by Color, on page 155</a> .

## Log In and Log Out

The Cisco Crosswork user interface is browser-based. For the supported browser versions, see the [Cisco Crosswork Network Controller 6.0 Installation Guide](#).

**Attention**

- Cisco Crosswork locks out users for a specified period of time after repeated unsuccessful login attempts. Users can attempt to log in with the correct credentials once the wait time is over. Users remain locked out until they enter the valid login credentials. The number of unsuccessful login attempts and the lockout time are configured by the administrators in the **Local Password Policy**. For more information, see [Configure AAA Settings, on page 385](#).
- The Crosswork login page is not rendered when the CAS (Central Authentication Service) pod is restarting or not running.
- If a user has multiple sessions open from same client (via multiple tabs/windows) and logout/terminate session is performed for that session from one of the windows, the logout screen is displayed on that window while the following error message is displayed on all other tabs/windows: "Your session has ended. Log into the system again to continue".

---

**Procedure**

---

**Step 1** Open a web browser and enter:

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

or

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

**Note**

- The IPv6 address in the URL must be enclosed with brackets.
- When you access 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.

The default administrator user name and password is **admin**. This account is created automatically at installation (see [Administrative Users Created During Installation, on page 346](#)). The initial password for this account must be changed during installation verification. Cisco strongly recommends that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user roles with appropriate privileges and assign new users to those roles. At least one of the users you create must be assigned the "admin" role.

**Step 3** Click **Log In**.**Step 4** To log out, click  in the top right of the main window and choose **Log out**.





## CHAPTER 2

# Manage the Crosswork Cluster

---

This section contains the following topics:

- [Cluster Management Overview, on page 7](#)
- [Check Cluster Health, on page 8](#)
- [Import Cluster Inventory, on page 9](#)
- [Deploy New Cluster Nodes, on page 10](#)
- [Rebalance Cluster Resources, on page 12](#)
- [View and Edit Data Center Credentials, on page 16](#)
- [View Job History, on page 17](#)
- [Export Cluster Inventory, on page 17](#)
- [Retry Failed Nodes, on page 17](#)
- [Erase Nodes, on page 18](#)
- [Manage Maintenance Mode Settings, on page 19](#)
- [Cluster System Recovery, on page 20](#)
- [Collect Cluster Logs and Metrics, on page 23](#)

## Cluster Management Overview

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

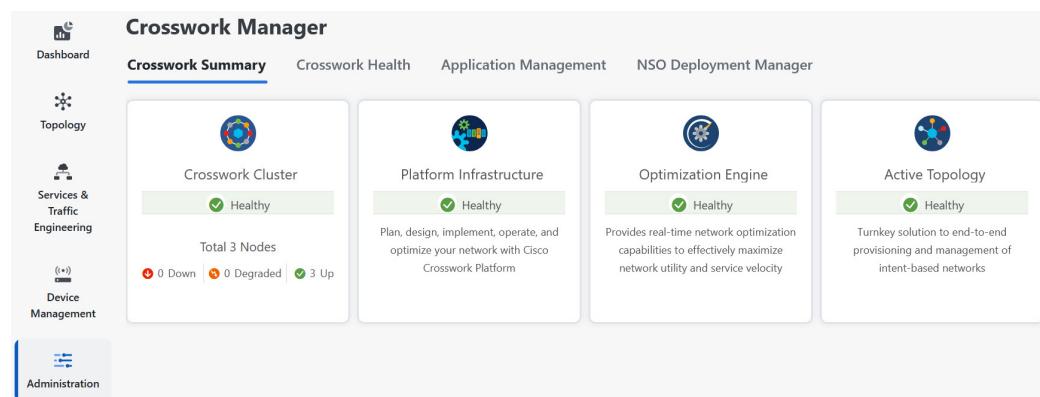
A single Crosswork cluster consists of a minimum of three nodes, all operating in a hybrid configuration. These three hybrid nodes are mandatory for all Cisco Crosswork deployments. If you have more demanding scale requirements, you can add up to two worker nodes. For more information, see [Deploy New Cluster Nodes, on page 10](#).

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

## 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.

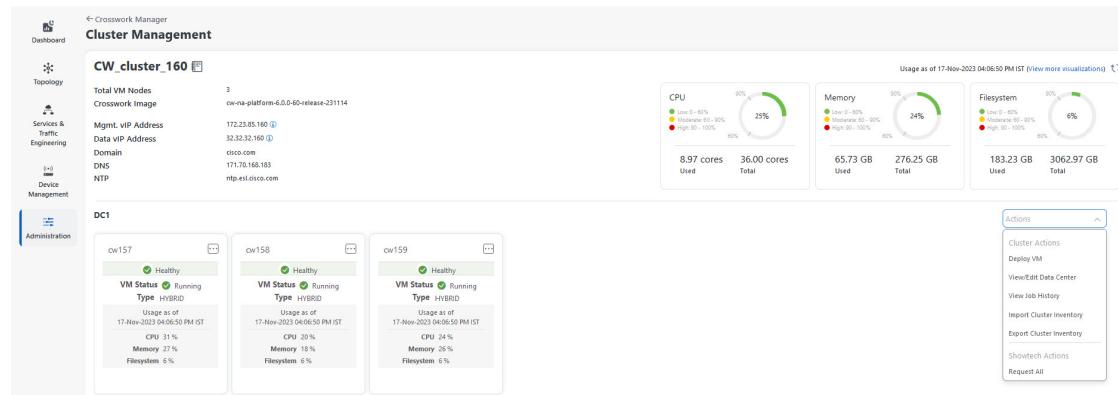
The top left section of the window provides details about the cluster while the top right provides details about overall cluster resource consumption. The bottom section breaks down the resource utilization by node, with a separate detail tile for each node. The window shows other details, including the IP addresses in use, whether each node is a hybrid or worker, and so on.

On the top-right corner, click the **View more visualizations** link to [Visually Monitor System Functions in Real Time, on page 399](#).

## Cluster Management

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**



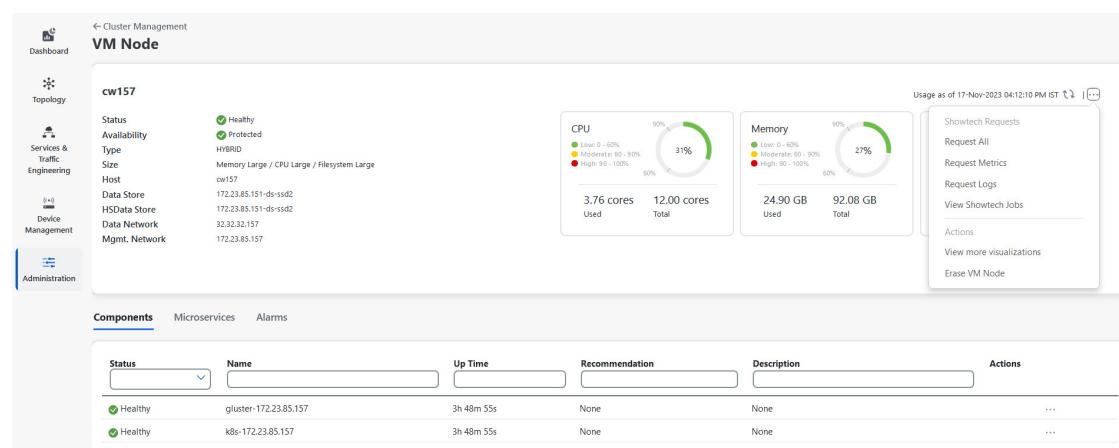
**Attention**

In some cases of manual installations, the Cluster Management window may not display the inventory details in the upper left corner of this screen correctly. In such cases, you need to manually import the cluster inventory file as described in [Import Cluster Inventory, on page 9](#). Failure to import the inventory can impact your ability to deploy additional nodes and manage the cluster properly.

**VM Node Details**

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: Cluster Management 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 398](#).

**Failed Nodes**

- If one of the hybrid nodes is faulty, along with one or more worker nodes and applications, try the *Clean System Reboot* procedure described in [Cluster System Recovery, on page 20](#).
- If more than one hybrid node is faulty, follow the *Redeploy and Recover* procedure described in [Cluster System Recovery, on page 20](#).

# Import Cluster Inventory

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

**Attention**

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

**Note**

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

**Procedure**

**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.

## Deploy New Cluster Nodes

After your Cisco Crosswork cluster is formed, you may need more nodes to meet your requirements. The following steps show how to deploy a new VM node:

**Note**

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

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

**Before you begin**

You must know the following:

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

- If you installed your cluster manually, you must import the cluster inventory file to Cisco Crosswork before you can deploy a new node. For more information, see [Import Cluster Inventory, on page 9](#). The **Deploy VM** option will be disabled until you complete the import operation.

## Procedure

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

**Step 6**

If this node was added to reduce the heavy load (running > 90%) on the existing nodes, you can rebalance the resources (see [Rebalance Cluster Resources, on page 12](#) for details), or restart some processes to force the system to move them to the newly added node.

## Rebalance Cluster Resources

As part of cluster management, Crosswork constantly monitors the resource utilization in each cluster node. If the CPU utilization in any of the nodes becomes high (by default, the "high" range is set as 90-100%), Crosswork triggers a notification prompting you to take action. You can then use the **Rebalance** feature to reallocate the resources between the existing VM nodes in your cluster.

If the other nodes in your cluster are also nearing their full capacity, you are recommended to deploy a new worker node before attempting the **Rebalance** option to ensure easy reallocation of resources. For more information about adding a worker node, see [Deploy New Cluster Nodes, on page 10](#).

**Caution**

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

**Before you begin**

- Crosswork must be in maintenance mode before rebalancing to ensure data integrity.
- Any users logged in during the rebalancing will lose their sessions. Notify other users beforehand that you intend to put the system in maintenance mode for rebalancing, and give them a timeline to log out.

### Procedure

**Step 1**

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

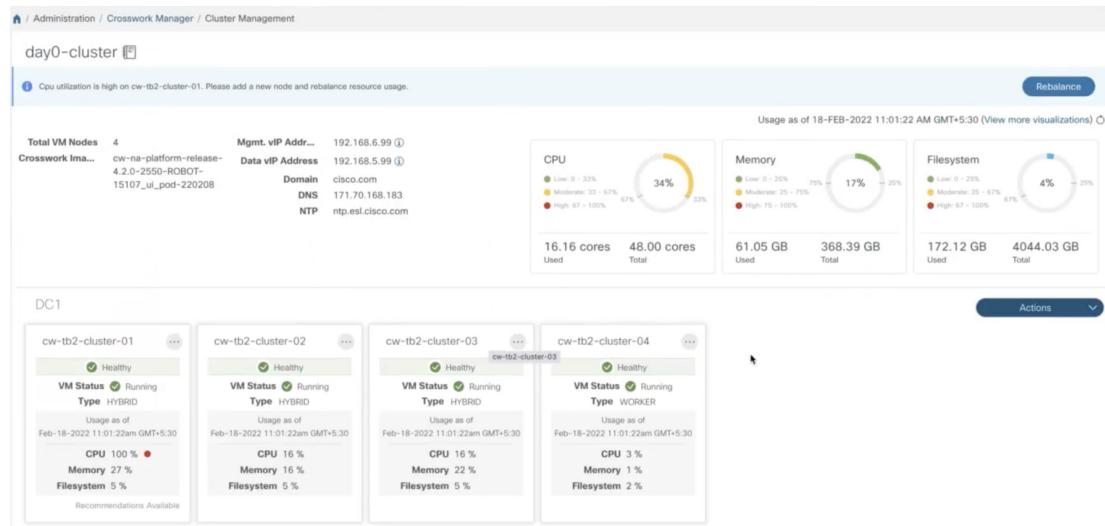
**Step 2**

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

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

A banner displayed below the cluster name warns you about the resource over utilization in the cluster node and recommends adding more worker nodes.

Figure 5: Rebalance notification

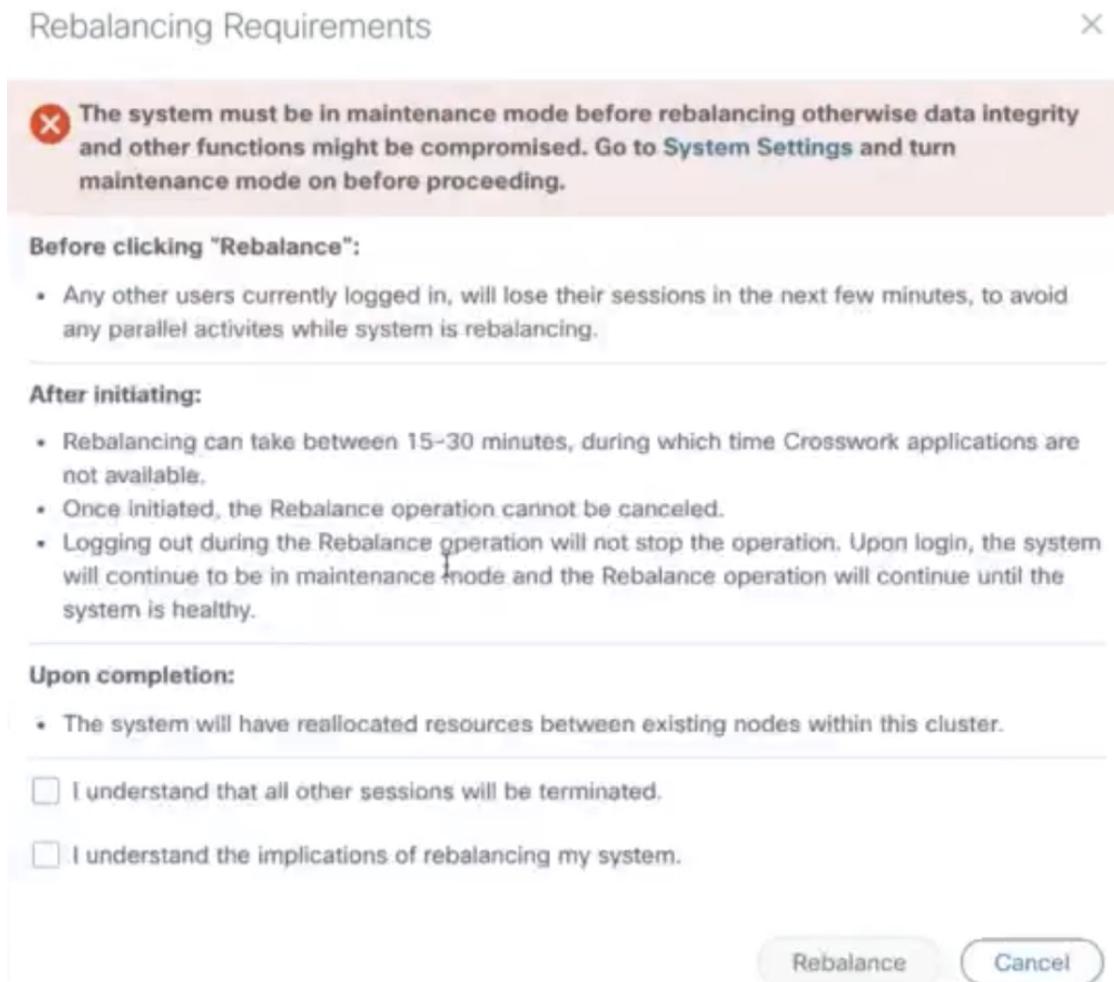


On the tile for the node, you can click and choose **View Details** to see more details.

### Step 3

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

Figure 6: Rebalancing Requirements



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

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

Figure 7: Rebalancing Status

### Rebalancing In Progress...

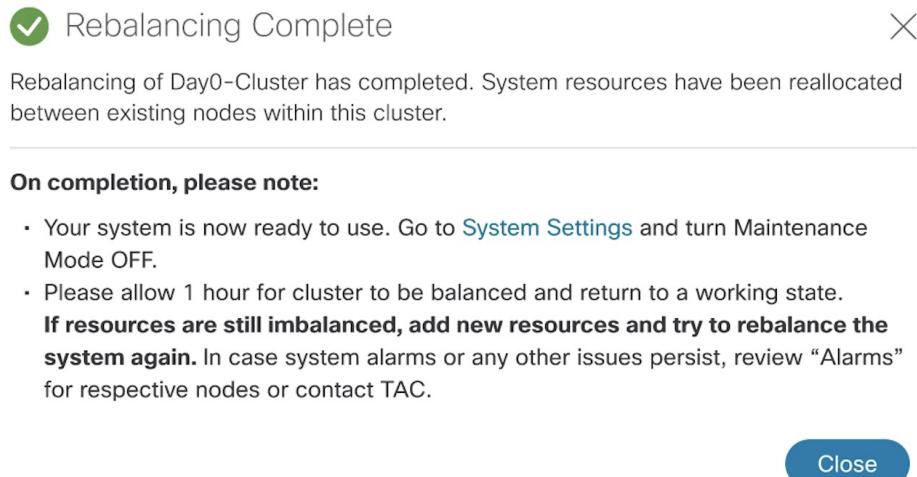
Rebalancing of day0-cluster has started. This process may take 15-30 mins and System will be unavailable for this duration.

Wait for the balancer to finish

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

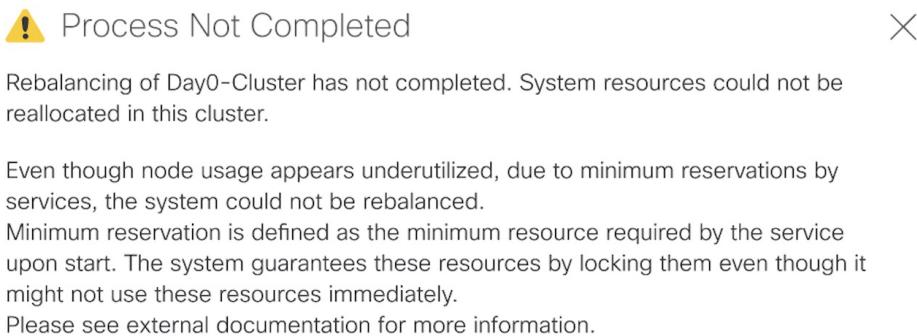
- **Success scenario:** A dialog box indicating successful rebalancing operation. Follow the instructions in the dialog box to proceed further.

**Figure 8: Rebalancing Result - Success**



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

**Figure 9: Rebalancing Result - Add new Worker node**



**Add a new worker node and rebalance again.**

**Close**

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

Figure 10: Rebalancing Result - Add new Worker node



## Process Not Completed



Rebalancing of Day0-Cluster has not completed. System resources could not be reallocated in this cluster.

Even though node usage appears underutilized, due to minimum reservations by services, the system could not be rebalanced.

See More 

New worker nodes cannot be added. Please contact TAC.

[Close](#)

## View and Edit Data Center Credentials

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

### Before you begin

Ensure you have the current credentials for vCenter.



**Note**

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

### Procedure

- 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 Job History

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

## Procedure

---

- Step 1** From the main menu, choose **Administration > Crosswork Manager**.
  - Step 2** On the **Crosswork Summary** tab, click the **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.
- 

# Export Cluster Inventory

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

## Procedure

---

- 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.
- 

# Retry Failed Nodes

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

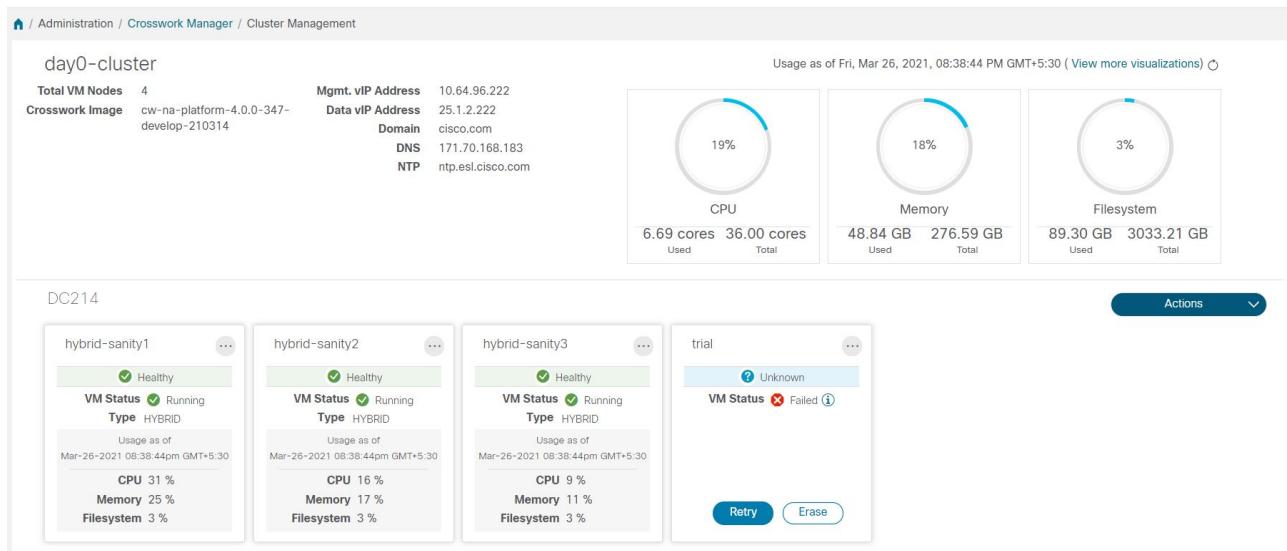
## Procedure

---

- Step 1** From the main menu, choose **Administration > Crosswork Manager**.
- Step 2** On the **Crosswork Summary** tab, click the **Crosswork Cluster** tile to display the **Cluster Management** window.

## Erase Nodes

Figure 11: 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 the Cisco Crosswork cluster. Erasing a node removes the node reference from the Cisco Crosswork cluster and deletes it from the host VM.

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

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

**Warning**

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

**Note**

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

**Procedure**

- 
- 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.

**Note**

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

## Manage Maintenance Mode Settings

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

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

### Before you begin

**Attention**

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

**Procedure****Step 1**

To put Crosswork in maintenance mode:

- From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance Mode**.
- Drag the **Maintenance** slider to the right, or **On** position.
- Crosswork warns you that it is about to initiate a shutdown. Click **Continue** to confirm your choice.

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

**Note**

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

**Step 2**

To restart Crosswork from maintenance mode:

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

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

**Note**

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

# Cluster System Recovery

## When System Recovery Is Needed



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

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

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

The cluster can tolerate one hybrid node reboot (whether graceful or ungraceful). During the hybrid node reboot, the system is still functional, but degraded from an availability point of view. The system can tolerate any number of failed worker nodes, but again, system availability is degraded until the worker nodes are restored.

Cisco Crosswork generates alarms when nodes, applications, or services are malfunctioning. If you are experiencing system faults, examine the alarm and check the health of the individual node, application, or service identified in the alarm. You can use the features described in [Cluster Management Overview, on page 7](#) to drill down on the source of the problem and, if it turns out to be a service fault, restart the problem service.

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

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

**Important**

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

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

### Clean System Reboot (VMware)

Follow these steps to perform a clean system reboot:

1. Put Crosswork in Maintenance mode. See [Manage Maintenance Mode Settings, on page 19](#) for more details.
2. Power down the VM hosting each node:
  - a. Log in to the VMware vSphere Web Client.
  - b. In the **Navigator** pane, right-click the VM that you want to shut down.
  - c. Choose **Power > Power Off**.
  - d. Wait for the VM status to change to **Off**.
3. Repeat Step 2 for each of the remaining VMs, until all the VMs are shut down.
4. Power up the VM hosting the first of your hybrid nodes:
  - a. In the **Navigator** pane, right-click the VM that you want to power up.
  - b. Choose **Power > Power Up**.

- c. Wait for the VM status to change to **On**, then wait another 30 seconds before continuing.
- 5. Repeat Step 4 for each of the remaining hybrid nodes, staggering the reboot by 30 seconds before continuing. Then continue with each of your worker nodes, again staggering the reboot by 30 seconds.
- 6. The time taken for all the VMs to be powered on can vary based on the performance characteristics of your hardware. After all VMs are powered on, wait for a few minutes and login to Crosswork.
- 7. Move Crosswork out of Maintenance mode. See [Manage Maintenance Mode Settings, on page 19](#) for more details.

**Note**

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

### 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 116](#).

1. Power down the VM hosting each node:
  - a. Log in to the VMware vSphere Web Client.
  - b. In the **Navigator** pane, right-click the VM that you want to shut down.
  - c. Choose **Power > Power Off**.
  - d. Wait for the VM status to change to **Off**.
  - e. Repeat these steps as needed for the remaining nodes in the cluster.
2. Once all the VMs are powered down, delete them:
  - a. In the VMware vSphere Web Client **Navigator** pane, right-click the VM that you want to delete.
  - b. Choose **Delete from Disk**.
  - c. Wait for the VM status to change to **Deleted**.
  - d. Repeat these steps as needed for the remaining VM nodes in the cluster.
3. Deploy a new Cisco Crosswork cluster, as explained in [Cisco Crosswork Network Controller 6.0 Installation Guide](#).
4. Recover the system state to the newly deployed cluster, as explained in [Restore Cisco Crosswork After a Disaster, on page 119](#).

# Collect Cluster Logs and Metrics

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

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.



**Note** Showtech logs must be collected separately for each application.

## Procedure

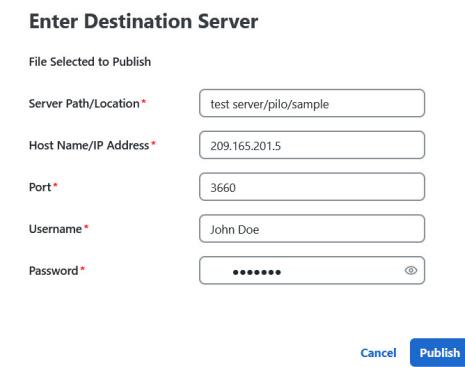
- Step 1** From the main menu, choose **Administration > Crosswork Manager**.
- Step 2** On the **Crosswork Summary** tab, click the **Crosswork Cluster** tile to display the **Cluster Management** window.
- Step 3** To collect logs and metrics for the cluster, click **Actions** and select the showtech option that you want to perform.
- Step 4** To collect logs and metrics for any node in the cluster:
  - Click the node tile.
  - Click **Showtech Options** and select the operation that you want to perform.
- Step 5** To collect logs and metrics for the individual microservices running on the VM node, click  under the **Actions** column. Then select the showtech option that you want to perform.
- Step 6** (Optional) Click **View Showtech Jobs** to view the status of your showtech jobs. The **Showtech Requests** window displays the details of the showtech jobs.

**Figure 12: Showtech Requests window**

Status	Job ID	Created Time	Scope	Description	Action	Publish Details
Completed	20231130115334	30-Nov-2023 05:23:34 PM IST	optima-ui-service	showtech_optima-ui-service_logs_20231130115334.tar.gz	Publish	Details
Completed	20231130112838	30-Nov-2023 04:58:38 PM IST	optima-ui-service	showtech_optima-ui-service_logs_20231130112838.tar.gz	Publish	Details

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

**Figure 13: Destination Server window**



Enter Destination Server

File Selected to Publish

Server Path/Location\*

Host Name/IP Address\*

Port\*

Username\*

Password\*

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



## CHAPTER 3

# Cisco Crosswork Data Gateway

---

This section contains the following topics:

- [Overview of Cisco Crosswork Data Gateway, on page 25](#)
- [Set Up Crosswork Data Gateway to Collect Data, on page 32](#)
- [Manage Crosswork Data Gateway Post-Setup, on page 40](#)
- [Configure Crosswork Data Gateway Global Settings, on page 51](#)
- [Manage Crosswork Data Gateway Collection Jobs, on page 66](#)
- [Troubleshoot Crosswork Data Gateway, on page 108](#)

## Overview of Cisco Crosswork Data Gateway

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

---

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

---

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

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

Crosswork Data Gateway uses the following concepts:

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

**Attention**

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

- **Crosswork Data Gateway Pool:** A logical unit of one or more Crosswork Data Gateway instances with an option to enable high availability. When a Crosswork Data Gateway instance goes down, Cisco Crosswork automatically replaces the instance with a spare instance from the pool to ensure that data collections have minimal disruption.
- **Crosswork Data Gateway:** A Crosswork Data Gateway instance that is assigned a virtual IP address when it is added to a Crosswork Data Gateway pool.  
Operations such as attaching or detaching devices, creating collection jobs happen on the Crosswork Data Gateway.
- **Data Destination:** Internal or external recipients of data collected by the Crosswork Data Gateway. By default, Cisco Crosswork is defined as a data destination. Other destinations (external users) can be defined using the Cisco Crosswork UI or APIs.
- **Collection Job:** A task that Crosswork Data Gateway has to complete to collect data. Crosswork applications create collection jobs to check device reachability, collect telemetry data needed to determine network and service health. The Cisco Crosswork UI and API allow you to configure collection jobs for non-Crosswork applications.
- **Custom Software Packages:** Files and device model definitions to extend device coverage and support data collection from currently unsupported devices.

**Note**

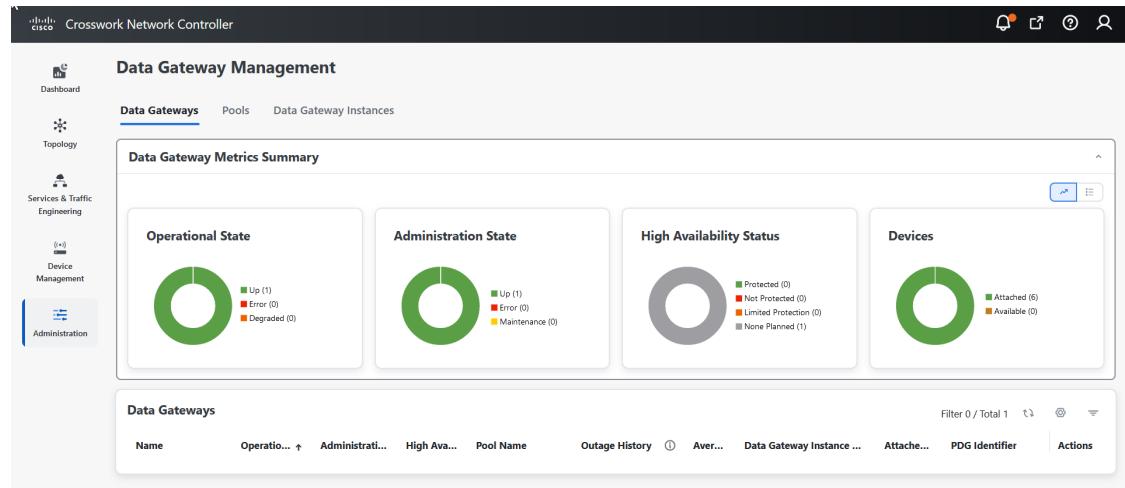
This chapter explains only the Cisco Crosswork Data Gateway features that can be accessed via Cisco Crosswork UI.

For more information about the Interactive Console of the Cisco Crosswork Data Gateway instance and how to manage it, see [Appendix A: Configure Crosswork Data Gateway Instance, on page 419](#).

### Crosswork Data Gateway UI Overview

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

Figure 14: Data Gateway Management Window



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

- **Data Gateways:** Displays details of the virtual Cisco Crosswork Data Gateways in the network. You can attach or detach devices to the Data Gateway from this tab.
- **Pools:** Manages Cisco Crosswork Data Gateway pools.
- **Data Gateways Instances:** Manages virtual Cisco Crosswork Data Gateway instances.

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

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

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

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

Table 2: Cisco Crosswork Data Gateway UI

Column	Description
<b>Operational State</b>	<p>Operational state of the Cisco Crosswork Data Gateway instance. A Crosswork Data Gateway instance has the following operational states:</p> <ul style="list-style-type: none"> <li>•  <b>Degraded:</b> The Cisco Crosswork Data Gateway instance is reachable but one or more of its components are in a state other than OK.</li> <li>•  <b>Up:</b> The Cisco Crosswork Data Gateway instance is operational and all individual components are "OK".</li> <li>•  <b>Error:</b> The Cisco Crosswork Data Gateway instance is unreachable or some of its components are in Error state.</li> </ul>
<b>Administration State</b>	<p>Administration state of the Cisco Crosswork Data Gateway instance. The state could be any of the following:</p> <ul style="list-style-type: none"> <li>•  <b>Up:</b> The instance is administratively up.</li> <li>•  <b>Maintenance:</b> Operations between Cisco Crosswork and the Cisco Crosswork Data Gateway are suspended to perform upgrades or other maintenance activities (for example, uploading certificates).</li> </ul>
<b>High Availability Status</b>	<p>High availability status of a Crosswork Data Gateway could be either:</p> <ul style="list-style-type: none"> <li>• <b>Protected:</b> All instances are UP and there is at least one standby available in the pool.</li> <li>• <b>Not Protected:</b> All standby instances are DOWN.</li> <li>• <b>Limited Protection:</b> Some standby instances are DOWN, but there is still at least one standby that is UP.</li> <li>• <b>None Planned:</b> No standby instances were added to the pool during pool creation.</li> </ul>
<b>Devices</b>	Number of devices attached to the Cisco Crosswork Data Gateway pool.

Column	Description
<b>Name</b>	<p>Name of the Cisco Crosswork Data Gateway instance.</p> <p>Clicking the  icon next to the name displays the enrollment details of each instance. This includes details such as, the:</p> <ul style="list-style-type: none"> <li>• Virtual IP Addresses</li> <li>• Data Gateway Instance Name</li> <li>• Description</li> <li>• Data Gateway Instance Type that indicates the profile of the Crosswork Data Gateway.</li> <li>• Data Gateway Instance UUID</li> </ul> <p>Click the instance name to open the Crosswork Data Gateway vitals page. The page displays the operations and health summary of a Crosswork Data Gateway.</p>
<b>Pool Name</b>	Name of the Crosswork Data Gateway pool. On clicking the pool name, the Crosswork Data Gateway vitals page opens.
<b>Site Name</b>	Site to which the data gateway instance is assigned. <p><b>Note</b></p> <p>This column is only displayed with the Geo Redundancy feature is enabled.</p> <p>For information on the Geo Redundancy capabilities, see the <i>Enable Geo Redundancy</i> section in <a href="#">Cisco Crosswork Network Controller 6.0 Installation Guide</a>.</p>
<b>Data Gateway Instance Role</b>	Indicates the current role of the data gateway instance. The role could be any of the following: <ul style="list-style-type: none"> <li>• <b>Assigned</b>: The data gateway instance is attached to a pool.</li> <li>• <b>Unassigned</b>: The data gateway instance is not attached to any pool.</li> <li>• <b>Spare (Active)</b>: The data gateway instance is a spare instance that can be used during a failover process in an active site.</li> <li>• <b>Spare (Standby)</b>: The data gateway instance acts as a spare instance for failover procedures in a standby site.</li> </ul>

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

Column	Description
<b>Data Gateway Instance Name</b>	<p>Name of the Cisco Crosswork Data Gateway that is created automatically when you add a Crosswork Data Gateway instance to a pool.</p> <p>Clicking the  icon next to the instance name displays the enrollment details of each instance. This includes details such as, the:</p> <ul style="list-style-type: none"> <li>• Data Gateway Instance Name</li> <li>• Description</li> <li>• Data Gateway Instance Type</li> <li>• Data Gateway Instance Role</li> <li>• CPU</li> <li>• Memory</li> <li>• Number of NICs</li> <li>• Data Gateway Instance UUID</li> <li>• Version</li> <li>• Data Gateway Instance OS</li> <li>• Interface Name</li> <li>• Interface Role(s)</li> <li>• Interface Mac</li> <li>• Interface Name</li> </ul> <p>The <b>Additional Interface Role Information</b> describes the interface roles available in Crosswork Data Gateway.</p>
<b>Attached Device Count</b>	<p>Indicates the number of the devices that are attached to the Crosswork Data Gateway pool.</p>
<b>PDG Identifier</b>	<p>Unique identifier of the physical data gateway instance.</p>
<b>Actions</b>	<p>Click  to view the actions that you can perform on the pool:</p> <ul style="list-style-type: none"> <li>• Attach Devices. For more information, see <a href="#">Attach Devices to a Crosswork Data Gateway, on page 39</a>.</li> <li>• Detach Devices. For more information, see <a href="#">Manage Cisco Crosswork Data Gateway Device Assignments, on page 46</a>.</li> <li>• Move Devices. For more information, see <a href="#">Manage Cisco Crosswork Data Gateway Device Assignments, on page 46</a>.</li> <li>• Initiate Failover. For more information, see <a href="#">Perform a Manual Failover, on page 38</a>.</li> </ul>

You can configure the Crosswork Data Gateway dashlet in the **Crosswork Home** page > **Dashboard**. The dashboard allows you to customize the dashlet to display the summary of the Crosswork Data Gateway instances and pools. For information on using Dashboard, see [Overview of the Topology Map, on page 131](#).

## Set Up Crosswork Data Gateway to Collect Data

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



**Note** This workflow assumes that you have already installed Cisco Crosswork Data Gateway as explained in [Cisco Crosswork Network Controller 6.0 Installation Guide](#).

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

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

**Table 3: Tasks to Complete to Set Up Cisco Crosswork Data Gateway to Collect Data**

Task	Follow the steps in...
1. Create Crosswork Data Gateway pools.	<a href="#">Create a Cisco Crosswork Data Gateway Pool, on page 34</a>
2. Attach devices to Crosswork Data Gateway.	<a href="#">Attach Devices to a Crosswork Data Gateway, on page 39</a>
3. Verify that the default collection jobs are created and running successfully.	<a href="#">Monitor Collection Jobs, on page 104</a>
4. (optional) Extend device coverage to collect data from currently unsupported devices or third-party devices.	<a href="#">Manage Device Packages, on page 59</a>
5. (optional) Forward data to external data destinations.	<a href="#">Create and Manage External Data Destinations, on page 52</a>
6. (optional) Create custom collection jobs (outside of those built for you by Cisco Crosswork).	<a href="#">Manage Crosswork Data Gateway Collection Jobs, on page 66</a>

## Crosswork Data Gateway High Availability with Pools

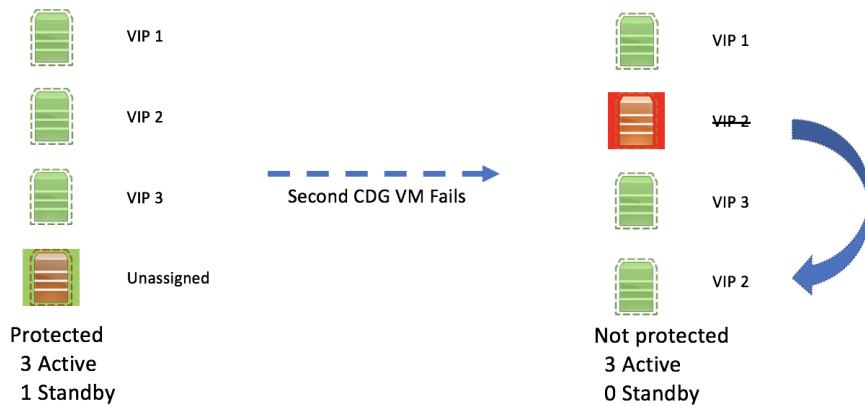
A Cisco Crosswork Data Gateway pool ensures that your device-specific data collection occurs with minimal disruption.

A pool can consist of one or more Cisco Crosswork Data Gateway instances with an option to enable high availability.

If a Crosswork Data Gateway instance in the pool goes down, Cisco Crosswork automatically replaces that instance with a standby instance from the pool (failover) or lets you manually initiate a failover. For information on how to initiate a failover, see [Perform a Manual Failover, on page 38](#).

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

**Figure 15: Crosswork Data Gateway High Availability**



**Note** If more than one Crosswork Data Gateway instance in a pool has same Southbound IP address, reboot the standby Crosswork Data Gateway, so that the standby Crosswork Data Gateway instance loses its southbound IP address once it comes up.

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

A Crosswork Data Gateway pool has following states:

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

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

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

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

## Create a Cisco Crosswork Data Gateway Pool

When you create a Cisco Crosswork Data Gateway pool, follow these guidelines:

- You must create at least one pool and assign Crosswork Data Gateway instances to it. This step is mandatory to set up the Crosswork Data Gateway for collection.
- All the Crosswork Data Gateway instances in a pool need to be of the same configuration (either Standard, or Extended).
- If you have deployed the VMs on Amazon EC2, all the Crosswork Data Gateway instances in a pool must be from the same availability zone.

To create a Crosswork Data Gateway pool:

### Before you begin

Before creating a Crosswork Data Gateway pool:

- Decide if you wish to enable high availability for the pool.
- Ensure that you have installed all Crosswork Data Gateway instances that you wish to add to the pool.
- The number of Crosswork Data Gateway instances you add to the pool should be equal to the total number of virtual IPs and standby Crosswork Data Gateway instances. For example, if you have entered 3 virtual IPs and wish to have 2 standby instances, add 5 Cisco Crosswork Data Gateway instances to the pool.
- Ensure that you are familiar with the pool types:
  - **VIP-based:** A pool where network devices connect to Crosswork Data Gateway instances within a high-availability pool on a single IP subnet. The subnet can be intra-DC (Data Center) or inter-DC extended.
  - **FQDN-based:** A pool where network devices connect to Crosswork Data Gateway instances located in multiple subnets within the same HA pool. To create a pool based on the FQDN, an external Network Load Balancer (NLB) must host a VIP that directs traffic towards the network devices, thus safeguarding the internal subnet addresses of the Crosswork Data Gateway HA pool.



### Note

The **FQDN-based** pool type is supported only when you are creating a pool in the Amazon EC2 environment.

- Confirm that the Operational State of the Crosswork Data Gateway instances is **Not Ready**.

- Have network information such as virtual IP address (one virtual IP for each active data gateway), subnet mask and gateway information ready.



**Note** Gateway is only required when using 3 NICs.

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

- An additional IP address on the Management Network in a single NIC deployment.
- An additional IP address on the Data Network for 2 NIC deployment.
- An IP address on the Southbound Network for 3 NICs deployment.

These virtual IP addresses must be planned during the network design phase.

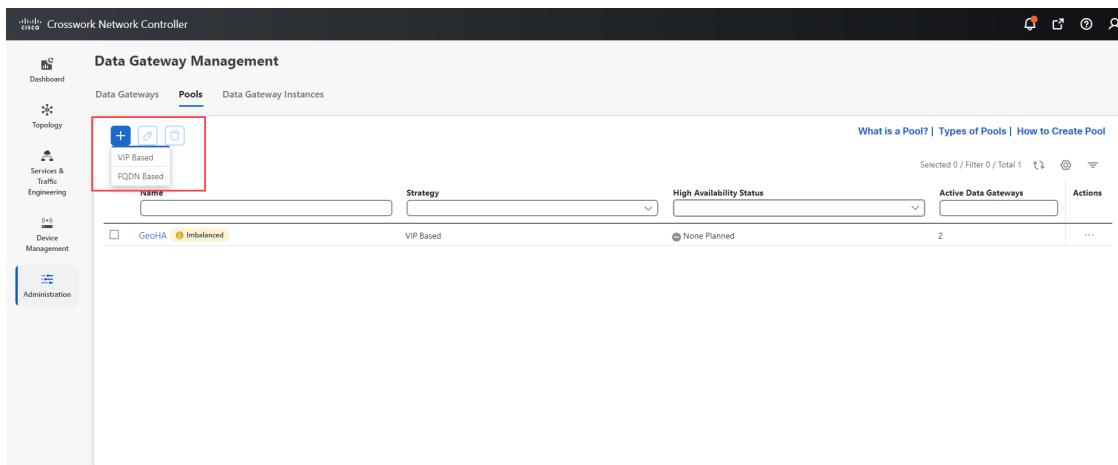
- Decide if you wish to enable Fully Qualified Domain Name (FQDN) for virtual IP(s) addresses in the pool. If yes, ensure that you have configured FQDN for virtual IP(s) in the DNS server to create the pool successfully.

## Procedure

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

**Step 2** In the **Pools** tab, click the **+** button and select **VIP Based** or **FQDN Based**. For information on the pool types, on the top-right, click **Types of Pools**.

*Figure 16: Pools Window*



The **Create Pool** page opens.

**Step 3** In the **Global Pool Parameters** pane, enter the values for the following parameters:

- **Pool Name:** Name of the pool that suitably describes the network.
- **Description:** A description of the pool.

## Create a Cisco Crosswork Data Gateway Pool

- **The Number of Standby Data Gateways:** Number of data gateways that operate as the standby instances. When an active data gateway is unavailable, the spare gateway assumes the role of the active gateway.

Depending on the selected pool type, certain fields may vary for VIP and FQDN.

### Step 4 If VIP-based pool is selected:

Under **Virtual IP Configuration**, select **Shared VIP** or **Site-Specific VIP**.

Depending on your selection, you have to enter the following:

#### Shared VIP:

- **Virtual IP Type:** Select either an IPv4 or IPv6 address family for virtual IPs.
- **Subnet:** Subnet mask for each Cisco Crosswork Data Gateway. IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535.
- **Network Gateway:** Data Gateway address for each Cisco Crosswork Data Gateway to communicate with the devices.

#### Site-Specific VIP:

- **Virtual IP Type:** Select either an IPv4 or IPv6 address family for virtual IPs.

### If FQDN-based pool is selected:

Under **FQDN Configuration**, select **Shared FQDN** or **Site-Specific FQDN**.

### Step 5

(Optional) **Enable FQDN based device configuration Virtual IP address:** Select this option to use hostname or Fully Qualified Domain Name (FQDN) for each virtual IP address of the Crosswork Data Gateway in the syslog certificate.

### Step 6

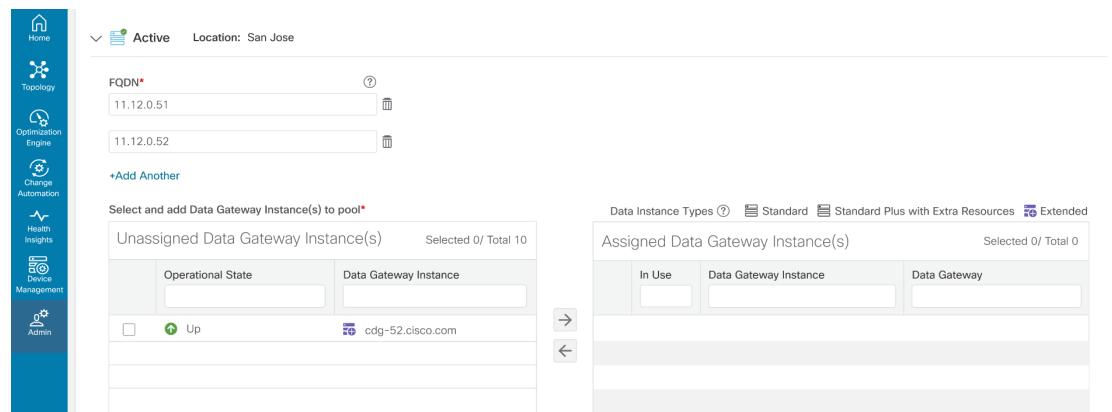
**Add Virtual IP Address or FQDN:** Based on the address family you chose earlier (IPv4 or IPv6, FQDN), enter a virtual IP address or FQDN for every active Cisco Crosswork Data Gateway instance.

### Step 7

In the **Active** pane, select the Data Gateway instances from **Unassigned Data Gateway Instance(s)** on the left and click right arrow to move the instances to **Data Gateway Instance(s) Added to Pool**.

For FQDN-based pools, enter an FQDN for every active Cisco Crosswork Data Gateway instance. For including additional FQDN addresses, click **Add Another**.

**Figure 17: Active Pane for FQDN-based Pools**

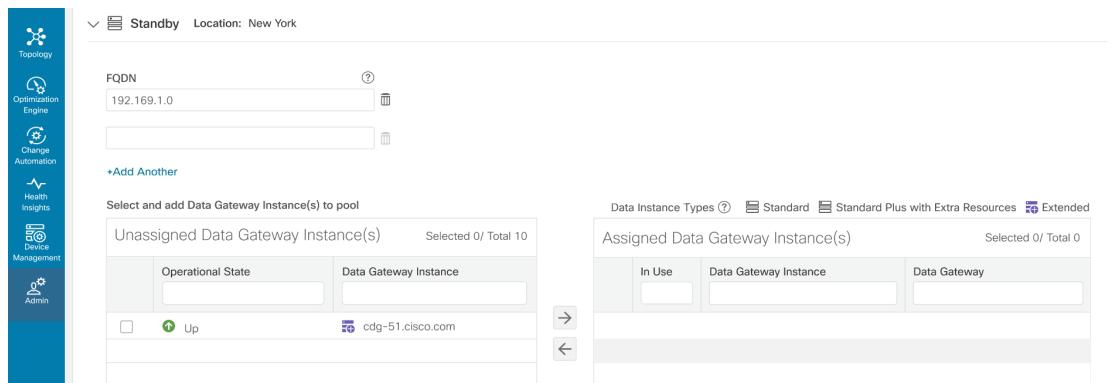


### Step 8

In the **Standby** pane, select the Data Gateway instances from **Unassigned Data Gateway Instance(s)** on the left and click right arrow to move the instances to **Data Gateway Instance(s) Added to Pool**.

With FQDN-based pools, provide an FQDN for every active instance of the Cisco Crosswork Data Gateway. To add more FQDN addresses, click **Add Another**.

**Figure 18: Standby Pane for FQDN-based Pools**



### Step 9 Click Save.

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

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



**Note** Pool creation fails if the FQDN configurations are missing for virtual IP(s) in the DNS server. Either check FQDN configuration in the DNS server or disable the FQDN option and try again.

## Assign Data Gateway to Geo Redundancy-enabled Sites

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

### Before you begin

Ensure that you are aware of the following:

- The data gateway instances can be assigned to sites only with the Geo Redundancy feature is enabled. For information on how to enabled the Geo Redundancy capabilities, see the *Enable Geo Redundancy* section in [Cisco Crosswork Network Controller 6.0 Installation Guide](#).
- When the data gateways are in the unassigned state, you have the option to assign them to either an Active or Standby site.
- If the data gateway is a member of a pool, you can assign it to a site only during Crosswork migration using the edit pool option. During the Crosswork migration, a notification is shown on the **Data Gateway Management** page, to indicate the ongoing migration.

## Perform a Manual Failover

### Procedure

- 
- Step 1** From the main menu, choose **Administration > Data Gateway Management** and click the **Data Gateway Instances** tab.
- Step 2** Click **Assign DG Instance to Site**. The **Assign Data Gateway Instance(s) to Site** window opens. The window displays the data gateway instances in the unassigned state.
- Step 3** Select the data gateway instance that you want to change the assigned site.
- Step 4** Click the **Select Site** drop-down and select the site.
- Step 5** Click **Assign**.

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

---

## Perform a Manual Failover

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

### Before you begin

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

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

Follow the steps below to initiate a manual failover of the Crosswork Data Gateway instance:

### Procedure

- 
- Step 1** From the main menu, choose **Administration > Data Gateway Management > Data Gateways** tab.
- Step 2** For the Crosswork Data Gateway from which you want to initiate a failover, under **Actions** column, click, and select **Initiate Failover**.
- Step 3** In the **Warning** window, if you want to move the selected data gateway to the maintenance mode after the failover is complete, select the check box.

**Step 4** Click **Continue**.**What to do next**

If the failover is not complete due to database connectivity or OAM channel issues, reattempt the failover after confirming you have at least standby instance in the **NOT\_READY** state.

Before initiating a subsequent failover, wait for 10-30 seconds for the standby data gateway to move to the **NOT\_READY** state. If the standby instance remains in the **UP** state after 30 seconds, restart the **oam-manager** of the data gateway to restore the operational state as **NOT\_READY**.

## Attach Devices to a Crosswork Data Gateway

Follow these guidelines when you attach devices to a Crosswork Data Gateway.

- The Crosswork Network Controller allows the connection of a device to only one Crosswork Data Gateway at a time.
- For optimal performance, we recommend attaching devices to a Crosswork Data Gateway in batches of 300 devices or fewer.

**Before you begin**

Take a note of the following:

- Ensure that the **Admin state** and **Operational state** of the Crosswork Data Gateway to which you want to attach devices is **Up**.
- Crosswork Data Gateway does not support the usage of older insecure key exchange algorithms (KEX), as it can result in SSH connection failure.

**Procedure**

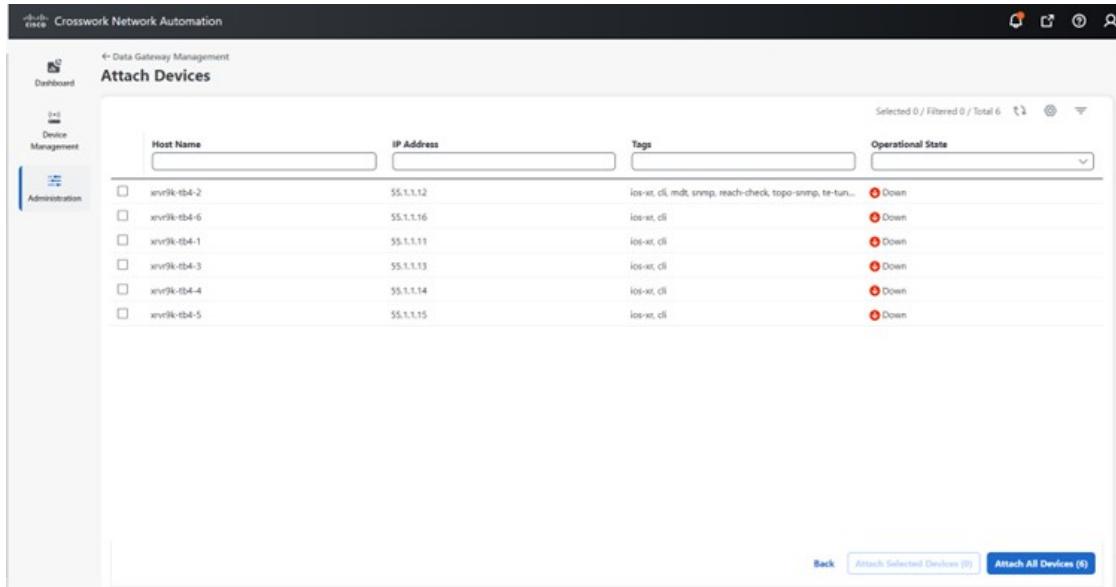
**Step 1** (Optional) Before attaching devices to an existing Crosswork Data Gateway, we recommend that you check the health of the Crosswork Data Gateway. See [Monitor Crosswork Data Gateway Health](#), on page 40 for more information.

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

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

## Manage Crosswork Data Gateway Post-Setup

**Figure 19: Attach Devices Window**



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

**Step 5** In **Confirm - Attach Devices** dialog, click **Attach**.

Verify that your changes are successful by checking the **Attached Device Count** column in the **Data Gateways** pane.

Monitor the Crosswork Data Gateway health to ensure that the Crosswork Data Gateway is functioning well with the newly attached devices. For information on how to monitor the health, see [Monitor Crosswork Data Gateway Health, on page 40](#).

# Manage Crosswork Data Gateway Post-Setup

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

- Monitor Crosswork Data Gateway Health, on page 40
  - Crosswork Data Gateway High Availability with Pools, on page 32
  - Manage Cisco Crosswork Data Gateway Device Assignments, on page 46
  - Maintain Crosswork Data Gateway Instances, on page 48

# Monitor Crosswork Data Gateway Health

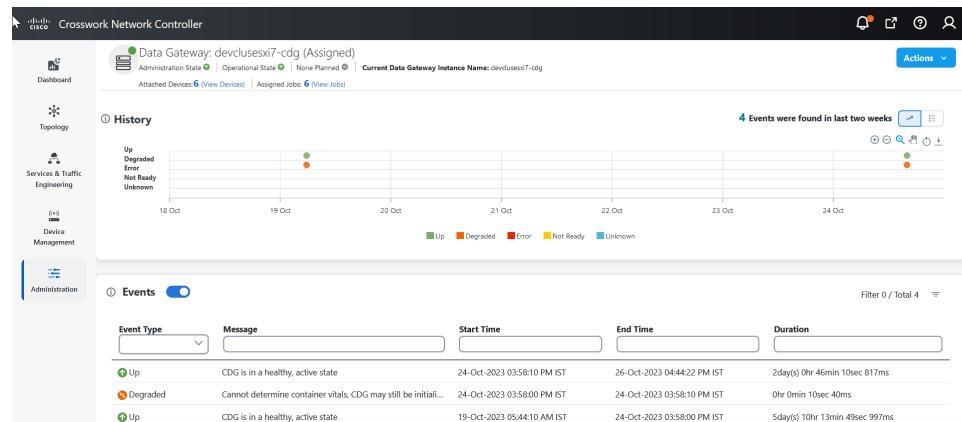
You can view the operations and health summary of a Crosswork Data Gateway from the Crosswork Data Gateway vitals page at **Administration > Data Gateway Management > Data Gateways > (click){Crosswork Data Gateway}**. This page also has details of the health of various containerized services

running on the Crosswork Data Gateway. The overall health of Crosswork Data Gateway also depends on the health of each containerized service.

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

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

**Figure 20: Data Gateway Window**



The following parameters are displayed on this page:

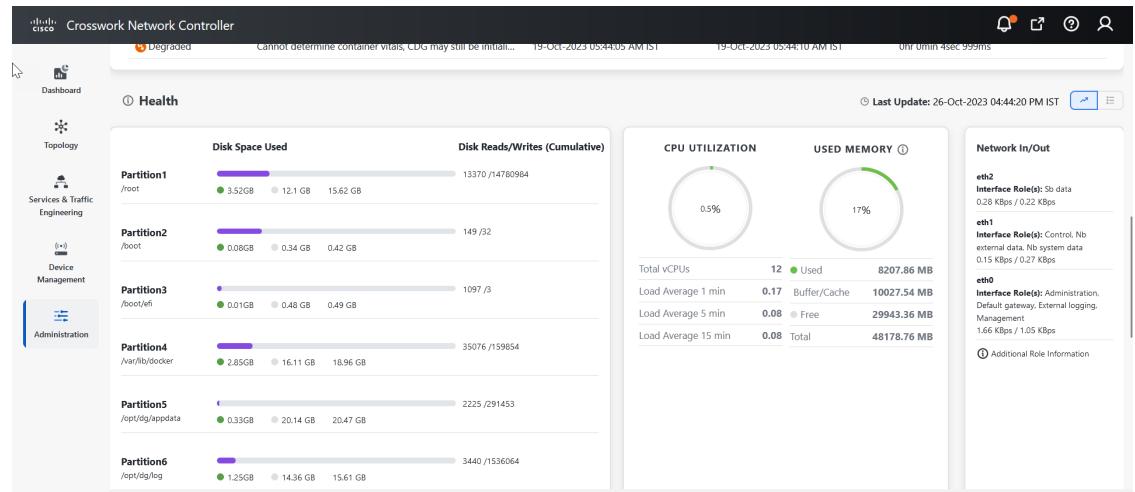
- **General Cisco Crosswork Data Gateway Details** – Displays general details of the Crosswork Data Gateway including operational state, high availability state, attached device count, and assigned jobs. The **Actions** option lists the various troubleshooting options that are available from the UI.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

## Monitor Crosswork Data Gateway Health

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

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

**Figure 21: Crosswork Data Gateway Health Window**



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



**Note**

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

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

Figure 22: Service Status Window

We recommend monitoring the health of the Crosswork Data Gateways in your network periodically to prevent overloading and take corrective actions, such as adding additional resources or reducing load on the Crosswork Data Gateway well in time proactively.

1. The DG-Manager generates alarms when Crosswork Data Gateway fails or is reaching the resource capacity limits. You can review the alarm details through **Crosswork UI > Showtech Requests** or by logging in to the Alarm pods. The alarms include the event title, severity, the configuration stage (Day 0, 1, or 2), description, and the remediation action. For more information on how to navigate to the **Showtech Requests** window, see [Viewing Crosswork Data Gateway Alarms, on page 43](#).
2. If the **CPU Utilization** of a Crosswork Data Gateway exceeds 80%, we recommend that you do not create more collection jobs until you have reduced the **CPU Utilization** by moving devices to another CDG or have added other VMs to the pool or the increased the cadence of existing collection jobs.
3. If the **CPU Utilization** of a Crosswork Data Gateway exceeds 90%, we recommend that you move devices to another Crosswork Data Gateway that has a lower **CPU Utilization** percentage.
4. We recommend that you check the system alarms weekly. Investigate to confirm it is not because of a resource problem and data drops are not frequent. Then fix issues on the data destinations or increase cadence of the collection job.

## Viewing Crosswork Data Gateway Alarms

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

To view the alarms, navigate to the Crosswork UI:



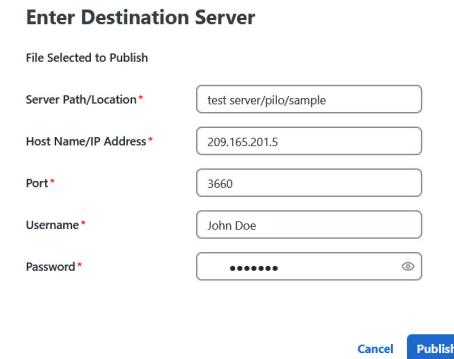
**Note**

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

## Procedure

- Step 1** From the main menu, choose **Administration > Crosswork Manager > Application Management** tab and click **Applications**.
- Step 2** In the **Platform Infrastructure** tile, click **View Details**. The **Application Details** window opens.
- Step 3** In the **Microservices** tab, type alarms in the **Name** field to locate the alarm pod. The status of the alarm pod must be healthy.
- Step 4** Click the  icon under **Actions** and select **Showtech Requests**. The **Showtech Requests** window displays the details of the showtech jobs.
- Step 5** (Optional) Log in to the alarm pod and view the alarms or download the alarms by clicking **Publish** to publish the showtech logs. The **Enter Destination Server** dialog box is displayed. Enter the relevant details and click **Publish**.

*Figure 23: Showtech Requests Window*



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

## Manage a Crosswork Data Gateway Pool

Follow the steps to edit or delete a Cisco Crosswork Data Gateway pool. To create a pool, see [Create a Cisco Crosswork Data Gateway Pool, on page 34](#).

### Before you begin

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

- Virtual data gateways or pools that have devices attached cannot be deleted.
- A data gateway instance can be removed from the pool only when all the mapped devices are unmapped from Crosswork Data Gateway. When a Crosswork Data Gateway instance is removed from the pool, a standby instance from the same pool becomes its replacement after you perform a failover procedure. For information about manual failovers, see [Perform a Manual Failover, on page 38](#).

- Before you delete a Crosswork Data Gateway pool, detach devices from the Crosswork Data Gateway first or move the devices to another Crosswork Data Gateway.

## Procedure

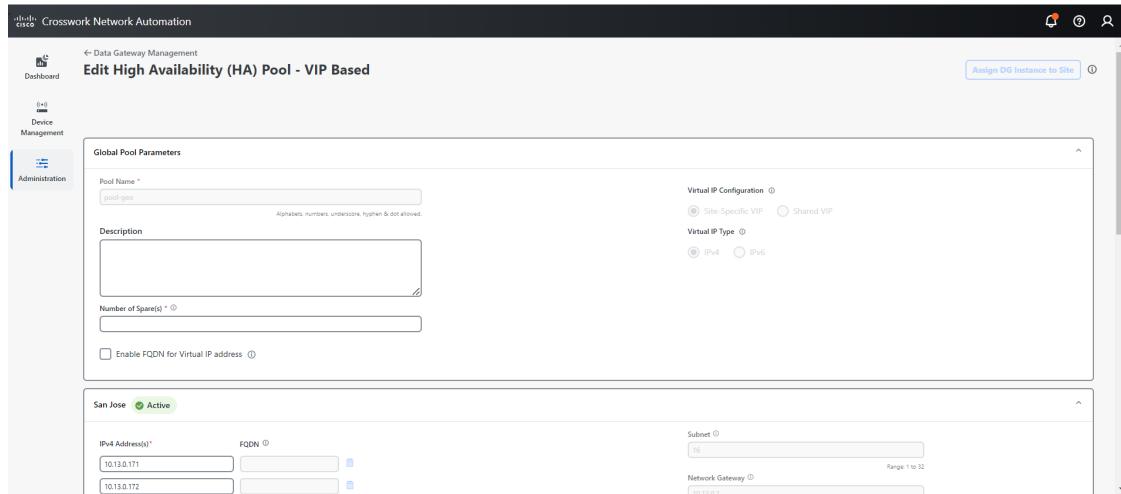
**Step 1** From the main menu, choose **Administration > Data Gateway Management** and click **Pools** tab.

**Step 2 Edit a Crosswork Data Gateway Pool:**

- Select the pool which you wish to edit from the list of pools that is displayed in this page.
- Click  button to open **Edit High Availability (HA) Pool** page.

When you edit a resource pool, you can only change some of the parameters in the **Global Pool Parameters** pane. To make changes to the rest of the parameters in the **Global Pool Parameters** pane, create a new pool with the desired values and move the Cisco Crosswork Data Gateway instances to that pool.

**Figure 24: Data Gateway Management - Edit HA Pool Window**



- In the **Pool Resources** pane, you can modify the resource parameters that change depending on the pool type:
  - Add a virtual IP address or FQDN for every active data gateway needed.
  - Change the number of standby Crosswork Data Gateway instances.
  - Add and remove Crosswork Data Gateway instances from the pool.
  - Enable or disable FQDN for the pool.
- In the **Active** and **Standby** site parameters pane, you can modify the IP or FQDN addresses of the Crosswork Data Gateway VM. The Active and Standby panes are visible only when the Geo Redundancy feature is enabled. For information on the Geo Redundancy capabilities, see the *Enable Geo Redundancy* section in [Cisco Crosswork Network Controller 6.0 Installation Guide](#).
- Click **Save** after you have completed making your changes.

**Step 3 Delete a Crosswork Data Gateway Pool:**

- Select the pool that you want to delete and click .

## Manage Cisco Crosswork Data Gateway Device Assignments

- b) Click **Delete** in the **Delete High Availability (HA) Pool** window to delete the pool.

# Manage Cisco Crosswork Data Gateway Device Assignments

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

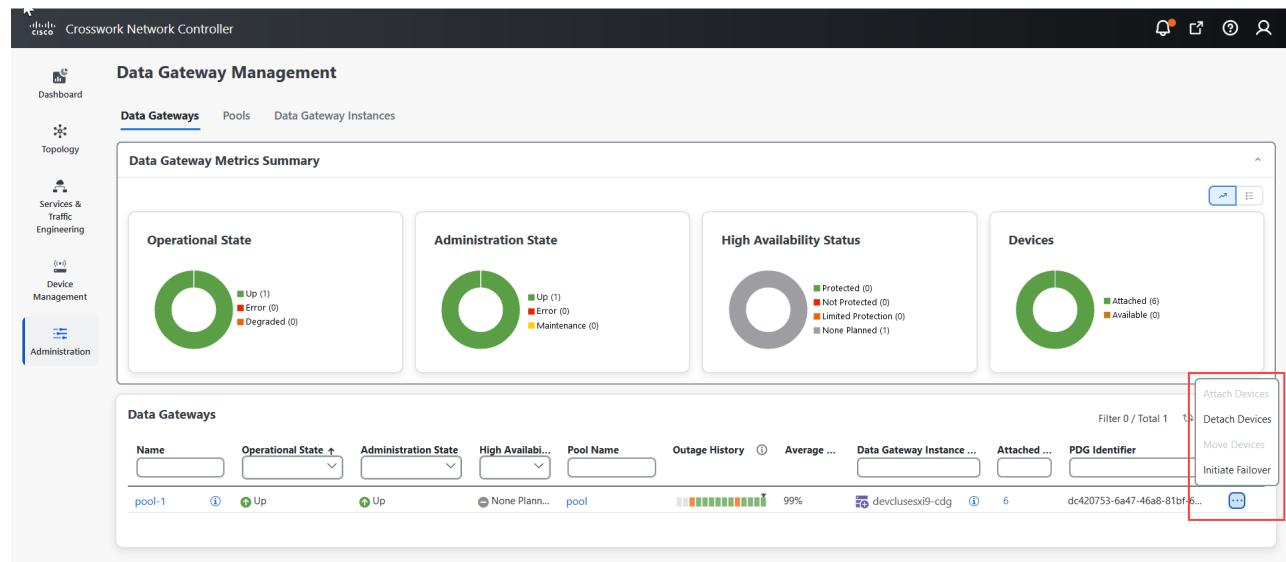
- A device can be attached to only one Crosswork Data Gateway.
- When moving devices to a Crosswork Data Gateway in different pool, ensure that the Gateway of the pool is same as the Gateway of the current pool. Moving devices to a Crosswork Data Gateway with mismatching Gateway results in failed collections.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

Follow the steps below to move or detach devices from a Crosswork Data Gateway pool. To add devices to the pool, see [Attach Devices to a Crosswork Data Gateway, on page 39](#).

## Procedure

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

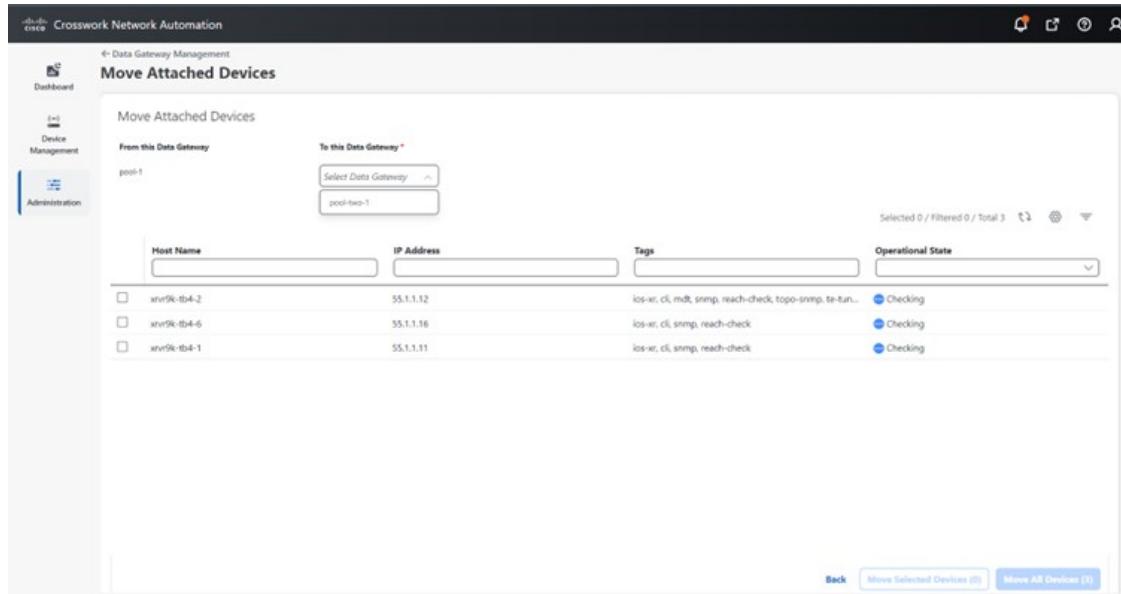
*Figure 25: Data Gateways Window*



- Step 2 Move Devices:**

- For the Crosswork Data Gateway from which you want to move devices, under the **Actions** column, click and select **Move Devices**. The **Move Attached Devices** window opens showing all the devices available for moving.
- From the **To this Data Gateway** drop down, select the data gateway to which you want to move the devices.

Figure 26: Move Attached Devices Window



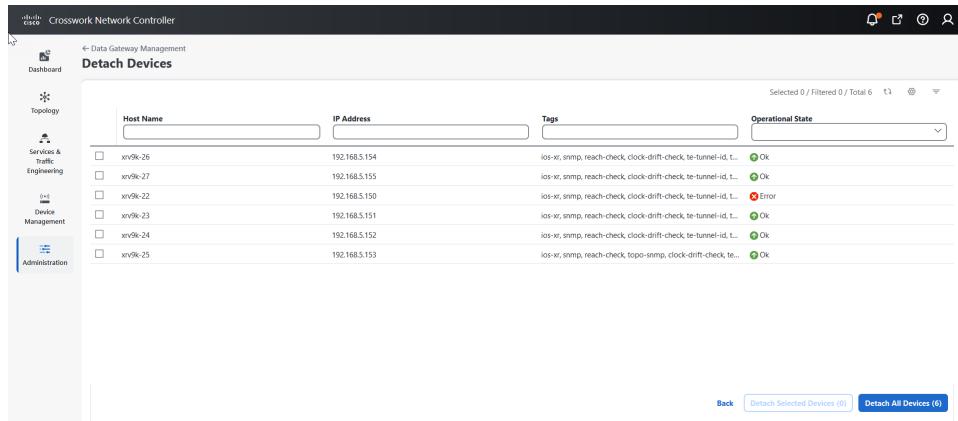
- c) To move all the devices, click **Move All Devices**. Otherwise, select the devices you want to move and click **Move Selected Devices**.
- d) In the **Confirm - Move Devices** window, click **Move**.

### Step 3

#### Detach Devices:

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

Figure 27: Detach Devices Window



- b) To detach all the devices, click **Detach All Devices**. Otherwise, select the devices you want to detach and click **Detach**.
- c) In the **Confirm - Detach Devices** window, click **Detach**.

## Maintain Crosswork Data Gateway Instances

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

For information on how initiate a failover, see [Perform a Manual Failover, on page 38](#).

# Maintain Crosswork Data Gateway Instances

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

- [Change the Administration State of Cisco Crosswork Data Gateway Instance, on page 48](#)
- [Delete Crosswork Data Gateway Instance from Cisco Crosswork, on page 49](#)
- [Redeploy a Crosswork Data Gateway Instance, on page 51](#)

## Change the Administration State of Cisco Crosswork Data Gateway Instance

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, the administrator can modify Cisco Crosswork Data Gateway, such as updating the certificates, and so on.



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

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



**Note** In the **Assigned** state, a data gateway cannot be switched directly to the maintenance mode. To enter the maintenance mode, you must either execute a manual failover when standby is available or remove the data gateway from the pool. See [Perform a Manual Failover, on page 38](#) for information on manual failover.

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

### Before you begin

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

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

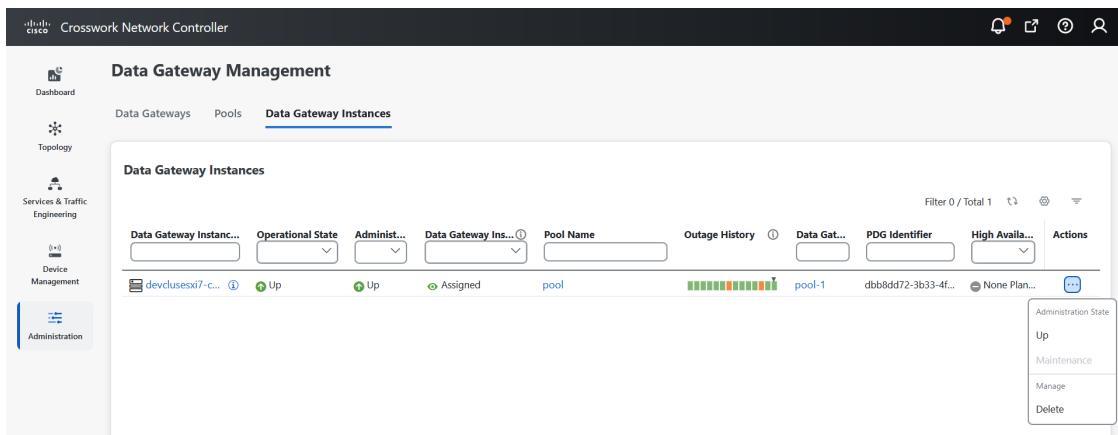
## Procedure

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

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

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

**Figure 28: Data Gateway Instances Window**



**Step 3** Select the administration state to which you want to switch to.

## Delete Crosswork Data Gateway Instance from Cisco Crosswork

Follow the steps below to delete a Cisco Crosswork Data Gateway instance 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 instance, then the corresponding jobs are deleted.

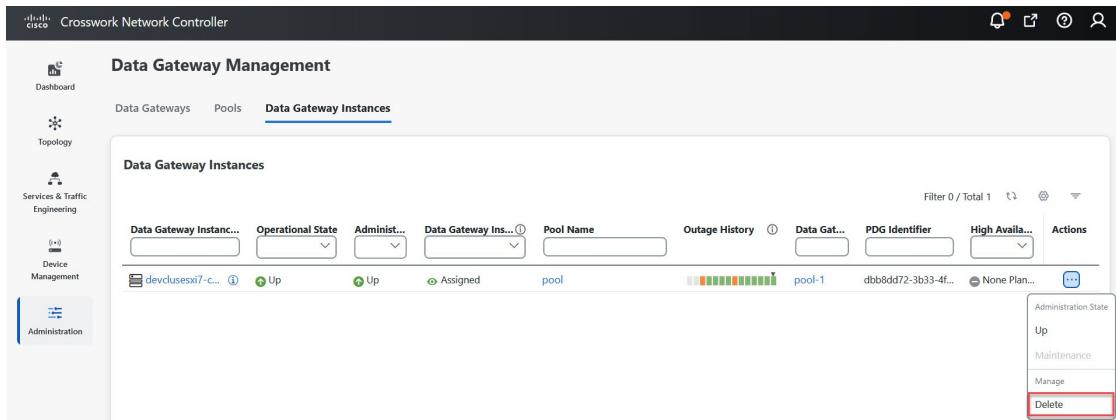
## Procedure

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

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

## Delete Crosswork Data Gateway Instance from Cisco Crosswork

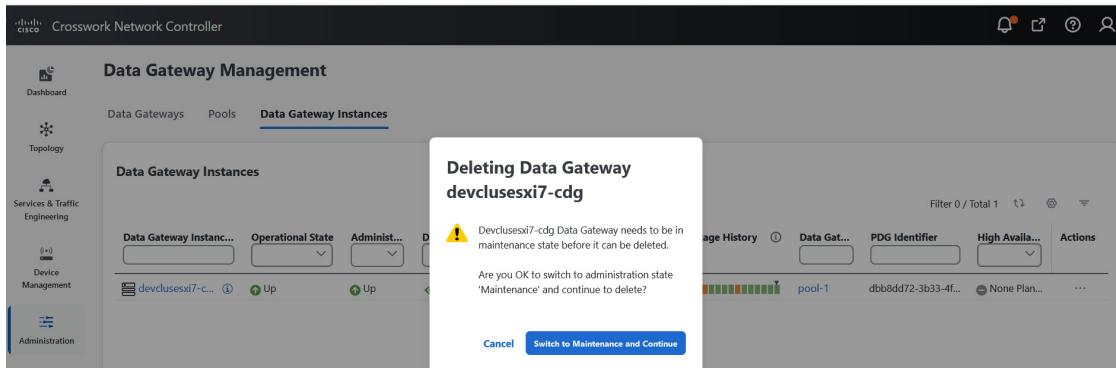
Figure 29: Data Gateway Instances Window



### Step 3

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

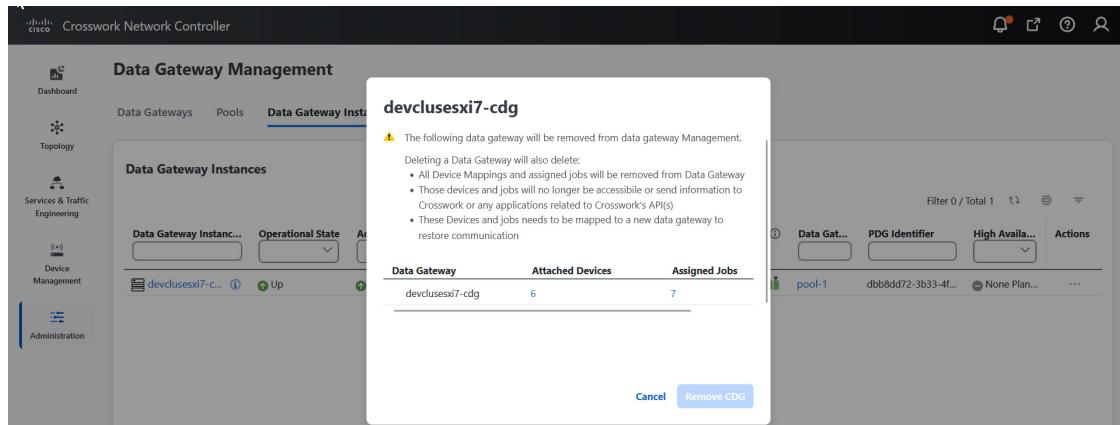
Figure 30: Switch to maintenance & continue Pop-up Window



### Step 4

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

Figure 31: Delete Data Gateway Confirmation Dialog Box



## Redeploy a Crosswork Data Gateway Instance

To redeploy a Crosswork Data Gateway instance, delete the old instance and install a new one. For details on how to install a new Crosswork Data Gateway instance, see [Cisco Crosswork Network Controller 6.0 Installation Guide](#).

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

### Important points to consider

1. If the Crosswork Data Gateway instance was already enrolled with Cisco Crosswork and you have installed the instance again with the same name, change the **Administration State** of the Crosswork Data Gateway instance to **Maintenance** for auto-enrollment to go through.
2. If a Crosswork Data Gateway instance was already enrolled with Cisco Crosswork and Cisco Crosswork was installed again, re-enroll the existing Crosswork Data Gateway instance with Cisco Crosswork.

See [Re-enroll Crosswork Data Gateway, on page 448](#).

## Configure Crosswork Data Gateway Global Settings

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

- [Manage Device Packages, on page 59](#)
- [Configure Crosswork Data Gateway Global Parameters, on page 61](#)
- [Allocate Crosswork Data Gateway Resources, on page 63](#)

# Create and Manage External Data Destinations

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

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

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



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

**Figure 32: Data Destinations Window**

Destination Name	Server Type	Compression Type	Encoding	UUID
Crosswork_Kafka	Kafka	snappy	gpbkv	c2a8fba8-8363-3d22-b0c2-a9e449693fae
cdg-astack-pipeline	gRPC	gzip	gpbkv	e9b4c2ec-b2e6-4db0-a942-0402dd347a1d
icon-server-grpc-destination	gRPC	gzip	gpbkv	155e716-93a1-49f9-9207-1239189b9113

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

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

## Licensing Requirements for External Collection Jobs

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

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

- **Registration Status - Registered**

Indicates that you have registered with Cisco Smart Software Manager (CSSM) and are authorized to use the reserved licensed features.

- **License Authorization Status - Authorized** (In Compliance).
 

Indicates that you have not exceeded the device count in the external collection jobs.
- Under Smart Licensing Usage, **CW\_EXTERNAL\_COLLECT** has status as **In Compliance**.

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

## Add or Edit a Data Destination

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

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

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

```
destinationContext: topiccmdt4
org.apache.kafka.common.errors.UnknownTopicOrPartitionException: This server does not
host this topic-partition.
```

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



**Note** This feature is not supported on a gRPC destination.

- Global properties entered in the **Destination Details** pane are mandatory and will be applied to the Kafka destination by default unless there are custom values specified at the individual collector level. Custom values that you specify for a collector apply only to that collector.

- The external destination must be IPv4 or IPv6 depending on the protocol specified when deploying Crosswork Data Gateway. For instance, if IPv4 was chosen during the deployment, the external destination should also be IPv4.
- Modifications to the hostname and IP address mapping reflect on Crosswork Data Gateway only after the duration configured in the Time to Live (TTL) field on the DNS server is completed. If you want the change to reflect immediately, we recommend rebooting the VM.

### Before you begin

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

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



**Note**

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

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

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

### Procedure

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

**Step 2** In the **Data Destinations** page, click  button. The **Add Destination** page opens.

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

**Note**

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

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

Field	Value	Available in gRPC	Available in Kafka
<b>Destination Name</b>	Enter a descriptive data destination name. The name can contain a maximum of 128 alphanumeric characters, plus underscores ("_") or hyphens ("-"). No other special characters are allowed.  If you have many data destinations, make the name as informative as possible to be able to distinguish later.	Yes	Yes
<b>Server Type</b>	From the drop-down, select the server type of your data destination.	Yes	Yes
<b>Encoding</b>	From the drop-down, select the encoding (json or gpbkv).	Yes	Yes
<b>Compression Type</b>	From the drop-down, select the compression type.	Yes  Supported compression types are Snappy, gzip, lz4, zstd, and none.  <b>Note</b> zstd compression type is supported only for Kafka 2.0 or higher.	Yes  Supported compression types are Snappy, gzip, and deflate.
<b>Dispatch Type</b>	This field is available when the <b>Server Type</b> field is set to <b>gRPC</b> .  From the drop-down, select the dispatch method as stream or unary.  Crosswork Data Gateway transmits the collected data to the destination as data streams or unary. The default value is unary.	Yes	No
<b>Maximum Message Size (bytes)</b>	Enter the maximum message size in bytes. <ul style="list-style-type: none"><li>• <b>Default Value:</b> 100000000 bytes/ 30 MB</li><li>• <b>Min:</b> 1000000 bytes/1 MB</li><li>• <b>Max:</b> 100000000 bytes/ 30 MB</li></ul>	No	Yes
<b>Buffer Memory</b>	Enter the required buffer memory in bytes. <ul style="list-style-type: none"><li>• <b>Default Value:</b> 52428800 bytes</li><li>• <b>Min:</b> 52428800 bytes</li><li>• <b>Max:</b> 314572800 bytes</li></ul>	No	Yes

## Add or Edit a Data Destination

Field	Value	Available in gRPC	Available in Kafka
<b>Batch Size (bytes)</b>	Enter the required batch size in bytes. <ul style="list-style-type: none"> <li><b>Default Value:</b> 6400000 bytes/6.4 MB</li> <li><b>Min:</b> 16384 bytes/ 16.38 KB</li> <li><b>Max:</b> 6400000 bytes/6.4 MB</li> </ul>	No	Yes
<b>Linger (milliseconds)</b>	Enter the required linger time in milliseconds. <ul style="list-style-type: none"> <li><b>Default Value:</b> 5000 ms</li> <li><b>Min:</b> 0 ms</li> <li><b>Max:</b> 5000 ms</li> </ul>	No	Yes
<b>Request Timeout</b>	Enter the duration that the request waits for a response. After the configured duration is met, the request expires. <ul style="list-style-type: none"> <li><b>Default Value:</b> 30 ms</li> <li><b>Min:</b> 30 ms</li> <li><b>Max:</b> 60 ms</li> </ul>	Yes	Yes

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

**Step 4**

(Optional) To configure custom values that are different from global properties for a Kafka destination, in the **Customize Collector Settings** pane:

- Select a **Collector**.
- Enter values for the following fields:

- Custom Buffer Memory**

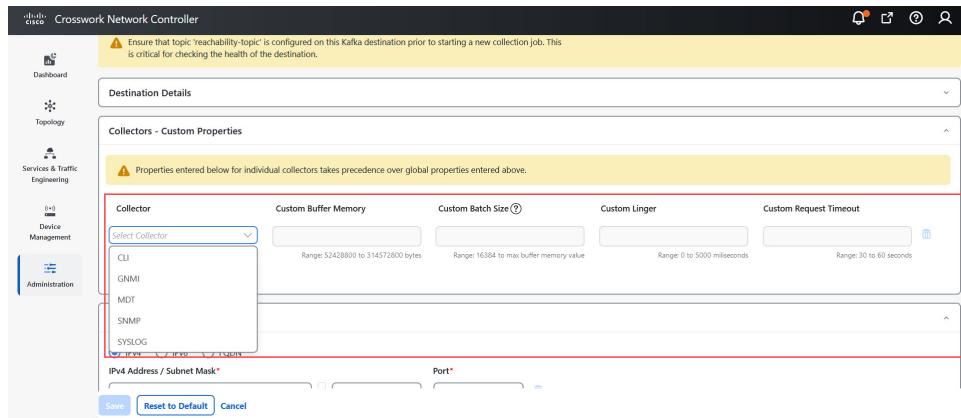
- Custom Batch Size**

**Note**

The **Custom Batch Size** cannot exceed the value of the **Custom Buffer Memory** at run time. In case, you do not provide a value in the **Custom Buffer Memory** field, the **Custom Batch Size** will be validated against the value in the **Buffer Memory** field.

- Custom Linger**
- Custom Request Timeout**

Figure 33: Add Destination Window



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

**Note**

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

**Step 5**

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

**Note**

The FQDN addresses are supported only for the Kafka destinations.

**Step 6**

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

Connectivity Type	Fields	Available in gRPC	Available in Kafka
<b>IPv4</b>	Enter the required <b>IPv4 Address/ Subnet Mask</b> , and <b>Port</b> . You can add multiple IPv4 addresses by clicking + <b>Add Another</b>  IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535.	Yes	Yes
<b>IPv6</b>	Enter the required <b>IPv6 Address/ Subnet Mask</b> , and <b>Port</b> . You can add multiple IPv6 addresses by clicking + <b>Add Another</b> .  IPv6 subnet mask ranges from 1 to 128 and port range from 1024 to 65535.	Yes	Yes
<b>FQDN</b>	Enter the required <b>Host Name, Domain Name</b> , and <b>Port</b> . The supported port range is from 1024 to 65535.  You can add multiple FQDN addresses by clicking + <b>Add Another</b> .	Yes	Yes

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

**Delete a Data Destination**

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

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

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

**Note**

The authentication options are available only when **Enable Secure Communication** is enabled.

**Step 9** Click **Save**.

**What to do next**

If you have enabled the **Enable Secure Communication** option, navigate to the **Certificate Management** page in the Cisco Crosswork UI (**Administration > Certificate Management**) and add the relevant certificate for the newly added data destination. This step is mandatory to establish a secure communication to the device. See [Manage Certificates, on page 321](#) for more information.



**Note** If you do not add the certificate or the certificate is incomplete for the data destination after enabling the **Enable Secure Communication** option, Cisco Crosswork sets the destination to an error state.

**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.

**Procedure**

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

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

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

# Manage Device Packages

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

The system device and MIB packages are bundled in the Crosswork software and are automatically downloaded to the system instances. You cannot modify the system device and MIB packages.

Custom device package extends device coverage and collection capabilities to third-party devices.

The **Packages** pane can be accessed via **Administration > Data Gateway Global Settings > Packages**.

## Custom Package

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

- CLI Device Package:** To use CLI-based KPIs to monitor device health for third-party devices. All custom CLI device packages along with their corresponding YANG models should be included in file `custom-cli-device-packages.tar.xz`. Multiple files are not supported.
- 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 packages can be edited. All custom SNMP MIB packages along with YANG models should be included in file `custom-mib-packages.tar.xz`. Multiple files are not supported.



**Note** 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.

- 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.

## Add Custom Packages

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

- You can upload one or more xar files in a single package tar.gz file.
- Cisco Crosswork doesn't allow Custom MIB package files to overwrite the System MIB Package files. It results in a failed upload attempt.
- Ensure that the custom package TAR file has just the 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 package.



**Note** Cisco Crosswork does not validate the files being uploaded other than checking the file extension.

Follow these steps to upload a custom software package:

**Delete Custom Package****Before you begin**

When uploading new MIBs as a part of Custom MIB Package, ensure that those new MIBs files can be uploaded within collectors along with existing System MIB files i.e., all dependencies in the files are resolved properly.



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

For information on how to validate custom MIBs and YANGs that is, to check if they can be uploaded to Cisco Crosswork, see [Use Custom MIBs and Yangs on Cisco DevNet](#).

**Procedure**

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

**Step 2** In the **Custom Packages** pane, click .

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 Packages** window that appears, select the type of package you want to import from the **Type** drop-down.

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

**Step 5** Add a description of the package in the **Notes** field. 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 Custom Package**

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

Follow the steps to delete a custom package:

**Procedure**

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

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

**Step 3** In the **Delete Custom Package** window that appears, click **Delete** to confirm.

## System Device Package

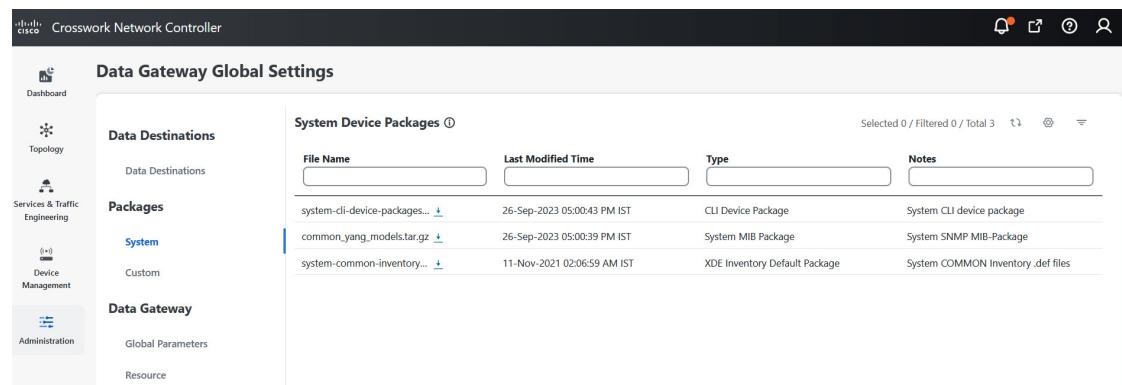
A system device package contains one or more separate installable. Each file set in a package belongs to the same application.

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



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

**Figure 34: System Device Packages Window**



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

## Configure Crosswork Data Gateway Global Parameters

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



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

### Procedure

**Step 1** Navigate to **Administration > Data Gateway Global Settings > Data Gateway > Global Parameters**.

## Configure Crosswork Data Gateway Global Parameters

Figure 35: Global Parameters Window

**Data Gateway Global Settings**

Global Parameters ⓘ	
<p><b>⚠</b> Ensure the values entered for ports shown below do not conflict with the existing values configured on CDG. Syslog/SNMP Port Changes are not applicable to CDG instances running on EKS.</p>	
<b>Data Destinations</b>	Number of CLI Sessions* ⓘ <input type="text" value="3"/> Numeric value
<b>Packages</b>	System: SSH Session Timeout* ⓘ <input type="text" value="120"/> Range: 0-2147483647
	Custom: SNMP Trap Port* ⓘ <input type="text" value="1062"/> Range: 1-65535
<b>Data Gateway</b>	Syslog UDP Port* ⓘ <input type="text" value="9514"/> Range: 1-65535
Global Parameters	Syslog TCP Port* ⓘ <input type="text" value="9898"/> Range: 1-65535
Resource	Syslog TLS Port* ⓘ <input type="text" value="6514"/> Range: 1-65535
	Force Re-Sync USM Engine Details for SNMPv3 <input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Reset to Default"/> <input type="button" value="Discard Changes"/>	

**Step 2** Change one of more of the following parameters.**Note**

Ensure that the port values that you wish to update with are valid ports and do not conflict with the existing port values. Same port values must be configured on the device.

Parameter Name	Description
<b>Number of CLI sessions</b>	Maximum number of CLI sessions between a Crosswork Data Gateway and devices. The default value is 3. <b>Note</b> This value overrides any internal configuration set for the same parameter.
<b>SSH Session Timeout</b>	The session timeout (in seconds) is the duration for which a CLI connection can remain idle in the CLI and SNMP collectors. The default value is 120.
<b>SNMP Trap Port</b>	Default value is 1062.
<b>Syslog UDP Port</b>	Default value is 9514.

Parameter Name	Description
<b>Syslog TCP Port</b>	Default value is 9898.
<b>Syslog TLS Port</b>	Default value is 6514.
<b>Force Re-Sync USM Engine Details for SNMPV3</b>	<p>USM details change whenever a device is rebooted or reimaged. SNMPV3 collections stop working whenever there is a change in any of the USM details.</p> <p>Enable this option to sync the USM details automatically whenever there is a change, after the very first collection failure.</p> <p>The default value is False.</p>

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

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

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

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



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

#### What to do next

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

## Allocate Crosswork Data Gateway Resources

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



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

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



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

To update resource allocation for collectors:



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

## Procedure

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

*Figure 36: Resource Window*

Resource ①		
<b>Collector</b> ① <b>Memory (MB)</b> ① <b>Enable Collector</b> ①		
<small>⚠ Recommend a minimum memory setting of 2000 mb for CLI &amp; SNMP, 1000 mb for NETCONF collectors. System resource updates are not applicable to CDG instances running on EKS.</small>		
Data Destinations	9216	<input checked="" type="checkbox"/>
Packages	10240	<input checked="" type="checkbox"/>
Data Gateway	5120	<input checked="" type="checkbox"/>
Resource	10240	<input checked="" type="checkbox"/>
SYSLOG	5120	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Reset to Default"/> <input type="button" value="Discard Changes"/>		

**Note**

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

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

**Attention**

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

**Step 3** Drag the **Enable Collector** slider to On position to enable the data collection.

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

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

---

**Enable or Disable Collectors**

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

To enable or disable the collectors:

**Before you begin**

Review the following information before enabling or disabling a collector:

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



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

---

**Procedure**

**Step 1** Navigate to **Administration > Data Gateway Global Settings > Data Gateway > Resource**.

The list of collectors and the resource limits is displayed.

## Manage Crosswork Data Gateway Collection Jobs

Figure 37: Enabling or Disabling Collectors

Collector	Memory (MB)	Enable Collector
*CLI	9216	<input checked="" type="checkbox"/>
GNMI	10240	<input checked="" type="checkbox"/>
MDT	5120	<input checked="" type="checkbox"/>
*SNMP	10240	<input checked="" type="checkbox"/>
SYSLOG	5120	<input checked="" type="checkbox"/>

**Note**

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

- Step 2** Drag the **Enable/Disable Collectors** slider to On position to enable the collectors. A confirmation dialog box indicating that the enabling or disabling causes the collector to restart appears.
- Step 3** Click **Yes**.
- Step 4** Click **Save** to apply your changes.

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

## Manage Crosswork Data Gateway Collection Jobs

A collection job is a task that 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.

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



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

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

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

1. Data collection request to forward data for internal processes within Cisco Crosswork. Cisco Crosswork creates system jobs for this purpose. You cannot create or edit system jobs.
2. Data collection request to forward data to external data destinations. For more information on configuring the external data destinations (Kafka or gRPC), see [Create and Manage External Data Destinations, on page 52](#).

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



- Note**
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 unsolicited device (that is, 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.

---

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

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

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



- 
- Note**
- The **Parametrized Jobs** pane has no data and remains empty if Cisco Crosswork Service Health has not been deployed.

---

For more information, see [Monitor Collection Jobs, on page 104](#).

## Types of Collection Jobs

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



- 
- Note**
- The SNMP OID-based collection jobs can be created from the Cisco Crosswork UI or using the API, and SNMP-traps using the API.
- 
- [CLI Collection Job, on page 68](#)
  - [SNMP Collection Job, on page 69](#)
  - [MDT Collection Job, on page 76](#)

- [Syslog Collection Job, on page 78](#)
- [gNMI Collection Job, on page 87](#)

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

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

The initial status for all the collection jobs in the Cisco Crosswork UI is Unknown. Upon receiving a 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. This value can be set between 10 seconds and 2764800 seconds ( i.e. at most 32 days) max, depending on how frequently configured sensor data should be collected.



**Note** We recommend a cadence of 60 seconds.

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.

## CLI Collection Job

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

- show and the short version sh
- traceroute
- dir

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

You can create a CLI collection job from the Cisco Crosswork UI or using APIs. See [Cisco DevNet](#) for more information.

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

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

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    }
  }
}
```

```

"job_device_set": {
  "device_set": {
    "devices": {
      "device_ids": [
        "658adb03-cc61-448d-972f-4fcec32cbfe8"
      ]
    }
  }
},
"sensor_input_configs": [
  {
    "sensor_data": {
      "cli_sensor": {
        "command": "show platform"
      }
    },
    "cadence_in_millisec": "tel:60000"
  }
],
"sensor_output_configs": [
  {
    "sensor_data": {
      "cli_sensor": {
        "command": "show platform"
      }
    },
    "destination": {
      "destination_id": "le71f2fb-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 prepackaged 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.

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

The device packages can be imported into the Crosswork Data Gateway instance as described in Section [Add Custom Packages, on page 59](#).

Supported SNMP versions for data polling and traps are:

- Polling Data
- SNMP V2

- SNMP V3 (no auth nopriv, auth no priv, authpriv)
- Supported auth protocols – SHA-1, MD5
- Supported priv protocols – AES-128, AES-192, AES-256, CiscoAES192, CiscoAES256, DES, and 3-DES.
- Traps
  - SNMP V2
  - SNMP V3 (no auth nopriv, auth no priv, authpriv)

### Sample Configurations on Device:

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

**Table 4: Sample configuration to enable SNMP on device**

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

Version	Command	To...
V3  <b>Note</b> Password for a SNMPv3 user must be at least 8 bytes.	<pre>snmp-server host &lt;host_IP&gt; traps version 3 priv &lt;user_name&gt; udp-port 1062</pre>	<p>Define the destination to which trap data must be forwarded.</p> <p><b>Note</b> The IP address mentioned here must be the virtual IP address of the Crosswork Data Gateway.</p>
	<pre>snmp-server user &lt;user_name&gt; &lt;group_name&gt; v3 auth md5 &lt;password&gt; priv aes 128 &lt;password&gt;</pre>	<p>Configures the SNMP server group to enable authentication for members of a specified named access list.</p>
	<pre>snmp-server view &lt;user_name&gt; &lt; MIB &gt; included</pre>	<p>Define what must be reported.</p>
	<pre>snmp-server group &lt;group_name&gt; v3 auth notify &lt;user_name&gt; read &lt;user_name&gt; write &lt;user_name&gt;</pre>	<p>Define the SNMP version, user/user group details.</p>
	<pre>snmp-server enable traps snmp [authentication ] [linkup ] [linkdown ] [warmstart ] [coldstart ]</pre>	<ul style="list-style-type: none"> <li>When used without any of the optional keywords, enables authenticationFailure, linkUp, linkDown, warmStart, and coldStart traps.</li> <li>When used with keywords, enables only the trap types specified. For example, to globally enable only linkUp and linkDown SNMP traps for all interfaces, use the <b>snmp-server enable traps snmp linkup linkdown</b> form of this command.</li> </ul>

The SNMP Collector supports the following operations:

- SCALAR



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

- TABLE
- WALK
- COLUMN

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



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

The value for **snmpRequestTimeoutMillis** should be specified in milliseconds:

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

Following is an SNMP collection job sample:

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

```

```

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

```

### SNMP Traps Collection Job

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



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

Crosswork Data Gateway listens on UDP port 1062 for Traps.



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

### SNMP Trap Collection Job Workflow

On receiving an SNMP trap, Cisco Crosswork Data Gateway:

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



**Note** To prevent Crosswork Data Gateway from checking the community string for SNMP traps, select the **SNMP Disable Trap Check** check box when adding a device through the Crosswork UI. For more information about this option, see [Add Devices through the UI, on page 211](#).

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



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

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

If the collection job is invalid, there is missing configuration on the device, or no trap is received, the status of the job remains "Unknown". For list of supported Traps and MIBs, see [List of Pre-loaded Traps and MIBs for SNMP Collection, on page 451](#).

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

**Table 5: List of Supported Non-Yang/OID based Traps**

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

Following is an SNMP-Trap collection job sample:

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

```

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

```

### Enabling Traps forwarding to external applications

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

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

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

- Link up

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4

- Link Down

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3

- Syslog

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1

- Cold Start

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1

```

{
    "nodeIdStr": "BF5-XRV9K1.tr3.es",
    "nodeIdUuid": "C9tZ51JoSJKf5OZ67+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": "YmNjZjEzMTktZjF1OS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVE9S",
    "status": {
        "status": "SUCCESS"
    },
    "modelData": {},
    "sensorData": {
        "trapSensor": {
            "path": "1.3.6.1.6.3.1.1.5.4"
        }
    },
    "applicationContexts": [
        {
            "applicationId": "APP1",
            "contextId": "collection-job-snmp-traps"
        }
    ]
}

```

## MDT Collection Job

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

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

- MDT TCP Dial-out Mode

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


**Note**

- If there is some change (update) in existing MDT jobs between backup and restore operations, Cisco Crosswork does not replay the jobs for config update on the devices as this involves NSO. You have to restore configs on NSO/devices. Cisco Crosswork only restores the jobs in database.
- Before using any YANG modules, check if they are supported. See Section: [List of Pre-loaded YANG Modules for MDT Collection , on page 459](#)

Following is a sample of MDT collection payload:

```
{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "device_group": "mdt"
      }
    },
    "sensor_output_configs": [
      {
        "sensor_data": {
          "mdt_sensor": {
            "path": "Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
          }
        },
        "destination": {
          "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
          "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
      },
      {
        "sensor_data": {
          "mdt_sensor": {
            "path": "Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
          }
        },
        "destination": {
          "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
          "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
      }
    ],
    "sensor_input_configs": [
      {
        "sensor_data": {
          "mdt_sensor": {
            "path": "Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
          }
        },
        "cadence_in_millisec": "70000"
      },
      {
        "sensor_data": {
          "mdt_sensor": {
            "path": "Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
          }
        }
      }
    ]
  }
}
```

```

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

```

### MDT Collection Job Workflow

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

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

## Syslog Collection Job

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



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

The following Syslog formats are supported:

- RFC5424 syslog format
- RFC3164 syslog format



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

While the order of the configuration steps does not matter, you must complete both the steps, or no data will be sent or collected. For sample device configuration, see [Configure Syslog \(Non-Secure\) on Device, on page 82](#). Cisco Crosswork also allows you to set up secure syslog communication to the device. For more information, see [Configure Secure Syslog on Device, on page 84](#).

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": "demomilestone2syslog",
    "application_id": "SyslogDemo2"
},
"collection_mode": {
    "lifetime_type": "APPLICATION_MANAGED",
    "collector_type": "SYSLOG_COLLECTOR"
}
}
}

```

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

## Syslog Collection Job Output

When you onboard a device from 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 syslog events as received from device.

**Note**

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

Sample output:

```

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

```

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



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

RFC5424

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

### Sample output:

• • • •

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

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

## Configure Syslog (Non-Secure) on Device



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

RFC3164

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

Sample output:

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

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

## Configure Syslog (Non-Secure) on Device

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



**Note** The syslog format that you configure for the device must match the format that you specified when the device was added through the Crosswork UI. See [Add Devices through the UI, on page 211](#) for more information.

### Configure RFC3164 Syslog format



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

#### For IOS XR:

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

#### For IOS XE:

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

### Configure RFC5424 Syslog format

#### For IOS XR:

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

#### For IOS XE:

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

## Configure Secure Syslog on Device

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

1. Download the Cisco Crosswork trust chain from the **Certificate Management UI** page in Cisco Crosswork.
2. Configure the device with the Cisco Crosswork trustchain.

### Download Syslog Certificates

1. In the Cisco Crosswork UI, go to **Administration > Certificate Management**.
2. Click *i* in the **crosswork-device-syslog** row.
3. Click **Export All** to download the certificates.

The following files are downloaded to your system.



## Configure Cisco Crosswork Trustpoint on Device

### Sample IOS XR device configuration to enable TLS

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

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

```
-----BEGIN CERTIFICATE-----
MIIGKzCCBBOgAwIBAgIRAKfyU89yjmrXVDRKBWuSGPgwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
...
...
jPQ/UrO8N3sC1gGJX7CIIh5cE+KIJ51ep8i1eKSJ5wHWRTmv342MnG2StgOTtaFF
vrkWHD02o6jRuYXDWEUptDOg8oEritZb+SNPWXUc/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/ygAwIBAgIRAkhhQXcJzQzeQK6U2wn8PIwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAKNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
-----
51Bk617z6cxFER5c+/PmJFhcreisTxXg1aJbFdnB5C8f+0uUIdLghykQ/zaZGuBn
AAB70c9r90eKGJWzvv1e2U8HH1pdQ/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

```

## Configure Secure Syslog on Device

```

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#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG Southbound IP>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

RP/0/RSP0/CPU0:ASR9k#

```

### Sample IOS XE device configuration to enable TLS

```

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

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

-----BEGIN CERTIFICATE-----
MIIFPjCCAyYCCQCO6pK5AOGYdjANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCE1pbHBpdGFzMQ4wDAYDVQQKDAVDaXNj
.....
.....
JbimOpXAncoBLo14DXOJLvvMVRjn1EULE9AXXCNfnrnBx7jL4CV+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
EzARBgNVBAgMCKNhbg1mb3JuaWExDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQLDAVT
.
.
.
Nmz6NQynD7bxQa9Xq9kyPuY3ZVKXkf312IRH0MEy2yFX/tAen9JqOeZ1g8canmw
TxsWA5TLzy1RmxqQh88f0CM=
-----END CERTIFICATE-----
Trustpoint 'syslog-intermediate' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
  Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
  Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19

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

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

### Syslog configuration to support FQDN

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

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

#### For IOS XR:

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

#### For IOS XE:

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

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

#### For IOS XR:

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

#### For IOS XE:

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

## gNMI Collection Job

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 the requested destinations.



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

To configure gNMI on the device, see [Device Configuration for gNMI, on page 96](#).

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

If a device reloads, gNMI collector ensures that the existing subscriptions are re-subscribed to the device. gNMI specification does not have a way to mark end of message. Hence, Destination and Dispatch cadence is not supported in gNMI collector.

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

**Table 6: gNMI Subscription Options**

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

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

**Note**

- Crosswork Data Gateway relies on the device to declare the support of one or more modes.
- gNMI sensor path with default values does not appear in the payload. This is a known protobuf behavior. For boolean the default value is false. For enum, it is gnmi.proto specified.

**Example 1:**

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

**Example 2:**

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

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

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

**Enable Secure gNMI communication between Device and Crosswork Data Gateway**

## Enable Secure gNMI communication between Device and Crosswork Data Gateway

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

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

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

1. Generate the certificates. See [Generate Device Certificates](#), on page 91.

2. Upload the certificates to the Crosswork Certificate Management UI in Cisco Crosswork. See [Configure gNMI Certificate, on page 92](#).
3. Update device configuration with secure gNMI port details from Cisco Crosswork UI. See [Update Protocol on Device from Cisco Crosswork, on page 95](#).
4. Enable gNMI on the device. See [Device Configuration for gNMI, on page 96](#).
5. Enable gNMI bundling on the device. See [Configuring gNMI Bundling for IOS XR, on page 97](#).
6. Configure the certificates and device key on the device. See [Import and Install Certificates on Devices, on page 94](#).

### Generate Device Certificates

This section explains how to create certificates with OpenSSL.

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



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

#### 1. Create the rootCA certificate

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

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

#### 2. Create device key and certificate

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

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

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

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

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

The following is a sample output:

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

## Configure gNMI Certificate

```

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

```

## Configure gNMI Certificate

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



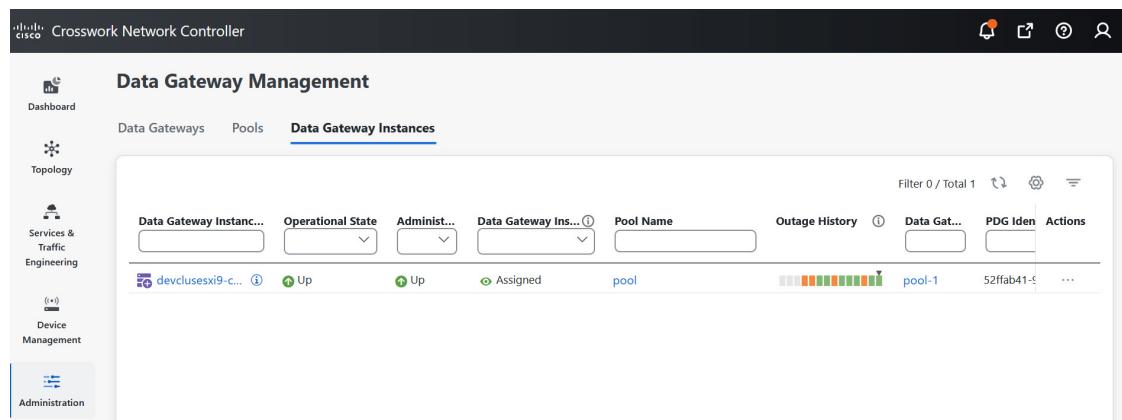
**Note** You can upload only one gNMI certificate to Crosswork.

To add the gNMI certificate.

## Procedure

- Step 1** From the Cisco Crosswork UI, go to **Administration > Certificate Management**.
- Step 2** Click the + icon to add the certificate.
- Step 3** In **Add Certificate** window, enter the following details:
- **Device Certificate Name** - Enter a name for the certificate.
  - **Certificate Role** - Select **Device gNMI Communication** from the drop-down list.
  - **Device Trust Chain** - Browse your local file system to the location of the rootCA file and upload it.

*Figure 38: Add Certificate Window*



### Note

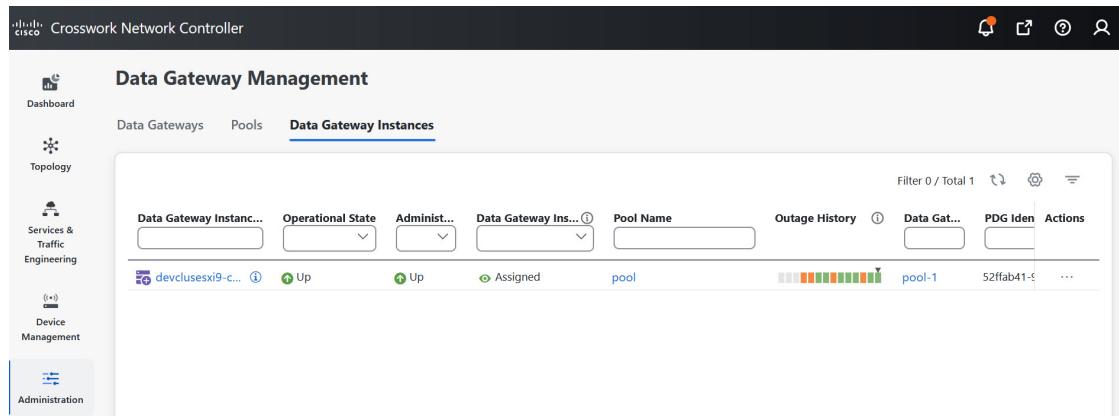
If gNMI certificate is already configured and you wish to onboard a device with a different trust chain, update the existing .pem file to include details of the new CA. Select the existing gNMI certificate from the list, click the Edit icon and upload the new .pem file.

- Step 4** Click **Save**.

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

## Import and Install Certificates on Devices

Figure 39: Certificates Window



## Import and Install Certificates on Devices

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

### Certificates on a Cisco IOS XR Device

To install certificates on a Cisco IOS XR device.

1. Copy rootCA.pem, device.key, and device.crt to the device under /tmp folder.
  2. Log in into the IOS XR device.
  3. Use the run command to enter the VM shell.
- ```
RP/0/RP0/CPU0:xrvr-7.2.1#run
```
4. Navigate to the following directory:
- ```
cd /misc/config/grpc
```
5. Create or replace the content of the following files:



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

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

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

### Certificates on a Cisco IOS XE Device

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

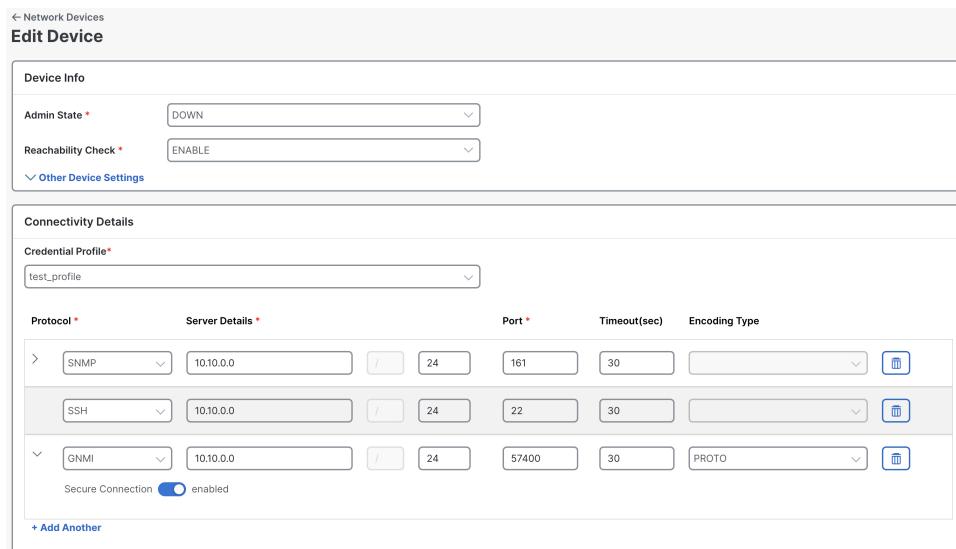
```
# Send:  
Device# configure terminal  
Device(config)# crypto pki import trustpoint1 pem terminal password password1  
  
# Receive:  
% Enter PEM-formatted CA certificate.  
% End with a blank line or "quit" on a line by itself.  
  
# Send:  
# Contents of rootCA.pem, followed by newline + 'quit' + newline:  
-----BEGIN CERTIFICATE-----  
<snip>  
-----END CERTIFICATE-----  
quit  
  
# Receive:  
% Enter PEM-formatted encrypted private General Purpose key.  
% End with "quit" on a line by itself.  
  
# Send:  
# Contents of device.des3.key, followed by newline + 'quit' + newline:  
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20  
<snip>  
-----END RSA PRIVATE KEY-----  
quit  
  
# Receive:  
% Enter PEM-formatted General Purpose certificate.  
% End with a blank line or "quit" on a line by itself.  
  
# Send:  
# Contents of device.crt, followed by newline + 'quit' + newline:  
-----BEGIN CERTIFICATE-----  
<snip>  
-----END CERTIFICATE-----  
quit  
  
# Receive:  
% PEM files import succeeded.  
Device(config)#  
  
# Send:  
Device(config)# crypto pki trustpoint trustpoint1  
Device(ca-trustpoint)# revocation-check none  
Device(ca-trustpoint)# end  
Device#
```

### ***Update Protocol on Device from Cisco Crosswork***

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

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

Figure 40: Edit Device Details Window



## Device Configuration for gNMI

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

### Cisco IOS XR devices

1. Enable gRPC over an HTTP/2 connection.

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

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

2. Set the session parameters.

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

where:

- **address-family**: Set the address family identifier type.
- **dscp**: Set QoS marking DSCP on transmitted gRPC.
- **max-request-per-user**: Set the maximum concurrent requests per user.
- **max-request-total**: Set the maximum concurrent requests in total.
- **max-streams**: Set the maximum number of concurrent gRPC requests. The maximum subscription limit is 128 requests. The default is 32 requests.
- **max-streams-per-user**: Set the maximum concurrent gRPC requests for each user. The maximum subscription limit is 128 requests. The default is 32 requests.
- **no-tls**: Disable transport layer security (TLS). The TLS is enabled by default.

- **service-layer**: Enable the grpc service layer configuration.
- **tls-cipher**: Enable the gRPC TLS cipher suites.
- **tls-mutual**: Set the mutual authentication.
- **tls-trustpoint**: Configure trustpoint.
- **server-vrf**: Enable the server vrf.

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

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

## Cisco IOS XE Devices

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

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

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

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

## Configuring gNMI Bundling for IOS XR

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

### Before you begin

Make sure that you are aware of the following:

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

## Procedure

- Step 1** Enable the bundling feature using the following command:

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

The gNMI bundling capability is disabled by default.

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

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

The default bundling size is 32768 bytes.

**Important**

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

## What to do next

Verify that the bundling capability is configured using the following:

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

## Create a Collection Job from Cisco Crosswork UI

Follow the steps to create a collection job:



**Note** Collection jobs created through the 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.

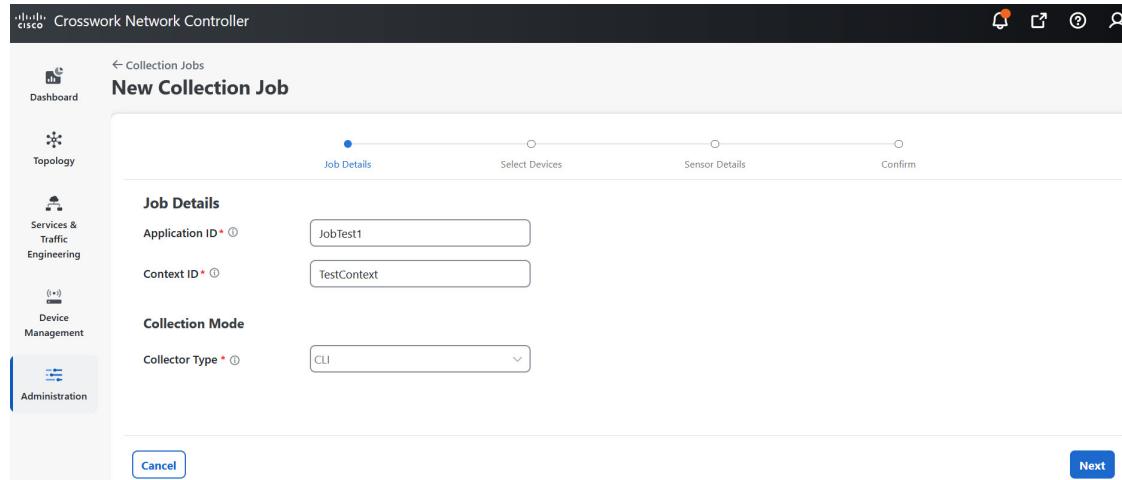
## Procedure

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

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

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

**Figure 41: Job Details Window**



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

Click **Next**.

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

## Create a Collection Job from Cisco Crosswork UI

Figure 42: Select Devices Window

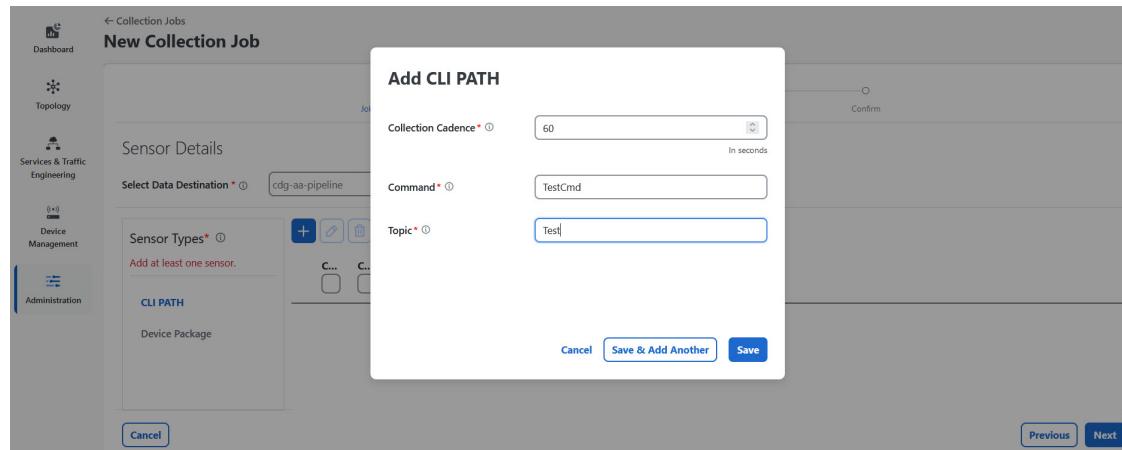
**Step 5** (Applicable only for CLI collection) Enter the following sensor details:

Figure 43: Sensor Details Window for CLI Path

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

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

Figure 44: Add CLI Path Dialog Box



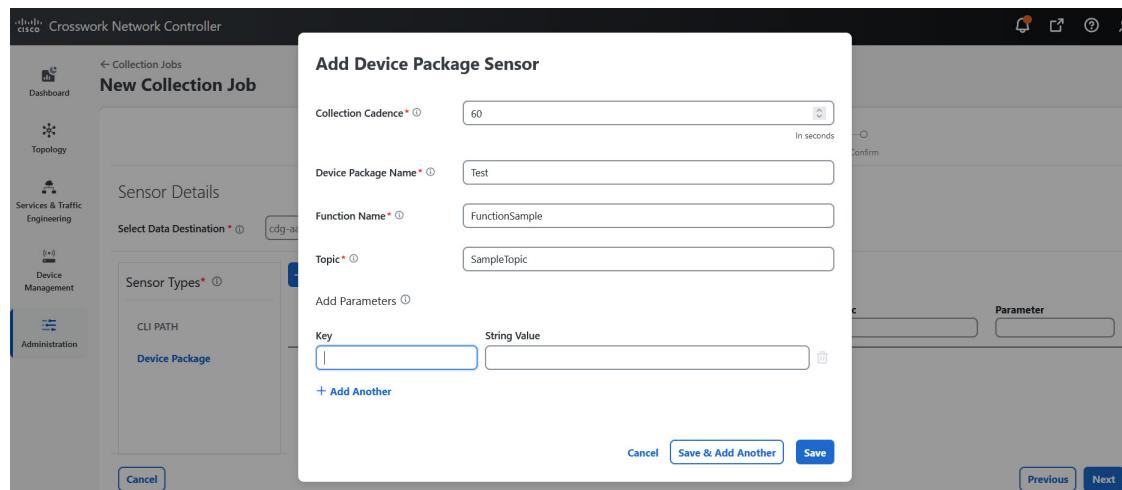
- Collection Cadence: Push or poll cadence in seconds.
- Command: CLI command
- Topic: Topic associated with the output destination.

**Note**

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

If you selected **Device Package**, click **+** button and enter values for the following parameters in the **Add Device Package Sensor** dialog box:

Figure 45: 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.

## Create a Collection Job from Cisco Crosswork UI

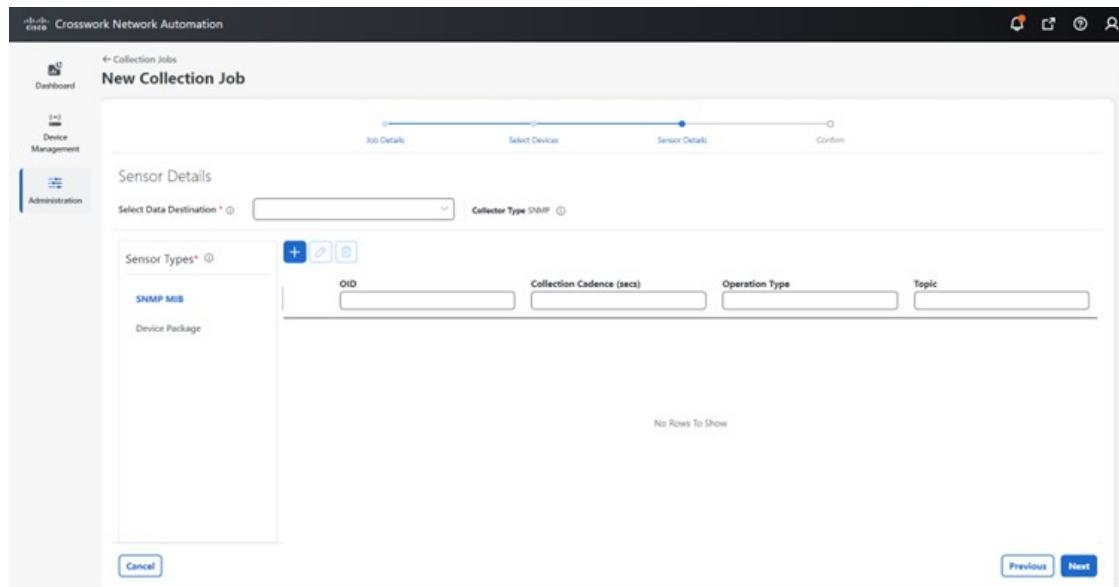
Enter Key and String value for the parameters.

Click **Save**.

### Step 6

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

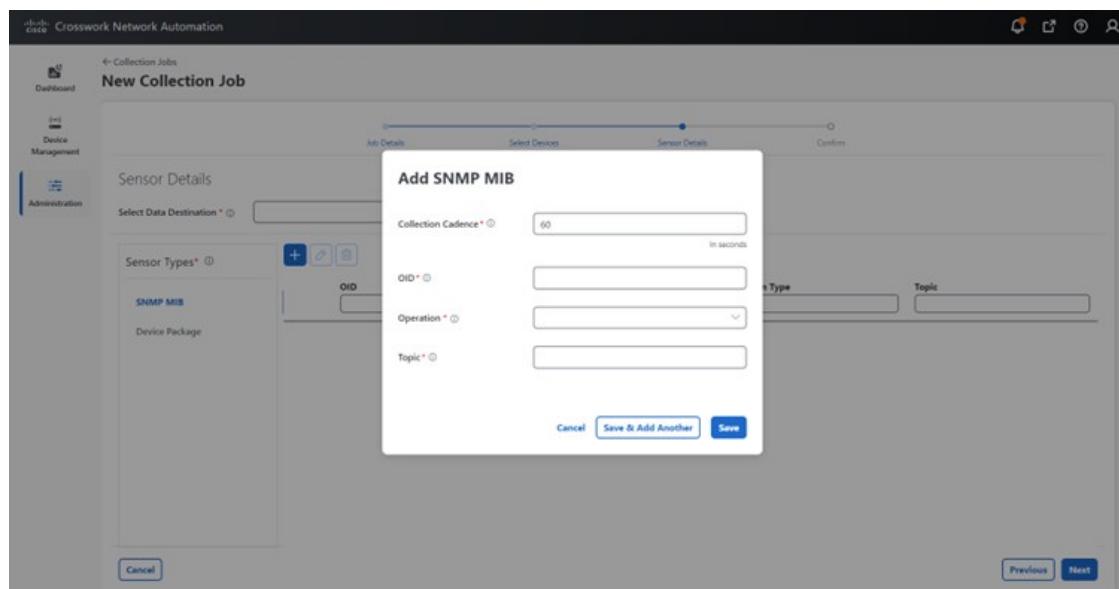
Figure 46: Sensor Details Window for SNMP Path



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

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

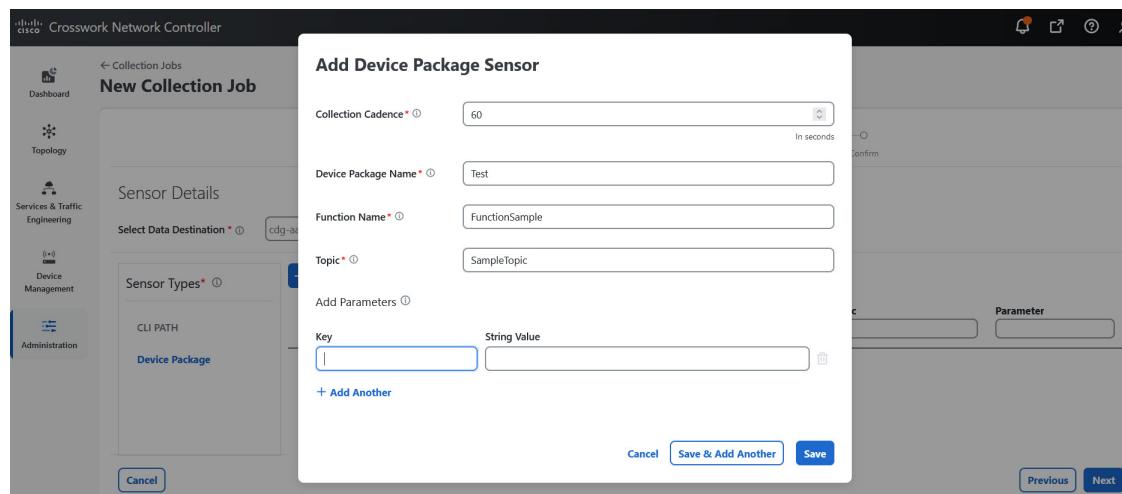
Figure 47: Add SNMP MIB Dialog Box



- Collection Cadence: Push or poll cadence in seconds.
- OID
- Operation: Select the operation from the list.
- Topic: Topic associated with the output destination.

If you selected **Device Package**, click **+** button and enter values for the following parameters in the **Add Device Package Sensor** dialog box:

**Figure 48: Add Device Package Sensor Dialog Box**



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

Enter Key and String value for the parameters.

Click **Save**.

#### Step 7 Click **Create Collection Job**.

##### Note

When a collection job is submitted for an external Kafka destination i.e., unsecure Kafka, the dispatch job to Kafka fails to connect. The error seen in collector logs is `org.apache.kafka.common.errors.TimeoutException: Topic cli-job-kafka-unsecure not present in metadata after 60000 ms.` In Kafka logs, the error seen is `SSL authentication error` "[2021-01-08 22:17:03,049] INFO [SocketServer brokerId=0] Failed authentication with /80.80.80.108 (SSL handshake failed) (org.apache.kafka.common.network.Selector).

This happens because port is blocked on external Kafka VM. You can use the following command to check if port is listening on Kafka docker/server port:

```
netstat -tulpn
```

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

---

## Monitor Collection Jobs

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

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

This left pane lists all active collection jobs along with their Status, App ID, and Context ID. The **Job Details** pane shows the details of all collection tasks associated with a particular job in the left pane. The overall status of the Collection job in the **Collection Jobs** pane is the aggregate status of all the collection tasks in the **Jobs Details** pane.

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

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

**Note**

- The status of a collection task associated with a device after it is attached to a Crosswork Data Gateway, is **Unknown**.
- A job could have status as **Unknown** for one of the following reasons:
  - Crosswork Data Gateway has not yet reported its status.
  - Loss of connection between Crosswork Data Gateway and Cisco Crosswork.
  - Crosswork Data Gateway has received the collection job, but actual collection is still pending. For example, traps are not being sent to Crosswork Data Gateway southbound interface, or device is not sending telemetry updates.
  - The trap condition in a SNMP trap collection job which we are monitoring has not occurred. For example, if you are looking for Link Up or Link down transitions and the link state has not changed since the collector was established, then the state will report as **Unknown**. To validate that trap-based collections are working it is therefore necessary to actually trigger the trap.
- After the collection job is processed, the status changes to 'Successful' if the processing was successful or else it changes to 'Failed'.
- If a collection job is in degraded state, one of the reasons might be that the static routes to the device have been erased from Crosswork Data Gateway.
- Collections to a destination that is in an Error state do not stop. The destination state is identified in background. If the destination is in an Error state, the error count is incremented. Drill down on the error message that is displayed in the **Distribution** status to identify and resolve the issue by looking at respective collector logs.
- Cisco Crosswork Health Insights - KPI jobs must be enabled only on devices mapped to an extended Crosswork Data Gateway instance. Enabling KPI jobs on devices that are mapped to a standard Crosswork Data Gateway instance reports the collection job status as **Degraded** and the collection task status as **Failed** in the **Jobs Details** pane.

- 
- Job configuration of the collection job that you pass in the REST API request. Click  icon next to **Config Details** to view the job configuration. 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	<p>Sensor path</p> <p>Click  to see collection/distribution summary. From the sensor data summary pop up you can copy the sensor data by clicking <b>Copy to Clipboard</b>.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• last_collection_time_msec</li> <li>• total_collection_message_count</li> <li>• last_device_latency_msec</li> <li>• last_collection_cadence_msec</li> </ul> <p>It shows the following metrics for a collection:</p> <ul style="list-style-type: none"> <li>• total_output_message_count</li> <li>• last_destination_latency_msec</li> <li>• last_output_cadence_msec</li> <li>• last_output_time_msec</li> <li>• total_output_bytes_count</li> </ul>
Destination	Data destination for the job.

Field	Description
Last Status Change Reported Time	Time and date on which last status change was reported for that device sensor pair from Crosswork Data Gateway

**Note**

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

**Note**

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.

### Collection Status for Event-based collection jobs

1. When data collection is successful, status of the Collection job changes from **Unknown** to **Success** in the **Collection Jobs** pane.
2. When a device is detached from the Crosswork Data Gateway, all corresponding collection jobs are deleted and collection job status is displayed as **Success** in the **Collection Jobs** pane. There are no devices or collection tasks displayed in the **Job Details** pane.
3. When a device is attached to a Crosswork Data Gateway, Crosswork Data Gateway receives a new collection job with the status set to **Unknown** that changes to **Success** after receiving events from the device.
4. If the device configuration is updated incorrectly on a device that is already attached to a Crosswork Data Gateway and after the Crosswork Data Gateway has received the job and events, there is no change in status of the collection task in the **Jobs Details** pane.
5. If the device inventory is updated with incorrect device IP, the collection task status in the **Jobs Details** pane is **Unknown**.

## Delete a Collection Job

System jobs (default jobs created by various Crosswork Applications) should not be deleted as it will cause issues. Jobs created by Health Insights should only be deleted by disabling the KPI profile which will remove the collection jobs it deployed. Use this procedure to delete external collection jobs from the **Collection Jobs** page.

Follow the steps to delete a collection job:

## Procedure

- 
- Step 1** Go to **Administration > Collection Jobs**.
- Step 2** Select either the **Bulk Jobs** tab or **Parametrized Jobs** tab.
- Step 3** In the **Collection Jobs** pane on the left hand side, select the collection job that you want to delete.
- Step 4** Click .
- Step 5** Click **Delete** when prompted for confirmation.
- 

## Troubleshoot Crosswork Data Gateway

You can troubleshoot the Crosswork Data Gateway from the UI or from the Interactive Console of the Crosswork Data Gateway VM.

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

**Figure 49: Data Gateway - Troubleshooting**



For details on troubleshooting options available from the Interactive Console of the Crosswork Data Gateway VM, see [Troubleshooting Crosswork Data Gateway VM, on page 442](#).

## Check Connectivity to the Destination

To check connectivity to a destination from the Cisco Data Gateway, use the **Ping** and **Traceroute** options from Troubleshooting Menu.



**Note** Ping traffic should be enabled on the network to ping the destination successfully.

- 
1. Go to **Administration > Data Gateway Management > Data Gateways**.
  2. Click the Cisco Crosswork Data Gateway name from which you want to check the connectivity.

3. In the Crosswork Data Gateway details page, on the top right corner, click **Actions** and choose: **Ping** or **Traceroute**.
  - **Ping** - Enter details in the **Number of Packets**, and **Destination Address** fields and click **Ping**.
  - **Traceroute** - Enter the **Destination Address**, and click **Traceroute**.
4. If the destination is reachable, Cisco Crosswork displays details of the **Ping** or **Traceroute** test in the same window.

## Download Service Metrics

Use this procedure to download the metrics for all collection jobs for a Crosswork Data Gateway from the Cisco Crosswork UI.

### Procedure

- 
- Step 1** Go to **Administration > Data Gateway Management > Data Gateways**.
- Step 2** Click the Crosswork Data Gateway name for which you want to download the service metrics.
- Step 3** In the Crosswork Data Gateway details page, on the top right corner, click **Actions > Download Service Metrics**.
- Step 4** Enter a passphrase.
- Note**  
Ensure that you make a note of this passphrase. This passphrase will be used later to decrypt the file.
- Step 5** Click **Download Service Metrics**. The file is downloaded to the default download folder on your system in an encrypted format.
- Step 6** After the download is complete, run the following command to decrypt it:

**Note**  
In order to decrypt the file, you must use openssl version 1.1.1i. Use the command `openssl version` to check the openssl version on your system.

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <service metrics file> -out <decrypted filename> -pass pass:<encrypt string>
```

---

## Download Showtech Logs

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



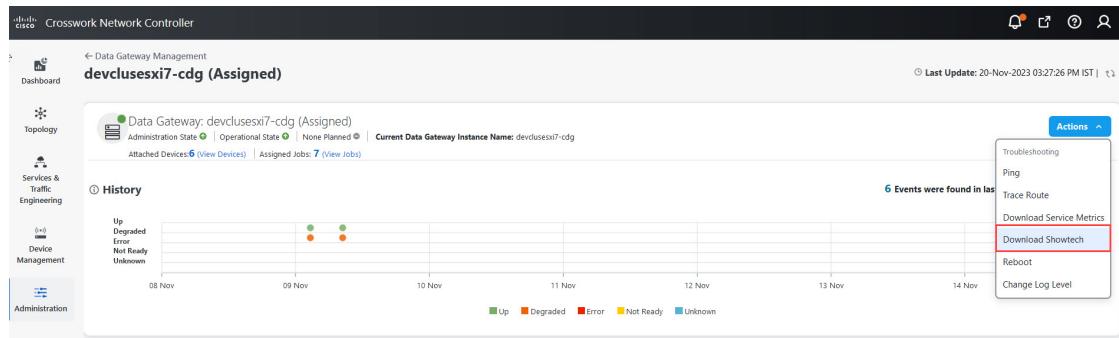
- Note** Showtech logs cannot be collected from the UI if the Crosswork Data Gateway is in an **ERROR** state. In the **DEGRADED** state of the Cisco Crosswork Data Gateway, if the OAM-Manager service is running and not degraded, you will be able to collect logs.

## Download Showtech Logs

### Procedure

- 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**.

**Figure 50: Data Gateway - Download Showtech**

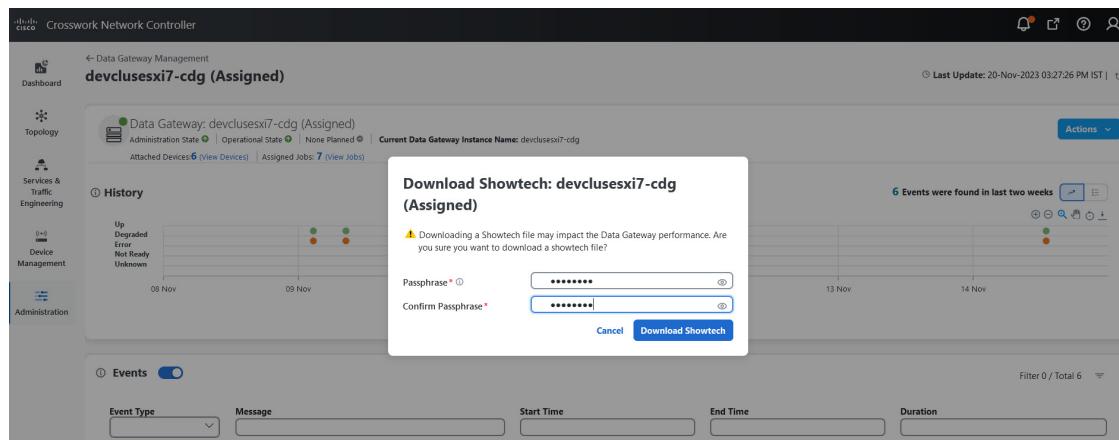


- Step 4** Enter a passphrase.

#### Note

Ensure that you make a note of this passphrase. You will need to enter this passphrase later to decrypt the showtech file.

**Figure 51: Download Showtech Pop-up Window**



- Step 5** Click **Download Showtech**. The showtech file downloads in an encrypted format.

#### Note

Depending on how long the system was in use, it may take several minutes to download the showtech file.

- Step 6** After the download is complete run the following command to decrypt it:

#### Note

In order to decrypt the file, you must use OpenSSL version 1.1.1i. Use the command `openssl version` to check the OpenSSL version on your system.

To decrypt the file on a MAC, you must install OpenSSL 1.1.1+. This is because LibreSSL's `openssl` command does not support all the switches supported by OpenSSL's `openssl` command.

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>
```

## Reboot Cisco Crosswork Data Gateway VM

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



**Note** Rebooting the Crosswork Data Gateway pauses its functionality until it is up again.

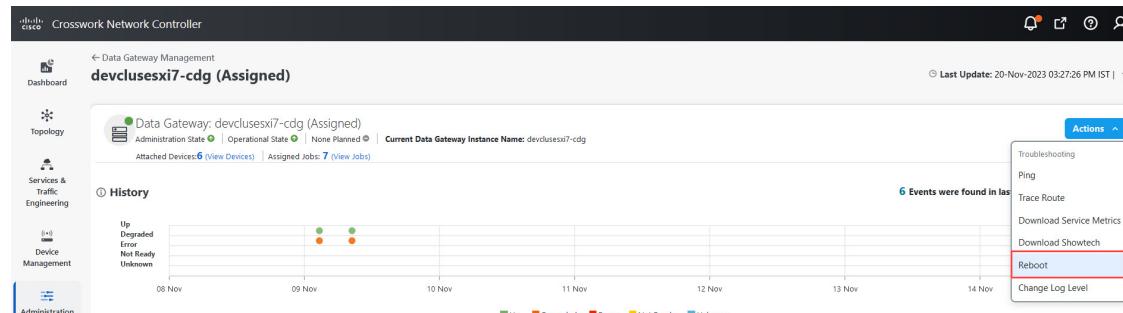
### Procedure

**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**.

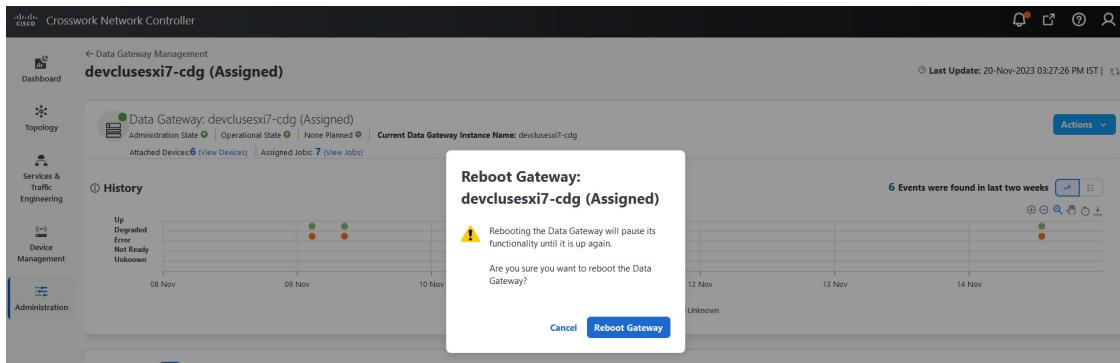
**Figure 52: Data Gateway - Reboot**



**Step 4** Click **Reboot Gateway**.

## Change Log Level of Crosswork Data Gateway Components

Figure 53: Reboot Gateway Popup Window



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

## Change Log Level of Crosswork Data Gateway Components

Cisco Crosswork UI offers the option to change the log level of a Crosswork Data Gateway's components, for example collectors (cli-collector) and infra services (oam-manager). Log level changes apply only to the Crosswork Data Gateway on which you are making the change.



### Note

Changing the log level for offload services is not supported.

### Procedure

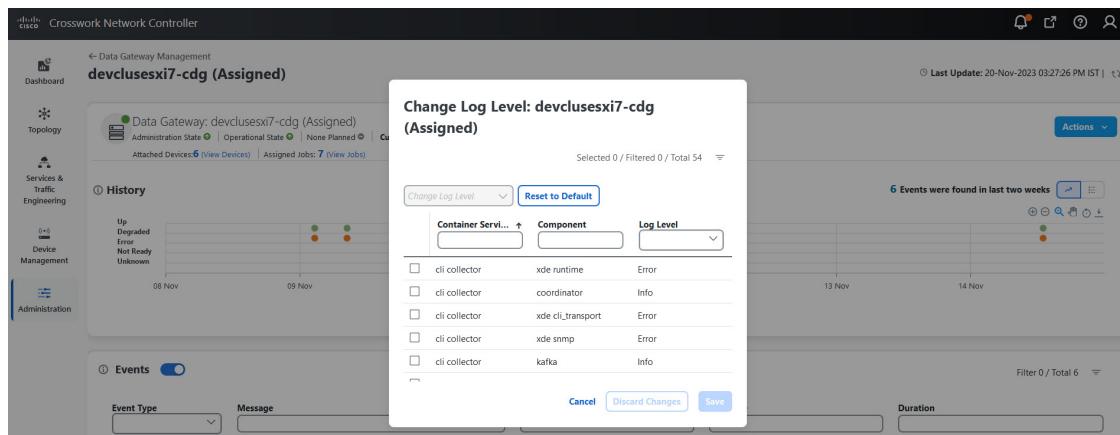
**Step 1** Go to **Administration > Data Gateway Management > Data Gateways**.

**Step 2** Click the Crosswork Data Gateway name on which you wish to change the log level for the collectors of Crosswork Infrastructure services.

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

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

Figure 54: Change Log Level Window



**Step 4** Select the check box of the container service for which you wish to change the log level.

**Step 5** From the **Change Log Level** drop-down list at the top of the table, select a log level from **Debug**, **Trace**, **Warning**, **Info** and **Error**.

**Note**

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

**Step 6** Click **Save** to save the log level change.

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

## Network Load Balancer Displays Incorrect Health Status for Active Crosswork Data Gateway

During the pool creation, Crosswork Data Gateway opens a health port for Network Load Balancer (NLB) to indicate Crosswork Data Gateway's health status. However, if the NLB FQDN resolves to IP addresses that are on different subnets of eth2 then Crosswork Data Gateway adds a static route to VM. The inclusion of the static route may fail with an error due to network configuration issues. Crosswork Data Gateway disregards the failure and creates the HA pool. As a consequence, Crosswork Data Gateway does not collect any data from the device.

To resolve this issue, use the following procedure:

### Procedure

**Step 1** Log in to the system identified as NLB and view the health status of the Crosswork Data Gateway.

**Step 2** If status is unhealthy, verify if the NLB subnet address conflicts with the interfaces such as eth1 or eth0. To resolve the conflict, perform one of the following:

- Modify the NLB IP addresses and restart the Infra services (oam-manager).

**Collection Job Status on the Collection Jobs Page is in the DEGRADED State**

- Redeploy the Crosswork Data Gateway VMs using new subnet configurations.
- 

**Collection Job Status on the Collection Jobs Page is in the DEGRADED State**

If a collection job on the Collection Jobs page is in the DEGRADED state, check the **Service Status** table on the **Administration > Data Gateway Management > Data Gateways** > (click) {Crosswork Data Gateway} page. This table provides the list of services on the system and the collector that is responsible for running the job.

If the collector is not listed, use the following procedure:

**Procedure**

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

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

**Step 3** In the confirmation box, select Yes.

---

**Data Gateway continues to collect data regardless of a change to the SNMPv3 Engine ID**

When the SNMPv3 device engine ID is changed and the device experiences a downtime with reachability errors, the SNMP collector continues to collect data from the device. Ideally, the data gateway must pause the data collection when the engine ID is modified.

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

To resolve this issue, enable **Force Re-Sync USM Engine Details for SNMPV3** in the Global Parameters window or change the device admin state from DOWN to UP. For more information about enabling the resync option, see [Configure Crosswork Data Gateway Global Parameters, on page 61](#).



## CHAPTER 4

# Manage Backups

This section contains the following topics:

- [Backup and Restore Overview, on page 115](#)
- [Manage Cisco Crosswork Backup and Restore, on page 116](#)
- [Restore Cisco Crosswork After a Disaster, on page 119](#)
- [Crosswork Data Gateway Disaster Recovery Scenarios, on page 120](#)
- [Resolve SR-TE Policies and RSVP-TE Tunnels, on page 124](#)
- [Backup Cisco Crosswork with Cisco NSO, on page 124](#)
- [Restore Cisco Crosswork with Cisco NSO, on page 125](#)
- [Migrate Data Using Backup and Restore, on page 127](#)

## Backup and Restore Overview

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

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

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

*Table 7: Backup and Restore options*

Menu option	Description
<b>Actions &gt; Data Backup</b> (See <a href="#">Manage Cisco Crosswork Backup and Restore, on page 116</a> for details)	Preserves the Cisco Crosswork configuration data. The backup file can be used with the data disaster restore ( <a href="#">Restore Cisco Crosswork After a Disaster, on page 119</a> ) to recover from a serious outage.  Among the backup options, you can also choose to <b>Backup with NSO</b> . This option preserves the Cisco NSO data along with the Cisco Crosswork configuration. See <a href="#">Backup Cisco Crosswork with Cisco NSO, on page 124</a> for details.

Menu option	Description
<b>Actions &gt; Data Disaster Restore</b> (See <a href="#">Restore Cisco Crosswork After a Disaster, on page 119</a> for details)	Restores the Cisco Crosswork configuration data after a natural or human-caused disaster has destroyed a Crosswork cluster. You must deploy a new cluster first, following the instructions in <a href="#">Cisco Crosswork Network Controller 6.0 Installation Guide</a> , and must install the exact versions of the applications that were present in your old Crosswork cluster (when you made the data backup) in your new Crosswork cluster. Any mismatch in the build versions of the applications can result in data loss and failure of the restore job.
<b>Actions &gt; Data Migration</b> (See <a href="#">Migrate Data Using Backup and Restore, on page 127</a> for details)	Migrates data from an older version of Cisco Crosswork to a newer version.

## Manage Cisco Crosswork Backup and Restore

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



### Attention

- Building a target machine for the backup is out of scope for this document. The operator is expected to have the server in place, to know the credentials for the server, and to have a target directory with adequate space for the backups in place.
- Crosswork does not manage the backups. It is up to the operator to periodically delete old backups from the target server to make room for future backups.
- Cisco Crosswork backup process depends on having SCP access to a server with sufficient amount of storage space. The storage required each backup will vary based on the your cluster size, applications in the cluster, and the scale requirements.
- The time taken for the backup or restore processes will vary based on the the type of backup, your cluster size and the applications in the cluster.

When you create backups for a Crosswork cluster, or restore a 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 *data 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 the 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 Crosswork cluster and the SCP server must be in the same IP environment. For example, if Crosswork is communicating over IPv6, so must the backup server.
- To save space on your backup server, you can delete older backups, but they may still appear in the job list in this version.
- Operators that make more changes should back up more often (possibly daily) while others might be comfortable with doing a backup once a week or before major system upgrades.
- By default, Cisco Crosswork will not allow you to make a backup of a system that it does not consider as healthy. However, there are provisions to override this protection to facilitate the sharing of an image with Cisco for additional analysis or other troubleshooting efforts.
- We recommend that you export the cluster inventory file when you perform a data backup.
- If Crosswork is installed (fresh install or reinstalled) after a disaster or failure and the data gateways are enrolled or integrated to the new Crosswork instance before the restore operation, it results in a certificate mismatch and the data gateways are moved to an error state. To correct the certificate issue, navigate to the Crosswork Data Gateway VM's interactive menu and re-import the certificates from the **Change Current System Settings** menu. For information on how to import the certificate, see [Change Current System Settings, on page 425](#).

### Before you begin

Before you begin, ensure that you have:

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

### Procedure

---

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

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

#### Step 2    Create a backup:

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

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

If you do 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 124](#) instead of the instructions here.

- f) Complete the remaining fields as needed.

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

- g) (Optional) Click **Verify Backup Readiness** to verify that 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** to continue.
- h) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.
- i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup Restore Job Sets** table. Then click on the job set you want.

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

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

#### Note

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

### Step 3

#### To restore from a backup file:

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

#### Attention

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

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

- Restore the backup taken for NSO (only possible if the backup was created with NSO).
- Move the devices associated with MDT collection DOWN and UP in Device Management.

- Detach and attach devices to the Crosswork Data Gateway pool.

## Restore Cisco Crosswork 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 must deploy a new cluster first, following the instructions in [Cisco Crosswork Network Controller 6.0 Installation Guide](#).

If your cluster only has one malfunctioning hybrid node, or one or more malfunctioning 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 the [Manage the Crosswork Cluster, on page 7](#) chapter in this guide.

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. 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 7](#) chapter in this guide.

When conducting a data disaster recovery, note the following:

- Before performing the **Data Disaster Restore**, the exact versions of the applications that were present in your old Crosswork cluster (when you made the data backup) must be installed and available in your new Crosswork cluster. Any mismatch in the build versions of the applications can result in data loss and failure of the restore job.
- 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.
- Smart licensing registration for Crosswork applications are not restored during a disaster restore operation, and must be registered again.

To perform a disaster recovery:

### Before you begin

Get the full name of the backup file you want to use in your disaster recovery from the SCP backup server. 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`.

## Procedure

---

- Step 1** From the main menu of the newly deployed cluster, choose **Administration > Backup and Restore**.
- Step 2** Click **Actions > Data Disaster Restore** to display the **Data Disaster Restore** dialog box with the remote server details pre-filled.
- Step 3** In the **Backup File Name** field, enter the file name of the backup from which you want to restore.
- Step 4** Click **Start Restore** to initiate the recovery operation.

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

---

# Crosswork Data Gateway Disaster Recovery Scenarios

This section explains the various scenarios to restore the CrossworkData Gateways after Cisco Crosswork recovers from a disaster.

Cisco Crosswork's disaster recovery process restores the CrossworkData Gateways in the network automatically. The following procedures are required only in case the CrossworkData Gateway VMs have been deleted from Cisco Crosswork.

- [Crosswork Data Gateway Disaster Recovery with High Availability, on page 120](#): All active and standby Crosswork Data Gateway VMs in a pool have the **Operational state** as **Error**.
- [Crosswork Data Gateway Disaster Recovery without High Availability, on page 122](#): A pool that has only one Crosswork Data Gateway VM, or a pool that has multiple active Crosswork Data Gateway VMs in the **Error** state without any standby VMs.

## Crosswork Data Gateway Disaster Recovery with High Availability

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

## Before you begin

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



**Note** Do not redeploy the data gateways before verifying that Crosswork is fully restored and all the pods are healthy.

## Procedure

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

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

**Step 2** Log in to Cisco Crosswork.

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

**Step 4** Select and edit the pool to remove (unassign) the standby VM from the pool. See [Manage a Crosswork Data Gateway Pool, on page 44](#)

**Step 5** Change the **Administration State** of the standby VM to the **Maintenance** mode. See [Change the Administration State of Cisco Crosswork Data Gateway Instance, on page 48](#).

**Note**

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

In the dg-manager logs:

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

In the controller-gateway logs:

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

To rectify the problem, you can switch the Data Gateway to the **Maintenance** mode or manually re-enroll the gateway. For more information, [Re-enroll Crosswork Data Gateway](#).

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

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

**Step 7** Repeat steps 4 to 7 to restore the (now) standby VM that has the **Operational State** as **Error**.

**Step 8** Verify the following:

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

- Collection jobs are running as expected.

## Crosswork Data Gateway Disaster Recovery without High Availability

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

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

### Before you begin

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

### Procedure

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

- Log in to Cisco Crosswork.
- Navigate to **Administration > Data Gateway Management > Data Gateways**.
- Delete the existing pool.
- Change the **Administration State** of the VM to the **Maintenance** mode. See [Change the Administration State of Cisco Crosswork Data Gateway Instance, on page 48](#).
- Install a new Crosswork Data Gateway VM with the same information as the older VM.
- Change the **Administration State** of the VM to **Up** from **Maintenance**.

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

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

Verify the CrossworkData Gateway has the **Operational State** as **Up**

- Attach devices to the Data Gateway. See [Attach Devices to a Crosswork Data Gateway, on page 39](#).
- Verify that collection jobs are running as expected.

#### Step 2 Detach devices or move devices to another Data Gateway in the network

- Log in to Cisco Crosswork.
- Navigate to **Administration > Data Gateway Management > Data Gateways**.
- Detach devices from the VM or move devices to another Data Gateway that is operationally **Up**. See [Manage Cisco Crosswork Data Gateway Device Assignments, on page 46](#).
- Delete the existing pool.

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

- e) Change the **Administration State** of the VM to the **Maintenance** mode. See [Change the Administration State of Cisco Crosswork Data Gateway Instance, on page 48](#).
- f) Reboot the VM. With this step, the VM is unassigned from the pool.

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

**Note**

You can also manually re-enroll the VM with Cisco Crosswork from the Interactive Console of the Data Gateway VM. See [Re-enroll Crosswork Data Gateway, on page 448](#).

- g) Create a new pool with the same name as the older pool and add the VM to the pool.
- h) Verify the CrossworkData Gateway has the **Operational State** as **Up**.
- i) Attach devices or move devices back to this Data Gateway. See [Manage Cisco Crosswork Data Gateway Device Assignments, on page 46](#).
- j) Verify that collection jobs are running as expected.

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

**Note**

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

- a) Install a new CrossworkData Gateway VM.
- b) Log in to Cisco Crosswork.
- c) Navigate to **Administration > Data Gateway Management > Pools**.
- d) Select and edit the pool to add the newly installed VM to the pool. See [Manage a Crosswork Data Gateway Pool, on page 44](#)

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

- e) Edit the pool and remove the (now) standby VM from the pool.
- f) Change the **Administration state** of the standby VM to **Maintenance** mode. See [Change the Administration State of Cisco Crosswork Data Gateway Instance, on page 48](#).

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

**Note**

You can also manually re-enroll the VM with Cisco Crosswork from the Interactive Console of the Data Gateway VM. See [Re-enroll Crosswork Data Gateway, on page 448](#).

- g) Edit the pool again and add the standby VM to the pool.
- h) Verify the CrossworkData Gateway is operationally **Up** and the pool has an active and standby VM.
- i) Verify the following:
  - Devices are attached to active VM in the pool.
  - Collection jobs are running as expected.

# Resolve SR-TE Policies and RSVP-TE Tunnels

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

Crosswork provides APIs to help clear these orphans. To get a list of orphan SR-TE policies or RSVP-TE tunnels use **cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** or **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** where **is-orphan=True** and default action is GET. To make the orphans manageable again, use a SAVE action for the corresponding URL per policy type. For more information see [API documentation on Devnet \(Crosswork Optimization Engine APIs > 6.0 Release APIs\)](#).

# Backup Cisco Crosswork with Cisco NSO

You have the option to create backup of only Crosswork or create a backup that also captures a copy of the NSO CDB (the default data store for configuration data in NSO). The ability to backup the CDB requires your Crosswork user account to meet specific requirements detailed here and in the [Add Cisco NSO Providers, on page 174](#) section.



**Note** While the backup can be automated (as described), the restore of the NSO CDB is a manual process (see [Restore Cisco Crosswork with Cisco NSO, on page 125](#)).

## 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:

- Ensure that SSH is enabled on the NSO provider configuration.
- The user ID associated with the SSH connectivity type in the credential profile assigned to the NSO provider has sudo permissions.
- The NSO server has NCT ([NSO Cluster Tools](#)) installed, and the user in the credential profile for the NSO provider can execute `nct` commands.

- The user in the NSO provider's credential profile has full access to the NSO server's backup folder and the files in it. This requirement usually means full read and write access to the NSO server's `/var/opt/ncs/backups/` folder.

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

In addition to these special requirements, the normal guideliness for backups discussed in [Manage Cisco Crosswork Backup and Restore, on page 116](#) also apply to backups containing NSO data.

## Procedure

---

### Step 1 Configure an SCP backup server:

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

### Step 2 Create Cisco Crosswork and Cisco NSO backups:

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

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

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

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

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

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

---

## Restore Cisco Crosswork with Cisco NSO

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

## Restore Cisco Crosswork with Cisco NSO

- 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.



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

### Before you begin

Get the full name of the backup file you want to restore from the SCP server. This file will contain both the 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`.

## Procedure

- 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_nsol21.backup.gz NS0_RESTORE_PATH_nsol21
[root@localhost nsol21]# more NS0_RESTORE_PATH_nsol21
/var/opt/ncs/backups/
[root@localhost nsol21]#
...
```

**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_nsol21.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.

## Migrate Data Using Backup and Restore

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

Follow these guidelines whenever you create a data migration backup:

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

### Before you begin

Ensure that you have:

- The hostname or IP address and the port number of a secure SCP server.
- A file path on the SCP server, to use as the destination for your data migration backup files.
- User credentials for an account with file read and write permissions to the remote path on the destination SCP server.

## Procedure

---

### Step 1 Configure a SCP backup server:

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

### Step 2 Create a backup:

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

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

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

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

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

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

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

- Log in as an administrator on the Cisco Crosswork installation to which you want to migrate data from the backup.
- From the main menu, choose **Administration > Backup and Restore**.
- Click **Actions > Data Migration** to display the **Data Migration** dialog box with the remote server details pre-filled.
- In the **Backup File Name** field, enter the file name of the backup from which you want to restore.
- Click **Start Migration** to initiate the data migration. Cisco Crosswork creates the corresponding migration job set and adds it to the job list.

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

### Step 4 Deploy Crosswork Data Gateway:

- a. After the migration is complete, log out from the Crosswork UI and log in again to the UI using [https://<new\\_crosswork\\_ip>:30603](https://<new_crosswork_ip>:30603).  
The **Action to be taken** pop-up appears with the message **Please Acknowledge once redeploy of the CDGs is done**.
- b. In the **Action to be taken** pop-up, click **Cancel**.
- c. Delete the old data gateway VMs and install new gateways. Ensure that they have the identical IPs and names as the previous gateway VMs.
- d. Verify that the deployment of the data gateway is complete, and the gateway is registered with Crosswork Network Controller.
- e. Verify that the data gateway is in the same state as it was before the upgrade by choosing **Administration > Data Gateway Management > Virtual Machines**. The **Operation** and **Administration** state of the data gateways should be UP.
- f. After all the data gateways are active, navigate to **Administration > Data Gateway Management > Pools** page to verify the successful migration of all pools from the previous cluster version and ensure that data gateways are automatically enrolled with Crosswork Network Controller.
- g. Log out from the Crosswork UI and log in back to the UI using [https://<new\\_crosswork\\_ip>:30603](https://<new_crosswork_ip>:30603). The **Action to be taken** pop-up appears.

**Note**

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

- h. In the pop-up, click **Acknowledge**. With this step, the migration should be complete.
  - i. If the NSO is set to the read-only mode, disable it.
-





## CHAPTER 5

# Set Up and Use Your Topology Map for Network Visualization

---

- [Overview of the Topology Map, on page 131](#)
- [Use Device Groups to Filter your Topology Map, on page 135](#)
- [View Device Details from the Topology Map, on page 139](#)
- [Get Details About Topology Links, on page 143](#)
- [Import and Export Geographical Data, on page 150](#)
- [Customize your Map for your Needs, on page 151](#)
- [Troubleshoot your Topology Map, on page 156](#)

## Overview of the Topology Map

You can view the network devices and their connections in different ways on the topology map.

You can choose between a logical map or a geographical map, depending on your preference. The logical map arranges the devices and links based on an algorithm that you can modify, without considering their physical location. You can view up to 5000 devices on the logical map.

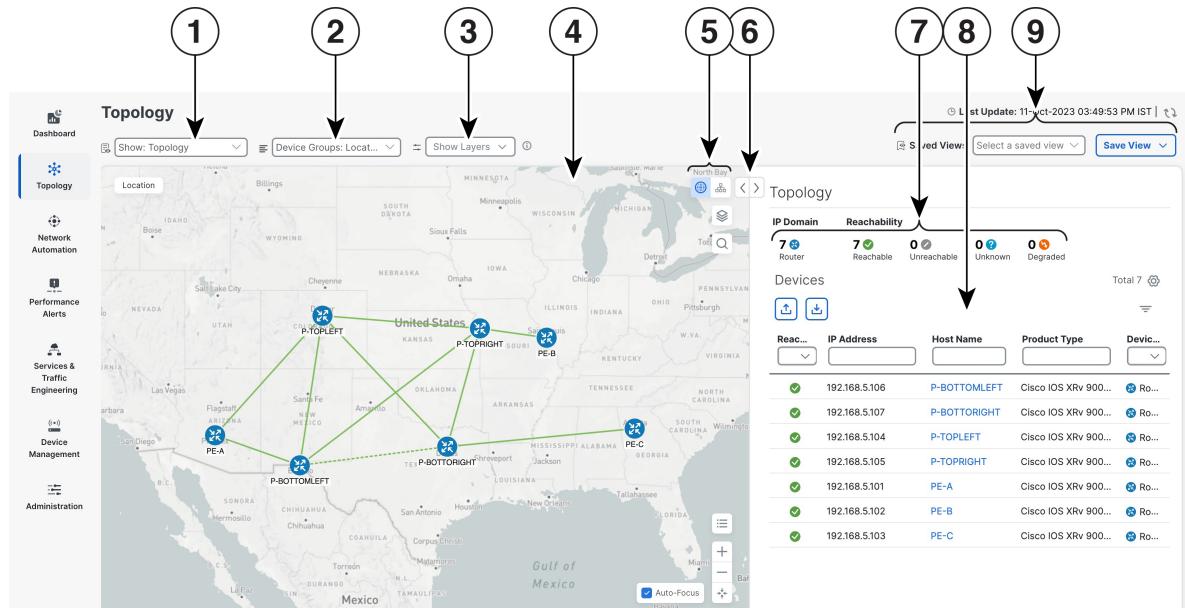
The geographical map places the devices, clusters, links, and tunnels on a world map, using the GPS coordinates of each device from the device inventory.

To use the topology map, you have to onboard the devices on the system first, for more information refer to [Add Devices to the Inventory, on page 205](#).

You can also filter your topology view by creating device groups. For more information, refer to [Use Device Groups to Filter your Topology Map, on page 135](#).

## Overview of the Topology Map

Figure 55: Topology Home page



522060

Callout No.	Description
1	<p><b>Topology Map View:</b> From the <b>Show</b> drop-down list, click the option that displays the data that you would like to see on the map.</p> <p>You can view the following options.</p> <ul style="list-style-type: none"> <li>• Topology</li> <li>• Traffic Engineering</li> <li>• VPN Services</li> <li>• Transport Slicing</li> </ul>
2	<b>Device Groups:</b> From the drop-down list, click the group of devices you want to display on the map. All other devices will be hidden.
3	<b>Show Layers:</b> From the drop-down list, click the network layers you want displayed on the map. All devices and links that belong to the selected layers are then displayed. By default, all layers are displayed.

Callout No.	Description
4	<p><b>Topology Map:</b> The topology map can be displayed on a logical map or a geographical map, where the devices and links are shown in their geographic context. From the map, you can drill down to get detailed information about devices and links.</p> <p><b>Devices:</b></p> <ul style="list-style-type: none"> <li>• To view basic device information, hover the mouse pointer over the device icon. A pop up window displaying the host name, state, node IP, and device type appears.</li> <li>• To view device details, click on the device icon. For more information see, <a href="#">View Basic Device Details, on page 139</a></li> </ul> <p><b>Note</b> If you have installed Element Management Functions, the following additional information will be displayed in the Device Details screen.</p> <ul style="list-style-type: none"> <li>• Alarm information under Summary in the <b>Details</b> tab.</li> <li>• An <b>Alarms</b> tab displaying information such as severity, source, category, and condition of the alarms. The columns can be customized based on your preferences.</li> <li>• An <b>Inventory</b> tab displaying the product name, product id, admin status, oper status, and serial number. The columns can be customized based on your preferences.</li> </ul> <p>You can enable alarm visualization using the <b>Show Alarms</b> option on the <b>Alarms</b> tab and set a severity filter to show only the alarms of the selected severity or higher. Once enabled, the alarm notification icon will be displayed on the devices in the topology map in case of an alarm.</p> <p><b>Links:</b></p> <ul style="list-style-type: none"> <li>• A solid line indicates a <i>single link</i> between two devices. A dashed line indicates an <i>aggregated link</i> that represents more than one link, or the use of multiple protocols (for example, IPv4 and IPv6) on the same physical link. To configure the dashed link, refer to <a href="#">Differentiate Aggregated Links from Single Links, on page 153</a>.</li> </ul> <p>For easy identification, you can color links on the map based on criteria such as link down and utilization. For more information, refer to <a href="#">Differentiate all Down Links by Color, on page 154</a> and <a href="#">Show Link Utilization by Color, on page 155</a>.</p> <ul style="list-style-type: none"> <li>• A and Z indicates headend and endpoint, respectively.</li> <li>• To view link information details, click on the link, and the <b>Links</b> panel is displayed on the right-hand side with information.</li> </ul>

Callout No.	Description
5	 The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm.
	 The geographical map shows single devices, device clusters, and links, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory.
	 The Display Preferences window allows you to change display settings for devices, links.
	<b>Note</b>
	<p>If you have installed Element Management Functions, you can also change the display preferences for the alarms. You can enable alarm visualization using the <b>Show Alarms</b> option and set a severity filter to show only the alarms of the selected severity or higher. Once enabled, the alarm notification icon will be displayed on the devices in the topology map in case of an alarm.</p>
	<b>Note</b>
	<p>Settings changes only apply to the current session and will revert to the defaults when you log out and log in again. To retain your changes for future use, save your view before logging out.</p>
	 The global search allows you to search the topology using device names, location or the device civic location.
6	<b>Expand/Collapse/Hide Side Panel:</b> Expand or collapse the contents of the side panel. Close the side panel to get a larger view of the topology map.
7	The <b>Mini Dashboard</b> provides a summary of the IP Domain and device reachability status. If filters are applied, the <b>Mini Dashboard</b> is updated to reflect what is displayed in the Devices table.
	<b>Note</b>
	<p>If you have installed Element Management Functions, the <b>Alarm Severity</b> information is displayed in the Mini Dashboard and a <b>Severity</b> column is added to the Devices table. You can refine the table based on the severity value. The Alarm Status feature is available for select licensing packages.</p>
8	The content of this window changes depending on what applications you have installed, what <b>Show</b> is set to for the topology map and if you have selected to view more information on the device.
9	<b>Saved Custom Map Views:</b> Lets you create a named custom view using the settings and layout for your current map, settings of the tables saved in the saved views, or display a custom view you have created previously.


**Note**

Crosswork Network Controller (CNC) 6.0 requires ENTITY-MIB, Interface-MIB, and SYSTEM-MIB for detailed inventory with Element Management Functions for third-party devices. Ensure support for these MIB's for compatibility for CNC's inventory collection features.

## Use Internal Maps Offline for Geographical Map Display

The system is set up by default to get the geo map tiles from a specific Mapbox URL through a direct Internet connection. If you do not have an Internet connection and therefore the system cannot access an external map provider to retrieve geographical map tiles, you can upload internal map files to represent the areas of the world you require for your network. These map files must be downloaded from Cisco.com and then uploaded into the system. The name of the map file indicates the area of the world it contains, for example, **africa-geomaps-1.0.0-for-Crosswork-x.x-signed.tar.gz**. If you will be managing a network in a specific part of the world, upload only the relevant map files. You do not need to upload all available map files.



**Note** If you choose to work offline with internal maps and you do not upload map files, your geographical map will display as a generic world map without details of cities, streets, and so on.

To use internal maps to display the geographical map:

### Before you begin

Download the required map files from Cisco.com and place them on an accessible server. The server must support SCP protocol for file transfer.

### Procedure

**Step 1** From the main menu, choose **Administration > Settings > System Settings**.

**Step 2** Under **Topology**, click the **Map** option.

**Step 3** Select the **Work offline with internal maps** radio button and click **Manage**.

**Step 4** In the Manage Internal Maps dialog, click



to upload a new map file. Note that you can upload one file at a time.

**Step 5** In the Upload Map File dialog, browse to the location of the map file you downloaded so that the system can access the file.

**Step 6** Click **Upload**.

The system uploads the map from the specified location. The upload process might take some time and must not be interrupted by closing the browser or clicking **Cancel**. When the process is complete, the new map appears under **Uploaded Maps** in the Manage Internal Maps dialog.

**Step 7** Upload additional maps, as required.

## Use Device Groups to Filter your Topology Map

Device groups let you organize and manage your devices according to your needs. You can use device groups to filter and display data from specific devices on your dashboard. Device groups also allow you to visualize and zoom in on data specific to a particular group of devices. It reduces the clutter on your screen and allows you to focus on data that is most important to you.

## Create Device Groups Individually

# Create Device Groups Individually

You can create device groups and add devices to the groups either manually (as described in this section) or automatically, as described in [Create Rules for Dynamic Device Grouping, on page 136](#). A device can belong to only one device group.

**Figure 56: Device Groups**

Device IP	Host Name	Product Type
192.168.15.63	CL3-P-BOTTOM-LEFT	Cisco IOS Xrv 9000 Router
192.168.15.64	CL3-P-BOTTOMRIGHT	Cisco IOS Xrv 9000 Router
192.168.15.67	Node3	Cisco IOS Xrv 9000 Router

## Procedure

- Step 1** From the main menu choose **Device Management > Device Groups**. We see that the East Coast device group has been selected. Also note that only the devices belonging to the East Coast device group are listed in the devices table in the right pane.
- Step 2** To add a new sub-group, click the three dots next to any group and then click **Add a Sub-group**.
- Step 3** Fill in the details and click **Create**.  
A new sub-group is added under the selected parent group.

# Create Rules for Dynamic Device Grouping

You can create a rule to dynamically create device groups and automatically add unassigned devices to these groups using a Regular Expression (regex) on the device host name or IP address. Any newly added or discovered devices that match the rule will be placed in the appropriate group.

Dynamic rules do not apply to devices that already belong to groups. You must move them to Unassigned Devices if you want them to be considered by the rule.

## Before you begin

While you can follow examples given in the Dynamic Groups dialog, it is helpful to be familiar with Regular Expressions.

## Procedure

- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** Click next to **All Locations > Manage Location Dynamic Groups**.

- Step 3** Click **Show more details and examples** to help you fill out the required host name or IP address.
- Step 4** If there are any existing devices in the Unassigned Devices group, click **Test Rule** to view a sampling of what type of group names will be created.
- Step 5** Turn the **Enable Rule** toggle ON to enable the rule. After the rule is enabled, the system checks for unassigned devices every minute and will assign them to the appropriate group based on the rule.
- Step 6** Click **Save**.
- Step 7** Groups that are created this way initially appear under Unassigned Groups (created when a rule is enabled for the first time). Move newly created groups to the desired group hierarchy.
- 

## Modify Device Groups

You can modify device groups to add or edit the device group details. You can change the group name, or assign a different parent group.

### Procedure

---

- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** To edit the group details, click the three dots next to the group name and then click **Edit Group Properties**. You can update the parent group, group name and the description.
- Step 3** Click **Save**.
- 

## Delete Device Groups

You can delete a device groups from the system. This will unassign all the devices that belong to that group and make them available for other groups.

### Procedure

---

- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** To delete the device group, click the three dots next to the group name and then click **Delete Group**.
- Step 3** On the **Delete Group** pop-up, click **Delete** to confirm your deletion.
- 

## Move Devices from One Group to Another

If you need to reorganize your devices, you can move them from one group to another.

**Procedure**

- 
- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** Select the group from which you wish to move the devices.
- Step 3** Select the devices from the right pane.
- Step 4** From the **Move** drop-down, select the appropriate group and click **Move**. You can also create a new group to which you can move your selected devices. For more information refer to [Create Device Groups Individually, on page 136](#)
- 

## Import Multiple Device Groups

When you import device groups from a CSV file, the import process creates new device groups that does not exist in the database, and updates the existing device groups that have the same data as the imported ones. This means that you might lose some of your original data if you import device groups without backing them up first. Therefore, we recommend that you export a copy of all your current device groups before you perform an import.

**Procedure**

- 
- Step 1** From the main menu, choose **Device Management > Device Groups**.
- Step 2** Click  to open the **Import Groups** dialog box.
- Step 3** If you have not already created a device groups CSV file to import:
- Click the **Download device groups (\*.csv)' template** link and save the CSV file template to a local storage resource.
  - Open the template using your preferred tool. Begin adding rows to the file, one row for each device group.
- Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank.
- Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.
- When you are finished, save the new CSV file.
- Step 4** Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.
- Step 5** With the CSV file selected, click **Import**.

**Note**

While importing device groups using a CSV file, you should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries.

## Export Multiple Device Groups

You can export the device groups details to a CSV file. This is useful for creating a record of all the device groups in the system at a given time. You can also modify the CSV file as you wish, and import it back to update the existing data.

### Procedure

- 
- Step 1** From the main menu, choose **Device Management > Device Groups**.
- Step 2** Click  to export the device groups in CSV format. The CSV file is then downloaded in your systems download folder.
- 

## View Device Details from the Topology Map

The topology map lets you view the information of any device in your network. You can see various details, such as device specifications, routing configurations, and device links. The topology map enables you to monitor and manage your network devices with ease and efficiency.

## View Basic Device Details

You can view the basic device details and its connections in a graphical way. It displays the host name, type, status, and IP address. The map also allows you to adjust the view of the device by zooming in and out, panning, and rotating.



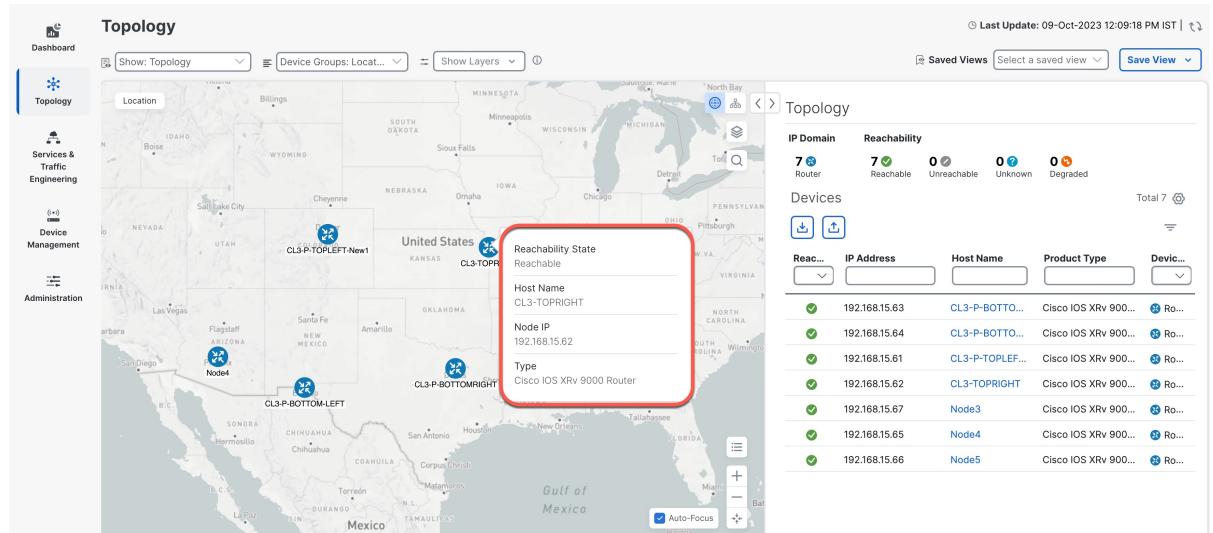
- 
- Note** If you are viewing the HTML version of this guide, click on the images to view them in full-size.
- 

### Procedure

- 
- Step 1** From the main menu choose **Topology**.
- Step 2** Hover the mouse over the device icon, to quickly view the host name, reachability state, IP address and type of device.

## View All Device Details

Figure 57: Basic Device Details



## View All Device Details

The device icon on your topology map lets you view more details about your device, such as where it is located, what kind of device it is, when it was last updated and more.

### Procedure

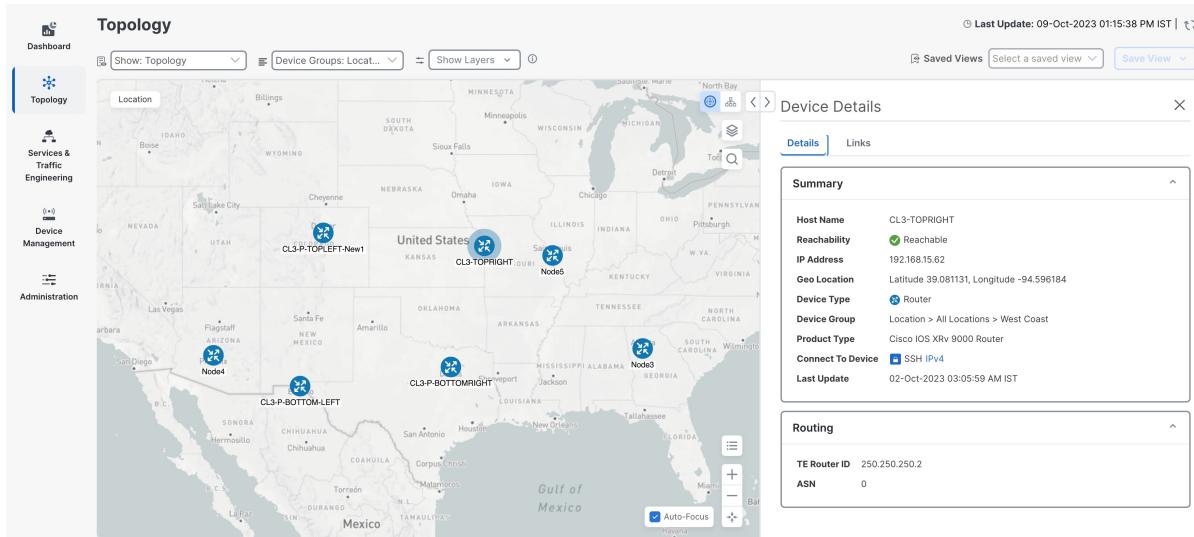
#### Step 1

From the main menu choose **Topology**.

#### Step 2

To view device details, click on the device icon. The following example shows the Device Details in the right pane under the Details tab.

Figure 58: Device Details

**Note**

If you have installed Element Management Functions, the following additional information will be displayed in the Device Details screen.

- Alarm information under Summary in the **Details** tab.
- An **Alarms** tab displaying information such as severity, source, category, and condition of the alarms. The columns can be customized based on your preferences.
- An **Inventory** tab displaying the product name, product id, admin status, oper status, and serial number. The columns can be customized based on your preferences.

## Identify Device Routing Details

Device routing determines how data packets are transmitted from one device to another in the network and ensures that data packets reach their intended destination, avoiding congestion or loops in the network.

**Note**

If you are viewing the HTML version of this guide, click on the images to view them in full-size.

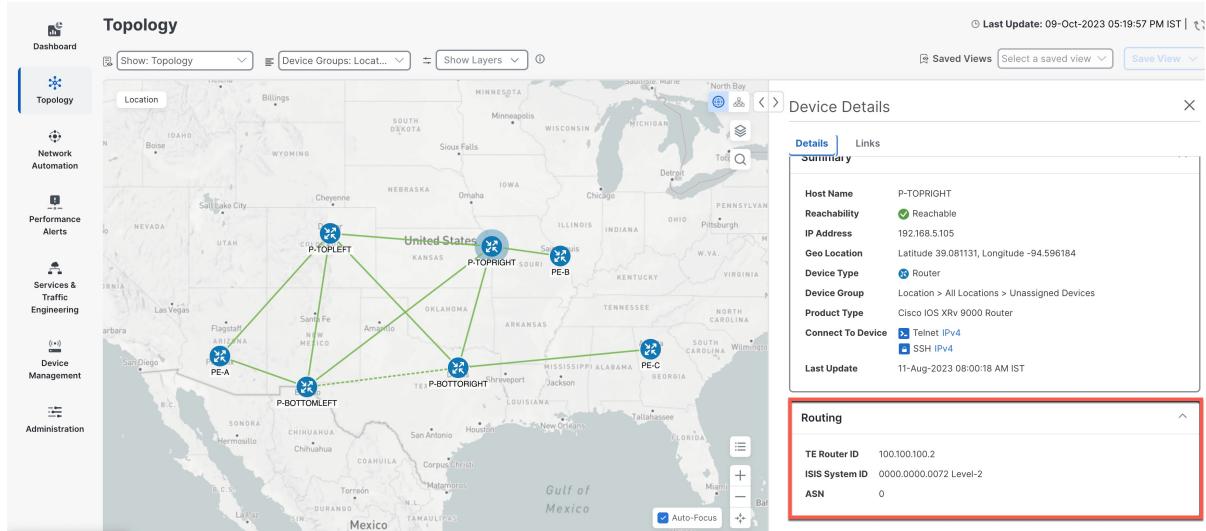
### Procedure

**Step 1** From the main menu choose **Topology**.

**Step 2** To view the device routing details, on the topology map, click the device icon. You can view the routing details in the right pane.

## Identify the Links on a Device

Figure 59: Device Routing Details



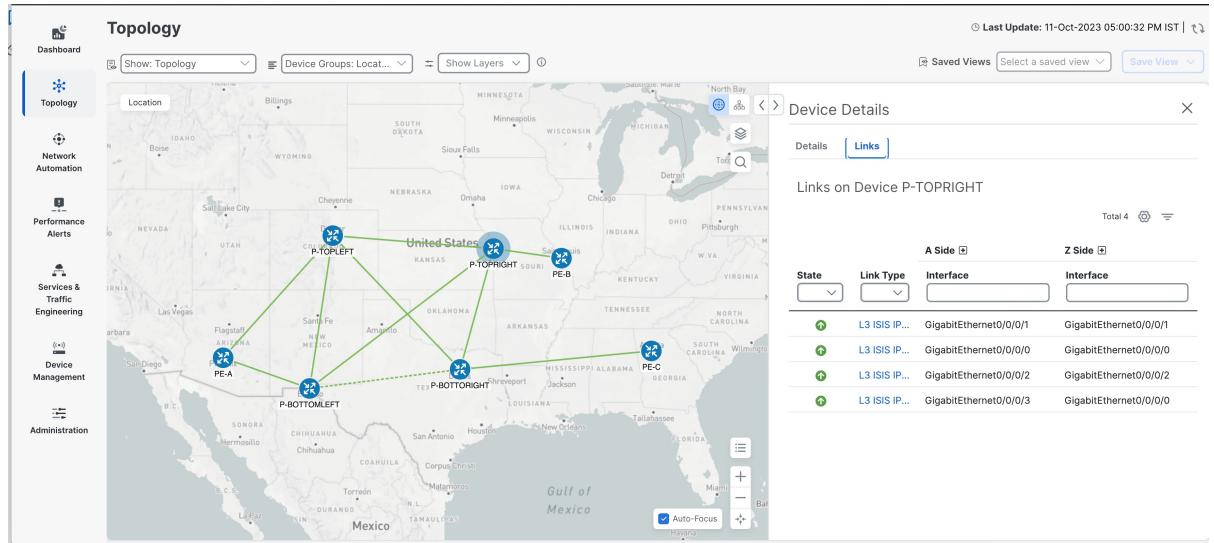
## Identify the Links on a Device

You can see which links are connected to the device in the **Links** tab in the Device Details pane.

### Procedure

- Step 1** From the main menu choose **Topology**.
- Step 2** To view links on the device, click on the device icon.
- Step 3** In the right pane, click the **Links** tab and expand the right panel to view all the link details.

Figure 60: Links on a Device



## Get Details About Topology Links

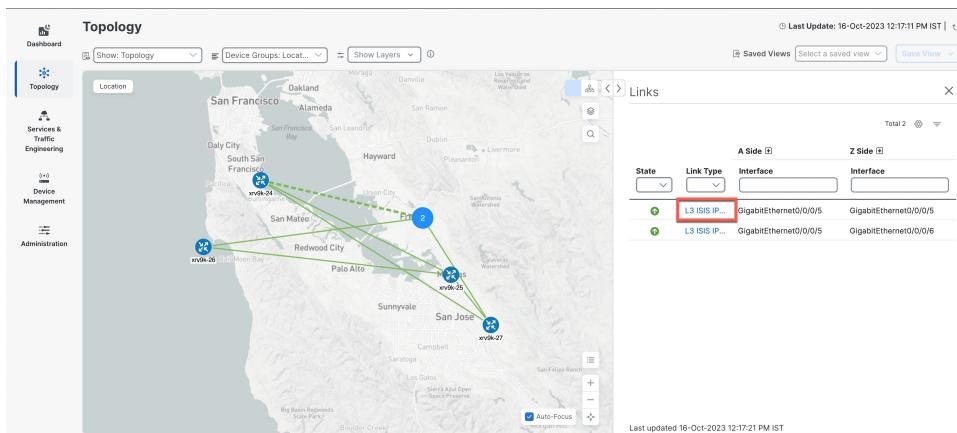
You can view detailed information about any link on the topology map, such as the link name, source and destination devices, link status, bandwidth, latency, and link details. You can also view link utilization to see how much bandwidth the link is using, as well as packet drops and traffic volume.

## View Link Details

You can view the link details such as name, state, type, and endpoint interface information for each link. For more information on the link state, refer to [Link States and Discovery Methods, on page 147](#)

### Procedure

- Step 1** From the main menu choose **Topology**.
- Step 2** Click a link on the topology map.

**View Link Details****Figure 61: Link Type**

**Step 3** Under the **Link Type** column, click the link entry to see the link's details.

Figure 62: Link Details

The screenshot shows the 'Link Details' interface with a 'Summary' tab selected. The summary table includes the following data:

Name	GigabitEthernet0/0/0/0-GigabitEthernet0/0/0/1	
State	Up	
Link Type	L3 ISIS IPv4	
ISIS Level	2	
Last Update	10-Oct-2023 01:04:09 AM IST	

Below the summary is a table comparing 'A Side' and 'Z Side' interface details:

	A Side	Z Side
Node	xrv9k-23	xrv9k-27
TE Router ID	192.168.0.23	192.168.0.27
IPv6 Router ID	2001:192:168::23	2001:192:168::27
IF Name	GigabitEthernet0/0/0/0	GigabitEthernet0/0/0/1
IF Description	GigabitEthernet0/0/0/0	GigabitEthernet0/0/0/1
IF Alias		T-SDN Interface
Type	ETHERNETCSMACD	ETHERNETCSMACD
IP Address	10.0.0.41	10.0.0.42
Utilization	0% (2.74Kbps/1Gbps)	0% (1.6Kbps/1Gbps)
Packet Drops	0%	0%
IGP Metric	10	10
Delay Metric	10	10
TE Metric	10	10
Admin Groups	2,5	2,5

#### Step 4 View aggregate link details.

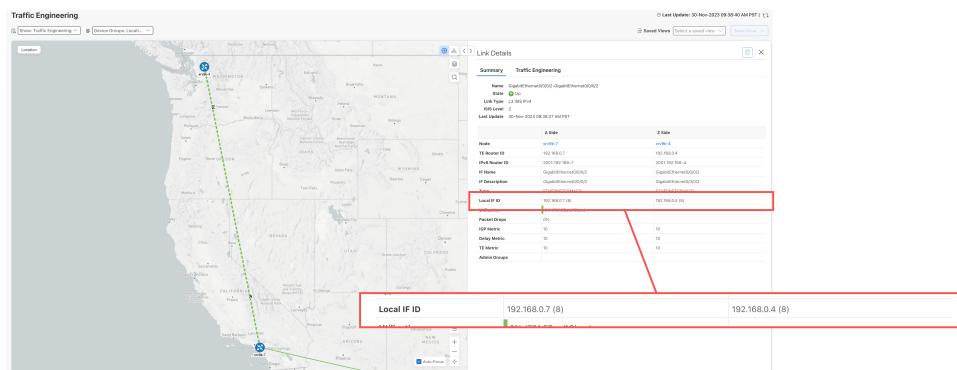
Click on a dashed line. A dashed line indicates an aggregated link that represents more than one link.

##### Note

Dual stack links (although aggregate) are shown as one single line.

#### Step 5 View IPv4 unnumbered interface information (if available).

IPv4 unnumbered interfaces information is displayed as a combination of the TE Router ID and the index.

**View Link Interface Metrics****Figure 63: IPv4 Unnumbered Interface****View Link Interface Metrics**

Link interface metrics are a set of indicators that measure the performance and quality of the communication between two or more network devices. They include parameters such as bandwidth, delay, jitter, packet loss. Link interface metrics can help network administrators to monitor and troubleshoot network issues, optimize network resources, and plan for future network expansion or upgrade.

**Procedure**

**Step 1** From the main menu choose **Topology**.

**Step 2** Click a link on the topology map.

**Step 3** To view interface utilization, expand **A side** or **Z side**.

The utilization shown on IPv4 and IPv6 links represents the aggregate traffic and packet drops on the interface, not specific to each address family. Sub-interfaces will not show a utilization since they do not have a bandwidth like a physical interface. Traffic measurements will still be collected and displayed.

**Note**

If you have Service Health installed, you can also view Delay and Jitter information in the link interface metrics table.

**Figure 64: Link Interface Metrics**

## Link States and Discovery Methods

**Table 8: Link Types, Discovery and States**

Link Type	Discovery	Link State
L3 link (ISIS, OSPF and eBGP)	via SR-PCE	SR-PCE set it to UP or DOWN based on the link operational state
L2 link (CDP, LLDP, LAG)	via SNMP MIB: CDP, LLDP and LAG	<p>The link state is based on the two link endpoints operational states (via IF MIB).</p> <ul style="list-style-type: none"> <li>Link state is UP when initially discovered.</li> <li>When one of the endpoint interfaces is operationally down, then the link state is set to DOWN.</li> <li>When both endpoint interfaces are operationally up, then the link state is set to UP.</li> </ul>

The table below lists the link state and its definition:

**Table 9: Link State Definitions**

Link State	Description
UP	Link state is UP when discovered in both directions.
DEGRADED	Link state is UP in only one direction.
DOWN	Link is reported down in both directions.

## Protocols Used for Topology Services

The following table lists the protocols and methods used for obtaining the topology information.

## Enable or Disable Topology Link Discovery

Protocol/Method	Provides	Use Cases
IGP/ BGP-LS (via SR-PCE)	Real time topology (nodes, links, link metrics, and so on.)	L3 topology visualization
PCEP (via SR-PCE)	Real time LSP status and CRUD of SR-PCE initiated LSPs	<ul style="list-style-type: none"> <li>SR/SRv6, RSVP-TE LSP visualization</li> <li>SR-PCE initiated LSP create/update/delete</li> </ul>
SNMP (SNMPv2-MIB, IP-MIB, IF-MIB, LLDP-MIB, (CISCO CDB-MIB) (via CDG)	System info, interface table (interface and SR-TE/RSVP-TE traffic Utilization) IP address table, L2 adjacency information	Device management and details and Crosswork Optimization Engine model building: <ul style="list-style-type: none"> <li>L2/L3 topology</li> <li>Interface name, admin/oper status</li> <li>Interface and SR policy and RSVP-TE tunnel utilization</li> </ul>
CLI (via CDG) - show mpls	TE router ID and so on.	To match the DLM node with the same TE router ID that is learned from the SR-PCE

## Enable or Disable Topology Link Discovery

To control the visibility of L2 topology links on the maps, you can change the system settings for the discovery of LLDP, CDP and LAG protocols. These protocols are used to identify the neighboring devices and their connections. The discovery option is disabled by default, which means the links of these protocols, including the ones that were already discovered, will not show up on the maps. You can enable the discovery option to see the links of the selected protocols on the maps.

To enable topology discovery:

### Before you begin

- Make sure all pods are healthy before changing the settings.

### Procedure

**Step 1** From the main menu, choose **Administration > Settings > System Settings**.

**Step 2** Under **Topology**, click the **Discovery** option.

**Step 3** Select the checkbox of the protocols for which you want to enable discovery.

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

When you enable discovery, the collection jobs will be created. The table below lists the collections jobs created for each protocol setting along with the sensor paths.

Table 10: Collection Jobs for each setting

L2 Configuration Setting	Helios collection Jobs ID	Context ID	MIBs collected	Sensor paths
None (default)	cw.topo_svc	cw.toposvc.snmp cw. toposvc.snmptraps	IF-MIB, IP-MIB, LAG-MIB IF-MIB:notification <b>Note</b> IF-MIB is required, but it is collected in the ICON jobs.	IP - MIB : IP-MIB / ipAddressTable / ipAddressEntry IF-MIB:notifications
CDP	cw.topo_svc	cw.toposvc.cdp	IF-MIB, CDP-MIB, LAG-MIB	CISCO - CDP - MIB : CISCO - CDP - MIB / cdpCacheTable / cdpCacheEntry CISCO - CDP - MIB : CISCO - CDP - MIB / cdpInterfaceTable / cdpInterfaceEntry
LLDP	cw.topo_svc	cw.toposvc.lldp	IF-MIB, LLDP-MIB, LAG-MIB	LLDP - MIB : LLDP - MIB / lldpLocPortTable / lldpLocPortEntry LLDP - MIB : LLDP - MIB / lldpRemTable / lldpRemEntry
LAG	cw.topo_svc	cw.toposvc.lag	IF-MIB, LAG-MIB	IEEE8023 - LAG - MIB : IEEE8023 - LAG - MIB / dot3adAggTable / dot3adAggEntry IEEE8023 - LAG - MIB : IEEE8023 - LAG - MIB / dot3adAggPortTable / dot3adAggPortEntry

The table below lists the common errors when enabling or disabling topology discovery:

Table 11: Common error scenarios:

Possible Error Scenario	Cause	Cause Recommended Action
After disabling, some of the disabled links are displayed in the maps.	A protocol that is disabled soon after being enabled may cause a problem. The system may stop the collection job for the previous enabled job before it finishes processing the SNMP data. This may lead to a mismatch between the actual and the displayed status of the links. The links that are disabled may still appear as enabled.	Enable and disable the protocol again with sufficient wait time in between, or restart robot-topo-svc. To restart the robot-topo-svc, refer to <a href="#">Monitor Platform Infrastructure and Application Health</a> .
When you try to enable discovery, the helios job fails and settings are disabled from further editing.	A possible cause of the collection job being stuck in an unsuccessful state is that the helios pod is unhealthy. Crosswork prevents users from modifying the L2 discovery settings while the collection job is in progress. This means that the collection job cannot be canceled or restarted until the helios pod is healthy again.	Ensure that the pods are healthy, and then enable and disable the protocol with sufficient wait time in between, or restart robot-topo-svc. To restart the robot-topo-svc, refer to <a href="#">Monitor Platform Infrastructure and Application Health</a> .
When you change the discovery settings, the topology UI or topology service crashes resulting in an unpredictable status.	The mechanism to disable users from further editing while the collection job is being created or deleted, relies on pods communicating via Postgres flag. If any pod crashes during this time, the Postgres flag key is not set correctly.	

## Import and Export Geographical Data

Using Keyhole Markup Language (KML) files, you can import and export the geographic location identifiers for your devices. KML is a format that encodes and stores geographic information for display on a map.

### Import Geographical Data to Keyhole Markup Language (KML) Format

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 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.

## Procedure

---

- Step 1** From the main menu, choose **Device Management > Device Groups**.
- 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:
- Click the **Download device groups (\*.csv)' template** link and save the CSV file template to a local storage resource.
  - Open the template using your preferred tool. Begin adding rows to the file, one row for each device.
- Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank.
- Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.
- 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.

---

## Export Geographical Data to Keyhole Markup Language (KML) Format

You can export geographic location identifiers for your devices to a KML file. You can use the exported data in other contexts, if required. To export a KML file, follow these steps:

## Procedure

---

- Step 1** From the main menu, choose **Topology**.
- Step 2** In the right pane, click the  to export the geographical data to a KML file. The KML file is downloaded to your system's download folder.
- 

## Customize your Map for your Needs

You can configure various visual settings in order to customize the map display for your requirements.

## Show or Hide Device State

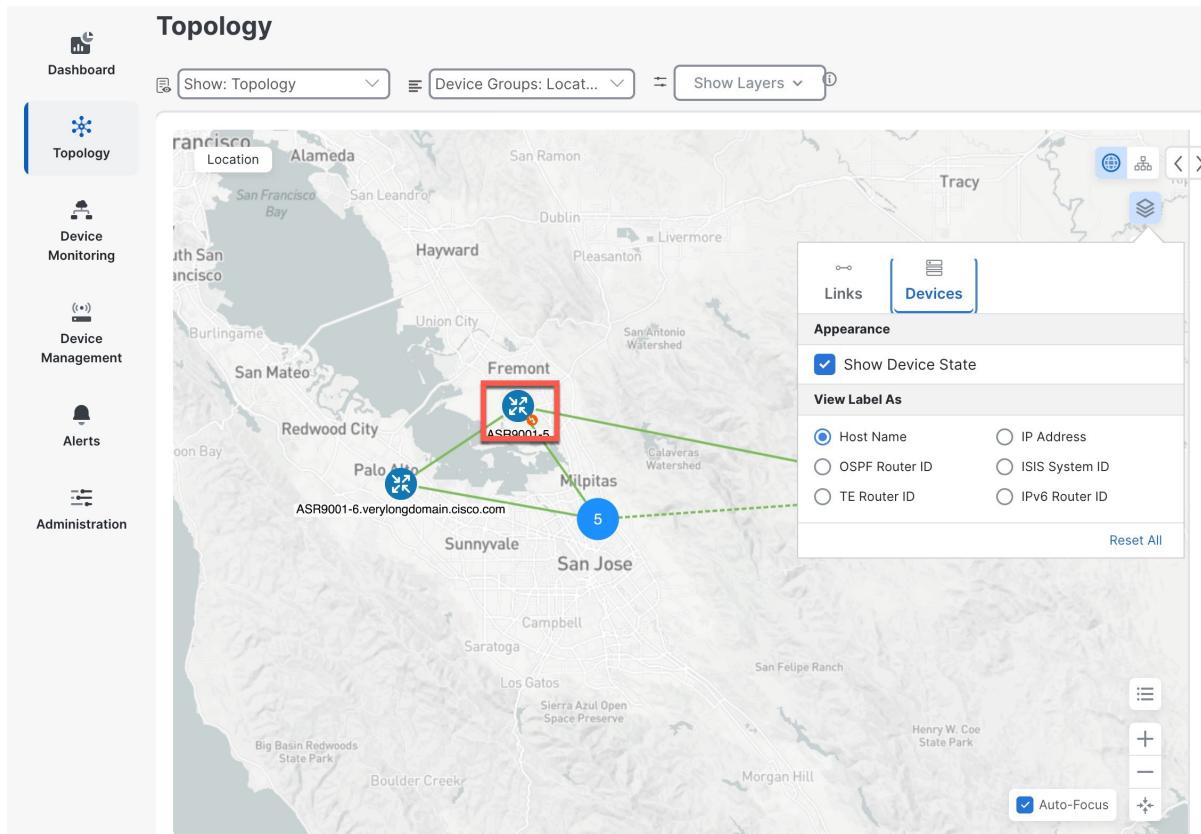
# Show or Hide Device State

This option allows you to decide whether or not to show the device state on the topology map. You can choose to show or hide the device state according to your preference.

## Procedure

- Step 1** From the main menu click **Topology**.
- Step 2** Click  on the topology map to open the **Display Preference** dialog box.
- Step 3** Click the **Devices** tab and check the **Show Device State** checkbox. By default the Device State is enabled and is shown on the map.

**Figure 65: Show or Hide Device State**



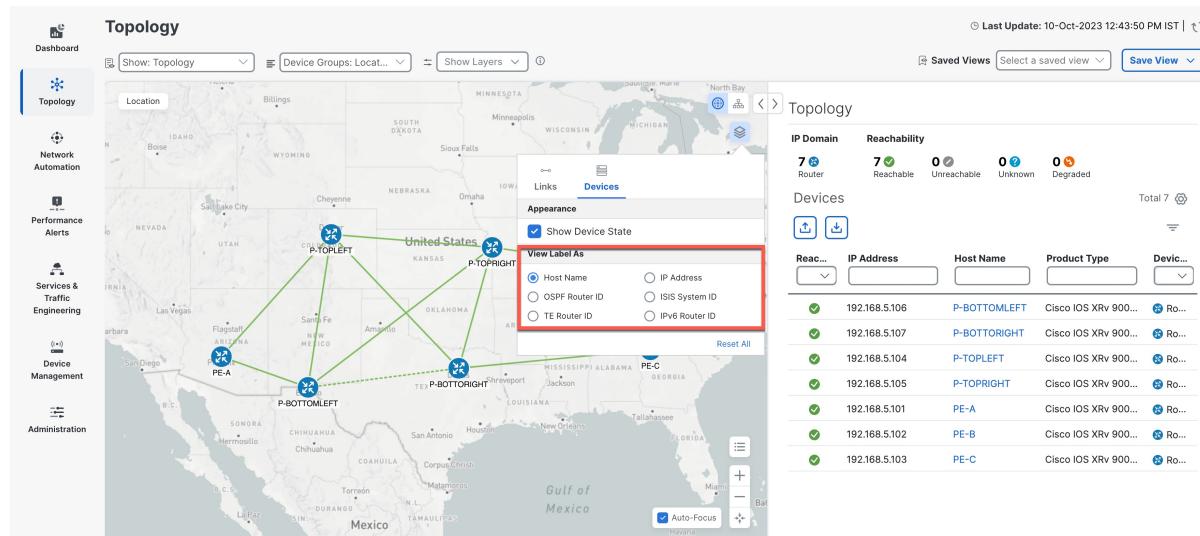
# Define the Device Label Type

You can customize how you want to identify the devices on your Network Topology. You can use different label types to identify the devices, such as IP Address, OSPF Router ID, or the default option of device host name.

## Procedure

- Step 1 From the main menu click **Topology**.
- Step 2 Click  on the topology map to open the **Display Preference** dialog box.
- Step 3 Click **Devices** tab and under **View Label As** select the desired option from the list of labels. You can select only one label for your devices.

Figure 66: Define the Device Label Type



## Differentiate Aggregated Links from Single Links

An aggregated link is a type of link that combines multiple physical links or multiple protocols, such as IPv4 and IPv6, into one logical link. This allows for better bandwidth utilization and redundancy. On the topology map, an aggregated link is shown as a dashed line, while a single link is shown as a solid line. This helps to simplify the network topology and show the logical connections between devices.



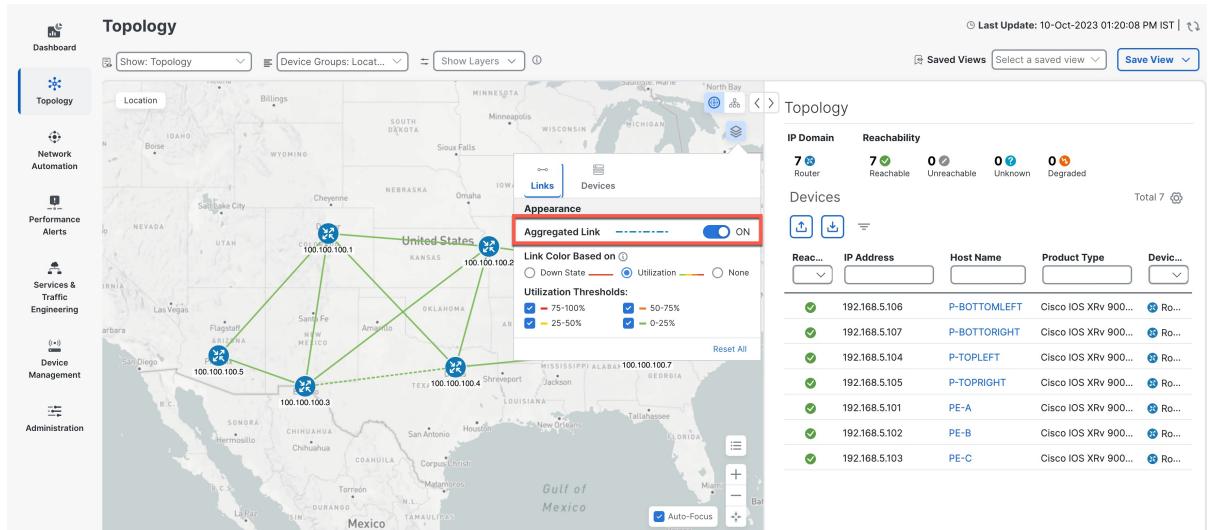
**Note** Although aggregated, dual stack links show as one single line

## Procedure

- Step 1 From the main menu click **Topology**.
- Step 2 Click  on the topology map to open the **Display Preference** dialog box.
- Step 3 Click **Links** tab, toggle to enable the **Aggregated Link** option.

## Differentiate all Down Links by Color

Figure 67: Aggregated Link



## Differentiate all Down Links by Color

To make it easier to identify the links that are not working, you can make all down links appear in red. The color will remain red regardless of the link status. This way, you can quickly identify and fix the broken links and take appropriate actions.

### Procedure

#### Step 1

From the main menu click **Topology**.

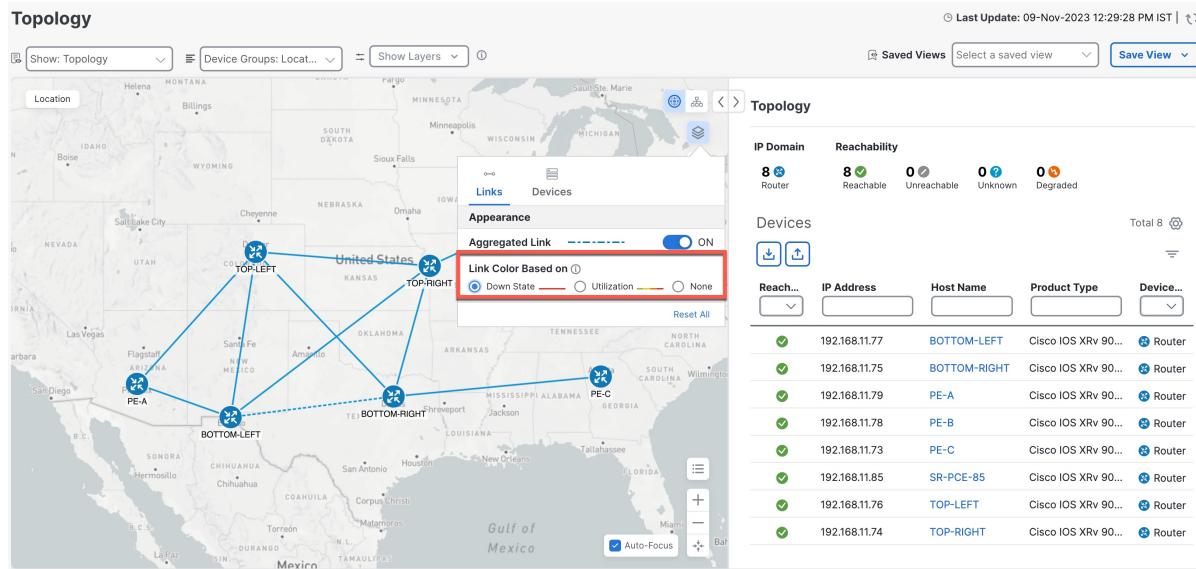
#### Step 2

Click  on the topology map to open the **Display Preference** dialog box.

#### Step 3

Click the **Links** tab and under **Link Color Based on** select the **Down State** option. All the links that are down will appear in red. If you select the **Utilization** option, the links are colored based on the percentage of total bandwidth currently utilized on the link. For more information on the link color based on utilization threshold refer to [Show Link Utilization by Color, on page 155](#)

Figure 68: Link Utilization based on Color



## Show Link Utilization by Color

Link bandwidth utilization can be visualized and monitored in the logical and geographical maps. 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:

### Procedure

- Step 1** From the main menu, choose **Administration > Settings > System Settings**.
- Step 2** Under **Topology**, click the **Bandwidth Utilization** option.
- Step 3** In the **Link utilization 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.
  - 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 4** Click **Save**.

---

## Troubleshoot your Topology Map

To resolve any problems with your topology map, you need to check the network connectivity and configuration of your devices. Ensure that they are online and have the correct IP addresses, subnet masks, gateways, and DNS settings. You also need to make sure that your topology map matches the actual physical layout of your network. This will help you to optimize the performance and accuracy of your topology map.

## Rebuild the Topology

Rebuilding the topology is a process of creating a new topology for our system. This is useful when the topology becomes inconsistent because of network problems or other unforeseen events. You should only rebuild the topology as a last resort.

The topology rebuild will refresh the topology and update the links and devices. The topology pages will show no links and devices while the rebuild is in progress. They will reappear when the rebuild is finished.

### Before you begin

To start the topology rebuild, the system must be in maintenance mode.

### Procedure

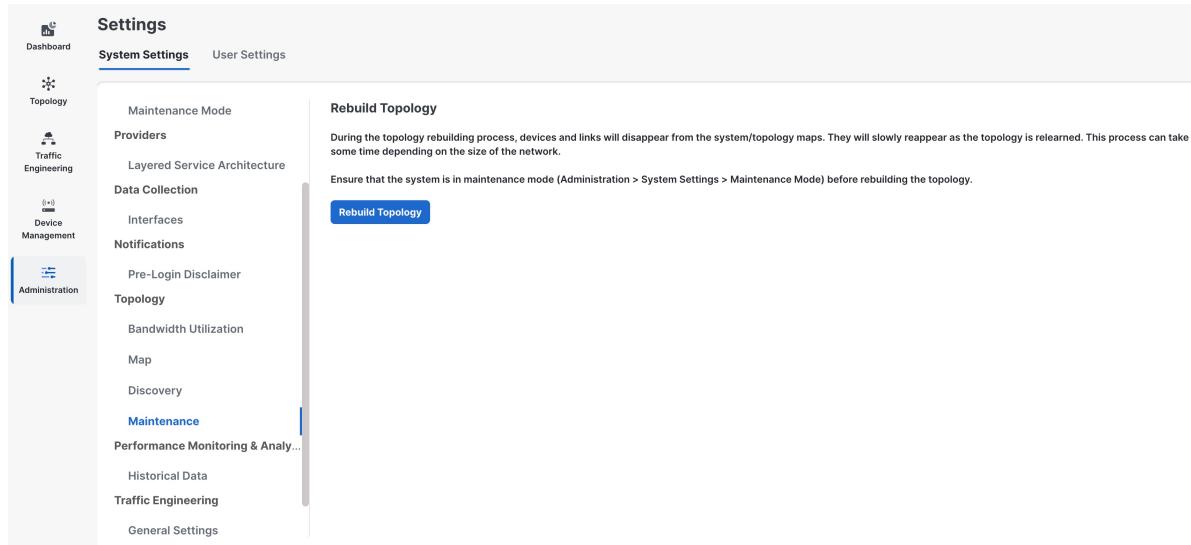
---

**Step 1** From the main menu, choose **Administration > Settings > System Settings**.

**Step 2** Under **Topology**, click the **Maintenance** option.

**Step 3** In the **Rebuild Topology** section, click **Rebuild Topology**.

Figure 69: Rebuild the Topology



- Step 4** To confirm your Topology rebuild, in the **Confirm Topology Rebuild** pop-up, click **Rebuild Topology** again.
- 

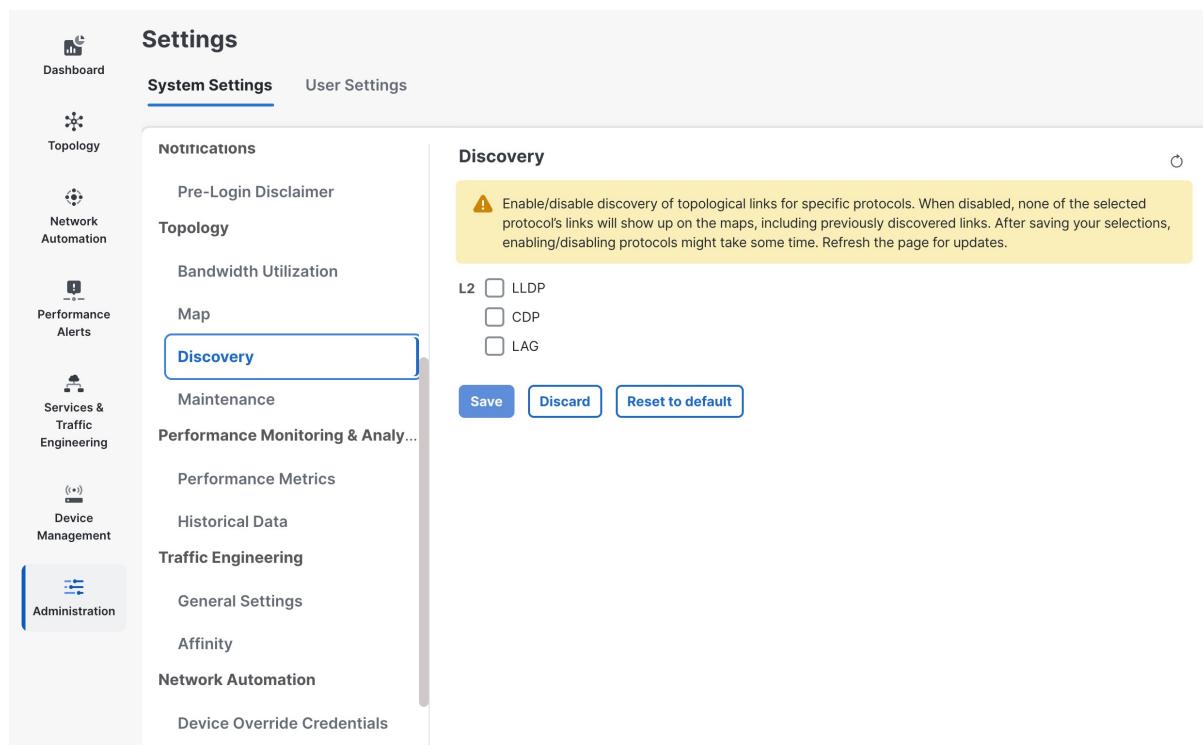
## Find Missing L2 Links

If L2 links are missing, it is important to check the protocol settings and ensure that they are enabled. By default, L2 link discovery is not enabled, so you may need to manually enable it in order to discover L2 links. Once the protocol settings are correctly configured, you should be able to discover and view L2 links in your network. For more information refer to [Enable or Disable Topology Link Discovery, on page 148](#).

### Procedure

---

- Step 1** From the main menu, click **Administration > Settings > System Settings**.  
**Step 2** Under **Topology**, click the **Discovery** option.

**Missing L3 Links****Figure 70: L2 Link Discovery**

- Step 3** Select the desired option and click **Save**.

## Missing L3 Links

One of the possible reasons for missing L3 links is a device level issue. This means the SR-PCE cannot learn the IGP information for that device. Some of the factors that can cause a device level issue are hardware failure, software bugs, misconfiguration, or interference. To troubleshoot this problem, you should first check the device status and logs for any errors or warnings. Then check the IGP configurations for that device and check if the SR-PCE has that device in its topology.

### Procedure

- Step 1** From the main menu, click **Administration > Manage Provider Access**.  
**Step 2** Under **Reachability** column, ensure that the providers are reachable.

Figure 71: Manage Provider Access

## Error Record in Alarm/Events Report of Topology Services

The topology service may encounter errors during its operation, such as missing or incorrect data, communication failures, or configuration issues. These errors are recorded in the alarms/events report, which can help you to diagnose and resolve the problems.

### Procedure

**Step 1** From the main menu, click **Administration > Alarms**.

**Step 2** Enter "topo" in the Source filter. This will display only the alarms and events related to the Topology.

Figure 72: Alarm Events Report of Topology Service

Source	Severity	Description	Creation Time	Category	Correlated Alarm
cw.topo_svc:robot-topo-svc-1	Info	Topo-Svc instance robot-topo-svc-1 has the Follower role.	05-Oct-2023 09:08:49 AM IST	System	NO
cw.topo_svc:robot-topo-svc-1	Info	Topo-Svc instance robot-topo-svc-1 has the Follower role.	05-Oct-2023 05:48:35 AM IST	System	NO
cw.topo_svc:XtcTopoNotifMgrResyncE...	Info	Completed resync of IGP topology data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:48:24 AM IST	System	NO
cw.topo_svc:XtcP2mpNotifMgrResync...	Info	Performing resync of PCE data with SR-PCE for P2MP data 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO
cw.topo_svc:XtcLspNotifMgrResyncEv...	Info	Performing resync of PCE data with SR-PCE 'SR-PCE'.	05-Oct-2023 05:47:59 AM IST	System	NO





# CHAPTER 6

## Prepare Infrastructure for Device Management

This section contains the following topics:

- [Manage Credential Profiles, on page 161](#)
- [Manage Providers, on page 168](#)
- [Manage Tags, on page 199](#)

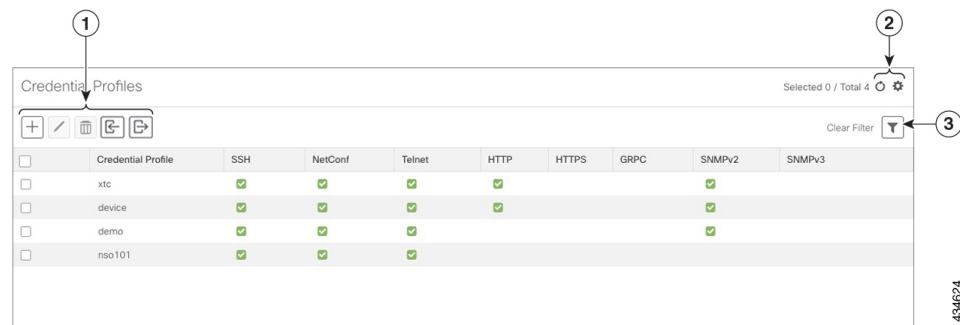
### Manage Credential Profiles

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 73: Credentials Profile window*



434624

Item	Description
1	Click  to add a credential profile. See <a href="#">Create Credential Profiles, on page 162</a> .
	Click  to edit the settings for the selected credential profile. See <a href="#">Edit Credential Profiles, on page 166</a> .
	Click  to delete the selected credential profile. See <a href="#">Delete Credential Profiles, on page 167</a> .
	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 <a href="#">Import Credential Profiles, on page 164</a> .
	Click  to export credential profiles to a CSV file. See <a href="#">Export Credential Profiles, on page 167</a> .
2	Click  to refresh the <b>Credential Profiles</b> window.
	Click  to choose the columns to make visible in the <b>Credential Profiles</b> window.
3	Click  to set filter criteria on one or more columns in the <b>Credential Profiles</b> window.
	Click the <b>Clear Filter</b> 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 164](#).

When creating device credential profiles that contain SNMP credentials, Cisco recommends that the profile contains credentials for the version of SNMP enabled on the device, and that version only. For example: If SNMPv3 is not enabled in the device configuration, do not include SNMPv3 credentials in the device credential profile.

If you plan to use the import and export features and CSV files to create credential profiles in bulk, please note that:

- All the characters in each password or community string entry in every credential profile exported to a CSV file are replaced with asterisks ([Export Credential Profiles, on page 167](#)).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see [Import Credential Profiles, on page 164](#)).

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 166](#) to replace the asterisks with actual passwords and community strings.

## Procedure

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

**Step 2** Click .

**Step 3** In the **Profile Name** field, enter a descriptive profile name. The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("\_") or hyphens (""). No other special characters are allowed.

If you will have many credential profiles, make the name as informative as possible because that information will be displayed on the Credential Profiles panel.

**Step 4** Select a protocol from the **Connectivity Type** dropdown.

**Step 5** Complete the credentials fields described in the following table. The required and optional fields displayed varies with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
SSH	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> . The <b>Enable Password</b> is optional.
SNMPv2	Enter the required SNMPv2 <b>Read Community</b> string. The <b>Write Community</b> string is optional.
NETCONF	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
TELNET	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> . The <b>Enable Password</b> is optional.
<b>Note</b> There may be some security limitations when using this protocol.	
HTTP	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
HTTPS	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
GRPC	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
gNMI	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
TL1	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .

Connectivity Type	Fields
SNMPv3	<p>Choose the required <b>Security Level</b> and enter the <b>User Name</b>.</p> <p>If you chose the <b>NO_AUTH_NO_PRIV Security Level</b> of <b>AUTH_NO_PRIV</b> or <b>AUTH_PRIV</b>, the remaining fields are optional.</p> <p>If you chose the <b>AUTH_NO_PRIV Security Level</b>, you must choose an <b>Auth Type</b> and enter an <b>Auth Password</b>.</p> <p>If you chose the <b>AUTH_PRIV Security Level</b>, you must choose an <b>Auth Type</b> and <b>Priv Type</b>, and enter an <b>Auth Password</b> and <b>Priv Password</b>.</p> <p>The following SNMPv3 Privacy Types are supported:</p> <ul style="list-style-type: none"> <li>• CFB_AES_128</li> <li>• CBC_DES_56</li> <li>• AES-192</li> <li>• AES-256</li> <li>• 3-DES</li> </ul>

**Step 6** (Optional) Click + **Add Another** and repeat the previous steps, as needed, for all other protocols and corresponding credentials you want to add to this credential profile.

**Step 7** Click **Save**.

---

## Import Credential Profiles

Complete the steps below to create a CSV file that specifies multiple credential profiles and then import it into the Cisco Crosswork application.

Importing credential profiles from a CSV file adds any profiles not already in the database. You cannot import a credential profile that already exists.

If you are re-importing a credential profile CSV file that you previously exported and modified, remember that all the passwords and community strings in the exported credential profile CSV file are replaced with asterisks. You cannot re-import an exported credential profile CSV file with blank passwords. To maintain security, Cisco recommends that you use asterisks in place of real passwords and community strings in the CSV file. After the import, follow the steps in [Edit Credential Profiles, on page 166](#) to replace the asterisks with actual passwords and community strings.

### Procedure

---

**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
<b>Credential Profile</b>	The name of the credential profile. For example: .	Required
<b>Connectivity Type</b>	Valid values are: <b>SSH, SNMPv2, NETCONF, TELNET, HTTP, HTTPS, GRPC or SNMPv3</b>	
<b>User Name</b>	For example:	Required if <b>Connectivity Type</b> is <b>SSH, NETCONF, TELNET, HTTP, HTTPS, SNMPv3</b> or <b>GRPC</b> .
<b>Password</b>	The password for the preceding <b>User Name</b> .	Required if <b>Connectivity Type</b> is <b>SSH, NETCONF, TELNET, HTTP, HTTPS or GRPC</b>
<b>Enable Password</b>	Use an Enable password. Valid values are: <b>ENABLE, DISABLE</b>	
<b>Enable Password Value</b>	Specify the Enable password to use.	
<b>SNMPv2 Read Community</b>	For example: <b>readprivate</b>	Required if <b>Connectivity Type</b> is <b>SNMPv2</b>
<b>SNMPv2 Write Community</b>	For example: <b>writeprivate</b>	
<b>SNMPv3 User Name</b>	For example: <b>DemoUser</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b>
<b>SNMPv3 Security Level</b>	Valid values are <b>noAuthNoPriv, AuthNoPriv or AuthPriv</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b>

**Edit Credential Profiles**

Field	Entries	Required or Optional
<b>SNMPV3 Auth Type</b>	Valid values are <b>HMAC_MD5</b> or <b>HMAC_SHA</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmpV3 Security Level</b> is <b>AuthNoPriv</b> or <b>AuthPriv</b>
<b>SNMPV3 Auth Password</b>	The password for this authorization type.	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmpV3 Security Level</b> is <b>AuthNoPriv</b> or <b>AuthPriv</b>
<b>SNMPV3 Priv Type</b>	Valid values are <b>CFB_AES_128</b> or <b>CBC_DES_56</b>  The following SNMPv3 privacy types are not supported: AES-192, AES-256, 3-DES	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmpV3 Security Level</b> is <b>AuthPriv</b>
<b>SNMPV3 Priv Password</b>	The password for this privilege type.	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmpV3 Security Level</b> is <b>AuthPriv</b>

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.

- 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 167](#)).

---

### Procedure

**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 166](#) to replace the asterisks with actual passwords and community strings.

### Procedure

- 
- 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.
- 

### Procedure

- 
- Step 1** Export a backup CSV file containing the credential profile you plan to delete (see [Export Credential Profiles, on page 167](#)).
  - 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 168](#) and [Edit Providers, on page 197](#)).
  - Step 4** After all devices and providers have had their credential profiles reassigned: From the main menu, choose **Device Management > Credential Profiles**.

**Change the Credential Profile for Multiple Devices**

- Step 5** In the **Credential Profiles** window, choose the profile that you want to delete and then click .

## Change the Credential Profile for Multiple Devices

If you want to change the credential profile for a large number of network devices, you may find it more efficient to make the change by editing a devices CSV file. The basic method is:

1. Export a CSV file containing the devices whose credential profiles you want to change (see [Export Device Information to a CSV File, on page 218](#)).
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.

### Procedure

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

- Step 2** Choose the devices whose credential profiles you want to change. Your options are:

- Click  to include all devices.
- Filter the device list by entering text in the **Search** field or by filtering specific columns. Then click  to include only the filtered list of devices.
- Check the boxes next to the device records you want to change. Then click  to include only the devices that have been checked.

- Step 3** Edit and save the new CSV file using the tool of your choice. Be sure to enter the correct credential profile name in the **Credential Profile** field for each device.

- Step 4** Click .

- Step 5** In the **Import** dialog box, click **Browse**, choose the new CSV file, and click **Import**.

## Manage Providers

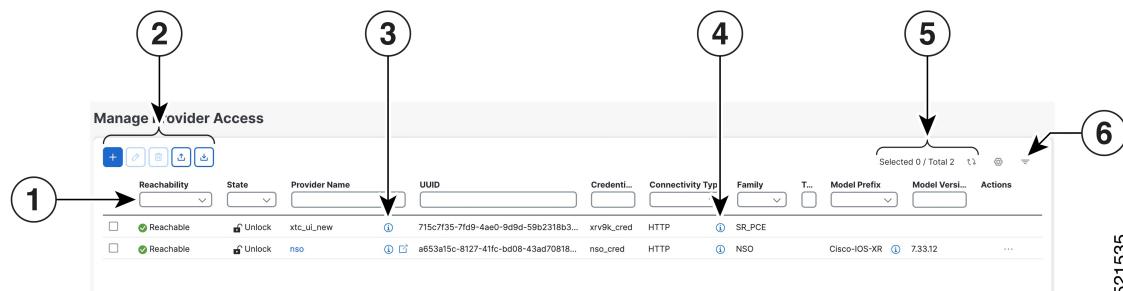
Cisco Crosswork applications communicate with external providers. Cisco Crosswork stores the provider connectivity details and makes that information available to applications. For more information, see [Before You Begin, on page 1](#).

From the **Providers** window, you can add a new provider, update the settings configured for an existing provider, and delete a particular provider. To open this window, choose **Administration > Manage Provider Access**.



**Note** Wait until the application responds between performing a succession of updates. For example, wait for some time between adding, deleting, or reading providers. Topology services may not receive these changes if you perform these actions too quickly. However, if you find that topology is out of sync, restart the topology service.

**Figure 74: Providers Window**



521535

Item	Description
1	The icon shown next to the provider in this column indicates the provider's <b>Reachability</b> . See <a href="#">Device State, on page 219</a> .
2	Click  to add a provider. See <a href="#">About Adding Providers, on page 171</a> .
	Click  to edit the settings for the selected provider. See <a href="#">Edit Providers, on page 197</a> .
	Click  to delete the selected provider. See <a href="#">Delete Providers, on page 198</a> .
	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 <a href="#">Import Providers, on page 195</a> .
	Click  to export a provider to a CSV file. See <a href="#">Export Providers, on page 199</a> .
3	Click  next to the provider in the <b>Provider Name</b> column to open the <b>Properties for</b> pop-up window, showing the details of any startup session key/value pairs for the provider.
4	Click  next to the provider in the <b>Connectivity Type</b> column to open the <b>Connectivity Details</b> pop-up window, showing the protocol, IP, and other connection information for the provider.

Item	Description
5	Click  to refresh the <b>Providers</b> 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 <b>Providers</b> window.
	Click the <b>Clear Filter</b> 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 12: Supported Provider Families**

Provider Family	Description
NSO	Instances of Cisco Network Services Orchestrator (Cisco NSO), used to configure network devices. See <a href="#">Add Cisco NSO Providers, on page 174</a> .
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 <a href="#">Add Cisco SR-PCE Providers, on page 178</a> .
WAE	Instances of Cisco WAN Automation Engine (Cisco WAE) provide "what if" analysis used to evaluate network changes. See <a href="#">Add Cisco WAE Providers, on page 190</a> .
Syslog Storage	Instances of storage servers (remote or on the Cisco Crosswork application VM itself) where you want to store syslogs and other data retrieved from devices by KPIs and Playbooks. See <a href="#">Add Syslog Storage Providers, on page 191</a> .
Alert	Instances of providers (such as Cisco Crosswork Situation Manager) to which alerts collected during KPI monitoring are to be forwarded. See <a href="#">Add an Alert Provider, on page 193</a> .
Proxy	Instances of proxy providers. See <a href="#">Add Proxy Providers, on page 194</a>

## Provider Dependency

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

Cisco Crosswork Network Controller is an integrated solution that combines Cisco Crosswork Active Topology and Cisco Crosswork Optimization Engine. You can also optionally integrate Crosswork Network Controller with Crosswork Change Automation, Crosswork Health Insights, and Crosswork Zero Touch Provisioning.

**Table 13: Provider Dependency matrix**

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider	Cisco WAE Provider	Syslog Storage Provider	Alert Provider
Crosswork Network Controller	Mandatory Required protocol is HTTPS  Provider property key <b>forward</b> must be set as <i>true</i> .	Mandatory Required protocol is HTTP.	Optional	Optional	Optional
Crosswork Optimization Engine	Optional	Mandatory Required protocol is HTTP.	Optional	Optional	Optional
Crosswork Change Automation	Mandatory Required protocol is HTTPS.	Optional	Optional	Optional	Optional
Crosswork Health Insights	Provider property key <b>forward</b> must be set as <i>true</i> .				
Crosswork Zero Touch Provisioning	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:

- Adding providers via the UI:** This method is explained in [Add Providers Through the UI, on page 172](#). Although this method is the most time-consuming, it is more often used because most deployments will not need a lot of provider instances.
- Importing providers from a providers CSV file:** This method is explained in [Import Providers, on page 195](#). 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:

**Add Providers Through the UI**

- Create a corresponding credential profile, beforehand, so that the Cisco Crosswork applications can access the provider. For help, see [Create Credential Profiles, on page 162](#).
- 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.

**Procedure**

**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 14: Add Provider Fields (\*=required)**

Field	Description
* <b>Provider Name</b>	The name for the provider that will be used to refer to it in the Cisco Crosswork application. For example: <b>Linux_Server</b> . The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens (""). No other special characters are allowed.
* <b>Credential Profile</b>	Select the name of the credential profile that is used by the Cisco Crosswork application to connect to the provider.
* <b>Family</b>	Select the provider family. Choices are: <b>NSO</b> , <b>WAE</b> , <b>SR-PCE</b> , <b>ALERT</b> and <b>SYSLOG_STORAGE</b> .
<b>Connection Type(s)</b>	
* <b>Protocol</b>	<p>Select the principal protocol that the Cisco Crosswork application will use to connect to the provider. Options include: <b>HTTP</b>, <b>HTTPS</b>, <b>SSH</b>, <b>SNMP</b>, <b>NETCONF</b>, <b>TELNET</b>, and more.</p> <p>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.</p> <p>You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol.</p>
* <b>Server Details</b>	Select and provide one of the options: <ul style="list-style-type: none"> <li>• IP Address (IPv4 or IPv6) and subnet mask of the provider's server.</li> <li>• FQDN (Domain name and Host name)</li> </ul>

Field	Description
* <b>Port</b>	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.
<b>Timeout</b>	Enter the amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.
<b>Model Prefix Info</b>	
* <b>Model</b>	<p>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:</p> <p><b>Cisco-IOS-XR</b></p> <p><b>Cisco-NX-OS</b></p> <p><b>Cisco-IOS-XE</b></p> <p>For telemetry, only <b>Cisco-IOS-XR</b> is supported.</p> <p>To add more model prefix information for this Cisco NSO provider, click the  at the end of any row in the <b>Model Prefix Info</b> section. To delete a model prefix you have entered, click the  shown next to that row.</p>
* <b>Version</b>	Required only if you are adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the NSO server.
<b>Provider Properties</b>	
<b>Property Key</b>	<p>Enter the name of the key for the special provider property you want to configure.</p> <p>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.</p> <p><b>Note</b></p> <p>In a two network interface configuration, the Cisco Crosswork applications default to communicating with providers using the Management Network Interface (<b>eth0</b>). You can change this behavior by adding <b>Property Key</b> and <b>Property Value</b> as <b>outgoing-interface</b> and <b>eth1</b> 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.</p>
<b>Property Value</b>	<p>Enter the value to assign to the property key.</p> <p>To add more special properties for this provider, click  at the end of any key/value pair in the <b>Provider Properties</b> section. To delete a key/value pair you have entered, click  shown next to that pair.</p>

## Add Cisco NSO Providers

This topic explains the steps to add a Cisco NSO provider through the Crosswork UI.

The Cisco Network Services Orchestrator (Cisco NSO) provider functions as the provider for Cisco Crosswork to configure the devices according to their expected functions, including optionally configuring MDT sensor paths for data collection. Cisco NSO provides the important functions of device management, configuration and maintenance services.

Cisco Crosswork also supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.



### Note

- The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team. See [View Installed NSO Function Packs, on page 178](#) to monitor the state of the installed NSO function packs.
- The NSO Function Pack deployment via Crosswork UI is supported for NSO system installation and as a root user.



### Attention

Crosswork does not scan NSO continuously for NSO device status changes. When devices are newly added to NSO, those devices are learned by Crosswork only when there is an explicit action from Crosswork towards NSO. For example, when you edit and save the policy details of an existing NSO Provider (select **Actions > Edit Policy Details** > set **Onboard from** to **TRUE** > **Save**) Crosswork triggers the service to rescan NSO which leads to onboarding the newly added devices from NSO to Crosswork. Even during device addition from Crosswork to NSO, after the devices are added, the necessary operations (fetch keys and sync actions) are performed only once.

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 195](#)).

### Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see [Create Credential Profiles, on page 162](#)).
- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology. You can find the Cisco NSO version using the `version` command.

- Know the Cisco NSO server IP address or FQDN (Domain name and host name). When NSO is configured with HA, the IP address would be management VIP address.
- Confirm Cisco NSO device configurations. For more information, see [Sample Configuration for Cisco NSO Devices, on page 211](#).
- The NSO cross launch feature is not available for user roles with read-only permissions.

#### For NSO LSA deployment:

- If you plan to add a NSO LSA provider, you must first enable LSA settings. See [Enable Layered Service Architecture \(LSA\), on page 176](#) for details.
- If you forgot to enable the LSA setting or misconfigures the provider property values, please perform the recovery steps mentioned in [NSO LSA Setup Recovery, on page 177](#).
- The RFS node IP addresses used on the CFS must match with the IP addresses on the Crosswork UI. A mismatch will generate the error "*LSA cluster is missing RFS providers*".
- In case of the CFS node, only the **forward** property key is used.

### Procedure

**Step 1** From the main menu, choose **Administration > Manage Provider Access**.

**Step 2** Click .

**Step 3** Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name:** Enter a name for the provider.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO**.
- **Protocol:** Select **HTTPS**. For more information, see [Provider Dependency, on page 170](#).
- **Server Details:** Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) of the server.
- **Port:** For HTTPS, enter the port that corresponds with what is configured on the NSO VM in etc/ncs/ncs.conf to access NSO using HTTPS. NSO uses **8888** as default port.
- **Model:** Select the model (Cisco-IOS-XR, Cisco-NX-OS, or Cisco-IOS-XE). Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.
- **Version:** Enter the NED software version installed for the device model in NSO.

#### Important

When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

b) Optional values:

## Enable Layered Service Architecture (LSA)

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

- c) **Provider Properties:** Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
<b>forward</b>	<b>true</b> 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.
<b>nso_crosslaunch_url</b> <b>Note</b> This property is used only for NSO standalone provider.	Enter the URL for cross-launching NSO in the format: <b>https://&lt;NSO IP address/FQDN&gt;: port number</b> To enable cross-launch of the NSO application from the Crosswork UI. Requires a valid protocol ( <b>HTTP</b> or <b>HTTPS</b> ), and the provider must be reachable.  The cross launch icon (  ) is displayed in the <b>Provider Name</b> column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.
<b>input_url_prefix</b> <b>Note</b> This property is used only for NSO LSA provider.	Enter the RFS ID in the format: <b>/rfc-x</b> , where <b>x</b> refers to the number of the RFS node. Example (for RFS node 1): <b>input_url_prefix: /rfc-1</b>

**Step 4** When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

**Step 5** In the Providers window, select the NSO provider you created and click **Actions > Edit Policy Details**.

The **Edit Policy Details** window for the selected NSO provider is displayed.

**Step 6** Edit the configuration fields to match the requirements of your environment. Click **Save** to save your changes.

---

## Enable Layered Service Architecture (LSA)

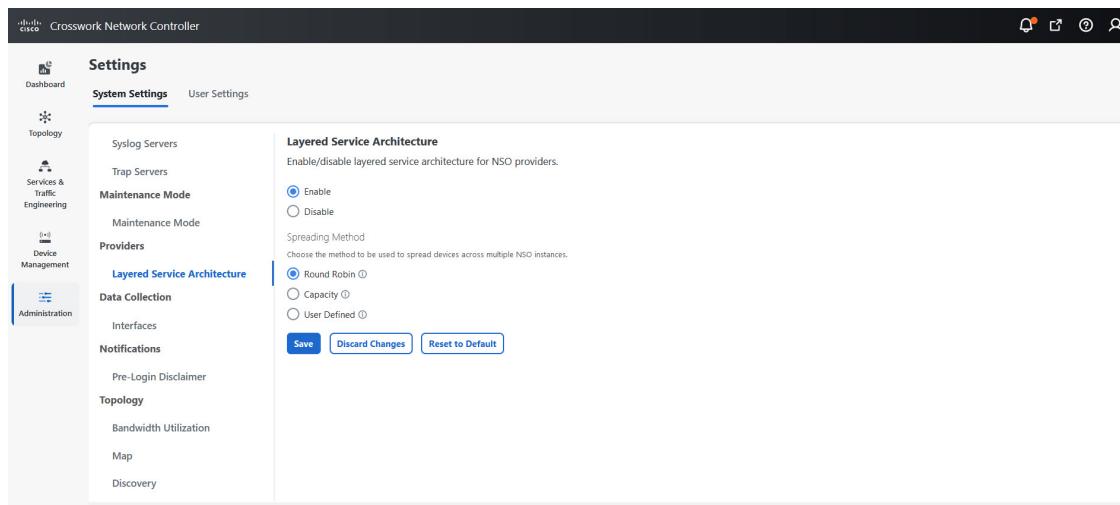
This procedure is applicable only when you have opted for Cisco NSO LSA deployment to add arbitrarily many device nodes for improved memory and provisioning throughput.

### Procedure

---

**Step 1** From the main menu, select **Administration > Settings > System Settings > Layered Service Architecture**.

Figure 75: Enabling Layered Service Architecture Window



**Step 2** Select **Enable**.

**Step 3** Select the method to spread the devices across multiple NSO instances:

- **Round Robin** - Even distribution of devices to RFS nodes in a cyclical manner (for example, Device 1 to RFS1, Device 2 to RFS2, and so on).
- **Capacity** - The number of devices are assigned to each RFS instance based on its total capacity.
- **User Defined** - Devices are assigned to the NSO providers specified for the device in the device settings. For more information, see [Add Devices through the UI, on page 211](#).

**Step 4** Click **Save**.

**Note**

Once you have saved the settings, you cannot disable it without removing all the NSO providers.

## NSO LSA Setup Recovery

This topic explains the steps for NSO LSA setup recovery in case of any misconfigurations.

### Procedure

**Step 1** Remove the NSO providers and associated devices on Device Management window.

**Step 2** Clean up the associated services on the Cisco NSO application.

**Step 3** Enable the LSA settings and add the NSO LSA provider with correct property values.

**Step 4** Add the NSO providers and devices again to Crosswork, and map them to the Crosswork Data Gateway.

**Step 5** Perform the sync operation on the NSO nodes (RFS and CFS) again to sync the devices correctly.

## View Installed NSO Function Packs

This will recover the functionality as expected.

## View Installed NSO Function Packs

Cisco Crosswork allows you to monitor the status of the installed NSO Function Packs.

### Procedure

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

**Step 2** On the **Crosswork Manager** window, select the **NSO Deployment Manager** tab.

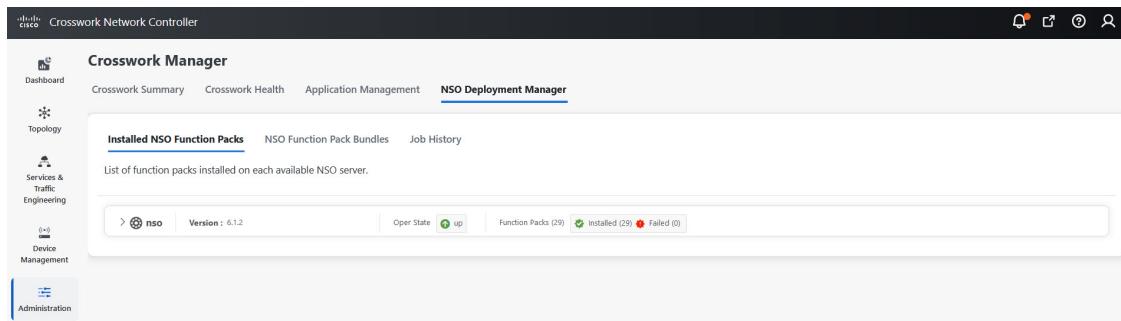
The **Installed NSO Function Packs**, **NSO Function Pack Bundles**, and **Job History** tabs are displayed.

#### Note

You can also navigate here from the NSO provider entries in the **Providers** window (click **Actions > View Function Packs**).

The **Installed NSO Function Packs** tab displays a list of NSO function pack bundles deployed on the configured NSO server.

**Figure 76: Installed NSO Function Packs**



**Step 3** Expand the bundles to view the number of function packs within each bundle, the function pack name, operational state as **Up** or **Down**, description, and version.

## 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:

- Configure a device to act as the SR-PCE. See SR configuration documentation for your specific device platform to enable SR (for IS-IS or OSPF protocols) and configure an SR-PCE (for example: *Segment Routing Configuration Guide for Cisco NCS 540 Series Routers*).
- Create a credential profile for the Cisco SR-PCE provider (see [Create Credential Profiles, on page 162](#)). 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 .

### Procedure

**Step 1** From the main menu, choose **Administration > Manage Provider Access**.

**Step 2** Click .

**Step 3** Enter the following values for the SR-PCE provider fields:

a) Required fields:

- **Provider Name:** Name of the SR-PCE provider.
- **Credential Profile:** Select the previously created Cisco SR-PCE credential profile.

- **Family:** Select **SR\_PCE**. All other options should be ignored.
- **Protocol:** Select **HTTP**.
- **Server Details:** Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) and subnet mask of the server.
- **Port:** Enter **8080** for the port number.
- **Provider Properties:** Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
<b>auto-onboard</b>	<p><b>off</b></p> <p><b>Note</b> Use this option if you plan to manually (via UI or CSV import) enter all of your network devices.</p> <p>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.</p>
<b>auto-onboard</b>	<p><b>unmanaged</b></p> <p>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 <b>unmanaged</b>. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the <b>managed</b> state later, you will need to either edit them via the UI or export them to a CSV make modifications and then import the updated CSV. You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).</p>
<b>auto-onboard</b>	<p><b>managed</b></p> <p>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 <b>managed</b>. SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (TE Router ID for IPv4, or IPv6 Router ID for IPv6 deployment). The devices will be added with the credential profile associated with the device-profile key in the SR-PCE provider configuration.</p>

Property Key	Value
<b>device-profile</b>	<p>The name of a credential profile that contains SNMP credentials for all the new devices.</p> <p><b>Note</b> This field is necessary only if <b>auto-onboard</b> is set to <b>managed</b>. If the <b>auto-onboard</b> is set to <b>managed</b> and there is no valid <b>device-profile</b> set, the device will be onboarded as <b>unmanaged</b> instead.</p>
<b>outgoing-interface</b>	<p><b>eth1</b></p> <p><b>Note</b> 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.</p>
<b>topology</b>	<p><b>off</b> or <b>on</b>. This is an optional property. If not specified, the default value is <b>on</b>. If value is specified as <b>off</b>, it means that L3 topology is not accessible for the SR-PCE provider.</p>
<b>pce</b>	<p><b>off</b> or <b>on</b>. This is an optional property. If not specified, the default value is <b>on</b>. If value is specified as <b>off</b>, it means that LSPs and policies are not accessible for the SR-PCE provider.</p>

#### Note

Topology can be visualized even with **auto-onboard** as **off** and no **device-profile**.

**Figure 77: Provider Property Key and Value Example**

Provider Properties

Property Key *	Property Value *
auto-onboard	off
outgoing-interface	eth1

#### 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 196](#)). 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:

## Procedure

---

- Step 1** Check device credentials.
  - Step 2** Ping the provider host.
  - Step 3** Attempt a connection using the protocols specified in the connectivity settings for the provider. For an SR-PCE provider, it is typically HTTP and port 8080.
  - Step 4** Check your firewall setting and network configuration.
  - Step 5** Check the Cisco SR-PCE host or intervening devices for Access Control List settings that might limit who can connect.
- 

## Multiple Cisco SR-PCE HA Pairs

You can set up to eight Cisco SR-PCE HA pairs (total of 16 SR-PCEs) to ensure high availability (HA). Each HA pair of Cisco SR-PCE providers must have matching configurations, supporting the same network topology. In HA, if the primary SR-PCE becomes unreachable, Cisco Crosswork Optimization Engine uses the secondary SR-PCE to discover the network topology. If this pair fails, then the next HA pair takes over and so forth. The network topology will continue to be updated correctly and you can view SR-PCE connectivity events in the Events table (  ).

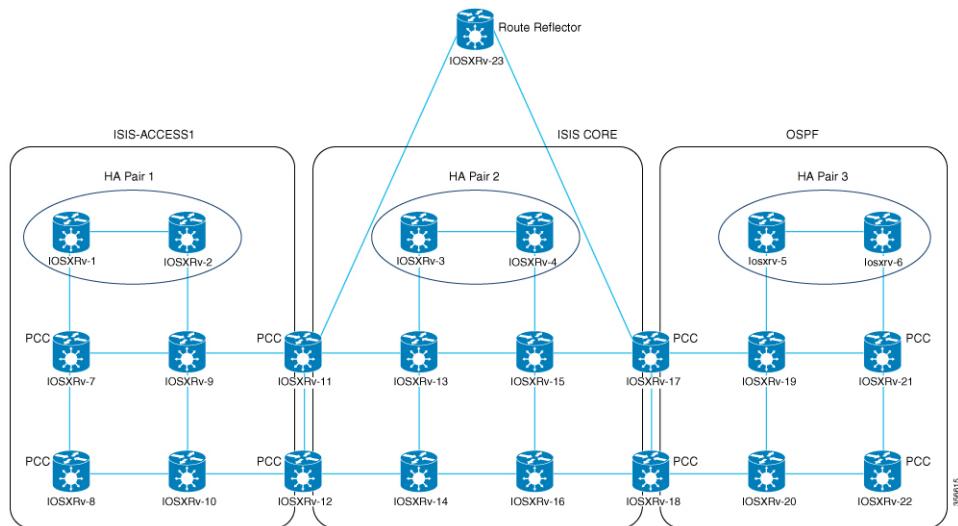
### Multiple HA Pairs

In the case of multiple SR-PCE HA pairs, each SR-PCE pair sees the same topology but manages and only knows about tunnels created from its Path Computation Clients (PCCs). The following figure is a sample of a three SR-PCE HA pair topology. Note the following:

- HA Pair 1—PCE iosxrv-1 and iosxrv-2 provisions and discovers *only* tunnels whose headends are iosxrv-7 and iosxrv-8. Note that iosxrv-9 and iosxrv-10 are not PCC routers.
- HA Pair 2—PCE iosxrv-3 and iosxrv-4 provisions and discovers *only* tunnels whose headends are iosxrv-11, iosxrv-12, iosxrv-17, and iosxrv-18. Note that iosxrv-13, iosxrv-14, iosxrv-15, and iosxrv-16 are not PCC routers.
- HA Pair 3—PCE iosxrv-5 and iosxrv-6 provisions and discovers *only* about tunnels whose headends are iosxrv-21, and iosxrv-22. Note that iosxrv-19, and iosxrv-20 are not PCC routers.

## Multiple Cisco SR-PCE HA Pairs

Figure 78: Sample 3 HA Pair Topology



**Note** If any of the SR-PCEs are included in a *subset* of the main network topology, then that SR-PCE provider must be added with the Property Key as **topology** and the Property Value as **off**. When this value is set, then this SR-PCE will not be used to learn the topology.

## Configure HA

The following configurations must be done to enable each pair of HA Cisco SR-PCE providers to be added in Cisco Crosswork Optimization Engine.



**Note** There must be resilient IPv4 connectivity between both SR-PCEs to enable HA. The PCE IP address of the other SR-PCE should be reachable by the peer at all times.

Issue the following commands on *each* of the Cisco SR-PCE devices:

Enable the interface:

```
# interface <interface><slot>/<port>
  ipv4 address <sync-link-interface-ip-address> <subnet-mask>
  no shut
```

Enable HA:

```
# pce api sibling ipv4 <other-node-pce-address>
```

Establish a sync link between the two SR-PCEs:

```
# router static
  address-family ipv4 unicast
  <other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

(Optional) # pce segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>

It should be entered for each PCC and not for other PCE nodes.

Issue the following command on the PCC:

For SR Policies: # segment-routing traffic-eng pcc redundancy pcc-centric

For RSVP-TE Tunnels: # mpls traffic-eng pce stateful-client redundancy pcc-centric

### Confirm Sibling SR-PCE Configuration

From the SR-PCE, enter the `show tcp brief` command to verify synchronization between SR-PCEs in HA are intact:

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

Confirm that following information is correct:

Local Address	Foreign Address	State
<local-SR-PCE-router-id>:8080	<remote-SR-PCE-router-id>:<any-port-id>	ESTAB
<local-SR-PCE-router-id>:<any-port-id>	<remote-SR-PCE-router-id>:8080	ESTAB

For example:

```
RP/0/0/CPU0:iosxrv-1#sh tcp brief | i 192.168.0.2:
Mon Jun 22 18:43:09.044 UTC
0x153af340 0x60000000 0 0 192.168.0.1:47230 192.168.0.2:8080 ESTAB
0x153aaa6c 0x60000000 0 0 192.168.0.1:8080 192.168.0.2:16765 ESTAB
```

In this example, 192.168.0.2 is the remote SR-PCE IP.

### SR-PCE Delegation

Depending on where an SR-TE policy is created, the following SR-PCE delegation occurs:

- SR-PCE initiated—Policies configured on a PCE. SR-TE policies are delegated back to the source SR-PCE.

#### Note

- The policy can be PCE initiated even if it is created using the UI, but in that case it is not configured explicitly on SR-PCE.
- RSVP-TE tunnels cannot be configured directly on a PCE.
- PCC initiated—An SR-TE policy or RSVP-TE tunnel that is configured directly on a device. The SR-PCE configured with the lowest precedence is the delegated SR-PCE. If precedence is not set, then SR-PCE with the lowest PCE IP address is the delegated SR-PCE. The following configuration example, shows that **10.0.0.1** is assigned a precedence value of 10 and will be the delegated SR-PCE.

```
segment-routing
  traffic-eng
    pcc
      source-address ipv4 10.0.0.2
      pce address ipv4 10.0.0.1
        precedence 10
      !
      pce address ipv4 10.0.0.8
        precedence 20
```

```

!
report-all
redundancy pcc-centric

```

For RSVP-TE Tunnel:

```

mpls traffic-eng
interface GigabitEthernet0/0/0/0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
!
pce
  peer source ipv4 192.168.0.02
  peer ipv4 192.168.0.9
    precedence 10
  !
  peer ipv4 192.168.0.10
    precedence 20
  !
  stateful-client
    instantiation
    report
    redundancy pcc-centric
    autoroute-announce
  !
!
auto-tunnel pcc
  tunnel-id min 1000 max 5000

```

- Cisco Crosswork SR-PCE initiated—An SR-TE policy that is configured using Cisco Crosswork. SR-PCE delegation is random per policy.



**Note**

Only SR-TE policies or RSVP-TE tunnels created by Cisco Crosswork Optimization Engine can be modified or deleted by Cisco Crosswork Optimization Engine.

### HA Notes and Limitations

- It is assumed that all PCCs are PCEP connected to both SR-PCEs.
- When an SR-PCE is disconnected only from Cisco Crosswork, the following occurs:
  - SR-PCE delegation assignments remain, but the SR-PCE that has been disconnected will not appear in Cisco Crosswork.
  - You are not able to modify Cisco Crosswork SR-PCE initiated SR-TE policies if the disconnected SR-PCE is the delegated PCE.
- In some cases, when an SR-TE policy that was created via the UI is automatically deleted (intentional and expected) from Cisco Crosswork Optimization Engine, a warning message does not appear. For example, if the source PCC is reloaded, the UI created SR policy disappears and the user is not informed.
- In an extreme case where one SR-PCE fails on all links (to PCCs/topology devices) except the up-link to Cisco Crosswork Optimization Engine, then topology information will not be accurate in Cisco

Crosswork Optimization Engine. When this happens, fix the connectivity issue or delete both SR-PCEs from the Provider page and re-add the one that is reachable.

## SR-PCE Configuration Examples

The following configurations are *examples* to guide you in a multiple SR-PCE setup for HA. Please modify accordingly.

### Sample redundant SR-PCE configuration (on PCE with Cisco IOS-XR 7.x.x)

```
pce
  address ipv4 192.168.0.7
  state-sync ipv4 192.168.0.6
  api
    sibling ipv4 192.168.0.6
```

### Sample redundant SR-PCE Configuration (PCC)

```
segment-routing
  traffic-eng
    pcc
      source-address ipv4 192.0.2.1
      pce address ipv4 192.0.2.6
        precedence 200
      !
      pce address ipv4 192.0.2.7
        precedence 100
      !
      report-all
      redundancy pcc-centric
```

### Sample redundant SR-PCE Configuration (on PCC) for RSVP-TE



**Note** Loopback0 represents the TE router ID.

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mpls traffic-eng
  pce
    peer source ipv4 209.165.255.1
    peer ipv4 209.165.0.6
      precedence 200
    !
    peer ipv4 209.165.0.7
      precedence 100
    !
    stateful-client
      instantiation
      report
      redundancy pcc-centric
      autoroute-announce
    !
  !
auto-tunnel pcc
  tunnel-id min 1000 max 1999
!
!
```

### Sample SR-TM Configuration

```

telemetry model-driven
  destination-group crosswork
    address-family ipv4 198.1.219 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_4b3c69a200668b0a8dc155caff295645c684a8f8 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 195](#)).

## Before you begin

You will need to:

- Create a credential profile for the Cisco WAE provider (see [Create Credential Profiles, on page 162](#)). 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.

## Procedure

---

**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 195](#)).

### Before you begin

You will need to:

- Create a credential profile for the storage provider (see [Create Credential Profiles, on page 162](#)). 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.

### Procedure

---

**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
<b>DestinationDirectory</b>	The absolute path where the collected data will be stored on the server. For example: <b>/root/cw-syslogs</b>

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 195](#)).

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 162](#)). 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.

## Procedure

---

**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 **alertViewUrl** 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.

**Add Proxy Providers**

- Step 4** When you have completed entries in all of the required fields, click **Save** to add the alert provider.

## Add Proxy Providers

This section explains how to add a proxy provider in Crosswork. Crosswork supports the addition of the following proxy providers:

- Cisco NSO
- Cisco Optical Network Controller (ONC) version 1.0

The NSO APIs can be directly accessed if NSO is configured with an externally accessible IP address. However, if NSO is deployed in the same private network as the Crosswork network, then it will be reachable only through the Crosswork interface. Proxy providers enables you to use Crosswork interface to perform service provisioning with NSO.

### Before you begin

You will need to:

- Create a credential profile for the Proxy provider (see [Create Credential Profiles, on page 162](#)). This should be a basic HTTP or HTTPS text-authentication credential.
- Know the name of the Resource Facing Service (RFS) node added to the Customer Facing Service (CFS) node in your LSA cluster.
- Know the name you want to assign to the provider. This is usually the DNS hostname of the Proxy server.
- Know the Proxy server IP address and port. The connection protocol will be HTTP or HTTPS.
- Ensure that the Cisco NSO providers are added. For more information, see [Add Cisco NSO Providers, on page 174](#).
- In case of NSO proxy provider, please create a credential profile with **HTTP/HTTPS with Basic Authentication**.
- In case of ONC 1.0 proxy provider, please create a credential profile with **HTTPS with Basic Authentication**.

### Procedure

- Step 1** From the main menu, choose **Administration > Manage Provider Access**.

- Step 2** Click .

- Step 3** Enter the following values for the provider fields:

- **Provider Name:** Name of the Proxy provider.
- **Credential Profile:** Select the previously created credential profile.

**Note**

In case of ONC provider, please select the credential profile configured with ONC TAPI APIs. This is not the ONC UI credentials.

- **Family:** Select **PROXY**.
- **Protocol:** Select **HTTP** or **HTTPS**.
- **IP Address/ Subnet Mask:** Enter the IP address (IPv4 or IPv6) and subnet mask of the NSO cluster or the ONC 1.0 cluster VIP.
- **Port:** Enter the port number (usually, **30603** for HTTPS).
- **Timeout:** (Optional) The amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

**Step 4** Under Provider Properties, enter the following properties:

**Table 15: Provider Properties for NSO proxy provider**

Property Key	Property Value
<b>forward</b>	<b>true</b>
<b>input_url_prefix</b>	<b>/&lt;rfs-node-name&gt;</b>
<b>Note</b> This property is required only in case of RFS nodes.	<b>&lt;rfs-node-name&gt;</b> refers to the name of the RFS node added to the CFS node in the LSA cluster.

**Table 16: Provider Properties for ONC 1.0 proxy provider**

Property Key	Property Value
<b>forward</b>	<b>true</b>
<b>input_url_prefix</b>	<b>/onc-tapi</b>
<b>output_url_prefix</b>	<b>/crosswork/onc-tapi</b>

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

## Import Providers

Complete the steps below to create a CSV file that specifies providers and then import it into the Cisco Crosswork application.

Importing providers from a CSV file adds any providers not already in the database, and updates any providers with the same name as an imported provider. For this reason, it is a good idea to export a backup copy of all your current providers before an import (see [Export Providers, on page 199](#)).

**Procedure**

- 
- 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:
- Click the **Download sample 'Provider template (\*.csv)' file** link and save the CSV file template to a local storage resource.
  - 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.
- 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.

**Procedure**

- 
- Step 1** From the main menu, choose **Administration > Manage Provider Access**.
- For each provider configured in the Cisco Crosswork application, the **Providers** window lists information such as the provider's name, universally unique identifier (UUID), associated credential profile and more, as shown in the figure below.

Figure 79: 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 [Device State, on page 219](#).

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:

- In the **Provider Name** column, click the to view provider-specific key/value properties.
- 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.
- 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).
- 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 182](#). Check that HTTP and port 8080 is set.

For general provider reachability problems, you can troubleshoot as follows:

- Ping the provider host.
- 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"
```

- Check your firewall setting and network configuration.
- 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 178](#) 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 199](#)).

**Procedure**

**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.

**Procedure**

**Step 1** Export a backup CSV file containing the provider you plan to delete (see [Export Providers, on page 199](#)).

**Step 2** (Optional) Check whether any devices are mapped to the provider and change the provider before deletion.

- From the main menu, choose **Device Management > Network Devices**. The **Network Devices** tab is displayed by default.
- In the **Network Devices** window, enter the obsolete provider name in the **Search** field.
- Check the check box for the device that is mapped to the obsolete provider, and click .
- Choose a different provider from the **Provider** drop-down list.
- Click **Save**.

**Step 3** Delete the provider as follows:

- From the main menu, choose **Administration > Manage Provider Access**.
- 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.

---

### Procedure

---

- 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**.



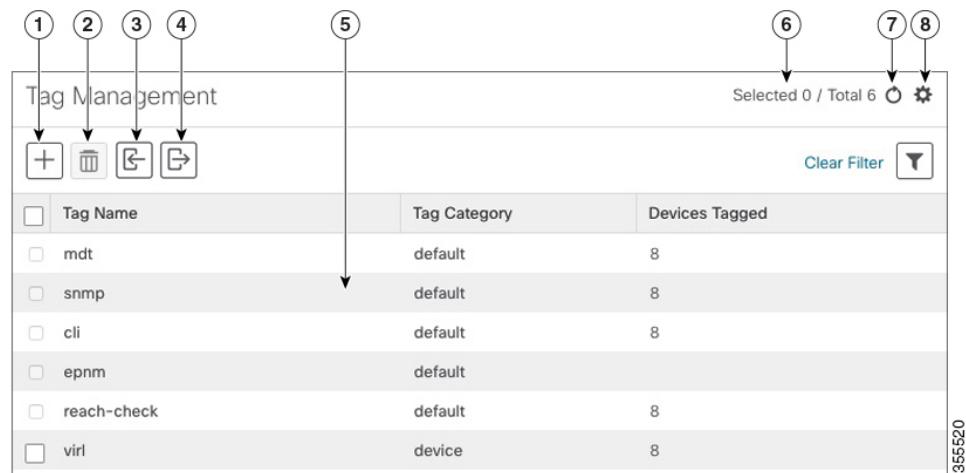
**Note** Cisco Crosswork applications automatically create a default set of tags and assign them to every device they manage:

- cli
- mdt
- reach-check
- snmp
- clock-drift-check

You cannot select, edit, delete, or manually associate these default tags with any device.

---

Figure 80: Tag Management Window



Item	Description
1	Click  to create new device tags. See <a href="#">Create Tags, on page 201</a> .
2	Click  to delete currently selected device tags. See <a href="#">Delete Tags, on page 203</a> .
3	Click  to import the device tags defined in a CSV file into the Cisco Crosswork application. See <a href="#">Import Tags, on page 201</a> . 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 <a href="#">Export Tags, on page 203</a> .
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 <b>Tag Management</b> window.
8	Click  to choose the columns to make visible in the <b>Tag Management</b> window.
	Click  to set filter criteria on one or more columns in the <b>Tag Management</b> window.
	Click the <b>Clear Filter</b> 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 201](#).

**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.

### Procedure

**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 202](#).

## 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 203](#)).

## Procedure

- 
- 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:
- Click the **Download sample 'Tags template (\*.csv)' file** link and save the CSV file template to a local storage resource.
  - 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
<b>Tag Name</b>	Enter the name of the tag. For example: <b>SanFrancisco</b> or <b>Spine/Leaf</b> .	Required
<b>Tag Category</b>	Enter the tag category. For example: <b>City</b> or <b>Network Role</b> .	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.

- 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 202](#).

## Apply or Remove Device Tags

Tags and their categories are your main tool for grouping devices. Once you have tagged a set of devices with the same tag, they are considered part of a group, and you can manage them more easily.

In order to apply a tag to a device or group of devices, the tag must already exist. See [Create Tags, on page 201](#) for more information.

For efficiency, Cisco Crosswork automatically updates inventory data, including topology, for all the devices in a tagged group, as a single set of inventory collection jobs. But please note that tag-group membership is static for other functions.

You can apply a maximum of 15 tags to any one device.

To apply tags to a device or set of devices, do the following:

## Procedure

---

- 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.
- 

## Procedure

---

- Step 1** Export a backup CSV file containing the tags you plan to delete (see [Export Tags, on page 203](#)).
- 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.

## Procedure

---

- 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, on page 205](#)
- [Manage Network Devices, on page 218](#)
- [Device State, on page 219](#)
- [Filter Network Devices by Tags, on page 221](#)
- [Get More Information About a Device, on page 222](#)
- [View Device Job History, on page 222](#)
- [Edit Devices, on page 223](#)
- [Delete Devices, on page 224](#)
- [Work With Device Alerts, on page 225](#)

## 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 206](#) and [Sample Configuration for Cisco NSO Devices, on page 211](#).

In order of preference for most users, the methods and their prerequisites are:

1. **Importing devices using the Crosswork APIs:** : This is the fastest and most efficient of all the methods, but requires programming skills and API knowledge. For more, see the [Inventory Management APIs On Cisco Devnet](#).
2. **Importing devices from a Devices CSV file:** This method can be time-consuming. To succeed with this method, you must first:
  - Create the provider(s) that will be associated with the devices. See [About Adding Providers, on page 171](#).
  - Create corresponding credential profiles for all of the devices and providers listed in the CSV file. See [Create Credential Profiles, on page 162](#).
  - Create tags for use in grouping the new devices. See [Create Tags, on page 201](#).
  - 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 211](#).
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 178](#).
5. **Auto-onboarding using Zero Touch Provisioning:** This method is automated, but requires that you create device entries first and modify your installation's DHCP server. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After provisioning and onboarding devices using this method, you will need to edit each device to add information that is not automatically supplied. For more information, see the *Zero Touch Provisioning* chapter in the *Cisco Crosswork Network Controller 7.0 Device Lifecycle Management Guide*.

**Note**

Cisco Crosswork only supports single-stack deployment modes. The devices can be onboarded with either an IPv4 address or an IPv6 address, not both.

If a device onboarded in Cisco Crosswork is on the same subnet as a 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 Reverse Path Forwarding (RPF) checks and the source address of devices cannot be on the management or northbound networks if multiple 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, GNMI and Telnet. Use them as a guide to configuring the devices you plan to manage.

**Note**

- SNMPv2 and SNMPv3 (Auth/Priv) traps are supported.
- For the device to work seamlessly in Crosswork, the SNMP EngineID generated/configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is re-configured in the device.

### Configure Devices to Forward Events to Crosswork

To ensure that Crosswork can query devices and receive events and notifications from them, you must configure devices to forward events to the Crosswork server. For most devices, this means you must configure the devices to forward SNMP traps and syslogs, and the Data Gateway IP acts as the receiver IP.

If you have a high availability deployment, you must configure devices to forward events to both the primary and secondary servers (unless you are using a virtual IP address).

In most cases, you should configure this using the **snmp-server host** command.

### 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.



**Note** When collecting interface MIB data from IOS XR and XE devices, collectors may receive two split column sets for the same interface index, causing one set to overwrite the other and resulting in the loss of column data. To address this issue, it is recommended to add a configuration to the device's Day 0 setup that sets the SNMP packet size to 4096 bytes. This configuration prevents splits in column sets, thereby improving the reliability of data collection.

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
  exec-timeout 0 0
  width 107
  length 37
  absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
snmp-server packetsize 4096
ntp
  server <NTPServerIPAddress>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf-yang agent
  ssh
!
netconf agent tty
!
xml agent tty
!
```

### 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>
```

## Pre-Onboarding SNMPv2 and SNMPv3 Trap Configuration

If you want the device to send SNMP traps to Cisco Crosswork, use the following commands to perform a pre-onboarding device configuration and test for the trap version you want.

For SNMP v2 traps:

```
snmp-server trap link ietf
snmp-server host <CrossworkDataGatewaySouthboundIPAddress> traps version 2c <Community String>
snmp-server udp-port 1062
snmp-server community <Community String>
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

For SNMP v3 traps:

```
snmp-server trap link ietf
snmp-server host <CrossworkDataGatewaySouthboundIPAddress> traps version 3 <Community String>
snmp-server udp-port 1062
snmp-server community <Community String>
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

For traps to be received, the `node_ip` field for the device as listed in the Cisco Crosswork inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork will reject the traps. Also, the device needs to be in `ADMIN_UP` state for traps to be received.

## Required Settings—Cisco IOS XR Device Operating System

Note that `<SystemOwner>` is a user supplied variable.

```
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered <307200-125000000>

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name cdg_virtualIP
```

Set up VTY options:

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

Telnet and SSH Settings:

```
telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
ssh server v2
```

```
ssh server rate-limit 60
cinetd rate-limit 60
```

Configure the Netconf and XML agents:

```
xml agent tty
netconf agent tty
```

Monitor device with Virtual IP address :

```
ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask
```

Enable CFM modeling:

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read vldefault write vldefault notify vldefault
```

Configure the following to improve the SNMP interface stats response time:

```
snmp-server ifmib stats cache
```

Configure SNMP traps for virtual interfaces to ensure that link-down scenarios are captured:

```
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown
```

Enable SNMP entity field replaceable unit (FRU) control traps:

```
snmp-server traps fru-ctrl
```

Syslogs are used by Crosswork for alarm and event management. NTP settings ensure that Crosswork receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging cdg_virtualIP vrf name
```

Enable performance management on all optical data unit (ODU) controllers:

```
controller oduX R/S/I/P
per-mon enable
```

## Required Settings—Cisco IOS and IOS-XE Device Operating System

```

snmp-server host cdg_virtualIP
snmp-server community public-cmty RO
snmp-server community private-cmty RW
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered 64000 informational

logging source-interface interface_name
logging trap informational
logging event link-status default

```



**Note** The <CrossworkDataGatewaySouthboundIPAddress> denotes the virtual IP address used in the Crosswork Data Gateway pool creation.

Disable domain lookups to avoid delay in Telnet/SSH command response:

```
no ip domain-lookup
```

Enable SSH

```

crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]

```

Setup VTY options:

```

line vty <number of vty>
exec-timeout
session-timeout
transport input ssh (require only if ssh is used)
transport output ssh (required only if ssh is used)

```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

For SNMPv3 only, configure the following settings:

```

snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group

```

```

snmp-server group Group v3 priv read v1default write v1default notify v1default
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify crosswork read crosswork

```

Configure the cache settings at a global level to improve the SNMP interface response time using the configuration:

```
snmp-server cache
```

Syslogs are used by Crosswork for alarm and event management. NTP settings ensure that Crosswork receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```

clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging cdg_virtualIP vrf default severity info [port default]

```

## Sample Configuration for Cisco NSO Devices

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.

### Procedure

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

## Add Devices through the UI

- 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 17: Add New Device Window (\*=Required)

Field	Description
* <b>Administration State</b>	The management state of the device. Options are <ul style="list-style-type: none"> <li>• <b>UNMANAGED</b>—Crosswork is not monitoring the device.</li> <li>• <b>DOWN</b>—The device is being managed and is down.</li> <li>• <b>UP</b>—The device is being managed and is up.</li> </ul>
* <b>Reachability Check</b>	Determines whether Crosswork performs reachability checks on the device. Options are: <ul style="list-style-type: none"> <li>• <b>ENABLE</b> (In CSV: <b>REACH_CHECK_ENABLE</b>)—Checks for reachability and then updates the Reachability State in the UI automatically.</li> <li>• <b>DISABLE</b> (In CSV: <b>REACH_CHECK_DISABLE</b>)—The device reachability check is disabled.</li> </ul> Cisco recommends that you always set this to <b>ENABLE</b> . This field is optional if <b>Configured State</b> is marked as <b>UNMANAGED</b> .
* <b>Credential Profile</b>	The name of the credential profile to be used to access the device for data collection and configuration changes. For example: <b>nso23</b> or <b>srpce123</b> . This field is optional if <b>Configured State</b> is marked as <b>UNMANAGED</b> .
<b>Host Name</b>	The host name of the device.
<b>Inventory ID</b>	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.
<b>Software Type</b>	Software type of the device. <b>Note</b> Some third-party vendor devices require a specific string to be entered as part of the <b>Software Type</b> field. These are the required strings for different vendors: <ul style="list-style-type: none"> <li>• Juniper devices: JUNOS</li> <li>• Huawei devices: VRP</li> <li>• Nokia devices: TIMOS</li> </ul>
<b>Software Version</b>	Software version of the device.

Field	Description
<b>UUID</b>	Universally unique identifier (UUID) for the device.
<b>Serial Number</b>	Serial number for the device.
<b>MAC Address</b>	MAC address of the device.
<b>* Capability</b>	<p>The capabilities that allow collection of device data and that are configured on the device. You must select at least <b>SNMP</b> as this is a required capability. The device will not be onboarded if <b>SNMP</b> is not configured. Other options are <b>YANG_MDT</b>, <b>YANG_CLI</b>, <b>TL1</b>, and <b>GNMI</b>. The capabilities you select will depend on the device software type and version.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>For devices with MDT capability, do not select <b>YANG_MDT</b> at this stage.</li> <li>To enable Crosswork to receive the Syslog-based data, select <b>YANG_CLI</b>.</li> </ul>
<b>Tags</b>	<p>The available tags to assign to the device for identification and grouping purposes.</p> <p>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.</p>
<b>Product Type</b>	Product type of the device.
<b>Syslog Format</b>	<p>The format in which syslog events received from the device should be parsed by the Syslog Collector. The options are:</p> <ul style="list-style-type: none"> <li><b>UNKNOWN</b> - 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.</li> <li><b>RFC5424</b> - Choose this option to parse syslog events received from the device in RFC5424 format.</li> <li><b>RFC3164</b> - Choose this option to parse syslog events received from the device in RFC5424 format.</li> </ul> <p>Refer to Section: <a href="#">Syslog Collection Job Output, on page 79</a> for more details.</p>
<b>Connectivity Details</b>	
<b>Protocol</b>	<p>The connectivity protocols used by the device. Choices are: <b>SNMP</b>, <b>NETCONF</b>, <b>TELNET</b>, <b>HTTP</b>, <b>HTTPS</b>, <b>GNMI</b>, <b>TL1</b>, and <b>GRPC</b>.</p> <p><b>Note</b></p> <p>Toggle the <b>Secure Connection</b> slider to secure the GNMI protocol that you have selected.</p> <p>To add more connectivity protocols for this device, click <b>+</b> at the end of the first row in the <b>Connectivity Details</b> panel. To delete a protocol you have entered, click <b>×</b> shown next to that row in the panel.</p> <p>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 <b>SSH</b> and <b>SNMP</b>. If you do not configure <b>SNMP</b>, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for <b>NETCONF</b>. <b>TELNET</b> connectivity is optional.</p>

## Add Devices through the UI

Field	Description
* IP Address / Subnet Mask	<p>Enter the device's IP address (IPv4 or IPv6) and subnet mask.</p> <p><b>Note</b> 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.</p> <p><b>Note</b> If you have multiple protocols with same IP address and subnet mask, you can instruct Crosswork to autofill the details in the other fields.</p>
* Port	<p>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 <b>Protocol</b> you chose. The standard port assignments for each protocol are:</p> <ul style="list-style-type: none"> <li>• SSH: 22</li> <li>• SNMP: 161</li> <li>• NETCONF: 830</li> <li>• TELNET: 23</li> <li>• HTTP: 80</li> <li>• HTTPS: 443</li> </ul> <p>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.</p>
Timeout	<p>The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds.</p> <p>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.</p>
Encoding Type	<p>This field is only applicable for <b>GNMI</b> and <b>GNMI_SECURE</b> protocols. The options are <b>PROTO</b> and <b>JSON IETF</b>.</p> <p>Based on device capability, only one encoding format is supported at a time in a device.</p>
Encryption	<p>This field is only applicable for <b>SNMP</b> protocol.</p> <p>From the drop-down menu, select the relevant SNMPv3 protocol supported by the device. The default value is <b>NONE</b>.</p> <p>The drop-down menu lists Advanced Encryption Standard (AES) specifications in Counter mode (CTR), Galois/Counter mode (GCM), and Cipher Block Chaining mode (CBC) for different key lengths (128-bit, 192-bit, 256-bit).</p> <p>The credential profile supports generic privacy types such as AES-192 and AES-256. In case of Cisco devices, AES-192 and AES-256 are customized as CiscoAES192 and CiscoAES256 protocols. On the devices, these protocols are displayed as aes256-ctr, <a href="mailto:aes256-gcm@openssh.com">aes256-gcm@openssh.com</a>, aes256-cbc, aes192-ctr, and aes192-cbc. The Cisco devices will only respond to Crosswork's polling if it is based on the new protocol variations.</p> <p>For devices other than Cisco, select <b>None</b> in the <b>Encryption</b> field.</p>

Field	Description
<b>SNMP Disable Trap Check</b>	This check box appears when the protocol field is set to <b>SNMP</b> . Selecting this check box, disables the SNMPv2 community string validation between the network device and Crosswork Data Gateway.
<b>Routing Info</b>	
<b>ISIS System ID</b>	The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.
<b>OSPF Router ID</b>	The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.
<b>*TE Router ID</b>	The traffic engineering router ID for the respective IGP.  <b>Note</b> For visualizing L3 links in topology, devices should be onboarded to Cisco Crosswork with the <b>TE Router ID</b> field populated.
<b>IPv6 Router ID</b>	IPv6 router ID for the device. This field is a configurable parameter, and cannot be autodiscovered by Crosswork.
<b>Streaming Telemetry Config</b>	
<b>Vrf</b>	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
<b>Source Interface</b>	The range of loopback in the device type. This field is optional.  <b>Note</b> This field can be edited only when the device is in DOWN or UNMANAGED state.
<b>Opt Out MDT Config</b>	Enabling this checkbox skips Crosswork from pushing telemetry configuration to the device via NSO. The default setting state is Disabled (which allows Crosswork to push telemetry configuration to the device via NSO).  The device must be in ADMIN DOWN state to toggle this setting. Any out of band configuration setup needs to be cleared before moving the setting from Enabled to Disabled.
<b>Location</b>	
All location fields are optional, with the exception of <b>Longitude</b> and <b>Latitude</b> , which are required for the geographical view of your network topology.	
<b>Longitude, Latitude</b>	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.
<b>Altitude</b>	The altitude, in feet or meters, at which the device is located. For example, <b>123</b> .
<b>Providers and Access</b>	
To add more providers for this device, click  at the end of the first row in the <b>Providers and Access</b> panel. To delete a provider you have entered, click  shown next to that row in the panel.	
<b>Provider Family</b>	Provider type used for topology computation. Choose a provider from the list.

**Add Devices by Importing from CSV File**

Field	Description
<b>Provider Name</b>	Provider name used for topology computation. Choose a provider from the list. <b>Note</b> For Cisco NSO LSA deployment, the user can select the resource-facing service (RFS) node to which they want to assign the device.
<b>Credential</b>	The Credential profile used for the provider. This field is read-only and is autopopulated based on the provider you select.

## Add Devices by Importing from CSV File

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

Importing devices from a CSV file adds any devices not already in the database, and overwrites the data in any device record with an Inventory Key Type field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import). For this reason, it is a good idea to export a backup copy of all your current devices before an import.

**Attention**

- While importing a 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, log in to Cisco Crosswork in a new tab or window, and onboard devices with correct CSV values.
- The CSV files created on a Windows machine should contain a newline (marked with a 'newline' character) for the file to be processed as expected. Any newline created using the "carriage return" option will not work.

### Procedure

- 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:
- Click the **Download sample 'Device Management template (\*.csv)' file** link and save the CSV file template to a local storage resource.
  - 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 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 211](#).

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 created in the previous steps 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, the 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.

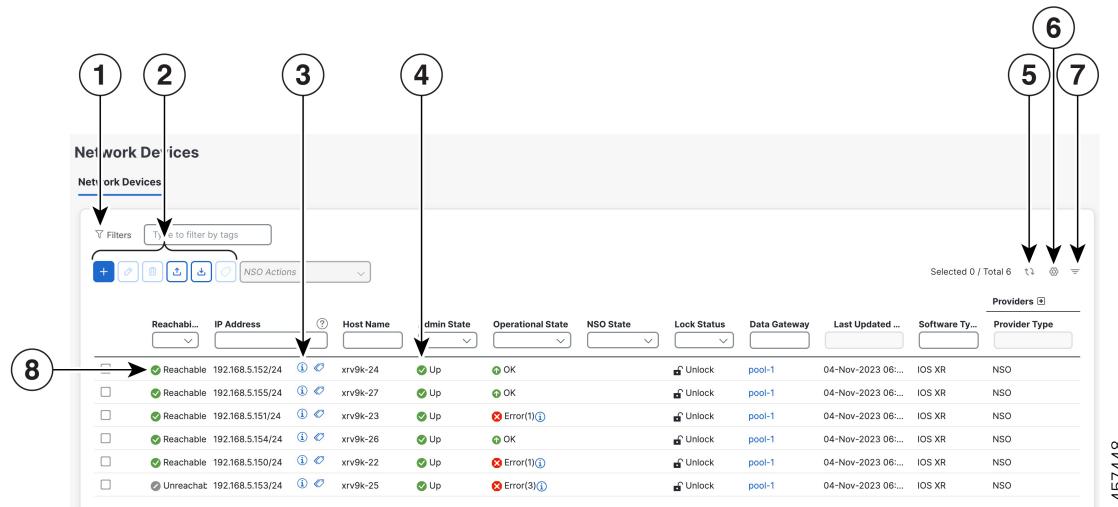
### Procedure

- Step 1** From the main menu, choose **Device Management > Network Devices**. The **Network Devices** tab is displayed by default.
- Step 2** (Optional) Filter the device list as needed.
- Step 3** Check the check boxes for the devices you want to export. 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 81: Network Devices Window*



457448

Item	Description
1	The <b>Filter by tags</b> 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	<p>Click the  to add a new device to the device inventory.</p> <p>Click the  to edit the information for the currently selected devices. .</p> <p>Click the  to delete the currently selected devices.</p> <p>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.</p> <p>Click the  to export information for selected devices to a CSV file.</p> <p>Click the  to modify tags applied to the selected devices. See .</p>
3	Click the  to open the <b>Device Details</b> pop-up window, where you can view important information for the selected device.
4	Icons in the <b>Administration State</b> 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	<p>Click  to set filter criteria on one or more columns in the Devices list.</p> <p>Click the <b>Clear Filter</b> link to clear any filter criteria you may have set.</p>
8	Icons in the <b>Reachability State</b> column show whether a device is reachable or not.

## Device State

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

**Table 18: Device State Icons**

This Icon...	Indicates...
<b>Reachability State</b> 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 the provider.

This Icon...	Indicates...
	Reachability Degraded: The device or provider can be reached by at least one protocol, but is not fully configured for it.
	Unreachable: The device or provider cannot be reached by any protocol configured for it.
	Reachability Unknown: Cisco Crosswork cannot determine if the device is reachable, degraded, or 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".
	The device's operational or configuration state is unknown.
	The device's operational or configuration state is degraded.
	The device's operational or configuration state is in an error condition. It is either not up, or unknown. It is also used when Cisco Crosswork is attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available for all device types).
	The device's operational state is currently being checked.
	The device is being deleted.
	The device is unmanaged.

**NSO State** icons show whether a device is synced with Cisco NSO or not.

#### Note

In the initial sync between Cisco Crosswork and NSO after onboarding a device, the NSO state column in the device will be UNKNOWN. This is because NSO state is not determined if the device needs to sync with NSO based on the policy, and cannot select the default state in the initial sync.

	The device is in sync with Cisco NSO.
	The device is out of sync with Cisco NSO.

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:

### Procedure

**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 82: 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.

## Procedure

- 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 83: Inventory Jobs window**

Status	Description	Impacted	Start Time	End Time	User Name
Completed	Add Tags to Node		20-Nov-2023 08:23:03 PM IST	20-Nov-2023 08:23:03 PM IST	internal@capp-hi
Completed	Insert 1 Tag(s)		20-Nov-2023 08:21:44 PM IST	20-Nov-2023 08:21:44 PM IST	internal@capp-hi
Completed	Update 1 Credential(s)		17-Nov-2023 12:08:29 AM IST	17-Nov-2023 12:08:29 AM IST	admin
Completed	Update 1 Credential(s)		17-Nov-2023 12:05:58 AM IST	17-Nov-2023 12:05:59 AM IST	admin
Completed	Update 1 Credential(s)		17-Nov-2023 12:04:40 AM IST	17-Nov-2023 12:04:40 AM IST	admin
Completed	NSO Device Check Sync		16-Nov-2023 11:48:15 PM IST	16-Nov-2023 11:48:20 PM IST	admin
Completed	NSO Device Sync From		16-Nov-2023 02:17:45 AM IST	16-Nov-2023 02:18:56 AM IST	admin
Completed	NSO Device Fetch Ssh Keys		16-Nov-2023 02:16:17 AM IST	16-Nov-2023 02:16:33 AM IST	admin
Completed	Update Mappings for 1 Data Gateway		16-Nov-2023 01:22:47 AM IST	16-Nov-2023 01:22:47 AM IST	admin
Completed	Insert 1 Tag(s)		15-Nov-2023 03:45:26 AM IST	15-Nov-2023 03:45:26 AM IST	internal@cw-fault-event-process...
Completed	Insert 1 Tag(s)		15-Nov-2023 03:45:17 AM IST	15-Nov-2023 03:45:17 AM IST	internal@cw-fault-event-process...
Warning ⓘ	Add/Replace 6 Node(s) Via CSV Upload (Completed with ...)		15-Nov-2023 03:32:10 AM IST	15-Nov-2023 03:32:10 AM IST	admin
Completed	Delete 1 Provider(s)		15-Nov-2023 03:21:53 AM IST	15-Nov-2023 03:21:53 AM IST	admin
Completed	Update 1 Provider(s)		15-Nov-2023 03:21:54 AM IST	15-Nov-2023 03:21:54 AM IST	admin
Completed	Update 1 Credential(s)		15-Nov-2023 03:21:12 AM IST	15-Nov-2023 03:21:12 AM IST	admin
Completed	Update 1 Credential(s)		15-Nov-2023 03:15:03 AM IST	15-Nov-2023 03:15:03 AM IST	admin
Completed	Add/Update 2 Provider(s) Via CSV Upload		15-Nov-2023 03:14:28 AM IST	15-Nov-2023 03:14:28 AM IST	admin
Completed	Update 1 Provider(s)		15-Nov-2023 03:14:28 AM IST	15-Nov-2023 03:14:28 AM IST	admin

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.

### Note

The status may be displayed as **Successful** even when the device is not reachable. You can verify that the status of the jobs that is displayed is correct by also looking into the status of the device (**Device Management > Network Devices**).

## 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.

## Procedure

- Step 1** From the main menu, choose **Device Management > Network Devices**.
- Step 2** (Optional) Filter the list of devices by filtering specific columns.

**Delete Devices**

**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**

User-configured parameters like ISIS System ID and OSPF Router ID are not auto-discovered by Crosswork device management for onboarded devices. These fields may appear blank when you edit the device, however, the topology page for the same device will display the parameters.

**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 **auto-onboard** property as **managed** or **unmanaged** for an SR-PCE provider, set **auto-onboard** as **off** for one or more SR-PCEs.
- 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 **auto-onboard** is not **off** and it is still functional and connected to the network, the device will be rediscovered as unmanaged when it is deleted.

**Procedure**

**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**.

# Work With Device Alerts

Cisco Crosswork refers to device alarms and events as "alerts". The **Device Alarms** and **Device Events** windows give you a consolidated list of all alerts for your devices. You can toggle between the **Device Alarms** and **Device Events** windows using the **Show** option on each window.

To view the **Device Alarms** window, select **Alerts > Device Alarms**. By default, Crosswork displays the **Device Alarms** window with the **Show** selection set to **Alarms**, as shown in the first figure below.

To view the **Device Events** window, first select **Alerts > Device Alarms**. Then change the **Show** selection to **Events**. Crosswork displays the **Device Events** window, as shown in the second figure below.

**Figure 84: Device Alarms Window**

523501

Alarm ID	Severity	Source	Status	Description	Condition	Managed Object	Last Updated
470470	Major	P-TOPLEFT	Not Acknowledged	Device: P-TOPLEFT RSVP lost a flow...	lostFlow	Device: P-TOPLEFT	09-Oct-2023 08:44:57 P...
470471	Major	P-BOTTOMLEFT	Not Acknowledged	Device: P-BOTTOMLEFT RSVP ...	lostFlow	Device: P-BOTTOMLEFT	09-Oct-2023 08:44:57 P...
470500	Major	P-BOTTOMLEFT	Not Acknowledged	EVPN id: 11, with Source: 114...	EVPN-5-VC_STATUS	EVPN-5-VC	09-Oct-2023 08:44:52 P...
469471	Major	PE-B	Not Acknowledged	Device: PE-B' Peer2 FSM with B...	cbgpPeer2 fsmStateCh...	Device: PE-B'	09-Oct-2023 08:43:22 P...
470514	Minor	P-BOTTOMLEFT	Not Acknowledged	Device: 192.168.6.1:80: Received...	isisOrgLSPBufSizeMsm...	MgmtEth0/RP0/CPU0/...	09-Oct-2023 08:40:41 P...
469526	Minor	P-TOPRIGHT	Not Acknowledged	Device: 192.168.6.1:81: Received...	isisOrgLSPBufSizeMsm...	Device: 192.168.6.1:81...	09-Oct-2023 08:40:39 P...
470513	Minor	P-TOPLEFT	Not Acknowledged	Device: 192.168.6.1:80: Received...	isisOrgLSPBufSizeMsm...	Device: 192.168.6.1:80...	09-Oct-2023 08:40:37 P...
469525	Minor	PE-C	Not Acknowledged	Device: 192.168.6.1:79: Received...	isisOrgLSPBufSizeMsm...	MgmtEth0/RP0/CPU0/0	09-Oct-2023 08:40:35 P...
469524	Minor	PE-B	Not Acknowledged	Device: 192.168.6.1:78: Received...	isisOrgLSPBufSizeMsm...	MgmtEth0/RP0/CPU0/0	09-Oct-2023 08:40:34 P...

**Figure 85: Device Events Window**

523502

Event ID	Severity	Source	Description	Timestamp
431	Minor	PE-B	Device: PE-B', Generic Event for: <logMessageGenera...	09-Oct-2023 08:48:05 PM IST
442	Minor	P-BOTTOMLEFT	Device: P-BOTTOMLEFT: Generic Event for: <logMess...	09-Oct-2023 08:48:05 PM IST
441	Minor	P-TOPRIGHT	Device: P-TOPRIGHT: Generic Event for: <SECURITY-...	09-Oct-2023 08:48:05 PM IST
440	Minor	P-BOTTOMRIGHT	Device: P-BOTTOMRIGHT: Generic Event for: <SECURI...	09-Oct-2023 08:48:05 PM IST
439	Minor	P-BOTTOMRIGHT	Device: P-BOTTOMRIGHT: Generic Event for: <SECURI...	09-Oct-2023 08:48:05 PM IST
438	Minor	PE-A	Device: PE-A: Generic Event for: <logMessageGenera...	09-Oct-2023 08:48:05 PM IST
437	Minor	PE-A	Device: PE-A: Generic Event for: <SECURITY-LOGIN-...	09-Oct-2023 08:48:05 PM IST
436	Minor	PE-C	Device: PE-C: Generic Event for: <SECURITY-LOGIN-...	09-Oct-2023 08:48:05 PM IST
435	Minor	PE-C	Device: PE-C: Generic Event for: <logMessageGenera...	09-Oct-2023 08:48:05 PM IST

Item	Description
1	<p>Click the selection box next to the <b>Alarm ID</b> or <b>Event ID</b> column to select one or more alerts. Click the blue ID link in the <b>Alarm ID</b> or <b>Event ID</b> column to view details for that alert. See <a href="#">View Alert Details, on page 227</a> for more information.</p> <p>On the <b>Device Alarms</b> window only: When you have one or more alarms selected, Crosswork enables the <b>Actions</b> menu, so you can acknowledge, clear or annotate the selected alarms.</p>
2	<p>Click the  icon to export a PDF or CSV file listing full information for all the alerts shown in the window. If you have one or more alerts selected at the time you click the icon, the file will contain information for the selected alerts only. See <a href="#">Export Alerts, on page 231</a> for more information.</p>
3	<p>On the <b>Device Alarms</b> window only:</p> <p>Click the <b>Actions</b> dropdown menu to perform one or more of these actions on the currently selected alarms:</p> <ul style="list-style-type: none"> <li>• <b>Acknowledge:</b> Marks the currently selected alarms as acknowledged. See <a href="#">Acknowledge Alarms, on page 228</a> for more information.</li> <li>• <b>Unacknowledge:</b> If any of the currently selected alarms have been acknowledged, restores them to the unacknowledged state.</li> <li>• <b>Clear:</b> Removes all currently selected alarms from the <b>Device Alarms</b> window. See <a href="#">Clear Alarms, on page 229</a> for more information.</li> <li>• <b>Clear all of this condition:</b> Removes all currently selected alarms that share the same condition.</li> <li>• <b>Notes:</b> Lets you add a text note to all of the currently selected alarms. See <a href="#">Annotate Alarms, on page 229</a> for more information.</li> </ul> <p>Crosswork enables the <b>Actions</b> menu only until you select one or more alarms using the selection box next to the <b>Alarm ID</b> column.</p>
4	<p>Toggles between the <b>Device Alarms</b> and <b>Device Events</b> windows.</p>
5	<p>On the <b>Device Alarms</b> window only:</p> <p>Move the slider to set the window to display <b>All Alarms</b> or <b>Active Alarms only</b>. The default is <b>Active Alarms only</b>.</p>
6	<p>Click on <b>More Options</b> to specify whether you want to view all alerts or only the latest, and how often to sync the alerts display with the Crosswork database.</p> <p>If you uncheck the <b>Alarm History</b> or <b>Event History</b> checkbox, the list shows all alerts.</p> <p>If you uncheck the <b>Auto Sync</b> checkbox, Crosswork pauses synchronization.</p>
7	<p>Click in the <b>Saved Views</b> field to manage the previously saved views created using the <b>Save View</b> button. The popup <b>Manage Saved Views</b> window allows you to view, sort, see all views or only those you have saved. See <a href="#">Work With Saved Alert Views, on page 230</a> for more information.</p>

Item	Description
8	Click the <b>Save View</b> button to save the current view. Crosswork will prompt you to enter and save the view under a unique name.
9	Click the  to select which columns to display in the alerts list.
10	Click the  to toggle display of the floating filter fields at the top of the alerts list. You can use these fields to set filter criteria on one or more columns in the list. Click the <b>Filters Applied</b> link, shown next to the icon, to clear any filter criteria you have set.

Crosswork lets you customize the alert settings to suit your production requirements. Click on the below topics for more information:

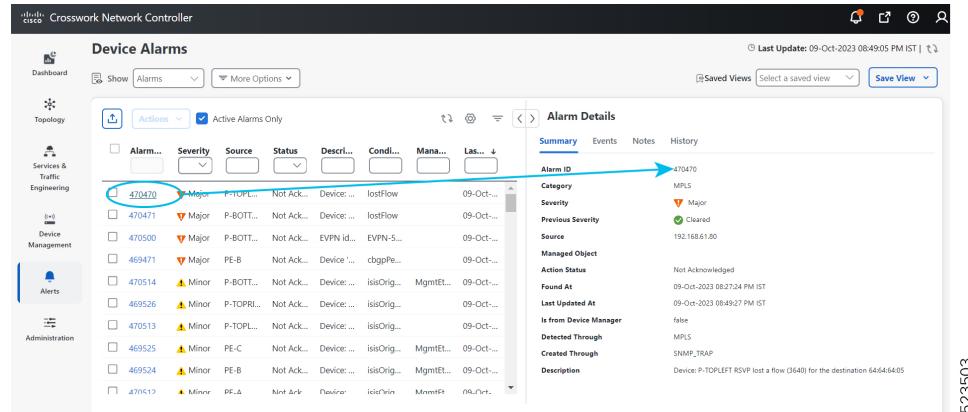
- [Customize Alerting Devices, on page 232](#)
- [Customize Alarm Auto Clear, on page 232](#)
- [Customize Instructive Text for Alarms, on page 233](#)
- [Customize Alert Cleanup, on page 234](#)
- [Customize Alarm Severity, on page 235](#)

## View Alert Details

Whenever you select **Alerts > Device Alerts** and display the list of alarms or events, you can click the ID number for any alert in the **Alarm ID** or **Event ID** column to get more information about that alert.

For example: If you select **Alerts > Device Alerts** to display the **Device Alarms** window, clicking on an ID number in the **Alarm ID** column opens an **Alarm Details** window like the one shown in the illustration below:

**Figure 86: Alarm Details Window: Summary Tab**



The **Summary** tab is the default, showing basic information about the alarm you selected.

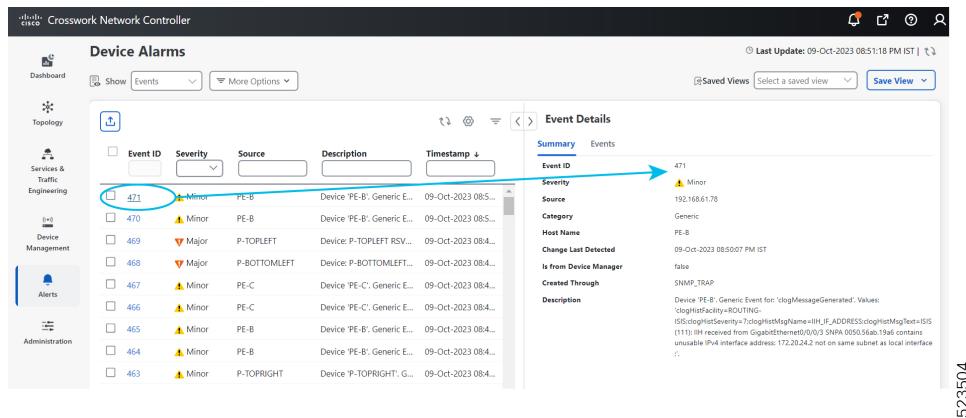
While viewing the **Alarm Details** window, you can click on:

## Acknowledge Alarms

- The  next to the **Condition** field on the **Summary** tab. If customized for your organization, this displays a description of the condition and the action your organization recommends that you take to clear the alarm.
  - The **Events** tab to see correlated events for the alarm you selected.
  - The **Notes** tab to view annotations you or your colleagues have added to the alarm.
  - The **History** tab to see information about when and how the alarm was raised and resolved.

You can do the same thing with events. For example: If you select **Alerts > Device Alerts** and then select **Events** in the **Show** field, Crosswork displays the **Device Events** window. If you then click on an ID number in the **Event ID** column, Crosswork displays an **Event Details** window like the one shown below:

**Figure 87: Event Details Window: Summary Tab**



The **Event Details** window's **Summary** tab is the default, showing basic information about the event you selected.

While viewing the **Event Details** window, you can click on the **Events** tab to see other events correlated with the event you selected.

## Acknowledge Alarms

Follow these steps to acknowledge device alarms, or return acknowledged alarms back to unacknowledged status. You can acknowledge multiple alarms at the same time by selecting their check boxes before selecting **Actions > Acknowledge**.

Acknowledging an alarm clears it permanently, but the alarm will still be listed in the **Device Alarms** window.

## Procedure

- Step 1** From the main menu, choose **Device Alerts > Device Alarms**. Crosswork displays the **Device Alarms** window.

**Step 2** (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider, or adding or removing columns using the 

- Step 3** (Optional) Filter the list of alarms by filtering columns, or by adding or removing columns using the  and then filtering again. Use the **More Options** dropdown to choose whether you want to see only current alarms, and how often the window syncs the displayed list with the Crosswork database. Move the **Active Alarms Only** slider to show all alarms.
- Step 4** Check the check box next to the ID of the alarm(s) you want to acknowledge.
- Step 5** Select **Actions > Acknowledge**.
- Step 6** Click **OK** to complete the acknowledgment action.
- Step 7** To return an acknowledged alarm to the unacknowledged status:
- Check the check box next to the ID of an acknowledged alarm.
  - Select **Actions > Unacknowledged**. Crosswork resets the alarm status to unacknowledged.
- 

## Clear Alarms

Follow these steps to clear device alarms. You can clear one or multiple alarms by selecting their check boxes. You can also choose to clear all alarms reporting the same alarm condition (such as "lostFlow" or "mplsTunnelDown").

Clearing an alarm removes it from the **Device Alarms** window, but the alarm will be generated again if the triggering event recurs.

### Procedure

---

- Step 1** From the main menu, choose **Device Alerts > Device Alarms**. Crosswork displays the **Device Alarms** window.
- Step 2** (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider to show all alarms, or by adding or removing columns using the . Use the **More Options** dropdown to choose whether you want to see only current alarms or all alarms, and how often the window syncs the displayed list with the Crosswork database.
- Step 3** Check the check box next to the ID of the alarm(s) you want to clear, then select **Actions > Clear**.
- Step 4** Click **OK** to complete the clear action.
- Step 5** To clear all alarms sharing the same condition:
- Check the check box next to the ID of one or more alarms sharing the conditions you want to clear (you may select alarms with different conditions).
  - Select **Actions > Clear all of this condition**.
  - Click **OK** to complete the clear-all action.
- 

## Annotate Alarms

Alarm notes are a handy way to share information with colleagues and record important information missed by automated monitoring. Notes are permanently attached to the alarm and are retrievable until the alarm is cleared from the database or deleted by a user. The user ID of the note taker is stored with the note.

Follow the steps below to annotate device alarms. You can annotate multiple alarms at the same time by selecting their check boxes before choosing to add a note. Notes support entries in plain text only.

## Procedure

- 
- Step 1** From the main menu, choose **Device Alerts > Device Alarms**. Crosswork displays the **Device Alarms** window.
- Step 2** (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider to show all alarms, or by adding or removing columns using the . Use the **More Options** dropdown to choose whether you want to see only current alarms or all alarms, and how often the window syncs the displayed list with the Crosswork database.
- Step 3** Check the check box next to the ID of the alarm(s) you want to annotate.
- Step 4** Select **Actions > Notes**. Crosswork displays the **Add annotation** popup.
- Step 5** Enter the text of the note you want to add to the selected alarm(s).
- Step 6** Click **Add** to add the note.
- 

## Work With Saved Alert Views

You can use the filtering options on the **Device Alarms** and **Device Events** windows to show only the alerts you want. You can then save this filtered display as a saved view. You and other Crosswork users can recall the saved view to the window with a few clicks.

Note that individual Alarms and Events shown when you recall a saved view may vary from the alerts shown in the view when you first saved it, depending on the current state of your network devices.

### To filter your view to the alerts you want:

- Click the  as needed to toggle on the floating filter fields at the top of the **Device Alarms** or **Device Events** list. Then, in one or more of the fields, enter or select the criteria that the alerts must match to appear in the list.
- Click the  to choose the columns shown in the **Device Alarms** or **Device Events** list.
- On the **Device Alarms** window only: Move the **Active Alarms Only** slider to the left to enable display of all alarms, or to the right to display only active alarms.

### To save the current view as a new saved view:

1. Filter the alerts on your current view as needed.
2. If a saved view is already displayed, click the  icon next to the saved view's name in the **Saved Views** field. If you don't do this, you will overwrite the current saved view with the current view, and will not be prompted to change the saved view's name.
3. Click **Save View**.
4. Enter a unique name for the new saved view.
5. Click **Save**.

### To display a saved view:

1. Next to the **Saved Views** field, click the . Crosswork displays the **Manage Saved Views** window.

2. Find the saved view you want to display by clicking on the **My Views** or **All Views** tab, selecting an option from the **Sort By** menu, or by entering criteria in the search field with the .
3. Click on the name of the saved view you want to display. Crosswork changes the alerts list to display the saved view.

**To overwrite the current saved view:**

1. Display the save view you want to overwrite.
2. Filter the alerts as needed.
3. Click **Save View**. Crosswork overwrites the saved view with the current view.

**To delete a saved view:**

1. Next to the **Saved Views** field, click the . Crosswork displays the **Manage Saved Views** window.
2. Find the saved view you want to delete by clicking on the **My Views** or **All Views** tab, selecting an option from the **Sort By** menu, or by entering criteria in the search field with the .
3. Click the  next to the name of the saved view you want to delete. Crosswork deletes the saved view.

## Export Alerts

Follow these steps to export device alerts for offline storage and analysis.

You must be viewing alarms to export alarms, or events if you want to export events. You can choose to export alerts to comma-separated values (CSV) or PDF file formats.

By default, Crosswork exports all the alerts currently visible in the **Device Alarms** or **Device Events** list. You can limit the contents of the exported file to just the alerts you want by filtering the list, or selecting the checkbox next to the alerts you want, before clicking the .

### Procedure

- 
- Step 1** From the main menu, choose **Device Alerts > Device Alarms**. Crosswork displays the **Device Alarms** window. If you want to export events instead of alarms: In the **Show** dropdown, select **Events**.
- Step 2** (Optional) Filter the list of events to be exported by filtering columns, or by adding or removing columns using the  and then filtering again. Use the **More Options** dropdown to choose whether you want to see only current alerts or all alerts, and how often the window syncs the displayed list with the Crosswork database. For alarms only: Move the **Active Alarms Only** slider. You can also check the check box next to the ID of only the alerts you want to export. For alarms only: Move the **Active Alarms Only** slider. You can also check the check box next to the ID of the alerts you want to export.
- Step 3** Click . Crosswork displays an export popup window appropriate for the type of alert you want to export.
- Step 4** In the **Name** field, enter the name of the destination file (don't include a filename extension).
- Step 5** Using the **Format** button, select **CSV** or **PDF**.

- Step 6** Click **OK** to begin the export, and specify the storage location for the new file.

## Customize Alerting Devices

Crosswork lets you customize the set of Cisco devices from which you want to receive alerts.

### Procedure

- Step 1** From the main menu, choose **Administration > System Settings > Device Alarm Settings > Device Alarm Admin > Manager Settings**. Crosswork displays the **Manager Settings** window, with a list of all the Cisco devices from which Crosswork can receive alerts.
- Step 2** (Optional) Filter the list of devices by filtering on the **Name** and **Status** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To start receiving alerts from a device type, click the checkbox shown next to the device type's name and then click **Enable**.
- Step 4** To stop receiving alerts from a device type, click the selection checkbox shown next to the device type's name and then click **Disable**.
- Step 5** When you are finished making changes, click **Save** to apply them.

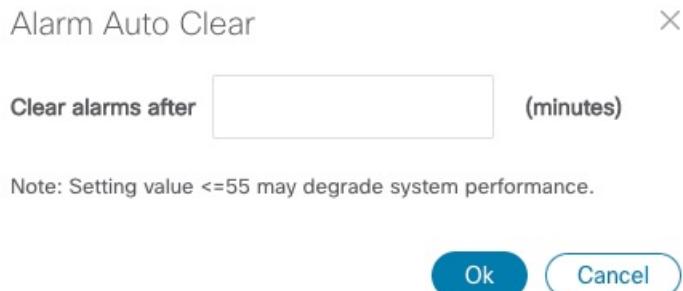
## Customize Alarm Auto Clear

Crosswork lets you customize whether an alarm can be automatically cleared and how many minutes to wait before automatically clearing it.

### Procedure

- Step 1** From the main menu, choose **Administration > System Settings > Device Alarm Settings > Severity and Auto Clear**. Crosswork displays the **Severity and Auto Clear** window, showing the list of all the standard alarm types.
- Step 2** (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto Clear Duration** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To assign a time after which an alarm will be automatically cleared, click on the check box shown next to that alarm's name in the list. Then click **Alarm Auto Clear**.
- Step 4** With the **Alarm Auto Clear** window displayed, enter the number of minutes to wait before clearing in the **Clear alarms after** field. Then click **OK**.

Figure 88: Alarm Auto Clear Window



- Step 5** To stop an alarm from being automatically cleared, first select it in the list and then click **Revert Alarm Auto Clear**.  
**Step 6** When you are finished making changes, click **Save** to apply them.
- 

## Customize Instructive Text for Alarms

Crosswork enables you customize the instructive "explanation" and "recommended action" text available for each of the alarms in the Crosswork database. If you or another user have made changes to these texts, you can also choose to restore the original text.

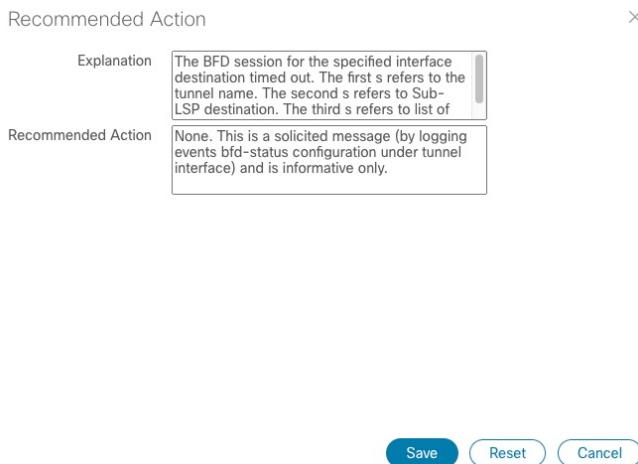
### Procedure

---

- Step 1** From the main menu, choose **Administration > System Settings > Device Alarm Settings > Severity and Auto Clear**. Crosswork displays the **Severity and Auto Clear** window, showing the list of all the standard alarm types.
- Step 2** (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto Clear Duration** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To customize an alarm's instructive text, click on the check box shown next to that alarm's name in the list. Then click **Recommended Action** to display the **Recommended Action** window.

## Customize Alert Cleanup

Figure 89: Recommended Action Window



- Step 4** Click in the **Explanation** and **Recommended Action** fields and enter the text you want. You can enter any form of plain ASCII text in these fields, or edit the text already there. When you are finished, click **Save**.
- Step 5** To revert back to the original Crosswork instructive text for an alarm: First select the alarm in the list, click **Recommended Action**, and then click **Reset**. When you are finished, click **Save**.

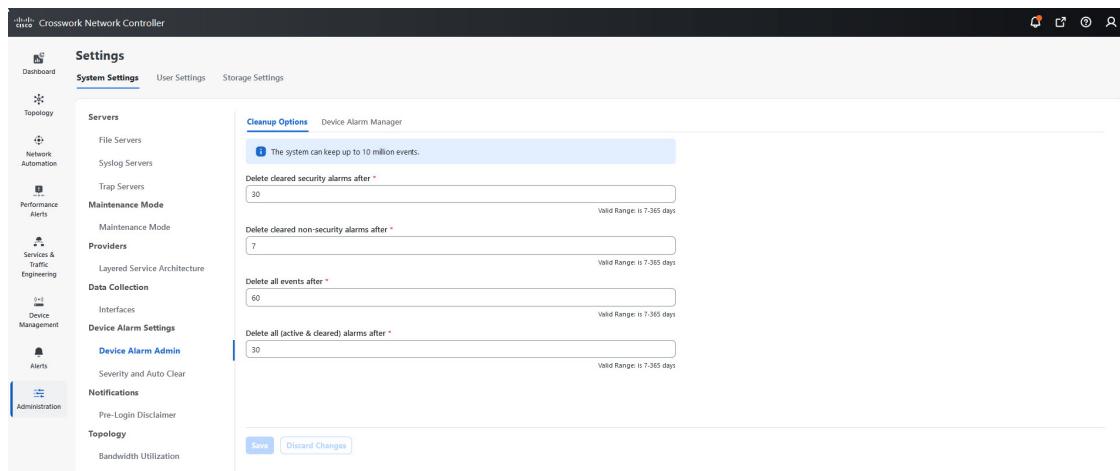
## Customize Alert Cleanup

Crosswork can store up to a maximum of 10 million events. Before reaching that limit, the system automatically begins deleting events and active or cleared alarms on a regular schedule. You can view and customize the schedule by following the steps below.

### Procedure

- Step 1** From the main menu, choose **Administration** > **System Settings** > **Device Alarm Settings** > **Device Alarm Admin** > **Cleanup Options**. Crosswork displays the **Cleanup Options** window.

Figure 90: Alert Cleanup Options



- Step 2** Change the cleanup schedule for each type of alert, as needed. To change the schedule, enter the number of days after which Crosswork deletes each type of alert. The valid range is between 1 and 365 days. Entries are required in all fields.
- Step 3** When you are finished, click **Save** to apply your changes.

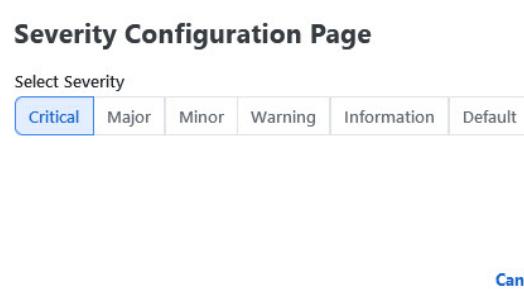
## Customize Alarm Severity

You can customize the Crosswork alarm database to assign your choice of severity levels to particular alarms.

### Procedure

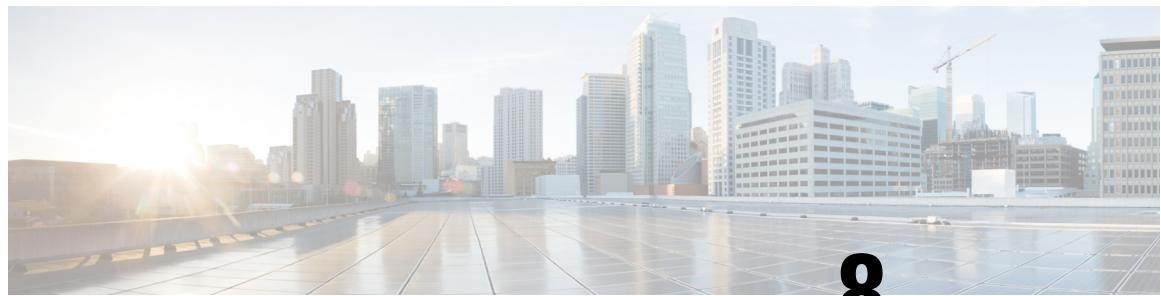
- Step 1** From the main menu, choose **Administration > System Settings > Device Alarm Settings > Severity and Auto Clear**. Crosswork displays the **Severity and AutoClear** window, showing the list of all the standard alarm types.
- Step 2** (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto Clear Duration** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To customize the severity of an alarm, click on the check box shown next to that alarm's name in the list. Then click **Severity Configuration** to display **Severity Configuration Page**.

Figure 91: Severity Configuration Page



## Customize Alarm Severity

- Step 4** click on the severity level you want to assign to the alarm. Then click **OK**.
- Step 5** When you are finished making changes, click **Save** to apply them.
-



## CHAPTER 8

# Zero Touch Provisioning

---

This section contains the following topics:

- [Zero Touch Provisioning Concepts, on page 237](#)
- [ZTP Setup Workflow, on page 246](#)
- [ZTP Provisioning Workflow, on page 277](#)
- [Reconfigure Onboarded ZTP Devices, on page 302](#)
- [Retire or Replace Devices Onboarded With ZTP, on page 302](#)
- [ZTP Asset Housekeeping, on page 303](#)
- [Troubleshoot ZTP Issues, on page 304](#)

## Zero Touch Provisioning Concepts

The Cisco Crosswork Zero Touch Provisioning (ZTP) application allows you to ship factory-fresh devices to a branch office or remote location and provision them once physically installed. 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. The device will download and apply a software image and configurations to the device automatically (you can also apply configurations only). Once configured, ZTP onboards 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. Due to the fact that it does not use secure communications, it is not suitable for use over public networks.
- **Secure ZTP:** A secure 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, which makes it more suitable for use over public networks.
- **PnP ZTP:** A secure process to download and apply software images and configuration files to Cisco IOS-XE devices. It uses Cisco Plug and Play (Cisco PnP) to verify devices and perform downloads over a secure, encrypted channel. It offers much the same level of security as Secure ZTP, but only for Cisco IOS-XE devices.
- **Evaluation License Countdown:** You can use ZTP to onboard devices without licenses for 90 days. After this evaluation period expires, you cannot use ZTP to onboard new devices until you purchase and

install a license bundle with enough capacity to cover all prior devices onboarded using ZTP, as well as your projected future needs.

- **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 images. Software image installation is an optional part of ZTP processing. When configured to do so, the ZTP process downloads the image from Cisco Crosswork to the device, and the device installs it. If you must also install SMUs, ZTP can install them as part of configuration processing in Classic and Secure ZTP (SMUs are not supported in PnP ZTP).
- **Cisco Plug and Play (Cisco PnP):** Cisco's proprietary zero-touch provisioning solution, bundled in most IOS software images. Cisco PnP uses a software PnP agent and a PnP server to distribute images and configurations to devices. To ensure communications are secure, the server and agent communicate using HTTPS.
- **Configuration file:** A file used to set the operating parameters of the newly imaged or re-imaged device. Depending on the ZTP mode you plan to use, the file may be a Python script, Linux shell script, or a sequence of Cisco IOS CLI commands stored as ASCII text (not all of these are supported in all ZTP modes). The ZTP process downloads the configuration file to the newly imaged device, which then executes it. ZTP processing requires configuration files. Secure ZTP also supports up to three different configuration files, which are applied during onboarding in the following order: pre-configuration, day-zero, and post-configuration.
- **Configuration handling method:** A Secure ZTP user option. It allows you to specify whether you want to merge a new configuration into the existing device configuration or to overwrite it. It is only available when implementing Secure ZTP.
- **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 boot loader. iPXE allows devices without built-in PXE support to boot from the network. The iPXE boot process is a normal part of Classic ZTP processing only.
- **Owner Certificate:** The Certificate Authority (CA)-signed end-entity certificate for your organization, which binds a public key to your organization. You install Owner Certificates on your devices as part of Secure ZTP processing.
- **Ownership Voucher:** The Ownership Voucher is used to identify the owner of the device by verifying the Owner Certificate that is stored in the device. Cisco supplies Ownership Vouchers in response to requests from your organization.
- **Cisco PnP agent:** A software agent embedded in Cisco IOS-XE devices. Whenever a device that supports PnP agent powers up for the first time without a startup configuration file, the agent tries to find a Cisco

PnP server. The agent can use various means to discover the server's IP address, including DHCP and DNS.

- **Cisco PnP server:** A central server for managing and distributing software images and configurations to Cisco PnP-enabled devices. Cisco Crosswork ZTP has an embedded PnP server, which is configured to communicate with PnP agents using HTTPS.
- **SUDI:** The [Secure Unique Device Identifier \(SUDI\)](#) is a certificate with an associated key pair. The SUDI contains the device's 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 validated 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 you have uploaded to Cisco Crosswork. You use the UUID of the software image file in the DHCP bootfile URL with Classic and Secure ZTP.
- **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 recommend them. They are an easy way to organize ZTP images and configurations around device families, classes, and roles, and help maintain consistency.
- **ZTP repository:** The location where Cisco Crosswork stores image and configuration files.

## Platform Support for ZTP

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

### Platform Support for Classic ZTP

The following platforms support Classic ZTP:

- **Software:** Cisco IOS-XR versions 6.5.3, 6.6.3, 6.7.2, 7.0.1, 7.0.2, 7.0.12, 7.3.1, 7.3.2, 7.4.1 or later.
- **Hardware:**
  - Cisco Aggregation Services Router (ASR) 9000
  - Cisco Network Convergence Systems (NCS) 540 and 560 Series Routers
  - Cisco NCS 55xx Series Routers
  - Cisco NCS 8xxx Series Routers

Classic ZTP doesn't support third-party devices.

## Platform Support for Secure ZTP

The following platforms support Secure ZTP:

- **Software:** Cisco IOS-XR version 7.3.1 or later (using FQDN).

Customers using IOS-XR 6.6.3 must upgrade to IOS-XR 7.3.1 before they can use Secure ZTP. Users can perform the upgrade as a single, manual image installation.

- **Hardware:**

- Cisco Network Convergence Systems (NCS) 540 Series Routers
- Cisco NCS 55xx Series Routers
- Cisco NCS 8xxx Series Routers

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)(<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, [Secure ZTP: Guidelines for Third-Party Device Certificates and Ownership Vouchers](#).

## Platform Support for PnP ZTP

The following platforms support PnP ZTP:

- **Software:** Cisco IOS-XE versions 16.12, 17.4.1, 17.5.1.

- **Hardware:**

- Cisco Aggregation Services Router (ASR) 903
- Cisco ASR 907
- Cisco ASR 920

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

# ZTP Implementation Decisions

As a best practice, always choose the most secure implementation supported by your devices. That said, 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 Pinned Domain Certificate (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 and PnP ZTP don't support the earlier software. Although Classic ZTP 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:

- Your ZTP traffic must traverse unsecured public networks.

- Your Cisco IOS-XR devices support Secure ZTP and are at the required software level (see [Platform Support for Secure ZTP, on page 240](#)).

The additional security that Secure ZTP provides requires a more complex setup than either Classic or PnP ZTP. This complexity can make processing error-prone if you're new to the setup tasks. Secure ZTP setup also requires a PDC, owner certificates and ownership vouchers from Cisco.

You will also want to consider using Secure ZTP if your devices are from third-party manufacturers; Classic and PnP ZTP don'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 doesn'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 239](#).

- **When to Use PnP ZTP:** Use PnP ZTP when you want a secure provisioning setup for Cisco IOS-XE devices that support the Cisco PnP protocol. Less complicated to set up than Secure ZTP, but only slightly more complicated than Classic ZTP, it's your best choice when your network devices happen to meet these base requirements.
- **When to Use ZTP With Imaged Devices:** There's no need to specify a software image when you use any of the ZTP modes. 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.

Secure ZTP offers more flexibility with compatible devices because it offers pre-configuration, day-zero, and post-configuration script execution capability. While both Classic and Secure ZTP modes can chain configuration files, Classic ZTP's ability to execute additional scripts will be limited to the support for script execution allowed on specific devices. PnP ZTP can only execute CLI commands, which doesn't allow for script execution.

In all cases, the result is to onboard the device. Once onboarded to Cisco Crosswork, you will want to avoid using ZTP to configure the device again (see [Reconfigure Onboarded ZTP Devices, on page 302](#) for details).

- **Organize Your 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, or chain, other scripts for devices with special roles. If you're using Classic ZTP, the script is in the specified configuration file. To extend our example, that script would apply a common configuration, then download and apply other scripts depending on the branch type. If using Secure ZTP, you have even more flexibility, as you can specify pre-configuration and post-configuration scripts in addition to the day-zero configuration script.

# ZTP Processing Logic

Cisco Crosswork ZTP processing differs depending on whether you choose to implement Classic ZTP, Secure ZTP, or PnP ZTP. The following sections of this topic provide details on each step of ZTP processing for each ZTP mode.

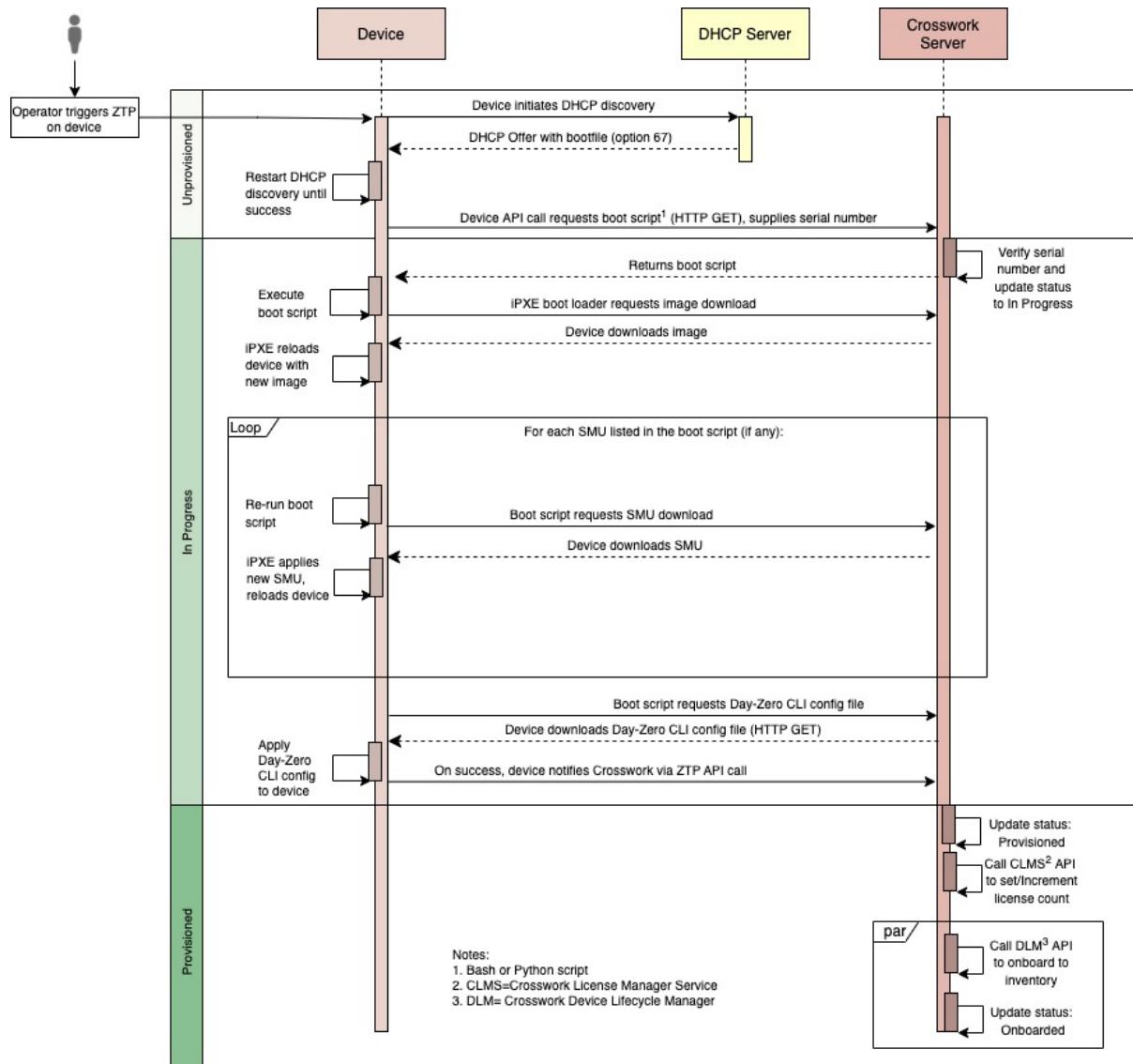
Once initiated by a device reset or reload, the ZTP process proceeds automatically. Crosswork also updates the Zero Touch Devices window with status messages showing the state each device reaches as it is processed. The figures in each of the sections indicate these state transitions with blocks in shades of green on the left side of each diagram. The transition to the Onboarded state is not shown, as reaching the Onboarded state only happens at the end of ZTP processing. Once a device has reached the Onboarded state, there are additional steps you will want to perform that are beyond the scope of ZTP processing (see, for example, [Complete Onboarded ZTP Device Information, on page 301](#)).

As indicated in the figures, the configuration scripts you use with ZTP must report device state changes to Cisco Crosswork using Cisco Crosswork API calls. If your configurations fail to do this, Crosswork can't register state changes when they occur, resulting in failed ZTP provisioning and onboarding. To see examples of these calls, select **Device Management > ZTP Configuration Files**, then click **Download Sample Script (XR)**.

## Classic ZTP Processing

The following illustration shows the process logic that Classic ZTP uses to provision and onboard devices.

Figure 92: Classic ZTP Processing

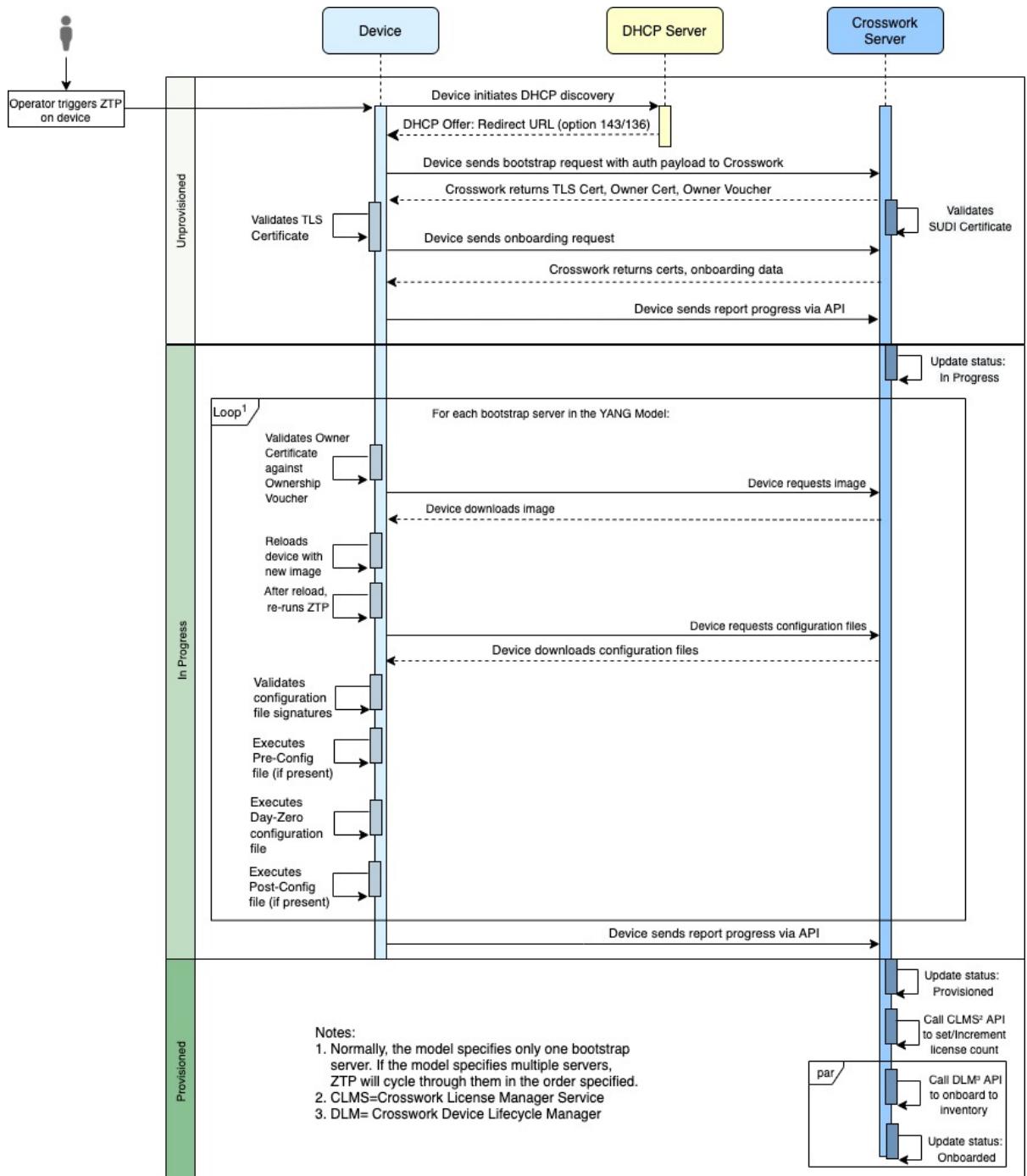


The DHCP server verifies the device identity based on the device serial number, then offers downloads of the boot file and image. Once ZTP images the device, the device downloads the configuration file and executes it.

### Secure ZTP Processing

The following illustration shows the process logic that Secure ZTP uses to provision and onboard devices.

Figure 93: Secure ZTP Processing

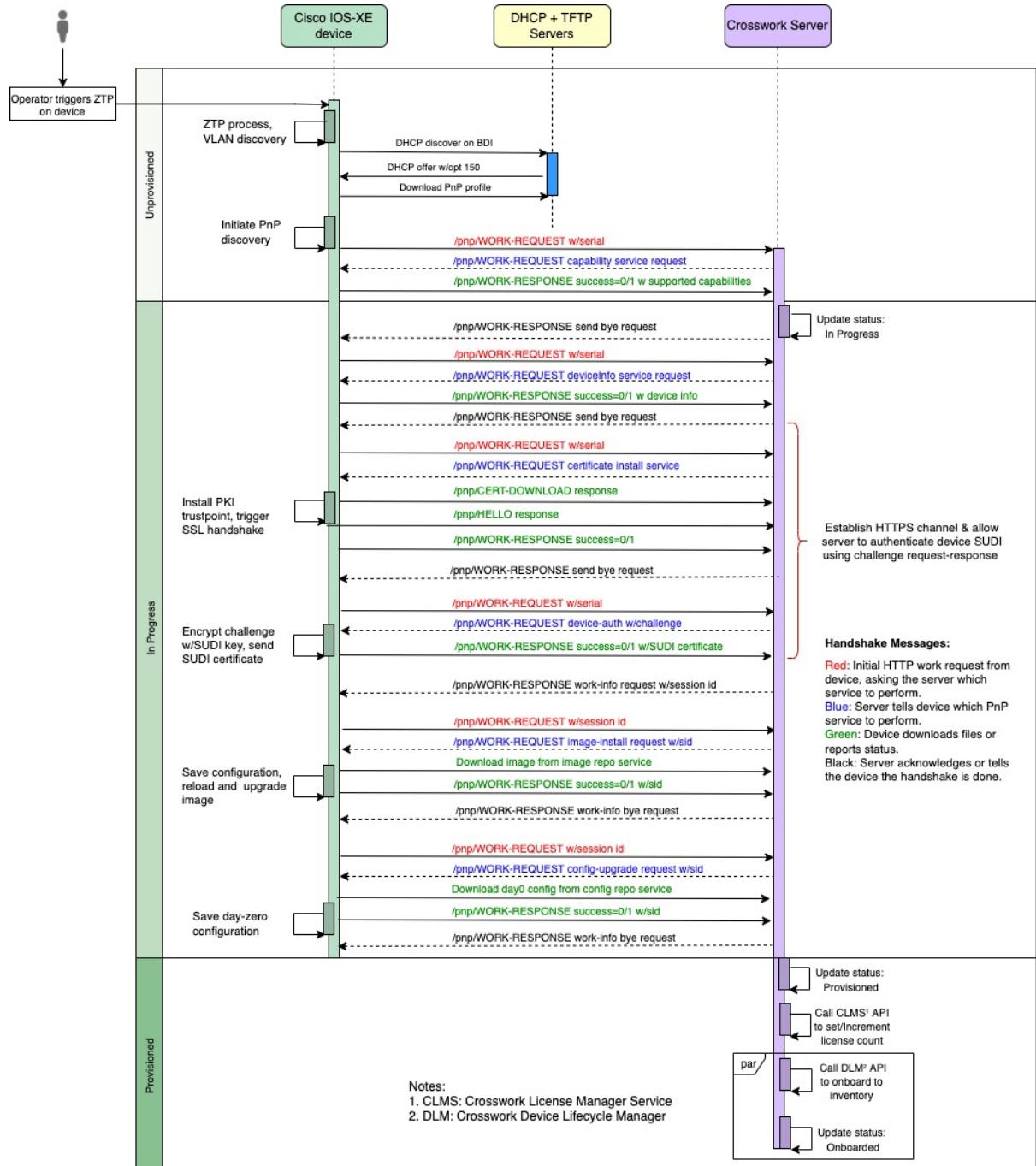


The device and the ZTP bootstrap server authenticate each other using the Secure Unique Device Identifier (SUDI) on the device and server certificates over TLS/HTTPS. Over a secure HTTPS channel, the bootstrap server lets the device download signed image and configuration artifacts. These artifacts must adhere to the [RFC 8572 YANG schema](https://tools.ietf.org/html/rfc8572#section-6.3) (<https://tools.ietf.org/html/rfc8572#section-6.3>). Once the device installs the new image (if any) and reloads, the device downloads configuration scripts and executes them.

## PnP ZTP Processing

The following illustration shows the process logic that PnP ZTP uses to provision and onboard devices.

Figure 94: PnP ZTP Processing



Once an operator triggers PnP ZTP processing, the device performs VLAN discovery and creates a BDI interface, on which DHCP discovery is initiated. As part of the DHCP discovery, the device also fetches the external TFTP server IP address using the DHCP Option 150 configuration. The device downloads the PnP

Profile from the TFTP server without authentication and copies it to the device's running configuration. The PnP Profile is a CLI text file. The profile activates the device's PnP agent and sends work requests to the embedded Crosswork PnP server over HTTP on port 30620. The PnP server then validates the device's serial number against Crosswork's "allowed" list of serial numbers (previously uploaded to Crosswork) and then initiates a PnP capability service request. A successful PnP work response from the device changes the device provisioning status from Unprovisioned to In Progress. Thereafter, the PnP server initiates a series of service requests, including requests for device information, certificate installation, image installation, configuration upgrade, and so on. Each of these service requests involves a four-way handshake between the PnP server and PnP agent. As part of certificate-install request, Crosswork PnP server shares its certificate with the device. Successful installation of this trustpoint on the device changes the PnP profile configuration to start using HTTPS and port 30603 on Crosswork. Subsequent image and config download requests use HTTPS to secure transactions. There is currently no SUDI certificate authentication support on the device. Once the device downloads and installs a new image (if any) and reloads, the PnP process will continue to download CLI configuration files and apply them to device running configuration. The device status is then set to Provisioned and the license count is updated in Crosswork. The device status is then set to Onboarded, and the device stops communicating with the PnP server.

## ZTP and Evaluation Licenses

All Cisco Crosswork applications can be used for 90 days without a license. Any time users log into the system, Crosswork displays a banner showing the number of days left in the trial period. When the trial expires, the banner will indicate it. At that point, no more devices will be able to complete the ZTP onboarding process. ZTP licensing follows a consumption-based model with licenses sold in blocks. In order to regain the ability to onboard devices using ZTP, you must install a license block that covers both the number of devices you onboarded during the trial period as well as the new devices you expect to onboard with ZTP in the future. For example: If you onboard 10 devices during the trial and then install a license bundle for 10 devices on day 91, you have no licenses left to use, and must install at least one more license block before onboarded another device. You can add more license blocks as needed. Operators should monitor license consumption to avoid running out of licenses unexpectedly. To see how many licenses you have used and are still available, check the Cisco Smart Licensing Site.

Your onboarded ZTP devices are always associated with either:

- A serial number, or
- For IOS-XR devices: 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.

## ZTP Setup Workflow

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

1. Make sure that your environment meets ZTP prerequisites for security, provider configuration, and device connectivity. See [Meet ZTP Prerequisites, on page 247](#).

2. Assemble and load into Crosswork the types of assets that ZTP needs for processing. Depending on the ZTP mode you want to use and the devices you are onboarding, you may need to prepare as few as three or as many as eight types of assets. See [Assemble and Load ZTP Assets, on page 248](#)
3. Optional: Create ZTP Profiles, which can help you simplify and standardize device imaging and configuration during the onboarding process. See [Create ZTP Profiles, on page 270](#).
4. Create ZTP device entries. ZTP uses these device entries as database "anchors" when onboarding devices to the Cisco Crosswork device inventory. If you have many devices to onboard, create the entries in bulk by importing a CSV file (see [Upload ZTP Device Entries, on page 278](#)). 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 (see [Prepare Single ZTP Device Entries, on page 276](#)). You can also use Crosswork APIs to onboard devices (see the ZTP API reference on the [Cisco Crosswork DevNet Page](#)).

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

## Meet ZTP Prerequisites

For compatibility with ZTP, your setup must meet the following prerequisites:

1. **Onboard to NSO:** 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`.
2. **Confirm Device Reachability:** The Cisco Crosswork cluster nodes must be reachable from the devices, and the nodes 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 [Cisco Crosswork Installation Guide for your version of the product](#). Enabling this kind of access may require you to change firewall configurations.
3. **Set Up Static Routes:** If your Crosswork cluster nodes and the devices you want to onboard using Crosswork ZTP are in completely different subnets, you will need to set up one or more static routes from your Crosswork cluster nodes to each separate device subnet. To do this from the Crosswork main menu, select **Administration > Settings > Zero Touch Provisioning > Static Routes**. Click the , enter the destination subnet IP address and mask (in slash notation), then click **Add**.
4. **Set Up TFTP Server for PnP ZTP:** If you plan to use PnP ZTP, you must add a TFTP server as a Cisco Crosswork provider. The TFTP server can be configured with a generic profile like the one following:

```
pnp profile test-profile
  transport http ipv4 192.168.100.205 port 30620
```
5. **Set boot-level license levels on IOS-XE devices:** If you plan on using PnP ZTP, check that the minimum license boot-level on each IOS-XE device is set to **metroipaccess** or **advancedmetroipaccess**. Be sure to perform this check **before** you trigger ZTP processing. If the boot level has been set properly, the output of the IOS-XE `#sh run | sec license` CLI command on the device should contain statements showing either of these two license levels: `license boot level advancedmetroipaccess` or `license boot level metroipaccess`. If the command output shows any other license level, especially one lower than these two, the Cisco PnP cryptographic functionality will not be enabled. This will cause certificate installation to fail, which will then cause PnP ZTP device provisioning to fail.
6. **Avoid IPv6 SLAAC IP address conflicts:** Incorrect DHCPv6 and IPv6 gateway configuration can cause IP address assignment conflicts with Stateless Address Autoconfiguration (SLAAC). These conflicts

## Assemble and Load ZTP Assets

result in a variety of ZTP failures, including preventing image upgrade on a destination device. If you plan to use ZTP on an IPv6 network, ensure that:

- Your DHCPv6 subnet range specifies a `/64 prefixlen`. This simple specification can prevent many failures.
- The default gateway is configured to avoid SLAAC IP assignment and uses DHCPv6 and stateful IP configuration only.
- The VMs used to host DHCPv6 allow Router Advertisements but do not allow autoconfig IPs.

## Assemble and Load ZTP Assets

The term "ZTP Assets" refers to the software and configuration files, credentials, certificates and other assets shown in the following checklist. The number of assets you will need to prepare and load into Crosswork will vary, depending on whether they are required for the ZTP mode you want to use, the state of your devices at the time you begin onboarding them, and other factors.

For your convenience, we recommend that you prepare and load these assets in the order given in the checklist. For details on how to prepare and then load each asset, including optional assets like software images, see the linked topic in the checklist's last column.

Many organizations maintain libraries of ZTP assets such as serial numbers and configuration files. If your organization has libraries like this, ensure that they are easily accessible from your desktop. Doing so makes it easier for you to complete ZTP setup.

For more background on using Secure ZTP with IOS-XR devices, see the [Securely Provision Your Network Devices](#) chapter of the [System Setup and Software Installation Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.3.x](#).

Cisco Crosswork supplies its own TLS certificate, with Cisco Crosswork as the Certificate Authority, for IOS-XR devices. You need not supply or upload your own TLS CA certificate chain, as IOS-XR devices do not perform X.509 validation on the Crosswork TLS server certificate.

**Table 19: ZTP Asset Checklist**

Order	Asset	Classic ZTP	Secure ZTP	PnP ZTP	For Details, see
1	Software image	Optional	Optional	Optional	A software image is required if the device has no software image installed. <a href="#">Find and Load Software Images, on page 249</a>
2	Configurations	<b>Required</b>	<b>Required.</b> Supports multiple configurations.	<b>Required</b>	<a href="#">Prepare and Load Configuration Files, on page 250</a>
3	Software Maintenance Updates (SMUs)	Optional	Optional	Not Supported	<a href="#">Find and Load SMUs, on page 263</a>

Order	Asset	Classic ZTP	Secure ZTP	PnP ZTP	For Details, see
4	Device Credentials	Required	Required	Required	<a href="#">Create Credential Profiles for ZTP, on page 264</a>
5	Serial Numbers	Required	Required	Required	<a href="#">Find and Load Device Serial Numbers, on page 265</a>
6	Pinned Domain Certificate (PDC), Owner Certificates (OCs) and Owner Key	Not Used	Required	Not used	<a href="#">Update the PDC, Owner Certificates, and Owner Key, on page 266.</a>
7	Ownership Vouchers	Not Used	Required	Not used	<a href="#">Load Ownership Vouchers, on page 268.</a>
8	SUDI Root Certificate	Not used	Required	Required for IOS-XE devices only	<a href="#">Prepare and Load the SUDI Root Certificate, on page 269</a>

## Find and Load Software Images

A software image is a file containing the installable network operating system software (such as Cisco IOS-XR or, for PnP ZTP, Cisco IOS-XE) that enables a network device to function.

Software image loading is optional for all ZTP modes, although it is required if the device you are onboarding has no software image installed. You are not required to apply a software image to a device that is already imaged. You can also apply configuration files to a device without loading an image. Loading images is required only when the device you want to onboard does not have an image installed on it, or when you want to upgrade the network OS at the same time you onboard the device.

Cisco distributes IOS-XR images as TAR, ISO, BIN, or RPM files. Cisco distributes IOS-XE images as BIN files only. Each Cisco image file represents a single release of the given network OS for a given device platform or family.

Download software image files from the [Cisco Support & Downloads page](#). During the download, record the file's MD5 checksum. You can also generate your own MD5 checksum for an image file you want to upload. Cisco Crosswork uses the MD5 checksum to validate the integrity of the file.

Load software image files to Cisco Crosswork one at a time, and enter the MD5 checksum for each file during the load.

### To load software images to Cisco Crosswork:

1. Log in to Cisco Crosswork.
2. From the main menu, select **Device Management > Software Images**
3. Click the 
4. Enter the name of, or click **Browse** and select, the file you want to upload. When prompted, enter the MD5 checksum for the file.

5. Click **Add** to finish adding the file.
6. Repeat as needed until you have loaded all the files to be used in the planned ZTP run.

## Prepare and Load Configuration Files

Configuration files are script files that configure the features of the installed software image on a given device. They are required for all ZTP modes.

Configuration files used with Classic and Secure ZTP modes can be Linux shell scripts (SH), Python scripts (PY), or device operating system CLI commands stored in an ASCII text file (TXT). For Cisco IOS-XR devices and with Classic or Secure ZTP only, you can also use configuration files to upgrade an installed network OS software version using an SMU (see [Find and Load SMUs, on page 263](#)).

Classic ZTP supports only one day-zero configuration file per device. Secure ZTP allows you to apply up to three configuration files during onboarding: one for pre-configuration preparation, a second that is the day-zero or main configuration, and a third post-configuration file to be applied after the day-zero configuration is complete. Only the day-zero configuration is required. The order of application is fixed.

Cisco PnP ZTP supports only day-zero configuration TXT files on Cisco ASR 900 and Cisco NCS 520 devices. Your PnP ZTP configuration files must use IOS-XE CLI commands. PnP ZTP does not support Linux shell (SH) or Python (PY) script files.

Your organization or Cisco consultants can create configuration files. The following sections provide guidelines for preparing configuration files for use when onboarding devices using any of the ZTP modes, as well as how to load these files into Cisco Crosswork.



**Note** When entering configuration file names in Crosswork, be sure to enter the filename *extension* in lowercase letters only (for example: myConfig.py, not myConfig.PY). Crosswork screens for and will only accept configuration filenames with all-lowercase filename extensions.

### Download the Sample Configuration File

The contents of your configuration script file will vary greatly, depending on the devices you use and how your organization uses them. A complete description of all the options available to you is therefore beyond the scope of this document.

The main guidelines to remember are:

1. Your custom configuration code can use both default and custom replaceable (or "placeholder") parameters. This allows you to insert values at runtime using the **Configuration Attributes** field when importing device entries in bulk or creating them one at a time.
2. You can create new, custom replaceable parameters as needed. You can name them anything you like, as long as they do not use the same names as the default parameters and follow the variable naming conventions discussed in this topic. If you do use the default replaceable parameters, their runtime values will be inserted from the sources described in the "Use Default Replaceable Parameters in Configuration Files" section of this topic, instead of the values you set in the device entry's **Configuration Attributes** field.
3. Replaceable parameter names are case-sensitive, and must include the braces and dollar sign. They must not include spaces (use underscores instead).

4. Be sure all of your custom replaceable parameters have a runtime value specified in the **Configuration Attributes** field. If you fail to specify a runtime value for even one of your custom replaceable parameters, the device configuration process will fail.
5. If you're using Secure ZTP, you can use custom replaceable parameters for the day-zero configuration only. Custom replaceable parameters are not supported for pre-configuration and post-configuration files.
6. Your configurations must use Cisco Crosswork API calls to complete some 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.
7. While any configuration file can call another configuration file and run it (if it can be successfully downloaded to the device), only Secure ZTP lets you specify separate pre-configuration, post-configuration, and day-zero configuration files as part of the initial, secure download.
8. Configuration file names cannot contain more than one period, and must use underscores in place of spaces.
9. Additional file restrictions are noted in the sample configuration file discussed below.

For examples of how to use the replaceable parameters and API calls, see the sample ZTP configuration file for Cisco IOS-XR devices supplied with the Cisco Crosswork ZTP application. To download the sample ZTP configuration file from Cisco Crosswork, select **Device Management > ZTP Configuration Files**, then click **Download Sample Script (XR)**. The sample configuration script is commented and provides examples of the more commonly used API calls and replaceable parameters.

For more details on replaceable parameters, see the following sections, "Use Default Replaceable Parameters in Configuration Files", and "Use Custom Replaceable Parameters in Configuration Files".

For more details on Crosswork API calls, see the section on ZTP device and configuration APIs in the "Crosswork API References" menu, available on the [Cisco Developer Network \(DevNet\) site for Cisco Crosswork](#).

The section "Sample ZTP Configuration Scripts", later in this topic, provides examples of how to use replaceable parameters and APIs.

### Preview Configuration Files

To preview the contents of any configuration file previously uploaded to Cisco Crosswork, select **Device Management > ZTP Configuration Files**, then click the configuration file name. The pop-up preview includes code syntax styling for important code features, as shown in the following table.

**Table 20: Code Syntax Colors in ZTP Config File Preview**

These code features...	... are shown in this color
Punctuation, Operator, Entity, URL, Variable, Class Name, Constant	Black
Comment	Gray
Property, Tag, Boolean, Function Name, Symbol	Orange
Selector, Attribute Name, Char, Builtin, Inserted	Dark Green
Function	Purple

These code features...	... are shown in this color
Keyword, Attribute Value	Blue
Regex, Important	Brown
String	Green
Number, Ethernet Address, MAC Address	Magenta

### Use Default Replaceable Parameters in Configuration Files

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: **Device Management > ZTP Configuration Files > Download Sample Script (XR)**. For examples showing how to use these default replaceable parameters, see the section later in this topic, "Sample ZTP Configuration Scripts".

*Table 21: Default Parameters in ZTP Configuration Files*

Cisco Crosswork substitutes this placeholder...	...Using the value from the...
<code>{\$HOSTNAME}</code>	Host name of the device as specified in the ZTP device entry.
<code>{\$IP_ADDRESS}</code>	IP address of the device as specified in the ZTP device entry.
<code>{\$SSH_USERNAME}</code>	The value of the <b>User Name</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SSH</b> ).
<code>{\$SSH_PASSWORD}</code>	The value of the <b>Password</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SSH</b> ).
<code>{\$SSH_ENPASSWORD}</code>	The value of the <b>Enable Password</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SSH</b> )
<code>{\$SNMP_READ_COM}</code>	The value of the <b>Read Community</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv2</b> ).
<code>{\$SNMP_WRITE_COM}</code>	The value of the <b>Write Community</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv2</b> ).
<code>{\$SNMP_SEC_LEVEL}</code>	The value of the <b>Security Level</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv3</b> ).
<code>{\$SNMP_USERNAME}</code>	The value of the <b>User Name</b> field in the credential profile (when the <b>Connectivity Type</b> is either <b>SNMPv2</b> or <b>SNMPv3</b> ).
<code>{\$SNMP_AUTH_TYPE}</code>	The value of the <b>User Name</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>Security Level</b> is <b>AUTH_NO_PRIV</b> or <b>AUTH_PRIV</b> ).

Cisco Crosswork substitutes this placeholder...	...Using the value from the...
<code>/{\$SNMP_AUTH_PASS}</code>	The value of the <b>User Name</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>Security Level</b> is <b>AUTH_NO_PRIV</b> or <b>AUTH_PRIV</b> ).
<code>/{\$SNMP_PRIV_TYPE}</code>	The value of the <b>User Name</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>Security Level</b> is <b>AUTH_PRIV</b> ).
<code>/{\$SNMP_PRIV_PASS}</code>	The value of the <b>Priv Password</b> field in the credential profile (when the <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>Security Level</b> is <b>AUTH_PRIV</b> ).

### Use Custom Replaceable Parameters in Configuration Files

You can create your own custom replaceable parameters in configuration files, as shown in the following sample. You can use custom and default replaceable parameters in the same configuration file, as shown in the sample.

You can assign any name you want to a custom replaceable parameter, so long as you:

- Follow the given variable definition format (for example, `{$MyParm}`)
- Substitute an underline character in place of spaces in the parameter name.
- Don't re-use the same names and capitalization as any of the default replaceable parameters.
- Supply values for each of your custom parameters in the **Configuration Attributes** field in the device entry file. To use the following sample CLI configuration file and its custom parameters with a ZTP device entry file, you would need to specify a value for the `/{$LOOPBACK0_IP}` custom parameter in each device's **Configuration Attributes** field in the ZTP device entry file. If you forget to specify values for any custom parameter, the configuration will fail.

If you're using Secure ZTP, custom replaceable parameters are supported for the day-zero configuration file only.

The first line in this sample script is required in CLI scripts for IOS-XR devices. It allows ZTP to verify whether the file is a CLI script or bash/Python script. Be sure to update the version number as appropriate. No such line is required for IOS-XE devices.

*Figure 95: Sample IOS-XR CLI Configuration Script With Mixed Replaceable Parameters*

```
!! IOS XR Configuration 7.3.1
!
hostname {$HOSTNAME}
username {$SSH_USERNAME}
group root-lr
group cisco-support
password 0 {$SSH_PASSWORD}
!
cdp
!
line console
exec-timeout 0 0
!
line default
exec-timeout 0 0
session-timeout 120
```

```

!
call-home
  service active
  contact smart-licensing
  profile CiscoTAC-1
    active
    destination transport-method http
  !
!
interface Loopback0
  ipv4 address {$LOOPBACK0_IP} 255.255.255.255
!
interface MgmtEth0/RP0/CPU0/0
  description OOB Management ZTP
  ipv4 address {$IP_ADDRESS}
!
end

```

## Sample ZTP Configuration Scripts

This section provides examples of configuration scripts for ZTP.

**Figure 96: Classic ZTP: Day-Zero Configuration Script for IOS XR Devices**

```

#!/bin/bash

#####
#
# ztpSampleScriptFile.sh
#
# Purpose: This sample script is required to notify Crosswork of the status of
# ZTP processing on an IOS XR device, and to update the device's IP address and
# hostname in Crosswork. It is also used to download a day0 config file from
# Crosswork config repository and apply this initial configuration to the device.
#
# To use: Modify the sample script as needed, following the comment guidance.
# Then upload the modified script to the Crosswork config repository.
# Next, copy the URL of this file from the repository and set that
# value in the DHCP server boot filename for ZTP config download. When ZTP is
# triggered on the device, it will download and run the script, then notify
# Crosswork.
#
# Replace the following variables with valid values & upload to Crosswork config
# repository. Sample values are provided for reference.
# - XRZTP_INTERFACE_NAME: e.g., MgmtEth0/RP0/CPU0/0 interface where ZTP triggered
# - CW_HOST_IP: Crosswork VM management or data network IP address
# - CW_PORT: 30604 for HTTP & 30603 only for HTTPS download of config file
# - CW_CONFIG_UUID: Replace with UUID of day0 config file from Crosswork repo,
#   assuming user has already uploaded device day-0 config file.
#
# This script has been tested and is known to work on Cisco NCS5501, NCS5401,
# ASR9901, and 8800 routers.
#
#####
export LOGFILE=/disk0:/ztp/customer/user-script.log

XRZTP_INTERFACE_NAME="MgmtEth0/RP0/CPU0/0"
# ZTP helper library is assumed to be installed in IOS-XR linux shell
source /pkg/bin/ztp_helper.sh
interfacedata=$(xrcmd "show interface ${XRZTP_INTERFACE_NAME}")

```

```

CW_HOST_IP="<EnterIPv4AddressHere>"
CW_PORT="30604"
CW_CONFIG_UID="e04661f8-0169-4ad3-82b8-a7c26c4f2565"

# Send logging information to log file on device disk0:/ztp/user-script.log
function ztp_log() {

    echo "$(date +"%b %d %H:%M:%S") \"$1 >> $LOGFILE"
}

#
# Get chassis serial number of the device, required by ZTP process.
# This works on Cisco NCS5501, NCS5401, 8800 series routers.
#
function get_serialkey(){

    local sn=$(dmidecode | grep -m 1 "Serial Number:" | awk '{print $NF}');
    if [ "$sn" != "Not found" ]; then
        ztp_log "Serial $sn found.";
        # The value of $sn from dmidecode should be same as serial number
        # of XR device chassis.
        DEVNAME=$sn;
        return 0
    else
        ztp_log "Serial $sn not found.";
        return 1
    fi
}

#
# Get chassis serial number of the device, required by ZTP process.
# This is tested and works on Cisco ASR 9901, but not other devices.
#
function get_serialkey_asr9901(){

    udi=$(xrcmd "show license udi")
    sn="$((cut -d':' -f4 <<<"$udi"))"
    pid="$((cut -d':' -f3 <<<"$udi"))"
    pid="$((cut -d',' -f1 <<<"$pid"))"
    echo "Serial Number $sn"
    echo "product id $pid"
}

#
# Get IP address and subnet mask from device. IP address is assigned from DHCP
# server on interface where ZTP was triggered.
#
function get_ipaddress(){

    local ipvar=$(echo $interfacedata | awk -F "Internet address is " '{sub(/.*,"",\$2);print \$2}');
    local ipv4addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv4 address" | awk '{print \$3}');
    local ipv6addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv6 address" | awk '{print \$3}');
    local ipaddress=$(echo $ipvar | awk -F "/" '{sub(/ .*/,"",\$1);print \$1}');
    local mask=$(echo $ipvar | awk -F "/" '{sub(/ .*/,"",\$2);print \$2}');
    local maskv6=$(echo $ipv6addr | awk -F "/" '{sub(/ .*/,"",\$2);print \$2}');

    ztp_log "### Value of interfacedata => $interfacedata ###"
    ztp_log "### Value of ipvar => $ipvar ###"
    ztp_log "#####IPv4 address $ipaddress and mask $mask found. #####";
    IPADDR=$ipaddress
}

```

## Prepare and Load Configuration Files

```

MASK=$mask
MASKV6=$maskv6

return 0
}

#
# Fetch hostname from device configuration.
#
function get_hostname(){

hostnamedata=$(xrcmd "show running-config hostname")
local hostname=(${echo $hostnamedata | awk -F "hostname " '{sub(/ .*/,"",\$2);print \$2}'}');

ztp_log "####hostname $hostname found.";
HOSTNAME=$hostname;
return 0;
}

#
# Download day-0 config file from Crosswork config repository using values
# set for CW_HOST_IP, CW_PORT and CW_CONFIG_UUID.
# The MESSAGE variable is optional, can be used to display a suitable message
# based on the ZTP success/failure log.
#
function download_config(){

ztp_log "### Downloading system configuration ::: ${DEVNAME} ###";
ztp_log "### ip address passed value ::: ${IPADDR} ###";
ip netns exec global-vrf /usr/bin/curl -k --connect-timeout 60 -L -v --max-filesize
104857600
http://${CW_HOST_IP}:${CW_PORT}/crosswork/configsvc/v1/configs/device/files/${CW_CONFIG_UUID}
-H X-cisco-serial*:${DEVNAME} -H X-cisco-arch*x86_64 -H X-cisco-uuid* -H
X-cisco-oper*:exr-config -o /disk0:/ztp/customer/downloaded-config 2>&1

if [[ "$?" != 0 ]]; then
    STATUS="ProvisioningError"
    ztp_log "### status::: ${STATUS} ###"
    ztp_log "### Error downloading system configuration, please review the log ###"
    MESSAGE="Error downloading system configuration"
else
    STATUS="Provisioned"
    ztp_log "### status::: ${STATUS} ###"
    ztp_log "### Downloading system configuration complete ###"
    MESSAGE="Downloading system configuration complete"
fi
}

#
# Apply downloaded configuration to the device and derive ZTP status based on
# success/failure of ZTP process. The MESSAGE variable is optional, can be used
# to display a suitable message based on the ZTP success/failure log.
#
function apply_config(){
ztp_log "### Applying initial system configuration ###";
xraply_with_reason "Initial ZTP configuration" /disk0:/ztp/customer/downloaded-config
2>&1 >> $LOGFILE;
ztp_log "### Checking for errors ###";
local config_status=$(xrcmd "show configuration failed");
if [[ $config_status ]]; then
    echo $config_status >> $LOGFILE
    STATUS="ProvisioningError"
    ztp_log "### status::: ${STATUS} ###"
}

```

```

        ztp_log "!!! Error encountered applying configuration file, please review the log
!!!!";
        MESSAGE="Error encountered applying configuration file, ZTP process failed"
    else
        STATUS="Provisioned"
        ztp_log "### status::: ${STATUS} ###"
        ztp_log "### Applying system configuration complete ###";
        MESSAGE="Applying system configuration complete, ZTP process completed"
    fi
}

#
# Call Crosswork ZTP API to update device ZTP status, IP address, hostname.
# Without this function, device status will remain in "In Progress" and not
# be updated in Crosswork.
#
# Using this API, device SSH/SNMP connectivity details can also be updated.
# Values for connectivity details values can be added as part of
# "connectivityDetails" array in below curl command. Sample snippet provided:
#
#   "connectivityDetails": [
#     "protocol": "SSH",
#     "inetAddr": [
#       "inetAddressFamily": "IPV4/IPV6",
#       "ipaddrs": "<ssh/snmp ipaddress>",
#       "mask": <ipaddress mask(Integer).>,
#       "type": "CONNECTIVITYINFO"
#     ],
#     "port": <ssh/snmp port(Integer)>,
#     "timeout": <ssh/snmp timeout(Integer). default to 60sec>
#   ]
#
function update_device_status() {

    echo """$IPADDR"""
    echo """$MASK"""
    echo """$DEVNAME"""
    echo """$STATUS"""
    echo """$HOSTNAME"""
    echo """$MESSAGE"""

    curl -d '{
        "ipAddress":{
            "inetAddressFamily": "IPV4",
            "ipaddrs": """$IPADDR""",
            "mask": '$MASK'
        },
        "serialNumber": """$DEVNAME""",
        "status": """$STATUS""",
        "hostName": """$HOSTNAME""",
        "message": """$MESSAGE"""
    }' -H "Content-Type: application/json" -X PATCH
    http://${CW_HOST_IP}:${CW_PORT}/crosswork/ztp/v1/deviceinfo/status
}

# ===== Script entry point =====
STATUS="InProgress"
get_serialkey;
#get_serialkey_asr9901; // For Cisco ASR9901, replace get_serialkey with
get_serialkey_asr9901.
ztp_log "Hello from ${DEVNAME} !!!";
get_ipaddress;

```

## Prepare and Load Configuration Files

```

ztp_log "Starting autoprovision process...";
download_config;
apply_config;
get_hostname;
update_device_status;

ztp_log "Autoprovision complete...";
exit 0

```

**Figure 97: Secure ZTP: Simple Day-Zero Configuration Script**

```

!! IOS XR
!
hostname ztpdevice1
!
interface MgmtEth0/RP0/CPU0/0
  ipv4 address dhcp
!

```

**Figure 98: Secure ZTP: Day-Zero Configuration Script Using Replaceable Parameters**

```

!! IOS XR
!
hostname {$hname}
!
interface MgmtEth0/RP0/CPU0/0
  ipv4 address {$mgmt_ipaddr} {$mgmt_subnet_mask}
!
```

**Figure 99: Secure ZTP: Post-Configuration Script**

```

#!/bin/bash

#####
#
#SZTP post script to update hostname and ipaddress for the device
# input - serial key and crosswork host and port
#
#####

export LOGFILE=/disk0:/ztp/customer/user-script.log

XRZTP_INTERFACE_NAME="MgmtEth0/RP0/CPU0/0"
# ZTP helper library is assumed to be installed in IOS-XR linux shell
source /pkg/bin/ztp_helper.sh
interfacedata=$(xrcmd "show interface ${XRZTP_INTERFACE_NAME}")

CW_HOST_IP=""    #update from the post script prepare code
CW_PORT="30603"                      #update from the post script prepare code

# Send logging information to log file on device disk0:/ztp/user-script.log
function ztp_log() {

    echo "$(date +"%b %d %H:%M:%S") \"$1 >> $LOGFILE"
}

#
# Get IP address and subnet mask from device. IP address is assigned from DHCP
# server on interface where ZTP was triggered.
#
function get_ipaddress() {

```

```

local ipvar=$(echo $interfacedata | awk -F "Internet address is " '{sub(/.*,"",$2);print $2"')});
local ipv4addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv4 address" | awk '{print $3}');
local ipv6addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv6 address" | awk '{print $3}');
local ipaddress=$(echo $ipvar | awk -F "/" '{sub(/.*,"",$1);print $1}');
local mask=$(echo $ipvar | awk -F "/" '{sub(/.*,"",$2);print $2}');
local maskv6=$(echo $ipv6addr | awk -F "/" '{sub(/.*,"",$2);print $2}');

ztp_log "### Value of interfacedata => $interfacedata ###";
ztp_log "### Value of ipvar => $ipvar ###";
ztp_log "#### IPv4 address $ipaddress and mask $mask found. #####";

IPADDR=$ipaddress
MASK=$mask
MASKV6=$maskv6

return 0
}

#
# Fetch hostname from device configuration.
#
function get_hostname() {

hostnamedata=$(xrcmd "show running-config hostname")
local hostname=$(echo $hostnamedata | awk -F "hostname " '{sub(/.*,"",$2);print $2}');

ztp_log "#### hostname $hostname found.";
HOSTNAME=$hostname;
return 0;
}

#
# Call Crosswork ZTP API to update device ZTP status, IP address, hostname.
# Without this function, device status will remain in "In Progress" and not
# be updated in Crosswork.
#
# Using this API, device SSH/SNMP connectivity details can also be updated.
# Values for connectivity details values can be added as part of
# "connectivityDetails" array in below curl command. Sample snippet provided:
#
#   "connectivityDetails": [
#     "protocol": "SSH",
#     "inetAddr": [
#       "inetAddressFamily": "IPV4/IPV6",
#       "ipaddrs": "<ssh/snmp ipaddress>",
#       "mask": <ipaddress mask(Integer).>,
#       "type": "CONNECTIVITYINFO"
#     ],
#     "port": <ssh/snmp port(Integer)>,
#     "timeout": <ssh/snmp timeout(Integer). default to 60sec>
#   ]
#
function update_device_status() {

echo """$IPADDR"""
echo """$MASK"""
echo """$SERIAL_KEY"""
echo """$HOSTNAME"""
}

```

```

curl -d '{
  "ipAddress": {
    "inetAddressFamily": "IPV4",
    "ipAddrs": "'"$IPADDR"'",
    "mask": '$MASK'
  },
  "serialNumber": """$SERIAL_KEY""",
  "hostName": """$HOSTNAME""",
  "message": "Post config script updated successfully"
}' -H "Content-Type: application/json" -X PATCH
http://{$CW_HOST_IP}:{$CW_PORT}/crosswork/ztp/v1/deviceinfo/status
}

function get_sudi_serial() {
  local rp_card_num=`ip netns exec xrnns /pkg/bin/show_platform_sysdb | grep Active | cut -d ' ' -f 1`
  echo $rp_card_num
  xrcmd "show platform security tam all location $rp_card_num" > tamfile.txt
  local sudi_serial=$(sed -n -e '/Device Serial Number/ s/.*/- */p' tamfile.txt)
  echo $sudi_serial
  SERIAL_KEY=$sudi_serial
  return 0
}

function ztp_disable()
{
  xrcmd "ztp disable noprompt"
}

function ztp_enable()
{
  xrcmd "ztp enable noprompt"
}

# ===== Script entry point =====
get_sudi_serial;
ztp_log "Hello from ${SERIAL_KEY} !!!";
get_ipaddress;
get_hostname;
update_device_status;

ztp_log "Autoprovision complete...";
ztp_log "Disabling secure mod"
ztp_disable;
exit 0

```

## Load Configuration Files

To load configuration files to Cisco Crosswork:

1. Launch Cisco Crosswork.
2. From the main menu, select **Device Management > ZTP Configuration Files**.
3. Click the 
4. Click **Browse** to select a configuration file.
5. Enter the required configuration information:

For Classic and PnP ZTP, always select **Day0-config** in the **Type** dropdown.

If you're using Secure ZTP, use the **Type** dropdown to specify whether the configuration file you are adding is a **Pre-config**, **Day0-config**, or **Post-config**.

6. Click **Add** to finish adding the configuration file.
7. Repeat as needed until you have loaded all the configuration files to be used in the planned ZTP run.

## Load ZTP Assets

Upload the ZTP assets you assembled, per the requirements of the ZTP mode you want to use.

Classic ZTP requires you to load:

- Configuration files (TXT, SH, or PY files)
- Device serial numbers

Secure ZTP requires you to load:

- Configuration files (TXT, SH, or PY files)
- Device serial numbers
- Pinned domain certificate
- Ownership certificates
- Ownership Vouchers
- SUDI Root Certificates

PnP ZTP requires you to load:

- Configuration files (TXT files only)
- Device serial numbers

If you plan to image, re-image, or update the device operating system software as part of ZTP onboarding, you must also load software images and SMUs, as follows:

- Classic ZTP: TAR, ISO, BIN, or RPM image files, and SMUs
- Secure ZTP: TAR, ISO, BIN, or RPM image files, and SMUs
- PnP ZTP: BIN only. SMUs are not supported.

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

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

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



**Note** When entering file names in Crosswork, be sure to enter the filename *extension* in lowercase letters only (for example: myConfig.py, not myConfig.PY). Crosswork screens for and will only accept configuration filenames with all-lowercase filename extensions.

## Procedure

### Step 1

(Optional) Upload software images and SMUs:

- From the main menu, select **Device Management** > **Software Images** and then click the .
- 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 software image file.

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

### Step 2

Upload configuration files:

- From the main menu, select **Device Management** > **ZTP Configuration Files** and then click the .
- Enter the required configuration information and then click **Add**.

Click **Browse** to select a configuration file.

If you're implementing Secure ZTP, use the **Type** dropdown to specify whether the configuration file you are adding is a **Pre-config**, **Day0-config**, or **Post-config**. For Classic and PnP ZTP, always select **Day0-config**.

- Click  again and repeat step 2b until you have loaded all the configuration files.

### Step 3

Upload device serial numbers:

- From the main menu, select **Device Management** > **Serial Numbers & Vouchers**, then click **Add Serial Number(s)**.
- Click **Upload CSV**, then click the **serialnumber.csv** link to download the sampleSerialnumber.csv template file.
- 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 template under a new file name.
- Select **Add Serial Number(s)** again and click **Upload CSV**. Click **Browse** to select the updated CSV file, then click **Add Serial Number(s)** to import the serial numbers from the updated CSV template file.

### Step 4

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

### Step 5

Update the pre-installed default Secure ZTP ownership certificate with your Pinned Domain Certificate, Owner Certificate, Owner Key, and Owner Passphrase:

- From the main menu, select **Administration** > **Certificate Management**.
- In the **Name** column, find the pre-installed **Crosswork-ZTP-Owner** certificate.
- Click the **...** in the same row as **Crosswork-ZTP-Owner**, then click **Update Certificate**.
- Next to the **Pin Domain CA Certificate** field, click **Browse**. Browse to and select the PDC file (PEM or CRT) and then click **Save**.
- Next to the **Owner Certificate** field, click **Browse**. Browse to and select the Owner Certificate file (PEM or CRT) and then click **Save**.

- f) Next to the **Owner Key** field, click **Browse**. Browse to and select the Owner Key file (PEM, KEY, CRT), then click **Save**.
- g) In **Owner Passphrase** enter the owner passphrase.
- h) Click **Save** to update the default owner certificate with your uploads.

**Step 6**

Update the pre-installed default Secure ZTP SUDI device certificate with your SUDI certificate:

- a) From the main menu, select **Administration > Certificate Management**.
- b) In the **Name** column, find the pre-installed **Crosswork-ZTP-Device-SUDI** certificate.
- c) Click the **...** in the same row as **Crosswork-ZTP-Device-SUDI**, then click **Update Certificate**.
- d) Next to the **Cisco M2 CA Certificate** field, click **Browse**. Browse to and select the Cisco M2 CA certificate file (PEM or CRT), then click **Save**.

**Step 7**

Upload additional ownership vouchers, as needed:

- a) From the main menu, select **Device Management > Serial Numbers & Vouchers**.
- b) Click **Add Voucher(s)**.
- c) Click **Browse** to browse to and select the TAR or VCJ voucher files you want to upload. Note that Crosswork supports both compressed and uncompressed TAR files.

If you are uploading vouchers for third party devices, ensure that the uploaded VCJ file or files in the TAR follow the name convention *serial.vcj*, where *serial* is the serial number of the corresponding device. Cisco Crosswork requires this type of naming in order to map the ownership voucher to the device.
- d) Click **Upload**.

## Find and Load SMUs

A Software Maintenance Update (SMU) is a Cisco software package file that provides point fixes for critical issues in a given release of a Cisco network operating system software image. Cisco [distributes SMUs in nonbootable format](#) with a `readme.txt` file explaining the issues associated with the SMU. Cisco rolls SMU contents into the next maintenance release of a software image.

Applying an SMU to a device during ZTP onboarding is supported for Classic and Secure ZTP only, and then only during application of a configuration file (see [Prepare and Load Configuration Files, on page 250](#)). SMUs are not supported for Cisco IOS-XE devices or for PnP ZTP.

As with software images, download SMU files from the [Cisco Support & Downloads page](#). During the download, record the SMU file's MD5 checksum. Cisco Crosswork uses the MD5 checksum to validate the integrity of the SMU file. Load SMUs to Cisco Crosswork one at a time, and enter the MD5 checksum for each SMU file during the load.

**To load SMUs to Cisco Crosswork:**

1. Launch Cisco Crosswork.
2. From the main menu, select **Device Management > Software Images**
3. Click the 
4. In the **Software Image** field, enter or click **Browse** to select, the name of the SMU file you want to upload (ISO, TAR, or RPM).
5. In the **MD5 Checksum** field, enter the checksum you recorded when you downloaded the SME file.

Then complete the other fields as required.

6. Click **Add** to finish adding the SMU.
7. Repeat these steps as needed until you have loaded all the SMU files to be used in the planned ZTP run.

## 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.

You can also add credential profiles one at a time. To do so, select **Device Management > Credential Profiles**, then click the .

Credential profiles allow you to specify different credentials for each protocol the device supports. When creating device credential profiles that contain SNMP credentials, we recommend 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.

### Procedure

---

**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 columns sets the following mapping between the three password types and the three user names and three passwords 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:
- With the **Credential Profiles** window displayed, click the selection box next to the profile you want to update, then click the .
  - Enter the passwords and community strings for the credential profile and then click **Save**.
  - Repeat these steps as needed until you have entered all passwords and community strings for all the credential profiles needed to access your devices.

## Find and Load Device Serial Numbers

Device serial numbers are required for all ZTP modes.

Most organizations maintain a database of network device serial numbers as part of their non-sales inventory records. When adding new devices to the network, they will typically add the new device serial numbers to the same database at the time of purchase. This is the first place to look for serial numbers for devices you plan to onboard using ZTP.

You can also [Contact Cisco Support](#) for help getting the serial numbers for newly purchased devices.

As a last resort, and for a Cisco IOS device that is already imaged, log in to the device console and run the `show inventory` CLI command. In the command output, look for a device name and description section like the one shown in the following illustration. In the case of devices with line cards or other options (as shown in this example), you will want to load both the serial numbers for both the chassis and card.

```
RP/0/RP0/CPU0:ios#sh inv
Wed May 18 13:33:53.674 UTC
NAME: "0/RP0", DESC: "NC5501 w/o TCAM Route Processor Card"
PID: NCS-5501      , VID: V01, SN: FOC23297HGS

NAME: "Rack 0", DESC: "NCS5501 w/o TCAM 1RU Chassis"
PID: NCS-5501      , VID: V01, SN: FOC2332R014
...
```

### To load device serial numbers to Cisco Crosswork:

- Launch Cisco Crosswork.
- From the main menu, select **Device Management > Serial Numbers & Vouchers**.
- Click **Add Serial Number(s)**.
- Click **Upload CSV**, then click the **serialnumber.csv** link to download the `sampleSerialnumber.csv` template file.
- 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.
- Select **Add Serial Number(s)** again.
- Click **Browse** to select the updated CSV file.

## Update the PDC, Owner Certificates, and Owner Key

- Click **Add Serial Number(s)** to import the serial numbers.

## Update the PDC, Owner Certificates, and Owner Key

The Pinned Domain Certificate, Owner Certificate, and Owner Key are required only for Secure ZTP. They are not used with Classic ZTP and PnP ZTP.

In a test environment, you can use the default Pinned Domain Certificate (PDC), Owner Certificates (OCs) and Owner Key that Cisco Crosswork generates when ZTP is first installed. These credentials rely on Cisco as the Certificate Authority (CA) and are offered solely for the convenience of product testing. Cisco assumes that when you are using these default credentials, you are testing Cisco Crosswork in a protected "sandbox" environment that does not expose your network to security risks.

For production use, you must pin the Domain Certificate, generate intermediate OCs, and sign the Owner Key. You can then update the default versions of these credentials using the steps in the following section, "Update the Default PDC, OCs and Owner Key".

Organizations with their own certificate management staff and procedures will be familiar with how to generate a PDC, OCs and Owner Key using their chosen CA. Organizations that need more assistance with these tasks should see the examples and advice in the later section of this topic, "Pin the Domain Certificate, Generate Owner Certificates and Sign the Owner Key".

### Update the Default PDC, OCs and Owner Key

To update the default Pinned Domain Certificate (PDC), Owner Certificate (OCs), and Owner Key:

- Launch Crosswork.
- From the main menu, select **Administration > Certificate Management**.
- Under the **Name** column, find the **Crosswork-ZTP-Owner** certificate. Then click the **...** in the same row and select **Update Certificate**.
- Next to the **Pin Domain CA Certificate** field, click **Browse** and select your Pinned Domain Certificate file (PEM or CRT only). With the file selected, click **Save**.
- Next to the **Owner Certificate** field, click **Browse** and select your Owner Certificate file (PEM or CRT only). With the file selected, click **Save**.
- Next to the **Owner Key** field, click **Browse** and select your Owner Key file (PEM, KEY, CRT). With the file selected, click **Save**.
- Click **Save** to update the default certificates and key.

### Pin the Domain Certificate, Generate Owner Certificates and Sign the Owner Key

The following steps provide a series of examples showing how to use OpenSSL and the Linux Bash shell to generate a PDC, OCs and a signed Owner Key using your own Certificate Authority. You can find additional explanations and examples of this process at the following public resource: [OpenSSL Certificate Authority](#). Once you've generated these credentials, follow the procedure in the preceding section, "Update the Default PDC, OCs and Owner Key".

- Create a set of directories to manage the certificate and other files you will use or generate. For example:

```
#!/bin/sh
mkdir ./ca
mkdir ./ca/certs
```

```

mkdir ./ca/crl
mkdir ./ca/newcerts
mkdir ./ca/private
chmod 700 ./ca/private
touch ./ca/index.txt
echo 1000 > ./ca/serial
mkdir ./ca/intermediate
mkdir ./ca/intermediate/certs
mkdir ./ca/intermediate/crl
mkdir ./ca/intermediate/csr
mkdir ./ca/intermediate/newcerts
mkdir ./ca/intermediate/private
chmod 700 ./ca/intermediate/private
touch ./ca/intermediate/index.txt
echo 1000 > ./ca/intermediate/serial
echo 1000 > ./ca/intermediate/crlnumber

```

2. Generate the root key. For example:

```

#!/bin/bash
cd ca
openssl genrsa -aes256 -out private/ca.key.pem 4096
chmod 400 ./private/ca.key.pem

```

3. Create the root certificate. For example:

```

#!/bin/bash
cd ca
##-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" \
openssl req -config openssl.cnf -key ./private/ca.key.pem -new -x509 -days 7300 -sha256
-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" -extensions v3_ca -out
certs/ca.cert.pem
chmod 444 ./certs/ca.cert.pem

```

4. Verify the root certificate. For example:

```

#!/bin/bash
cd ca
openssl x509 -noout -text -in certs/ca.cert.pem

```

5. Generate the intermediate key. For example:

```

#!/bin/bash
cd ca
openssl genrsa -aes256 -out intermediate/private/intermediate.key.pem 4096
chmod 400 ./intermediate/private/intermediate.key.pem

```

6. Create the intermediate certificate. For example:

```

#!/bin/bash
cd ca
##-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" \
openssl req -config intermediate/openssl.cnf -new -sha256 \
-key intermediate/private/intermediate.key.pem \
-out intermediate/csr/intermediate.csr.pem \
-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=intermediate.cisco.com"
chmod 444 ./certs/ca.cert.pem
© 2022 GitHub, Inc.

```

7. Sign the intermediate key. For example:

```

#!/bin/bash
cd ca
openssl ca -config openssl.cnf -extensions v3_intermediate_ca \
-days 3650 -notext -md sha256 \
-in intermediate/csr/intermediate.csr.pem \

```

```
-out intermediate/certs/intermediate.cert.pem
chmod 444 ./intermediate/certs/intermediate.cert.pem
```

8. Verify the intermediate certificate. For example:

```
#!/bin/bash
cd ca
openssl x509 -noout -text -in intermediate/certs/intermediate.cert.pem
```

9. Create the certificate chain. For example:

```
#!/bin/bash
cd ca
cat intermediate/certs/intermediate.cert.pem \
    certs/ca.cert.pem > intermediate/certs/ca-chain.cert.pem
chmod 444 intermediate/certs/ca-chain.cert.pem
```

10. Sign the Certificate Revocation List (CRL). For example:

```
#!/bin/bash
mycsr=$1
myip=$2
export SAN="IP:${myip}"
echo $SAN
cd ca
openssl ca -config intermediate/openssl.cnf \
    -extensions usrSrv_cert -days 750 -notext -md sha256 \
    -in intermediate/csr/${mycsr}.csr.pem \
    -out intermediate/certs/${mycsr}.cert.pem
chmod 444 intermediate/certs/${mycsr}.cert.pem
```

## Load Ownership Vouchers

Ownership Vouchers (OVs) are required for Secure ZTP only. They are not used with Classic or PnP ZTP.

Cisco supplies OVs to customers either on request or via download in the form of VCJ (containing a single voucher) or TAR (an archive of multiple vouchers) files. Once you have the voucher files in either format, you can upload them directly to Crosswork.

### Get Ownership Vouchers From Cisco

You can download OVs in bulk from Cisco's MASA (Manufacturer Authorized Signing Authority) server at <https://masa.cisco.com>. You will need a customer login to access the MASA server securely.

If you would rather request OVs from Cisco, [contact Cisco Support](#). You must provide the following with your request:

- Pinned Domain Certificate (PDC): A trusted digital certificate issued by a Certificate Authority (CA) and pinned by you. For details on pinning the PDC, see [Update the PDC, Owner Certificates, and Owner Key, on page 266](#).
- The serial number of each device you plan to onboard using Secure ZTP (see [Find and Load Device Serial Numbers, on page 265](#)).

Here is an example request for a single device:

```
{
  "expires-on": "2016-10-21T19:31:42Z",
  "assertion": "verified",
  "serial-number": "JADA123456789",
  "idevid-issuer": "base64encodedvalue==",
  "pinned-domain-cert": "base64endvalue==",
```

```
        "last-renewal-date": "2017-10-07T19:31:42Z"  
    }
```

Cisco Support will respond to your request for a single OV by sending you a VCJ file. If you requested OVs for more than one device, Cisco will send you multiple VCJs in a TAR file instead of a single VCJ file. We recommend that you perform the VCJ or TAR file exchange using a secure method that you have agreed upon with Cisco Support.

Remember that individual VCJ files, whatever the source, must have the device serial number as the file name. Following the example request given above, Cisco would return a file with this name: `JADA123456789.VCJ`.

### Get Ownership Vouchers From Third Parties

If you want to use Secure ZTP to onboard third-party devices, you must request VCJ files from the third-party manufacturer. VCJ files the manufacturer supplies must follow the naming convention `serial.vcj`, where `serial` is the serial number of the third-party device. Cisco Crosswork requires this file naming convention in order to map the Ownership Voucher to the device. For background about restrictions on vouchers from third-party manufacturers, see [#unique\\_206 unique\\_206\\_Connect\\_42\\_SecureZTPGuidelinesThird](#).

### Load Ownership Vouchers

To load Ownership Vouchers:

1. Launch Cisco Crosswork.
2. From the main menu, select **Device Management > Serial Numbers & Vouchers**.
3. Click **Add Voucher(s)**.
4. Enter the name of, or click **Browse** to select, the VCJ or TAR file containing the vouchers you want to upload.
5. Click **Upload** to finish uploading the OVs.

If you upload a TAR file, Crosswork will extract each of the VCJ files from the archive during the load.

## Prepare and Load the SUDI Root Certificate

The SUDI Root Certificate is required for Secure ZTP, and for PnP ZTP when onboarding IOS-XE devices. It is not used for Classic ZTP.

There are two types of "SUDI certificates":

- The device **SUDI Certificate** (also known as the Trust Anchor Certificate). Every Cisco IOS-XR and IOS-XE device has a SUDI Certificate stored on the device. The device SUDI certificate cannot be modified.
- The **SUDI Root Certificate**. This is the root CA certificate that enables the SUDI Certificate on each device.

Uploading the SUDI Root Certificate to Crosswork enables the Secure ZTP process (and, for IOS-XE devices, the PnP ZTP process) to authenticate each device by comparing the SUDI Root Certificate with the device's stored SUDI Certificate. This is required before the PnP ZTP or Secure ZTP processes can provide bootstrap information to the device.

**To prepare the SUDI Root Certificate and upload it to Cisco Crosswork:**

1. Download the "Cisco Root CA 2048" and "Cisco Root CA 2099" files, in PEM format, from [Cisco PKI: Policies, Certificates, and Documents](https://www.cisco.com/security/pki/policies/index.html) (<https://www.cisco.com/security/pki/policies/index.html>).

2. Use an ASCII text editor to combine the two downloaded PEM files into a single PEM file, as in the example below:

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCTU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
...
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFSHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
...
PKkmB1NQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
```

3. Launch Cisco Crosswork.
4. From the main menu, select **Administration > Certificate Administration**.
5. Under the **Name** column, find the **Crosswork-ZTP-Device-SUDI** certificate. Then click the **...** in the same row and select **Update Certificate**.
6. In the **Cisco M2 CA Certificate** field: Either enter, or click **Browse** and select, the SUDI Root Certificate file (PEM or CRT only) you prepared.
7. With the file name entered, click **Save**. Crosswork stores the SUDI Root Certificate.

## 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 and routinize the ZTP imaging and configuration process. You can use ZTP profiles to help organize defined sets of image and configuration files that you can then 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-configuration, post-configuration, and day-zero configuration files.

ZTP profiles don't require that you specify a software 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.

### Procedure

**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: Move the **Secure ZTP** slider to **Enabled**. Then enter the names of the pre- and post-configuration files.

The **Secure ZTP** slider is set to **Disabled** by default. The slider is not available if you select **IOS-XE** in the **OS Platform** field.

- 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 and then import 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.

The fastest way to create multiple ZTP device entries is to import them in bulk, using a device-entry CSV file. You can download a template for this CSV file from Crosswork. We recommend that you experiment with the device entry CSV file format until you get used to it. Download and make a copy of the template, modify the copy to add just one or two device entries, then import it. You can then see how to get the results you want.

The following topics explain how to download and use a device entry CSV file to create properly formatted ZTP device entries in bulk.

You can also create ZTP device entries one by one, using the Cisco Crosswork UI, as explained in [Prepare Single ZTP Device Entries, on page 276](#).

### Download and Edit the ZTP Device Entry CSV Template

1. From the main menu, choose **Device Management > Network 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 of the template copy, create an entry for each device you plan to onboard using ZTP. Refer to the next topic, "ZTP Device Entry CSV Template Reference", for help with the values to enter in each column.
6. Once you have completed preparing your ZTP device entry files, load them to Crosswork using the steps in [Upload ZTP Device Entries, on page 278](#).

### ZTP Device Entry CSV Template Reference

The following table explains how to use the columns in the device entry 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 22: ZTP Device Entry Template Column Reference

Template Column	Usage
Serial Number *	<p>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.</p> <p>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.</p>
Location Enabled	<p>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.</p>
Remote ID *	<p>If implementing Secure ZTP and using option 82: Identify the name of the remote host acting as the bootstrap server.</p> <p>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.</p> <p>If you're not using option 82, you can leave this field blank but you must specify the device serial number.</p>
Circuit ID *	<p>If implementing Secure ZTP and using option 82: Identify the interface or VLAN on which the bootstrap server receives requests.</p> <p>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.</p> <p>If you're not using option 82, you can leave this field blank but you must specify the device serial number.</p>
Host Name *	Enter the host name you want to assign to the device.
Credential Profile *	Enter the name of the credential profile you want Cisco Crosswork to use to access and configure the device. The name you enter must match the name of the credential profile as specified in Cisco Crosswork.
OS Platform *	Enter the OS platform for the device. For example: IOS XR. Note that you must enter Cisco IOS platform names with a space, not a hyphen.
Version *	<p>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.</p> <p>Required only if you don't specify a ZTP profile in the Profile Name column.</p>
Device Family *	<p>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.</p> <p>Required only if you don't specify a ZTP profile in the Profile Name column.</p>

Template Column	Usage
Config ID *	<p>Enter the Cisco Crosswork-assigned ID for the configuration file you want to use when configuring the device. Cisco Crosswork assigns a unique ID for every configuration file during upload.</p> <p>Required only if you don't specify a ZTP profile in the Profile Name column.</p>
Profile Name *	<p>Enter the name of the ZTP profile you want to use to provision this device.</p> <p>Required only if you want to use a ZTP profile to specify things like the configuration ID, image ID, OS platform, and so on.</p>
Product ID *	<p>Enter the Cisco-assigned PID (product identifier) coded into the device hardware. You can retrieve the PID from the UDI (Unique Device Identifier) information printed on the label affixed to every Cisco networking device when it leaves the factory.</p> <p>Please note that, in this release, no verification is performed on the PID. We recommend that you supply a correct PID anyway, in case of future requirements.</p>
UUID	<p>You can choose to generate and specify a Universally Unique Identifier (UUID) to be assigned to the device when it is onboarded. If you choose this option, enter the 128-bit UUID in this column. Otherwise, leave the field blank and Cisco Crosswork will assign a random UUID when it onboards the device.</p>
MAC Address	<p>Enter the device's MAC address.</p>
IP Address	<p>Enter the device's IP address (IPv4 or IPv6), along with its subnet mask in slash notation.</p>
Configuration Attributes	<p>Enter the values you want Cisco Crosswork to use for the custom replaceable parameters in the configuration file for the device. If you are using only the default replaceable parameters, leave this field blank. If you're using Secure ZTP, you can use custom replaceable parameters only for day-zero configuration file parameters. For help using replaceable parameters, see <a href="#">Prepare and Load Configuration Files, on page 250</a>.</p>
Connectivity Protocol	<p>The connectivity protocols needed to monitor the device or to support Cisco Crosswork applications and features. Choices are: <b>SSH</b>, <b>SNMPv2</b>, <b>NETCONF</b>, <b>TELNET</b>, <b>HTTP</b>, <b>HTTPS</b>, <b>GRPC</b>, and <b>SNMPv3</b>. For help selecting the correct mix of protocols, see the table in the following topic, "Crosswork Connectivity Protocol Requirements".</p>
Connectivity IP Address	<p>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.</p>

Template Column	Usage
Connectivity Port	<p>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.</p> <p>Specify at least one port and protocol for every device, except if you want to:</p> <ul style="list-style-type: none"> <li>Set the status of the onboarded device as unmanaged or down.</li> <li>Disable Cisco Crosswork reachability checks for the onboarded device.</li> </ul> <p>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. For help selecting the correct mix of protocols, see the table in the following section, "Crosswork Connectivity Protocol Requirements".</p>
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, as specified in Cisco Crosswork.
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.
Secure ZTP Encrypted	Currently unsupported. Enter FALSE.
Image ID	<p>Cisco Crosswork assigns a unique ID for every software image file during upload. Enter the Cisco Crosswork-assigned ID for the software image file you want to install on the device.</p> <p>Required only if you want to include installation of a software image during onboarding, and you did not specify a ZTP profile with this software image in the Profile Name column.</p>
PreConfig ID	<p>Cisco Crosswork assigns a unique ID for every configuration file during upload. Enter the Cisco Crosswork ID of the configuration script you want to run before running the configuration file specified in the Config ID column.</p> <p>Required only if you want to run a pre-configuration file during onboarding.</p>
PostConfig ID	<p>Cisco Crosswork assigns a unique ID for every configuration file during upload. Enter the Cisco Crosswork ID of the configuration script you want to run immediately after running the configuration file specified in the Config ID column.</p> <p>Required only if you want to run a post-configuration file during onboarding.</p>

Template Column	Usage
SZTP Config Mode	Enter <b>merge</b> if you want Secure ZTP to merge the configuration files you specify in the Config ID, PreConfig ID, and PostConfig ID columns with a pre-existing configuration on the device. Leave this column blank if you want to overwrite any existing configuration with the content of the specified configuration files (overwrite is the default specified by leaving the column blank).
Version ID	<p>The version ID of the configuration.</p> <p>Required only if you specified a pre-configuration and a post-configuration file to run during onboarding.</p>
routingInfo.globalospfrouterid	If implementing OSPF on the device: Enter the OSPF Router ID for the device. Otherwise, leave this field blank.
routingInfo.globalisisystemid	If implementing IS-IS on the device: Enter the IS-IS System ID for the device. Otherwise, leave this field blank.
routingInfo.teRouterid	If implementing Traffic Engineering on the device: Enter the TE router ID for the device. Otherwise, leave this field blank.

### Crosswork Connectivity Protocol Requirements

Cisco Crosswork applications require you to enable a range of connectivity protocols for each device. The following table identifies these requirements for each supported connectivity protocol. If you use the applications listed in this table, be sure to enable these protocols on your devices. You must enable at least one of these protocols on each device in order to onboard it; you cannot onboard a device without at least one of these protocols.

*Table 23: Connectivity Protocol Requirements for Applications and Features*

Protocol	Port	Crosswork Application	Application Feature
GRPC	9090	<ul style="list-style-type: none"> <li>Cisco Crosswork Network Controller</li> <li>Cisco Crosswork Change Automation and Health Insights</li> <li>Cisco Crosswork Optimization Engine</li> </ul>	Cisco Crosswork API communication
HTTP	80	<ul style="list-style-type: none"> <li>Cisco Crosswork Network Controller</li> <li>Cisco Crosswork Change Automation and Health Insights</li> <li>Cisco Crosswork Optimization Engine</li> </ul>	Onboarding of the device to Cisco Network Services Orchestrator

## ■ Prepare Single ZTP Device Entries

Protocol	Port	Crosswork Application	Application Feature
HTTPS	443	<ul style="list-style-type: none"> <li>• Cisco Crosswork Network Controller</li> </ul>	Onboarding of the device to Cisco Network Services Orchestrator
NETCONF	830	<ul style="list-style-type: none"> <li>• Cisco Crosswork Network Controller</li> <li>• Cisco Crosswork Change Automation and Health Insights</li> <li>• Cisco Crosswork Optimization Engine</li> </ul>	Onboarding of the device to Cisco Network Services Orchestrator
SNMPv2	161	<ul style="list-style-type: none"> <li>• Cisco Crosswork Network Controller</li> <li>• Cisco Crosswork Change Automation and Health Insights</li> <li>• Cisco Crosswork Optimization Engine</li> </ul>	SNMPv2 data collection
SNMPv3	161	<ul style="list-style-type: none"> <li>• Cisco Crosswork Network Controller</li> <li>• Cisco Crosswork Change Automation and Health Insights</li> <li>• Cisco Crosswork Optimization Engine</li> </ul>	SNMPv3 data collection
SSH	22	<ul style="list-style-type: none"> <li>• Cisco Crosswork Network Controller</li> <li>• Cisco Crosswork Change Automation and Health Insights</li> <li>• Cisco Crosswork Optimization Engine</li> </ul>	<ul style="list-style-type: none"> <li>• CLI data collection</li> <li>• SSH access to devices</li> </ul>

## Prepare Single ZTP Device Entries

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

The ZTP device entries you create using this method always appear in the **Zero Touch Devices** tab with their **Status** set to **Unprovisioned**. They remain **Unprovisioned** until you trigger ZTP processing.

After ZTP onboards your device entries, Cisco Crosswork will display fields calling for more information about the device, such as its geographical location. You will need to supply this additional information by editing the device's inventory record, as explained in [Complete Onboarded ZTP Device Information, on page 301](#).

## Procedure

---

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

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

**Step 3** Click the **+**.

**Step 4** Enter values for the new ZTP device entry.

For help with the types of information called for in each device entry field, see the template reference in [Prepare ZTP Device Entry Files, on page 271](#).

**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 re-onboarding 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 ZTP device-entry CSV files. If you plan to use this method for creating ZTP device entries, you must prepare these files in advance, as explained in [Prepare ZTP Device Entry Files, on page 271](#).

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.

After ZTP onboards your device entries, Cisco Crosswork will display fields calling for more information about each device, such as its geographical location. You will need to supply this additional information by editing the device's inventory record, as explained in [Complete Onboarded ZTP Device Information, on page 301](#).

### Procedure

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

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

**Step 3** Click the .

**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, you must update the configuration of your DHCP server (and, for PnP ZTP only, your TFTP server) with information that permits Cisco Crosswork to communicate with your devices and respond to their requests for downloads.

The following topics provide examples showing how to update your server configurations to meet this requirement. The instructions and examples you choose to follow will depend on the ZTP mode you have chosen to use:

- For Classic ZTP, see [Set Up DHCP for Classic ZTP, on page 278](#).
- For Secure ZTP, see [Set Up DHCP for Secure ZTP, on page 282](#).
- For PnP ZTP, see [Set Up DHCP and TFTP for PnP ZTP, on page 283](#).

For a set of configuration scripts for Classic ZTP and Cisco PNR, see [Classic ZTP DHCP Setup Scripts for Cisco Prime Network Registrar \(CPNR\), on page 284](#)

### Set Up DHCP for Classic ZTP

Before triggering Classic 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.

**Figure 100: Classic ZTP DHCP Context (ISC)**

```
#authoritative;

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

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;
}
```

### Examples: 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) (<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 cluster.
- 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 in this topic, "Copy Bootfile Names and UUIDs for DHCP Setup".
- Configuration files do not require UUIDs.

**Figure 101: 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>";
```

## Set Up DHCP for Classic ZTP

```

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

```

Figure 102: 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 103: 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 104: 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";
    }
}

```

## Examples: Generic Internet Systems Consortium (ISC) DHCP Setup for Classic ZTP

The following figures show examples of the type of host entries you would make for Classic ZTP 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 105: 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 106: Classic ZTP ISC IPv6 DHCP Configuration Example

```

host 5501
{
    host-identifier option dhcp6.client-id
00:02:00:00:00:09:4f: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";
    }
}

```

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

Table 24: ISC IPv4 DHCP Configuration Host Entries and Values (Classic ZTP)

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 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 <code>show inventory</code> 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 <code>filename =</code> parameter.

IPv4 Entry	Description
option user-class = "exr-config" and ffl filename =	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 <code>filename =</code> parameter.

### 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.

## Set Up DHCP for Secure ZTP

Before triggering Secure 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 provides an example showing how to update the DHCP server configuration file to meet this requirement. The example assumes you are using an Internet Systems Consortium (ISC) DHCP server. The line enabling the `sztp-redirect` option is required for Secure ZTP.

Please note that the device sends the user-class option `xr-config` along with option 143, so this needs to be configured as shown as part of the `host` block.

**Figure 107: Secure ZTP DHCP Configuration File (ISC)**

```
# dhcpcd.conf
#
# Sample configuration file for ISC dhcpcd
#
# Attention: If /etc/ltsp/dhcpcd.conf exists, it will be used as the
# configuration file instead of this file.
#
#
# option definitions common to all supported networks...
option domain-name "cisco.com";
option domain-name-servers 192.168.100.101, 171.70.168.183;
option sztp-redirect code 143 = text;
```

```
option subnet-mask 255.255.255.0;
default-lease-time 600;
max-lease-time 7200;
INTERFACES="ens192";

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none'), since DHCP v2 does not
# have support for DDNS.
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, uncomment the "authoritative" directive below.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers 192.168.100.100;
    range 192.168.100.105 192.168.100.150;
}

host sztpdevice {
    hardware ethernet 08:4f:a9:0e:43:c8;
    fixed-address 192.168.100.153;
    if exists user-class and option user-class ="xr-config" {
        # If you want to use a remote circuit ID to identify a remote host
        # comment out the first option line and uncomment the second.
        option sztp-redirect
        "https://<CrossworkHostIP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";

        #option sztp-redirect
        #"
```

## Set Up DHCP and TFTP for PnP ZTP

Before triggering PnP ZTP processing, you must:

1. Set up an external TFTP server that is reachable by your IOS-XE devices.
2. Upload PnP profile to the external TFTP server.
3. Update your DHCP configuration file with information pointing to the location of the Cisco Crosswork PnP Server.

The following topics provide examples showing how to perform each of these tasks.

### Set Up the External TFTP server

An external TFTP server is required for all of the supported IOS-XE routers. The server must be active on port 69 UDP. If your organization does not already have a TFTP server, [see \(for example\) the guidance here](#).

### Upload the PnP Profile to TFTP

The PnP profile is a simple generic configuration file. Uploading the PnP profile to the configuration service on the TFTP repository is a one-time activity.

The profile's contents must specify use of the Crosswork cluster's virtual data port. In this example, the IP address 192.168.100.211 is the data VIP for the embedded Cisco Crosswork PnP server and 30620 is the PnP server external port.

**Figure 108: Example: Generic PnP Profile**

```
pnp profile cwpnp-data
transport http ipv4 192.168.100.211 port 30620
```

### Configure the DHCP Server

The DCHCP entry redirects traffic from the PnP agent on the device to the IP address of the external TFTP server.

**Figure 109: Sample PnP ZTP DHCP Setup**

```
option tftp code 150 = text;
host cztp1 {
    hardware ethernet 00:a7:42:86:54:f1;
    option tftp150 "192.168.100.205";
}
```

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

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



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

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.

**Figure 110: 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-b2e5-051249d9b0db"

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 111: 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 112: 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 113: 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 114: IPv6 Script 2 of 5: ztp-v6-client-class-exp.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 115: IPv6 Script 3 of 5: ztp-v6-iso-lookup-exp.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 116: IPv6 Script 4 of 5: ztp-v6-script-lookup-exp.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 117: 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 )
    }
  ]
)
}

```



```
( 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 restarting each of the devices.

### Before you begin

Before triggering ZTP bootstrap on any of your devices, ensure that you have finished:

- All of the preliminary setup tasks explained in [ZTP Setup Workflow, on page 246](#).
- Creating ZTP device entries for the devices you want to bootstrap, as explained in [Prepare ZTP Device Entry Files, on page 271](#) and [Prepare Single ZTP Device Entries, on page 276](#).
- DHCP (and TFTP, if using PnP ZTP) setup, as appropriate for your choice of ZTP mode, as explained in the corresponding topic in [Set Up DHCP for Crosswork ZTP, on page 278](#).

### If you are using Secure ZTP:

1. Telnet to the console on each of the device(s) you want to onboard: `telnet <device IP> <userID><password>`.
2. Check if Secure ZTP is enabled on the device:
  - a. For IOS-XR versions 7.5.2 or earlier: Enter Bash run mode and issue the following command:  
`[xr-vm_node:~]$pyztp2 --ztp-mode ZTP Mode: Secure`
  - b. For IOS-XR versions later than 7.5.2: Go to the IOS CLI command prompt and enter the following command `show ztp information`.
3. Issue the following commands to clean logs and configurations:

```
ios#ztp clean  
ios#config terminal  
ios(config)#commit replace  
ios(config)#end
```

**If you are using PnP ZTP:** Be sure to set the minimum license boot-level on each IOS-XE device to **metroipaccess** or **advancedmetroipaccess** **before** you trigger ZTP processing. If the boot level has been set properly, the output of the IOS-XE `#sh run | sec license` CLI command on the device should contain statements showing either of these two license levels: `license boot level advancedmetroipaccess` or `license boot level metroipaccess`. If the command output shows any other license level lower than these two, the Cisco PnP cryptographic functionality will not be enabled. This will cause certificate installation to fail, which will then cause PnP ZTP device provisioning to fail.

## Procedure

### Step 1

Initiate ZTP processing as appropriate for the ZTP mode you are using:

- For Classic ZTP, use one of these 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 the device console via Telnet, then issue the **ztp initiate** command.
- For Secure ZTP, use one of these 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 the device console via Telnet, then issue the following commands (the `ztp initiate interface` value given here starts Secure ZTP on the device management port):
 

```
ztp enable noprompt
ztp initiate debug verbose interface MgmtEth 0/RP0/CPU0/0
```
- For PnP ZTP, use the option appropriate for your devices:
  - On Cisco ASR 903, ASR 907, and NCS 520 devices: Connect to it via Telnet, then issue a **write erase** command, followed by a **reload** command.
  - On Cisco ASR 920 devices: Press the ZTP button on the chassis for 8 seconds.

Repeat this step as needed for each of the devices you plan to provision during this session. You can restart all or as few devices as needed during a single session.

### Step 2

Monitor the progress of ZTP processing 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 is a requirement for most organizations with active networks, and can only be added by human operators.

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 this needs update from people.

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.

### Procedure

#### 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 the . 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.

## Reconfigure Onboarded ZTP Devices

- f) Click the .
  - 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 send experts to the same site as 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 the .

## 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 > Network 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 > Network 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

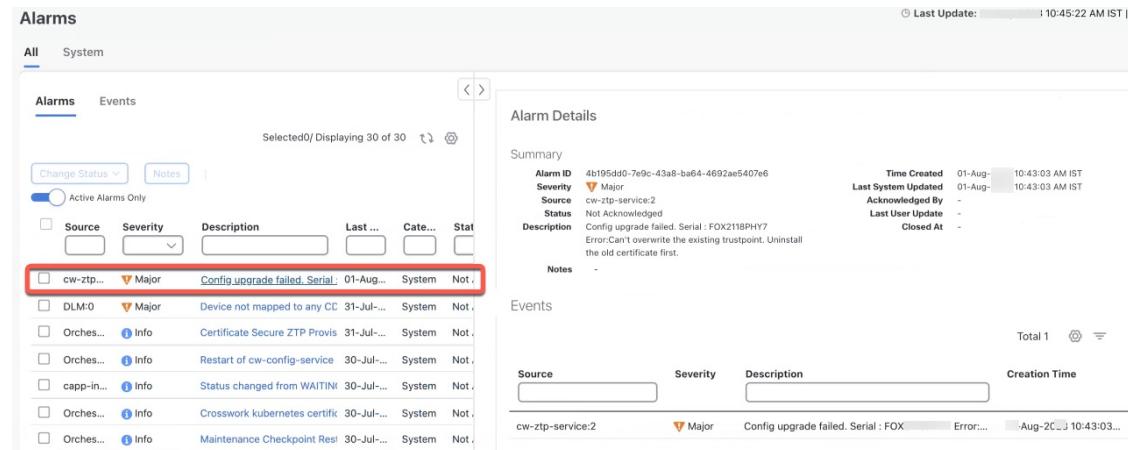
Normally, Cisco Crosswork ZTP provisioning and onboarding happen quickly and automatically. Issues do occur at times, so the following topics explain how to diagnose and remedy issues, including common issues and issues specific to ZTP modes. For reference, this section also supplies a comprehensive index of ZTP errors indicated in Crosswork alarms or events.

## Diagnose ZTP Issues Using the Alarms Window

You can use the Crosswork Alarms window to view summary and detail information for any ZTP-related error, whether propagated as an alarm or an event. The alarm details contain information about the likely cause of the error and, where appropriate, how to recover from it.

1. Select **Administration > Alarms** to display the Alarms window.
2. (Optional) If the ZTP error is propagated only as an event: Click the **Events** tab to view the event. If the event has a correlated alarm, click the **Yes** link in the **Correlated Alarms** column to view details for the correlated alarm.
3. For ZTP errors propagated as alarms: Click the link in the **Description** column in the Alarms window row displaying the ZTP error whose details you want to see. The **Alarms** window displays **Alarm Details** on the right panel, as shown in the illustration below.

**Figure 118: Alarms View with Detail Window**



For a comprehensive list of ZTP-related errors and how they are propagated, see [Troubleshoot ZTP: Alarms and Events Reference, on page 310](#).

## Diagnose ZTP Issues Using the Status Column

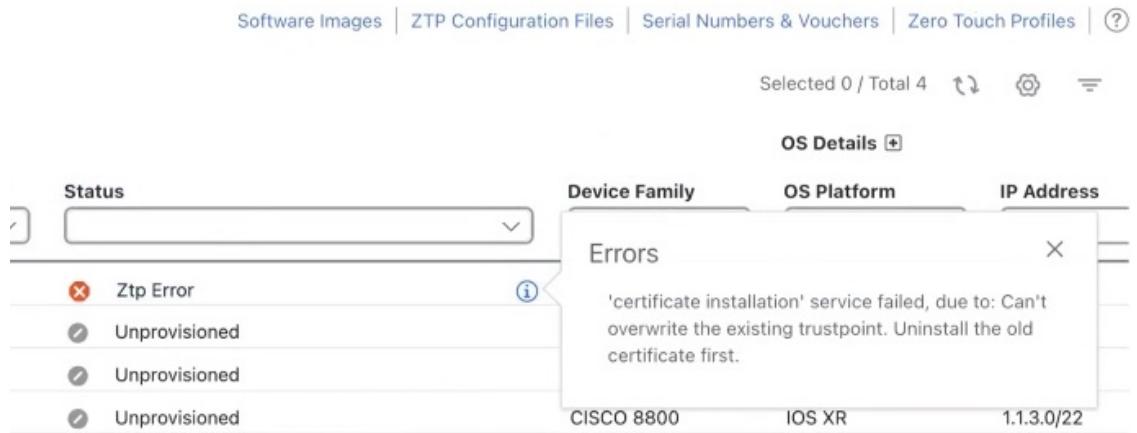
You can use the **Zero Touch Devices** tab on the **Network Devices** window to view summary and detail information for any ZTP-related error. The alarm details contain information about the likely cause of the error and, where appropriate, how to recover from it.

1. Select **Device Management > Network Devices > Zero Touch Devices**. The Zero Touch Devices window displays a list of all the devices that are onboarding using ZTP.

The **Status** column 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 ⓘ to display a popup window with information about the error, like the one shown in the following example.

**Figure 119: Error Popup Window**



- When you're finished viewing the popup window, click the X to close it.

For a comprehensive list of ZTP-related errors, see [Troubleshoot ZTP: Alarms and Events Reference, on page 310](#).

## Diagnose ZTP Issues Using Error Logs

You can diagnose ZTP issues by viewing ZTP error logs. You can view or request error logs directly from the Crosswork user interface, using a `showtech` request. You can also download error logs using an SSH login to one or more of the virtual machines running Crosswork and the instance of the Crosswork ZTP service running on that VM.

To view or request copies of ZTP error log files using a `showtech` request from the Crosswork user interface, follow these steps:

- Using an ID with administrator privileges, log into the Crosswork user interface.
- Select **Administration > Crosswork Manager**
- With the **Crosswork Summary** page displayed, click on the **Zero Touch Provisioning** tile. Crosswork displays details for the ZTP application.
- With the application details displayed, select **Showtech Options > Request Logs**. Then select **Showtech Requests**. You can retrieve your log files from the dashboard when the request is completed.

You can also choose to simply view the most recent log files by selecting **Showtech Options > View Showtech Logs**.



**Tip** If ZTP processing seems to be completing successfully but you are having issues with the onboarding phase, you may want to see logs for the Crosswork device inventory manager application (known as `dlminvmgr`) in addition to the logs for the ZTP service. You can do that by selecting **Platform Infrastructure** instead of **Zero Touch Provisioning** on the **Crosswork Summary** page (during step 3, above).

To download error log files from the Crosswork ZTP service, follow these steps:

1. Log in to the VM using an Secure Shell command like the following:

```
ssh admin@VMIP
```

Where:

- `admin` is the Crosswork administrator ID. For example: `cw-admin`.
- `VMIP` is the IP address of the virtual machine running Crosswork. For example: `192.168.100.102`.

2. Access the `cw-ztp-service` Kubernetes pod using a command like the following:

```
# kubectl exec -it PodID# bash
```

Where `PodID#` is the ID of the `cw-ztp-service` Kubernetes pod. Change the pod ID number as needed to match the number of the pod you want to access (pod 0 is always the first). For example: `cw-ztp-service-0`, `cw-ztp-service-1`, `cw-ztp-service-2`, and so on.

3. Change to the log folder with a command like the following: `cd /var/log/robot/`. You can then open any of the following ZTP-specific files in the folder:

- `cw-image-service_stdout.log`
- `cw-image-service_stderr.log`
- `cw-config-service_stdout.log`
- `cw-config-service_stderr.log`

## Troubleshoot Common ZTP Issues

The following table identifies remedies for common issues that can occur with any of the ZTP modes. For details on ZTP processing for all three ZTP modes, see [ZTP Processing Logic, on page 242](#).

Table 25: Common ZTP Issues and Remedies

Phase	Issue	Symptoms	Remedy
Setup	Image, configuration, or SMU file upload fails	Error messages displayed in the user interface during upload	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 files aren't in the drop-down menu when creating ZTP device entries or ZTP profiles	Files missing from the dropdown list	The drop-down menu selects files based on the device family and IOS 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 creating.
	Errors during device entry CSV file import	Varies; see error log	If devices in inventory have the same serial numbers as the devices you're importing, check that the devices are in the <b>Unprovisioned</b> state before import. All the devices imported using CSV files have their status set to <b>Unprovisioned</b> 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 UIDs before import.
Unprovisioned	DHCP is unresponsive or offer execution fails	ZTP processing hangs	Test access to the DHCP server from the Cisco Crosswork server, using ping and similar tools

Phase	Issue	Symptoms	Remedy
In Progress	Image or SMU file download fails	ZTP processing hangs	<p>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.</p> <p>If you must correct the image UUID specified in the configuration file, make sure you restart the DHCP server before initiating ZTP processing again.</p>
	Configuration file download fails	Logged errors	<p>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 re-initiating ZTP processing. Make sure that the device serial number matches the serial number on the chassis of the device.</p> <p>Ensure that the status of the device is either <b>Unprovisioned</b> or <b>In Progress</b> before initiating ZTP processing. Configuration downloads continue to fail as long as the device is in any other state.</p>
Onboarded	Device state is showing <b>Onboarded</b> and not <b>Provisioned</b>	Status column did not show <b>Provisioned</b>	<b>Provisioned</b> is an intermediate state in ZTP processing. When the device state changes to <b>Provisioned</b> , Cisco Crosswork attempts to onboard the device immediately. The status changes to <b>Onboarded</b> or <b>Onboarding Error</b> after.
	Onboarding Error	Status column shows <b>Onboarding Error</b>	<p>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 <b>Provisioned</b>, then to <b>Onboarding Error</b>. 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.</p> <p>Onboarding can only succeed when you fill all the DLM policy fields with unique, non-blank values. If onboarding fails, inspect the popup error message, update the corresponding fields and retry onboarding.</p>

## Troubleshoot Classic ZTP Issues

The following table identifies remedies for issues that can occur during Classic ZTP processing. For details on processing steps during each phase of Classic ZTP processing, see [#unique\\_209 unique\\_209\\_Connect\\_42\\_ClassicZTPProcessing, on page 242](#).

**Table 26: Classic ZTP Issues and Remedies**

Phase	Issue	Symptoms	Remedy
Unprovisioned	Crosswork cannot verify the device serial number	Status column does not show "In Progress"	ZTP supports addition of multiple serial numbers irrespective of how many devices there are to be added. While creating a device entry, make sure to assign the correct serial number. ZTP is initiated based on the serial number, and the connected device entry will start to show state changes based on it.
In Progress	Boot script execution fails	Processing hangs. See error log.	Examine the boot script for errors, correct them and try again.
	iPXE reload fails	Processing hangs. See error log.	This is likely due to a temporary issue with the device. Try again. If the process fails repeatedly, contact the Cisco device support team.
Unprovisioned, In Progress	Device progress report API call fails	Processing hangs. See error log.	Make sure the API call is properly formatted and has correct values. Correct them and try again. May also be the result of temporary connectivity loss due to network issues.

## Troubleshoot PnP ZTP Issues

The following table identifies remedies for issues that can occur during PnP ZTP processing. For details on steps during each phase of PnP ZTP processing, see [#unique\\_209 unique\\_209\\_Connect\\_42\\_PnPZTPProcessing, on page 245](#).

Table 27: PnP ZTP Issues and Remedies

Phase	Issue	Symptoms	Remedy
Unprovisioned	PnP profile download fails	Device stays in Unprovisioned state	The download may have failed due to packets being dropped or similar network traffic issues. First ensure that the PnP profile has the correct file name, protocol, IP address, and port specified. Ensure that the TFTP server is up and reachable. Then try triggering ZTP from the device again.
Unprovisioned, In Progress	Capability service request fails	ZTP device entry is moved to error state with the message "service 'capability check' failed". Reason: Device doesn't support the minimum required capabilities.	For PnP ZTP to work, the XE device being provisioned must support the following minimum Cisco IOS-XE capabilities: <ul style="list-style-type: none"> <li>• device-info</li> <li>• certificate-install</li> <li>• image-install</li> <li>• config-upgrade</li> <li>• backoff</li> </ul> If you are having trouble with this requirement, contact the Cisco device support team.
In Progress	Certificate install fails	ZTP device goes into error state with the message "certificate installation service failed."	First, log in to the XE device and clean up trustpoint "CrossworkPnP" if it already exists. Then, from the Crosswork GUI, move the device back to the UnProvisioned state and re-trigger ZTP from the beginning.

## Troubleshoot ZTP: Alarms and Events Reference

The following tables identify alarms and events for all ZTP processing modes and phases.

### ZTP Service Alarms and Events

Component	Description	Severity	Event/Alarm	Clearing Event	Notes
Device Delete API	ZTP Device Delete operation failed	Major	Event	No	Admin operation
Device Delete API	ZTP Device Delete was successful	Info	Event	No	Admin operation

Component	Description	Severity	Event/Alarm	Clearing Event	Notes
Device Import API	ZTP Device Bulk Add failed	Major	Event	No	Admin operation
Device Import API	ZTP Device(s) Import successful	Info	Event	No	Admin operation
Device POST API	ZTP Add Device Failed	Major	Event	No	Admin operation
Device POST API	ZTP Device Added Successfully	Info	Event	No	Admin operation
Device PUT API	ZTP Update Device not allowed as status is Onboarded	Major	Event	No	Admin operation
Device PUT API	ZTP Update Device was successful	Info	Event	No	Admin operation
Device Patch API	ZTP status update failed	Major	Event	No	Admin operation. For device status update API.
Device Patch API	ZTP status updated, Error in Reporting License Entitlement	Major	Event	No	Admin operation. For device status update API.
Device Policy Post	Failed to update device policies	Major	Event	No	Notification operation. No need of alarms for policy notification. As policies are impacted on DLM onboarding, Crosswork adds alarms for onboarding flow.
Device Policy Post	Device policies updated successfully	Info	Event	No	Notification operation. No need of alarms for policy notification. As policies are impacted on DLM onboarding, Crosswork adds alarms for onboarding flow.
SN Import OV API	SZTP Invalid Ownership Voucher data, failed to read	Major	Event	No	Admin operation
SN Import OV API	SZTP Failed to save Ownership Voucher data	Major	Event	No	Admin operation
SN Import OV API	SZTP Ownership Voucher data saved successfully	Info	Event	No	Admin operation
SN Delete API	Failed to delete ZTP Serial Number	Major	Event	No	Admin operation

Component	Description	Severity	Event/Alarm	Clearing Event	Notes
SN Delete API	ZTP Serial Number(s) deleted successfully	Info	Event	No	Admin operation
SN Post API	Failed to add ZTP Serial Number(s)	Major	Event	No	Admin operation
SN Put API	Failed to update ZTP Serial Number	Major	Event	No	Admin operation
Profile Put API	ZTP Profile update failed	Major	Event	No	Admin operation
Profile Put API	ZTP Profile update successful	Info	Event	No	Admin operation
Static Route Add API	Add Static Route successful	Info	Event	No	Admin operation
Static Route Add API	Add Static Route failed	Major	Event	No	Admin operation, so raised as a Major event
Static Route Delete API	Delete Static Route successful	Info	Event	No	Admin operation
Static Route Delete API	Delete Static Route failed	Major	Event	No	Admin operation, so raised as a Major event
SN Post API	ZTP SerialNumber(s) added successfully	Info	Event	No	Admin operation, only as newly added
SN Put API	ZTP SerialNumber updated successfully	Info	Event	No	Admin operation, only as newly added
Profile Post API	ZTP Profile added successfully	Info	Event	No	Admin operation, only as newly added
Profile Post API	ZTP Profile addition failed	Major	Event	No	Admin operation, only as newly added
Profile Delete API	ZTP Profile deleted successfully	Info	Event	No	Admin operation, only as newly added
Profile Delete API	ZTP Profile deletion failed	Major	Event	No	Admin operation, only as newly added
SN Import OV API	SZTP OV tar file read success	Info	Event	No	Admin operation
ZTP Service CLMS	CLMS Client Connection Error	Major	Alarm	Yes	Admin operation
ZTP Service CLMS	CLMS Client Connection Success	Info	Event	N/A	Admin operation

### Classic ZTP Processing Alarms and Events

Component	Description	Severity	Event/Alarm	Clearing Event	Notes
Device Unauth API	ZTP Update Status from device failed	Major	Alarm	Yes	The Unauth API raises an alarm if it detects a duplicate connectivity protocol or a bad serial number.
Device Unauth API	ZTP Update Status from device was processed successfully	Clear	Alarm	N/A	Raised as a clearing alarm as part of the Unauth API flow.
Device Unauth API	ZTP Update Status. Device not found	Major	Event	No	Raised as an event if the device UUID is not found. It's not possible to raise this as an alarm since the Device is not found.
Device Unauth API	ZTP Update Status, delete the processing device	Clear	Alarm	N/A	Clears major alarms raised for a Device UUID that is being deleted.
Device Unauth API	ZTP status update API from device (fail in report entitlement to CLMS)	Major	Event	No	The license call has failed. Raised as an event, as there is no way to clear it as an alarm.
Device Unauth API	ZTP status update API, service is in maintenance mode	Major	Event	No	The system is in maintenance mode. Raised as an event, as there is no way to clear it as an alarm while the system is in maintenance mode.

### Secure ZTP (SZTP) Processing Alarms and Events

Component	Description	Severity	Event/Alarm
Device SZTP API	SZTP parsing of Owner signing key failed as part of refresh/update certificate notification	Major	Event
Device SZTP API	SZTP parsing of Owner certificate failed as part of refresh/update certificate notification	Major	Event
Device SZTP API	SZTP flow, ZTP Service in Maintenance Mode	Major	Event
Device SZTP API	SZTP flow, ZTP License Validation failed	Major	Event

Component	Description	Severity	Event/Alarm
Device SZTP API	SZTP device bootstrap failed, device serial not in allowed list or invalid	Major	Event
Device SZTP API	SZTP device bootstrap request failed, device not found	Major	Event
Device SZTP API	SZTP report progress request failed due to empty serial key	Major	Event
Device SZTP API	SZTP device Report progress request failed, device not found	Major	Event
Device SZTP API	SZTP device bootstrap failed, not enabled on device	Major	Alarm
Device SZTP API	SZTP device bootstrap failed, not allowed when device status is Onboarded or ProvisioningError	Major	Alarm
Device SZTP API	Report progress failed as SZTP not enabled on device	Major	Alarm
Device SZTP API	SZTP report progress not allowed when status is Onboarded or ProvisioningError	Major	Alarm
Device SZTP API	SZTP device redirect info request failed	Major	Alarm
Device SZTP API	SZTP device redirect info request successful	Info	Alarm
Device SZTP API	SZTP device onboard info request failed	Major	Alarm
Device SZTP API	SZTP device report progress request failed	Major	Alarm

Component	Description	Severity	Event/Alarm
Device SZTP API	SZTP device report progress request successful.	Clear	Alarm
Device SZTP API	SZTP process. delete the processing device	Clear	Alarm

### Plug n Play ZTP (PnPZTP) Processing Alarms and Events

Component	Description	Severity	Event/Alarm
PNP Put API	PnPZTP device state update failed	Major	Event
Device PNP API	Initial WorkRequest parsing fails, sending backoff to device PnP agent	Major	Event
Device PNP API	Failed to save PnP request to database	Major	Event
Device PNP API	Invalid Work Request due to wrong serial number	Major	Event
Device PNP API	Invalid Work Request, no such device exists	Major	Event
Device PNP API	Invalid Work Request, Secure ZTP incorrectly configured	Major	Event
Device PNP API	PnP WorkRequest will ignore the request if the device status is not in Unprovisioned, In Progress or ZtpError state	Info	Event
PNP Work Request API	Capability Check: Device does not support minimum capabilities.	Major	Alarm
PNP Work Request API	Capability Check: Database update failed to save device details during capability check. Failed to find the service during capability check.	Major	Alarm

Component	Description	Severity	Event/Alarm
PNP Work Request API	Device Info Check: Database update failed, PNPRequestTable save failed during device info check. Failed to find the service during device info check.	Major	Alarm
PNP Work Request API	Certificate Install: Cannot install server certificate. Device does not support valid config register.	Major	Alarm
PNP Work Request API	Certificate Install: Server certificate install not required, device PnP profile is already using HTTPS	Major	Event
PNP Work Request API	Certificate Install: Database update failed, PNPRequestTable save failed during certificate install. Failed to find the service for certificate install.	Major	Alarm
PNP Work Request API	Image Install: Image Upgrade cannot proceed, could not fetch image from image service.	Major	Alarm
PNP Work Request API	Image Install: Image Upgrade cannot proceed, not enough free disk space.	Major	Alarm
PNP Work Request API	Image Install: Database update failed to save device during image install. Failed to find the service during image install.	Major	Alarm

Component	Description	Severity	Event/Alarm
PNP Work Request API	Config Upgrade: Config Upgrade failed.	Major	Alarm
PNP Work Request API	Config Upgrade: Database update failed to save device details in PNPRequest Table during config upgrade, or failed to find the service during config upgrade.	Major	Alarm
Device PNP API	Work Response parsing failed, failed to save/update WorkResponse for PnP service	Major	Event
PNP Work Request API	Device capability and Device Info checks successful.	Clear	Alarm
PNP Work Request API	Certificate install, image install and config upgrade successful.	Clear	Alarm
Device PNP API	Device Provisioned via PnP, waiting to Onboard to Crosswork (4-way PnP handshake was successful)	Clear	Alarm

#### ZTP-Related Image Service Alarms and Events

Component	Description	Severity	Event/Alarm
Upload Image	Image Upload was successful	Info	Event
Update Image	Update Image metadata was successful	Info	Event
Delete Image	Deletion of image was successful	Info	Event
Upload Image	Image Upload failed	Major	Event
Update Image	Updating Image metadata failed	Major	Event
Delete Image	Image Deletion Failed	Major	Event
Image download validation by Image UUID	ZTP Image file download validation failed	Major	Event
Image download validation by Image UUID	ZTP Image file download validation success	Info	Event
Image download validation by random token	SZTP Image file download validation failed	Major	Event

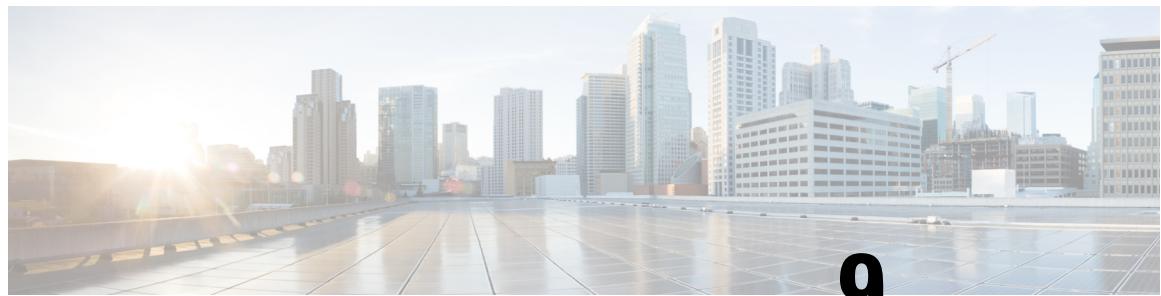
Component	Description	Severity	Event/Alarm
Image download validation by random token	SZTP Image file download validation success	Info	Event
Image download by Image UUID	Image download via DHCP to device failed	Major	Alarm
Image download by Image UUID	Image download via DHCP to device was successful	clear	Alarm
Image download by random token	Image download via DHCP to device failed	Major	Alarm
Image download by random token	Image download via DHCP to device was successful	clear	Alarm

### ZTP-Related Configuration Service Alarms and Events

Component	Description	Severity	Event/Alarm
Upload Config	Upload ZTP Config File was successful	Info	Event
Update Config	Updating Config file metadata was successful	Info	Event
Delete Config	ZTP Config file deletion was successful	Info	Event
Upload Config	Failed to Upload ZTP Config File	Major	Event
Update Config	Updating Config file metadata failed	Major	Event
Delete Config	ZTP Config file deletion failed	Major	Event
Config download validation with/without serial	Download Config file failed due to any validation issues	Major	Event
Config download validation with/without serial	Config file successfully downloaded	Info	Event

Component	Description	Severity	Event/Alarm
Config download with/without serial	Download Config file failed due to some issues	Major	Alarm
Config download with/without serial	Config file successfully downloaded	clear	Alarm
Config download with Config UUID	Download ZTP Config file to device based on UUID failed	Major	Alarm
Config download with Config UUID	Download ZTP Config file to device based on UUID was successful	clear	Alarm





## CHAPTER 9

# Manage System Access and Security

---

This section contains the following topics:

- [Manage Certificates, on page 321](#)
- [Manage Licenses, on page 334](#)
- [Manage Users, on page 344](#)
- [Manage Device Access Groups, on page 362](#)
- [Set Up User Authentication \(TACACS+, LDAP, and RADIUS\), on page 373](#)
- [Enable Single Sign-on \(SSO\), on page 386](#)
- [Security Hardening Overview, on page 388](#)
- [Configure System Settings, on page 391](#)

## 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 389](#) and [HTTPS, on page 388](#).

### How are Certificates Used in Crosswork?

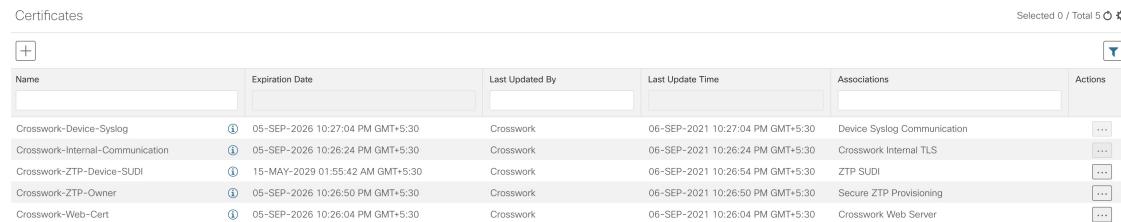
Communication between Crosswork applications and devices as well as between various Crosswork components are secured using the TLS protocol. TLS uses X.509 certificates to securely authenticate devices and encrypt data to ensure its integrity from source to destination. Crosswork uses a mix of generated and client uploaded certificates. Uploaded certificates can be purchased from Certificate authorities (CA) or can be self-signed.

## Certificate Types and Usage

For example, the Cisco Crosswork VM-hosted web server and the client browser-based user interface communicate with each other using Crosswork generated X.509 certificates exchanged over TLS.

The Crosswork Cert Manager is a proxy for multiple microservices and services within the distributed framework and manages all the Crosswork certificates. The Certificate Management UI (**Administration > Certificate Management**) allows you to view, upload, and modify certificates. The following figure displays the default certificates provided by Cisco Crosswork.

**Figure 120: Certificate Management UI**



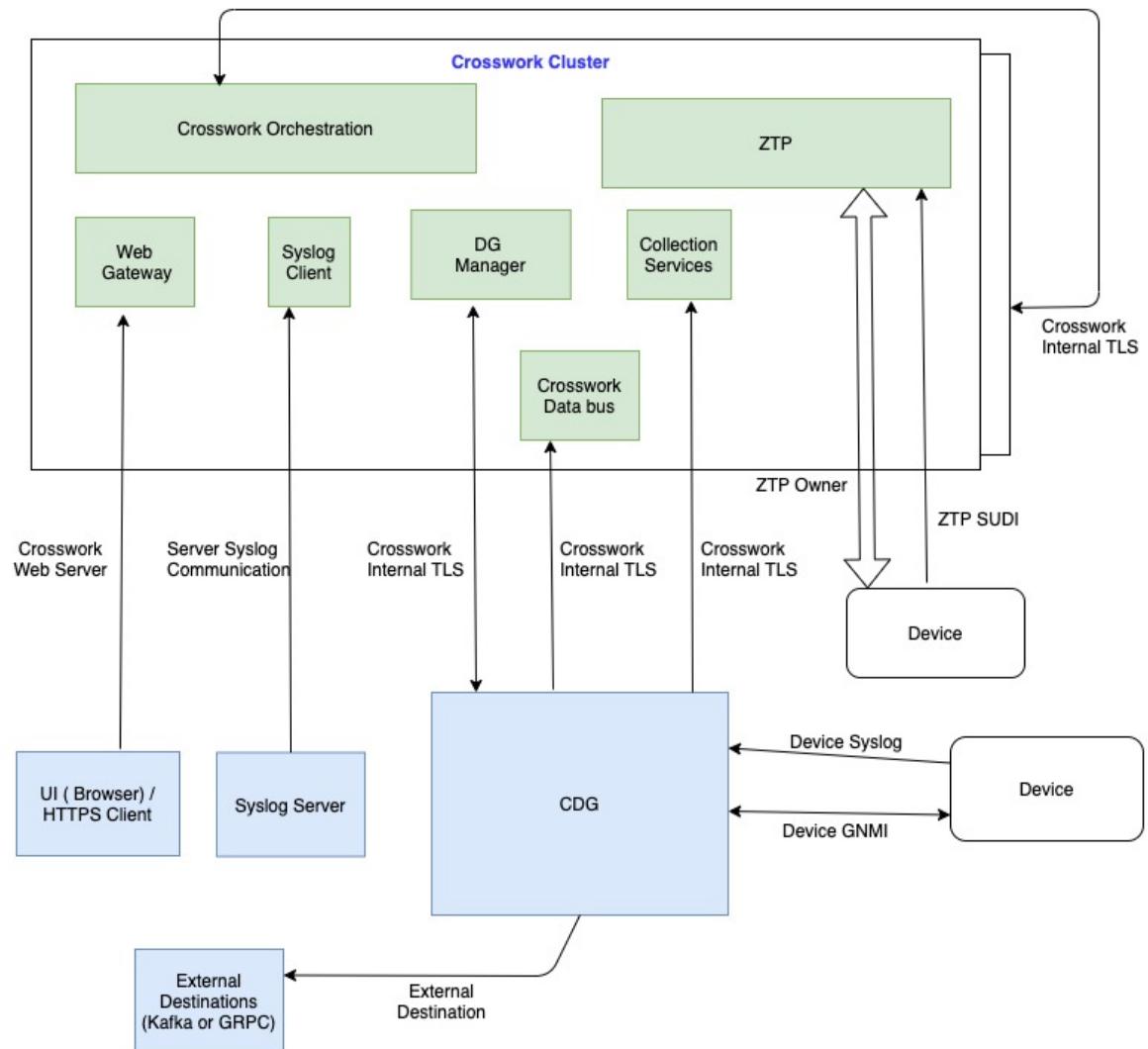
The screenshot shows a table titled 'Certificates' with the following data:

Name	Expiration Date	Last Updated By	Last Update Time	Associations	Actions
Crosswork-Device-Syslog	05-SEP-2026 10:27:04 PM GMT+5:30	Crosswork	06-SEP-2021 10:27:04 PM GMT+5:30	Device Syslog Communication	...
Crosswork-Internal-Communication	05-SEP-2026 10:26:24 PM GMT+5:30	Crosswork	06-SEP-2021 10:26:24 PM GMT+5:30	Crosswork Internal TLS	...
Crosswork-ZTP-Device-SUDI	15-MAY-2029 01:55:42 AM GMT+5:30	Crosswork	06-SEP-2021 10:26:54 PM GMT+5:30	ZTP SUDI	...
Crosswork-ZTP-Owner	05-SEP-2026 10:26:50 PM GMT+5:30	Crosswork	06-SEP-2021 10:26:50 PM GMT+5:30	Secure ZTP Provisioning	...
Crosswork-Web-Cert	05-SEP-2026 10:26:04 PM GMT+5:30	Crosswork	06-SEP-2021 10:26:04 PM GMT+5:30	Crosswork Web Server	...

## Certificate Types and Usage

The following figure shows how Crosswork uses certificates for various communication channels.

Figure 121: 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-InternalCommunication	<ul style="list-style-type: none"> <li>Generated and provided by Crosswork.</li> <li>This trust-chain is available in the UI (including the server and client leaf certificates) and is created by Crosswork during initialization. They are used for interprocess communications between Crosswork and Crosswork Data Gateway and communication between internal Crosswork components.</li> <li>Allows mutual and server authentication.</li> </ul>	Crosswork	<ul style="list-style-type: none"> <li>Crosswork Data Gateway</li> <li>Crosswork</li> </ul>	Download	5 years	—
CW Web Server	CW-Web-Certificate Server Authentication	<ul style="list-style-type: none"> <li>Generated and provided by Crosswork.</li> <li>Provides communication between the user browser and Crosswork.</li> <li>Allows server authentication.</li> </ul>	Crosswork Web Server	User Browser or API Client	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul>	5 years	30 day - 5 years

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
ZTP SUDI	CW-ZTP-Device-SUDI	<ul style="list-style-type: none"> <li>A public Cisco certificate that is provided as part of Crosswork.</li> <li>Provides ZTP protocol communication channel between the ZTP application and device.</li> <li>Allows server authentication.</li> </ul>	Crosswork ZTP	Device	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul>	100 days	30 day - User-defined
Secure ZTP Provisioning	CW-ZTP-Owner	<ul style="list-style-type: none"> <li>Generated and provided by Crosswork.</li> <li>Forwarded by ZTP to devices and used for second layer of encryption.</li> </ul>	Crosswork ZTP	Device	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul>	5	30 day - User-defined
Device Syslog	CW-Device-Syslog	<ul style="list-style-type: none"> <li>Generated and provided by Crosswork.</li> <li>Provides Syslog telemetry communications between devices and Crosswork Data Gateway.</li> <li>Allows server authentication.</li> </ul>	Crosswork Data Gateway	Device	Download	5 years	—
Device gNMI Communication	—	Provides gNMI telemetry communications between devices and Crosswork Data Gateway.	Crosswork Data Gateway	Device	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul>	Not Applicable	30 day - User-defined

## Add a New Certificate

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Server Syslog Communication	—	<ul style="list-style-type: none"> <li>Allows syslog events and logs from Crosswork to an external Syslog server.</li> <li>Allows server authentication.</li> </ul>	External Syslog Server	Crosswork	<ul style="list-style-type: none"> <li>Upload</li> <li>You can upload multiple certificates associated with different servers.</li> <li>Download</li> </ul>	—	30 day - User-defined
External Destination	—	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a mutual-authentication.	External Destinations (Kafka or gRPC)	Crosswork Data Gateway	<ul style="list-style-type: none"> <li>Upload <sup>1</sup></li> <li>Download</li> </ul>	—	30 day - User-defined
External Destination Server Auth	—	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a server-based authentication.	External Crosswork Data Gateway Destinations (Kafka or gRPC)	Crosswork Data Gateway	<ul style="list-style-type: none"> <li>Upload <sup>2</sup></li> <li>Download</li> </ul>	—	30 day - User-defined
Secure LDAP Communication	—	Crosswork uses the trust chain of this certificate to authenticate the secure LDAP server.	Secure LDAP server	Crosswork	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul>	—	30 day - User-defined

<sup>1</sup> You can upload multiple certificates associated with different destinations.

<sup>2</sup> You can upload multiple certificates associated with different destinations.

There are two category roles in Crosswork:

- Roles which allow you to upload or download trust chains only.
- Roles that allow upload or download of both the trust chain and an intermediate certificate and key.

## Add a New Certificate

This topic explains the steps to add a new certificate.

You can add certificates for these roles.

- **External Destination:** Certificates uploaded for this role are used to secure communication between Crosswork Data Gateway and external destinations like Kafka servers. To enable mutual authentication, the user uploads a **CA Certificate Trustchain** that will be common to both Crosswork Data Gateway and the external server. This trust chain contains a root CA certificate and any number of optional intermediate CA certificates. The last intermediate certificate in the chain and its corresponding private key is uploaded separately in the UI using **Intermediate key**, **Intermediate certificate**, and optionally **Passphrase** (if one was used for generating the intermediate key). Crosswork internally creates a client certificate using this intermediate key for the Crosswork Data Gateways that connects to the external destination. The destination (for example: Kafka) server certificate trust needs to be derived from the same root CA certificate.

You can upload certificates to the **External Destination** role, the authentication type must be opted as **Mutual-Auth** on the **Add Destination** page. For more information about the authentication types, see [Add or Edit a Data Destination, on page 53](#).

- **Server Syslog Communication:** The user uploads the trust chain of the Syslog server certificate. This trust chain is used by Crosswork to authenticate the Syslog server. Once this trust chain is uploaded and propagated within Crosswork, the user can add the syslog server (**Administration > Settings > Syslog Server Configuration**) and associate the certificate to enable TLS. For more information, see [Configure a Syslog Server, on page 391](#).
- **Devices gNMI communication:** The user uploads a bundle of trust chains used by Crosswork Data Gateway to authenticate the devices connecting to it. This trust chain and the device gNMI certificate must also be configured on the device. The trust chain file that is uploaded can contain multiple hierarchies of trust certificates as needed to allow all the devices in the network to connect. For more information, see [Configure gNMI Certificate, on page 92](#).
- **Secure LDAP Communication:** The user uploads the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork, the user can add the LDAP server (see [Manage LDAP Servers, on page 379](#)) and associate the certificate.
- **External Destination Server Auth:** The user uploads the root CA certificate. This certificate is used to establish a secure communication between Crosswork Data Gateway and external destinations like Kafka servers.

You can upload the certificates to the **External Destination Server Auth** role only when the authentication type is set to **Server-Auth**. For more information about the authentication types, see [Add or Edit a Data Destination, on page 53](#).

- **Application External Destination:** The user can upload the application certificates to ensure secure transfer of telemetry data to an external Kafka destination. The Kafka channel is safeguarded through mutual TLS, and the TLS Manager is responsible for managing the certificates used by external Kafka.

For information on certificate types and usage, see [Certificate Types and Usage, on page 322](#).



**Note**

Cisco Crosswork does not receive a web certificate directly. It accepts an intermediate CA and intermediate Key to create a new web certificate, and apply it to the Web Gateway.

If you prefer to upload your own ZTP and web certificates (instead of using the default certificates provided within Cisco Crosswork), use the Edit function (see [Edit Certificates, on page 328](#)).

### Before you begin

- All certificates that are uploaded must be in Privacy Enhanced Mail (PEM) format. Note where these certificates are in the system so that you can navigate to them easily.
- Trust chain files that are uploaded may contain the entire hierarchy (root CA and intermediate certificates) in the same file. In some cases, multiple chains are also allowed in the same file.
- Intermediate Keys need to be either PKCS1 or PKCS8 format.
- A data destination must be configured prior to adding a new certificate for an external destination. For more information, see [Add or Edit a Data Destination, on page 53](#).
- Ensure that the *tyk* service is in a healthy state.

### Procedure

---

**Step 1** From the main menu, choose **Administration > Certificate Management** and click .

**Step 2** Enter a unique name for the certificate.

**Step 3** From the **Certificate Role** drop-down menu, select the purpose for which the certificate is to be used. For more information, see [Certificate Types and Usage, on page 322](#).

**Note**

You can select available destinations (Kafka/gRPC) while adding or updating an **External Destination** certificate.

**Step 4** Click **Browse**, and navigate to the certificate trustchain.

**Step 5** In the case of an **External Destination** certificate, you must select one or more destinations and provide the CA certificate trustchain, intermediate certificate, and intermediate key. The passphrase field is optional and is used to create the intermediate key (if applicable).

**Step 6** Click **Save**.

**Note**

Once uploaded, the Crosswork Cert manager accepts, validates, and generates the server certificate. Upon successful validation, an alarm ("Crosswork Web Server Restart") indicates that the certificate is about to be applied. The Certificate Management UI then logs out automatically and applies the certificate to the Web Gateway. The new certificate can be checked by clicking the lock <Not Secure>/<secure> icon next to the `https://<crosswork_ip>:30603`.

---

## Edit Certificates

Crosswork Network Controller allows you to update web certificates by importing an intermediate Certificate Authority (CA) certificate. You can edit certificates to add or remove connection destinations, and upload or replace expired or misconfigured certificates. This applies to user-provided certificates, ZTP certificates, and web certificates. However, system certificates provided by Cisco Crosswork cannot be modified and will not be available for selection.

Crosswork Network Controller also allows you to configure the client authentication for web certificates. Client authentication offers an alternative method for setting up user authentication in Crosswork, requiring

both the client and server to present digital certificates to verify their identities. Enabling this feature can provide a more seamless login experience for users.

You can also “remove” a certificate by following this procedure to replace the certificate or by disabling security (disable **Enable Secure Communication** option) for any assigned destinations (see [Add or Edit a Data Destination, on page 53](#)). Permanently deleting a certificate from the Cisco Crosswork system is not supported.

### Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- This process requires the Crosswork server to be restarted, which will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

### Procedure

**Step 1** From the main menu, choose **Administration > Certificate Management** to view the **Certificate Management** window.

**Step 2** To update a certificate:

- a) Click  on the certificate that you want to modify, and select **Update Certificate**.
- b) Fill in the appropriate values for the fields based on the certificate you wish to update. Click the  icon next to the field for more information.

*Table 28: Update Certificate*

Certificate Type	Mandatory Fields
Crosswork-ZTP-Device-SUDI	<ul style="list-style-type: none"><li>• <b>Cisco M2 CA certificate:</b> You can upload a trusted CA certificate in PEM format for secure communication. The file should have either a .PEM or .CRT extension.</li></ul>
Crosswork-ZTP-Owner	<ul style="list-style-type: none"><li>• <b>Pin domain CA certificate:</b> You can upload a trusted CA certificate in PEM format for secure communication. The file should have either a .PEM or .CRT extension.</li><li>• <b>Owner certificate:</b> You can upload certificates issued by a trusted CA for end-entity server or leaf certificates. Ensure the file has a .PEM or .CRT extension.</li><li>• <b>Owner key:</b> The key used by the intermediate certificate to generate Crosswork leaf certificates. The file should have a .KEY, .PEM, or .CRT extension.</li></ul>

Certificate Type	Mandatory Fields
Crosswork-Web-Cert	<ul style="list-style-type: none"> <li>• <b>Crosswork Web CA:</b> Trustchain file (in .PEM format) containing the root CA certificate and zero or more intermediate certificates.</li> <li>• <b>Crosswork Web Intermediate:</b> An intermediate CA certificate signed with the root CA certificate.</li> <li>• <b>Crosswork Web Intermediate Key:</b> The key associated with the intermediate CA certificate.</li> </ul>

Upon successful validation, the Certificate Management UI logs out automatically and applies the certificate to the Web Gateway.

- Click **Save** to save the changes.

### Step 3

To enable the client certificate authentication of a web certificate:

- Click **[...]** on the Crosswork web certificate that you want to modify, and select **Configure Client Certificate Authentication**.

The **Configure Client Authentication** window is displayed.

- Click the **Enable** checkbox.

The **Certificate schema** and **OCSP** settings are displayed.

The **OCSP** settings are enabled by default, but you can disable it if desired. If enabled, you can check the certificate revocation status using the Online Certificate Status Protocol (OCSP).

- Choose the **Certificate schema** value.

- **Automatic:** Searches for the user principal name (UPN) in the alternate subject name area. If a UPN is not found, the system will use the common name value. This is the default selection.
- **Manual:** Searches for the username in the subject area based on the user identity source and the specified regular expression.

- (Optional) Choose the **OCSP** value:

- **Automatic:** Extracts the responder URL from the certificate and uses it to perform OCSP validation.
- **Manual:** You must provide the OCSP responder URL.

- Click **Save** to save the changes.

### Step 4

To update certificate and configure client authentication in a single step:

- Click **[...]** on the Crosswork web certificate that you want to modify, and select **Update Certificate & Config. Client Cert. Authentication**.

The **Update Certificate and Configure Client Authentication** window is displayed.

#### Note

Choosing the combined option to update the certificate and configure client authentication minimizes downtime during the Crosswork server restart, as it occurs only once instead of twice if these actions are performed separately.

- Provide the data as per the instructions in step 2 and step 3.

- c) Click **Save** to save the changes.
- 

## Download Certificates

To export certificates, do the following:

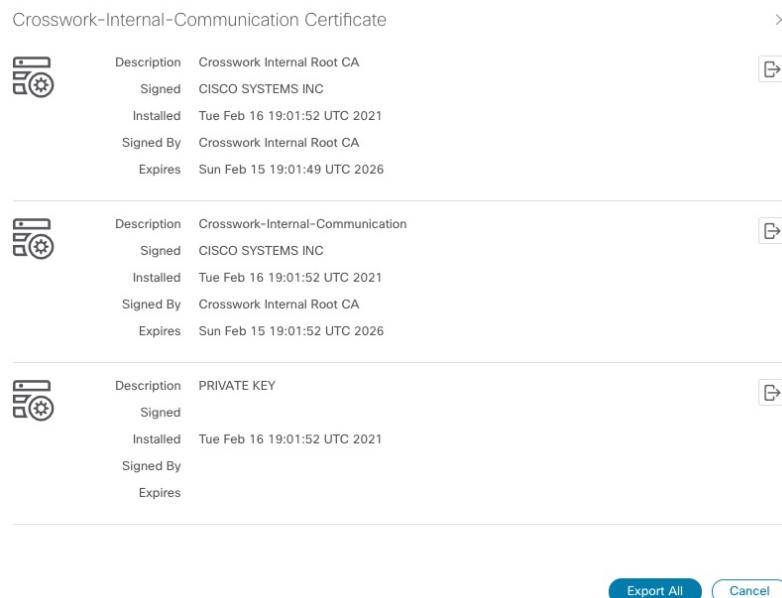
### Procedure

---

**Step 1** From the main menu, choose **Administration > Certificate Management**.

**Step 2** Click  for the certificate you want to download.

**Figure 122: Export Certificates**



Category	Description	Signed	Installed	Signed By	Expires
Crosswork-Internal-Communication Certificate	Crosswork Internal Root CA	CISCO SYSTEMS INC	Tue Feb 16 19:01:52 UTC 2021	Crosswork Internal Root CA	Sun Feb 15 19:01:49 UTC 2026
	Crosswork-Internal-Communication	CISCO SYSTEMS INC	Tue Feb 16 19:01:52 UTC 2021	Crosswork Internal Root CA	Sun Feb 15 19:01:52 UTC 2026
	PRIVATE KEY		Tue Feb 16 19:01:52 UTC 2021		

**Step 3** To separately download the root certificate, intermediate certificate, and the private key, click . To download the certificates and private key all at once, click **Export All**.

---

## Renew Certificates

Certificates are valid for 1 year before they expire. The below procedure needs to be executed sequentially on each node (hybrid and worker) in the cluster. After renewing the certificates in one node, ensure that the pods are healthy before proceeding to the next node.



**Note** When renewing certificates before expiry, it is recommended to perform this activity during a maintenance window as the cluster is in an operational state.

To renew a certificate, perform the following:

## Procedure

**Step 1** Create a backup of your Crosswork Network Controller.

**Step 2** **Renew certificate in a Hybrid node:**

- In the node, run command to move to root user.

```
sudo -i
```

You will be prompted to enter your password. Enter the `cw-admin` user password.

- Verify if the certificate date has expired.

```
kubeadm certs check-expiration
```

The following image is a sample of the output:

*Figure 123: Certificate expiration sample output*

```
root@10-90-147-67-hybrid:~# kubeadm alpha certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -oyaml'

CERTIFICATE          EXPIRES          RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf           May 16, 2023 21:31 UTC  343d           ca                  no
apiserver            May 16, 2023 21:31 UTC  343d           ca                  no
apiserver-etcd-client  May 16, 2023 21:31 UTC  343d           etcd-ca            no
apiserver-kubelet-client  May 16, 2023 21:31 UTC  343d           ca                  no
controller-manager.conf  May 16, 2023 21:31 UTC  343d           ca                  no
etcd-healthcheck-client  May 16, 2023 21:31 UTC  343d           etcd-ca            no
etcd-peer             May 16, 2023 21:31 UTC  343d           etcd-ca            no
etcd-server            May 16, 2023 21:31 UTC  343d           etcd-ca            no
front-proxy-client     May 16, 2023 21:31 UTC  343d           front-proxy-ca      no
scheduler.conf         May 16, 2023 21:31 UTC  343d           ca                  no

CERTIFICATE AUTHORITY  EXPIRES          RESIDUAL TIME   EXTERNALLY MANAGED
ca                  May 13, 2032 21:31 UTC  9y            no
etcd-ca              May 13, 2032 21:31 UTC  9y            no
front-proxy-ca       May 13, 2032 21:31 UTC  9y            no
root@10-90-147-67-hybrid:~#
```

- Make a backup of the certificates and conf files.

```
mkdir $HOME/Old-K8-Certs
mkdir $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/pki/*.* $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/*.conf $HOME/Old-K8-Certs
~#
```

- Run command to renew the certificate.

```
kubeadm certs renew all
```

- Repeat step 1(b) to verify the creation of new certificates.
- Run command to restart the kubelet.

```
systemctl stop kubelet
```

### Note

The restart occurs on all the nodes and the refreshed certificates do not take effect until the `kubelet` and `kube-apiserver` are restarted. It is recommended to stop any operations from the applications from running when the restart occurs.

After stopping `kubelet`, find the following processes (using `ps -eaf | grep <process name>`):

```
kube-apiserver
controller-manager
kube-scheduler
```

Kill them (using `kill -9 <pid>`). After killing the above processes, perform the following to restart the `kubelet`:

```
systemctl daemon-reload
systemctl start kubelet
```

The node will first move to `degraded` state, and then to `down` state.

#### Note

The syslog may continue to show traffic even after the node has moved to `down` state.

```
10-90-147-67-hybrid kernel: [1897091.695393] 11 header: 00000000: ff ff ff ff ff ff fa 51 56 a2
9c 7c 08 0
10-90-147-67-hybrid kernel: [1897091.695414] IPv4: martian source 169.254.1.1 from 10.244.215.17,
on dev calieff0340c649
10-90-147-67-hybrid kernel: [1897091.695416] 11 header: 00000000: ff ff ff ff ff 72 e8 75 10
bb 64 08 06
```

#### Important

Check the status of the `kubelet` using the command `systemctl status kubelet`.

- If the status shows `running`, repeat steps 1(a) to 1(f) on the other two nodes. Check the status by executing steps 1(g) and 1(h).
- If the status is not `running`, execute step 1(i) on all three nodes. Repeat steps 1(a) to 1(f) and step 1(i) on the other two nodes. Check the status by executing steps 1(g) and 1(h).

- g) Verify if all the pods are healthy and running.

```
kubectl get nodes
kubectl get pods -A -o wide
```

It also verifies the running pods on the hybrid node that you have restarted.

- h) Verify if the certificate has been renewed.  
i) If the issue is still seen, change the conf file.

```
kubeadm config print init-defaults > init.config
kubeadm kubeconfig user --org system:nodes --client-name system:node:$ (hostname) --config
init.config > k.conf
vi k.conf - Update line number 5 with correct VIP address of your cluster (you will see an value
like https://1.2.3.4:664) and save the file.
cp k.conf /etc/kubernetes/kubelet.conf
```

Check the status of the `kubelet` using the command `systemctl status kubelet`.

Repeat the above steps for each node in your cluster.

### Step 3    Renew certificate in a Worker node:

- a) In the worker node, run command to move to root user.

```
sudo -i
```

You will be prompted to enter your password. Enter the `cw-admin` user password.

- b) Make a backup of the `/etc/kubernetes/kubelet.conf` and `/var/lib/kubelet/pki/kubelet-client*` files, and delete them from the worker node.
- c) Log in to one of the hybrid nodes (where you generated `init.config`) and generate `kubelet.conf` for the worker nodes.

```
kubeadm kubeconfig user --org system:nodes --client-name system:node:$NODE > kubelet.conf
```

Example:

```
sudo kubeadm kubeconfig user --org system:nodes --client-name
system:node:10-10-0-17-worker.sitcw.com > /tmp/kubelet17.conf
```

```
vi /tmp/kubelet17.conf - Update line number 5 with correct VIP address of your cluster (you will
see an entry like https://1.2.3.4:664) and save the file.
```

Repeat the same for other worker nodes.

- d) Move these files from the hybrid node to the respective worker node under `/tmp/kubelet17.conf`
- e) Copy from `/tmp` to Kubernetes.

Example: `cp /tmp/kubelet17.conf /etc/kubernetes/kubelet.conf`

- f) Restart the `kubelet` (`systemctl restart kubelet`) on the failed node and wait for `/var/lib/kubelet/pki/kubelet-client-current.pem` to be recreated.
- g) Execute `kubectl get nodes` on the hybrid node to ensure the node becomes `Ready`.

#### Step 4

(Optional) **Recover cluster:** If multiple pods are stuck in `ContainerCreating` state after renewing the Kubernetes certificate, please run the following commands on any hybrid node.

```
kubectl delete pods -n kube-system -l k8s-app=calico-node
```

Wait for the `calico-node` pods to come up in the `kube-system` namespace.

## Manage Licenses

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central ([software.cisco.com](http://software.cisco.com)). A **Cisco Smart Account** provides the repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage and track Cisco purchases. The **Cisco Smart Software Manager (CSSM)** enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart

Software Manager, you may create and manage multiple virtual accounts within your Smart Account to manage licenses. For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](http://cisco.com/go/licensingguide).

From the main menu, select **Administration > Smart Licensing Registration** to display the **Smart License** tab under the **Application Management** window. In the **Smart License** tab, you can register your Cisco Crosswork application, edit the transport settings, renew the license, and de-register your application.



**Important** All unmanaged devices are counted towards the device limits associated with Crosswork licenses. To prevent this, delete your unmanaged devices in the Crosswork UI.

### Tracked Node Counts for Crosswork Optimization Engine

For Crosswork Optimization Engine, the node count is reported in the following cases:

- After initial installation and startup of the following pods: Crosswork UI, RESTCONF, or any of the feature packs (Local Congestion Mitigation, Bandwidth on Demand, or Circuit Style Manager).
- Manually restarting the pods.
- Daily at a fixed time (1:00 AM).

## Configure Transport Settings

You can configure the transport settings to decide how 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.

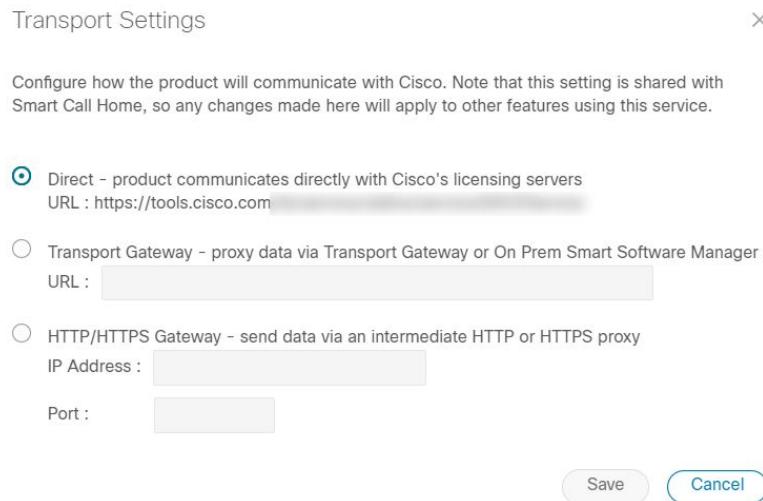


**Note** Transport Settings cannot be changed while the Crosswork product is in Registered mode. You have to de-register to change them.

### Procedure

- Step 1** In the **Smart License** tab, the Transport Settings display the current transport mode selected. To modify, click **View/Edit**. The **Transport Settings** dialog box is displayed.

Figure 124: Transport Settings Dialog Box



- Step 2** Select the relevant transport mode and make relevant entries in the fields provided.  
**Step 3** Click **Save**.
- 

## Register Cisco Crosswork Application via Token

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.



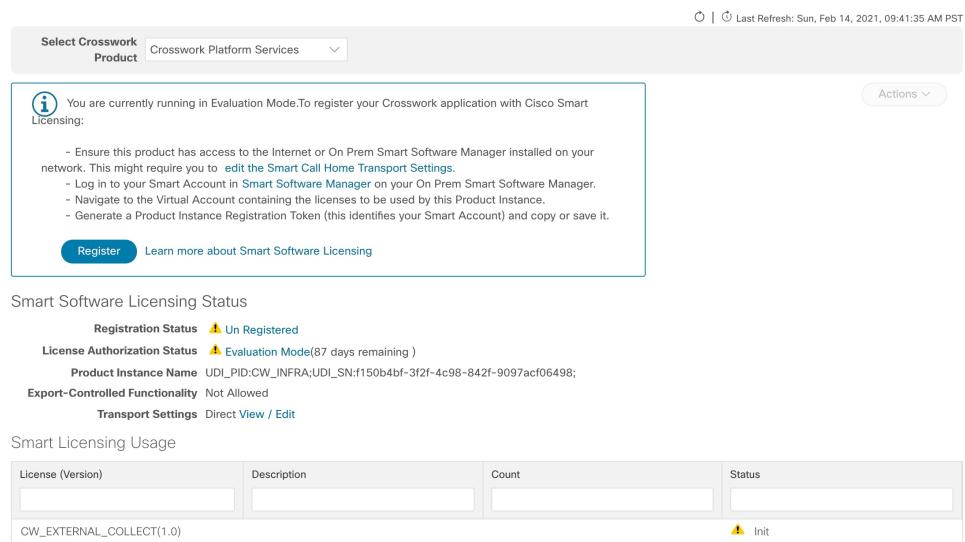
**Note** For information on generating the registration token, please refer to the support resources provided in the [Smart Software Manager](#) webpage.

---

### Procedure

---

- Step 1** From the main menu, select **Administration > Smart Licenses** to display the **Smart License** tab.  
 The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

**Figure 125: Smart Software Licensing Unregistered Example**

## Step 2 In the Smart Software Licensing dialog box, click Register.

The Smart Software Licensing Product Registration dialog box is displayed.

**Figure 126: Smart Software Licensing Product Registration Dialog Box**

### Smart Software Licensing Product Registration

Register via Token  Register via Reserved License

To register the product for Smart Software Licensing:

- Ensure you have connectivity to the URL specified in your Smart Call Home settings. By default, this will require internet access. See the online help registering to a On Prem Smart Software Manager.
- Paste the Product Instance Registration Token you generated from [Smart Software Manager](#) or your On Prem Smart Software Manager.

**i** After successful registration, page may need to be refreshed to see the updated status.

#### Product Instance Registration Token

Re-register this product instance if it is already registered

[Cancel](#) [Register](#)

**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](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** check box.

**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 registration error (for example, "Communication send error" or "Invalid response from licensing cloud"), please wait for some time and retry the registration. If the error persists after multiple attempts, please contact the Cisco Customer Experience team.
- 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.

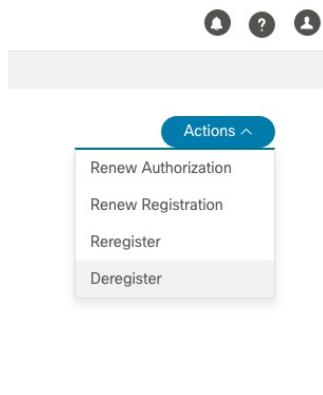


**Note**

In the case of the Cisco Optimization Engine smart license, the node count is tracked during the initial onboarding of devices and during the registration and entitlement of the license. Any further changes to node count are synced with the Smart Licensing server after every 24 hours GMT. If you prefer not to wait, you can reregister the application license to update the node count immediately.

## Procedure

**Step 1** In the **Smart License** tab, 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 342](#).

- Step 2** The selected action is executed successfully.
- 

## Register Cisco Crosswork Applications via Offline Reservation

Cisco Crosswork applications that use Smart Licensing share usage information to CSSM at regular intervals. If you do not want to connect with CSSM regularly, Cisco Smart Licensing provides an option of offline reservation.

There are two modes of offline reservation:

- Specific License Reservation (SLR)—In this mode, you can select the number of licenses of each entitlement that has to be reserved.
- Permanent License Reservation (PLR)—In this mode, there will be a single license that will make the entire product In Compliance.

### Before you begin

Confirm that you have a Smart Account. If not, go to [Smart Account Request](#) and follow the instructions on the website.

### Procedure

---

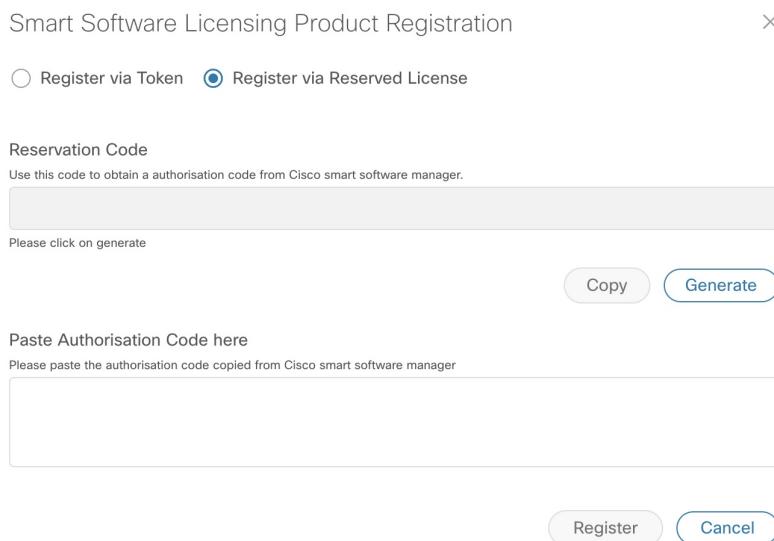
- Step 1** From the main menu, select **Administration > Smart Licensing Registration** to display the **Smart License** tab.

**Step 2** Click **Register**.

The Smart Software Licensing Product Registration dialog box is displayed.

**Step 3** Select the **Register via Reserved License** option.

**Figure 127: Smart Software Licensing Product Registration Dialog Box**



**Step 4** Click the **Generate** button under the Reservation Code section. Your Reservation Request Code is generated and populated in the text field. Copy this code using **Copy** button.

**Step 5** Go to the [Cisco Software Central](#) website and select the appropriate virtual account.

**Step 6** Click the **Licenses** tab, then click **License Reservation**. Paste the Reservation Request Code that you generated in Step 4 and click **Next**.

**Step 7** In the Select Licenses page, select the **Reserve a specific license** radio button, reserve the necessary licenses from the list, and click **Next**.

**Step 8** In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using the **Copy to Clipboard** button.

**Step 9** Navigate back to the Smart Software Licensing Product Registration page on the Cisco Crosswork UI. Paste the Authorization Code in the text field under the **Paste Authorisation Code here** section.

**Step 10** Click **Register**. It may take a few minutes to process the registration.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

## Update Offline Reservation

Use the **Update Reservation** option to update the license counts reserved via offline reservation.

## Procedure

---

- Step 1** From the main menu, select **Administration > Smart Licensing Registration** to display the **Smart License** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).
- Step 2** Go to the [Cisco Software Central](#) website and select the appropriate virtual account.
- Step 3** Click the name of the product instance that matches your Product Instance Name.
- Step 4** Click the **Actions** drop-down button and choose **Update Reservation**.
- Step 5** In the Select Licenses page, select the **Reserve a specific license** radio button, update the count of the necessary licenses from the list and click **Next**.
- Step 6** In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using **Copy to Clipboard** button.
- Step 7** Navigate back to the Smart License page on the Cisco Crosswork UI. Click the **Actions** drop-down button and choose **Update Reservation**. Paste the Authorization Code that you generated in Step 6 and click **Update**.  
A Confirmation Code is generated. You can find this under the Smart Software Licensing Status section. Copy this code.
- Step 8** Navigate back to the [Cisco Software Central](#) website. Click the required product instance name.
- Step 9** Click the **Actions** drop-down button and choose **Enter Confirmation Code**.
- Step 10** Enter/paste the Reservation Confirmation Code that was generated in Step 7 and click **OK**.  
The license count will be updated on the Smart License page of the Cisco Crosswork UI.
- 

## Disable Offline Reservation

Use the **Disable Reservation** option to release the reserved licenses. Once the licenses are released, the application will be moved to **Evaluation** mode (if evaluation period is available), or **Evaluation Expired** mode. For more information, see [License Authorization Statuses, on page 342](#).

## Procedure

---

- Step 1** From the main menu, select **Administration > Smart Licensing Registration** to display the **Smart License** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).
- Step 2** Click the **Actions** drop-down button and choose **Disable Reservation**.
- Step 3** In the Confirm Disable Reservation window, click **Confirm**.  
A Release Code (Reservation Return Code) is generated. Copy this code using the **Copy** button.
- Step 4** Navigate to the [Cisco Software Central](#) website and select the appropriate virtual account.
- Step 5** Click the name of the product instance that matches your Product Instance Name.
- Step 6** Click the **Actions** drop-down button and choose **Remove**.
- Step 7** In the Remove Reservation pop-up, paste the Reservation Return Code that you generated in Step 3 and click **Remove Reservation**.

The Registration Status will be updated to Un Registered state on the Smart License page of the Cisco Crosswork UI.

## License Authorization Statuses

Based on the registration status of your Cisco Crosswork application, you can see the following License Authorization Statuses.

**Table 29: License Authorization Statuses**

Registration Status	License Authorization Status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which the licensed features of the application can be freely used. This state is initiated when you use the application for the first time.
	Evaluation Expired	The application has not been successfully registered at the end of the evaluation period. During this state, the application features are disabled, and you must register to continue using the application.
	Registered Expired	The application is unable to contact the CSSM before the expiration of Identity Certificates and has returned to the unregistered state. The application resumes the remaining evaluation period, if available. At this stage, new registration ID token is required to reregister the application.
Registered	Authorized (In Compliance)	The application has been fully authorized to use the reserved licensed features. The authorization is automatically renewed every 30 days.
	Out of Compliance	The associated Virtual Account does not have enough licenses to reserve for the application's current feature use. You must renew the entitlement/usage limit registered with the token to continue using the application.
	Authorization Expired	The application is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

## Authorization Status Response

This section explains the actions or message enforced by Crosswork in case of "Out of Compliance" or "Evaluation Expired" status.

The behavior is covered for Right-to-Use (RTU) and Right-to-Manage (RTM) licenses.

**Table 30: Out of compliance status action for registered systems**

Registration Status	License Authorization Status	Application or Component	Enforced Action or Message
Registered	Out of Compliance	Crosswork Optimization Engine	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Active Topology	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Service Health	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Change Automation	RTU: Playbook execution is not allowed. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Health Insights	RTU: Health Insights usage is not allowed. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Zero Touch Provisioning	RTM: No action taken (in case of normal token-based registration).
		Element Management Functions	No action taken.

Table 31: Evaluation expired status action for unregistered systems

Registration Status	License Authorization Status	Application or Component	Enforced Action or Message
Unregistered	Evaluation Expired	Crosswork Optimization Engine	Only READ operations are allowed. Create, update, and delete operations are restricted.
		Crosswork Active Topology	No action taken. No impact on provisioning UI (NSO) workflows.
		Crosswork Service Health	Monitoring cannot be enabled or resumed. An error message ("License evaluation expired or reservation exceeded, Service Health functionality disabled") is displayed.
		Crosswork Change Automation	RTU: Playbook execution is not allowed. A major alarm is raised.
		Crosswork Health Insights	RTU: Health Insights usage is not allowed. A message is logged with license state indicating that "License is expired". RTM: Critical alarm is raised.
		Crosswork Zero Touch Provisioning	RTM: ZTP API operations are not allowed. An error message is displayed ("Your License Evaluation Period has expired or there are no Reserved Licenses").
		Crosswork External Collection	RTM: Collection Job creation, Template Collection Job creation, and Bulk template collection operation requests are rejected.
		Element Management Functions	No action taken.

## 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 347](#)).

### Procedure

- 
- Step 1** From the main menu, select **Administration > Users and Roles > Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

**Step 2** To add a new user:

- a) Click  and enter the required user details.

When you are configuring Device Access Groups for your users, select the **Device Access Group** listed in the right pane to assign it to the new user you are creating.

**Note**

1. By default users associated with ALL-ACCESS Device Access Group are provided access to ALL devices.
2. You must associate at least one Device Access Group to a user.

- b) Click **Save**.

**Step 3** To edit a user:

- a) Click the checkbox next to the User and click .
- b) After making changes, click **Save**.

**Step 4** To delete a user:

- a) Click the checkbox next to the User and click .
- b) In the **Confirm Deletion** window, click **Delete**.

**Step 5** To view the audit log for a user:

- a) Click the  icon under the **Actions** column, and select **Audit Log**.

The **Audit Log** window is displayed for the selected user name. For more information on the Audit Logs, see [View Audit Log, on page 416](#).

**Step 6** (Optional) To view NACM rules for a user:

- a) Click the  icon under the **Actions** column, and select **Generate NACM Rules**.

The **NACM Rules** window is displayed for the selected user name.

If you have an NSO service configured on your Crosswork Network Controller, you can generate NACM rules by

clicking the  icon under the **Actions** column for a user and selecting **Generate NACM Rules**. This rule list for the device level NACM control will integrate Crosswork Network Controller with the NSO workflow. Note that for every unique combination of Device Access Group that is associated with a user, there is—

- A NACM group associated with the user.
- A corresponding NACM rule list associated with the user.

The rule will allow access to devices in selected Device Access Groups and deny access to other devices. You can copy the XML rules file and add it in your NSO NACM Rule configuration setup. The options available under the NSO Actions tab, located in Device **Management > Network Devices**, will also be restricted based on the Device Access Groups permissions of the user.

You also view the Crosswork Audit log and the NSO commit logs to track and verify the activities of users using the NACM rules, ensuring traceability.

## Administrative Users Created During Installation

During installation, Crosswork creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **cw-admin**, and the default password **admin**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Crosswork server.
2. The **Cisco Crosswork administrator**, with the username **admin** and the default password **admin**. Product administrators use this ID to log in to and configure the user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used. You can also change the Cisco Crosswork administrator password using the following methods:

- Log in as the admin user and edit the admin user password .
- Enter the following command: `admin(config) # username admin <password>`

## User Roles, Functional Categories and Permissions

The **Roles** window lets users with the appropriate privileges define custom user roles. As with the default *admin* role, a custom user role consists of:

- A unique name, such as “Operator” or “admin”.
- One or more selected, named functional categories, which control whether or not a user with that role has access to the APIs needed to perform specific Cisco Crosswork functions controlled by that API.
- One or more selected permissions, which control the scope of what a user with that role can do in the functional category.

For a user role to have access to a functional category, that category and its underlying API must show as selected on the **Roles** page for that role. If the user role shows a functional category as unselected, then users with this role assigned will have no access to that functional area at all.

Some functional categories group multiple APIs under one category name. For example: The “AAA” category controls access to the Password Change, Remote Authentication Servers Integration, and Users and Role Management APIs. With this type of category, you can deny access to some of the APIs by leaving them unselected, while providing access to other APIs under the category by selecting them . For example: If you want to create an “Operator” role who is able to change his own password, but not see or change the settings for your installation’s integration with remote AAA servers, or create new users and roles, you would select the “AAA” category name, but uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” checkboxes.

For each role with a selected category, the **Roles** page also lets you define permissions to each underlying functional API:

- **Read** permission lets the user see and interact with the objects controlled by that API, but not change or delete them.
- **Write** permission lets the user see and change the objects controlled by that API, but not delete them.
- **Delete** permission gives the user role delete privileges over the objects controlled by that API. It is useful to remember that delete permission does not override basic limitations set by the Crosswork platform and its 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 32: Sample custom user roles**

Role	Description	Categories/API	Privileges
Operator	Active network manager, triggers Playbooks in response to KPI alerts	All	Read, Write
Monitor	Monitors alerts only	Health Insights, Inventory, Topology	Read only
API Integrator	All	All	All



**Note** Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions. Using Zero Touch Provisioning features requires access to all ZTP APIs.

## Create User Roles

### Procedure

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

**Clone User Roles**

The **Roles** window has a **Roles** table on the left side and a corresponding **Global API Permissions** tab on the right side which shows the grouping of user permissions for the selected role.

**Step 2** On the **Roles** table, click  to display a new role entry in the table.

**Step 3** Enter a unique name for the new role.

**Step 4** To define the user role's privilege settings, select the **Global API Permissions** tab and perform the following:

- Check the check box for every API that users with this role can access. The APIs are grouped logically based their corresponding application.
- 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 349](#)).

---

## 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 344](#)). Later, you can edit the roles themselves to give users the privileges you want (see [Edit User Roles, on page 349](#)).

### Procedure

---

**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:

- Check the check box for every API that the cloned role can access.
- For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.

**Step 6** Click **Save** to create the newly cloned role.

## Edit User Roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

### Procedure

- 
- Step 1** From the main menu, choose **Administration > Users and Roles > Roles** tab.
- Step 2** Click and select on an existing role from the left side table. The **Global API Permissions** tab on the right side displays the permission settings for the selected role.
- Step 3** Define the role's settings:
- Check the check box for every API that the role can access.
  - For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.
- Step 4** When you are finished, click **Save**.
- 

## Delete User Roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

### Procedure

- 
- Step 1** From the main menu, choose **Administration > Users and Roles > Roles** tab.
- Step 2** Click on the role you want to delete.
- Step 3** Click .
- Step 4** Click **Delete** to confirm that you want to delete the user role.
- 

## Global API Permissions

The **Roles** window lets users with the appropriate privileges define custom user roles.

The following table is an overview of the various **Global API Permissions** in Cisco Crosswork:

Table 33: Global API Permission Categories

Category	Global API Permissions	Description
AAA	Password Change APIs	Provides permission to manage passwords. The READ and WRITE permissions are automatically enabled by default. The DELETE permission is not applicable to the password change operation (You cannot delete a password, you can only change it.)
	Remote Authentication Servers Integration APIs	Provides permission to manage remote authentication server configurations in Crosswork. You must have READ permission to view/read configuration, and WRITE permission to add/update the configuration of any external authentication server (e.g. LDAP, TACACS) into Crosswork. The Delete permissions are not applicable for these APIs.
	Users and Roles Management APIs	Provides permission to manage users, roles, sessions, and password policies. Supported operations include "Create new user/role", "Update user/role", "Delete a user/role", "Update task details for a user/role", "Session management (Idle-timeout, max session..)", "update password policy", "get password tooltip help text", "get active sessions", etc. The READ permission allows you to view the content, the WRITE permission allows you to create and update, and the DELETE permission allows you to delete a user or role.
Alarms  <b>Attention</b> The Alarm APIs are deprecated in the Crosswork 6.0 release.	Alarms APIs	Allows you to manage alarms. The READ permission allows you to get events/alarms according to request criteria, get the list of Syslog destinations, and get the list of trap destinations. The WRITE permission allows you to set a response for when an alarm is raised or acknowledged, create/raise an event, update the event info manifest, and add notes to alarms. The DELETE permission allows you to delete REST destinations, Syslog destinations and trap destinations.

Category	Global API Permissions	Description
Automated Assurance DSS Instance	Data Store Service Administrator Settings	Allows Administrators to view Datastore storage info (READ permission) and run diagnostic tests for external storage (WRITE permission).
	Data Store Service API	<p>Allows you to use external storage for longer retention, and to manage external datastore used by Service Assurance for archiving service metrics data.</p> <p>The READ permission allows you to get storage provider information, check storage stats, etc.</p> <p>The WRITE permission allows you to sync the local CW datastore with the external storage and run diagnostics.</p> <p>The DELETE permission allows you to delete an external storage provider.</p>

Category	Global API Permissions	Description
Crosswork Network Controller	CAT FP Deployment Manager APIs	<p>Allows you to manage function pack upload and deployment.</p> <p>The READ permission enables you to get the list of packages, files, and deployment information.</p> <p>The WRITE permission allows you to upload/deploy/un-deploy a package/function pack/file.</p> <p>The DELETE permission is not applicable for these APIs.</p>
	CAT Inventory RESTCONF APIs	<p>North Bound Interface (NBI) RESTCONF interface for the CAT services inventory data (from CAT to external consumers).</p> <p>The READ permission allows you to fetch the services information from CAT, while the WRITE permission allows you to invoke operations APIs to retrieve the service information from CAT. The DELETE permission is not applicable for these APIs.</p>
	CAT ISTP REST APIs	<p>System use only.</p> <p>The READ/WRITE permissions are mandatory for CAT UI/ISTP to function. The DELETE permission is not applicable for these APIs.</p>
	CAT Service Overlay APIs	<p>Primarily used to investigate issues in the overlay. Only READ permission is applicable.</p>
	CAT UI APIs	<p>Mandatory APIs that enable CAT UI to fetch all NSO services and resources.</p> <p>The READ permission allows you to fetch and display all service information, while WRITE permission allows you to commit service assurance information. The DELETE permission is not applicable for these APIs.</p>
	NSO Connector APIs	<p>Allows you to perform services resync, full-resync, change log-level and return service HA status.</p> <p>The READ permission allows you to check the service status, while WRITE permission is required for all other operations. The DELETE permission is not applicable for these APIs.</p>
	OAM Service APIs	Not Applicable

Category	Global API Permissions	Description
Change Automation	Administration APIs	<p>Provides administrative control to manage job scheduling, manage override credentials, and configuration of user roles for playbook executions.</p> <p>The READ permission allows you to check the status and fetch the information, while the WRITE permission allows you to make changes. The DELETE permission is not applicable for these APIs.</p>
	Application APIs	<p>Allows you to manage the Change Automation tasks (for example, schedule playbook executions, execute playbooks, update playbook jobs, check playbook executions status, check playbook job-set details, list supported YANG modules, etc.)</p> <p>The READ permission allows you to view the applicable information (for example, check the job status, fetch job details, etc.), while the WRITE permission is required for playbook job scheduling/execution. The DELETE permission is not applicable for these APIs.</p>
	Playbook APIs	<p>Allows you to manage playbooks.</p> <p>The READ permission allows you to retrieve playbooks, params, and policy specs.</p> <p>The WRITE permission allows you to import/export, and generate playbooks.</p> <p>The DELETE permission enables you to delete playbooks.</p>
	Play APIs	<p>Allows you to manage plays.</p> <p>The READ permission allows you to fetch or view plays, while the WRITE permission allows you to create, update or import a play. The DELETE permission allows you to delete a play.</p>
Collection Infra	Collection APIs	<p>Permissions for APIs to manage collection jobs.</p> <p>Based on the READ/WRITE/DELETE permissions, you can view collection jobs, create/update new collection jobs (external), or delete existing collection jobs. System collection jobs (data collection setup internally for Crosswork consumption) cannot be modified irrespective of these permissions (permitted for Administrators only), but users with the READ permission will be able to view the details of all collection jobs including system collection jobs.</p> <p>For most users, READ-only permissions would be enough as it enables them to view Collection jobs detail (request and status) and actual data collection status/metrics per device/sensor path level.</p>
	Data Gateway Manager APIs	<p>Permissions to perform CRUD operations on Destinations, Data Gateways, Custom Packages, etc.</p> <p>The READ permission allows you to view the data, while the WRITE permission allows you to add/update/delete the data.</p>

Category	Global API Permissions	Description
Crosswork Optimization Engine	OPTIMA Analytics API	<p>Allows you to manage analytics in Crosswork Optimization Engine.</p> <p>The READ permission allows you to view/export historical data, while WRITE permission enables you to change the Traffic Engineering Dashboard settings.</p>
	Optimization Engine UI APIs	<p>Allows you to manage SR policies, RSVP tunnels, LCM, BWoPT, BWoD, Traffic Engineering settings, and Preview policies.</p> <p>The READ permission allows you to view deployed policies, settings, routes, LCM domain config/data, service overlay data, path queries, dashboard metrics, etc.</p> <p>The WRITE permission allows you to configure LCM, BWoD, BWoPT, deploy policies, preview Crosswork Optimization Engine-managed policies, etc.</p> <p>The DELETE permission allows you to delete SR policies, RSVP tunnels, remove affinity mapping, and delete LCM domains.</p>
Crosswork Optimization Engine v2	Optimization Engine RESTCONF API v2	<p>Allows you to customize the RESTCONF interface permissions in Crosswork Optimization Engine.</p> <p>The READ permission enables you to fetch L2 and L3 topology details, and Segment Routing Policy details.</p> <p>The WRITE permission allows you to fetch policy routes, provision/modify/delete/preview SR policies, and manage LCM configuration.</p> <p>The DELETE permission is not applicable for these APIs.</p>
Data Gateway Global Settings	Data Gateway Global Parameters API	<p>There are certain parameters in CDG, which can be changed globally across all CDGs in a Deployment.</p> <p>The READ permission allows you to view the data, while the WRITE permission is required to reset/update the data.</p>
	Data Gateway Global Resources Reset API	<p>Allows you to reset updates done to the Global Parameters.</p> <p>The READ permission allows you to view the data, while the WRITE permission resets the data.</p>
	Data Gateway Global Resources Update API	<p>Allows you to update the Global Parameters.</p> <p>The READ permission allows you to view the data, while the WRITE permission updates the data.</p>

Category	Global API Permissions	Description
Data Gateway Troubleshooting	Data Gateway Reboot API	<p>Reboots a Crosswork Data Gateway (CDG).</p> <p>The WRITE permission allows you to reboot the CDG.</p>
	Data Gateway Showtech API	<p>Generates and downloads showtech logs for a CDG</p> <p>The READ permission allows you to view showtech, while WRITE permission generates showtech.</p> <p>Write Permission allows u to generate showtech</p>
Health Insights	Health Insights APIs	<p>Allows you to manage Health Insights KPIs.</p> <p>The READ permission allows you to view all KPIs, KPI profiles, job details, alerts, etc.</p> <p>The WRITE permission allows you to create or update KPIs and KPI profiles, enable/disable KPI profiles, link KPIs to playbooks, etc.</p> <p>The DELETE permission allows you to delete custom KPIs and KPI profiles.</p>
ICON Server	ICON Server APIs	Allows you to update the collection setting for interface/IP data collection intended for topology and optimization use cases.

Category	Global API Permissions	Description
Inventory	Inventory APIs	<p>Allows you to manage inventory.</p> <p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>Fetch the list of nodes, the node credentials, and the count of nodes in the database.</li> <li>Retrieve the list of HA pools, DG enrollments, virtual data gateways, and inventory job information.</li> <li>Retrieve the list of policies, providers, and tags.</li> </ul> <p>The WRITE permission allows you to</p> <ul style="list-style-type: none"> <li>Update device mapping to virtual data gateway pool.</li> <li>Lock/unlock the requested nodes.</li> <li>Remove tag associations from nodes. Does not support partial un-assignment.</li> <li>Update input data to a set of devices.</li> <li>Set API endpoint for provider onboarding.</li> </ul> <p>The DELETE permission allows you to</p> <ul style="list-style-type: none"> <li>Perform bulk deletion of credential profiles and nodes.</li> <li>Upload CSV for delete operations.</li> <li>Delete HA pools, Data Gateway enrollments, and virtual data gateways.</li> <li>Delete policies, providers, and tags.</li> </ul>

Category	Global API Permissions	Description
Platform	Platform APIs	<p>The READ permission allows you to fetch the server status, cluster node information, application health status, collection job status, certificate information, backup and restore job status, etc.</p> <p>The WRITE permission allows you to</p> <ul style="list-style-type: none"> <li>• Enable/disable the xFTP server</li> <li>• Manage cluster (set the login banner, restart a microservice, etc.)</li> <li>• Rebalance cluster resources</li> <li>• Manage nodes (export cluster inventory, add VM, apply VM configuration, remove VM from a cluster, etc.)</li> <li>• Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, etc.)</li> <li>• Perform normal/data-only backup and restore operations.</li> <li>• Manage applications (activate, deactivate, uninstall, add package, etc.)</li> </ul> <p>The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.</p>
	Distributed Cache APIs	The READ permission allows you to fetch cache statistics for troubleshooting.
	Grouping APIs	<p>Grouping management and Topology groups selection tree.</p> <p>The READ permission allows you to view topology UI, while the WRITE permission allows you to create/update groups. The DELETE permission is needed to delete groups from the Grouping Management page.</p> <p><b>Note</b> When READ access is removed for Grouping APIs, in addition to being blocked out of the Grouping window, the users will also be unable to access the Traffic Engineering, VPN Services, and Topology Services windows.</p>
	View APIs	<p>Views Management in Topology.</p> <p>The READ permission allows you to see views, the WRITE permission allows you to create/update views, and the DELETE permission will enable delete capabilities.</p>

Category	Global API Permissions	Description
Topology	Geo APIs	<p>Provides geo service for offline maps.</p> <p>The READ permission allows you to use Geo Map in offline mode, the WRITE allows you to upload Geo Map files, and DELETE permission allows you to delete the map files in settings.</p>
	Topology APIs	<p>Allows you to manage topology pages, settings, or any other pages that uses the Topology visualization framework.</p> <p>The READ permission is mandatory for topology visualization. The WRITE permission enables you to update topology settings, and the DELETE permission allows you to delete a topological link if it goes down.</p>
Proxy	Crosswork Proxy APIs	<p>Permissions to manages Crosswork proxy APIs for NSO Restconf NBI.</p> <p>The READ permission allows all GET request for NSO REST conf NBI, the WRITE permission allows POST/PUT/PATCH operation, and the DELETE permission enables all delete APIs.</p>
SWIM	SWIM NB API	<p>Allows you to upload images to the SWIM repository, distribute them to devices and install them.</p> <p>The READ permission allows you to list all images from the SWIM repository, view image information from a device, and check the details of any SWIM job. The WRITE permission allows you to upload/distribute and perform all install-related operations. The DELETE permission allows you to delete copied images from a device.</p> <p>You require WRITE/DELETE permission to execute software install/uninstall playbooks in Change Automation.</p>

Category	Global API Permissions	Description
Service Health	Archiver APIs	<p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>• Check if Historical Data exists for a given service.</li> <li>• Get the Historical Timeline series for a given service.</li> <li>• Get a Service Graph for a selected timestamp of the service.</li> <li>• Get Service-Metric data</li> </ul> <p>The WRITE/DELETE permissions are not applicable for these APIs.</p>
	Assurance Graph Manager APIs	<p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>• Fetch details of a service.</li> <li>• Get the impacted list of services.</li> <li>• Retrieve the list of matching sub-services (transport or device only).</li> </ul> <p>The WRITE/DELETE permissions are not applicable for these APIs.</p>
	Heuristic Package Manager APIs	<p>Permissions for Heuristic package management and to manage plugins and config profiles for Service Assurance.</p> <p>The READ permission allows you to export heuristic packages, query for heuristic package details (Rules, Profiles, SubServices, Metrics, Plugins), and query for assurance options.</p> <p>The WRITE permission allows you to import heuristic packages and perform all create/update operations.</p> <p>The DELETE permission allows you to perform delete operations (for example, delete the RuleClass, MetricClass, etc.)</p>

Category	Global API Permissions	Description
Zero Touch Provisioning	CW Config Service APIs	<p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>• List all day-0 configuration files stored in the ZTP config repository.</li> <li>• Fetch count of day-0 configuration files stored in the ZTP config repository.</li> <li>• Download the day-0 configuration file from the ZTP config repository.</li> <li>• List all device family/device versions and device platforms based on information associated with day-0 config files stored in the CW ZTP repository.</li> </ul> <p>The WRITE permission allows you to</p> <ul style="list-style-type: none"> <li>• Upload the day-0 config file or script to the ZTP config repository.</li> <li>• List/update relevant metadata associated with specific day-0 config files stored in the ZTP config repository</li> </ul> <p>The DELETE permission allows you to delete config files and scripts uploaded in the ZTP config repository.</p>
CW Image Service APIs		<p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>• List all device image files stored in the ZTP image repository.</li> <li>• List all device platform/family names associated with image files stored in the CW ZTP repository.</li> <li>• Download the device image file by ID.</li> </ul> <p>The WRITE permission allows you to update relevant metadata associated with specific image files stored in the ZTP image repository.</p> <p>The DELETE permission allows you to delete image files uploaded in the ZTP image repository</p>
CW ZTP Service APIs		<p>Allows you to manage the ZTP devices and profiles - add/update/delete into Crosswork.</p> <p>The READ permission enables you to fetch ZTP devices, serial number/OVs, profiles, sample data CSV, list ZTP devices, profiles, and export ZTP devices and metadata.</p> <p>The WRITE permission allows you to add ZTP devices, serial numbers/OVs, profiles and add/update the ZTP device's attributes.</p> <p>The DELETE permission allows you to delete ZTP devices, profiles, serial numbers/ownership vouchers.</p>

Category	Global API Permissions	Description
CW-CLMS	Common Licensing Management Service (CLMS) APIs	Permissions for APIs to manage license registration in Crosswork. The READ permission enables you to view Smart Licensing settings, registration status, and license usage while the WRITE permission is required to change any Smart Licensing setting such as register, re-register, de-register, renew a license etc.

## Manage Active Sessions

As an administrator, you can monitor and manage the active sessions in the Cisco Crosswork UI, and perform the following actions:

- Terminate a user session
- View user audit log



**Attention**

- Non-admin users with permission to terminate can terminate their own sessions.
- Non-admin users with read-only permission can only collect the audit log for their sessions.
- Non-admin users without read permissions can't view the **Active Sessions** window.

### Procedure

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

The **Active Sessions** tab displays all the active sessions in the Cisco Crosswork with details such as user name, source IP, login time, and login method.

**Note**

The **Source IP** column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork. This option is available in the **Source IP** section of the **Administration > AAA > Settings** page.

**Step 2** To terminate a user session, click the  icon under the **Actions** column, and select **Terminate Session**. A dialog box is displayed to confirm your action. Select **Terminate** to terminate the session.

**Attention**

- You are recommended to use caution while terminating a session. A user whose session is terminated will not receive any prior warning and will lose any unsaved work.
- Any user whose session is terminated will see the following error message: "Your session has ended. Log into the system again to continue".

**Step 3** To view audit log for a user, click the  icon under the **Actions** column, and select **Audit Log**.

The **Audit Log** window is displayed for the selected user name. For more information on the Audit Logs, see [View Audit Log, on page 416](#).

## Manage Device Access Groups

Crosswork provides access-control based on a role assigned to a user and read/write/delete access that is associated with that role for specific set of APIs grouped by functional areas.

While this provides access-control that can be centralized, it is not extendible to device-level access control. To control or restrict device access for users, Device Access Groups can be used to logically group devices for user management. The Crosswork system-level task Device Access Groups-management can assist non-admin role users who are mapped to a task to create and manage Device Access Groups.

### APIs, Tasks and Device Access Groups- Know the Difference

Device Access Groups are not directly related with API access control and task-based access control. APIs control the **read/write/delete** access levels to the APIs, but do not control the UI access of a user. The access levels and permissions for APIs are defined and enforced at the API level, allowing you (as an administrator) to specify what actions can be performed by a user. Tasks, on the other hand, control access to certain functionalities by combining a set of APIs. When you enable a specific task, the corresponding APIs required for that task are also enabled.

Configuring Device Access Groups serve as an extra security layer to control access to specific devices or resources within Crosswork above and beyond the API and task-based access controls.

Administrators have full control over how they build user roles and permissions, including the ability to define Device Access Groups. If a user does not pass the API-based and/or task-based access control depending on the settings by an administrator, then the Device Access Group becomes irrelevant. Device Access Groups only come into play once a user has passed the initial access control levels set by an administrator and has been granted the necessary API and task permissions.

As administrators, you have the flexibility to define and configure the Device Access Groups according to your specific requirements. You can determine which devices a user is allowed to have WRITE permissions for provisioning based on the Device Access Group you configure. This provides an additional layer of control and customization for access management within Crosswork.

### How do Device Access Groups work?

When a user is associated with one or more Device Access Groups, they can make configuration changes and provision services on the devices that belong to those Device Access Groups. A Crosswork user with an administrator role or mapped Device Access Groups management task can:

- Create and manage access to device groups using the Device Access Groups management UI or REST APIs.
- Add/edit/update Device Access Groups and devices.

Based on task permissions for the user role, you can also restrict users to perform limited tasks. This level of control helps ensure that access is granted only to authorized individuals and provides overall control over the actions they can perform within the system.

If you have a NSO service that is configured for your setup, the role-based access control functionality available in Crosswork is synchronized with NSO and the Device Access Groups to streamline all device configurations. This integration of authentication and authorization between Crosswork and NSO for RESTCONF and json-rpc API workflows are based on JWT-tokens.

Note that reverse synchronization is not possible. Such as, when you add devices to Device Access Groups, they are mapped to NSO. However, if you add device groups in NSO, they are not reflected in Crosswork Device Access Groups. For detailed information on the prerequisites for setting up NSO, refer to the section, [Configure NSO Servers, on page 366](#).

All the external LDAP, TACACS, and RADIUS servers support the integration of Device Access Groups. To find the server information for configuring Device Access Group, please refer to the specific field description tables provided for each server in the [Set Up User Authentication \(TACACS+, LDAP, and RADIUS\), on page 373](#) section.

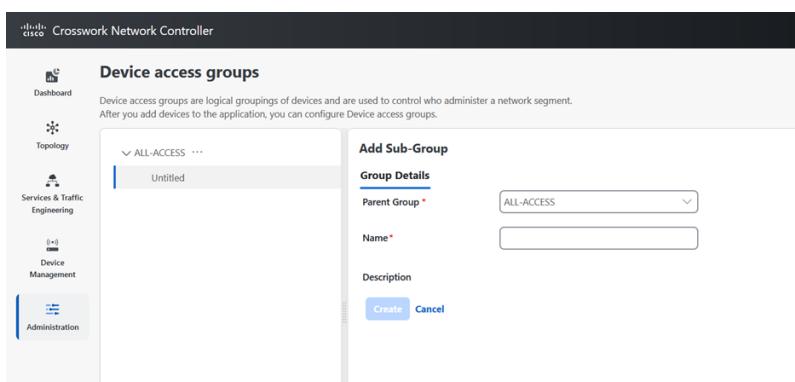
## Create Device Access Groups

To enable seamless device-level granular Role-Based Access Control across Crosswork applications and integrated NSO, create a Device Access Group that will allow for centralized management of device access permissions, ensuring consistent role based access implementation across the system. Only users belonging to a role that has the "Device Access Group Management" task enabled have the ability to perform Create, Read, Update and Delete operations on the Device Access Groups.

### Procedure

**Step 1** From the main menu, choose **Administration > Device Access Groups**.

**Step 2** Click the  icon next to ALL-ACCESS, then click **Add Sub-Group**.



**Step 3** Add the name and description of the sub-group under **Group Details**.

**Step 4** Click **Create**.

When you add a devices to a Device Access Group, you can view the **Devices** tab next to **Group Details**.

**Step 5** Click on **Add Devices**.

**Step 6** Select the devices you want to add and click **Save**.

You can also filter the devices that you want to add using the **Filter By** options for **Host Name, Product Type and Node IP**. The devices are added under Device Access Groups as well as updated in the NSO site.

**Step 7** Click **Save**.

---

## Edit Device Access Groups

You can add or remove a device from an existing Device Access Group.

### Procedure

**Step 1** From the main menu, choose **Administration > Device Access Groups**.

**Step 2** Click the Device Access Group that you want to edit and then click **Edit Group**.

You can add more devices by clicking **Add Devices** or remove them by clicking **Remove Devices**.

**Step 3** Click **Save**.

**Note**

If there is a user exclusively associated with a Device Access Group, you cannot delete that Device Access Group. However, if all users associated with a Device Access Group also have other Device Access Groups associated with them, you can delete that Device Access Group.

---

## Assign Task permissions

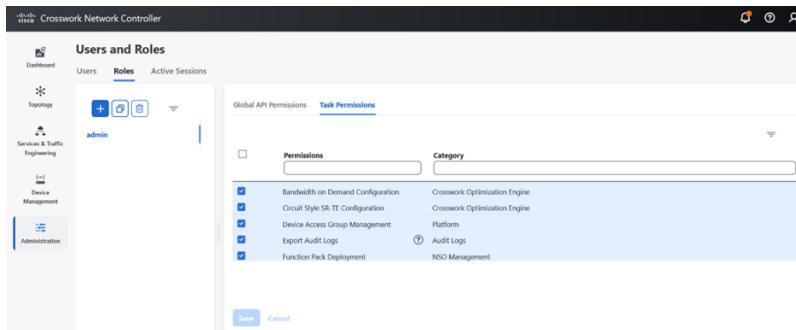
You can assign the tasks that you have created to a specific role. You can enable or disable these tasks based on the permissions you want to give for a role. The task permissions are defined by the Global APIs, which allow you to assign **Read/Write/Delete** permissions for that specific task.

### Procedure

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

**Step 2** Click **Task Permissions** to view a list of all the available tasks for your application.

Figure 128: Users and Roles Window



**Step 3** Select the task for which you want to assign permissions. Under the **Global API Permissions** tab, you can also view the specific **Read/Write/Delete** permissions that are automatically enabled for the selected task.

**Step 4** Click **Save**.

## Associate a User with a Device Access Group

Once you have created a user, you can associate that user with a specific Device Access Group. You can then assign task permissions for this user, which lets you restrict or allow certain tasks for them.

### Procedure

**Step 1** Create a role with **read/ write/ delete** API permissions and assign the set of specific tasks that need to be enabled within each role. Refer to the section, [User Roles, Functional Categories and Permissions, on page 346](#) for more details.

**Step 2** Assign this role and one or more Device Access Group to a user. Refer to the section, [Manage Users, on page 344](#) for more details.

When the user logs in, the user can only perform operations allowed by the tasks on devices belonging to the associated Device Access Groups. Based on task permissions and Device Access Group privileges, a restricted read-only Device Access Group user has the following capabilities while provisioning policies on BWoD, LCM, CSM, DLM, DGM and CAT. Such a user can-

- Preview and dry run policies but cannot provision or commit changes for the policies.
- View Services and Traffic Engineering configuration pages but cannot edit or import files.
- Perform Path Query operations.
- View Services and Traffic Engineering configuration pages but cannot edit or import files.
- Create VPN services.
- View the devices that are associated with a failed service, along with the detailed error message but cannot take actions on the errors.

Correspondingly, a Device Access Group user with all the **read/ write/ delete** permissions has the following capabilities. Such a user can-

- Perform all the tasks listed for a restricted read-only Device Access Group user.

- Provision policies for which they have been granted access to. For instance, if a user wants to create an RSVP-TE policy on a Tunnel, they will be able to do so only if they have been granted access to the head-end node. However, note that access to the end-points and hops is not checked for Device Access Group control.
- View the devices that are associated with a failed service, along with the detailed error message. Additionally, users with all privileges can take actions on errors such as Check-Sync, Sync-To, and Compare-Config at the node level.
- Run and execute Playbooks.

**Note**

To restrict device access in Crosswork for read-only users, the administrators must create an empty Device Access Group (for example, NO\_DEVICE\_ACCESS) without any devices, and assign it while creating read-only user profiles (or user profiles associated with read-only roles).

## Configure NSO Servers

The integration of authentication and authorization between Crosswork and NSO for RESTCONF and JSON-RPC API workflows is facilitated through the use of JWT. To enable role-based access control and seamless synchronization between Crosswork and NSO refer to the prerequisite steps listed under the following sections:

- [Configure Standalone NSO, on page 366](#)
- [Configure LSA NSO, on page 371](#)

**Note**

- Only administrators are allowed to make modifications to tasks.
- If any changes are made to NACM settings, the user must log out and then log back in. This is necessary to regenerate the JWT.
- When a user with limited device access tries to edit a service or upload an XML file in the Provisioning UI, the **commit** button is enabled. However, it throws an error when the user clicks the **commit** button.

## Configure Standalone NSO

Follow the steps below to configure a standalone NSO server to sync role-based access control functions with Crosswork.

### Procedure

**Step 1**

Enable `cisco-cfp-jwt-auth`.

- a) **Update the `ncs.conf` file:** Open the `ncs.conf` file in the NSO directory. Add the following configuration under the `<aaa>` section.

```
<aaa>
```

```

<package-authentication>
  <enabled>true</enabled>
  <packages>
    <package>cisco-cfp-jwt-auth</package>
  </packages>
</package-authentication>
</aaa>
- Make sure to restart ncs for the configuration in ncs.conf to take effect:
  /etc/init.d/ncs restart

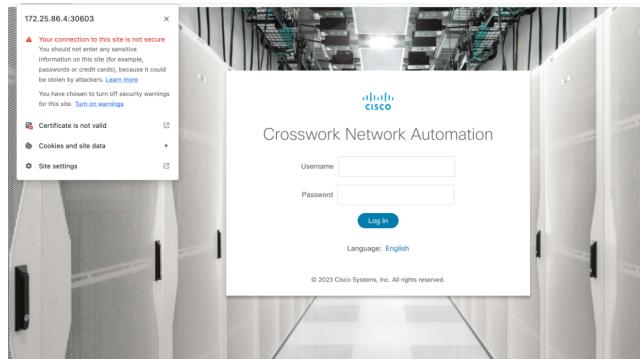
```

#### Note

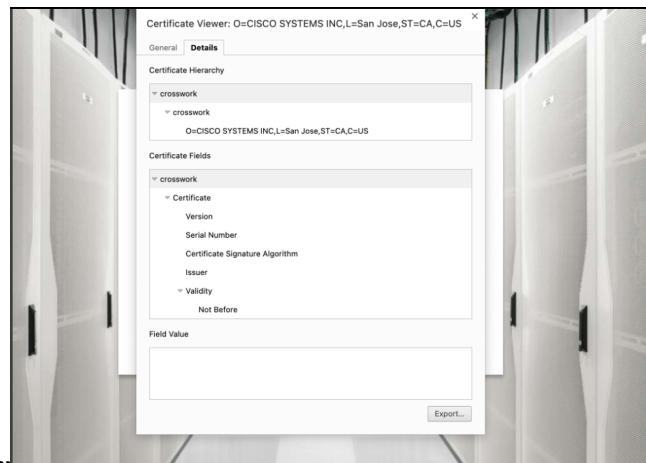
Make sure to restart NCS for the configuration in the `ncs.conf` file to take effect. If you do not want to use this feature, change 'package-authentication' to 'false' in '`ncs.conf`' in the AAA section under the NCS configuration file and restart NCS. This disables the package authentication for '`cisco-cfp-jwt-auth`'.

- Copy the certificate file from Crosswork to the NSO VM. To get the certificate from Crosswork to NSO VM, follow these steps:
  - Open the Chrome browser and navigate to the Crosswork website for which you want to import the certificate.
  - Click the padlock icon in the address bar to view the site information and then click **Certificate is not Valid > View Certificate**.

**Figure 129: View Certificate Window**



- In the **Certificate Viewer** window, go to the **Details** tab.



**Figure 130: Details for Certificate Viewer**

- Click **Crosswork** under **Certificate Hierarchy**.

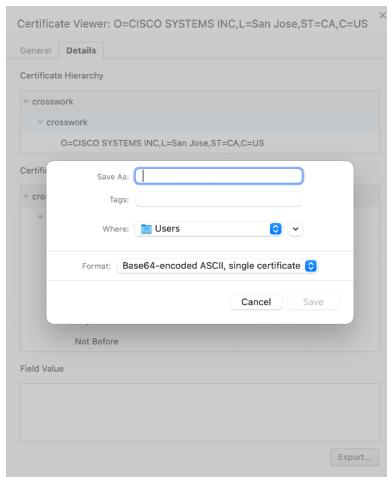
## Configure Standalone NSO

- Click the **Export** button and choose a file name and location to save the certificate. Choose the **Base64-encoded ASCII, single certificate** option and save it with the extension **.pem**. For example: crosswork.pem.

### Note

In case you encounter issues saving the file in the .pem format, an alternative is to save it as a .cer file. Once saved, proceed to use this .cer file during the bootstrap configuration process. Make sure to reference the file path of the .cer file in all subsequent steps that require it.

**Figure 131: Save the Certificate Window**



- Copy the .pem file to NSO VM.

### Note

Make sure that the value of the **pem-key-path** parameter and the filename are the same on the primary and secondary host.

- Configure Bootstrap:** To configure the Bootstrap authentication package, perform the following steps:

Login to NSO VM and load the cw-jwt-auth.xml file using the **merge** operation.

```
<config xmlns="http://tail-f.com/ns/config/1.0">
<jwt-auth xmlns="http://cisco.com/ns/ns0/cfp/cisco-cfp-jwt-auth">
<ip-address>172.20.100.42</ip-address>
<port>30603</port>
<pem-key-path>/home/ns0/crosswork.pem</pem-key-path>
</jwt-auth>
</config>
```

**OR**

Log in to **ncs\_cli** and enter config mode.

```
set jwt-auth cnc-host <Crosswork IP>
set jwt-auth port 30603
set jwt-auth pem-key-path /home/ns0/crosswork.pem
commit
```

### Step 2

Enable service level NACM.

Before creating a Rule-list, create the NACM group manually and update the user as needed when the same group applies to more than one user.

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

### Step 3 Create NACM Groups and Rule list.

- a) **For admin users:** Follow the steps below to create NACM groups and Rule-list for admin users.

- User Association:** If a NSO user is an admin user, they will automatically be part of the "ncsadmin" group, which grants them all access by default. However, if the admin user does not add this user to the "CNC#ALL-ACCESS" group, the functionalities will still work properly. If the NSO user has a different name, such as "cisco", then you must add the user to the "CNC#ALL-ACCESS" group.

Note that user creation is not required at this point.

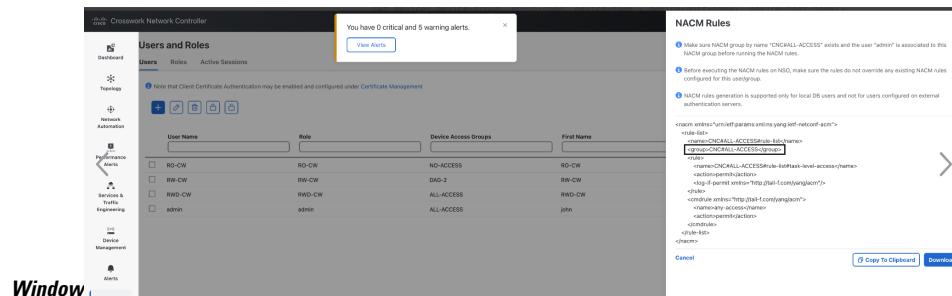
- Create Device group:** When a Device Access Group gets created in Crosswork, an equivalent device-group is created in NSO.

Note that the ALL-ACCESS Device Access Group is not created by default, and is not needed for an admin user. If you want, you can create it manually using the following command, where **group-name** is the name of the group you create.

```
ncs_cli -u admin
configure
set devices device-group "group-name" device-name [ device-host-name1, device-host-name2]
commit dry-run
commit
```

You can also copy this from Crosswork by navigating to **Administration > Users and Roles > Users > Generate NACM Rules**.

**Figure 132: Generate NACM Rules**



- Create a NACM group manually and update the user as needed when the same group applies to more than one user. Make sure to do this before you create the Rule-list.

```
ncs_cli -u admin
configure
set nacm groups group "CNC#ALL-ACCESS" user-name admin
commit dry-run
commit
```

- Create NACM Rule list:** When a User with a Role and Device Access Group is set in Crosswork, the UI displays an option to generate the NACM rules under each user. You can either copy these rules and apply them to NSO using the **commit manager** or copy the xml to the file <sample-nacm.xml> and load it using the **merge** operation. Note that for admin users only the task level access and cmd-rule are required.

```

<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>CNC#ALL-ACCESS#rule-list</name>
    <group>CNC#ALL-ACCESS</group>
    <rule>
      <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
      <action>permit</action>
      <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
    </rule>
    <cmdrule xmlns="http://tail-f.com/yang/acm">
      <name>any-access</name>
      <action>permit</action>
    </cmdrule>
  </rule-list>
</nacm>

```

- b) **For non-admin users:** Follow the steps below to create NACM groups and Rule-list for non- admin users.

In the code sample below, we have used RW-CW as an example for non-admin user and DAG-2 as a Device Access Group name.

1. **Create NACM Group:** See the code sample below:

```

ncs_cli -u admin
configure
set nacm groups group "CNC#DAG-2" user-name RW-CW
commit dry-run
commit

```

You can copy the Group name from Crosswork using the **Generate NACM Rules** option.

2. **Create NACM Rule list:** You can copy the Rule list from Crosswork using **Generate NACM Rules** option. Here is a sample-

```

<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>CNC#DAG-2#rule-list</name>
    <group>CNC#DAG-2</group>
    <rule>
      <name>CNC#DAG-2#rule-list#allow-DAG-2</name>
      <device-group
        xmlns="http://tail-f.com/yang/ncs-acm/device-group-authorization">DAG-2</device-group>
        <access-operations>create read update delete exec</access-operations>
        <action>permit</action>
        <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
      </rule>
      <rule>
        <name>CNC#DAG-2#rule-list#deny-others</name>
        <path>/devices</path>
        <access-operations>create update delete exec</access-operations>
        <action>deny</action>
      </rule>
      <rule>
        <name>CNC#DAG-2#rule-list#task-level-access</name>
        <action>permit</action>
        <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
      </rule>
      <cmdrule xmlns="http://tail-f.com/yang/acm">
        <name>any-access</name>
        <action>permit</action>
      </cmdrule>
    </rule-list>
</nacm>

```

You can push these rules to NSO via commit manager or copy them to a xml file (For example: sample-nacm.xml) and then add it on NSO with these commands:

Load sample-nacm.xml

```
ncs_cli -u admin
configure
load merge /home/ns0/sample-nacm.xml
commit
```

## Configure LSA NSO

Follow the steps below to configure a LSA NSO server to sync role-based access control functions with Crosswork.

### Procedure

**Step 1** Enable local authentication in the `ncs.conf` file under the AAA section on all the NSO RFS nodes. (If you are using the CFS node, you can skip this step)

```
<local-authentication>
<enabled>true</enabled>
</local-authentication>
```

Restart NSO by running the command `sudo /etc/init.d/ncs restart` on each RFS node.

**Step 2** **Enable cisco-cfp-jwt-auth:** Refer to the same steps to enable `cisco-cfp-jwt-auth` as described in the section, [Configure Standalone NSO, on page 366](#).

Make sure that the value of the **pem-key-path** parameter and the filename are the same on the primary and secondary host.

**Step 3** Enable service level NACM.

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

You must enable this on both the CFS and RFS nodes.

**Step 4** Create NACM Groups and Rule list. (This is applicable for both admin users and non admin-users)

- Associate Users:** To enhance security with LSA role-based authentication in NSO, we recommend that you remove the "auth-group default" map if NSO is exclusively used with Crosswork. However, if there are non-Crosswork NSO users, they must use the default map. In this case, every Crosswork user must have an entry in the "auth-group umap" to ensure the Role-Based Access Control flow functions correctly.
- Define a Crosswork user under "aaa:aaa" as an authentication user on every RFS node. This configuration enables communication between CFS and RFS for this user. Note that the username must match the username used in Crosswork, but the password can differ.
- Add every Crosswork user as a "umap" entry under the device authentication group in the CFS. This ensures proper functionality and enforces Role-Based Access Control for users in Crosswork. This also allows the CFS to pass user

requests to the RFS node as the corresponding user. If you want a role-based access for a user, you must create the umap entry in the CFS auth-group. Otherwise, the default map applies, which breaks the role-based access workflow.

- d) Define a generic NACM group and NACM rule with all permissions on the CFS, to enable access to RFS nodes for all users. This grants access to RFS for all users. Additionally, when creating any user in Crosswork, add that user to the "CNC#ALL-ACCESS" NACM group in CFS. This ensures that the user has the necessary access privileges and permissions to perform actions within Crosswork.

```
group "CNC#ALL-ACCESS" {
    user-name [ RW-CW admin rw-user ];
}
```

You can copy the NACM rules from Crosswork.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <!--NACM rules for NSO - CFS-->
    <rule-list>
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <!--NACM rules for NSO - RFS-->
    <rule-list>
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

## Step 5

**Create Device group:** Add the Device Access Groups and NACM rules on the RFS node. By defining NACM rules for a user, access to devices can be granted based on the specific rules that you configure for that user. Note that Device Access Group creation is automatically handled by Crosswork, so you do not need any additional steps for Device Access Group creation on NSO.

### Note

If you have Geo-HA set up, and encounter the 503 error, follow the steps below to resolve it.

Add the following configurations exclusively to the **/etc/environment** file within the CFS node:

- Open the file `sudo vi /etc/environment`.
- Add the following lines:

```
https_proxy="http://proxy.esl.cisco.com:80"
http_proxy="http://proxy.esl.cisco.com:80"
```

- c) Define exceptions with the line:

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,<az1 mgmt vip>,<az2 mgmt vip>,<fqdn of CW geo-mgmt VIP>"
```

For example:

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,192.168.6.50,192.168.5.50,geomanagement.cw.cisco,cw.cisco"
```

- d) Source the file: `source /etc/environment`  
e) Reboot the CFS nodes for the proxy settings to take effect.
- 

## Set Up User Authentication (TACACS+, LDAP, and RADIUS)

In addition to supporting local users, Cisco Crosswork supports TACACS+, LDAP, and RADIUS users through integration with the TACACS+, LDAP, and RADIUS servers. The integration process has the following steps:

- Configure the TACACS+, LDAP, and RADIUS servers.
- Create the roles that are referenced by the TACACS+, LDAP, and RADIUS users.
- Configure AAA settings.
- You can also enable Single Sign-on (SSO) for authentication of TACACS+, LDAP, and RADIUS users. For more information, see [Enable Single Sign-on \(SSO\), on page 386](#).
- You can create and manage Device Access Groups for users on these servers. For more information, see [Manage Device Access Groups, on page 362](#).



### Note

- The AAA server page works in bulk update mode wherein all the servers are updated in a single request. It is advised to give write permission for "Remote Authentication Servers Integration api" only to users who have the relevant authorization to delete the servers.
- A user with only Read and Write permissions (without 'Delete' permission) can delete the AAA server details from Cisco Crosswork since delete operations are part of 'Write' permissions. For more information, see [Create User Roles, on page 347](#).
- While making changes to AAA servers (create/edit/delete), you are recommended to wait for few minutes between each change. Frequent AAA changes without adequate intervals can result in external login failures.
- Cisco Crosswork supports the configuration of up to 5 external servers.



### Caution

Please note that any operation you do following the instructions in this section will affect all new logins to the Crosswork user interface. To minimize session interruption, Cisco recommends that you perform all your external server authentication changes and submit them in a single session.

# Manage TACACS+ Servers

Crosswork supports the use of TACACS+ servers to authenticate users.

You can integrate Crosswork with a standalone server (open TACACS+) or with an application such as Cisco ISE (Identity Service Engine) to authenticate using the TACACS+ protocols.

## Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see [Create Device Access Groups, on page 363](#)
- Configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the TACACS+ server (standalone or Cisco ISE), before configuring the AAA server in Cisco Crosswork. For more information on Cisco ISE procedures, see the latest version of [Cisco Identity Services Engine Administrator Guide](#).

## Procedure

**Step 1** From the main menu, select **Administration > AAA > Servers > TACACS+ tab**. From this window, you can add, edit, and delete a new TACACS+ server.

**Step 2 To add a new TACACS+ server:**

- a) Click the  icon.
- b) Enter the required TACACS+ server information.

**Table 34: TACACS+ field descriptions**

Field	Description
Authentication Order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP Address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS Name	Enter the DNS name (if DNS name is selected). Only IPv4 DNS name is supported.
Port	The default TACACS+ port number is 49.
Shared Secret Format	Shared secret for the active TACACS+ server. Select ASCII or Hexadecimal.
Shared Secret / Confirm Shared Secret	Plain-text shared secret for the active TACACS+ server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the <b>Shared Secret</b> parameter you enter on this screen must match with the shared secret value configured on the TACACS+ server.

Field	Description
Service	<p>Enter value of the service that you are attempting to gain access to. For example, "raccess".</p> <p>This field is verified only for standalone TACACS+. In case of Cisco ISE, you can enter a junk value. Do not leave the field blank.</p>
Policy Id	<p>Enter the user role that you created in the TACACS+ server.</p> <p><b>Note</b> If you try to login to Cisco Crosswork as a TACACS+ user before creating the required user role, you will get the error message: "Key not authorized: no matching policy". If this occurs, close the browser. Login as a local admin user and create the missing user roles in the TACACS+ server, and login back to Crosswork using the TACACS+ user credentials.</p>
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in (ISE/Standalone) TACACS+ server attributes. These values can be one or more than one comma separated values.
Retransmit Timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication Type	<p>Select the authentication type for TACACS+:</p> <ul style="list-style-type: none"> <li>• PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.</li> <li>• CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).</li> </ul>

See the example at the end of this topic for more details.

- c) After you enter all the relevant details, click **Add**.
- d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

### Step 3

**To edit a TACACS+ server:**

- a) Click the checkbox next to the TACACS+ server and click .
- b) After making changes, click **Update**.

### Step 4

**To delete a TACACS+ server:**

- a) Click the checkbox next to the TACACS+ server and click . The Delete server-IP-address dialog box opens.
- b) Click **Delete** to confirm.

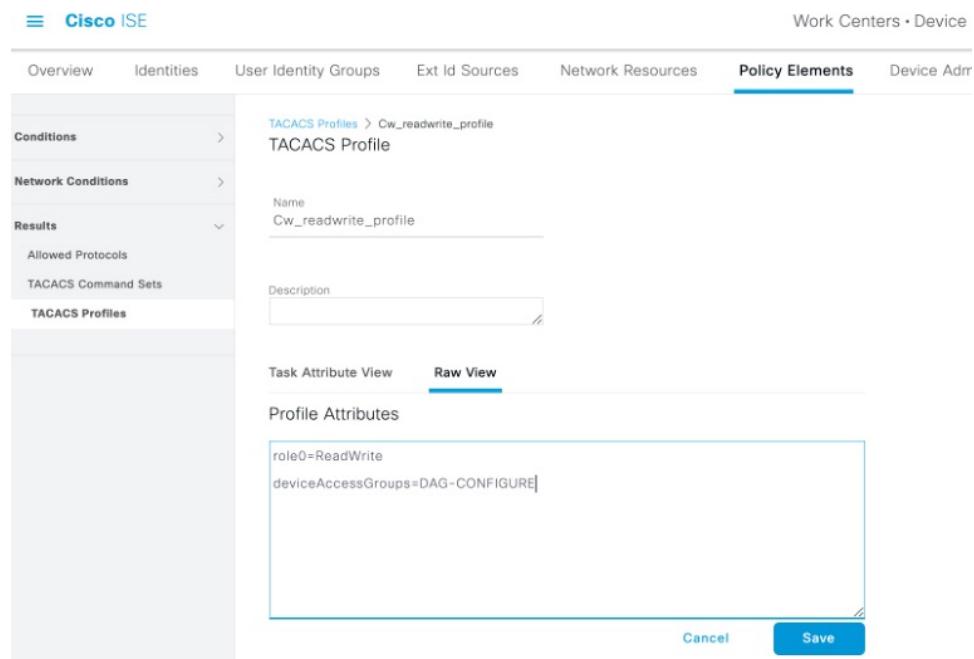
## Example

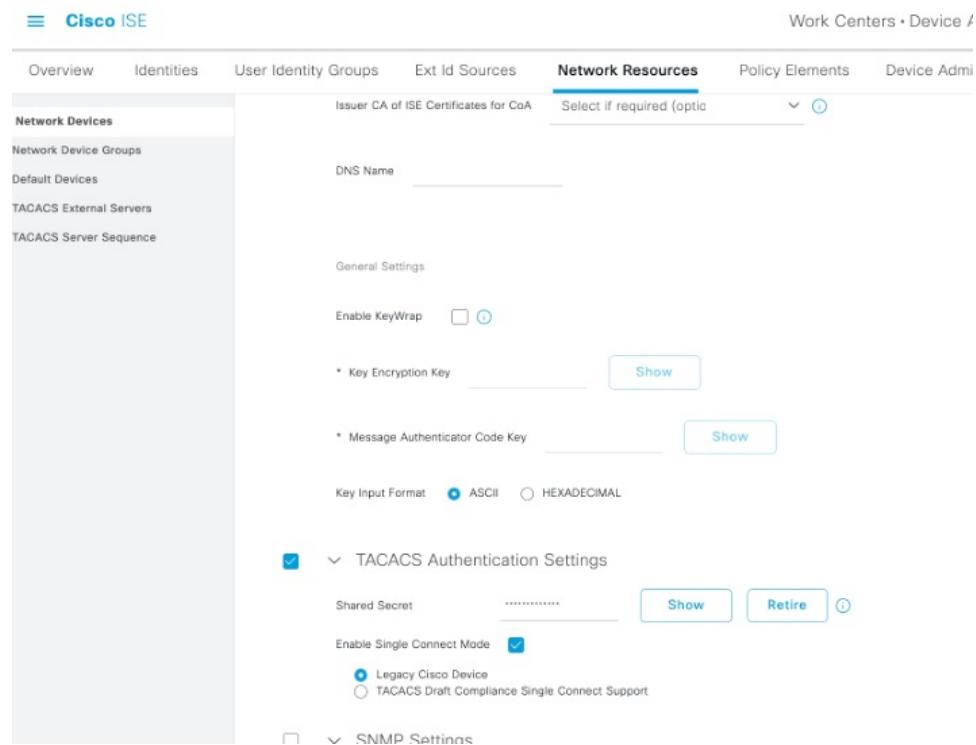
In this example, the TACACS+ parameters are configured in Cisco ISE. As a prerequisite, a Device Access Group has been created in Crosswork to manage the AAA operation access.

The relevant TACACS+ parameters are configured in Cisco ISE:

- User profile: `role0` (to be used in *Policy Id* field)
- Device Access Group Attribute: `DAG-CONFIGURE`
- Shared secret format: `ASCII`

**Figure 133: Configure TACACS+ Profile Attributes in Cisco ISE**



**Figure 134: Configure TACACS+ Authentication Settings in Cisco ISE**

Now, the TACACS+ server is added in Crosswork UI:

Figure 135: Add TACACS+ Server

← AAA

## Add TACACS+ Server

Authentication Order *	14
IP Address	<input type="text"/>
DNS Name *	<input checked="" type="radio"/> cw-qc-ise-1-ipv4
Port *	49
Shared Secret Format *	ASCII
Shared Secret *	<input type="text"/> ..... <a href="#">Show</a>
Confirm Shared Secret *	<input type="text"/> ..... <a href="#">Show</a>
Service *	raccess
Policy Id	role0
Device Access Group Attribute	deviceAccessGroups
ReTransmit Timeout	30
Retries *	10
Authentication Type *	PAP

Here is the sample API payload for the above example:

```
{
  "tacacs": {
    "tacacs_servers": [
      {
        "priority": 10,
        "host": "cw-qc-ise-1-ipv4",
        "dnsName": "",
        "port": 49,
        "secretFormat": "ascii",
        "secret": "sample",
        "service": "raccess",
        "policy-id": "role0",
        "virtualDomain": "deviceAccessGroups",
        "timeout": 30,
      }
    ]
  }
}
```

```

        "retries":10,
        "authType":"pap",
    }
]
}
}

```

CROSSWORK  
VALUE

CISCO ISE

```

Device Access Group Attribute=deviceAccessGroups      deviceAccessGroups=DAG-CONFIGURE
DAG-CONFIGURE
PolicyId=role0
ReadWrite
role0=ReadWrite
ReadWrite

```

## Manage LDAP Servers

Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. Crosswork supports the use of LDAP servers (OpenLDAP, Active Directory, and secure LDAP) to authenticate users. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

To use secure LDAP protocol, you must add **Secure LDAP Communication** certificate before adding the LDAP server. For more details on adding certificates, see [Add a New Certificate, on page 326](#).

### Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see [Create Device Access Groups, on page 363](#)
- Configure the relevant parameters (bind DN, policy baseDN, policy id, device access group attribute, etc.) in the LDAP server before configuring the AAA server in Cisco Crosswork.

### Procedure

**Step 1** From the main menu, select **Administration > AAA > Servers > LDAP** tab. Using this window, you can add, edit, and delete a new LDAP server.

**Step 2 To add a new LDAP server:**

- Click the  icon.
- Enter the required LDAP server details.

*Table 35: LDAP field descriptions*

Field	Description
Authentication Order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.

Field	Description
Name	Name of the LDAP handler.
IP Address/ Host Name	LDAP server IP address or host name
Secure Connection	Enable the <b>Secure Connection</b> toggle button if you want to connect to the LDAP server via the SSL communication. When enabled, select the secure LDAP certificate from the <b>Certificate</b> drop-down list.  <b>Note</b> The secure LDAP certificate must be added in the Certificate Management screen prior to configuring the secure LDAP server.  This field is disabled by default.
Port	The default LDAP port number is 389. If Secure Connection SSL is enabled, the default LDAP port number is 636.
Bind DN	Enter the login access details to the database. Bind DN allows user to login to the LDAP server.
Bind Credential / Confirm Bind Credential	Username and password to login to the LDAP server.
Base DN	Base DN is the starting point used by the LDAP server to search for user authentication within your directory.
User Filter	The filter for user search.
DN Format	The format used to identify the user in base DN.
Principal Attribute ID	This value represents the UID attribute in the LDAP server user profile under which a particular username is organized.
Policy BaseDn	This value represents the role mapping for user roles within your directory.
Policy Map Attribute	This helps in identifying the user under the policy base DN.  This value maps to the <code>userFilter</code> parameter in your LDAP server attributes.
Policy ID	The <b>Policy ID</b> field corresponds to the user role that you created in the LDAP server.  <b>Note</b> If you try to login to Cisco Crosswork as a LDAP user before creating the required user role, you will get the error message: "Login failed, policy not found. Please contact the Network Administrator for assistance.". To avoid this error, ensure to create the relevant user roles in the LDAP server, before setting up a new LDAP server in Crosswork.
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in LDAP server attributes. These values can be one or more than one comma separated values.
Connection Timeout	Enter the timeout value. Maximum timeout is 30 seconds.

See the example at the end of this topic for more details.

- c) Click **Add**.
- d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

**Step 3 To edit a LDAP server:**

- a) Select the LDAP server and click .
- b) After making changes, click **Update**.

**Step 4 To delete a LDAP server:**

- a) Select the LDAP server and click .
- b) Click **Delete** to confirm.

---

### Example

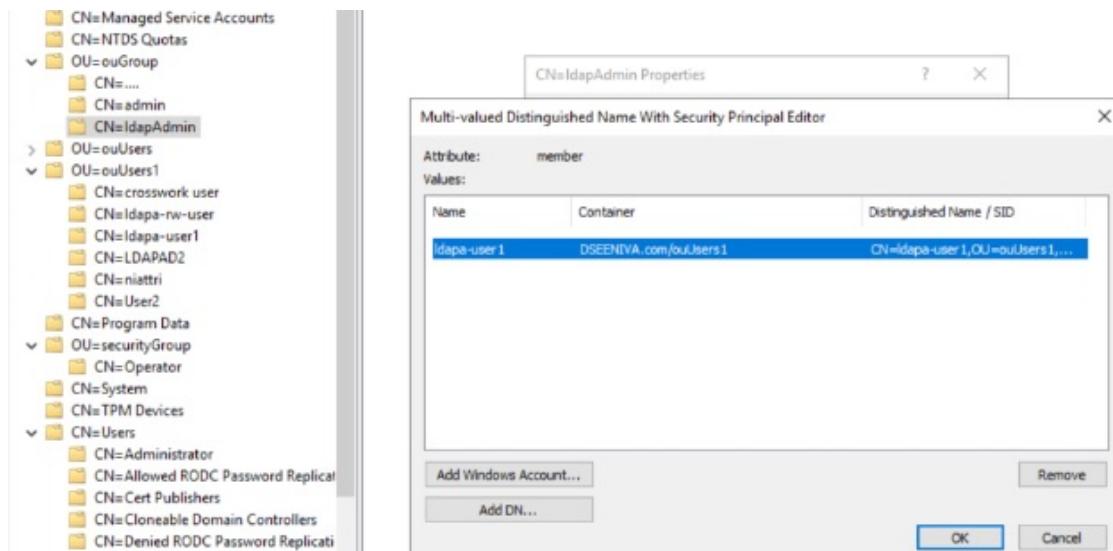
The below example shows the parameters entered for secure LDAP configuration. As a prerequisite, a Device Access Group has been created and configured in Crosswork to manage the AAA operation access.

The relevant parameters are configured in the LDAP server. Here are some of the key points:

- The user role is `ldap-user1` and it belongs to the user group `ldapAdmin`.
- The username is this example is `DSEENIVA`.
- The policy id is `sAMAccountName`.
- The `ldapUrl` parameter is a combination of address and port
- The parameters under the `ldap_attr_server` section are used for role mapping. The `baseDN` parameter maps to the *Policy baseDN* field and the `userFilter` parameter maps to the *Policy Map Attribute* field in the Crosswork UI.
- The device access group is configured in LDAP server as `'Description='ALL-ACCESS'`.

The user group and user role mapping configured in LDAP server:

Figure 136: Add LDAP Server



Here is the sample API payload for this example:

```
{
  "ldap": {
    "ldap_servers": [
      "ldap_server": [
        {
          "type": "DIRECT",
          "bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "connectionStrategy": "",
          "useSsl": false,
          "useStartTls": false,
          "connectTimeout": 10,
          "baseDn": "OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "userFilter": "cn={user}",
          "subtreeSearch": true,
          "usePasswordPolicy": false,
          "dnFormat": "cn=%s,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "principalAttributeId": "cn",
          "policyId": "Description",
          "minPoolSize": 1,
          "maxPoolSize": 1,
          "validateOnCheckout": false,
          "validatePeriodically": true,
          "validatePeriod": 600,
          "idleTime": 5000,
          "prunePeriod": 5000,
          "blockWaitTime": 5000,
          "providerClass": "org.ldaptive.provider.unboundid.UnboundIDProvider",
          "allowMultipleDns": false,
          "order": 16,
          "trustStore": "ldaps",
          "name": "ldapsecure",
          "ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
          "bindCredential": "<>"
        }
      ],
      "ldap_attr_servers": {
        "ldap_attr_server": [
          {
            "baseDn": "OU=ouGroup,dc=DSEENIVA,dc=COM",
            "trustStore": "ldaps",
            "name": "ldapsecure"
          }
        ]
      }
    ]
  }
}
```

```

"ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
"bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
"bindCredential": "<>",
"userFilter": "member=cn={user},OU=ouUsers1,dc=DSEENIVA,dc=COM",
"failFast": false,
"attributes": {
  "policy_id": "sAMAccountName"
}}]}}}
```

Here is the corresponding LDAP configuration in the Crosswork UI:

Figure 137: Add LDAP Server

← AAA

## Add LDAP Server

**Authentication order \*** ① 16

**Name \*** ldapsecure

**IP address/Host name \*** cw-qa-ldap-2-ipv4

**Secure connection\***

**Certificate \*** ldaps

**Port \*** 636

**Bind DN \*** cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM

**Bind credential \***  ..... [Show](#)

**Confirm bind credential \***  ..... [Show](#)

**Base DN \*** OU=ouUsers1,dc=DSEENIVA,dc=COM

**User filter \*** cn={user}

**DN format \*** cn=%s,OU=ouUsers1,dc=DSEENIVA,dc=COM

**Principal attribute ID \*** cn

**Policy baseDN \*** OU=ouGroup,dc=DSEENIVA,dc=COM

**Policy map attribute \*** member=cn={user},OU=ouUsers1,dc=DSEENIVA,dc=COM

**Policy ID \*** sAMAccountName

**Device access group \* ① attribute** Description

**Connect timeout \*** 10

# Manage RADIUS Servers

Crosswork supports the use of RADIUS (Remote Authentication Dial-In User Service) servers to authenticate users. You can also integrate Crosswork with an application such as Cisco ISE (Identity Service Engine) to authenticate using the RADIUS protocols.

## Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see [Create Device Access Groups, on page 363](#)
- Similar to TACACS+ server, you must configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the RADIUS server before configuring the AAA server in Cisco Crosswork. For more information on Cisco ISE procedures, see the latest version of [Cisco Identity Services Engine Administrator Guide](#).

## Procedure

**Step 1** From the main menu, select **Administration > AAA > Servers > RADIUS** tab. From this window, you can add, edit, and delete a new RADIUS server.

**Step 2 To add a new RADIUS server:**

- a) Click the  icon.
- b) Enter the required RADIUS server information.

**Table 36: RADIUS field descriptions**

Field	Description
Authentication Order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP Address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS Name	Only IPv4 DNS name is supported (if DNS name is selected).
Port	The default RADIUS port number is 1645.
Shared Secret Format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.
Shared Secret / Confirm Shared Secret	Plain-text shared secret for the active RADIUS server. The format of the text entered must match with the format selected (ASCII or Hexadecimal).  For Crosswork to communicate with the external authentication server, the <b>Shared Secret</b> parameter you enter on this screen must match with the shared secret value configured on the RADIUS server.
Service	Enter value of the service that you are attempting to gain access to. For example, "raccess".

Field	Description
Policy Id	<p>The <b>Policy Id</b> field corresponds to the user role that you created in the RADIUS server.</p> <p><b>Note</b> If you try to login to Cisco Crosswork as a RADIUS user before creating the required user role, you will get the error message: "Key not authorized: no matching policy". If this occurs, close the browser. Login as a local admin user and create the missing user roles in the RADIUS server, and login back to Crosswork using the RADIUS user credentials.</p>
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in RADIUS server attributes. These values can be one or more than one comma separated values.
Retransmit Timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication Type	<p>Select the authentication type for RADIUS:</p> <ul style="list-style-type: none"> <li>• PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.</li> <li>• CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).</li> </ul>

As RADIUS configuration is very similar to TACACS+, please refer to the detailed example in the [Manage TACACS+ Servers, on page 374](#) for more information.

- c) After you enter all the relevant details, click **Add**.
- d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

### Step 3

#### To edit a RADIUS server:

- a) Click the checkbox next to the RADIUS server and click .
- b) After making changes, click **Update**.

### Step 4

#### To delete a RADIUS server:

- a) Click the checkbox next to the RADIUS server and click . The Delete *server-IP-address* dialog box opens.
- b) Click **Delete** to confirm.

## Configure AAA Settings

Users with relevant AAA permissions can configure the AAA settings.

**Procedure**

**Step 1** From the main menu, choose **Administration > AAA > Settings**.

**Step 2** Select the relevant setting for **Fallback to Local**. By default, Crosswork prefers external authentication servers over local database authentication.

**Note**

Admin users are always authenticated locally.

**Step 3** Select the relevant value for the **Logout All Idle Users After** field. Any user who remains idle beyond the specified limit will be automatically logged out.

**Note**

The default timeout value is 30 minutes. If the timeout value is adjusted, the page will refresh to apply the change.

**Step 4** Enter a relevant value for the **Number of Parallel Sessions**.

**Note**

Crosswork supports between 5 to 200 parallel session for concurrent users. If the number of parallel sessions are exceeded, an error is displayed while logging in to Crosswork.

**Note**

Crosswork supports 50 simultaneous NBI sessions up to 400 sessions.

**Step 5** Check the **Enable source IP for auditing** check box to log the IP address of the user (source IP) for auditing and accounting. This check box is disabled by default. Once you enable this option and relogin to Cisco Crosswork, you will see the **Source IP** column on the **Audit Log** and **Active Sessions** pages.

**Step 6** Select the relevant settings for the **Local Password Policy**. Certain password settings are enabled by default and cannot be disabled (for example, Change password on first login).

**Note**

Any changes in the password policy is enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

**Note**

**Local Password Policy** allows administrators to configure the number of unsuccessful login attempts a user can make before they are locked out of Crosswork, and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

## Enable Single Sign-on (SSO)

Single Sign-on (SSO) is an authentication method that allows you to log in with a single ID and password to any of several related, yet independent, software systems. It allows you to log in once and access the services without reentering authentication factors. Cisco Crosswork acts as Identity Provider (IDP) and provides authentication support for the relying service providers. You can also enable SSO for authentication of TACACS+, LDAP, and RADIUS users.

**Attention**

- When Crosswork is re-installed, you must ensure that the latest IDP metadata from Crosswork is updated to the service provider applications. Failing to do this will result in authentication failure due to mismatched metadata information.
- First-time login users cannot switch to using a different username before mandatorily changing the password. The only workaround is for the administrator to terminate the session.

When Crosswork is re-installed, you must ensure that the latest IDP metadata from Crosswork is updated to the service provider applications. Failing to do this will result in authentication failure due to mismatched metadata information.

**Note**

The Cisco Crosswork login page is not rendered when the Central Authentication Service (CAS) pod is restarting or not running.

**Before you begin**

Ensure that the **Enable source IP for auditing** check box is selected on the **Administration > AAA > Settings** page.

**Procedure**

**Step 1** From the main menu, choose **Administration > AAA > SSO**. Using this window, you can add, edit settings, and delete service providers.

**Step 2 To add a new service provider:**

- Click the icon.
- In the **Service Provider** window, enter the values in the following fields:
  - Name:** Enter the name of the service provider.
  - Evaluation Order:** Enter a unique number which indicates the order in which the service definition should be considered.
  - Metadata:** Click the field, or click **Browse** to navigate to the metadata XML document that describes a SAML client deployment.

**Step 3** Click **Add** to finish adding the service provider.

**Step 4** Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

After the settings are saved, when you log into the integrated service provider application for the first time, the application gets redirected to the Cisco Crosswork server. After providing the Crosswork credentials, the service provider application logs in automatically. For all the subsequent application logins, you do not have to enter any authentication details.

**Step 5 To edit a service provider:**

- a) Click the check box next to the service provider and click . You can update the Evaluation Order and Metadata values as required.
- b) After making changes, click **Update**.

**Step 6****To delete a service provider:**

- a) Click the check box next to the service provider and click .
  - b) Click **Delete** to confirm.
- 

## Security Hardening Overview

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- Cisco Crosswork infrastructure
- Cisco Crosswork storage system (local or external)

Hardening Cisco Crosswork security requires completion of the following tasks:

- Shutting down insecure and unused ports
- Configuring network firewalls
- Hardening the Cisco Crosswork infrastructure, as needed

Although your primary source of information is your Cisco representative, who can provide server hardening guidance specific to your deployment, you can also follow the steps in this section to secure Cisco Crosswork.

## Authentication Throttling

Cisco Crosswork throttles the login attempts after a failed login attempt to avoid password guessing and other related abuse scenarios. After a failed login attempt for a username, all authentication attempts for that username would be blocked for 3 seconds. The throttling is applicable to all supported authentication schemes such as TACACS, LDAP and the default local authentication.

## Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco Crosswork product, you should have a good understanding of the following security concepts.

### HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco Crosswork now supports TLS only.



**Note** TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

## X.509 Certificates

X.509 certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.
2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.
- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

## 1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL or x.509 certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco Crosswork server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.



**Note** A client might need to store multiple server certificates to enable interaction with multiple servers.

## Disable Insecure Ports and Services



To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

## Disable Insecure Ports and Services

As a general policy, any ports that are not needed should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco Crosswork. You can do this by listing the ports that are open and comparing it with a list of ports needed for Cisco Crosswork.

To view a list of all open listening ports:

### Procedure

#### Step 1

Log in as a Linux CLI admin user and enter the **netstat -aln** command.

The **netstat -aln** command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. The command returns output similar to the following:

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp    0      0      0.0.0.0:111           0.0.0.0:*
                                         LISTEN
tcp    0      0      127.0.0.1:8080        0.0.0.0:*
                                         LISTEN
tcp    0      0      0.0.0.0:22           0.0.0.0:*
                                         LISTEN
tcp    0      0      127.0.0.1:25           0.0.0.0:*
                                         LISTEN
tcp    0      0      127.0.0.1:10248        0.0.0.0:*
                                         LISTEN
tcp    0      0      127.0.0.1:10249        0.0.0.0:*
                                         LISTEN
```

tcp	0	0	192.168.125.114:40764	192.168.125.114:2379	ESTABLISHED
tcp	0	0	192.168.125.114:48714	192.168.125.114:10250	CLOSE_WAIT
tcp	0	0	192.168.125.114:40798	192.168.125.114:2379	ESTABLISHED
tcp	0	0	127.0.0.1:33392	127.0.0.1:8080	TIME_WAIT
tcp	0	0	192.168.125.114:40814	192.168.125.114:2379	ESTABLISHED
tcp	0	0	192.168.125.114:40780	192.168.125.114:2379	ESTABLISHED
tcp	0	0	127.0.0.1:8080	127.0.0.1:44276	ESTABLISHED
tcp	0	0	192.168.125.114:40836	192.168.125.114:2379	ESTABLISHED
tcp	0	0	192.168.125.114:40768	192.168.125.114:2379	ESTABLISHED
tcp	0	0	127.0.0.1:59434	127.0.0.1:8080	ESTABLISHED
tcp	0	0	192.168.125.114:40818	192.168.125.114:2379	ESTABLISHED
tcp	0	0	192.168.125.114:22	192.168.125.1:45837	ESTABLISHED
tcp	0	0	127.0.0.1:8080	127.0.0.1:48174	ESTABLISHED
tcp	0	0	127.0.0.1:49150	127.0.0.1:8080	ESTABLISHED
tcp	0	0	192.168.125.114:40816	192.168.125.114:2379	ESTABLISHED
tcp	0	0	192.168.125.114:55444	192.168.125.114:2379	ESTABLISHED

**Step 2** Check the for the table of ports used by Cisco Crosswork, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product*.

**Note**

If you are not sure whether you should disable a port or service, contact the Cisco representative.

**Step 3** If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork to operate.

## Harden Your Storage

We recommend that you secure all storage elements that will participate in your Cisco Crosswork installation, such as the database, backup servers, and so on.

- If you are using external storage, contact the storage vendor and the Cisco representative.
- If you are using internal storage, contact the Cisco representative.
- If you ever uninstall or remove Cisco Crosswork, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted). Contact the Cisco representative for more information.

## Configure System Settings

Administrator users can configure the following system settings:

### Configure a Syslog Server

Cisco Crosswork allows external syslog consumers to:

- Register on Crosswork to system events, audit events, and internal collection jobs to the Syslog and Trap servers.
- 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.



**Note** After the Syslog TLS server certificate is added, wait for 5-10 minutes before configuring the syslog server.



**Attention** The APIs to configure a syslog server are deprecated in the Crosswork 6.0 release.

### Before you begin

Ensure that you have uploaded the Syslog TLS server certificate. For more information, see [Add a New Certificate, on page 326](#).

### Procedure

**Step 1** From the main menu, choose **Administration > Settings > System Settings** tab.

**Step 2** Under **Server**, click the **Syslog Configuration** option.

**Step 3** Click **+**.

**Step 4** Enter Syslog configuration details. For more information, click **ⓘ** next to each option.

Use the **Criteria** option to define scope and range of which kind of events should be forwarded as a syslog. For example: **(EventSeverity<2 or EventSeverity>=5) and OriginAppId=capp-infra and EventCategory=1**

The expression sends events as a syslog only if the event originates from the Infrastructure Platform, the category is the system, and the severity is either less than 2 or is equal or above 5.

**Caution**

Expressions are freeform and not validated.

**Step 5** Click **Save**.

## Syslog Events

After the Syslog destination is configured, Crosswork generates events in the form of Syslogs and sends it to the Syslog destination. The events have the following format:

`<pri><v> <stamp> <vip> <app> <PID> <Message ID> <Structure Data> <Message>`

The following table lists the fields that are sent in syslogs.

**Table 37: Syslog Event Fields and Description**

Field	Description	Example
Pri	<p>The priority of the event generated:</p> $\text{Priority} = (8 * \text{facility} + \text{severity})$ <p>Where <code>facility</code> is the category of the event generated.</p> <p>The category of the event generated represented using an integer value:</p> $\begin{aligned} \text{System} &= 3, \text{Network} = 7, \text{Audit} \\ &= 13, \text{Security} = 4, \text{External} \\ &= 1 \end{aligned}$ <p>The alarm severity indicates the severity of the event using an integer value:</p> $\begin{aligned} \text{Critical} &= 2, \text{Major} = 3, \\ \text{Warning} &= 4, \text{Minor} = 5, \\ \text{Info} &= 6, \text{Clear} = 7 \end{aligned}$	Event with the Category as System and Severity as Major, the PID = $8 * 3 + 3 = 27$ .
v	The version of the Syslog server.	NA
Stamp	The timestamp at which the event is created.	Mar 28 15:2:22 10.56.58.188
VIP	The Crosswork VIP address.	10.56.58.188
App	The event OriginServiceId and OriginAppId.	orchestrator-capp-infra
PID	The process ID.	NA
Message ID	The event ID.	8586f9cf-d05d-4d94-ab62-27d7e808b5f6
Structured Data	The event ObjectId and event type.	robot-topo-svc-0
Message	The description of the event.	Restart of robot-topo-svc successful.

## Configure a Trap Server

Cisco Crosswork allows external trap consumers to:

- Register on Crosswork and receive system events and audit log as traps.
- Define and filter which kind of events should be forwarded as a traps, per consumer.
- Define the rate of which traps are forwarded to the consumer.

## Configure the Interface Data Collection

For more information on trap handling, see [Enable Trap Handling, on page 414](#).



**Attention** The APIs to configure a trap server are deprecated in the Crosswork 6.0 release.

Follow the procedure below to manage Trap Servers from the Settings window:

### Procedure

**Step 1** From the main menu, choose **Administration > Settings > System Settings** tab.

**Step 2** Under **Server**, click the **Trap servers** option.

**Step 3** Click

**Step 4** Enter Trap server details. For more information, click next to each option.

Use the **Criteria** option to define scope and range of which kind of events should be forwarded as a trap.

Click **Events and Alarms examples** for more information on the attributes used to raise an event.

**Step 5** After entering all the relevant information, click **Add**.

## Configure the Interface Data Collection

Crosswork Data Gateway collects the interface state and stats data such as name, type, and traffic counters from the devices through the SNMP or gNMI protocol. Crosswork Data Gateway starts the data collection when a device is onboarded and attached to the data gateway.

Follow the steps to configure interface data collection settings:

### Before you begin

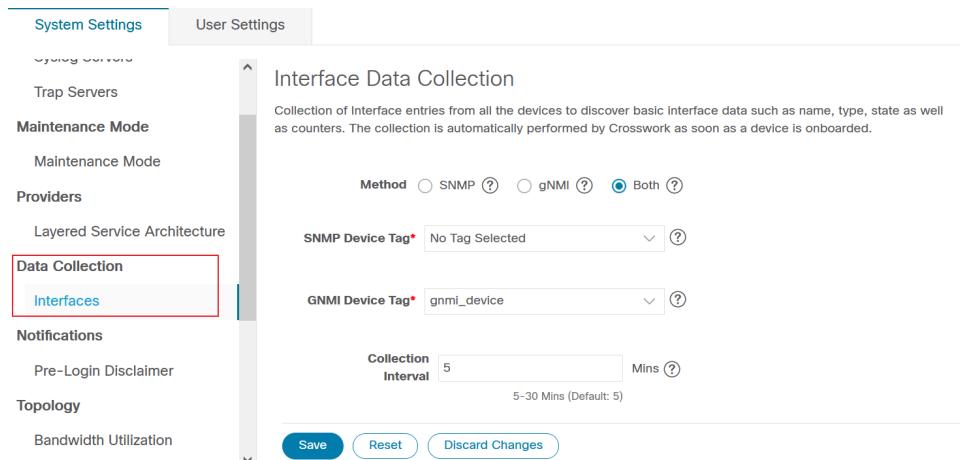
Create a tag and assign it to the device for which Crosswork collects the interface data. For information on how to create and assign a tag to the device, see [Create Tags, on page 201](#) and [Apply or Remove Device Tags, on page 202](#).

### Procedure

**Step 1** From the main menu, choose **Administration > Settings > System Settings** tab.

**Step 2** Under **Data Collection**, select **Interfaces**.

Figure 138: Interface Data Collection Window



**Step 3** In the **Interface Data Collection** pane, select the appropriate method:

- **SNMP:** Crosswork collects the IF-MIB and IP-MIB data from the devices.
- **gNMI:** Crosswork collects the openconfig-interfaces data from the devices.
- **Both:** Depending on the device's capability, select SNMP and gNMI protocol to discover the devices.

If you choose **Both** as the method, you must select the appropriate SNMP and gNMI device tags. If you choose **SNMP** or **gNMI** method, the device tags become optional.

**Step 4** From the **Select {SNMP or gNMI} Device Tag** drop-down, select unique tags for SNMP and gNMI protocols.

The precreated tags associated to the device are listed. If you select **No Tag Selected** option, Crosswork starts the data collection for devices with system SNMP or gNMI tags.

**Step 5** In the **Interface Collection Interval** field, specify the duration between the data collection requests. The default duration is 5 minutes.

**Step 6** Click **Save**.

## Set the Pre-Login Disclaimer

Many organizations require that their systems display a disclaimer message in a banner before users log in. The banner may remind authorized users of their obligations when using the system, or provide warnings to unauthorized users. You can enable such a banner for Crosswork users, and customize the disclaimer message as needed.

### Procedure

- Step 1** From the main menu, choose **Administration > Settings > System Settings** tab.
- Step 2** Under **Notifications**, click the **Pre-Login Disclaimer** option.
- Step 3** To enable the disclaimer and customize the banner:

- a) Check the **Enabled** checkbox.
- b) Customize the banner **Title**, the **Icon**, and the **Disclaimer Text** as needed.
- c) Optional: While editing the disclaimer, you can
  - Click **Preview** to see how your changes will look when displayed before the Crosswork login prompt.
  - Click **Discard Changes** to revert to the last saved version of the banner.
  - Click **Reset** to revert to the original, default version of the banner.
- d) When you are satisfied with your changes, click **Save** to save them and enable display of the custom disclaimer to all users.

**Step 4**

To turn off the disclaimer display: Select **Administration > Settings > System Settings > Pre-Login Disclaimer**, then uncheck the **Enabled** checkbox.

## Manage File Server Settings

Cisco Crosswork provides secure file transfer services (FTP and SFTP) for Crosswork applications that need them. They are disabled by default.



**Note** This feature is currently only supported for the EPNM application. For more information about the enabling scenarios, please refer to the [EPNM user documentation](#).

### Procedure

**Step 1**

To enable FTP server:

- a) From the main menu, choose **Administration > Settings > System Settings > File Servers**
- b) Under FTP, select on the **Enable** radio button.
- c) Click **Save** to save your settings.

**Step 2**

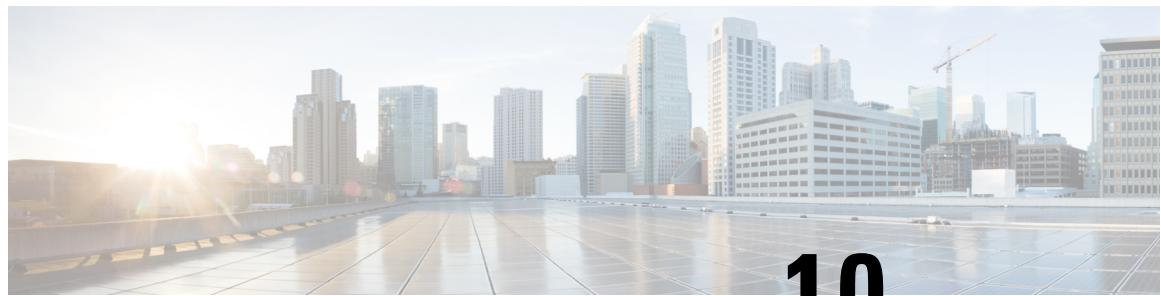
To enable SFTP server:

- a) From the main menu, choose **Administration > Settings > System Settings > File Servers**
- b) Drag the **Enable Server Upload** slider to **On** position.

**Caution**

SFTP supports upload option that allows write access to the Cisco Crosswork storage from the outside. You are recommended to use caution while enabling the upload, and it should be disabled as soon as it is no longer needed.

- c) Click **Save** to save your settings.



# CHAPTER 10

## Manage System Health

---

This section contains the following topics:

- [Monitor System and Application Health, on page 397](#)
- [View System and Network Alarms, on page 404](#)
- [Enable Trap Handling, on page 414](#)
- [Collect Audit Information, on page 414](#)

## 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 8](#).

In addition to accessing Crosswork Cluster health, you can click on the **Cisco Crosswork Platform Infrastructure** and application tiles to view more details such as microservices and alarms.

# Monitor Platform Infrastructure and Application Health

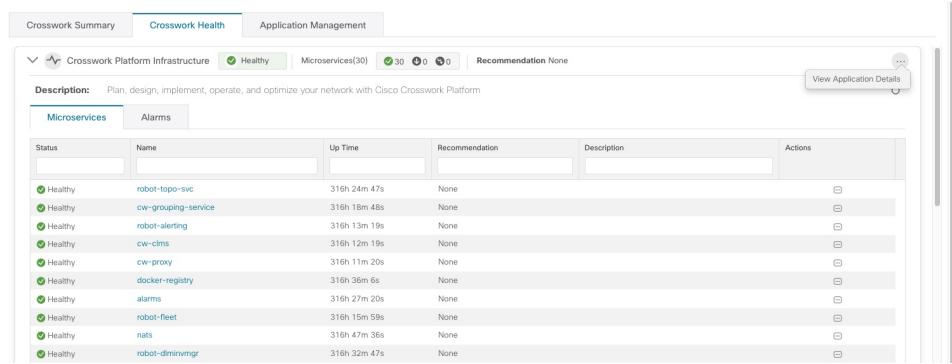
The **Crosswork Health** window (Crosswork Manager > Crosswork Health tab) provides health summaries for the Cisco Crosswork Platform Infrastructure and installed applications with the addition of microservice status details.

**Figure 139: Crosswork Health tab**



Within this window, expand an application row to view Microservice and Alarm information.

**Figure 140: Microservices Tab**



From the **Microservices** tab:

- View the list of microservices and, if applicable, associated microservices by clicking on the microservice name.
- Click to restart or obtain Showtech data and logs per microservice.

**Note** Showtech logs must be collected separately for each application.

From the **Alarms** tab:

- Click the alarm description to drill down on alarm details.
- Change status of the alarms (Acknowledge, Unacknowledge, Clear)
- 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 which Cisco Crosswork applications are installed.

**Table 38: Monitoring Dashboard Categories**

This dashboard category...	Monitors...
<b>Change Automation</b>	Playbook functions. Metrics include the number of MOP jobs executed, response latency, API calls, database activity, and so on.
<b>Optima</b>	Feature pack, traffic, and SR-PCE dispatcher functions.
<b>Collection - Manager</b>	Device-data collection functions. Metrics include telemetry collection latencies, total collection operations, memory and database activity related to telemetry, delayed collections, and so on.
<b>Health Insights</b>	Key Performance Indicator functions. Metrics include the number of KPI alerts, API calls, and so on.
<b>Infra</b>	System infrastructure messaging and database activity.
<b>Inventory</b>	Inventory manager functions. These metrics include total numbers of inventory change activities.
<b>Platform</b>	System hardware and communications usage and performance. Metrics include disk and CPU usage, database size, network and disk operations, and client/server communications.
<b>ZTP</b>	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>

### Procedure

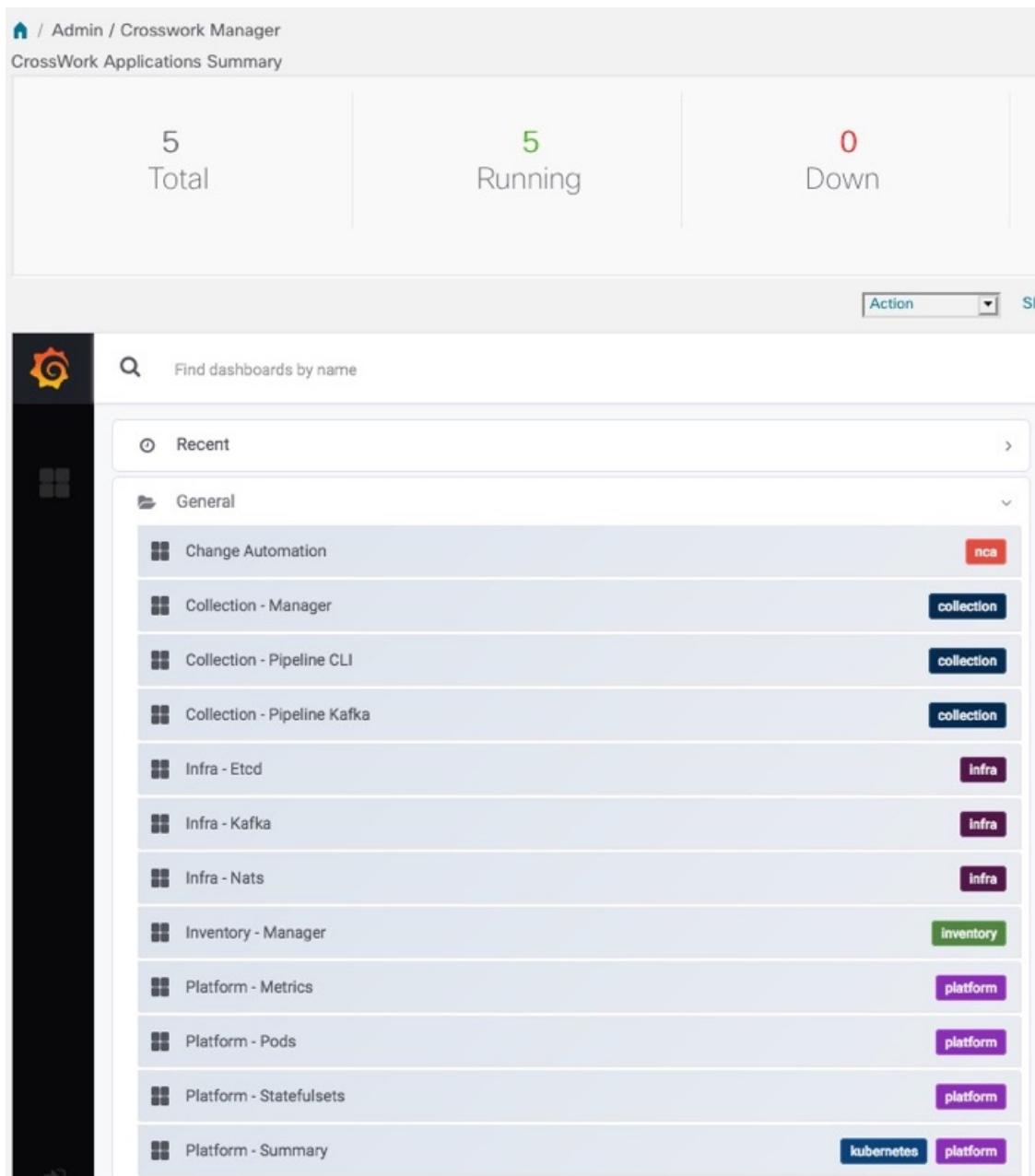
**Step 1** From the main menu, choose **Administration > Crosswork Manager > Crosswork Cluster**.

**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.



The screenshot shows the Grafana home page with the following statistics:

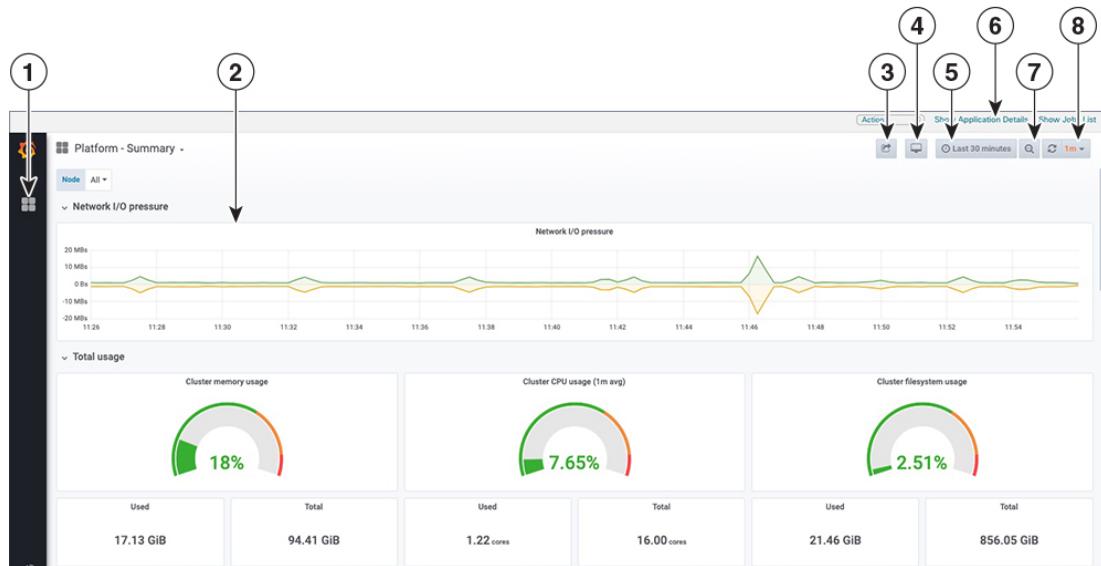
- Total: 5
- Running: 5
- Down: 0

Below the statistics is a search bar labeled "Find dashboards by name". The main content area displays a list of recent dashboards categorized as "Recent" and "General".

Category	Dashboard Name	Category Tag
Recent	Change Automation	nca
General	Collection - Manager	collection
General	Collection - Pipeline CLI	collection
General	Collection - Pipeline Kafka	collection
General	Infra - Etcd	infra
General	Infra - Kafka	infra
General	Infra - Nats	infra
General	Inventory - Manager	inventory
General	Platform - Metrics	platform
General	Platform - Pods	platform
General	Platform - Statefulsets	platform
General	Platform - Summary	kubernetes platform

**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	<b>Dashboard Icon:</b> Click the icon to re-display the dashboard list and select a different dashboard.
2	<p><b>Time Series Graph Zoom:</b> You can zoom in on a specific time period within the graph of any time series data, as follows:</p> <ol style="list-style-type: none"> <li>Click a time-period starting point in the graph line and hold down the mouse.</li> <li>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.</li> </ol> <p>To reset a zoomed time series graph to the default, click the <b>Zoom Out icon</b>.</p>
3	<p><b>Share Dashboard icon:</b> 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:</p> <ul style="list-style-type: none"> <li><b>URL Link:</b> Click the <b>Link</b> tab and then click <b>Copy</b> 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.</li> <li><b>Local Snapshot File:</b> Click the <b>Snapshot</b> tab and then click <b>Local Snapshot</b>. Grafana creates a local snapshot of the dashboard on the server. When the snapshot is ready, click <b>Copy Link</b> to copy the URL of the snapshot to your clipboard.</li> <li><b>Export to JSON File:</b> Click the <b>Export</b> tab and then click <b>Save to file</b>. 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 <b>Export for sharing externally</b> checkbox before clicking <b>Save to file</b>.</li> <li><b>View JSON File and Copy to Clipboard:</b> Click the <b>Export</b> tab and then click <b>View JSON</b> (you can choose to template data source names by selecting the <b>Export for sharing externally</b> checkbox before clicking <b>View JSON</b>). Grafana displays the exported JSON code in a popup window. Click <b>Copy to Clipboard</b> to copy the file to your clipboard.</li> </ul>

## Check System Health Example

Item	Description
4	<b>Cycle View Mode icon:</b> Click this icon to toggle between the default Grafana <b>TV</b> view mode and the <b>Kiosk</b> mode. The <b>Kiosk</b> view hides most of the Grafana menu. Press <b>Esc</b> to exit the <b>Kiosk</b> view.
5	<b>Time/Refresh Selector:</b> 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 <b>Last 30 minutes</b> or <b>Last 3 hours</b> . When you have finished making changes, click <b>Apply</b> . <b>Note</b> When making selections, remember only the last 24 hours of data is stored. If you select time ranges beyond that limit, the dashboard may be blank.
6	<b>Show Application Details:</b> Click this option to view details of the selected dashboard item.
7	<b>Zoom Out icon:</b> Click this icon to reset a zoomed time series graph back to the unzoomed state.
8	<b>Refresh icon:</b> Immediately or choose time interval to refresh the data shown. You can choose predefined refresh rates from <b>Off</b> to <b>2 Days</b> .

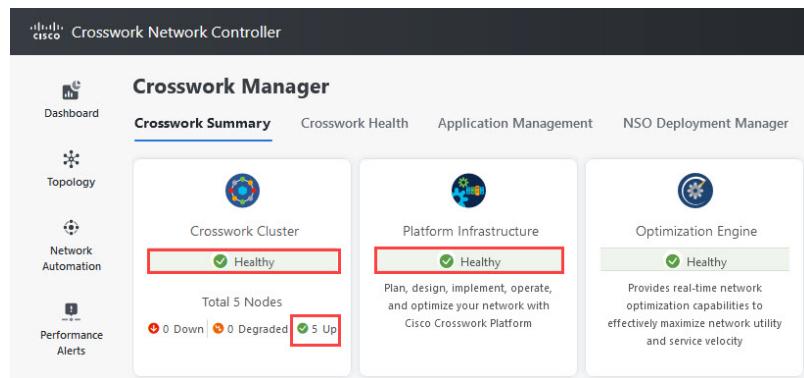
## Check System Health Example

In this example, we navigate through the various windows and what areas should be checked for a healthy Crosswork system.

### Procedure

- Step 1** Check overall system health.
- From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary** tab.
  - Check that all the nodes are in Operational state (Up) and that the Crosswork Cluster and Platform Infrastructure is Healthy.

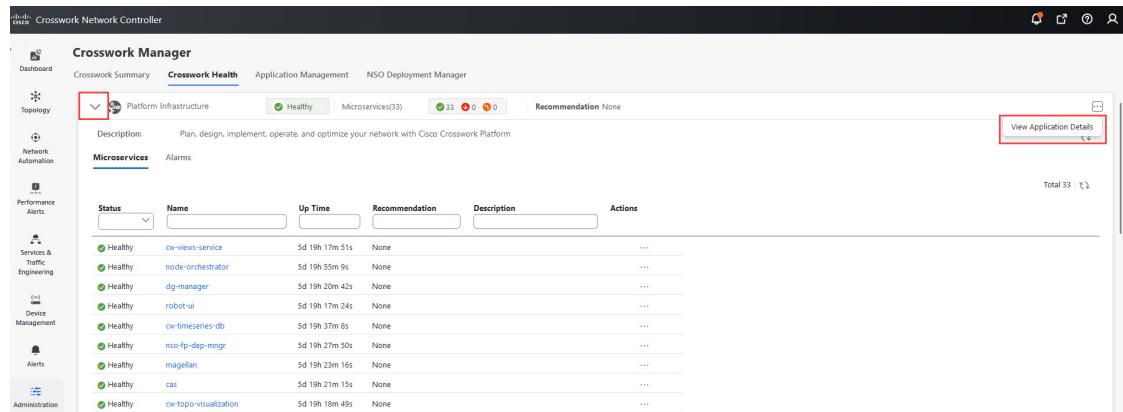
Figure 141: Crosswork Summary



**Step 2** Check and view detailed information about the microservices that are running as part of the Crosswork Platform Infrastructure.

- Click the **Crosswork Health** tab.
- Expand the Crosswork Platform Infrastructure row, click **[...]**, and select **Application Details**.

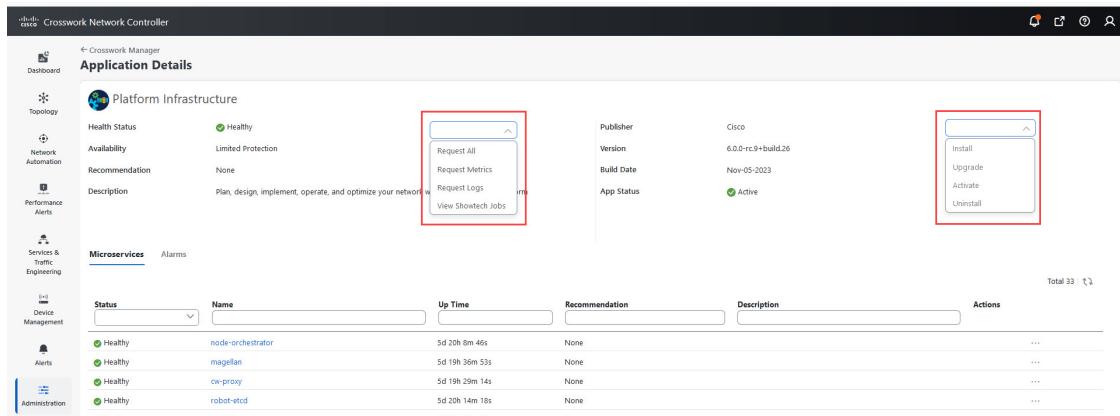
Figure 142: Crosswork Health



- 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.

## View System and Network Alarms

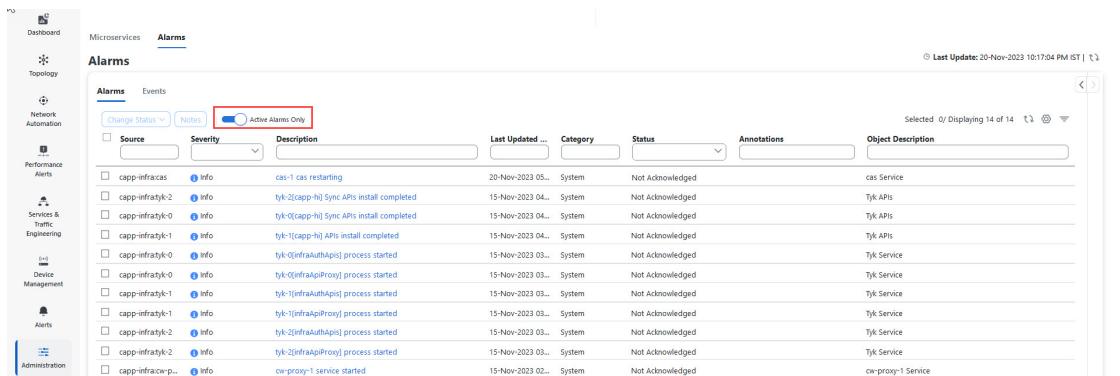
Figure 143: Application Details



**Step 3** Check and view alarms related to the microservices.

- Click the **Alarms** tab. The list only displays Crosswork Platform Infrastructure alarms. You can further filter the list by viewing only active alarms.

Figure 144: Alarms



**Step 4** View which Crosswork applications are installed.

- From the main menu, choose **Administration** > **Crosswork Manager** > **Application Management** tab and click **Applications**. This window displays all applications that have been installed. You can also click **Add File (.tar.gz)** to install more applications.

**Step 5** View the status of jobs.

- Click the **Job History** tab. This window provides the information regarding the status of jobs and the sequence of events that have been executed as part of the job process.

## 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** tab:

- Click the alarm description to drill down on alarm details.
- Change status of the alarms (Acknowledge, Unacknowledge, Clear)
- Add notes to alarms.

## System Events

To help an operator troubleshoot issues, Crosswork Infrastructure has a Syslog feature that forwards system-related events to an external server (see [Configure a Syslog Server, on page 391](#) and [Configure a Trap Server, on page 393](#)).

All the events related to the Crosswork platform are classified broadly into three categories: Day 0, Day 1, and Day 2. The following table lists the event categories (day 0, day 1, and day 2) and sample events or actions within that category:



**Note** See the [Cisco Crosswork Network Controller Supported Alarms and Events](#) document for the complete list of supported alarms and events.

**Table 39: Event Classification**

Event Classification	Sample Events and Actions
Day 0 – Events related only to Crosswork Infrastructure installation.	<ul style="list-style-type: none"> <li>Checking the status of the cluster</li> <li>Adding a worker node</li> <li>Slow disk or latency issues</li> </ul>
Day 1 – Events related to Crosswork application installation.	<ul style="list-style-type: none"> <li>Restarting a microservice</li> <li>Restarting a microservice fails</li> <li>Installing an application successfully</li> <li>Activating an application successfully</li> <li>Application is still not healthy within 3 minutes of activation</li> <li>Node drain fails</li> <li>Activating an application fails</li> <li>Removing a worker node</li> </ul>

## Sample Day 0, Day 1, and Day 2 Events

Event Classification	Sample Events and Actions
Day 2 – Events related to system operations and maintenance.	<ul style="list-style-type: none"> <li>• Node eviction</li> <li>• Node eviction clean up fails</li> <li>• Deactivating an application fails</li> <li>• Uninstallation of an application fails</li> <li>• Slow disk or network</li> <li>• Node removal</li> <li>• Node insertion</li> <li>• Node drain fails</li> <li>• K8S ETCD clean up</li> <li>• Node removal fails</li> <li>• Node deletion fails</li> <li>• Deactivating an application successfully</li> <li>• Uninstalling an application successfully</li> </ul>

## 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 40: 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	<pre> &lt;time_stamp&gt; &lt;hosting_hybrid_node&gt; &lt;time_stamp&gt; &lt;crosswork_VIP&gt; orchestrator-capp-infra - b54ec903-9e0f-49b8-aaf3-1d72cf644c28 vm4wkr-0 'Successfully added new VM into Inventory: vm4wkr'</pre>
Recommendation	Monitor and confirm that the VM node appears in the UI with a healthy status.

**Table 41: Slow Disk or Latency in Network Issues**

Severity	Critical
Description	<p>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.</p> <p>This message can be found in the firstboot.log file.</p>
Sample Alarm	Not applicable
Sample Syslog Message	Not applicable
Recommendation	<p>This issue must be addressed before further operations can be made on the system. Do the following:</p> <ul style="list-style-type: none"> <li>Check that disk storage and network SLA requirements are met.</li> <li>Confirm that the observed bandwidth is the same as what is provisioned between the nodes.</li> <li>If using RAID, confirm it is RAID 0.</li> </ul>

## Day 1 Events

**Table 42: Removing a Worker Node**

Severity	Major
Description	This event occurs when a VM node is erased.
Sample Alarm	None
Sample Syslog Message	<pre>&lt;time_stamp&gt; &lt;hosting_hybrid_node&gt; &lt;time_stamp&gt; &lt;crosswork_VIP&gt; 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 []]'</pre>
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 43: Adding an Application—Success**

Severity	Information
Description	This event occurs when an application is added successfully.

## Sample Day 0, Day 1, and Day 2 Events

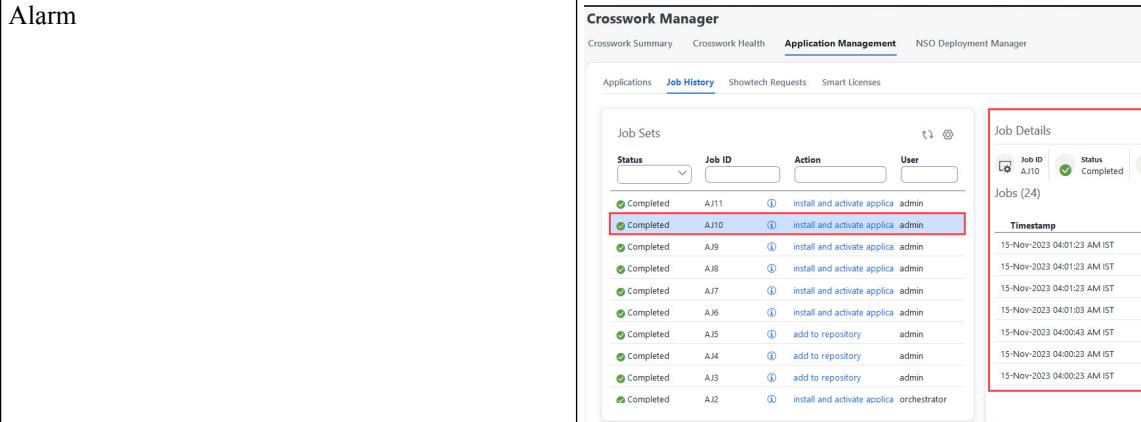
Alarm	
Syslog Message	<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> CLUSTER-CLUSTER - 627b2140-a906-4a96-b59b-1af22f2af9f6 CLUSTER-99 'job_type=INSTALL_AND_ACTIVATE_APPLICATION,manager=app_manager: ,user=admin,policyId=admin,backend=local,loginTime=2021-02- 28T09:34:54Z,payload={"package_identifier":{"id":"cappztp"," version":"1.1.0-prerelease.259+build.260"} } [accepted] '
Recommendation	None

Table 44: Adding an Application—Failure

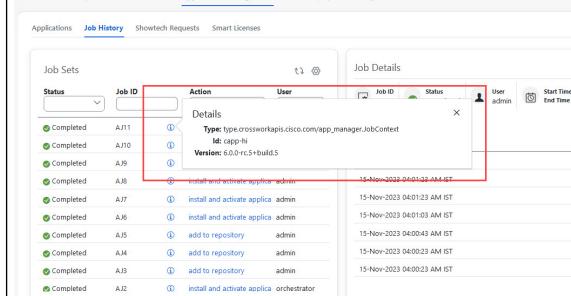
Severity	Information
Description	This event occurs when an application cannot be added.
Sample Alarm	
Sample Syslog Message	None
Recommendation	After fixing the error, try adding the application again.

Table 45: 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 46: 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	<p>Do the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Uninstall the application and then try installing the application again.</li> </ul>

**Table 47: 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 48: 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	<ul style="list-style-type: none"> <li>• Node Drain Failed</li> <li>• K8s ETCD Cleanup Failed on Node Removal</li> <li>• Node Delete</li> </ul>
Syslog Message	<pre>&lt;time_stamp&gt; &lt;hosting_hybrid_node&gt; &lt;time_stamp&gt; &lt;crosswork_VIP&gt; orchestrator-Crosswork Health Manager - b062232f-54dc-49b2-8283- 506b7bf672a6 astackserver-0-0 'astackserver-0 health is degraded.'</pre>
Recommendation	Monitor the operation. If the drain is a result of eviction, erase the respective node and insert a new one.

**Table 49: 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	<pre>&lt;time_stamp&gt; &lt;hosting_hybrid_node&gt; &lt;time_stamp&gt; &lt;crosswork_VIP&gt; orchestrator-Crosswork Health Manager - b062232f-54dc-49b2-8283- 506b7bf672a6 astackserver-0-0 'astackserver-0 health is degraded.'</pre>
Recommendation	Try erasing the node again.

**Table 50: Node Eviction—Failure**

Severity	Critical
----------	----------

Description	<p>In this scenario we assume that one of the hybrid nodes fails.</p> <p>This event occurs if the node has been down for more than 5 minutes and it is automatically taken out of service.</p> <p>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.</p>
Sample Alarm	<ul style="list-style-type: none"> <li>Node Eviction Cleanup Failure</li> <li>K8S ETCD Cleanup Failed on Node Removal</li> </ul>
Syslog Message	None
Recommendation	Erase the faulty node and insert a new VM.

**Table 51: 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 52: 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 53: Deactivating an Application—Success**

Severity	Minor
----------	-------

## Sample Day 0, Day 1, and Day 2 Events

Description	This event occurs when an application is deactivated.
Sample Alarm	None
Sample Syslog Message	<pre>&lt;time_stamp&gt; &lt;hosting_hybrid_node&gt; &lt;time_stamp&gt; &lt;crosswork_VIP&gt; 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]'</pre>
Recommendation	None

**Table 54: Deactivating an Application—Failure**

Severity	Critical
Description	This event occurs when an application cannot be deactivated. This can occur if microservices or pods are still running.
Sample Alarm	None
Syslog Message	None
Recommendation	<p>Do the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Uninstall the application and then try installing the application again.</li> </ul>

**Table 55: Slow Disk or Latency in Network Issues**

Severity	Critical
Description	<p>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.</p> <p>This message can be found in the firstboot.log file.</p>
Sample Alarm	Not applicable
Sample Syslog Message	Not applicable

Recommendation	<p>This issue must be addressed before further operations can be made on the system. Do the following:</p> <ul style="list-style-type: none"> <li>• Check that disk storage and network SLA requirements are met.</li> <li>• Confirm that the observed bandwidth is the same as what is provisioned between the nodes.</li> <li>• If using RAID, confirm it is RAID 0.</li> </ul>
----------------	---



**Note** There is a one-time check performed to ensure the hardware attempts to meet the Disk SLA. If this fails, a critical alarm is issued. User can address the alarm as needed and manually clear the alarm.

**Table 56: 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: <ul style="list-style-type: none"> <li>• K8S ETCD Cleanup Failed on Node Removal</li> <li>• Alarm Node Delete</li> </ul>
Syslog Message	None
Recommendation	Monitor operation.

**Table 57: 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 58: Restart Microservices—Failure**

Severity	Warning
Description	This event occurs when someone restarts a microservice or pod and the operation fails.

Sample Alarm	None
Sample Syslog Message	None
Recommendation	Restart the microservices or pods. You may have to do this a few times to see if it recovers.

## Enable Trap Handling

In addition to UI options, REST APIs, and Syslogs, Cisco Crosswork also provides the capability to generate SNMP traps for the events/alarms to notify the application and cluster health.

Crosswork supports using SNMPv3 and SNMPv2 to send the traps. The alarms and events are filtered based on the criteria set by user and converted to traps and sent to the trap server (see [Configure a Trap Server, on page 393](#)) using the alarm model in CISCO-EPM-NOTIFICATION-MIB. For more information, see [Cisco EPM Notification MIB, on page 463](#).

## 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 398](#).

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 59: 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).

Field	Description
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: <ul style="list-style-type: none"> <li>In the sample audit log entry for Cisco Crosswork Change Automation and Health Insights, the <b>playbook</b> field refers to the playbook that Change Automation executed.</li> <li>In the UI audit log entry for Crosswork Optimization Engine, <b>data</b> is a field that refers to the creation details of an SR-TE policy and its attributes.</li> </ul>

### Audit Log Location

Crosswork stores audit logs in `/var/log/audit/audit.log`, under the respective application pods. For example:

- The sample Change Automation audit log is in the `<robot-nca>` data directory under the pod.
- The sample Crosswork Optimization Engine UI audit log is in the `optima-uiservice` pod; the RESTCONF API audit log is under the `optima-restconf` pod.

In addition to the individual application audit logs, Cisco Crosswork collects all audit log files are once each hour. Crosswork stores them as separate gzipped tar files in the following data directory:  
`/mnt/robot_datafs/<app-name>/<instance>/auditlogs/auditlogs.tar.gz`

Crosswork collects audit log files based on the specified maximum size and number of backups for each application. For example: **MaxSize:20 megabytes** and **MaxBackups: 5**.

## View Audit Log

The **Audit Log** window tracks the following AAA-related events:

- Create, update, and delete users
- Create, update, and delete roles
- User login activites - login, logout, login failure due to maximum active session limit, and account locked due to maximum login failures.
- Source IP - IP address of the machine from where the action was performed. This column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork. This check box is available in the **Source IP** section of the **Administration > AAA > Settings** page.
- Password modification by user

To view the audit log, perform the following steps:

## Procedure

---

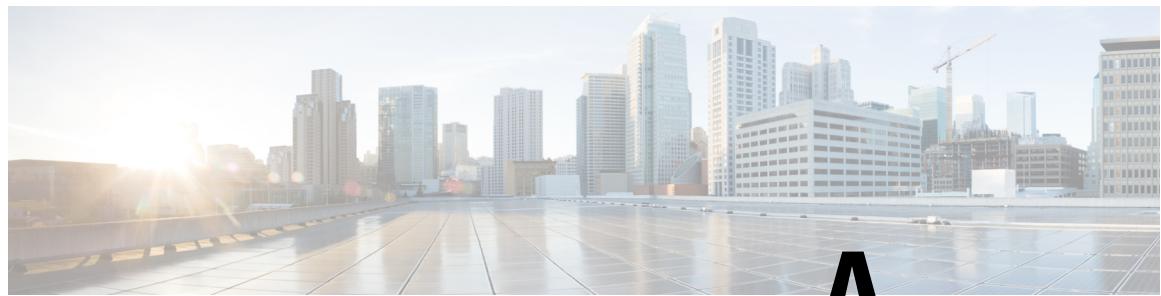
**Step 1** From the main menu, choose **Administration > Audit Log**.

The **Audit Log** window is displayed.

**Step 2** Click  to filter the results based on your query.

---





## APPENDIX A

# Configure Crosswork Data Gateway Instance

A Cisco Crosswork Data Gateway instance is created as a standalone instance and can be geographically separate from the controller application (the controller application could be Cisco Crosswork Infrastructure or Crosswork Cloud). This instance is capable of connecting to the controller application which will enable data collection from the network.

This chapter contains the following topics:

- [Use the Interactive Console, on page 419](#)
- [Manage Crosswork Data Gateway Users, on page 420](#)
- [View Current System Settings, on page 423](#)
- [Change Current System Settings, on page 425](#)
- [Troubleshooting Crosswork Data Gateway VM, on page 442](#)

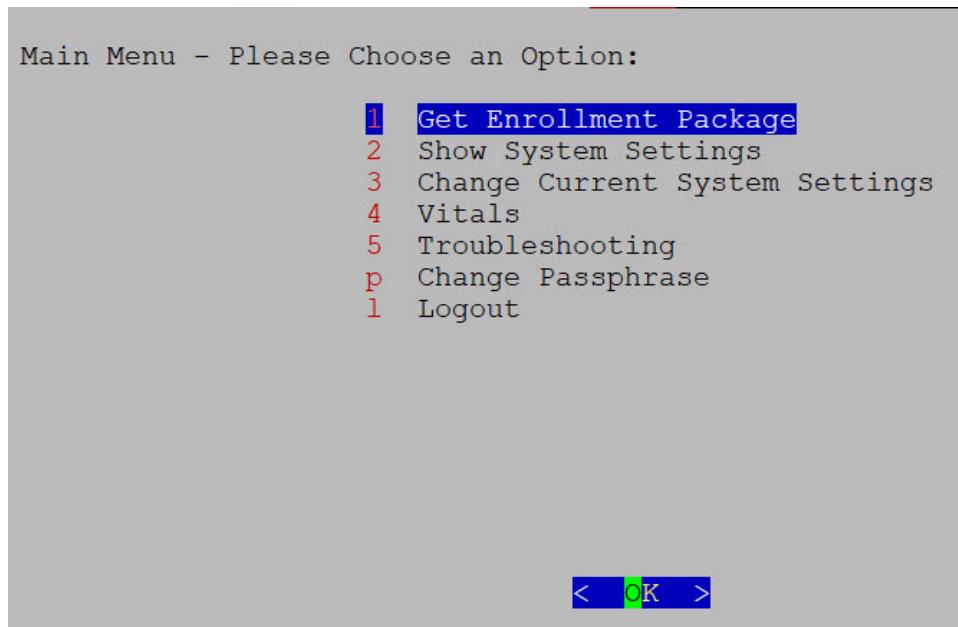
## Use the Interactive Console

Cisco Crosswork Data Gateway launches an interactive console upon successful login. The interactive console displays the **Main Menu** as shown in the following figure:



**Note** The Main Menu shown here corresponds to **dg-admin** user. It is different for **dg-oper** user as the operator does not have same privileges as the administrator. See Table [Table 60: Permissions Per Role, on page 421](#).

Figure 145: Interactive Console - Main Menu



The Main Menu presents the following options:

1. Get Enrollment Package
2. Show System Settings
3. Change Current System Settings
4. Vitals
5. Troubleshooting
- p. Change Passphrase
- l. Log out



**Important** When using an IPv6 address, it must be surrounded by square brackets ([1::1]).

## Manage Crosswork Data Gateway Users

This section contains the following topics:

- [Supported User Roles, on page 420](#)
- [Change Passphrase, on page 423](#)

## 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 starting and shutting down the Cisco Crosswork Data Gateway VM, registering an application, applying authentication certificates, configuring server settings, and performing a kernel upgrade.
- **Operator:** The **dg-oper** user is also created by default during the initial VM bring up. This user can review the health of the Cisco Crosswork Data Gateway, retrieve error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.

**Note**

- User credentials are configured for both the user accounts during Cisco Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

*Table 60: Permissions Per Role*

Permissions	Administrator	Operator
Get Enrollment Package	✓	✓
<b>Show system settings</b>		
vNIC Addresses	✓	✓
NTP		
DNS		
Proxy		
UUID		
Syslog		
Certificates		
First Boot Provisioning Log		
Timezone		
<b>Change Current System Settings</b>		

Permissions	Administrator	Operator
Configure NTP	✓	✗
Configure DNS		
Configure Control Proxy		
Configure Static Routes		
Configure Syslog		
Create new SSH keys		
Import Certificate		
Configure vNIC MTU		
Configure Timezone		
Configure Password Requirements		
Configure Simultaneous Login Limits		
Configure Idle Timeout		
Configure Login Check Frequency		
Configure Interface Address		
<b>Vitals</b>		
Docker Containers	✓	✓
Docker Images		
Controller Reachability		
NTP Reachability		
Route Table		
ARP Table		
Network Connections		
Disk Space Usage		
Linux services		
NTP Status		
System Uptime		
<b>Troubleshooting</b>		

Permissions	Administrator	Operator
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Remove All Non-Infra Containers and Reboot VM	✓	✗
Reboot VM	✓	✗
Export auditd logs	✓	✓
Re-enroll Data Gateway	✓	✓
Enable TAC Shell Access	✓	✗
Change Passphrase	✓	✓

## Change Passphrase

Both administrator and operator users can change their own passphrases but not each others'.

Follow these steps to change your passphrase:

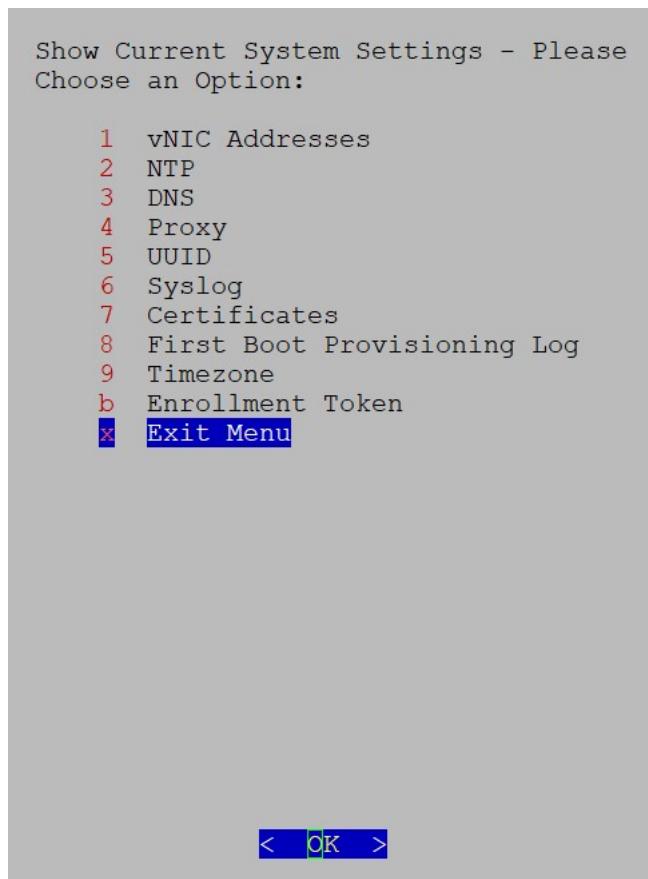
### Procedure

- 
- Step 1** From the Main Menu, select **Change Passphrase** and click **OK**.
- Step 2** Enter your current password and press **Enter**.
- Step 3** Enter new password and press **Enter**. Re-type the new password and press **Enter**.
- 

## View Current System Settings

Crosswork Data Gateway allows you to view the following settings:

Figure 146: Show Current System Settings Menu



Follow these steps to view the current system settings:

## Procedure

**Step 1** From the Main Menu, select **Show System Settings**.

**Step 2** In the prompt, click **OK** to open the **Show Current System Settings** menu.

**Step 3** Select the setting you want to view.

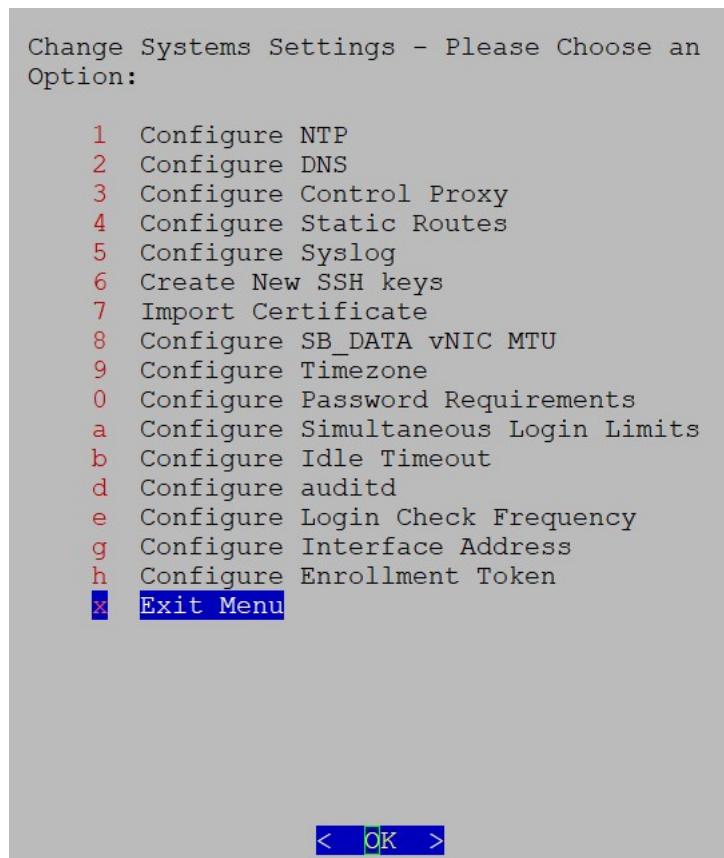
Setting Option	Description
1 vNIC Addresses	Displays the vNIC configuration, including address information.
2 NTP	Displays currently configured NTP server details.
3 DNS	Displays DNS server details.
4 Proxy	Displays proxy server details (if any configured).
5 UUID	Displays the system UUID.

Setting Option	Description
6 Syslog	Displays the Syslog forwarding configuration. If no Syslog forwarding is configured, this will display only "# Forwarding configuration follows" on screen.
7 Certificates	Provides options to view the following certificate files: <ul style="list-style-type: none"> <li>• Crosswork Data Gateway signing certificate file</li> <li>• Controller signing certificate file</li> <li>• Controller SSL/TLS certificate file</li> <li>• Syslog certificate file</li> <li>• Collector certificate file</li> </ul>
8 First Boot Provisioning Log	Displays the content of the first boot log file.
9 Timezone	Displays the current timezone setting.
b Enrollment Token	<p><b>Attention</b>  This menu option is for users of Crosswork Data Gateway for Cloud applications.</p> <p>Displays the token that Crosswork Data Gateway used to enroll with Crosswork Cloud.</p>

## Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

Figure 147: Change System Settings Menu



Follow these steps to modify the current system settings:

## Procedure

**Step 1** From the Main Menu, select **3 Change Current System Settings**.

**Step 2** Select the setting that you want to modify.

- NTP
- DNS
- Control proxy
- Static routes
- Syslog
- SSH keys
- Certificate
- vNIC MTU
- Timezone

- Password requirements
- Simultaneous login limits
- Idle timeout
- Auditd
- Login check frequency
- Interface address
- Enrollment token

**Note**

This Enrollment token menu option is for users of Crosswork Data Gateway for Cloud applications.

**Note**

- Crosswork Data Gateway system settings can only be configured by the administrator.
- When using an IPv6 address, it must be surrounded by square brackets ([1::1]).
- In the Settings options where you require to use SCP, if you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,  
`-P55 user@host:path/to/file`  
Where 55 is a custom port.

---

## Configure NTP

It is important that NTP time be synchronized with the controller application and its Crosswork Data Gateway instances. If not, then session handshake doesn't happen and functional images are not downloaded. In such cases, error message clock time not matched and sync failed is logged in controller-gateway.log. To access log files, see [Run show-tech, on page 447](#). 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 439](#). 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:

### Procedure

---

**Step 1** From the **Change Current System Settings** Menu, select **Configure NTP**.

**Configure DNS**

**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

**Procedure**

**Step 1** From the **Change Current System Settings** menu, select **Configure DNS** and click **OK**.

**Step 2** Enter the new DNS server address(es) and domain.

**Step 3** Click **OK** to save the settings.

## Configure Control Proxy

If you have not configured a proxy server during installation, avail this option to set up a proxy sever:

**Procedure**

**Step 1** From the **Change Current System Settings** menu, select **Configure Control Proxy** and click **OK**.

**Step 2** Click **Yes** for the following dialog if you wish to proceed. Click **cancel** otherwise.

**Step 3** Enter the new Proxy server details:

- Server URL
- Bypass addresses
- Proxy username
- Proxy passphrase

**Step 4** Click **OK** to save the settings.

# Configure Static Routes

The static routes are configured when Crosswork Data Gateway receives add/delete requests from the collectors. The **Configure Static Routes** option from the main menu can be used for troubleshooting purpose.



**Caution** Static routes configured using this option are lost when the Crosswork Data Gateway reboots.

## Add Static Routes

Follow the steps to add static routes:

### Procedure

- 
- Step 1** From the **Change Current System Settings** menu, select **4 Configure Static Routes**.
  - Step 2** To add a static route, select **a Add**.
  - Step 3** Select the interface for which you want to add a static route.
  - Step 4** Select the IP version.
  - Step 5** Enter IPv4 or IPv6 subnet in CIDR format when prompted.
  - Step 6** Click **OK** to save the settings.
- 

## Delete Static Routes

Follow the steps to delete a static route:

### Procedure

- 
- Step 1** From the **Change Current System Settings** Menu, select **4 Configure Static Routes**.
  - Step 2** To delete a static route, select **d Delete**.
  - Step 3** Select the interface for which you want to delete a static route.
  - Step 4** Select the IP version.
  - Step 5** Enter IPv4 or IPv6 subnet in CIDR format.
  - Step 6** Click **OK** to save the settings.
- 

# Configure Syslog

You can configure the remote servers during the Day0 installation through the configuration file. If you want to modify the Syslog server list, port number, protocol, and certificate file in Day1 installation or later use the Interactive Console.



**Note** For any Syslog server configuration with IPv4 or IPv6 support for different Linux distributions, please refer to your system administrator and configuration guides.

Follow the steps to configure Syslog:

### Before you begin

Crosswork Data Gateway lets you configure multiple servers through the following modes:

- **Simultaneous:** Crosswork Data Gateway sends messages to all the configured Syslog server addresses. When one of the servers is unresponsive, the message is queued to the disk until the servers are response.
- **Failover:** Crosswork Data Gateway sends message to the first Syslog server address. If the server is not available, the message is sent to the subsequent configured address. When all the servers in the list are unresponsive, the message is queued to the disk until the servers are response.

### Procedure

**Step 1** From the **Change Current System Settings** menu, select **5 Configure Syslog**.

**Step 2** In the **Use Syslog** window, select **True** to continue configuring the Syslog server.

**Step 3** In the **Select Syslog Multiserver Mode** window, select **Simultaneous** or **Failover**.

**Step 4** Enter the values for the following Syslog attributes:

- Server address or hostname: Space-delimited list of IPv4 or IPv6 address of Syslog server accessible from the management interface.
- Port: Port number of the Syslog server
- Protocol: Use UDP, TCP, or RELP when sending system logs.
- Use Syslog over TLS?: Use TLS to encrypt Syslog traffic.
- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
- Syslog Root Certificate File URI: PEM formatted root cert of Syslog server retrieved using SCP.
- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

**Step 5** Click **OK** to save the settings.

## Create New SSH Keys

Creating new SSH keys will remove the current keys.

Follow the steps to create new SSH keys:

## Procedure

**Step 1** From the **Change Current System Settings** Menu, select **6 Create new SSH keys**.

**Step 2** Click **OK**. Crosswork Data Gateway launches an auto-configuration process that generates new SSH keys.

## Import Certificate

Updating any certificate other than Controller Signing Certificate causes a collector restart.

Crosswork Data Gateway allows you to import the following certificates:

- Controller signing certificate file
- Controller SSL/TLS certificate file
- Syslog certificate file
- Proxy certificate file

## Procedure

**Step 1** From the **Change Current System Settings** Menu, select **Import Certificate**.

**Step 2** Select the certificate you want to import.

**Step 3** Enter 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.

## Procedure

**Step 1** From the **Change Current System Settings** menu, select **Configure vNIC1 MTU**.

**Step 2** Enter the vNIC2 MTU value.

- Step 3** Click **OK** to save the settings.

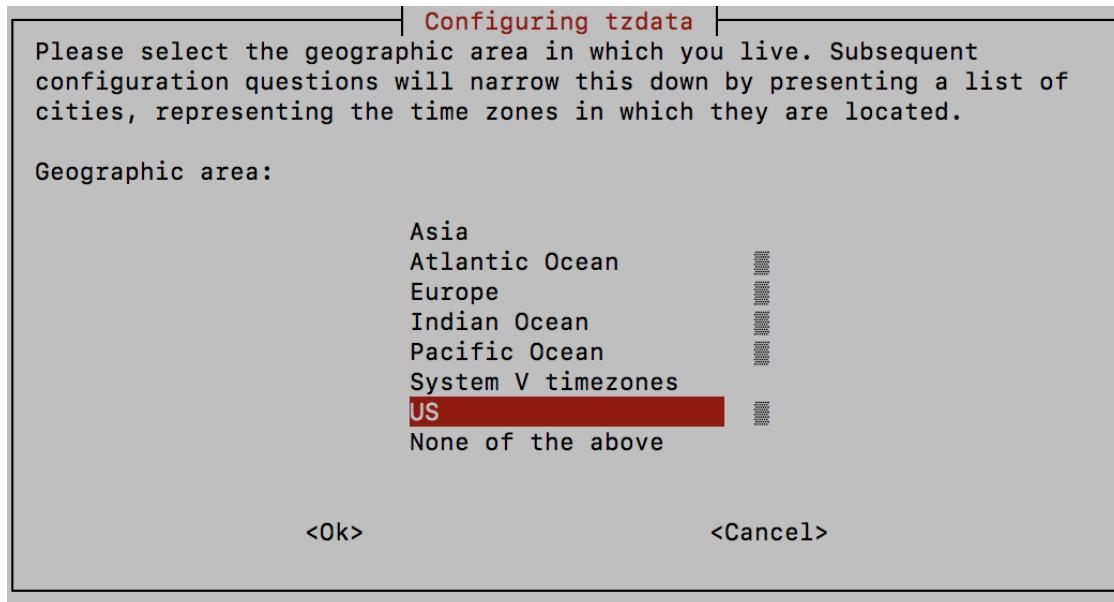
## Configure Timezone of the Crosswork Data Gateway VM

The Crosswork Data Gateway VM first launches with default timezone as UTC. Update the timezone with your geographical area so that all Crosswork Data Gateway processes (including the showtech logs) reflect the timestamp corresponding to the location you have chosen.

### Procedure

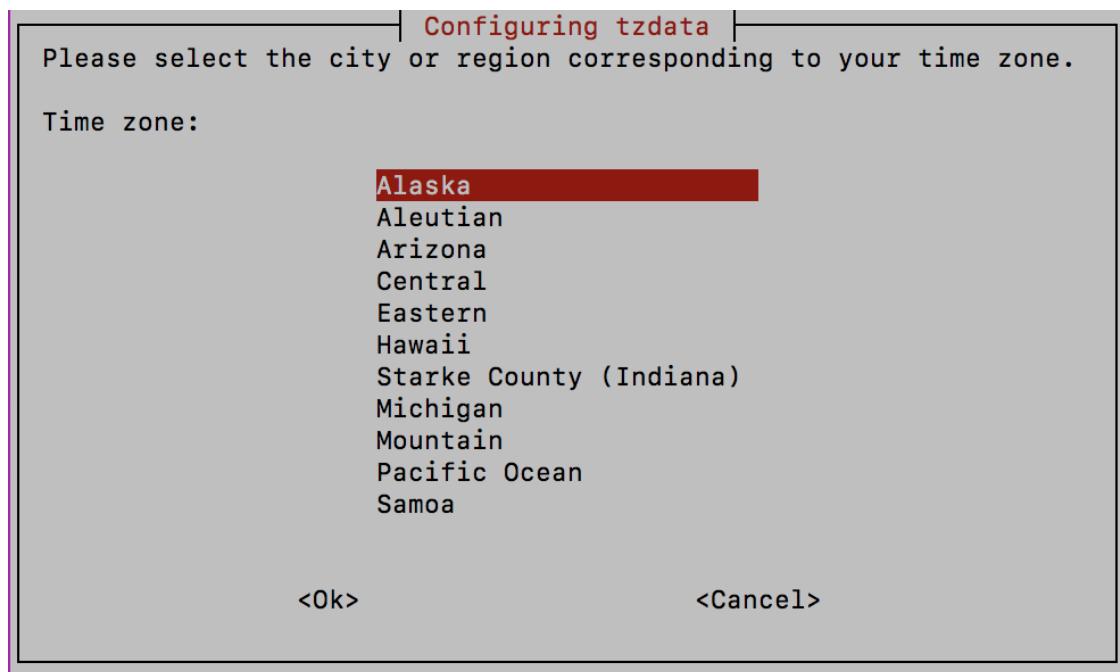
- Step 1** Log in to the Crosswork Data Gateway VM.  
**Step 2** In the Crosswork Data Gateway VM interactive menu, select **3 Change Current System Settings**.  
**Step 3** From the menu, select **9 Timezone**.  
**Step 4** Select the geographic area in which you live.

*Figure 148: Timezone Settings - Geographic Area Selection*



- Step 5** Select the city or region corresponding to your timezone.

Figure 149: Timezone Settings - Region Selection



**Step 6** Select **OK** to save the settings.

**Step 7** Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone. See *Reboot Crosswork Data Gateway VM* section in [Cisco Crosswork Network Controller 6.0 Administration Guide](#).

**Step 8** Log out of the Crosswork Data Gateway VM.

## Configure Password Requirements

You can configure the following password requirements:

- Password Strength
- Password History
- Password expiration
- Login Failures

### Procedure

**Step 1** From **Change Current System Settings** menu, select **Configure Password Requirements**.

**Step 2** Select the password requirement you want to change.

Set the options you want to change:

- **Password Strength**

## Configure Simultaneous Login Limits

- Min Number of Classes
- Min Length
- Min Changed Characters
- Max Digit Credit
- Max Upper Case Letter Credit
- Max Lower Case Letter Credit
- Max Other Character Credit
- Max Monotonic Sequence
- Max Same Consecutive Characters
- Max Same Class Consecutive Characters
  
- **Password History**
  - Change Retries
  - History Depth
  
- **Password expiration**
  - Min Days
  - Max Days
  - Warn Days
  
- **Login Failures**
  - Login Failures
  - Initial Block Time (sec)
  - Address Cache Time (sec)

**Step 3** Click **OK** to save the settings.

---

## Configure Simultaneous Login Limits

By default, Crosswork Data Gateway supports 10 simultaneous sessions for the **dg-admin** and **dg-oper** user on each VM. To change this:

### Procedure

---

- Step 1** From the **Change Current System Settings** menu, select a **Configure Simultaneous Login Limits**.
- Step 2** In the window that appears, enter the number of simultaneous sessions for the **dg-admin** and **dg-oper** user.

- 
- Step 3** Select **Ok** to save your changes.
- 

## Configure Idle Timeout

### Procedure

---

- Step 1** From the **Change Current System Settings** menu, select **b Configure Idle Timeout**.
- Step 2** Enter the new value of idle timeout in the window that appears.
- Step 3** Enter **Ok** to save your changes.
- 

## Configure Remote Auditd Server

Use this procedure to configure the auditd daemon export to a remote server.

### Procedure

---

- Step 1** From the **Change Current System Settings** menu, select **c Configure auditd**.
- Step 2** Enter the following details:
- Remote auditd server address.
  - Remote auditd server port.
- Step 3** Select **OK** to save your changes.
- 

## Configure Login Frequency

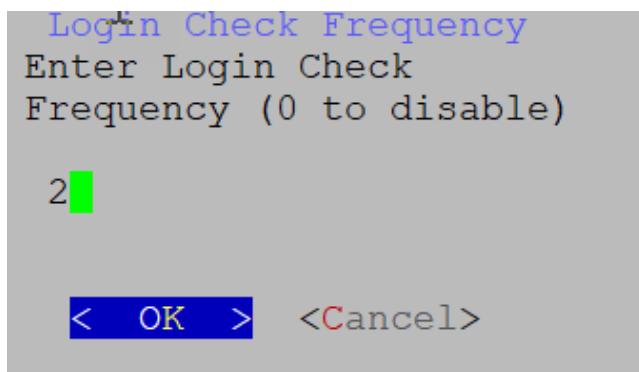
You can configure the number of permissible log in attempts the user can make after a log in failure.

### Procedure

---

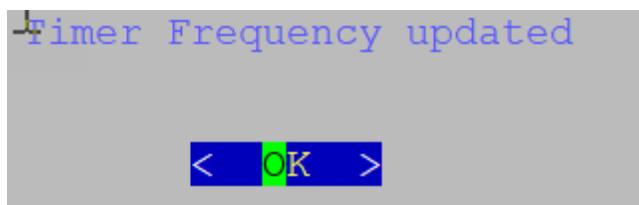
- Step 1** From the **Change Current System Settings** menu, select **Configure Login Check Frequency** and click **OK**.
- Step 2** In the **Login Check Frequency** window, enter the number of log in attempts you want to monitor. To disable the feature, enter 0.

Figure 150: Login Check Frequency Window



After the timer is updated, a confirmation window appears.

Figure 151: Timer Frequency Updated Window



## Configure Interface Address

After you have deployed a Crosswork Data Gateway instance, you can reconfigure the interfaces that are already associated with an instance. When you reconfigure an interface, you can change its name, associate IP address, or access the security group that is associated with an interface.

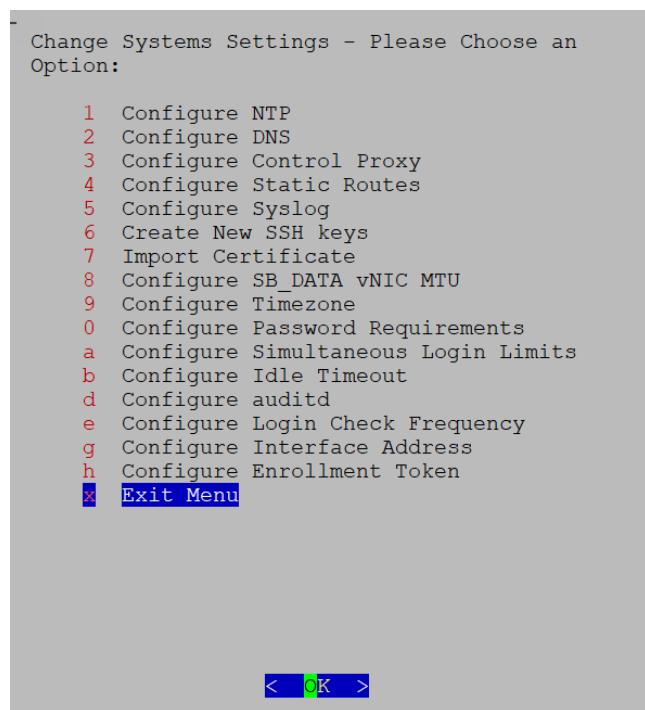
### Before you begin

- All the devices must be detached from the Crosswork Data Gateway instance for which you want to reconfigure the interface address.
- The Crosswork Data Gateway instance must be in the maintenance mode.

### Procedure

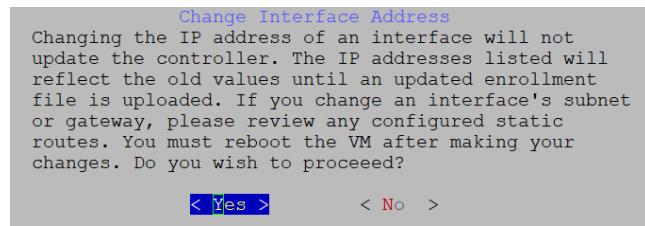
- 
- Step 1** From the **Change System Settings** menu, select **Configure Interface Address**.

Figure 152: Change System Settings Menu



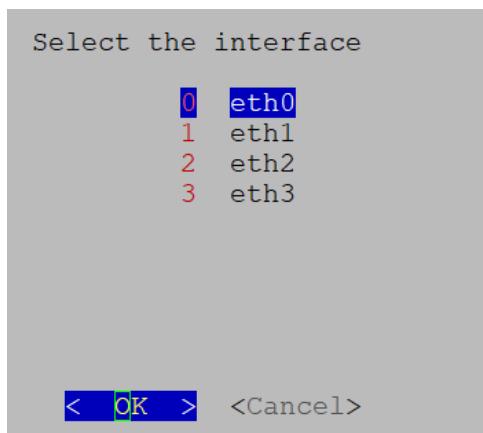
**Step 2** In the **Change Interface Address** confirmation box, click **Yes**.

Figure 153: Change Interface Address Confirmation Message



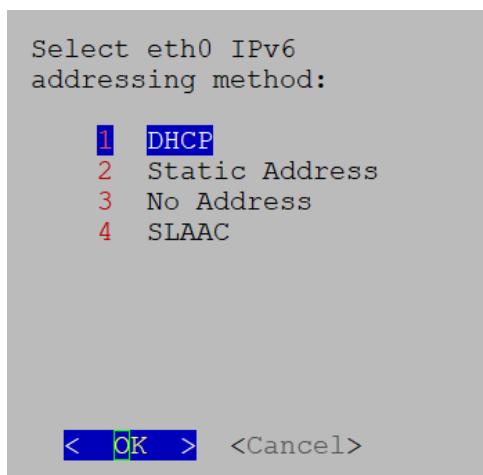
**Step 3** Select the interface that you want to reconfigure and click **OK**. The options are `eth0`, `eth1`, `eth2`, or `eth3`.

Figure 154: Interface Selection Menu



**Step 4** Select the <interface> IPv4 addressing method. The options are `DHCP`, `Static Address`, or `No address`. Cisco recommends that you select the option that you had specified during the Day0 installation.

Figure 155: IPv6 Address Selection



**Step 5** Enter the IPv4 address and click **OK**.

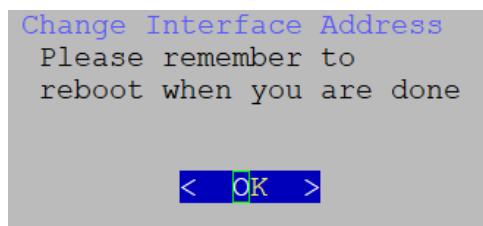
**Step 6** Enter the IPv4 Netmask address and click **OK**.

**Step 7** In the **Skip <interface> IPv4 gateway configuration confirmation** box, select `True` or `False` and click **OK**.

**Step 8** If you have selected `True` in the previous step, specify the IPv4 gateway address.

**Step 9** In the **Change Interface Address confirmation** box, click **OK**.

Figure 156: Confirmation Message



---

After the interface is configured, make sure to reboot the VM.

## View Crosswork Data Gateway Vitals

Follow these steps to view Cisco Crosswork Data Gateway vitals:

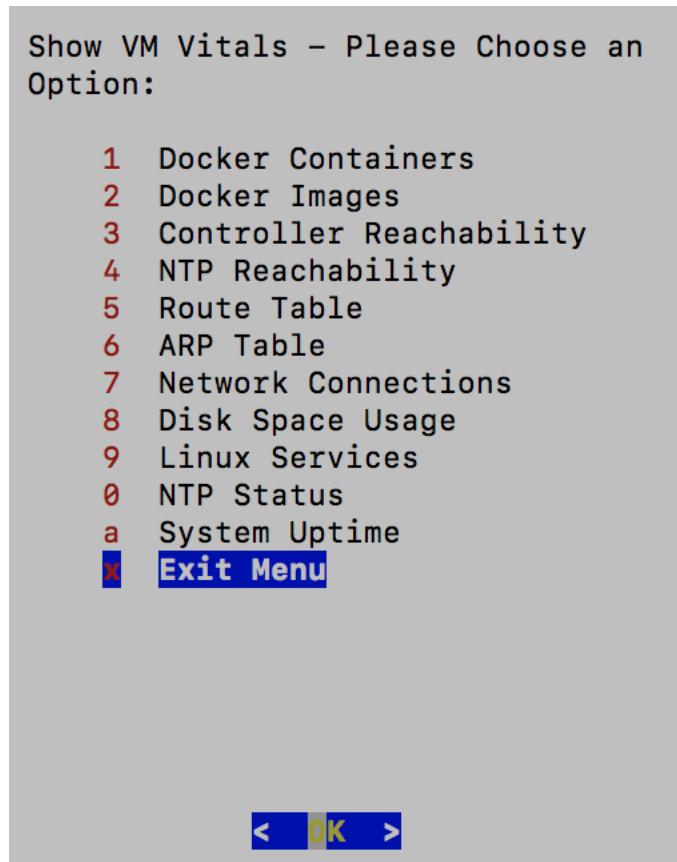
### Procedure

---

**Step 1** From the Main Menu, select **Vitals**.

**Step 2** From the **Show VM Vitals** menu, select the vital you want to view.

Figure 157: Show VM Vitals Menu



Vital	Description
Docker Containers	<p>Displays the following vitals for the Docker containers currently instantiated in the system:</p> <ul style="list-style-type: none"> <li>• Container ID</li> <li>• Image</li> <li>• Name</li> <li>• Command</li> <li>• Created Time</li> <li>• Status</li> <li>• Port</li> </ul>

Vital	Description
Docker Images	<p>Displays the following details for the Docker images currently saved in the system:</p> <ul style="list-style-type: none"> <li>• Repository</li> <li>• Image ID</li> <li>• Created Time</li> <li>• Size</li> <li>• Tag</li> </ul>
Controller Reachability	<p>Displays the results of controller reachability test run:</p> <ul style="list-style-type: none"> <li>• Default IPv4 gateway</li> <li>• Default IPv6 gateway</li> <li>• DNS server</li> <li>• Controller</li> <li>• Controller session status</li> </ul>
NTP Reachability	<p>Displays the result of NTP reachability tests:</p> <ul style="list-style-type: none"> <li>• NTP server resolution</li> <li>• Ping</li> <li>• NTP Status</li> <li>• Current system time</li> </ul>
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	<p>Displays the status of the following Linux services:</p> <ul style="list-style-type: none"> <li>• NTP</li> <li>• SSH</li> <li>• Syslog</li> <li>• Docker</li> <li>• Cisco Crosswork Data Gateway Infrastructure containers.</li> </ul>
Check NTP Status	Displays the NTP server status.

Vital	Description
Check System Uptime	Displays the system uptime.

## Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu.



**Note** The image shows the Troubleshooting menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table [Table 60: Permissions Per Role](#), on page [421](#).

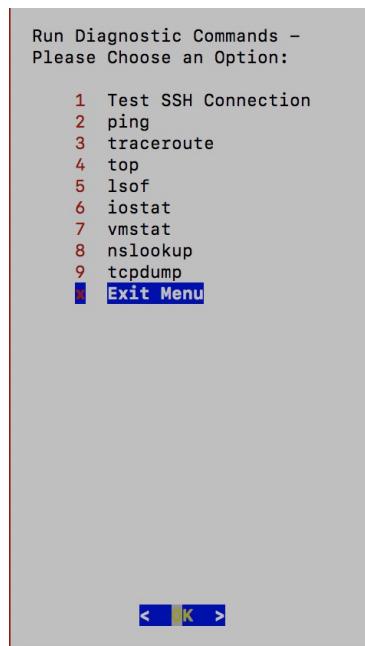
The **Troubleshooting** menu that provides the following options:

- [Run Diagnostic Commands](#), on page [442](#)
- [Run show-tech](#), on page [447](#)
- [Reboot Crosswork Data Gateway VM](#), on page [447](#)
- [Shutdown the Crosswork Data Gateway VM](#), on page [448](#)
- [Export audited Logs](#), on page [448](#)
- [Enable TAC Shell Access](#), on page [449](#)

## Run Diagnostic Commands

The **Run Diagnostics** menu provides you the following options in the console:

Figure 158: Run Diagnostics Menu



## Ping a Host

Crosswork Data Gateway provides you ping utility that can be used to check reachability to any IP address.

### Procedure

**Step 1** From Main Menu, navigate to **Troubleshooting > Run Diagnostics > ping**.

**Step 2** Enter the following information:

- Number of pings
- Destination hostname or IP
- Source port (UDP, TCP, TCP Connect)
- Destination port (UDP, TCP, TCP Connect)

**Step 3** Click **OK**.

## Traceroute to a Host

Crosswork Data Gateway provides the traceroute option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Crosswork Data Gateway to reach the destination.

**Command Options to Troubleshoot****Procedure**

- 
- Step 1** From Main Menu, navigate to **Troubleshooting > Run Diagnostics > traceroute**.
- Step 2** Enter the traceroute destination.
- Step 3** Click **OK**.
- 

**Command Options to Troubleshoot**

Crosswork Data Gateway provides several commands for troubleshooting.

**Procedure**

- 
- Step 1** From Main Menu, navigate to **Troubleshooting > Run Diagnostics**.
- Step 2** Select the command and other option or filters for each of the commands:
- **4 top**
  - **5 lsof**
  - **6 iostat**
  - **7 vmstat**
  - **8 nslookup**
- Step 3** Click **Ok**.
- 

Once you have selected all the options, Crosswork Data Gateway clears the screen and runs the command with the specified options.

**Download tcpdump**

Crosswork Data Gateway provides the tcpdump option that allows you to capture and analyze network traffic.



**Note** This task can only be performed by a **dg-admin** user.

**Procedure**

- 
- Step 1** From Main Menu, navigate to **Troubleshooting > Run Diagnostics > tcpdump**.
- Step 2** Select an interface to run the tcpdump utility. To run the utility for all the interfaces, select the **All** option.
- Step 3** Select the appropriate check box to view the packet information on the screen or save the captured packets to a file.

**Step 4** Enter the following details and click **OK**.

- Packet count limit
- Collection time limit
- File size limit
- Filter expression

---

Depending on the option you choose, Crosswork Data Gateway displays the packet capture information on the screen or saves it to a file. After the tcpdump utility reaches the specified limit, Crosswork Data Gateway compresses the file, and prompts for the SCP credentials to transfer the file to a remote host. The compressed file is deleted once the transfer is complete or if you've decided to cancel the file transfer before completion.

## Run a Controller Session Test

After Crosswork Data Gateway is installed, you can validate if the instance is able to establish a connection with Crosswork Cloud by using the controller session test option. In addition to the connection tests, the utility validates and analyzes the discrepancies between the resources (CPU and memory) assigned to the VM and the resources prescribed by the deployment profile.

### Procedure

---

From Main Menu, navigate to **Troubleshooting > Run Diagnostics > Run Controller Session Tests**. If the connection is completed, the console displays a message indicating that the instance was able to establish a connection. When the connection fails, additional validation tests are performed, and the following information is displayed:

- DNS server IP address
- DNS domain
- NTP server address
- NTP status
- Proxy URL
- Proxy reachability status
- Controller URL
- Controller reachability status
- The date when the tests were last performed.

Figure 159: Run Controller Session Tests Menu

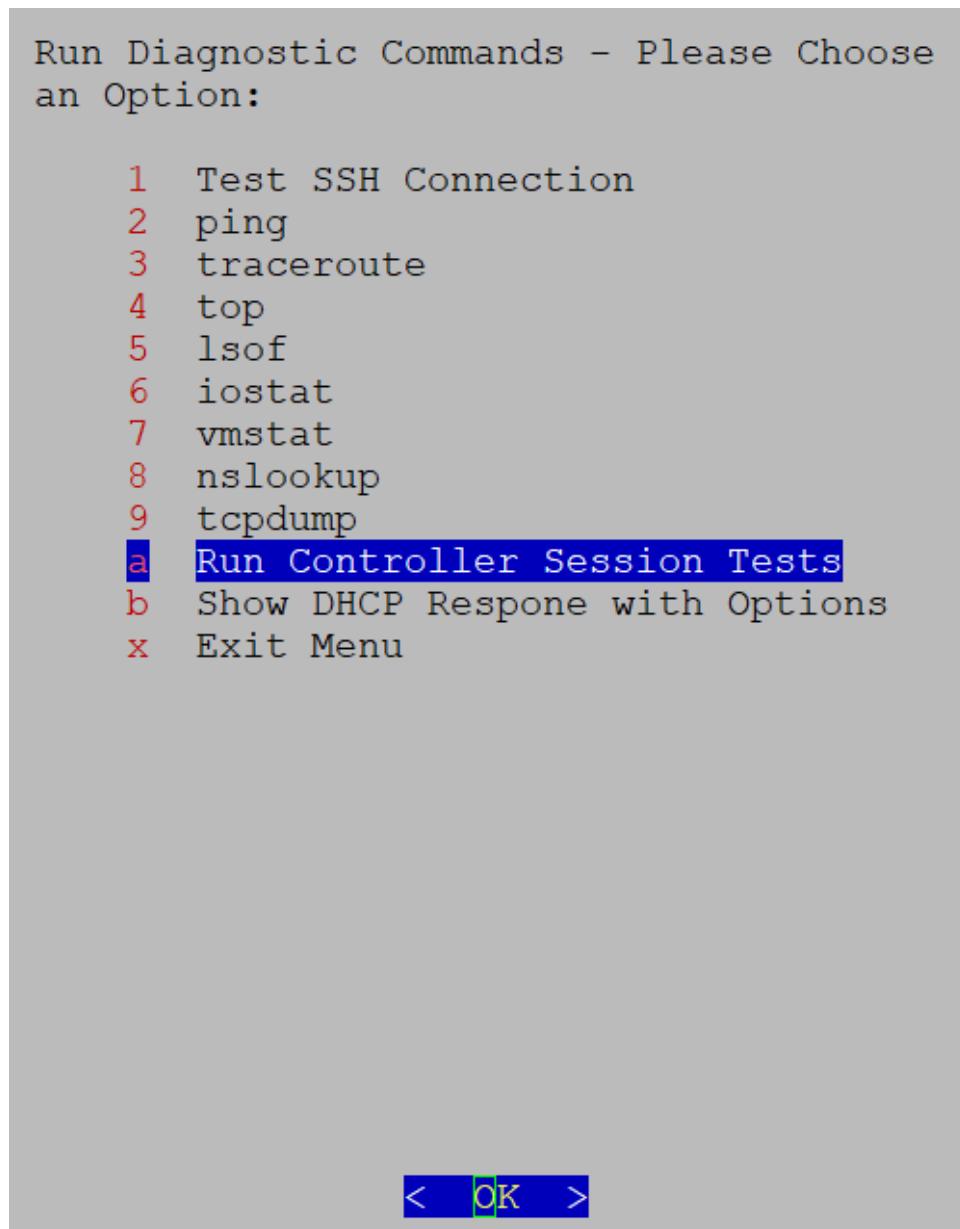


Figure 160: Result of the Run Controller Session Tests Menu

```
Controller Session: Established
Last Checked: Sun 23 Apr 2023 11:03:17 AM UTC
```

### What to do next

If the controller session was not established, review the information displayed on the console to determine the probable cause of the failure and perform the corrective actions proposed on the console.

## Run show-tech

Crosswork Data Gateway provides the show\_tech option to export its log files to a user-defined SCP destination.

The collected data includes the following:

- Logs of all the Data Gateway components running on Docker containers
- VM Vitals

It creates a tarball in the directory where it is executed. The output is a tarball named `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc`.

The execution of this command may take several minutes depending on the state of Crosswork Data Gateway.

### Procedure

**Step 1** From **Troubleshooting** menu, select **Show-tech** and click **OK**.

**Step 2** Enter the destination to save the tarball containing logs and vitals.

**Step 3** Enter your SCP passphrase and click **OK**.

The showtech file downloads in an encrypted format.

**Note**

Depending on how long the system was in use, it may take several minutes to download the showtech file.

**Step 4** After the download is complete run the following command to decrypt it:

**Note**

In order to decrypt the file, you must use OpenSSL version 1.1.1i. Use the command `openssl version` to check the openssl version on your system.

To decrypt the file on a MAC, you must install OpenSSL 1.1.1+. This is because LibreSSL's `openssl` command does not support all the switches supported by OpenSSL's `openssl` command.

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

## Reboot Crosswork Data Gateway VM



**Note** This task can only be performed by **dg-admin** user.

Crosswork Data Gateway gives you two options to reboot the VM:

## Shutdown the Crosswork Data Gateway VM

- **Remove all Collectors and Reboot VM:** Select this option from the **Troubleshooting** menu if you want to stop the containers that were downloaded after installation (collectors and offload), remove the images from docker, remove collector data and configuration and reboot VM. This returns the VM to a state just after initial configuration is complete with only infrastructure containers running.
- **Reboot VM:** Select this option from the **Troubleshooting** menu for a normal reboot.

## Shutdown the Crosswork Data Gateway VM

From the **Troubleshooting** Menu, select **5 Shutdown VM** to power off the Crosswork Data Gateway VM.

## Export auditd Logs

Follow the steps to export auditd logs:

### Procedure

- 
- Step 1** From **Troubleshooting**, select **Export audit Logs**.
  - Step 2** Enter a passphrase for auditd log tarball encryption.
  - Step 3** Click **OK**.
- 

## Re-enroll Crosswork Data Gateway

Follow the steps to re-enroll Crosswork Data Gateway:

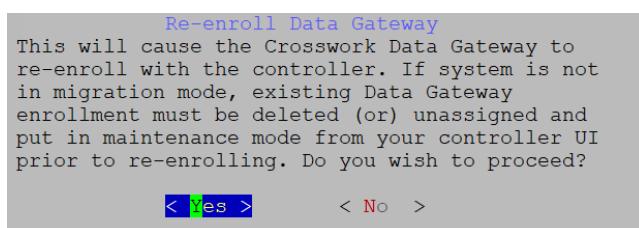
### Before you begin

The existing Crosswork Data Gateway enrollment must be deleted from the controller prior to re-enrolling.

### Procedure

- 
- Step 1** From **Troubleshooting** menu, select **Re-enroll Data Gateway**.
  - Step 2** Review the information inn the confirmation window and click **Yes**.

*Figure 161: Re-enroll Data Gateway Confirmation Window*



## Remove Rotated Log Files

Follow the steps to removes all rotated log files (\*.gz or \*.xz) in the /var/log and /opt/dg/log folders.

### Procedure

- 
- Step 1** From **Troubleshooting** menu, select **Remove Rotated Log files**.
- Step 2** Select **Yes** in the dialog that appears to save your changes.
- 

## Enable TAC Shell Access

The TAC Shell Access function allows a Cisco engineer to directly log in to the Ubuntu shell via multifactor authentication, using a reserved user named **dg-tac**.

Initially, the **dg-tac** user account is locked and password is expired to prevent the user from getting a shell prompt. Once enabled, the dg-tac user is active until the next calendar day, 12:00 a.m UTC (midnight UTC), which is less than 24 hours.

The steps to enable the **dg-tac** user are as follows:



**Note** Enabling this access requires you to communicate actively with the Cisco engineer.

### Before you begin

Ensure that the Cisco engineer who is working with you has access to the SWIMS Aberto tool.

### Procedure

- 
- Step 1** Log in to the Data Gateway VM as the **dg-admin** user.
- Step 2** From the main menu, select **Troubleshooting**.
- Step 3** From the **Troubleshooting** menu, select **t Enable TAC Shell Access**.
- A dialog appears, warning that the **dg-tac** user login requires a password that you set and a response to a challenge token from TAC. At this point, you may answer **No** to stop the enable process or **Yes** to continue.
- Step 4** If you continue, the system prompts for a new password to use and shows the day when the account disables itself.
- Step 5** Enter a password to unlock the account in the console menu.
- Step 6** Log out of the Crosswork Data Gateway.
- Step 7** Follow these steps if the Crosswork Data Gateway VM can be accessed by the Cisco engineer directly. Move to **Step 8** otherwise.
- Share the password that you had set in Step 5 for the **dg-tac** user with the Cisco engineer who is working with you.
  - The Cisco engineer logs in as the **dg-tac** user Via SSH with the password you had set.

After entering the password, the system presents the challenge token. The Cisco engineer signs the challenge token using the SWIMS Aberto tool and pastes the signed response to the challenge token back at the Crosswork Data Gateway VM.

- c) The Cisco engineer logs in successfully as the **dg-tac** user and completes the troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

- d) After troubleshooting is complete, the Cisco engineer logs out of the TAC shell.

#### Step 8

If Crosswork Data Gateway VM cannot be accessed directly by the Cisco engineer, start a meeting with the Cisco engineer with desktop sharing enabled.

- a) Log in as the **dg-tac** user Via SSH using the following command:

```
ssh dg-tac@<DG hostname or IP>
```

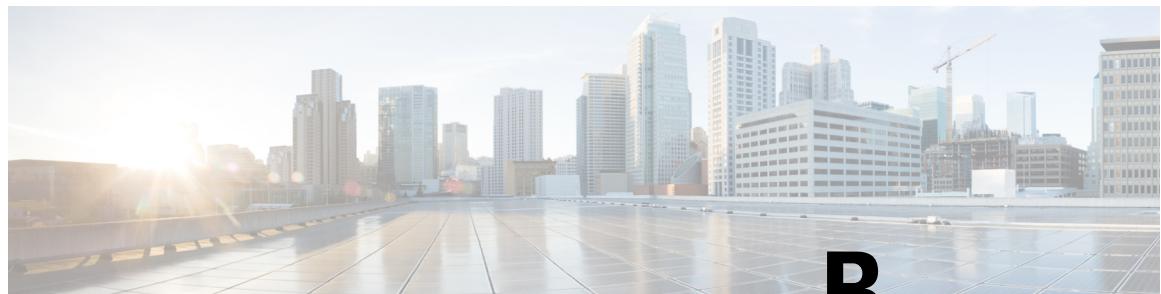
- b) Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. Share this token with the Cisco engineer who will then sign the token using the SWIMS Aberto tool and share the response with you.

- c) Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt.
- d) Share your desktop or follow the Cisco engineer's instructions for troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

- e) Log out of the TAC shell after troubleshooting is complete.



## APPENDIX B

# List of Pre-loaded Traps and MIBs for SNMP Collection

This section lists the traps and MIBs that the Cisco Crosswork Data Gateway supports for SNMP collection.



**Note** This list is applicable only when Crosswork is the target application and is not limited when the target is an external application.

Note the following constraints:

- The system cannot extract index values from OIDs of conceptual tables. If any of the columns that define indices in the conceptual table are not populated, the index value is replaced on the data plane with the instance identifier (oid suffix) of the row.
- The system cannot extract index values from conceptual tables that include the **AUGMENT** keyword or refer to indices of other tables.
- Named-number enumerations (using the integer syntax) are sent on the wire using their numeric value.

**Table 61: Supported Traps**

Trap	OID
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
coldStart	1.3.6.1.6.3.1.1.5.1
isisAdjacencyChange	1.3.6.1.2.1.138.0.17

ADSL-LINE-MIB.mib	CISCO-LWAPP-INTERFACE-MIB.mib	IANA-ITU-ALARM-TC-MIB.mib
ADSL-TC-MIB.mib	CISCO-LWAPP-IPS-MIB.mib	IANA-LANGUAGE-MIB.mib
AGENTX-MIB.mib	CISCO-LWAPP-LINKTEST-MIB.mib	IANA-RTPROTO-MIB.mib

## List of Pre-loaded Traps and MIBs for SNMP Collection

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

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

## List of Pre-loaded Traps and MIBs for SNMP Collection

CISCO-ENTITY-ASSET -MIB.mib	CISCO-ST-TC.mib	MPLS-TE-MIB.mib
CISCO-ENTITY-EXT -MIB.mib	CISCO-STACKWISE- MIB.mib	MPLS-TE-STD-MIB.mib
CISCO-ENTITY-FRU-CONTROL-MIB.mib	CISCO-STP-EXTENSIONS -MIB.mib	MPLS-VPN-MIB.mib
CISCO-ENTITY- QFP-MIB.mib	CISCO-SUBSCRIBER -IDENTITY-TC-MIB.mib	MSDP-MIB.mib
CISCO-ENTITY- REDUNDANCY-MIB.mib	CISCO-SUBSCRIBER- SESSION-MIB.mib	NET-SNMP-AGENT -MIB.mib
CISCO-ENTITY- REDUNDANCY-TC-MIB.mib	CISCO-SUBSCRIBER- SESSION-TC-MIB.mib	NET-SNMP-EXAMPLES -MIB.mib
CISCO-ENTITY- SENSOR-MIB.mib	CISCO-SYSLOG-MIB.mib	NET-SNMP-MIB.mib
CISCO-ENTITY- VENDORTYPE-OID-MIB.mib	CISCO-SYSTEM-EXT- MIB.mib	NET-SNMP-TC.mib
CISCO-ENVMON-MIB.mib	CISCO-SYSTEM-MIB.mib	NHRP-MIB.mib
CISCO-EPM- NOTIFICATION-MIB.mib	CISCO-TAP2-MIB.mib	NOTIFICATION-LOG- MIB.mib
CISCO-ETHER-CFM- MIB.mib	CISCO-TC.mib	OLD-CISCO-CHASSIS- MIB.mib
CISCO-ETHERLIKE- EXT- MIB.mib	CISCO-TCP-MIB.mib	OLD-CISCO-INTERFACES -MIB.mib
CISCO-FABRIC- C12K-MIB.mib	CISCO-TEMP-LWAPP -DHCP-MIB.mib	OLD-CISCO-SYS- MIB.mib
CISCO-FIREWALL -TC.mib	CISCO-TRUSTSEC -SXP-MIB.mib	OLD-CISCO-SYSTEM -MIB.mib
CISCO-FLASH-MIB.mib	CISCO-TRUSTSEC -TC-MIB.mib	OPT-IF-MIB.mib
CISCO-FRAME- RELAY-MIB.mib	CISCO-UBE-MIB.mib	OSPF-MIB.mib
CISCO-FTP-CLIENT -MIB.mib	CISCO-UNIFIED- COMPUTING-ADAPTOR -MIB.mib	OSPF-TRAP-MIB.mib
CISCO-HSRP-EXT -MIB.mib	CISCO-UNIFIED- COMPUTING-COMPUTE -MIB.mib	OSPFV3-MIB.mib
CISCO-HSRP-MIB.mib	CISCO-UNIFIED- COMPUTING-ETHER -MIB.mib	P-BRIDGE-MIB.mib
CISCO-IETF-ATM2 -PVCTRAP- MIB.mib	CISCO-UNIFIED- COMPUTING-FC- MIB.mib	PIM-MIB.mib
CISCO-IETF-BFD -MIB.mib	CISCO-UNIFIED- COMPUTING-MEMORY -MIB.mib	PIM-STD-MIB.mib
CISCO-IETF-FRR -MIB.mib	CISCO-UNIFIED- COMPUTING -MIB.mib	POWER-ETHERNET -MIB.mib

CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED-COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED-COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED-COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS-TE-EXT-STD-03- MIB.mib	CISCO-VLAN-IFTABLE-RELATIONSHIP -MIB.mib	PTOPO-MIB.mib
CISCO-IETF-MPLS-TE-P2MP-STD-MIB.mib	CISCO-VLAN-MEMBERSHIP-MIB.mib	PerfHist-TC-MIB.mib
CISCO-IETF-MSDP -MIB.mib	CISCO-VOICE-COMMON-DIAL-CONTROL-MIB.mib	Q-BRIDGE-MIB.mib
CISCO-IETF-PIM-EXT -MIB.mib	CISCO-VOICE-DIAL-CONTROL-MIB.mib	RADIUS-ACC-CLIENT -MIB.mib
CISCO-IETF-PIM -MIB.mib	CISCO-VOICE-DNIS -MIB.mib	RADIUS-AUTH-CLIENT -MIB.mib
CISCO-IETF-PW- ATM-MIB.mib	CISCO-VPDN-MGMT -MIB.mib	RFC-1212.mib
CISCO-IETF-PW- ENET-MIB.mib	CISCO-VTP-MIB.mib	RFC-1215.mib
CISCO-IETF-PW-MIB.mib	CISCO-WIRELESS-NOTIFICATION-MIB.mib	RFC1155-SMI.mib
CISCO-IETF-PW- MPLS-MIB.mib	CISCOSB-DEVICEPARAMS -MIB.mib	RFC1213-MIB.mib
CISCO-IETF-PW -TC-MIB.mib	CISCOSB-HWENVIRONMENT.mib	RFC1315-MIB.mib
CISCO-IETF-PW -TDM-MIB.mib	CISCOSB-MIB.mib	RFC1398-MIB.mib
CISCO-IETF-VPLS -BGP-EXT-MIB.mib	CISCOSB-Physicaldescription -MIB.mib	RIPv2-MIB.mib
CISCO-IETF-VPLS -GENERIC-MIB.mib	DIAL-CONTROL-MIB.mib	RMON-MIB.mib
CISCO-IETF-VPLS- LDP-MIB.mib	DIFFSERV-DSCP-TC.mib	RMON2-MIB.mib
CISCO-IF-EXTENSION -MIB.mib	DIFFSERV-MIB.mib	RSTP-MIB.mib
CISCO-IGMP-FILTER -MIB.mib	DISMAN-NSLOOKUP -MIB.mib	RSVP-MIB.mib
CISCO-IMAGE-LICENSE -MGMT-MIB.mib	DISMAN-PING-MIB.mib	SMON-MIB.mib
CISCO-IMAGE-MIB.mib	DISMAN-SCHEDULE -MIB.mib	SNA-SDLC-MIB.mib
CISCO-IMAGE-TC.mib	DISMAN-SCRIPT-MIB.mib	SNMP-COMMUNITY -MIB.mib

## List of Pre-loaded Traps and MIBs for SNMP Collection

CISCO-IP-LOCAL-POOL-MIB.mib	DISMAN-TRACEROUTE-MIB.mib	SNMP-FRAMEWORK-MIB.mib
CISCO-IP-TAP-MIB.mib	DOT3-OAM-MIB.mib	SNMP-MPD-MIB.mib
CISCO-IP-URPF-MIB.mib	DRAFT-MSDP-MIB.mib	SNMP-NOTIFICATION-MIB.mib
CISCO-IPMROUTE-MIB.mib	DS0-MIB.mib	SNMP-PROXY-MIB.mib
CISCO-IPSEC-FLOW-MONITOR-MIB.mib	DS1-MIB.mib	SNMP-REPEATER-MIB.mib
CISCO-IPSEC-MIB.mib	DS3-MIB.mib	SNMP-TARGET-MIB.mib
CISCO-IPSEC-POLICY-MAP-MIB.mib	ENTITY-MIB.mib	SNMP-USER-BASED-SM-MIB.mib
CISCO-IPSLA-AUTOMEASURE-MIB.mib	ENTITY-SENSOR-MIB.mib	SNMP-USM-AES-MIB.mib
CISCO-IPSLA-ECHO-MIB.mib	ENTITY-STATE-MIB.mib	SNMP-USM-DH-OBJECTS-MIB.mib
CISCO-IPSLA-JITTER-MIB.mib	ENTITY-STATE-TC-MIB.mib	SNMP-VIEW-BASED-ACM-MIB.mib
CISCO-IPSLA-TC-MIB.mib	ESO-CONSORTIUM-MIB.mib	SNMPv2-CONF.mib
CISCO-ISDN-MIB.mib	ETHER-WIS.mib	SNMPv2-MIB.mib
CISCO-LICENSE-MGMT-MIB.mib	EtherLike-MIB.mib	SNMPv2-SMI.mib
CISCO-LOCAL-AUTH-USER-MIB.mib	FDDI-SMT73-MIB.mib	SNMPv2-TC-v1.mib
CISCO-LWAPP-AAA-MIB.mib	FR-MFR-MIB.mib	SNMPv2-TC.mib
CISCO-LWAPP-AP-MIB.mib	FRAME-RELAY-DTE-MIB.mib	SNMPv2-TM.mib
CISCO-LWAPP-CCX-RM-MIB.mib	FRNETSERV-MIB.mib	SONET-MIB.mib
CISCO-LWAPP-CDP-MIB.mib	GMPLS-LSR-STD-MIB.mib	SYSAPPL-MIB.mib
CISCO-LWAPP-CLIENT-ROAMING-CAPABILITY.mib	GMPLS-TC-STD-MIB.mib	TCP-MIB.mib
CISCO-LWAPP-CLIENT-ROAMING-MIB.mib	GMPLS-TE-STD-MIB.mib	TOKEN-RING-RMON-MIB.mib
CISCO-LWAPP-DHCP-MIB.mib	HC-PerfHist-TC-MIB.mib	TOKENRING-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.mib	HC-RMON-MIB.mib	TRANSPORT-ADDRESS-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CCX-TC-MIB.mib	HCNUM-TC.mib	TUNNEL-MIB.mib
CISCO-LWAPP-DOT11-LDAP-MIB.mib	HOST-RESOURCES-MIB.mib	UDP-MIB.mib
CISCO-LWAPP-DOT11-MIB.mib	HOST-RESOURCES-TYPES.mib	VPN-TC-STD-MIB.mib

CISCO-LWAPP -DOWNLOAD-MIB.mib	IANA-ADDRESS- FAMILY-NUMBERS-MIB.mib	VRRP-MIB.mib
CISCO-LWAPP- IDS-MIB.mib	IANA-GMPLS-TC-MIB.mib	





## APPENDIX C

# List of Pre-loaded YANG Modules for MDT Collection

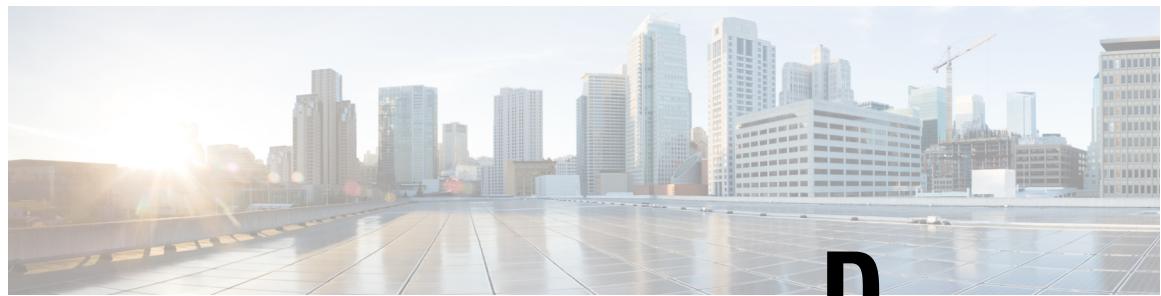
This section lists the YANG modules that the Cisco Crosswork Data Gateway supports for MDT collection on Cisco IOS XR devices.

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-wdysmon-fd-oper.yang
Cisco-IOS-XR-pbr-oper.yang	Cisco-IOS-XR-infra-objmgr-oper.yang
Cisco-IOS-XR-ip-rsvp-oper.yang	Cisco-IOS-XR-ipv6-io-oper.yang
Cisco-IOS-XR-terminal-device-oper.yang	Cisco-IOS-XR-plat-chas-invmgr-ng-oper.yang
Cisco-IOS-XR-mpls-oam-oper.yang	Cisco-IOS-XR-ncs5500-coherent-portmode-oper.yang
Cisco-IOS-XR-sse-span-oper.yang	Cisco-IOS-XR-infra-dumper-oper.yang
Cisco-IOS-XR-asr9k-sc-diag-oper.yang	Cisco-IOS-XR-mpls-io-oper.yang



## APPENDIX D

# Cisco EPM Notification MIB

This section contains the following topics:

- [Cisco EPM Notification MIB, on page 463](#)

## Cisco EPM Notification MIB

The following table shows the mapping of event fields to the alarm model in CISCO-EPM-NOTIFICATION-MIB.



**Note** Some of the values in the following table may appear truncated in a PDF. Please refer to the [HTML version](#) for clarity.

**Table 62: Cisco-EPM-Notification-MIB**

Event Field	Snmpvarbind	OID	Description	Example
TimeStamp	cenAlarmTimestamp	1.3.14.199311.1.12.1.3	The time when the event was raised	1639759929
AlarmId	cenAlarmInstanceID	1.3.14.199311.1.12.1.5	The unique alarm instance ID	57e3ef70-1597
Type	cenAlarmType	1.3.14.199311.1.12.1.8	Type of Event	2001
Category	cenAlarmCategory	1.3.6.1.4.9.9.311.1.12.1.9	The category of the event generated represented in an integer value  <i>System = 3, Network = 7, Audit = 13; Security = 4, External = 1</i>	3

Event Field	Snmpvarbind	OID	Description	Example
Category Definition	cenAlarmCategoryDefinition	1.3.6.1.4.9.9.311.1.1.2.1.10	The short description of the category of the event. The String is formatted in '<integer, eventCategory description>'	3, System
	cenAlarmServerAddressType	1.3.6.1.4.9.9.311.1.1.2.1.11	The type of internet address of the CW alarm centre (VIP) 1:ipv4, 2:ipv6	1:ipv4
	cenAlarmServerAddress	1.3.6.1.4.9.9.311.1.1.2.1.12	The IP Address of the CW alarm centre (VIP)	10.127.101.145
OriginAppId	cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	This attribute contains the OriginAppId of the application which generated the Event	DLM
Description	cenAlarmDescription	1.3.6.1.4.9.9.311.1.1.2.1.16	A detailed description of the event	Reachability request did not receive any response from CDG
Severity	cenAlarmSeverity	1.3.6.1.4.9.9.311.1.1.2.1.17	The alarm severity indicates the severity of the event in an integer value. Critical=2; Major=3; Warning=4; Minor=5, Info=6, Clear=7	5
Severity definition	cenAlarmSeverityDefinition	1.3.6.1.4.9.9.311.1.1.2.1.18	The short description of the severity of the event. The String is formatted in '<integer, eventSeverity description>'	3, Major

Event Field	Snmpvarbind	OID	Description	Example
ObjectDescription, ObjectId	cenUserMessage1	1.3.6.1.4.1.99311.1.12.1.21	Information about the Event ObjectDescription, ObjectId. The string is formatted in '<ObjectDescription=xx, ObjectId=xx>'	ObjectDescription=Node<xrvr9k>, ObjectId=NodeData [4a16368]
OriginServiceId	cenUserMessage2	1.3.6.1.4.1.99311.1.12.1.22	Information about the Event OriginServiceId	0
EventId	cenAlertID	1.3.6.1.4.99311.1.12.1.29	This attribute will contain the event id of the generated Event	9f19e5a9-a64c

