



Cisco Crosswork Change Automation and Health Insights 3.2.2 User Guide

First Published: 2020-07-06

Last Modified: 2020-07-06

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 NON-INFRINGEMENT 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.

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)

© 2020–2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview 1

- Audience 1
- Overview of Cisco Crosswork Change Automation and Health Insights 1
- API Documentation 2
- Licensing 2
- Log In and Log Out 3
- Use the Main Window Controls 4
- Set, Sort and Filter Table Data 6

CHAPTER 2

Get Started 9

- Basic Concepts 9
- Before You Begin 10
- High-Level Workflow 11
- Workflow 1: Setup 12
- Workflow 2: Monitor Key Performance Indicators 14
- Workflow 3: Respond to KPI Data 14
- Workflow 4: Schedule Playbooks 15
- Workflow 5: Develop Custom KPIs 16
- Workflow 6: Develop Custom Playbooks 16
- Workflow 7: Set Up Data Collection for External Data Destinations 17
- Workflow 8: Add Additional Device Collection Support 19

CHAPTER 3

Automate Network Changes 21

- Change Automation Overview 21
 - Use the Change Automation Dashboard 22
 - View the Playbook List 22

- About Running Playbooks 23
 - Playbook Execution Order 24
 - Perform a Dry Run of a Playbook 25
 - Run Playbooks In Single Stepping Mode 27
 - Run Playbooks In Continuous Mode 30
 - Schedule Playbook Runs 32
 - View or Abort Playbook Jobs 34
- About Customizing Playbooks 35
 - Playbook Components and Files 36
 - Export Playbooks 37
 - Import Playbooks 38
 - Delete Custom Playbooks 38
- Troubleshoot Change Automation 39

CHAPTER 4

- Monitor Network Health and KPIs 41**
 - Health Insights Overview 41
 - Health Insights Alert Dashboard 42
 - Create a New KPI Profile 44
 - Enable KPI Profile on Devices 47
 - View Alerts for Network Devices 50
 - Telemetry Data Retention 51
 - Manage KPI Profiles 52
 - Manage KPIs 53
 - Create a New KPI 54
 - Link KPIs to Playbooks 55
 - Verify the Deployment Status of Enabled KPIs 57
 - Disable KPI Profile on Devices or Device Groups 57
 - List of Health Insights KPIs 58
 - Troubleshoot Health Insights 63

CHAPTER 5

- Visualize the Network 65**
 - Network Visualization Overview 65
 - Identify the Members of a Cluster 67
 - Device and Link Icons 68

Get More Information About Devices on the Map	69
Access the Device Console	71
Get More Information About Links	72
Network Link Discovery	73
Show Bandwidth Utilization for Links on the Map	74
Define Color Thresholds for Link Bandwidth Utilization	74
Configure Geographical Map Settings	75
Change the Layout of a Logical Map	76
Create Custom Map Views	77
Manage Custom Map Views	77

CHAPTER 6
Manage Inventory 79

Device Management Overview	79
Reachability and Operational State	79
Manage Credential Profiles	81
Create Credential Profiles	82
Import Credential Profiles	84
Edit Credential Profiles	86
Delete Credential Profiles	87
Export Credential Profiles	87
Change the Credential Profile for a Device or Provider	88
Change the Credential Profile for Multiple Network Devices	88
Manage Network Devices	89
About Adding Devices to Inventory	90
Prerequisites for Onboarding Devices	91
Sample Configuration for Devices in Cisco NSO	93
Import Network Devices	94
Add Network Devices Through the UI	95
Get Network Device Details	99
Filter Network Devices by Tags	101
Edit Network Devices	101
Delete Network Devices	102
Export Network Devices	103
View Device Job History	103

Manage Devices Using Zero Touch Provisioning	104
Zero Touch Provisioning Concepts	109
Workflow: Zero Touch Provisioning	110
Upload Software Image Files	112
Edit Image Files	113
Delete Image Files	113
Copy Image File Paths and UUIDs	114
Upload Configuration Files	114
Prepare Your Custom Day-Zero Configuration Files	115
Use Custom Day-Zero Configuration Files	117
Edit Configuration Files	118
Download Configuration Files	118
Delete Configuration Files	119
Copy Configuration File Paths and UUIDs	119
Create Zero Touch Profiles	120
Edit Zero Touch Profiles	121
Delete Zero Touch Profiles	121
View Zero Touch Profile Details	122
Create ZTP Device Entries	122
Create ZTP Device Entries Using the UI	122
Create ZTP Device Entries Using Import	125
Prepare ZTP Device Import Files	126
Export ZTP Devices	127
Edit ZTP Devices	127
Delete ZTP Devices	128
DHCP Setup for Crosswork ZTP	128
Cisco Prime Network Registrar DHCP Setup	129
Generic ISC DHCP Setup	143
Troubleshoot ZTP Issues	145
CHAPTER 7	Perform Administrative Tasks 147
Manage Cisco Crosswork Network Automation	147
Monitor Cisco Crosswork Network Automation Functions in Real Time	150
Collect and Share Cisco Crosswork Network Automation Logs and Metrics	154

Audit Log	156
Control Cisco Crosswork Network Automation Applications and Services	157
Manage Backup and Restore	158
Disaster Restore	160
Integration with TACACS+ and LDAP servers	161
Manage TACACS+ Servers	161
Add a TACACS+ Server	162
Edit a TACACS+ Server	162
Delete a TACACS+ Server	162
Manage LDAP Servers	163
Add a LDAP Server	163
Edit a LDAP Server	163
Delete a LDAP Server	164
Manage Users	164
Administrative Users Created During Installation	164
Add Users	165
Edit Users	165
Delete Users	166
User Roles, Functional Categories and Permissions	166
Create User Roles	168
Edit User Roles	169
Clone User Roles	169
Delete User Roles	170
Manage Providers	170
About Provider Families	172
About Adding Providers	172
Add Providers Through the UI	173
Import Providers	175
Add Cisco NSO Providers	178
Add Cisco SR-PCE Providers	179
Add Cisco WAE Providers	182
Add Syslog Storage Providers	183
Add an Alert Provider	184
Add Optimization Engine Providers	185

Get Provider Details	186
Edit Providers	187
Delete Providers	187
Export Providers	188
Manage Tags	188
Create Tags	190
Import Tags	190
Apply or Remove Device Tags	191
Delete Tags	192
Export Tags	192
Define Network Visualization Display Settings	193
Manage Certificates	193
Extend Self-Signed Certificate Expiration	194
Substitute a User-Provided Certificate	195
Smart Licensing Registration	196
Overview	196
Configure Transport Settings	197
Register Cisco Crosswork Change Automation and Health Insights	198
Manual Actions	201
License Authorization Statuses	202
Security Hardening Overview	202
Authentication Throttling	203
Core Security Concepts	203
HTTPS	203
SSL Certificates	203
1-Way SSL Authentication	204
Disable Insecure Ports and Services	205
Harden Your Storage	206
CHAPTER 8	Manage Cisco Crosswork Data Gateway 207
Overview of Cisco Crosswork Data Gateway	207
Manage Cisco Crosswork Data Gateway Instances	208
Add a Cisco Crosswork Data Gateway Instance	212
Update Cisco Crosswork Data Gateway Instance Enrollment Settings	212

View Enrollment Details	213
Change the Administration State of a Cisco Crosswork Data Gateway Instance	215
De-enroll a Cisco Crosswork Data Gateway Instance	216
Attach a Device to a Cisco Crosswork Data Gateway Instance	217
Detach a Device From a Cisco Crosswork Data Gateway Instance	219
View Cisco Crosswork Data Gateway Instance Health	220
Configure Cisco Crosswork Data Gateway Settings	223
Manage Data Destinations	224
Add a Data Destination	225
Update a Data Destination	229
View Data Destination Details	230
Delete a Data Destination	231
Manage Custom Software Packages	232
Add a Custom Software Package	234
Delete a Custom Software Package	235
Download Custom or System MIBs and Packages	236

CHAPTER 9
Configure Collection 239

Collection Service Overview	239
Prerequisites for Device Model Driven Telemetry	239
About Collection Jobs	242
Collection Job Payload Model	242
Create Collection Jobs	248
Best Practices and Limitations for Creating Collection Jobs	248
Collection Jobs	249
CLI Collection Job	249
SNMP Collection Jobs	251
MDT Collection Job	257
Monitoring Collection Jobs	259
List of Pre-loaded Traps and MIBs for SNMP Collection	264
List of Pre-loaded YANG Modules for MDT Collection	270

APPENDIX A
Device and Credentials Sync With Cisco NSO 275

Add Devices and Credential Profiles By Synchronizing With Cisco NSO	275
---	-----

APPENDIX B

- Configure Cisco Crosswork Data Gateway Base VM 279**
 - About Cisco Crosswork Data Gateway Base VM 279
 - Base VM Contents 279
 - Log In and Log Out 280
 - Access Cisco Crosswork Data Gateway Through vCenter 280
 - Access Cisco Crosswork Data Gateway Via SSH 280
 - Use the Interactive Console 281
 - Basic Concepts 282
 - Cisco Crosswork Data Gateway Components 282
 - Controller Gateway 282
 - Image Manager 282
 - Vitals Monitor 283
 - Route Manager 283
 - Docker IPv6nat 283
 - Manage Users 283
 - Supported User Roles 283
 - Change Password 285
 - View Current System Settings 286
 - Change Current System Settings 290
 - Configure NTP 292
 - Configure DNS 293
 - Configure Control Proxy 293
 - Configure Static Routes 293
 - Add Static Routes 293
 - Delete Static Routes 295
 - Configure Syslog 296
 - Create New SSH Keys 297
 - Import Certificate 297
 - Configure vNIC1 MTU 298
 - Monitor Cisco Crosswork Data Gateway Health 299
 - Vitals Monitor 299
 - View Cisco Crosswork Data Gateway Vitals 299
 - collector-vitals Service 302

Troubleshooting	305
Ping a Host	306
Traceroute to a Host	307
Check NTP Status	308
Check System Uptime	308
Run show-tech	309
Reboot Crosswork Data Gateway VM	310

APPENDIX C

Supported Devices Information	311
Supported Devices and Software Types	311

APPENDIX D

Telemetry-Traffic Collector (TM-TC) Troubleshooting Procedures	313
Handling Zombies	313
Handling Device Cleanup Errors	315



CHAPTER 1

Overview

This section contains the following topics:

- [Audience, on page 1](#)
- [Overview of Cisco Crosswork Change Automation and Health Insights, on page 1](#)
- [API Documentation, on page 2](#)
- [Licensing, on page 2](#)
- [Log In and Log Out, on page 3](#)
- [Use the Main Window Controls, on page 4](#)
- [Set, Sort and Filter Table Data, on page 6](#)

Audience

This guide is for experienced network administrators who want to use Cisco Crosswork Change Automation and Health Insights in their network. This guide assumes that you are familiar with the following topics:

- Networking technologies and protocols (IS-IS, BGP, and so on)
- Network monitoring and troubleshooting
- Familiarity with the different operating systems used on devices that form your network, such as Cisco IOS-XR, IOS-XE, and NX-OS.

Overview of Cisco Crosswork Change Automation and Health Insights

Cisco Crosswork Change Automation and Health Insights is part of the Cisco Crosswork Network Automation suite of products. Cisco Crosswork Change Automation and Health Insights retrieves real-time information from the network, analyzes the data, and uses APIs to apply network changes. The Cisco Crosswork Change Automation and Health Insights platform brings together streaming telemetry and model-driven application programming interfaces (APIs) to redefine service provider network operations.

Cisco Crosswork Change Automation and Health Insights enables service providers to quickly deploy intent-driven, closed-loop operations. The platform provides a ready-to-use solution supporting the following use cases:

- Monitor Key Performance Indicators (KPIs) and notify of any anomalies.
- Intergration with other Crosswork products such as the Cisco Crosswork Situation Manager.
- Prepare network changes triggered by changes in KPIs and roll out these changes.
- Automate change-impact and remediation.

The data collection functionality is carried out by Cisco Crosswork Data Gateway, a software package that is separated out into its own VM. Cisco Crosswork Data Gateway gathers all the information from the managed devices and it to Cisco Crosswork Change Automation and Health Insights for analysis and processing. Cisco Crosswork Change Automation and Health Insights can then be used by the operator to manage the network or respond to changes in the network. Apart from Cisco Crosswork Change Automation and Health Insights, Cisco Crosswork Data Gateway can also be used for external data collection integration, which requires an additional license.

Cisco Crosswork Change Automation and Health Insights uses Cisco Network Services Orchestrator (Cisco NSO) as the default provider to configure the devices according to their expected functions, including configuring any required model-driven telemetry (MDT) sensor paths for data collection. Cisco NSO is vital in supplying device management and configuration-maintenance services

Cisco WAN Automation Engine (Cisco WAE) providers supply traffic and topology analysis to Cisco Crosswork Change Automation and Health Insights. The foundation software is Cisco WAE Planning, which provides a cross-sectional view of traffic, topology, and equipment state.

This guide explains how to use both Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway.

For more information about the Cisco Crosswork Network Automation platform and Cisco Crosswork Change Automation and Health Insights, see the [Cisco Crosswork Network Automation Product page on Cisco.com](#).

API Documentation

Advanced users can extend Cisco Crosswork Change Automation and Health Insights functions by using the product APIs.

For more about the product APIs, see the [Cisco Crosswork Network Automation API Documentation on Cisco DevNet](#).

Licensing

Licenses determine the applications you can use and the numbers of devices that Cisco Crosswork Change Automation and Health Insights can manage.

Change Automation, Health Insights, and Crosswork Zero Touch Provisioning (ZTP) are separately licensed applications. Change Automation license count is incremented each time a playbook is run. Health Insights is licensed based on the number of KPIs you have enabled (via a KPI Profile), with the license count incrementing for each enabled KPI. Crosswork Zero Touch Provisioning license count is incremented each time a device successfully completes the Zero Touch Provisioning process.

Cisco Crosswork Data Gateway license is included in Cisco Crosswork Change Automation and Health Insights license apart from Cisco Crosswork Data Gateway API access for external data collection integration which is separately licensed.

To purchase a Cisco Crosswork Change Automation and Health Insights license, contact your Cisco account representative.

For more about licensing, see the [Cisco Crosswork Network Automation Product Data Sheet on Cisco.com](#).



Note For demonstrations and field trials, Cisco Crosswork Change Automation and Health Insights can be used without a license for up to 90 days.

Log In and Log Out

The Cisco Crosswork Change Automation and Health Insights user interface is browser based. It supports the following browsers:

- Google Chrome, version 70 or later
- Mozilla Firefox, version 60 or later

Step 1 Open a web browser and enter:

```
https://<Crosswork_VM_management_IPv4_address>:30603/
```

or

```
https://[<Crosswork_VM_management_IPv6_address>]:30603/
```

Note Please note that the IPv6 address in the URL must be enclosed with brackets.

When you access Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights server as a trusted site in all subsequent logins.

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



Crosswork Network Automation

Username

Password

Log In

© 2019 Cisco Systems, Inc. All rights reserved.

Note The default Cisco Crosswork Change Automation and Health Insights administrator user name and password is **admin**. This account is created automatically at installation (see [Administrative Users Created During Installation, on page 164](#)). The initial password for this account must be changed during installation verification, as explained in the *Cisco Crosswork Change Automation and Health Insights Installation Guide*. Cisco strongly recommends that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user accounts with appropriate privileges and their own credentials (as explained in [Add Users, on page 165](#)) and use only those accounts for all subsequent user logins.

Step 3 Click **Log In**.

Note:

- You might need to log in again when you cross-launch from one application to another.
- A cross-launched application might remain open even after you log out of Cisco Crosswork Change Automation and Health Insights.
- If this is your first time logging in using your own user account, you will be prompted to create a new password for your account.

Step 4 To log out, click  in the top right of the Cisco Crosswork Change Automation and Health Insights main window and choose **Log out**.

Use the Main Window Controls

The Cisco Crosswork Change Automation and Health Insights main window (also known as the dashboard) provides the controls and dashboard tiles described below.

Figure 1: Main Window

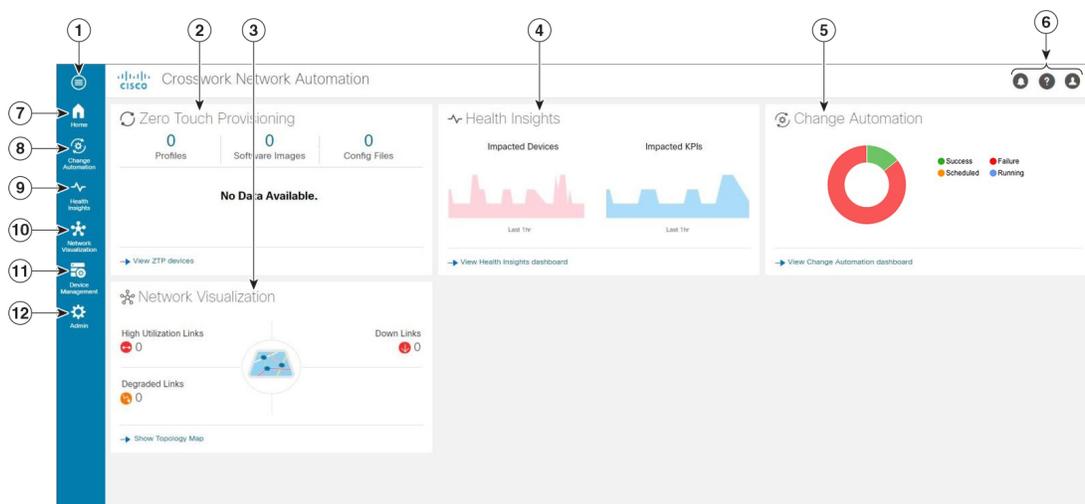


Table 1: Main Window Controls

Item	Description
1	More: Toggles the main menu between compact mode, which requires you to click on each menu icon before you can select the options under it, and expanded mode, which displays the entire menu and lets you pick options directly.
2	Zero Touch Provisioning Tile: Gives you a summary view of current ZTP processing status, with counts for all the devices, images, configuration files and profiles currently in use, and the number of devices in each of the possible ZTP transition states. Click on the View ZTP Devices link at the bottom of the tile to open the Zero Touch Devices application and get more details.
3	Network Visualization Tile: Summarizes overall device and link health across the network, showing the current number of high-use, degraded, or down links. Click on the Show Topology Map link at the bottom of the tile to open the Network Visualization application and get more details.
4	Health Insights Tile: Summarizes the number of affected devices and KPIs reporting problems, as a result of alerts generated over the reporting interval. Click on the View Health Insights Dashboard link at the bottom of the tile to open the Health Insights application and get more details.
5	Change Automation Tile: The ring chart summarizes the state of Playbook execution, showing how many of your playbooks are running, scheduled to run, succeeded, and failed. Click on the View Change Automation Dashboard link at the bottom of the tile to the Change Automation application and get more details.
6	<p>The  icon lets you access the list of current notifications, alerts and messages.</p> <p> The About icon displays the current version of Cisco Crosswork Change Automation and Health Insights.</p> <p> The User Account icon lets you view the currently logged in user's name, change your password, and log out.</p>
7	Home: Returns you to the Dashboard from any other window. The dashboard tiles on this window provide at-a-glance views of the most important data in your network.
8	Change Automation Menu: Lets you select from the options available in the Change Automation application, which automates the process of deploying changes to the network. Click the blue View Change Automation Dashboard link at the bottom of the Change Automation tile to bypass the menu and open the Change Automation application directly.
9	Health Insights Menu: Lets you select from the options available in the Health Insights application, which allows you to view the Alert Dashboard, Manage KPIs and KPI Profiles, enable or disable KPI Profiles on selected devices, and see the KPI Profile Job History. Click the blue Show Health Insights Dashboard link at the bottom of the Health Insights tile to bypass the menu and open the Health Insights application directly.

Item	Description
10	Network Visualization Menu: Lets you select from the options available in the Network Visualization application, which presents both a geographical and a logical map view of the devices in your network, their topology and the links between them, the general condition of those devices and links, and other information. Click the blue Show Topology Map link at the bottom of the Network Visualization tile to bypass the menu and open the Network Visualization application directly.
11	Device Management Menu: Lets you select from the options available in the Device Management application, which lets you add, organize, update and view information about the devices in your network; manage the credential profiles you use; provision and onboard devices to inventory; and view Job History for all device-related tasks.
12	<p>Admin Menu: Lets you access the Administrative section of the user interface, where you can:</p> <ul style="list-style-type: none"> • Collect Cisco show-tech and logs • Monitor system activity and restart services • Manage users, roles, AAA TACACS+, and AAA LDAP servers • Manage the providers and tags you use • Change Network Visualization topology map settings • Manage certificates • Manage Cisco Crosswork Data Gateway and collection jobs • Register with Cisco Smart Licensing

Set, Sort and Filter Table Data

Many Cisco Crosswork Change Automation and Health Insights windows show database records in tables. For example: You will see tables in the **Devices** and **Credentials** windows accessed directly from Device Management, and also in the **Links** window accessed via the topological map in Network Visualization.

Any window with a table will also provide column selection, sorting, and filter functions that let you control the database records shown in the tables and help you locate particular records quickly.

Click  to display a list of all the fields in the database for the kind of data record displayed in the table. You can choose which fields you want to display as table columns by checking or unchecking the box next to any field in the list. Your choices are enabled immediately and are permanent.

You can also sort all the records displayed in the table according to the data in any one column by clicking that column's title:

- To sort the records in ascending order, click the column title once.
- To sort the records in descending order, click the column title again.

Sorting takes place immediately. You can only have one active sort at a time. The example **Links** window, below, shows an active sort on the **Link Type** field.

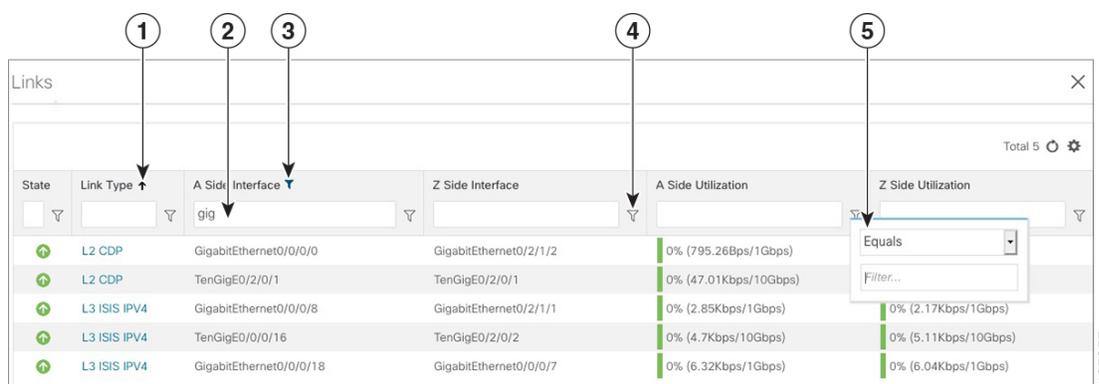
You can also filter the table to show only the records you want, using a quick filter or an advanced filter. Many tables have all these features enabled by default. If you cannot see the quick and advanced filter features displayed on a window with a table, click .

The quick filter displays only the records that match the value you enter above the column in the **quick filter** field (see item 2, below). Filtering takes place immediately, as you type.

The advanced filter (only available in some tables) narrows the content in the table by applying a filter that includes both a value and a logical operator, such as Equals, Starts with, Contains, and so on. Click  in the column header to access the advanced filter (see items 4 and 5, below).

In addition to these quick and advanced filters, you can also use tags to filter the devices shown in the **Devices** window and on the **Network Topology** map (see [Filter Network Devices by Tags](#), on page 101).

Figure 2: Links Window With Active Sort and Filters



Item	Description
1	Sort active icon: This arrow icon indicates that the user has sorted the links by clicking on the column header. The arrow's direction shows that the table is sorted by Link Type , in ascending order.
2	Quick filter field: Type a text or numeric value in this field to show only the links that match the value you enter. The field shows the values you entered for both quick and advanced filters.
3	Filter active icon: This icon shows that a quick or advanced filter is currently applied to the data in this column.
4	Advanced filter icon: Click  , shown in each column header, to specify an advanced filter on that column, using logical operators as well as alphanumeric values. Note Advanced filtering is not available on all tables.
5	Filter criteria fields: These fields appear in a popup next to the column after you click the  icon. Set the filter criteria by selecting the logical operator from the drop down list in the first field, and then entering the filter value in the second field. Your criteria will be applied immediately. You will then be prompted to enter more operators and values, and to decide if you want to concatenate them using logical AND or OR. The quick filter field shows the values you entered (but not the operators). Logical operators include Equals, Not equal, Starts with, Ends with, Contains, and Not contains.



CHAPTER 2

Get Started

This section contains the following topics:

- [Basic Concepts, on page 9](#)
- [Before You Begin, on page 10](#)
- [High-Level Workflow, on page 11](#)
- [Workflow 1: Setup, on page 12](#)
- [Workflow 2: Monitor Key Performance Indicators, on page 14](#)
- [Workflow 3: Respond to KPI Data, on page 14](#)
- [Workflow 4: Schedule Playbooks, on page 15](#)
- [Workflow 5: Develop Custom KPIs, on page 16](#)
- [Workflow 6: Develop Custom Playbooks, on page 16](#)
- [Workflow 7: Set Up Data Collection for External Data Destinations, on page 17](#)
- [Workflow 8: Add Additional Device Collection Support, on page 19](#)

Basic Concepts

Cisco Crosswork Change Automation and Health Insights makes extensive use of three basic concepts. It is helpful to be familiar with them before you get started.

- **Tags:** Tags will be familiar from other Web applications. They are simple text strings you can attach to objects to help group them. Cisco Crosswork Change Automation and Health Insights 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. For example, in addition to type and geolocation, which are already stored when you on-board devices, you may want to identify and group them by their location in your network topology (Spine vs. Leaf), or the function they serve on your network (Provider vs. ProviderEdge). Tags are especially useful when setting up KPI monitoring, as you can apply a KPI to every member of a tagged group. You will want to develop your own tags for your purposes, and rework them as needed to meet changing needs.
- **Providers:** Cisco Crosswork Change Automation and Health Insights does not perform network discovery, inventory collection, monitoring, or configuration changes directly. Instead, it relies on providers, such as Cisco Network Services Orchestrator and Cisco WAN Automation Engine, to deliver these special services. The provider family determines the type of service that provider supplies to Cisco Crosswork Change Automation and Health Insights, and the parameters unique to that service, which must be configured. Because these providers are separate applications, you will be asked to register them and provide values for their unique parameters when you set up Cisco Crosswork Change Automation and

Health Insights. This architecture permits Cisco Crosswork Change Automation and Health Insights to devote all of its resources to processing and interpreting network events and rolling out changes in response to these events.

- **Credential Profiles:** For Cisco Crosswork Change Automation and Health Insights to be able to access a device or to interact with a provider, it must be able to present credentials. Rather than entering credentials each time they are needed, you can instead create credential profiles to securely store this information. The platform supports unique credentials for each type of access protocol, and allows you to bundle multiple protocols and their corresponding credentials in a single profile. Devices that use the same credentials can share a credential profile. For example, if all of your routers in a particular building share a single SSH user ID and password, you can create a single credential profile to allow Cisco Crosswork Change Automation and Health Insights to access and manage them.

Before You Begin

Before you begin using Cisco Crosswork Change Automation and Health Insights, Cisco recommends that you complete the following planning and information-gathering steps:

- **User Accounts :** Cisco recommends as a best practice that you create separate accounts for all of your users, so that there is an audit record of user activity on the system. Prepare a list of the people who will use Cisco Crosswork Change Automation and Health Insights. Decide on their user names and preliminary passwords, and create user profiles for them (see [Manage Users, on page 164](#)).
- **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 (see [Create User Roles, on page 168](#)).
- **Credentials:** Gather the access credentials for your providers and for each supported protocol that you will use to monitor and manage your devices. For providers, this always includes user IDs, passwords, and connection protocols. For devices, it includes user IDs, passwords, and additional data such as the SNMP v2 read and write community strings, and SNMPv3 auth and privilege types. You will use these to create credential profiles (see [Basic Concepts, on page 9](#) and [Manage Credential Profiles, on page 81](#)).
- **Tags:** 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. As explained in [Basic Concepts, on page 9](#), you will want to consider grouping devices by functionality, so that you can apply KPI monitoring to tagged groups easily. You need not have a complete list of tags at first, as you can always add more later, but please note that all the tags you do plan to use must be in place before you need them; you cannot create them "on the fly" (see [Manage Tags, on page 188](#) and [Create Tags, on page 190](#)).
- **Providers:** As explained in [Basic Concepts, on page 9](#), providers do the basic work of direct interaction with network devices, so that Cisco Crosswork Change Automation and Health Insights can automate monitoring and responses to network events. Cisco Network Services Orchestrator (Cisco NSO) is the default provider used in nearly every Cisco Crosswork Change Automation and Health Insights installation, so you will need to gather the Cisco NSO IP address or host name, port and protocol, and the credentials to be used to communicate with it (which you will need to add as a credential profile). You will need to do the same for any other providers you may plan to use, such as Cisco Software Manager or Cisco WAN Automation Engine (see [Manage Providers, on page 170](#) and [Add Cisco NSO Providers, on page 178](#)).

This includes system service providers, such as an FTP server to store syslogs, or Cisco Crosswork Situation Manager for processing alerts.

- **Devices:** Decide how you are going to onboard your devices: manually, via the user interface, or automatically via synchronization or CSV import. This determines the amount of additional information you will need to onboard your devices, which is covered in [About Adding Devices to Inventory, on page 90](#).
- **External Data Destination(s):** Decide which external data destination (Kafka or gRPC) you are going to use and ensure it is set up to receive input from Cisco Crosswork Data Gateway.
- **KPI Profile(s):** KPIs (Key Performance Indicators) are used to monitor the health of the network. You can establish unique performance criteria based on the way a device or devices are used in the network. KPIs can be grouped to form a KPI Profile. It is helpful if you to have a good idea of the data you plan to monitor and the performance targets that you want to establish as you setup Health Insights.

Note that you can capture the devices, credential profiles, tags, and providers lists in spreadsheet form, convert the spreadsheet to CSV format, and then upload them in bulk to Cisco Crosswork Change Automation and Health Insights. You do this using the Import feature (accessed using the Import icon, )

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.

High-Level Workflow

The following workflow describes the main steps to getting started with Cisco Crosswork Change Automation and Health Insights.

Step	For details, see...
1. Populate the Cisco Crosswork Change Automation and Health Insights environment and set up Cisco Crosswork Data Gateway.	Workflow 1: Setup
2. Create KPI Profiles to monitor device Key Performance Indicators (KPIs) for issues and anomalies.	Workflow 2: Monitor Key Performance Indicators, on page 14
3. Link KPIs to playbooks.	Workflow 3: Respond to KPI Data, on page 14
4. Schedule Playbooks to perform routine maintenance.	Workflow 4: Schedule Playbooks, on page 15
5. Expand telemetry insight with custom KPIs.	Workflow 5: Develop Custom KPIs, on page 16
6. Remediate common scenarios and automate routine tasks with custom playbooks.	Workflow 6: Develop Custom Playbooks, on page 16

Step	For details, see...
7. Create collection jobs for external data destinations. Note This is applicable only if the add on entitlement license for Cisco Crosswork Data Gateway API access has been purchased.	Workflow 7: Set Up Data Collection for External Data Destinations, on page 17
8. Adding additional device collection support	Workflow 8: Add Additional Device Collection Support, on page 19

Workflow 1: Setup

The first step in getting started with Cisco Crosswork Change Automation and Health Insights is to prepare the system for use. The table below provides topics to refer to for help when executing each of the following tasks:

1. Create a credential profile for at least one provider
2. Gather the setup for the provider using that credential profile
3. Create credential profiles for the devices from that provider
4. Get the devices from that provider
5. Create tags.
6. Create any additional credential profiles for other providers you need, the setup for those providers, and credential profiles for the devices from those providers
7. Add devices to Cisco Crosswork Data Gateway.



Note This workflow assumes that you have already installed and enrolled Cisco Crosswork Data Gateway as explained in *Cisco Crosswork Change Automation and Health Insights 3.2 Installation Guide*.

If you were able to complete the recommended planning steps explained in [Before You Begin, on page 10](#), you should have all the information you need to finish each step in this workflow.

Step	Action
1. Ensure that your devices are themselves configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: Prerequisites for Onboarding Devices, on page 91 Sample Configuration for Devices in Cisco NSO, on page 93 Prerequisites for Device Model Driven Telemetry, on page 239

Step	Action
2. Create credential profiles for your device provider and for your devices.	Follow the steps in Create Credential Profiles , on page 82
3. Add the provider (Cisco NSO).	Follow the steps in About Adding Providers , on page 172
4. Validate communications with the provider.	Check on the provider's reachability using the steps in Get Provider Details , on page 186
5. Import or create tags.	To import them: Import Tags , on page 190 To create them: Create Tags , on page 190
6. Onboard devices using the method you prefer.	See About Adding Devices to Inventory , on page 90
7. Attach devices to Cisco Crosswork Data Gateway.	Review the Data Gateways pane (see Manage Cisco Crosswork Data Gateway Instances , on page 208). The operational state of the Cisco Crosswork Data Gateway instance to which you want to attach devices must be Up . Follow the steps in Attach a Device to a Cisco Crosswork Data Gateway Instance , on page 217
8. Validate Cisco Crosswork Change Automation and Health Insights communications with devices.	Review the Devices window (see Manage Network Devices , on page 89). All the devices you have onboarded should be reachable. Click  to investigate any device whose Reachability State is marked as  (unreachable),  (degraded), or  (unknown).
9. (Optional) Create additional user accounts.	Follow the steps in Add Users , on page 165
10. (Optional) Import or create additional credential profiles and providers.	To import providers: Import Providers , on page 175 To create providers: Add Providers Through the UI , on page 173

Workflow 2: Monitor Key Performance Indicators

Once you have completed initial setup, use Cisco Crosswork Change Automation and Health Insights to begin device performance monitoring using KPI Profiles.

Step	Action
1. (Optional) Tag all of the devices whose KPIs you plan to monitor with a tag indicating the function they perform, per your plan.	Follow the tasks in the Manage Tags, on page 188 section. You can Create Tags , or Import Tags , and then Apply or Remove Device Tags you want to monitor.
2. Plan which Cisco-supplied KPIs you want to begin using, based on each device's function and the device performance characteristics you want to monitor.	Review the Cisco-supplied KPIs documented in List of Health Insights KPIs, on page 58 .
3. Group the relevant KPIs to form KPI Profiles.	Follow the instructions in Create a New KPI Profile, on page 44 .
4. Enable the appropriate KPI Profiles on the devices you want to monitor.	Review and follow the instructions in Monitor Network Health and KPIs, on page 41

Workflow 3: Respond to KPI Data

The following workflow describes the steps to follow when using Cisco Crosswork Change Automation and Health Insights Playbook to reconfigure the network in response to changes in performance detected by your selected KPIs (after associating the Playbooks to the KPIs):

Step	Action
1. Research the KPIs that are triggering alerts, and determine the best corrective action to take for the situation your network has experienced.	Follow the instructions in Monitor Network Health and KPIs, on page 41 , using the View Alerts for Network Devices to research the alerts and their possible causes.
2. Review the Cisco-supplied Playbooks and determine which ones will allow you to address the situation.	Review the list of Plays, Playbooks, and generic parameters in the "Playbooks" and "Verbs" references in the Change Automation Developer Guide on Cisco Devnet .

Step	Action
3. Try out the selected Playbooks and see if they are applicable to your purposes. As you experiment, adjust the Playbook parameters as needed.	See: Perform a Dry Run of a Playbook, on page 25 Run Playbooks In Single Stepping Mode, on page 27 Run Playbooks In Continuous Mode, on page 30
4. If the Playbooks are appropriate for your purposes, and the situation occurs often, link the selected Playbooks and KPIs, so alerts triggered by a KPI will always display the linked Playbook for selection by operators. Once the KPI and Playbook are linked, operators can click on the Remediation icon, modify the Playbook parameters as needed, and execute the selected Playbook.	Follow the steps in Link KPIs to Playbooks, on page 55 . Use the Remediation icon shown in View Alerts for Network Devices, on page 50 to trigger a run of a linked Playbook from a device or KPI alert.

Workflow 4: Schedule Playbooks

The workflow below describes the steps to follow when using Cisco Crosswork Change Automation and Health Insights to automate routine network upkeep, and to verify that each routine change completed correctly.

Step	Action
1. Identify routine maintenance tasks (such as throughput checks, software upgrades, SMU installs, and so on) that you perform on a regular schedule and that may be suitable for automation using one or more Cisco Crosswork Change Automation and Health Insights Playbooks.	See About Running Playbooks, on page 23 and View the Playbook List, on page 22
2. Configure Playbooks to perform these tasks at the desired time.	See About Running Playbooks, on page 23 and Schedule Playbook Runs, on page 32
3. Review the Change Automation Job History to review the current status of the Playbook and confirm that it ran successfully.	See Use the Change Automation Dashboard, on page 22 and View or Abort Playbook Jobs, on page 34
4. Use the APIs to perform routine maintenance tasks from your own scripts and applications.	See the Cisco Crosswork Network Automation API Documentation on Cisco DevNet .

Workflow 5: Develop Custom KPIs

The following workflow describes the steps to follow when considering whether or not to develop Cisco Crosswork Change Automation and Health Insights custom KPIs for your special needs, and how to proceed if you decide you do.

Step	Action
1. Review the existing KPIs to make sure the telemetry you want to monitor is not already available.	Follow the instructions in Monitor Network Health and KPIs, on page 41 , using the View Alerts for Network Devices to research the alerts and their possible causes.
2. Review the data available from the devices you want to monitor to see if they can supply the needed information: <ul style="list-style-type: none"> • If they can, proceed with building a custom KPI. • If they cannot: Contact Cisco to see if we can include the required data in a future version of the device code. <p>The latest information on the data your devices can provide is always available at the Cisco Telemetry Data Mapper (https://tdm.cisco.com).</p>	Review the KPIs in List of Health Insights KPIs, on page 58 .
3. Build the custom KPI and add it to a KPI Profile.	See Create a New KPI, on page 54 and Create a New KPI Profile, on page 44
4. Enable the new KPI Profile on a test device and confirm that the data reported matches your expectations. Be aware that KPIs that depend on data over time to establish baseline performance will need some time to "calibrate" before they provide meaningful data.	See Enable KPI Profile on Devices, on page 47 and View Alerts for Network Devices, on page 50
5. If the KPI Profile is meeting expectations, enable it on all devices where you consider it applicable.	Follow the steps in Enable KPI Profile on Devices, on page 47 .
6. Review the Health Insights Job History to make sure the KPI Profile was deployed to all targeted devices	See Verify the Deployment Status of Enabled KPIs, on page 57

Workflow 6: Develop Custom Playbooks

The following workflow describes the steps to follow when deciding to develop a Cisco Crosswork Change Automation and Health Insights custom Playbook.

Step	Action
1. Review the existing Playbook to see if any of them meet your needs fully or partially.	Review the Plays, Playbooks, and parameters in the "Playbooks" and "Verbs" references in the Change Automation Developer Guide on Cisco Devnet .
2. Find the Playbook that most closely matches your requirements and export that Playbook. Once you get good at modifying Playbook, you may choose to build them from scratch and skip this step.	See Export Playbooks, on page 37
3. Modify the exported Playbook or create a new Playbook as necessary to meet your requirements.	Review the "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet .
4. Import the new Playbook and then perform a dry run, or run it in single-stepping or continuous mode against a test device or devices, to confirm that it performs as expected.	First, follow the instructions in Import Playbooks, on page 38 . Then: Perform a Dry Run of a Playbook, on page 25 Run Playbooks In Single Stepping Mode, on page 27 Run Playbooks In Continuous Mode, on page 30
5. For a Playbook you have developed that meets your needs: <ul style="list-style-type: none"> • In response to KPI alerts: If the Playbook is meeting expectations, link it to the KPI that indicates the need for the Playbook to be run, so that it is easy for operators to trigger the Playbook in response. • For planned maintenance or configuration changes: Schedule the Playbook to run, or run it, at the planned time. 	See: Link KPIs to Playbooks, on page 55 Schedule Playbook Runs, on page 32

Workflow 7: Set Up Data Collection for External Data Destinations

Crosswork allows you to add two types of external data destinations:

- Kafka Server
- gRPC Server

The following workflow describes the steps to follow to add external destinations to Crosswork and create collection jobs to feed these external data destinations.

Step	Action
<p>1. Ensure that you have set up the external data destination servers that you want to use.</p> <p>Also, if you are using an external Kafka server, ensure that you have created Kafka topics prior to Crosswork using them.</p>	<p>The target destination installation and administration are left to the user and outside the scope of this document. Please refer your Kafka/gRPC administration and configuration guide.</p> <p>Refer to the guidelines and sample configurations in:</p> <ul style="list-style-type: none"> Prerequisites for Onboarding Devices, on page 91 Sample Configuration for Devices in Cisco NSO, on page 93 Prerequisites for Device Model Driven Telemetry, on page 239
<p>2. Add a data destination to Crosswork.</p>	<p>Review the Data Destinations pane (see Manage Data Destinations, on page 224).</p> <p>Follow the steps in Add a Data Destination, on page 225.</p>
<p>3. Ensure that prerequisites for device telemetry are met.</p>	<p>Refer to the guidelines and sample configurations in:</p> <ul style="list-style-type: none"> Prerequisites for Device Model Driven Telemetry, on page 239
<p>4. Create collection jobs</p>	<p>Refer to the following topics (in order of their listing) for guidelines and sample configurations:</p> <ol style="list-style-type: none"> 1. About Collection Jobs, on page 242 2. Collection Job Payload Model, on page 242 3. Collection Jobs, on page 249 4. Best Practices and Limitations for Creating Collection Jobs, on page 248 <p>Then, follow the steps in Create Collection Jobs, on page 248.</p>
<p>5. Monitor collection jobs for status updates, issues, and alerts.</p>	<p>See Monitoring Collection Jobs, on page 259.</p>

Workflow 8: Add Additional Device Collection Support

Cisco Crosswork Data Gateway allows you to register and deploy three types of custom software packages to expand device coverage for external data collection:

1. CLI Device Package
2. Custom MIB Packages
3. SNMP Device Packages

The following workflow describes the steps to follow to add a custom package.

Step	Action
1. If you want to use a CLI Device Package, Custom MIB Package, or an SNMP Device Package, add them to Cisco Crosswork Data Gateway prior to creating collection jobs.	Review the Custom Software pane (see Manage Custom Software Packages, on page 232). Follow the steps in Add a Custom Software Package, on page 234



CHAPTER 3

Automate Network Changes

This section contains the following topics:

- [Change Automation Overview, on page 21](#)
- [About Running Playbooks, on page 23](#)
- [About Customizing Playbooks, on page 35](#)
- [Troubleshoot Change Automation, on page 39](#)

Change Automation Overview

The Change Automation application automates the process of deploying changes to the network. You can define automation tasks to achieve the intended network states in Change Automation using Playbooks that consists of plays written using YAML. You can then push configuration changes to Cisco Network Service Orchestrator (NSO), which deploys these changes to the network devices.

The difference between Change Automation and other existing scripted automation frameworks is that Change Automation is a *closed-loop framework*. Changes are deployed to the router or other device using programmable APIs, and the intent of the change is verified using telemetry that comes back from the router. Change Automation relies on telemetry to verify the intent of the change, avoiding the need to frequently poll the device for updates.

Traditional open source-based implementations use CLI towards network devices without a configuration store, which leads to out-of-sync states. Driving network configuration change with a store provides transactional rollback and locking abilities and enables a single source of truth for device configuration.

The following is a high-level Change Automation workflow:

1. Define your desired network changes in a Change Automation Playbook.
2. Push configuration changes to the network device indirectly, using Cisco Network Services Orchestrator, a configuration services provider.
3. Receive real-time feedback via telemetry from the devices, telling you that the network changes were made and the impact of the changes. You can also use post-change KPIs to determine if a particular change should be undone and the devices returned to their previous configuration.

Change Automation comes with a robust library of Playbooks, each with its own collection of atomic configuration and check plays. (A Playbook consists of multiple *plays*.)

You can configure what each Playbook does by specifying the values of runtime parameters to create a Playbook Job. With the correct programming skills, you can download, modify and then upload and run your

own versions of the Cisco-supplied Playbooks, or create your own custom Playbooks. For more information, see [About Customizing Playbooks, on page 35](#)

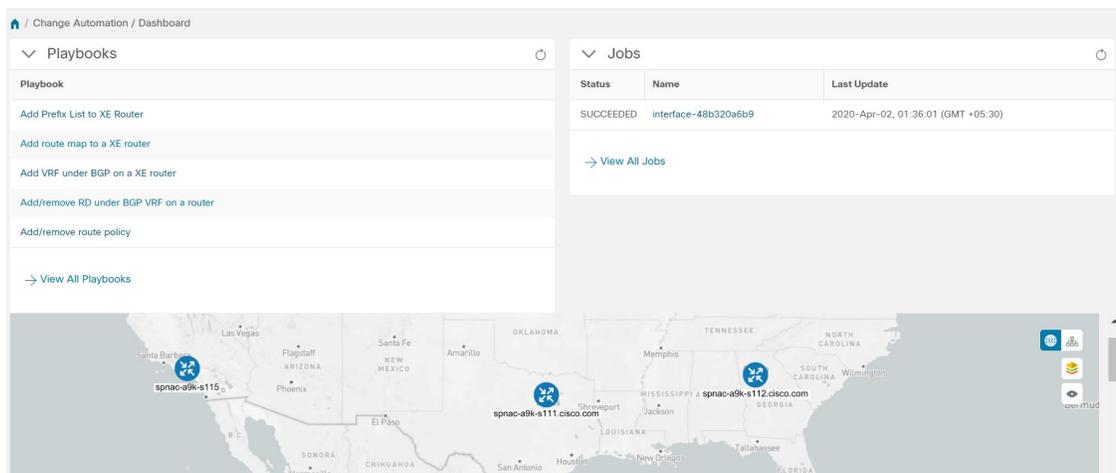
Use the Change Automation Dashboard

The Change Automation application's **Dashboard** window (shown in the following figure) lets you view all Playbook-related activity and initiate Playbook runs. It displays an alphabetical list of Playbooks, the most recently run Playbook jobs, and the same network topology map you see when you select **Network Visualization > View Topology**. For help using the topology map, see [Network Visualization Overview, on page 65](#).

To view the Change Automation **Dashboard** window, select **Change Automation > Dashboard**.

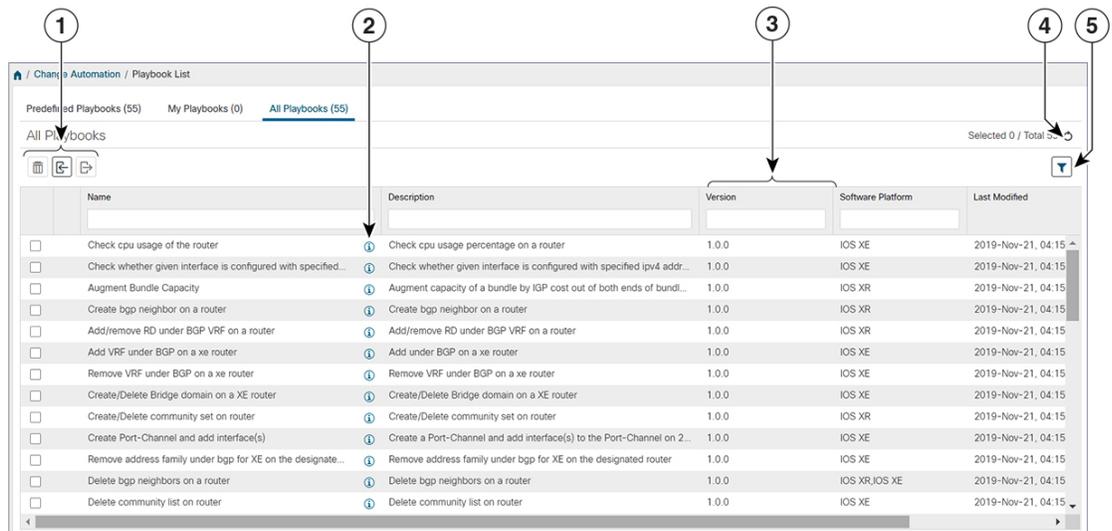
The **View All Playbooks** and **View All Jobs** links on the **Dashboard** window give you direct access to the Change Automation **Run Playbook** and **Job History** windows, respectively. For help using these two windows, see the topics in the section [About Running Playbooks, on page 23](#).

Figure 3: Change Automation Dashboard Window



View the Playbook List

The Change Automation application's **Playbook List** window (in the following figure) gives you a consolidated list of all the Playbooks in the system. To view the **Playbook List** window, select **Change Automation > Playbook List**.



Item	Description
1	<p>Click  to delete the currently selected custom Playbook. See Delete Custom Playbooks, on page 38.</p> <p>Click  to import Playbooks from a gzipped TAR archive file. See Import Playbooks, on page 38.</p> <p>Click  to export the currently selected Playbook(s) as a gzipped TAR archive file. See Export Playbooks, on page 37.</p>
2	<p>Click  to see a popup Playbook Details window showing the Playbook's description, hardware and software compatibility, version number, and its plays. When you are finished viewing these details, click  to close the popup window.</p>
3	<p>Click on the Name, Description, Version, Software Platform, and Last Modified column headings in the table to sort the table by that column's data. You can also choose which columns are shown, and set quick or advanced filters on any column. See Set, Sort and Filter Table Data, on page 6.</p>
4	<p>Click  to refresh the Playbooks list.</p>
5	<p>Click  to set filter criteria on one or more columns in the table.</p> <p>Click the Clear Filter link to clear any filter criteria you may have set.</p>

About Running Playbooks

Running any Playbook consists of five steps:

1. Select the **Playbook** you want to run (see [View the Playbook List, on page 22](#)).

2. Select the **device or devices** you want to run it on.
3. Enter the appropriate runtime **parameters** you want the Playbook to apply.
4. Select the **execution mode** you want to use:
 - a. [Perform a Dry Run of a Playbook, on page 25](#), where you can see what the Playbook will do before you commit to making changes to the network.
 - b. [Run Playbooks In Single Stepping Mode, on page 27](#), so you have a chance to pause after each Playbook check or action, and roll back changes you did not intend.
 - c. [Run Playbooks In Continuous Mode, on page 30](#) and apply the changes immediately.

While selecting the execution mode, you can also choose to:

- [Schedule Playbook Runs, on page 32](#) for another calendar date or time.
- **Collect syslogs** during and after the run. Syslog collection is available only when running the Playbook in single-stepping or continuous execution mode, and only if you have already configured a syslog storage provider (see [Add Syslog Storage Providers, on page 183](#)).
- Specify a **Failure Policy**, where you decide what the system should do in case a failure occurs at any time during the Playbook run.

5. **Confirm** your settings and run the Playbook in the execution mode you selected.

Depending on their complexity and on network factors, some Playbooks may take a lot of time to run. At any time during and after completion of a run, you can view the run details and status. If the Playbook is still running, you can also choose to abort it. For details, see [View or Abort Playbook Jobs, on page 34](#).

Playbook Execution Order

When it is running, every Playbook conducts checks and configuration changes in four phases, which correspond to sections of the Playbook code (identified using the tags discussed in [Playbook Components and Files, on page 36](#)):

1. **Pre-Maintenance**—This phase of the Playbook includes non-disruptive checks and any other operations on the device that prepare it for potentially traffic-impacting changes. For example:
 - Take snapshots of various routing protocol states.
 - Take snapshots of memory, CPU, and system health parameters.
 - Validate the capacity (storage, memory) on active and standby routers for the new software patch upgrade.
2. **Maintenance**—This phase of the Playbook includes any task that may disrupt traffic flowing through the router or impact neighboring routers. For example:
 - Cost out the router and wait until traffic drains out completely.
 - Verify that the redundant router is healthy and carrying traffic.
 - Perform the upgrade procedure on the device.
 - Reconfigure the device(s) to support a new configuration or feature.

3. **Post-Maintenance**—This phase of the Playbook includes verification tasks to perform on the router after any disruptive operation. For example:
 - Verify that the current state matches the desired state.
 - Cost in the router and wait for traffic to return to normal levels.
4. **Continuous**—In addition to the three serial phases already described, Change Automation also runs check tasks that span the entire duration of Playbook execution. These tasks check the state of the router while the Playbook is being deployed, and cancel the Playbook execution if any catastrophic or undesirable state change occurs. The checks in the Playbook may also monitor a neighboring router to guarantee that there are no second-order failures in the network while the changes are being deployed.

Perform a Dry Run of a Playbook

A dry run lets you view configuration changes that the Playbook will send to the device, without performing the actual commit of the changes, as you would with a run in the single-stepping or continuous execution modes.

It is a best practice to perform a dry run and verify the configuration changes before you deploy those changes to the router. If the dry run fails, you may want to debug its parameter values using another dry run. You can also debug by performing a single-stepping run, which will allow you to abort and rollback changes after one or more of the plays, instead of only at the end, as part of a continuous run's Failure Policy.

Note that dry run mode is intended for use only with Playbooks that perform actual device configuration changes via Cisco NSO. See the "Playbooks" and "Verbs" references in the [Change Automation Developer Guide on Cisco Devnet](#) for details on Playbooks that do not support dry run mode. These will include, for example, Node state snapshot, Install optional package or SMU, and Uninstall optional package or SMU.

Step 1 From the main menu, choose **Change Automation > Run Playbook**.

Step 2 In the **Select Playbook** list on the left, click on the Playbook you want to dry run. On the right, the window displays the Playbook name, hardware and software compatibility information, and descriptions for all the plays in the selected Playbook.

Step 3 Click **Next**. The **Select Devices** window appears. Using this window:

- You can toggle between the table view and topology map view by clicking and selecting the relevant option on the drop-down button on the upper left corner of the window. Choose **Select Devices From List** or **Select Devices From Map** to select the table view or topology map view respectively. By default, the table view is displayed.
- With the topology map view displayed, you can toggle between the map's geographical and logical views by clicking on the  or the . You can also zoom, display bandwidth utilization, and change logical view layouts as you do with the topology map you see when you select **Network Visualization > View Topology** (see [Network Visualization Overview, on page 65](#)).
- You can select the devices using **Static** or **Dynamic using Tags** device selection options. **Static** selection allows you to select devices from the list using quick and advanced filters and filter by tags on the left. **Dynamic using Tags** selection targets you to select the relevant tag instead of devices from the table on the left side, and all devices associated with the relevant tag are selected. Hover the mouse pointer over the  icon next to the options for more information. You can also view the selection criteria such as number of devices required for the selected playbook.

- In **Static** selection mode, you can check the **Allow Bulk Jobs** check box to select multiple devices and run the selected playbook on them at the simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the  icon next to the check box for more information. There is no limitation on the number of devices you can select for a bulk job.

Note **Allow Bulk Jobs** option is enabled for playbooks that can be executed on a single device.

Step 4 The **Select Devices** window will prompt you to select one or more of the devices shown (depending on the Playbook). Click on the devices you want to select, then click **Next**. The **Parameters** window appears.

Step 5 In the fields provided in the **Parameters** window, enter the Playbook parameter values to use for this dry run.

With the **Parameters** window displayed, you can also:

- Click **JSON** to enter the parameter values in JSON format. A popup text window displays the full list of JSON parameters, with empty values in quotes. Edit the values and, when you are finished, click **Save**.
- Click  to upload a JSON file with the parameter values you want. You will be prompted to navigate to the JSON parameters file you have previously prepared (or downloaded from a previous Playbook run) and then upload it as appropriate for your browser and operating system.
- Click + **Add** to add additional instances of a particular parameter, if required for the Playbook you are running. Click **X Remove** to delete instances added in this way.
- Click  to clear all the parameter values entered so far.

Step 6 With the parameter values set, click **Next**. The **Execution Policy** window appears.

Step 7 Choose **Dry Run** and click **Next**. The **Review your Job** window appears, displaying a summary of all of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can assign tags to your job. Click **New Job Tag**, provide a name and color and save your settings to create your own tag. You can also select from the list of existing job tags by clicking the corresponding checkboxes. Click **Manage Job Tags** to create, edit or delete job tags.
- You can click on any of the **Change** links in the **Review your Job** window summary to modify your choices.

Step 8 When you are ready to continue, click **Run Playbook**.

Step 9 At the confirmation prompt, click **Confirm**. The **Execution Mode** window is displayed.

Step 10 After the dry run is complete:

- Click the **Dry Run** tab and verify the configuration changes that would be pushed to the device had this not been a dry run. This tab will display a `no config change` message if no changes would have been made. Please note that this tab shows only cumulative configuration changes, not each individual change made. For example, if a Playbook configures `set-overload-bit` in one step and then unconfigures it using `no set-overload-bit` in a later step, the tab will show `no config change`.
- Click the **Events** tab to see success and failure messages for each step of the Playbook. This can help you diagnose and correct problems with individual plays and the run as a whole.
- Click the **Console** tab to see messages that are generated during the run.

As syslog collection is disabled for drying runs, the **Syslog** tab will contain only a message stating that.

- Step 11** (Optional) If you want to perform a single-step debugging run, or are ready to commit the changes to the device, click **Execute Now**. The **Execution Policy** window will display, with all of your parameter values from the dry run pre-filled.
-

Run Playbooks In Single Stepping Mode

Single-stepping execution mode is a handy way to test a custom or modified Playbook, or diagnose problems with a pre-packaged Playbook that is not giving you the results you want. Unlike a dry run, a single-stepping execution commits configuration changes to the device as the Playbook runs. However, you can set breakpoints on or pauses after any Maintenance or Post-Maintenance action in the Playbook. Please note that, while you can set breakpoints on Pre-Maintenance actions, doing so will have no effect, and these actions will not pause.

Whenever the Playbook hits a breakpoint, it will stop, and will not continue until you issue the command to proceed. At each pause, you can also choose to abort the entire run and roll back all changes made, or rollback to any previous play.

- Step 1** From the main menu, choose **Change Automation > Run Playbook**.
- Step 2** In the **Select Playbook** list on the left, click on the Playbook you want to run. On the right, the window displays the Playbook name, hardware and software compatibility information, and descriptions for all the plays in the selected Playbook.
- Step 3** Click **Next**. The **Select Devices** window appears. Using this window:
- You can toggle between the table view and topology map view by clicking and selecting the relevant option on the drop-down button on the upper left corner of the window. Choose **Select Devices From List** or **Select Devices From Map** to select the table view or topology map view respectively. By default, the table view is displayed.
 - With the topology map view displayed, you can toggle between the map's geographical and logical views by clicking on the  or the . You can also zoom, display bandwidth utilization, and change logical view layouts as you do with the topology map you see when you select **Network Visualization > View Topology** (see [Network Visualization Overview](#), on page 65).
 - You can select the devices using **Static** or **Dynamic using Tags** device selection options. **Static** selection allows you to select devices from the list using quick and advanced filters and filter by tags on the left. **Dynamic using Tags** selection allows you to select the relevant tag from the table on the left side, and all devices associated with the relevant tag are selected. Hover the mouse pointer over the  icon next to the options for more information. You can also view the selection criteria such as number of devices required for the selected playbook.
 - In **Static** selection mode, you can check the **Allow Bulk Jobs** check box to select multiple devices and run the selected playbook on them at the simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the  icon next to the check box for more information. There is no limitation on the number of devices you can select for a bulk job.
- Note** **Allow Bulk Jobs** option is enabled for playbooks that can be executed on a single device.
- Step 4** The **Select Devices** window will prompt you to select one or more of the devices shown (depending on the Playbook). Click on the devices you want. Click **Next**.
- Step 5** Click **Next**. The **Parameters** window appears.
- Step 6** In the fields provided in the **Parameters** window, enter the Playbook parameter values to use for this run.

With the **Parameters** window displayed, you can also:

- Click **JSON** to enter the parameter values in JSON format. A popup text window displays the full list of JSON parameters, with empty values in quotes. Edit the values and, when you are finished, click **Save**.
- Click  to upload a JSON file with the parameter values you want. You will be prompted to navigate to the JSON parameters file you have previously prepared (or downloaded from a previous Playbook run) and then upload it as appropriate for your browser and operating system.
- Click + **Add** to add additional instances of a particular parameter, if required for the Playbook you are running. Click **X Remove** to delete instances added in this way.
- Click  to clear all the parameter values entered so far.

Step 7 With the parameter values set, click **Next**. The **Execution Policy** window appears.

Step 8 Choose **Single Stepping**. The **Execution Policy** window displays additional features to customize the job:

- Under **Collect Syslogs**, click **Yes** if you want syslogs to be collected during and immediately after the run, **No** if you do not. **Yes** is the default selection only if you have a syslog provider configured (see [Add Syslog Storage Providers, on page 183](#)).
- From the **Failure Policy** dropdown, select:
 - **Abort** to abort the entire run, without rolling back any changes, if a failure occurs at any point. This is the default. Any configuration changes made up to the point of failure will not be rolled back.
 - **Pause** to pause the run and allow you to decide how to handle the failure. This pause will be in addition to any breakpoints you set using the **Single stepping breakpoints** dropdown.
 - **Complete Roll Back** to abort the entire run and roll back all configuration changes made.
- In the **Schedule** area, uncheck the default **Run Now** selection to schedule the job for a later time. See [Schedule Playbook Runs, on page 32](#) for help on using the **Schedule** area features

Step 9 From the **Single stepping breakpoints** dropdown, select either

- **Every step** to pause automatically after every step in the Playbook.
- **Customize** to select the steps where you want the Playbook to pause.

If you select **Customize**, the **Customize Breakpoints** popup displays a list of all the plays in the Playbook, with a  at the step between each play. Click the  at each step where you want to set a breakpoint. When you are finished, click **Done**.

Step 10 Click **Next**. The **Review your Job** window appears, displaying a summary of all of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can assign tags to your job. Click **New Job Tag**, provide a name and color and save your settings to create your own tag. You can also select from the list of existing job tags by clicking the corresponding checkboxes. Click **Manage Job Tags** to create, edit or delete job tags.
- You can click on any of the **Change** links in the **Review your Job** window summary to modify your choices.

Step 11 When you are ready to continue, click **Run Playbook**.

- Step 12** At the confirmation prompt, click **Confirm**. The **Job History** window is displayed, with the details of the current job displayed on the right side. The job details include information such as job status, job set tags, title of selected playbook, execution parameters and policy, last updated date and update comments (if any). Click the  icon next to the detail to view more information.
- Step 13** While the run is executing, the blue **Running** tile at the top of the window will change to **Paused** for each step at which you have set a breakpoint. Your choices at each pause will be displayed as buttons below the blue tiles:
- Click **Resume** to resume running from this point, with no changes. The **Resume** request includes the runtime parameters from the previous step; you can edit these, as needed, later.
 - Click **Roll Back** to roll back any changes made so far. You can choose how far to rollback:
 - Click **Complete Roll Back** to roll back all changes to the start of the Playbook run. Once you have rolled back to the start, you can choose to **Resume** from that point, **Abort** the run entirely, or **Edit runtime parameters** of the run.
 - Click **Select Roll Back Point** to roll back changes to the step you select. All the previous steps will then have a roll back point icon displayed next to them: . Click the  for the step to which you want to roll back. Once you have selected the step, you can choose to **Resume** from that step, **Roll Back** further, **Abort** the run entirely, or **Edit runtime parameters**.
 - Click **Abort** to abort the run entirely. No changes made will be rolled back.
 - Click **Edit runtime parameters** to edit the parameters the run is using. You edit using a popup version of the **Parameters** window, just as you did in step 6. The parameters exposed for editing when resuming are specific to the task being resumed, which means that they are not the same global parameters you defined in step 6. Most of the time, they are a subset of the global parameters. When you are finished, click **Apply**. You can then choose to **Resume** execution with the changed parameters.
- Step 14** While the run is executing, you can also use the following features of the progress window:
- View the execution status of each play in the Playbook in the **Maintenance** play list at the left side of the window. Plays that fail are indicated with a red icon; plays that succeed are indicated with a green icon.
 - See reminders of your choices in the blue **Playbook** and **Devices** tiles at the top of the window.
 - See the current status of the run in the blue **Running** tile at the top of the window.
 - Click **View** in the **Parameters** tile to view the run's parameters. While viewing the parameters, you can click **Download Parameters** to save them in a JSON file. You will be prompted to name and save the file as appropriate for your browser and operating system.
 - Use the network topology in the map at the right side of the window to view the device and its connections to the rest of your network.
- Step 15** After the run is complete:
- Click the **Events** tab to see success and failure messages for each step of the Playbook. This can help you diagnose and correct problems with individual plays and the run as a whole.
 - Click the **Syslogs** tab to access syslog messages collected during and immediately after the run. If syslog collection is enabled, the tab will provide a pointer to the path on the syslog storage provider where collected syslogs are stored. If you chose not to collect syslogs, or no syslog storage provider has been configured, this tab will display a message indicating that syslog collection is disabled.

- Click the **Console** tab to see relevant commands and responses from the device consoles that took place during the run. These messages can also help with diagnostics.

Run Playbooks In Continuous Mode

Continuous execution mode is the standard way to run Playbooks. Configuration changes are committed to the device during the run, with no checks or delays except those programmed into it for system resets or other purposes. The run continues until it succeeds or fails. If it fails, you can use the run's Failure Policy to abort, rollback all changes made to the device, or pause execution at the failure point.

It is always good practice to perform a dry run and verify the configuration changes before committing to a continuous run (see [Perform a Dry Run of a Playbook, on page 25](#)). You can also run the Playbook in single-stepping mode, which will allow you to pause execution after any play you select, abort and rollback changes as needed, and even change runtime parameters in the middle of the run (see [Run Playbooks In Single Stepping Mode, on page 27](#)).

- Step 1** From the main menu, choose **Change Automation > Run Playbook**.
- Step 2** In the **Select Playbook** list on the left, click on the Playbook you want to run. On the right, the window displays the Playbook name, hardware and software compatibility information, and descriptions for all the plays in the selected Playbook.
- Step 3** Click **Next**. The **Select Devices** window appears. Using this window:
- You can toggle between the table view and topology map view by clicking and selecting the relevant option on the drop-down button on the upper left corner of the window. Choose **Select Devices From List** or **Select Devices From Map** to select the table view or topology map view respectively. By default, the table view is displayed.
 - With the topology map view displayed, you can toggle between the map's geographical and logical views by clicking on the  or the . You can also zoom, display bandwidth utilization, and change logical view layouts as you do with the topology map you see when you select **Network Visualization > View Topology** (see [Network Visualization Overview, on page 65](#)).
 - You can select the devices using **Static** or **Dynamic using Tags** device selection options. **Static** selection allows you to select devices from the list using quick and advanced filters and filter by tags on the left. **Dynamic using Tags** selection allows you to select the relevant tag from the table on the left side, and all devices associated with the relevant tag are selected. Hover the mouse pointer over the  icon next to the options for more information. You can also view the selection criteria such as number of devices required for the selected playbook.
 - In **Static** selection mode, you can check the **Allow Bulk Jobs** check box to select multiple devices and run the selected playbook on them at the simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the  icon next to the check box for more information. There is no limitation on the number of devices you can select for a bulk job.
- Note** **Allow Bulk Jobs** option is enabled for playbooks that can be executed on a single device.
- Step 4** The **Select Devices** window will prompt you to select one or more of the devices shown (depending on the Playbook). Click on the devices you want to select them, then click **Next**. The **Parameters** window appears.
- Step 5** In the fields provided in the **Parameters** window, enter the Playbook parameter values to use for this dry run.

With the **Parameters** window displayed, you can also:

- Click **JSON** to enter the parameter values in JSON format. A popup text window displays the full list of JSON parameters, with empty values in quotes. Edit the values and, when you are finished, click **Save**.
- Click  to upload a JSON file with the parameter values you want. You will be prompted to navigate to the JSON parameters file you have previously prepared (or downloaded from a previous Playbook run) and then upload it as appropriate for your browser and operating system.
- Click + **Add** to add additional instances of a particular parameter, if required for the Playbook you are running. Click **X Remove** to delete instances added in this way.
- Click  to clear all the parameter values entered so far.

Step 6 With the parameter values set, click **Next**. The **Execution Policy** window appears.

Step 7 Choose **Continuous**. The **Execution Policy** window displays additional features to customize the job:

- Under **Collect Syslogs**, click **Yes** if you want syslogs to be collected during and immediately after the run, **No** if you do not. **Yes** is the default selection only if you have a syslog provider configured (see [Add Syslog Storage Providers, on page 183](#)).
- From the **Failure Policy** dropdown, select:
 - **Abort** to abort the entire run, without rolling back any changes, if a failure occurs at any point. This is the default. Any configuration changes made up to the point of failure will not be rolled back.
 - **Pause** to pause the run and allow you to decide how to handle the failure.
 - **Complete Roll Back** to abort the entire run and roll back all configuration changes made.
- In the **Schedule** area, uncheck the default **Run Now** selection to schedule the job for a later time. See [Schedule Playbook Runs, on page 32](#) for help on using the **Schedule** features.

Step 8 Click **Next**. The **Review your Job** window appears, displaying a summary of all of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can assign tags to your job. Click **New Job Tag**, provide a name and color and save your settings to create your own tag. You can also select from the list of existing job tags by clicking the corresponding checkboxes. Click **Manage Job Tags** to create, edit or delete job tags.
- You can click on any of the **Change** links in the **Review your Job** window summary to modify your choices.

Step 9 When you are ready to continue, click **Run Playbook**.

Step 10 At the confirmation prompt, click **Confirm**. The **Job History** window is displayed, with the details of the current job displayed on the right side. The job details include information such as job status, job set tags, title of selected playbook, execution parameters and policy, last updated date and update comments (if any). Click the  icon next to the detail to view more information.

Step 11 While the run is executing, the blue **Running** tile at the top of the window will change to **Paused** if you chose a **Failure Policy** of **Pause**. Your choices will be displayed as buttons below the blue tiles:

- Click **Resume** to resume running from this point, with no changes.
- Click **Roll Back** to roll back any changes made so far.
- Click **Abort** to abort the run entirely. No changes made will be rolled back.

Step 12 While the run is executing, you can also use the following features of the progress window:

- View the execution status of each play in the Playbook in the **Maintenance** play list at the left side of the window. Plays that fail are indicated with a red icon; plays that succeed are indicated with a green icon.
- See reminders of your choices in the blue **Playbook** and **Devices** tiles at the top of the window.
- See the current status of the run in the blue **Running** tile at the top of the window.
- Click **View** in the **Parameters** tile to view the run's parameters. While viewing the parameters, you can click **Download Parameters** to save them in a JSON file. You will be prompted to name and save the file as appropriate for your browser and operating system.
- Use the network topology in the map at the right side of the window to view the device and its connections to the rest of your network.

Step 13 After the run is complete:

- Click the **Events** tab to see success and failure messages for each step of the Playbook. This can help you diagnose and correct problems with individual plays and the run as a whole.
- Click the **Syslogs** tab to access syslog messages collected during and immediately after the run. If syslog collection is enabled, the tab will provide a pointer to the path on the syslog storage provider where collected syslogs are stored. If you chose not to collect syslogs, or no syslog storage provider has been configured, this tab will display a message indicating that syslog collection is disabled.
- Click the **Console** tab to see relevant commands and responses from the device consoles that took place during the run. These messages can also help with diagnostics.

Schedule Playbook Runs

The Change Automation application's **Execution Mode** window allows you to schedule future Playbook runs as jobs, and view all the jobs that have been scheduled. Use the **Schedule** area on the left to schedule a job. Use the **All Scheduled Jobs** area on the right to view scheduled jobs on the calendar.

The **Execution Mode** window's scheduling features are only displayed when you have chosen to run a Playbook in continuous or single-stepping mode. You cannot schedule a dry run of a Playbook.

Figure 4: Execution Mode Scheduling Features

Item	Description
1	Run Now: Running Playbooks immediately is the default for continuous and single-stepping execution modes. To schedule a run for a future time and date, you must uncheck this box.
2	Schedule Selectors: Use these fields to select the future time and date when the Playbook runs. Although it is the default for the Pre-Maintenance and Maintenance phases of a scheduled Playbook to start at the same time, you can use the upper Schedule Pre-check and lower Schedule Perform fields to schedule the start of Pre-Maintenance and the start of Maintenance independently. Note that the Schedule Perform time must always be greater than or equal to the Schedule Pre-check time.
3	Previous/Today/Next Selectors: Use these three selectors with the Month/Week/Day selectors to focus the calendar's display of scheduled jobs on the time range in which you are interested. For example: To show only those jobs scheduled for next week, click Next and Week .
4	Job Icons: Red, numbered icons in the squares representing each calendar date show how many jobs are scheduled for that date. Yellow circle icons represent each scheduled job.
5	Job Details Popup: Hover your mouse cursor over a yellow circle icon to see the details for the scheduled job represented by that icon. The popup shows the execution ID of the job and the name of the Playbook to be run.
6	Show jobs for selected devices only: Check this box to restrict the calendar display to only those jobs scheduled to run on the devices you have already selected. This is a handy way to see if the schedule you plan for your Playbook run will conflict with other scheduled jobs on the same devices.
7	Month/Week/Day Selectors: Use these three selectors with the Previous/Today/Next selectors to focus the calendar's display of scheduled jobs on the time range in which you are interested. For example: To show only those jobs scheduled for last month, click Last and Month .



Note Change Automation Playbooks have a `mop_timeout` parameter, which is a user specified input needed to schedule any Playbook. If you are scheduling a Playbook with **Failure Policy** set to **Complete Roll Back**, you must double the value of the `mop_timeout` parameter as it can possibly take as much time to roll back the Playbook as it takes to run it until the last step. For example, if Playbook timeout is typically set to 1 hour, set it to 2 hours instead when enabling complete rollback on failure policy. Without sufficient `mop_timeout`, the Playbook can end up in a bad state if the timeout gets triggered while roll back is in progress.

View or Abort Playbook Jobs

There are two ways to view Playbook jobs:

1. The Change Automation **Dashboard** window's **Jobs** panel, which shows general information about the Playbook jobs that have been run most recently, including whether these jobs succeeded or failed.
2. The Change Automation **Job History** window lists all Playbook jobs, with much more detail.

Both methods let you click on any individual job in the list to see that job's detailed execution progress panel, which displays the name of the Playbook, its plays, the devices it ran on, the parameters used, and all event, syslog, console and other messages. These details are useful when diagnosing failures.

The **Job History** window also allows you to abort *running* jobs.

Step 1 From the main menu, select **Change Automation > Dashboard**. The **Jobs** panel at the upper right displays summary information for jobs that are running or have been recently run.

Jobs 		
Job	Status	Time Stamp
router_check_accessibility	ABORTED	2019-Apr-09, 21:56:36 (GMT -07:00)
router_check_accessibility	SUCCEEDED	2019-Apr-09, 21:45:36 (GMT -07:00)
router_op_backup_restore_config	FAILED	2019-Apr-09, 21:10:31 (GMT -07:00)
router_config_bgp_vrf	FAILED	2019-Mar-14, 05:06:29 (GMT -07:00)

[→ View All Jobs](#)

Step 2 To view information about a specific Playbook job in the **Jobs** panel, click the blue job title link in the **Job** column. The job's execution progress panel displays.

Step 3 To view information about all jobs:

- Click the **View All Jobs** link at the bottom of the **Jobs** panel.
- From the main menu, choose **Change Automation > Job History**

The **Job History** window opens with a table of detailed job information. The table data is sorted by the **Last Update Time**, with running or most recently executed jobs at the top. You can apply quick or advanced filters to the **Playbook Title** and **Devices** columns as you would with columns in other table windows (see [Set, Sort and Filter Table Data](#), on page 6).

The screenshot shows the 'Job History' window with the following details:

- Job Sets:** Sort by Last Update (descending). Selected job set: SID-TGSIL3VTP-6T211679.
- Filters:** Status: Success (1). Job Set Tags: sjc, upgrade, router (+4). PlayBook Title: Router_config_bgp_rd (1).
- Table:** All Jobs in the Set (11). Selected 0 / Total 11.

Status	Device	Start Time	End Time	Execution ID
Success	SJC-Router-NW440	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621734-7d17bdef-44...
Success	SJC-Router-NW444	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-21...
Success	SJC-Router-NW395	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-22...
Success	SJC-Router-NW399	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-49...
Success	SFO-Router-NW440	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-52...
Success	SFO-Router-NW444	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-56...
Success	SFO-Router-NW395	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-51...
Success	SFO-Router-NW399	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-45...
Success	SFO-Router-NW440	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-14...
Success	PHX-Router-NW779	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-25...
Success	PHX-Router-NW787	21-SEP-2019 6:00:00 am PST	21-SEP-2019 8:30:00 am...	4462123621790-7d17bdef-51...

Step 4 To view information about a specific Playbook job in the **Job History** window, click the relevant job ID checkbox on the left. In the **Execution ID** column. The job's status and execution details are displayed on the right side.

Step 5 With the **Job History** window displayed, you can abort running, paused or scheduled jobs, as follows:

- To abort a specific job, click the check box next to it and then click **Abort Selected**.
- To abort all jobs immediately, click **Abort All**.

When prompted, click **Confirm**. Jobs that are currently paused or scheduled will abort once the current task has run to completion.

About Customizing Playbooks

Users can download and customize Cisco-supplied Playbooks, or create their own based on Cisco models or from scratch.

Creating and modifying Playbooks are engineering tasks that take place outside of the user interface for Cisco Crosswork Change Automation and Health Insights. As such, they are outside the scope of this User Guide.

Cisco supplies developer-level documentation for Cisco-supplied Playbooks, Cisco verbs used in these Playbooks, and tutorials on how to create custom plays and Playbooks. For help, see the:

- "[Playbooks](#)" and "[Verbs](#)" references in the [Change Automation Developer Guide on Cisco Devnet](#)
- "[Custom Playbooks](#)" tutorial in the [Change Automation Developer Guide on Cisco Devnet](#)

Playbook Components and Files

Change Automation Playbooks contain a variety of components, referred to using specialized names. The components are implemented in the Playbook as files. Some of these components' names are borrowed from the Ansible specification, but all have their own definitions, and not all of the corresponding files can be customized by users. Some components are Cisco-proprietary intellectual property; while you can use them in custom Plays and Playbooks, you cannot customize them directly. The following table explains the function of each of these components, explains how they are implemented, and shows which of them you can customize.

Table 2: Playbook Components and Files

Component	Description	File/Format	Customizable?
Play	A play is a single task to be executed. A task is a list of actions to be performed in service of that play. A play is typically a script that uses one or more verbs.	YAML/YML in the Playbook file	Yes
Playbook	A Playbook is an aggregation of one or more plays, and is structured by the plays it contains. There can be many plays inside a Playbook. The function of a Playbook is to map a set of actions onto the features of a particular host. For example: A query and configuration change script with abstract variables that can be mapped to a particular instance of a device. For more details, see the "Playbooks" and "Verbs" references in the Change Automation Developer Guide on Cisco Devnet .	YAML/YML file	Yes
Verb	A verb is a Cisco-supplied module, and functions as a granular unit of activity. These are Cisco intellectual property, supplied as object code, used under license and not modifiable by users. For more on Cisco verbs and how to use them, see the "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet .	Binary executable file	No
Params	Params are simply variables, used in Playbooks just as variables are used in any programming language. A Params file in a Playbook is an optional file that collects all the user-defined input variables in one place. It is optional because all these variables are also in the plays.	JSON file	Yes

Component	Description	File/Format	Customizable?
Specs	Short for "specifications", specs are Cisco verb-specific object files, written in JSON schema format. They define all the Playbook input parameters and their constraints.	JSON Schema file	Yes
Tags	Tags are predefined phases of execution for plays within a Playbook, and define the order of execution of all plays: <ul style="list-style-type: none"> • Continuous • Pre-Maintenance • Maintenance • Post-Maintenance Any play tagged as Continuous or Pre-Maintenance runs in parallel with other plays with the same tags. All plays tagged as Maintenance or Post-Maintenance run serially. These tags are Cisco intellectual property, used under license and not modifiable by users.	Binary Executable files	No, but you select from the predefined tag set.
Role	A role is a built-in wrapper for Cisco's verbs. These files are Cisco intellectual property, used under license and not modifiable by users.	YAML/YML file	No

Export Playbooks

You can export any Playbook as a gzipped tar archive. This includes any Cisco-supplied Playbook, as well as custom Playbooks that you or another party have authored and have imported into Cisco Crosswork Change Automation and Health Insights.

The exported archive will contain only the user-customizable files listed in [Playbook Components and Files, on page 36](#). Once you extract them from the archive, you can identify the Playbook components by their file names and filename extensions. The filename will include the Playbook's unique ID (for example: `router_config_bgp_rd.yaml` for the Playbook YAML code). If files share the same filename extension, the filename will also include an indicator of the type of Playbook component it is (for example: `router_config_bgp_rd_specs.json` and `router_config_bgp_rd_params.json` for the Specs and Params files, respectively). For details on each Cisco-supplied Playbook and its components, see the "Playbooks" and "Verbs" references in the [Change Automation Developer Guide on Cisco Devnet](#).

You can edit the exported files as needed, following the guidelines in the "Custom Playbooks" tutorial in the [Change Automation Developer Guide on Cisco DevNet](#). You can then import them as explained in [Import Playbooks, on page 38](#).

You cannot re-import an exported Cisco-supplied Playbook with the same name as the original.

Your user ID must have Change Automation read permission to export Playbooks.

-
- Step 1** From the main menu, choose **Change Automation > Playbook List**.
- Step 2** (Optional) In the **Playbook List** window, filter the table as needed (see).
- Step 3** Check the check boxes for the Playbooks you want to export. Check the check box at the top of the column to select all of the Playbooks for export.
- Step 4** Click . Your browser will prompt you to select a path and the file name to use when saving the gzipped tar archive. Follow the prompts to save the file.
-

Import Playbooks

You can import any custom Playbook, provided it meets the following requirements:

- The Playbook files must be packaged as a gzipped tar archive.
- The archive must contain a Playbook YAML file and a Specs JSON file, at minimum.
- The archive file must have a unique name.

Cisco recommends that your imported archive also contain:

- An ASCII TXT file documenting the Playbook, its plays, and their input parameters.
- A Params JSON file.

The individual files included in the archive must meet the additional validation requirements described in the ["Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet](#).

Note that you cannot overwrite a Cisco-provided Playbook. You *can* overwrite a custom Playbook. The system will warn you when you are about to overwrite a custom Playbook, but will not prevent you from doing so. Take precautions to ensure that you do not overwrite your custom Playbooks accidentally.

Your user ID must have Change Automation write permissions to import Playbooks.

- Step 1** From the main menu, choose **Change Automation > Playbook List**.
- Step 2** Click . Your browser will prompt you to browse to and select the gzipped archive file containing the Playbooks you want to import.
- Make sure there is no existing Playbook with the same name as the Playbook you intent to import, unless it is your intent to overwrite the existing Playbook.
- Step 3** Follow the prompts to import the archive file.
-

Delete Custom Playbooks

You can delete user-defined Playbooks only. You cannot delete a Cisco-supplied Playbook.

Your user ID must have Change Automation delete permission to delete Playbooks.

-
- Step 1** From the main menu, choose **Change Automation > Playbooks List**.
- Step 2** In the **Playbooks List** window, select the custom Playbook that you want to delete
- Step 3** Click **Delete**.
- Step 4** Click **Delete** again to confirm.
-

Troubleshoot Change Automation

The following table describes issues you may encounter when using the Change Automation application, and their solutions or workarounds.

Table 3: Change Automation Troubleshooting

Issue	Solution
Playbook run fails with messages indicating that Cisco Network Services Orchestrator (Cisco NSO) and the target device are out of sync or otherwise out of communication. Message text will vary, but may include "device out of sync", "NC client timeout", and other text indicating that there are connectivity or sync issues between Cisco NSO and the device.	Run the Playbook again. Under normal circumstances, doing so will initiate a sync operation between the device and NSO. Alternatively, you can also perform a sync-from or sync-to operation in NSO.
"Failed to end NSO transaction, 500:fatal:YClientError: Failed to send RPC:" error is displayed while running the playbook.	Include the below settings in the Cisco NSO configuration file (ncs.conf): <pre><ssh> <client-alive-interval>infinity</client-alive-interval> <client-alive-count-max>5</client-alive-count-max> </ssh></pre>
Playbook aborted due to failure in locking the device nodes.	In the Devices window, select the relevant devices and clear the lock by moving the device to DOWN and then UP. Go to Admin > Crosswork Manager , and restart the robot-nca process. Once the protocols are reachable, you can schedule to run a new playbook.



CHAPTER 4

Monitor Network Health and KPIs

This section contains the following topics:

- [Health Insights Overview](#), on page 41
- [Health Insights Alert Dashboard](#), on page 42
- [Create a New KPI Profile](#), on page 44
- [Enable KPI Profile on Devices](#), on page 47
- [View Alerts for Network Devices](#), on page 50
- [Manage KPI Profiles](#), on page 52
- [Manage KPIs](#), on page 53
- [Create a New KPI](#), on page 54
- [Link KPIs to Playbooks](#), on page 55
- [Verify the Deployment Status of Enabled KPIs](#), on page 57
- [Disable KPI Profile on Devices or Device Groups](#), on page 57
- [List of Health Insights KPIs](#), on page 58
- [Troubleshoot Health Insights](#), on page 63

Health Insights Overview

Health Insights is a network health application that performs real-time key performance indicator (KPI) monitoring, alerting, and troubleshooting. The Health Insights application enables programmable monitoring and analytics. With Health Insights, network operators can create a platform to dynamically address changes to the network infrastructure. Health Insights builds dynamic detection and analytics modules that allow operators to monitor and alert network events with user-defined logic. Health Insights uses the Device Management component to bring devices on board. For more information, see [Device Management Overview](#).

Health Insights provides prebuilt KPIs that are based on model-driven and SNMP-based telemetry. The Health Insights Recommendation Engine uses data mining to analyze your network and then recommends which telemetry paths you should enable and monitor.



Note For the recommendation engine to work in Health Insights, the reachability should be established between Cisco Crosswork Change Automation and Health Insights and the device. When a device is onboarded, Cisco Crosswork Change Automation and Health Insights installs an explicit static route pointing to the data network gateway on the device subnet. You need to ensure that direct connectivity is established between Cisco Crosswork Change Automation and Health Insights and the device.

The following high-level example shows how Health Insights interacts with the other Cisco Crosswork Network Automation components:

1. Health Insights detects an anomaly: The optical bit error rate that you are monitoring on each of the links in your network suddenly increases.
 2. Change Automation Playbooks automate remediation: Switch to the backup link immediately. Restore service. Open an RMA ticket (manually initiated by the user). Alert the network engineer.
- Any network remediation can be orchestrated via Change Automation Playbooks, which closes the loop on problem detection and resolution.

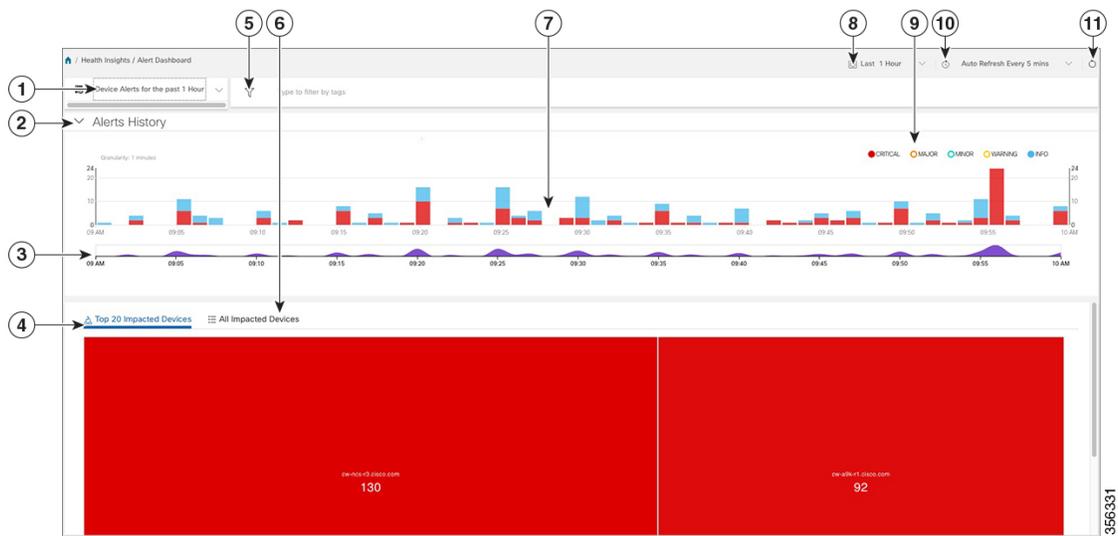
Health Insights Alert Dashboard

The Health Insights alert dashboard provides device health summary information that is based on real-time network state events. The dashboard displays a network view of KPI sensors that are paired to specific device groups. Health Insights raises customizable events and alerts that are based on user-defined logic.



Note Alert dashboard displays individual KPI alerts, even though the mechanism of enabling KPI on a device is done through a KPI profile.

To display the Health Insights dashboard, choose **Health Insights > Alert Dashboard** from the main menu.



Item	Description
1	Device/KPI Alert Selector: Click here to toggle between device alert and KPI alert information.
2	Alerts History: This dashlet shows the total number of device alerts or KPI alerts that have been raised during the chosen time period, with detailed time lines showing both individual sets of alerts and the overall alert trend.

Item	Description
3	<p>Alerts Trend Line: This line shows the overall trend in alerts for the chosen time period. You can use the Alerts Trend Line to select and zoom in on a specific time period within the Alerts History Line, as follows:</p> <ol style="list-style-type: none"> 1. Click the time-period starting point in the Alerts Trend Line and hold down the mouse. 2. Drag the cursor to the endpoint and then release the mouse. <p>The time range you selected is indicated by light gray shading on the Alerts Trend Line, with + and - zoom icons shown above the Alerts History Line. Click the + icon to zoom in on the time range you selected. Click the - to zoom out. To restore the full view of the Alerts History Line, click on any point outside of the light gray shading on the Alerts Trend Line.</p>
4	<p>Top 20 Impacted Devices/ Top 20 Impacted KPIs: When selected, this dashlet displays a map of tiles, each tile representing one of the 20 devices or KPIs with the most alerts during the selected time period. The amount of space that each tile occupies in the map corresponds to the number of alerts raised: the more alerts, the bigger the tile. To view more detailed information for a particular device or KPI, click the device or KPI name link in the center of the tile.</p>
5	<p>Filter By Tags: This field lets you filter the alert dashboard information by associated tag names. To select a tag, do one of the following:</p> <ul style="list-style-type: none"> • If you know the tag that you want to use, enter it in the Type to filter by Tags field and then check its check box. Repeat this step to select more tags. • If you want to select a tag from the tags that are currently available: <ol style="list-style-type: none"> 1. In the Type to filter by Tags field, type any character to open the results list. 2. Click the View All Tags link at the bottom of the list. 3. Check the check box for each tag you want to use and then click Apply Filters. 4. Delete the character that you typed in Step 1 to clear the results list. <p>Tag filters you create are not saved. If you open another window and then return to the alert dashboard, you will need to re-create tag filters.</p>

Item	Description
6	<p>All Impacted Devices/All Impacted KPIs: When selected, this dashlet provides a complete list of all devices or KPIs affected by alerts. The information for each affected device or KPI includes:</p> <ul style="list-style-type: none"> • Device Name or KPI Name • Device or KPI Type • IP address: The IP address of the impacted device. This column is only displayed for devices. • Alert count: The total number of alerts for that device or KPI during the selected period. • Impact score—This value is determined using the following formula: (4 x number of critical alerts) + (3 x number of major alerts) + (2 x number of minor alerts) + number of warning alerts. When monitoring the health of your network, focus on devices or KPIs with a higher impact score. • Severity distribution—Provides a visual breakdown of the severity that is associated with a device or KPI's alerts. To view a tooltip that indicates the number of raised alarms (by severity and in total), place your cursor over the appropriate bar segment.
7	<p>Alerts History: The Alerts History line shows alerts as discrete bar indicators whose height represents the total number of alerts gathered at each point in time. To see the total for each type of alert, hover your mouse cursor over the bar indicator. You can also use the Alerts Trend line to zoom in on particular portions of the alert history.</p>
8	<p>Time Period: Specifies the time period for which the dashboard provides alert information: The past one hour, past day, past week, and so on. Please note that the dashboard provides alert information only, not telemetry information.</p>
9	<p>Severity Legend: Maps the bar indicator colors that are used in the Alert History dashlet to the corresponding alert severity. To display or hide the alerts for a particular severity, click the circle representing that severity. A filled circle indicates that alerts of that severity have been raised and are being displayed. An empty circle indicates that alerts of that severity are either not being displayed or have not been raised during the displayed time period.</p>
10	<p>Auto Refresh: Specifies how often the dashboard is automatically refreshed.</p>
11	<p>Refresh Icon: Refreshes the dashboard.</p>



Note Composite Alerting is not displayed in the Alert dashboard.

Create a New KPI Profile

A KPI Profile is a collection of KPIs and their corresponding parameters such as alert frequency, alert type, cadence, and more. You can group relevant KPIs into a KPI Profile, give it meaningful name based on the purpose (for example, environmental or health check), and configure parameters that are relevant to monitoring

a specific type of devices (for example, edge routers). Once the KPI profiles are created and validated by the system, they are ready to be used. You can select the device(s) in Health Insights, select appropriate KPI Profiles and enable them. This action enables all the KPIs in the selected KPI Profile. Similarly, you can select the device(s) and choose to disable the KPI Profiles. This removes all KPIs enabled as part of the selected KPI profile(s).

You can create a KPI Profile and enable it on the desired devices. The workflow is as follows:

1. Supply basic information, such as the Profile name and a description.
2. Add KPI(s) and save the profile.
3. Edit KPI parameters and create alert groups.
4. Enable the KPI Profile on the devices.

The following steps explain how to perform all of these tasks.

-
- Step 1** From the main menu, choose **Health Insights > Manage KPI Profiles**. The **Manage KPI Profiles** window opens.
- Step 2** Click the . The **Create New Profile** window opens.
- Step 3** In the text fields provided, enter a unique **Profile Name**, a short **Description**. The **Profile Name** can contain a maximum of 32 alphanumeric characters, plus underscores ("_"). No other special characters are allowed.
- Step 4** Add KPI to the profile, using the following filter options:
- a) **All KPIs**: By default, this option is selected and the list of all KPIs are displayed in the list. You can select the required KPI by checking the relevant checkbox.
 - b) **Recommended KPIs**: You may also select KPIs based on the KPI recommendation for a specific device. Click **Recommended KPIs** and the device list is displayed. You may filter the device list by entering relevant values in the Name and State fields, or filter by tags. using tags. Select a device from the list and the recommended KPI list is displayed on the right side. Select the required KPI by checking the relevant checkbox.
- Note** Selecting KPIs from the recommended KPI list of a selected device does not automatically enable the KPI Profile in the selected device. The KPI Profile can be enabled after it is created. For more information, see [Enable KPI Profile on Devices, on page 47](#)
- Step 5** Click **Save** save the new KPI Profile and display the **Manage KPI Profiles** window.
- Step 6** In the **KPI Profiles** area on the left side, choose the KPI Profile that you created, and the individual KPI details are displayed on the right side.
- Step 7** You can leave the KPI parameters at the default or choose a different value. To edit the KPI parameters, click **Edit Details**, and the **KPI Details** window is displayed. Edit the parameter values as appropriate for the purpose of your KPI. The common parameters are:
- **Alert**: This is an on/off toggle switch for alerting. Based on the **Alert** parameter value, the corresponding alerting logic is deployed. Alerting can be enabled even after the KPI Profile has been applied to the devices.
- Note** Any KPI using the composite alerting logic need to have the alerting flag set to ON.
- **Cadence (sec)**: Set the frequency of sensor data. Set the frequency (in seconds) in which the KPI will gather sensor data from the devices on which the KPI Profile is enabled.
 - **Alerting Down Sample Rate**: Alert frequency rate. It determines how often KPI data will be evaluated for any alert conditions, and is relative to the Cadence. For example, if Cadence is 60 seconds and you want to do an alerting evaluation every 300 sec, then specify Alerting Down Sample Rate as "5".

Note Setting the alert flag as ON for an enabled KPI profile is not displayed on the corresponding Health Insights job details page as the update operation is an internal system transaction. If the job completes successfully, the alert triggered can be viewed on the alert dashboard.

Step 8 You can also edit the alert logic parameters of the selected KPI. To learn more about a parameter, hover your mouse cursor over the  shown next to the parameter name.

Note When different thresholds are desired for different types of devices in the network, it is advisable to create multiple profiles and split the KPIs across them to meet the needs of different device types.

Step 9 When you are finished making changes, click **Save** to save the new KPI Profile. Health Insights validates your input parameters and displays the **Manage KPI Profiles** window.

Note You can create up to 50 KPI profiles, and an individual KPI Profile can consist up to 50 KPIs. KPI profile creation can fail if the total number is exceeded, or if Health Insights could not create the required tags in Inventory manager. This status is reflected in the profile state. Once profile is ready, it can be applied on devices.

With the **Manage KPI Profiles** window displayed, you can enable the new KPI Profiles on one or more devices immediately, following the steps given in [Enable KPI Profile on Devices, on page 47](#).

See [Disable KPI Profile on Devices or Device Groups, on page 57](#) for instructions to disable KPI Profiles.

Step 10 (Optional) You can also create alert groups for a KPI Profile. Alert groups use boolean logic (cascaded OR and AND) to combine alert outputs from primary KPIs in your KPI profile and create a composite logic query. To create an alert group, click + **Alert Group**. The **Create Alert Group** window is displayed.

Note Configuring an alert provider enables composite alert forwarding. For information on adding alert providers, see [Add an Alert Provider, on page 184](#)

Step 11 Provide a relevant entry in the **Name** field. **Summary** and **Details** are optional fields.

Step 12 The **Alert Group Conditions** area on the right side lets you select a logic gate (AND/OR) and add a KPI on which the logic is applied. Your alert group can be based on the alert criteria of a single KPI, or it can be a combination of multiple KPI outputs. Click the desired logic (**AND** gate is selected by default), and click the + **ADD** dropdown list to add an **Item** or a **Group**.

Item allows you to add individual KPI items and set the corresponding alert level, and **Group** allows you to add a nested alert group.

Step 13 Choose the desired KPI from the **Select KPI** dropdown, and select the desired level(s) for which the alerts need to be set for the chosen KPI. The alert levels are CRITICAL, MAJOR, MINOR, WARNING and INFO. Based on the logic gate and alert criteria you select, the output of the KPIs are evaluated and the alert is generated.

The screenshot shows the 'Create Alert Group' window. On the left, there's a 'KPI List' with expandable items: CPU utilization, Interface bandwidth monitor, and Memory utilization. The main area is 'Alert Group Conditions', which contains a logic tree. The root is an OR gate with two children: 'Memory utilization' and 'Interface bandwidth monitor'. This OR gate's output is connected to an AND gate, which also has 'CPU utilization' as a child. The alert levels are set to MAJOR, MINOR, and CRITICAL. At the bottom, there are 'Cancel' and 'Save' buttons.

In the example shown above, the alert is set based on the output of two logic gates. The first logic gate is the output of an **OR** operation between the **Memory Utilization** and **Interface Bandwidth monitor** KPIs. If the set alert levels are met for either of the KPIs, the output of the first logic gate is set as true. This output is considered as the input for the second logic gate, which is an **AND** operation with the **CPU Utilization** KPI. If the alert levels of both the KPIs are met, the output of the second logic gate is set as true.

Step 14 Click **Save** to save the new alert group and display the **Manage KPI Profiles** window. Click **Edit Details** or  to edit or delete an existing alert group respectively.

Enable KPI Profile on Devices

With Health Insights, you can enable and monitor the KPI Profiles in which you are interested. Instead of sifting through all the data that a given device can supply, you choose to monitor only the information relevant to the role the device plays in your network. Your equipment and management infrastructure operates as efficiently as possible, without requiring the collection and storage of data that is unrelated to device roles. This operational efficiency reduces the amount of time required to set up specific monitoring, leading to faster problem identification and resolution.

Note that some KPIs trigger alerts based on deviation from an established level of performance. For these types of KPIs, it is necessary to allow the system some annealing time in order to establish normal performance levels.



Important

You can only enable KPI Profiles with MDT-based KPIs on a device that has been mapped to a Cisco Network Services Orchestrator (Cisco NSO) provider. See the following topics for more information:

- [Add Providers Through the UI](#)
- [Import Providers](#)
- [Sample Configuration for Devices in Cisco NSO](#)
- [Prerequisites for Onboarding Devices, on page 91](#)

To enable KPI Profile on devices:

Step 1 From the main menu, choose **Health Insights > Enable-Disable KPI Profiles**. The **Enable-Disable KPI Profiles** window is displayed.

Step 2 Select the devices for which you want to enable KPI Profiles. You can click the **Devices** or **Device Tags** buttons above the table on the left to toggle between selecting the devices by name or by tagged device group membership. Depending on your selection, the device list or the device tag list is displayed on the left.

If you choose to select by **Devices**:

- Click in the table on the right. Type a **Name** or **Device Type** in the filter fields. As you type, the table displays only the devices whose name or type match the text you typed.
- Click the check box next to the device(s) you want. You can select multiple devices at the same time.

If you choose to select by **Device Tags**:

- Type a tag name in the **Name** field to find a Device Group in the table. As you type, the table displays only the tag names that match the text you typed.
- Click the check box next to the group you want. The names of all the devices in that group appear in the devices table on the right.

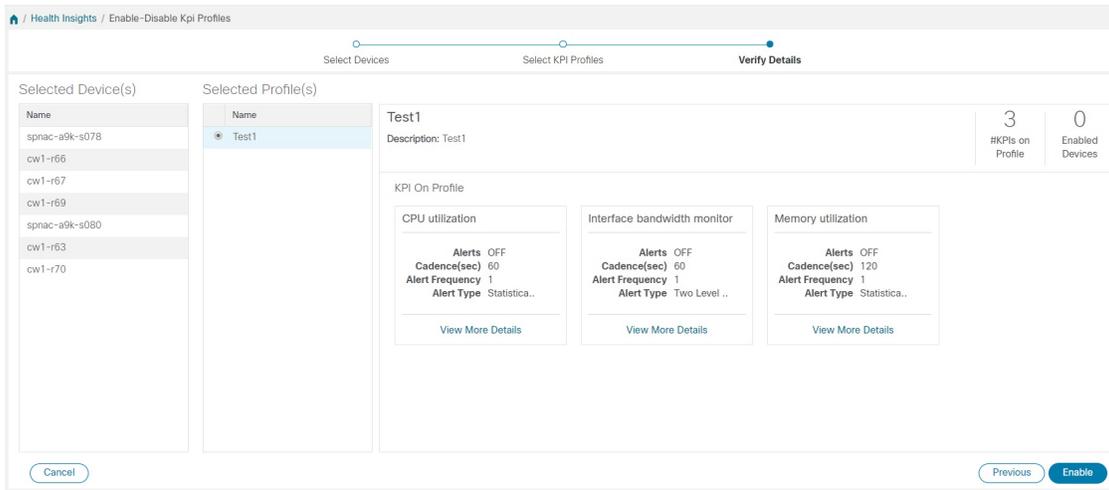
The screenshot shows the 'Enable-Disable KPI Profiles' interface. At the top, there are radio buttons for 'Devices' (selected) and 'Device Tags'. Below this is a search bar and a table of devices. The table has columns: Reachability, Name, Device Type, Operational State, and Enabled Profiles. The 'Enabled Profiles' column is currently empty. Several rows are highlighted in blue, indicating they are selected. The 'Enable KPI Profiles' button is visible at the top right of the table area.

Reachability	Name	Device Type	Operational State	Enabled Profiles
<input type="checkbox"/>	spnac-a9k-s077	ROUTER	+	
<input checked="" type="checkbox"/>	spnac-a9k-s078	ROUTER	+	
<input checked="" type="checkbox"/>	cw1-r66	ROUTER	+	
<input checked="" type="checkbox"/>	cw1-r67	ROUTER	+	
<input checked="" type="checkbox"/>	cw1-r69	ROUTER	+	
<input checked="" type="checkbox"/>	spnac-a9k-s080	ROUTER	+	
<input checked="" type="checkbox"/>	cw1-r63	ROUTER	+	
<input checked="" type="checkbox"/>	cw1-r70	ROUTER	+	
<input type="checkbox"/>	spnac-a9k-s079	ROUTER	+	
<input type="checkbox"/>	cw1-r61	ROUTER	+	
<input type="checkbox"/>	spnac-a9k-s074	ROUTER	+	
<input type="checkbox"/>	spnac-a9k-s075	ROUTER	+	

Step 3 Click **Enable KPI Profiles** to continue. Health Insights detects the selected devices, their types and models, and retrieves and analyzes their running configurations. The **KPI Profiles** window presents the KPI Profiles available for your selected devices.

Step 4 Choose the KPI Profiles you want to enable by clicking the check box next to the KPI Profile name. :

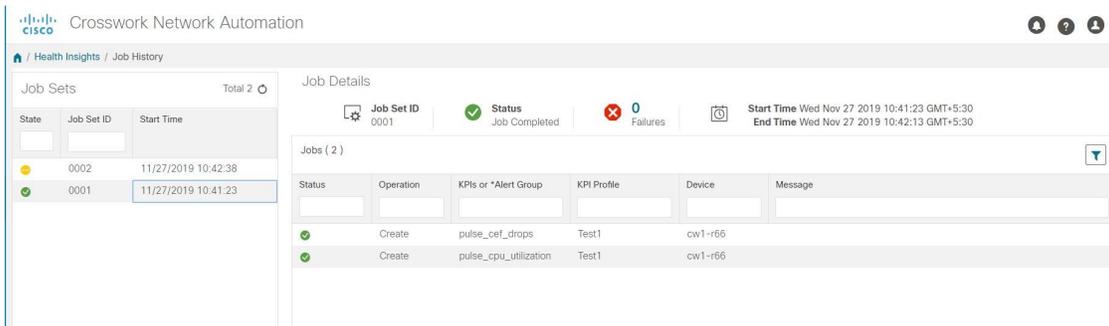
Step 5 When you are finished, click **Next**. The **Verify Details** window appears, listing all the KPI Profiles you have chosen to be enabled on the selected devices, as shown in the following figure.



Step 6 (Optional) To get information about the KPIs included in the KPI Profile. Click the KPI Profile in the **Selected Profile(s)** table, and the content of the selected KPI Profile is displayed on the right side. Click **View More Details** to view the parameters of a specific KPI. A popup window provides the details of the KPI. Click the **X** to close the popup window.

Step 7 To enable the selected KPI Profiles on the selected devices, click **Enable**. Health Insights schedules the KPI Profile(s) as a series of job sets.

Step 8 From the main menu, choose **Health Insights > Job History** to watch the progress of each job set, as shown below. You should see job sets completing with a status of "Success". If job sets complete with a "Partial" or "Failed" status, be sure to read the job completion messages, and check that the selected devices are still reachable.



When the job sets complete successfully, the KPIs are now associated to the devices and the platform begins the process of enabling the relevant collection procedures for those network elements. In making these changes, you are automating the configuration of both the platform and the devices themselves to collect only the information required.

Step 9 From the main menu, choose **Health Insights > Alert Dashboard**. The dashboard shows the alert status for the devices on which you have enabled KPI monitoring.



Note

- SNMP/MDT jobs may take more time than expected to reach the completed state when there is an increase in the number of devices, interfaces and KPIs.
- Enabling KPI profile per device takes around 3 to 5 seconds. If the device is not reachable, it will keep trying until it is timed out. This may result in the job taking more time to reach the completed state.

View Alerts for Network Devices

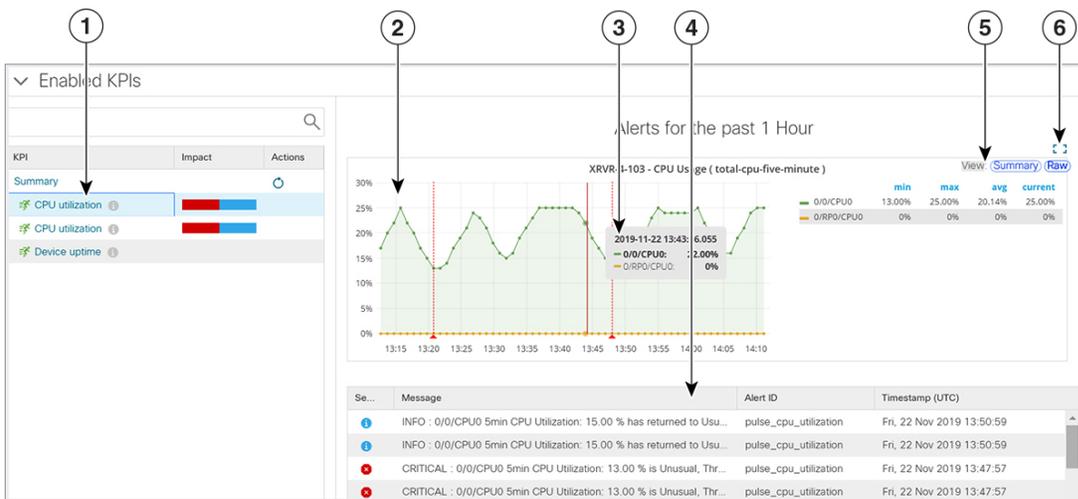
After enabling KPIs on a device, you can view alerts for that device and get data for each performance indicator being monitored.



Note The KPIs shown in the following steps are examples. There are many more KPIs available in Health Insights. For the complete list, see [List of Health Insights KPIs, on page 58](#).

- Step 1** From the main menu, choose **Health Insights > Alert Dashboard**. The Health Insights dashboard opens.
- Step 2** Make sure that the **Device Alerts** view is displayed (select the **Device Alerts** toggle, if needed). Then scroll down below the **Total Alerts** panel and click on the **All Impacted Devices** tab. The dashboard displays a list of devices with alerts.
- Step 3** Click on the **Device Name** for the device whose details you want to see. Health Insights displays the device's basic **Overview** information, **Total Alerts**, a **Topology** map, and the list of the device's currently **Enabled KPIs**.
The **Topology** map is a version of the map you see when you select **Network Visualization > View Topology**. For help using it, see [Network Visualization Overview, on page 65](#).
- Step 4** To see detailed KPI data, scroll down to the **Enabled KPIs** panel at the bottom of the window and click on one of the enabled KPIs in the list at left. A graphical representation of that KPIs data, along with a list of alert messages and other information, is displayed on the right.

In the example shown below, the **Interface rate counters** KPI was selected, so the accompanying information includes a list of the interfaces at the right of the graphic time-series data.



Item	Description
1	Click on the KPI name in the list to display its data on the right.

Item	Description
2	<p>Graphical time-series data for the selected KPI appears here. In the example shown, the KPI graphic shows real-time data that has been collected on the interfaces and the points at which the sensor detected an alert event.</p> <p>To have the graphic display data for a single interface instead of all interfaces, click on the interface name in the list at right.</p> <p>To zoom in on a period within the time series graph, click and drag within the graph.</p>
3	<p>Hover the mouse cursor over any data point in the KPI graphic to see additional popup information for that data point.</p> <p>A red line or tag represents a point at which the KPI was triggered. This can occur on any subscribed statistic the KPI is monitoring. Health Insights collects and identifies the time points and frequency, which help determine when these events become an operational concern.</p>
4	<p>Below the KPI timeline, the alerts panel shows each KPI alert that was generated on the device. It also shows which link or interface was affected and when the alert occurred. The blue color indicates that the alert has cleared and is informational only. Red signifies a critical alert.</p> <p>Search for alert messages in the list below by severity, any part of the message text, the alert ID, or by time and date.</p>
5	View additional information by clicking the Summary and Raw graph pages in the View widget.
6	<p>Click the empty square icon to use the whole page to display the Enabled KPIs panel only.</p> <p>If you choose to enlarge the Enabled KPIs panel, a blue < icon appears next to the list of KPIs. Click the icon to hide the list.</p> <p>Click the inverted versions of these icons to restore the KPI list and return the Enabled KPIs panel to its normal size.</p>

Telemetry Data Retention

Telemetry data is collected from devices and stored in the time-series database. This data is retained for one hour, and is used in the Health Insights Alert dashboard to identify alerts using a process known as stream based alerting. The resulting 'alerts', if any, are stored in the same time-series database. The alerts are retained for 30 days, and the messages showing the duration of alerts are displayed in the top right corner of the Device/KPI view in the Alert dashboard. For more information, see [View Alerts for Network Devices, on page 50](#). The alerts can also be queried using REST APIs.

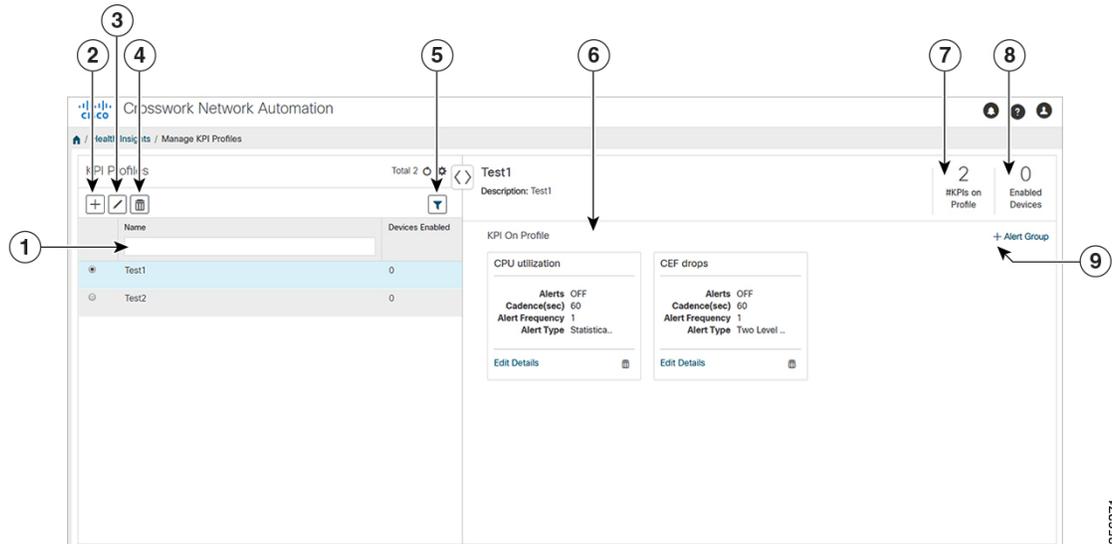


Note The telemetry data displayed in the Alerts dashboard is limited to last only for one hour.

Manage KPI Profiles

The Health Insights Manage KPI Profiles window allows you to create, edit, and delete KPI Profiles.

To display the Health Insights Manage KPI Profiles window, choose **Health Insights > Manage KPI Profiles** from the main menu.

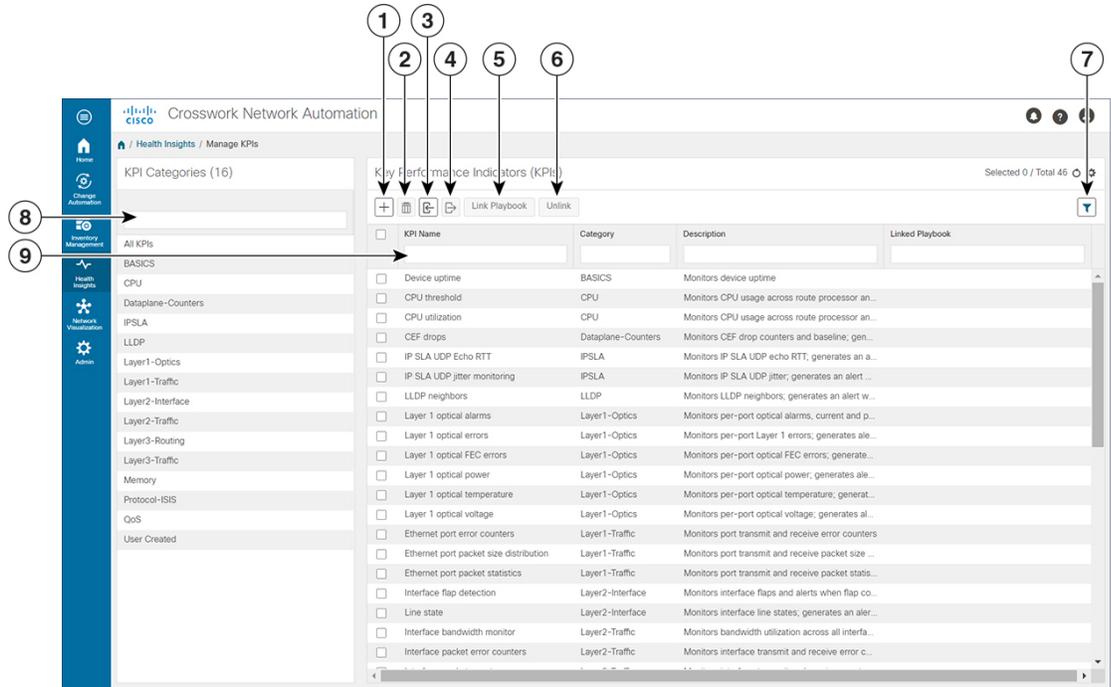


Item	Description
1	Filter KPI Profile: To find a KPI category, enter all or part of the KPI Profile name in this field, and the list is automatically filtered based on your input. Click to clear any filters you have set.
2	Create KPI Profile: Click to create a new, user-created KPI Profile. For help with this task, see Create a New KPI Profile, on page 44 .
3	Edit KPI Profile: Select a user-created KPI Profile in the list and then click to edit it. For help with this task, see Create a New KPI Profile, on page 44 .
4	Delete KPI Profile: Select a user-created KPI Profile in the list and then click to delete it. You cannot delete a KPI Profile that has been enabled on any device(s).
5	KPI On Profile: The KPI(s) added on the selected KPI Profile and the associated parameters are displayed here. You can edit the KPI parameters, or remove a KPI from the selected KPI Profile using the appropriate options here. For more information, see Create a New KPI Profile, on page 44 .
6	#KPIs on Profile: This is the number of KPIs added on the selected KPI Profile.
7	Enabled Devices: This is the number of devices on which the selected KPI Profile is enabled.
8	+Alert Group: Click this option to create Alert Group for the selected KPI Profile. For help with this task, see Create a New KPI Profile, on page 44

Manage KPIs

The Health Insights Manage KPIs window gives you complete access to Cisco-supplied and user-created KPIs. You can add, edit, delete, import, and export your KPIs. You can also link your KPIs to the Change Automation application's Playbooks, which enable scripted responses to KPI changes.

To display the Health Insights Manage KPIs window, choose **Health Insights > Manage KPIs** from the main menu.



Item	Description
1	Add KPIs: Click to add a new, user-created KPI. For help with this task, see Create a New KPI, on page 54 .
2	Delete KPIs: Select one or more existing user-created KPIs in the list and then click . You will be prompted to confirm that you want to delete the KPIs. Click Delete to confirm. Note that you can delete user-created KPIs only. You cannot delete Cisco-supplied KPIs.

Item	Description
3	<p>Import KPIs: Click  to import new user-written or Cisco-supplied KPIs.</p> <p>You will be prompted to browse to the gzipped tar archive containing the KPIs to be imported. When you have selected the archive, click OK to begin importing it. Once imported, the new KPIs will appear immediately in the list of KPIs, with each KPI name and category assigned based on the definition in the KPI itself.</p> <p>In order for Cisco Crosswork Change Automation and Health Insights to import them, KPI files must:</p> <ul style="list-style-type: none"> • Be packaged as a gzip tar archive. You can include more than one KPI in a single archive; each will be imported as a separate KPI. • Have unique names and descriptions. These must not match the name or description of any Cisco-supplied KPI. If the name or description of the KPI matches an existing user-created KPI, the import will overwrite the existing KPI. • Meet other minimum requirements for Health Insights KPIs, as explained in the Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet.
4	<p>Export KPIs: Select one or more existing KPIs in the list and then click  to export them. Health Insights will package the exported KPIs as a single TGZ archive with a unique name. Your browser will then prompt you to save the archive to a name and location in your local file system that you select.</p>
5	<p>Link Playbooks: Select a KPI and then click  to link it to a Playbook. That Playbook will execute whenever the KPI raises an alert thereafter. You can specify the values the Playbook will use when operators trigger it in response to the KPI alert. For help with this task, see Link KPIs to Playbooks, on page 55.</p>
6	<p>Unlink Playbooks: Select a KPI with a linked Playbook and then click  to unlink the Playbook. You will be prompted to confirm that you want to unlink the Playbook. Click Unlink to confirm.</p>
7	<p>Clear Filters: Click Clear All Filters to clear any filters you have set.</p>
8	<p>Filter KPI Categories: To find a KPI category, enter all or part of the KPI Category name in this field. Then click  to filter the list below.</p>
9	<p>Filter KPIs: To find a KPI, enter all or part of the KPI Name, Category, Description, or Linked Playbook in the fields provided. The list below is automatically filtered to match your typed entry.</p>

Create a New KPI

You can create a custom KPI and enable it on the desired devices. The workflow is as follows:

1. Supply basic information, such as the KPI name and a summary description.
2. Set the KPI cadence.

3. Select a YANG module and choose sensor paths
4. Select an alert template and set its parameters
5. Enable the KPI on the devices.

The following steps explain how to perform all of these tasks.

-
- Step 1** From the main menu, choose **Health Insights > Manage KPIs**. The **Manage KPIs** window opens.
- Step 2** Click the . The **Create KPI** window opens.
- Step 3** In the text fields provided, enter a unique **KPI Name**, a short **KPI Summary** description, and **KPI details**. The **KPI Group** is preset to `User Created`.
- Step 4** The **Cadence** field sets the number of times per minute the KPI will gather sensor data from the devices on which the KPI is enabled. Leave it at the default or use the numerical selector to choose a different value.
- Step 5** In the **Select YANG Paths** area, choose one module and one or more sensor leaf paths from which to stream data:
- a) Use **Filter Modules** to filter and choose the desired Cisco IOS XR YANG module.
 - b) Use **Filter Paths** to filter and choose the desired sensor path. When you choose a path, the leaf node gets resolved to the base encoding path. If the YANG module is hierarchical, the field names are concatenated down from the base path. Note that only one gather path is supported for user-created KPIs.
 - c) Click **Next** to display the **Select Alert Templates** window.
- Step 6** Choose the alert template you want to use with your new KPI: **No Alert**, **Standard Deviation**, **Two-Level Threshold** or **Rate Change**. Then click **Next** to display the **Alert Parameters** window appropriate for the type of alert template you chose.
- Step 7** Edit the alert template parameter values as appropriate for the template and the purpose of your KPI, as follows:
- Use the **Basic** and **Advanced Parameters** dropdowns to view and edit the parameter sets you need.
 - Change alert parameter numerical values using the selectors or by editing the field contents
 - Change alert parameters with discrete choices using parameter field dropdowns and select each choice as needed.
 - Learn more about an alert parameter: Hover your mouse cursor over the  shown next to the parameter name.
 - Click the **View Tick Script** link to view the tick script code you are generating with your changes. The tick script code updates as you make your edits. At any time, click the **Hide Tick Script** to close the tick script code window.
- Step 8** When you are finished making changes, click **Finish** to save the new KPI and display the **Manage KPIs** window.
-

Link KPIs to Playbooks

You can link any Health Insights KPI to one Change Automation Playbook of your choice. A user can run the linked Playbook whenever the linked KPI raises an alert in response to the event associated with the performance indicator the KPI is monitoring. The KPI alert can be raised in response to a threshold crossing, topology changes, flapping conditions, and other parameters. These parameters will vary, as appropriate, for each KPI.

You can specify the **Source** of the parameter values the linked Playbook will use when you run it. You can select these sources:

- **Playbook**: Use default values coded into the Playbook itself

- **KPI Alert:** Use values taken from the alert raised by the linked KPI.
- **Runtime Input:** Use values you enter only at the moment you run the Playbook.

The ability to set the source of these Playbook parameter values gives you flexibility in how you use the linked Playbook. For example: Link the KPI **Interface flap detection**, which detects interface flapping, to the Playbook **Interface state change**, which can be used to set the interface up or down. Depending on circumstances, you might want to set the Playbook parameters as follows:

- **Playbook:** You want to run the Playbook as it normally does, so you would set the **Source** as **Playbook** for the *provider*, *collection_type* and *mop_timeout* parameters. In the case of the *collection_type*, you can still choose between **telemetry** and **snmp**, depending on whether you want to use MDT or SNMP to gather device data.
- **KPI Alert:** You want the Playbook to run only on the host device and interface affected by the flapping, which are identified in the flap-detection Alert. So set the **Source** of the Playbook's *hosts* and *if_names* parameters to **KPI Alert**. You can then use the alert's data about the **Producer** device and the **interface_name** of the flapping interface on that device.
- **Runtime Input:** You want the freedom to decide at runtime whether to bring the flapping interface up or down. So set the **Source** of the Playbook parameter *admin_state* to **Runtime Input**. The Playbook will prompt you for an **up** or **down** choice when you initiate the run.

The following figure shows what this set of choices will look like:

Figure 5: Example: Specifying Parameter Value Sources for a Linked Playbook

Playbook Details (**Interface State change**)
Change line card interface(s) state to up/down

Hardware Platform: Software Platform: **IOS XR** Version:

Verify/Modify Parameters
Select a Source to determine the default input values.

Source	hosts
<input type="text" value="KPI Alert"/>	<input type="text" value="Producer"/>
<input type="text" value="Runtime Input"/>	admin_state
<input type="text" value="KPI Alert"/>	<input type="text" value="interface-name"/>
<input type="text" value="Playbook"/>	provider
<input type="text" value="Playbook"/>	collection_type
<input type="text" value="Playbook"/>	mop_timeout
	<input type="text" value="1h"/>

- Step 1** From the main menu, choose **Health Insights > Manage KPIs**. The **Manage KPIs** window opens, displaying lists of the KPI categories and the KPIs available in each category.
- Step 2** Select the KPI you want to link to a Playbook. You can use filters to find the KPI you want, as explained in [Manage KPIs, on page 53](#).

- Step 3** Click . The **Link KPI to Playbook** window opens.
- Step 4** The left side of the window lists the name of the selected KPI and the Playbooks appropriate for linking to it. Scroll through the list, or use the **Playbook Name** field and the to restrict the list to just the Playbooks you want.
- Step 5** When you have found the Playbook you want to link, click on its name. The right side of the window will then list the **Playbook Details** for the selected Playbook, including:
- The hardware and software platforms with which it is compatible.
 - The minimum software version requirement
 - The **Source** and default values that will be used when the Playbook runs. In many cases, you can select from a range of default values, or enter your own.
- Step 6** Verify or modify the **Source** and parameter values as needed.
- During the maintenance cycle, the Playbook will perform a variety of actions. To see a list of these actions, click the **View Maintenance** link. A popup **Maintenance** panel opens, listing them. Click  if you want to continue to refer to this action list while you adjust the Playbook runtime parameter sources and values. Click  at any time to close the **Maintenance** panel.
- Step 7** When you are finished making changes, click **Link to KPI**. Change Automation displays the **Manage KPIs** window again, this time with the linked Playbook shown next to name of the KPI in the **Key Performance Indicators (KPIs)** list.
- Step 8** To change the Playbook linked to a given KPI, repeat steps 3 through 7 for that KPI, this time choosing the Playbook you want. To unlink a Playbook entirely, select the KPI and click .
-

Verify the Deployment Status of Enabled KPIs

After you enable KPIs, you can verify their deployment status.

- Step 1** From the main menu, choose **Health Insights > Job History**. The **Job History** window lists the jobs that have been run most recently, indicating whether they succeeded or failed, when they ran, and on what devices.
- Step 2** Click the transaction ID in the job listing to view detailed KPI job information, including the device on which the KPI was enabled and the KPI ID.
-

Disable KPI Profile on Devices or Device Groups

You can use the **Enable-Disable KPI Profiles** window to disable all of the KPI Profiles running on device(s).

- Step 1** From the main menu, choose **Health Insights > Enable-Disable KPI Profiles**. The **Enable-Disable KPI Profiles** window opens.
- Step 2** To disable all KPI Profiles enabled on all the devices within a device group:

- a) Click the **Device Tags** button above the table on the left. The table displays the list of device tags.
- b) Click the checkbox next to the device tag(s) on which you want to disable KPI Profiles.

When you select a device tag, the **Devices** table on the right shows all the devices that are associated with that tag. All of the devices are preselected.

- c) Click **Disable KPI Profiles**. You will be prompted to confirm that you want to disable all the KPIs running on all the devices in the group. Click **Disable** to confirm.

Step 3 To disable KPIs enabled on one or more devices:

- a) Click the **Devices** button above the table on the left. The **Devices** table on the right shows all the devices, with the total number of KPIs enabled on each device.
- b) Click the checkbox next to the devices on which you want to disable KPIs.

If you select one device, you can disable all KPI Profiles for the device or just some of the KPI Profiles. If you select more than one device, you can only disable all KPIs for them.

- c) Click **Disable KPI Profiles**. You will be prompted to confirm that you want to disable the KPIs running on all the selected devices. If you selected only one device, click the checkboxes next to the KPI Profiles you want to disable on that device, or click the checkbox at the top of the column to disable all the KPI Profiles running on that device. Click **Disable** to confirm.

List of Health Insights KPIs

The table below lists the prebuilt Health Insights KPIs supplied with Cisco Crosswork Change Automation and Health Insights.

Alerting types in the table that you can select when you create a new KPI (see [Create a New KPI, on page 54](#)) are:

- **No Alert:** The KPI gathers, tracks and reports performance data without triggering alerts.
- **Standard Deviation:** The KPI detects spikes or drops in measured values and alerts when these values deviate some number of standard deviations away from their normal values.
- **Two-Level Threshold:** The KPI detects abnormal measured values using two custom thresholds and the ability to provide dampening intervals on the thresholds.
- **Rate Change:** The KPI detects abnormal rates of change in measured values to detect rising or falling values.

Additional alerting types that you can use when you export and use a prebuilt KPIs to create KPIs with custom parameters are:

- **Standard Deviation of Rate Change:** The KPI alerts on standard deviations of the rate of change.
- **Low Single Threshold:** The KPI alerts on a single threshold when the value falls below that threshold.
- **Direct Alarm Forwarding:** The KPI uses the alarm from the device directly, as a Health Insights KPI alert.
- **Major/Minor/Low/High Thresholds:** The KPI alerts on Major high, Minor high, Minor low, and Major low values.

- **Line State Changes:** The KPI alerts on shutdowns and flapping in line states.

For more on creating KPIs with custom parameters from exported KPIs, see the [Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet](#).

Table 4: Health Insights KPIs

Category	KPI Name	Description	Alerting	MDT or SNMP
Dataplane-Counters	CEF drops	Monitors CEF drop counters and baseline. Generates an alert for an unusual number of drops.	Rate Change	MDT
CPU	CPU threshold	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization exceeds the configured threshold	Two-Level Threshold	MDT
CPU	CPU utilization	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization is unusual.	Standard Deviation	MDT
Basics	Device uptime	Monitors device uptime.	Low Single Threshold	MDT
Layer 1-Traffic	Ethernet port error counters	Monitors port transmit and receive error counters.	Rate Change	MDT
Layer 1-Traffic	Ethernet port packet size distribution	Monitors port transmit and receive packet size distributions.	No Alert	MDT
Layer 1-Traffic	Ethernet port packet statistics	Monitors port transmit and receive packet statistics.	Standard Deviation of Rate Change	MDT
Layer 2-Traffic	Interface bandwidth monitor	Monitors bandwidth utilization across all interfaces on a router. Generates an alert when bandwidth exceeds the configured threshold.	Two-Level Threshold	MDT
Layer 3-Traffic	Interface counters by protocol	Monitors interface statistics (such as incoming and outgoing packets or byte counters) organized by protocol.	Standard Deviation	MDT
Layer2-Interface	Interface flap detection	Monitors interface flaps and alerts when flap count reaches set threshold.	Two-Level Threshold	MDT
Layer 2-Traffic	Interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	No Alert	MDT
Layer 2-Traffic	Interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	Rate Change	MDT

Category	KPI Name	Description	Alerting	MDT or SNMP
QOS	Interface QoS (egress)	Monitors interface QoS on the egress direction for queue statistics, queue depth, and so on.	No Alert	MDT
QOS	Interface QoS (ingress)	Monitors interface QoS on the ingress direction for queue statistics, queue depth, and so on.	No Alert	MDT
Layer 2-Traffic	Interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation	MDT
IPSLA	IP SLA UDP echo RTT	Monitors IP SLA UDP echo RTT. Generates an alert when unusual RTT values occur.	Standard Deviation	MDT
IPSLA	IP SLA UDP jitter monitoring	Monitors IP SLA UDP jitter. Generates an alert when an abnormal UDP jitter occurs.	Standard Deviation	MDT
Layer 3-Routing	IPv6 RIB BGP route count	Monitors IPv6 RIB for route count and memory used by BGP. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIB IS-IS route count	Monitors RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	IPv6 RIB IS-IS route count	Monitors IPv6 RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	IPv6 RIB OSPF route count	Monitors IPv6 RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Protocol-ISIS	ISIS neighbor summary	Monitors ISIS neighbor summaries for changes in neighbor status. Generates an alert when an anomaly is detected (such as neighbors down or flapping).	Standard Deviation	MDT
Layer 1-Optics	Layer 1 optical alarms	Monitors per-port optical alarms (current and past).	Direct Alarm Forwarding	MDT

Category	KPI Name	Description	Alerting	MDT or SNMP
Layer 1-Optics	Layer 1 optical errors	Monitors per-port Layer 1 errors. Generates an alert when error rates exceed the configured threshold.	Rate Change	MDT
Layer 1-Optics	Layer 1 optical FEC errors	Monitors per-port optical FEC errors. Generates an alert when FEC errors exceed the configured threshold.	Rate Change	MDT
Layer 1-Optics	Layer 1 optical power	Monitors per-port optical power. Generates an alert when power levels exceed the configured threshold.	Major/Minor/Low/High Thresholds	MDT
Layer 1-Optics	Layer 1 optical temperature	Monitors per-port optical temperature. Generates an alert when temperature exceeds the configured threshold.	Major/Minor/Low/High Thresholds	MDT
Layer 1-Optics	Layer 1 optical voltage	Monitors per-port optical voltage. Generates an alert when voltages exceed the configured threshold.	Major/Minor/Low/High Thresholds	MDT
Layer 2-Interface	Line state	Monitors interface line states. Generates an alert when link states change.	Line State Changes	MDT
LLDP	LLDP neighbors	Monitors LLDP neighbors. Generates an alert when any sudden changes are detected.	Standard Deviation	MDT
Memory	Memory utilization	Monitors memory usage across route processor and line cards on routers. Generates an alert when memory utilization is unusual.	Standard Deviation	MDT
Memory	Memory utilization (cXR)	Monitors memory usage across route processor and line cards on classic XR devices. Generates an alert when memory utilization is unusual.	Standard Deviation	MDT
Layer 3-Routing	RIB BGP route count	Monitors RIB for route count and memory used by BGP. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIB connected route count	Monitors RIB for route count and memory used by connected. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT

Category	KPI Name	Description	Alerting	MDT or SNMP
Layer 3-Routing	RIB IS-IS route count	Monitors RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts)	Standard Deviation	MDT
Layer 3-Routing	RIB local route count	Monitors RIB for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIB OSPF route count	Monitors RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIB static route count	Monitors RIB for route count and memory used by static. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIBv6 connected route count	Monitors RIBv6 for route count and memory used by connected. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIBv6 local route count	Monitors RIBv6 for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIBv6 static route count	Monitors RIBv6 for route count and memory used by static. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT
Layer 3-Routing	RIBv6 subscriber route count	Monitors RIBv6 for route count and memory used by subscriber. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT

Category	KPI Name	Description	Alerting	MDT or SNMP
Layer 2-Traffic	SNMP interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	No Alert	SNMP
Layer 2-Traffic	SNMP interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	Rate Change	SNMP
Layer 2-Traffic	SNMP interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation Rate of Change	SNMP
Layer 2-Traffic	SNMP traffic black hole	Monitors input and output data rates for black hole behavior. Checks the ratio of output data rate to input data rate and verifies that the ratio is within acceptable ranges, otherwise a black hole is occurring.	Two-Level Threshold	SNMP
Layer 2-Traffic	Traffic black hole	Monitors input and output data rates for black hole behavior. Checks the ratio of output data rate to input data rate and verifies that the ratio is within acceptable ranges, otherwise black hole.	Two-Level Threshold	MDT

Troubleshoot Health Insights

The following table describes issues you may encounter when using the Health Insights application, and their solutions or workarounds.

Table 5: Health Insights Troubleshooting

Issue	Solution
Apply a KPI to a device fails with messages indicating that Cisco Network Services Orchestrator (Cisco NSO) and the target device are out of sync or otherwise out of communication. Message text will vary, but may include "device out of sync", "NC client timeout", and other text indicating that there are connectivity or sync issues between NSO and the device.	Apply the KPI again. Under normal circumstances, doing so will initiate a sync operation between the device and NSO.

Issue	Solution
Health Insights not receiving data.	<p data-bbox="922 289 1484 323">Check the following and ensure they are responsive:</p> <ul data-bbox="954 336 1484 600" style="list-style-type: none"><li data-bbox="954 336 1484 432">• Crosswork Data Gateway health: View Cisco Crosswork Data Gateway Instance Health, on page 220<li data-bbox="954 453 1484 516">• Collection/distribution status: Monitoring Collection Jobs, on page 259<li data-bbox="954 537 1484 600">• Operational status of the devices: Reachability and Operational State, on page 79



CHAPTER 5

Visualize the Network

This section contains the following topics:

- [Network Visualization Overview, on page 65](#)
- [Identify the Members of a Cluster, on page 67](#)
- [Device and Link Icons, on page 68](#)
- [Get More Information About Devices on the Map, on page 69](#)
- [Access the Device Console, on page 71](#)
- [Get More Information About Links, on page 72](#)
- [Network Link Discovery, on page 73](#)
- [Show Bandwidth Utilization for Links on the Map, on page 74](#)
- [Define Color Thresholds for Link Bandwidth Utilization, on page 74](#)
- [Configure Geographical Map Settings, on page 75](#)
- [Change the Layout of a Logical Map, on page 76](#)
- [Create Custom Map Views, on page 77](#)
- [Manage Custom Map Views, on page 77](#)

Network Visualization Overview

Cisco Crosswork Change Automation and Health Insights provides a graphical, topological map view of devices and the links between them so that you can visualize your network. The network topology 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 in order to troubleshoot problems. You can also filter the devices shown on the map using tags (see [Filter Network Devices by Tags, on page 101](#)), and you can customize the map to show just the information you want, and save these custom maps for later recall.

To open the topology map view, choose **Network Visualization > View Topology** from the left navigation bar in the Cisco Crosswork Change Automation and Health Insights main window.

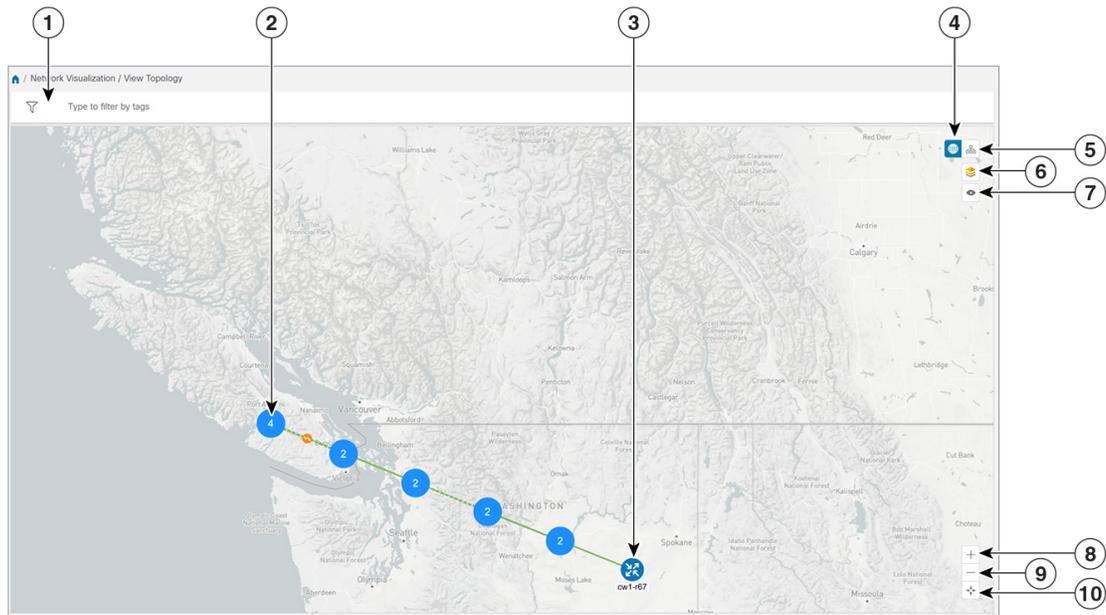


Note If you encounter topology issues, such as topology components not rendering as expected or component data not displaying on the map, Cisco recommends the following:

- If you cannot see geographical map tiles: Make sure your browser has Internet connectivity to your selected geographical map services vendor. The map services vendor and the vendor’s URL are set by the system administrator, as explained in [Configure Geographical Map Settings, on page 75](#).
- If your devices are missing from the geographical map: Ensure that geographic location data was included when onboarding your devices, or entered later. Cisco Crosswork Change Automation and Health Insights cannot position devices properly on the geographical map without location information.
- If you are having intermittent problems displaying the map or your devices: Clear your browser cache and try again.

Also, please note that disjoint network discovery and display are not supported.

Figure 6: Network Visualization: Geographical Map



Item	Description
1	Filter by Tags: If tags have been assigned to devices, you can filter the map to show only devices with specific tags. For help with this task, see Filter Network Devices by Tags, on page 101

Item	Description
2	<p>Device Cluster: If devices are in close physical proximity, the geographical map shows them as a cluster, represented by a solid blue circle with a number in the center, indicating the number of devices in the cluster. Displaying devices in this manner helps prevent overlap and clutter on the map. In this example, there are two devices in the cluster. To see the individual devices in the cluster, zoom in on the cluster or click on the cluster icon. If all the devices in the cluster are in the same location or extremely close to one another, you will be prompted to show the cluster devices in the logical map. See Identify the Members of a Cluster, on page 67.</p> <p>Links: A solid line indicates a <i>single link</i> between two devices. If there is more than one link between two devices, or between a device and a cluster of devices, the line is shown dashed instead. A dashed line indicates an <i>aggregated link</i> that represents more than one link.</p>
3	<p>Single Device: The device icon represents the type of device (router, switch, and so on). A blue icon means the device is reachable; a gray icon means the device is not reachable.</p> <p>Hover the mouse cursor over the device icon to see device details.</p>
4	<p>Geographical Map: Click this icon to toggle from the logical map to the geographical map.</p> <p>The geographical map shows single devices, device clusters, and the links between them, superimposed on a map of the world. The location of a device on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the Device Management application.</p>
5	<p>Logical Map: Click this icon to toggle from the geographical map to the logical map. 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; see Change the Layout of a Logical Map, on page 76.</p> <p>The logical map displays up to 1000 devices and never displays devices in clusters.</p>
6	<p>Display Preferences: Lets you view display settings for devices and link color. For example, you can toggle link color based on state or bandwidth utilization for the mapped links. For more information, see Show Bandwidth Utilization for Links on the Map, on page 74.</p>
7	<p>Custom Views: Lets you create a named custom view using the settings and layout for your current map, or display a custom view you have created previously. See Create Custom Map Views, on page 77.</p>
8	<p>Zoom In: Click the + icon to zoom in on a specific area.</p>
9	<p>Zoom Out: Click the - icon to zoom out.</p>
10	<p>Zoom Fit: Lets you automatically scale the map to fit your zoom area.</p>

Identify the Members of a Cluster

When there are multiple devices that are too close to be shown individually at the current Zoom level, they are combined together and shown as a single cluster. The cluster is represented on the geographical map by a circle with a number in its center, indicating the number of devices in the cluster.

Zoom in on a cluster to see the individual devices in the cluster displayed on the map.

If cluster members are very close to each other or in the same location, zooming in will not show the individual devices. In this case, follow these steps to see the individual members of the cluster:

-
- Step 1** In the geographical map, click . The map zooms in on the cluster area.
- Step 2** Click  again. If you are at the maximum zoom level, the geographical map toggles to the logical map and displays the individual devices in the cluster. When you close the view, you will be switched back to the geographical map.
-

Device and Link Icons

The following tables describe the icons used to represent device states, link states, and device types in the Cisco Crosswork Change Automation and Health Insights user interface.

Table 6: Device State Icons

Icon	Description
	The device is reachable.
	The device is unreachable.
	The device has an unknown reachability state (its reachability cannot be determined).
	The device is operational.
	The device is not operational. It is either not up, or unreachable, or both. In some Cisco Crosswork Change Automation and Health Insights applications (not Network Visualization), a number in a circle is shown next to this icon. The number indicates the number of recent errors and can be clicked on to display error details.
	Some connections to the device are down.

Table 7: Link State Icons

Icon	Description
	Link is down.
	Link is up and traffic is passing through it.
	Link is degraded. If some (but not all links) in an aggregated link are down, the aggregated link shows a degraded icon. The link will also show as degraded if only one direction of an L2 or L3 link was discovered instead of both directions. Click the degraded icon to see exactly which link or interface is down. If <i>all</i> links in an aggregated link are down, the connectivity link shows a link down icon.

Table 8: Device Icons

Icon	Description
	Switch
	Switch (unreachable)
	Router
	Router (unreachable)
	Amplifier
	Amplifier (unreachable)
	Converged Broadband Router (cBR)
	cBR (unreachable)
	Reconfigurable optical add/drop multiplexer (ROADM)
	ROADM (unreachable)
	Device is reachable, but is undefined or of an unknown type
	Unreachable device

Get More Information About Devices on the Map

In the topology map, hover over a device icon to open a popup window with the most important device details: hostname, reachability state, IP address, and type. Click on the device icon to open the **Device Details** pop-up

window, where you can view more detailed information about the device and its associated links. See the following examples.

Figure 7: Device Details

The screenshot displays the 'Network Topology' interface. On the left, a map of San Francisco shows the location of device NPE1-9K. A tooltip for this device provides the following information:

- Host Name: -9K-NGN
- State: Unknown
- Node IP: 10.56
- Type: ASR9K

The 'Device Details' window on the right is divided into two tabs: 'Details' (selected) and 'Links'. The 'Details' tab shows the following information:

- Summary**
 - Host Name: -9K-NGN
 - State: Unknown
 - Operational State: OK
 - Node IP: 10.56
 - Civic Address: San Francisco, California, United States, North America, 94539
 - Geo Location: Longitude: -122.446747, Latitude: 37.733795
 - Type: ASR9K
 - Connect To Device: Telnet IPv4, SSH IPv4
 - Last Update: (GMT -07:00)
- Routing**
 - TE router ID: .1.1
 - ISIS system ID: 1 level-2
 - ASN: 100

In the **Device Details** window, click on the **Links** tab to see a list of all of the device's links to other devices, as in the following example (see [Get More Information About Links, on page 72](#)):

Figure 8: Links Tab of Device Details Window

Device Details

Summary **Links**

Links on Device spnac-a9k-s

Showing 4 of 4 Clear Filter

State	Link Type	A Side Interf...	Z Side Interf...	A Side Utiliz...	Z Side Utiliz...
↑	L3 ISIS IPV4	GigabitEthern...	GigabitEthern...	0% (1.41Kbps/1)	52.1% (521.14M)
↑	L3 ISIS IPV4	GigabitEthern...	GigabitEthern...	52.2% (522.8Mt)	0% (1.53Kbps/1)
↑	L2 CDP	GigabitEthern...	GigabitEthern...	52.2% (522.8Mt)	0% (1.53Kbps/1)
↑	L2 CDP	GigabitEthern...	GigabitEthern...	0% (1.41Kbps/1)	52.1% (521.14M)

Access the Device Console

After drilling down to a device's details from the topology map, you can access the device's CLI command console from the **Device Details** window (see [Get More Information About Devices on the Map](#), on page 69).

Before you begin

- Depending on your environment, your local machine may not have direct access to your network devices (for example: you cannot ping the device's management address directly from the command line on your local machine). If this is the case, you may need to configure a tunnel. Contact Cisco Services for assistance with this more advanced configuration.
- Be sure you have installed on your client an application that can connect to devices via Secure Shell (SSH) or Telnet.

Step 1 From the main menu, choose **Network Visualization > View Topology**.

Step 2 In the topology map, click on the icon representing the device to which you want to connect. The **Device Details** window displays its **Details** tab, with the device hostname, reachability state, IP address, and other details.

Step 3 In the **Connect to Device** field, click the relevant link to connect to the device console via Telnet , or via SSH .

If you have already defined a default connectivity application that you want to launch, Cisco Crosswork Change Automation and Health Insights launches your selected application and attempts to connect to the device. Log into the device and enter the commands you want.

If you have not defined a default application to launch, your browser will prompt you to select one. Your choices and how they are presented will be appropriate for your client operating system, the applications you have installed, and the connectivity protocol you choose. Select the application you want and, for convenience, make sure that you select the check box indicating that this is your default choice before continuing.

Get More Information About Links

You can drill down in the topology map to view detailed information about links, using either of these methods:

- Click on an aggregated link (symbolized by a dashed line) to show the individual links in the side panel.
- Click on a single link (solid line) to show the **Link Details** page.

The **Links** page provides information about the configuration and status of all of a device's links, including each link's type, interfaces, and utilization (you can get the same information from the **Links** tab on the **Device Details** window; see [Get More Information About Devices on the Map, on page 69](#)). The **Links** window lists all the underlying links in the aggregation, as in the following example:

Figure 9: Links Window



The screenshot shows a window titled "Links" with a close button (X) in the top right corner. Below the title bar, there is a "Total 4" indicator with a refresh icon and a settings gear icon. The main content is a table with the following columns: State, Link Type, A Side Device, Z Side Device, A Side Device, and Z Side Device. Each column has a dropdown arrow. The table contains four rows of data, all with a green up arrow in the State column and "L3 OSPF V2" in the Link Type column. The A Side Device and Z Side Device columns show "GigabitEthernet..." for each row.

State	Link Type	A Side Device	Z Side Device	A Side Device	Z Side Device
↑	L3 OSPF V2	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...
↑	L3 OSPF V2	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...
↑	L3 OSPF V2	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...
↑	L3 OSPF V2	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...	GigabitEthernet...

Use the expand and collapse icons (< and >) to the left of the **Links** title to expand the window to the entire screen, or collapse the window back to its normal size.

Click  to choose the columns to make visible in the **Links** window's table:

- **State**—Displays each link's state: up, down, degraded, and so on (see [Device and Link Icons, on page 68](#)).
- **Link Type**—Displays the type of link. Click on the link type to open the **Link Details** window for the specific link.
- **A Side Device**—Displays the originating device for the link.
- **Z Side Device**—Displays the destination device for the link.

- A Side Interface—Displays the originating interface for the link.
- Z Side Interface—Displays the destination interface for the link.
- A Side Utilization—Displays the percentage of bandwidth consumption on the originating side of the link.
- Z Side Utilization—Displays the percentage of bandwidth consumption on the destination side of the link.

You can also use sorts and filters in the **Links** window to focus the table on only the links in which you are interested (see [Set, Sort and Filter Table Data, on page 6](#)).

The **Link Details** window provides information about the configuration and status of a single link, including link type, the link's interfaces, associated adjacent segment IDs, and so on.

Link Details
✕

< Summary
>

State ↑ Up

Link Type L3 OSPF V2

Last Update 2019-Feb-18, 13:21:34 (GMT -08:00)

Name GigabitEthernet0/0/0/2-GigabitEthernet0/0/0/2

	A Side	Z Side
Node	iosxrv-6	iosxrv-5
Interface	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/2
IP Address	10.0.0.50/0	10.0.0.49/0
Adj SID	24000 Unprotected 24001 Protected	24002 Unprotected 24003 Protected
IGP	1	1
TE	1	1
Delay	1	1

Network Link Discovery

Layer 2 links are discovered by enabling SNMP on the inventory. Devices must be onboarded in order to be visible on the topology. SNMP data is required as CDP MIB and/or LLDP MIB are needed to discover the Layer 2 links. For more information on onboarding prerequisites, see [Prerequisites for Onboarding Devices, on page 91](#)

Layer 3 links are discovered from adding the Cisco Segment Routing Path Computation Elements (SR-PCE) providers. At least one SR-PCE provider is required in order to discover the Layer 3 links. Devices must be onboarded (at least in unmanaged state) so that the Layer 3 links and nodes are properly displayed. For more information, see [Add Cisco SR-PCE Providers, on page 179](#)



Note The SR-PCE provider must be reachable from Cisco Crosswork Change Automation and Health Insights and must have a topology detected before the links can be displayed.

Show Bandwidth Utilization for Links on the Map

In the geographical map and in the logical map, you can enable visualization of the bandwidth utilization for links over which circuits are provisioned. When bandwidth utilization visualization is enabled, links in the map are colored based on the percentage of total bandwidth currently utilized on the link. The utilization value is a percentage calculated by dividing link traffic by link capacity.

In this way, you can easily identify when a link is over-utilized or approaching over-utilization. Bandwidth visualization is enabled by default. The color of the link indicates the percentage of total bandwidth being used by provisioned circuits on the link:

- Green—0–25% usage
- Yellow—25–50% usage
- Orange—50–75% usage
- Red—75–100% usage

You can adjust the thresholds for each color as needed (see [Define Color Thresholds for Link Bandwidth Utilization](#), on page 74). When visualization is disabled, the links are shown only in blue.

Please note that link bandwidth utilization data can be collected and displayed only if the linked devices are added to and managed in the device inventory.

To enable or disable visualization of bandwidth utilization:

Step 1 From the main menu, choose **Network Visualization > View Topology..**

Step 2 In the top-right corner of the map, click  to open display preferences which can be used to toggle the display of bandwidth utilization. When usage visualization is enabled, the links can be shown in green, yellow, orange, or red, depending on their utilization. If you see only blue links, usage visualization is disabled.

Define Color Thresholds for Link Bandwidth Utilization

Cisco Crosswork Change Automation and Health Insights comes with a default set of bandwidth utilization thresholds (percentage ranges) and corresponding color indicators. You can customize these to meet your needs, taking into account the following notes and limitations:

- You can enter values in the "To" ranges. 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.

Administrator privileges are required to change these settings.

-
- Step 1** From the main menu, choose **Admin > Visualization Settings**.
- Step 2** Click the **Bandwidth Utilization** tab.
- Step 3** In the **Polling Interval** field, enter a whole number from 5 to 60 (minutes) to specify how often links will be polled for bandwidth utilization. By default, link bandwidth is polled every 5 minutes.
- Step 4** In the **Link Coloring Thresholds** area, define the criteria for coloring the links. Each row defines a color and the bandwidth percentage range that the color will represent. The default thresholds are:
- Green—0–25% usage
 - Yellow—25–50% usage
 - Orange—50–75% usage
 - Red—75–100% usage
- Step 5** Click **Save**.
-

Configure Geographical Map Settings

The geographical map lets you position your network devices on a world map and monitor them within their geographical context. The displayed world map is imported by accessing the map vendor's site over the Internet (online mode). The look of the map will vary depending on the map vendor you choose.

By default, the client machine from where you access the Cisco Crosswork Change Automation and Health Insights UI is setup to get map tiles from a specific Mapbox URL over internet connection. If required, you can use a different map vendor (such as Google Maps or OpenStreetMap) by providing the appropriate URL. Both of these options require an Internet connection from your client machine.

Cisco Crosswork Change Automation and Health Insights administrator privileges are required to change these settings.

-
- Step 1** From the main menu, choose **Admin > Visualization Settings**.
- Step 2** Click the **Map** tab.
- Step 3** From the **Map Provider** drop-down list, choose one of the following:
- **Mapbox**—Specifies that you want to display the geographical map using the default map provider.
 - **Custom**—Identifies the map tiles source (using an Internet connection). To use a map provider other than Mapbox, you must provide the URL for map tiles access. Be sure to request the exact format of this URL from the map tiles provider.
- Step 4** If you are using a custom map provider, in the **Map Source URL** field, enter the URL for map access.

Step 5 Click **Save**.

Change the Layout of a Logical Map

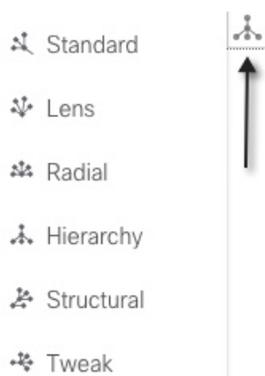
When you open the logical map, it is displayed according to the default standard layout. You can change the layout, but any changes you make will not persist if you close the map. To save your layout changes, create a custom view (see [Create Custom Map Views, on page 77](#)).

Step 1 From the main menu, choose **Network Visualization > View Topology**.

Step 2 In the top-right corner of the map, toggle from the geographical map view to the logical map view.

Step 3 In the logical map, click the **System Layouts** icon in the toolbar to access the layout options.

Figure 10: System Layouts



Step 4 Choose one of the predefined options to rearrange the devices and links in the map according to your preference:

- **Standard (default)**—Maintains consistent link length and distributes devices evenly. This ensures that adjacent devices are closer to each other and prevents overlap.
 - **Lens**—Positions highly connected devices in the center, and moves less-connected devices out to the edges. This layout is especially useful in large networks.
 - **Radial**—Arranges the devices in a circular style around the original subject. Each generation of devices becomes a new concentric ring that orbits the original parent. This layout is useful in networks where each parent has many child devices.
 - **Hierarchy**—Displays devices in a family tree, where child devices are shown in horizontal layers underneath their parents.
 - **Structural**—Groups devices with similar attributes together in a fan shape. This layout gives you an overview of the clusters in the network.
 - **Tweak**—Adjusts the layout as the network evolves. As devices and links are added and removed, the layout adapts itself, allowing you to visualize network changes.
-

Create Custom Map Views

When you rearrange the devices and links on a map, your changes are not normally saved. When you open the map later, your map settings are lost.

To easily recreate a useful map layout, you can save it as a named custom view and quickly retrieve it, without having to rearrange the map each time. This is especially useful when managing large networks with many devices.

When you save a custom view, the following settings will be saved:

- Whether it is a geographical or logical map.
- Device positions in the logical map layout.
- Whether bandwidth utilization visualization is enabled or disabled.
- Tag filters that have been applied to the map.



Note

- The map zoom level will not be saved.
 - Your custom map views are not user-specific. Any Cisco Crosswork Change Automation and Health Insights user who is logged into the same host as you can see and further customize the map views you create.
-

To create custom views:

-
- Step 1** Choose **Network Visualization > View Topology** from the left navigation bar.
 - Step 2** Customize the current map view until it contains only the information you want and until the layout meets your needs.
 - Step 3** When you have the view the way you want it, click .
 - Step 4** Click **Save View** and the Save View popup displays a new, blank input field under the **Name** field.
 - Step 5** Enter a unique name for the new custom view and click **Save**.
-

What to do next

Retrieve, update and delete your custom views as explained in [Manage Custom Map Views, on page 77](#).

Manage Custom Map Views

You can display, update or delete any of the custom views created using the instructions in [Create Custom Map Views, on page 77](#). This includes custom views created by other users.

To manage custom views:

-
- Step 1** Open the topology map by choosing **Network Visualization > View Topology** from the left navigation bar.

Step 2 Click  and the following options are displayed:

- **View Saved Views**—Displays all saved custom views. You can choose to see only custom views saved with your user ID (My Views tab) or all custom views that have been saved on the server (All Views tab).
- **Save View**—Allows you to save the current view.
- **Save View As**—Click this option if you are currently modifying a custom view and want to save changes as a new custom view with a new name.
- **Rename View**—Click this option if you are currently modifying a custom view and want to rename it.

Step 3 To delete a custom view:

- a) Click the **View Saved Views** to display the list of custom views.
 - b) Find the view you want to delete and click  from the custom view.
-



CHAPTER 6

Manage Inventory

This section contains the following topics:

- [Device Management Overview, on page 79](#)
- [Reachability and Operational State, on page 79](#)
- [Manage Credential Profiles, on page 81](#)
- [Manage Network Devices, on page 89](#)
- [Manage Devices Using Zero Touch Provisioning, on page 104](#)

Device Management Overview

The Device Management application lets you create, edit, and delete:

- The **credential profiles** that control Cisco Crosswork Change Automation and Health Insights's access to devices and providers. See [Manage Credential Profiles, on page 81](#).
- The **devices** you manage using Cisco Crosswork Change Automation and Health Insights. See [Manage Network Devices, on page 89](#).

You can also use Device Management to review the **jobs** executed on your devices. See [View Device Job History, on page 103](#).

Reachability and Operational State

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

Table 9: Reachability and Operational State Icons

This Icon...	Indicates...
Reachability State icons show whether a device or a provider is reachable or not	
	Reachable: The device or provider can be reached by all configured protocols configured for it.

This Icon...	Indicates...
	Reachability Degraded: The device or provider can be reached by at least one protocol, but is not reachable by one or more of the other protocols configured for it.
	Unreachable: The device or provider cannot be reached by any protocol configured for it.
	Reachability Unknown: Cisco Crosswork Change Automation and Health Insights cannot determine if the device is reachable, degraded, or unreachable. This state can also occur if the device is not connected to Cisco Crosswork Data Gateway.
Operational State icons show whether a device is operational or not.	
	The device is operational and under management, and all individual protocols are "OK" (also known as "up").
	The device is not operational ("down"). The same icon is used when the device has been set "administratively down" by an operator.
	The device's operational or configuration state is unknown.
	The device's operational or configuration state is degraded.
	The device's operational or configuration state is in an error condition. It is either not up, or unreachable, or both, due to errors encountered while attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of recent errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available in the Network Visualization application.)
	The device's operational state is currently being checked
	The device is being deleted.
	The device is unmanaged.

The Reachability State of a device is computed as follows:

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

The Operational State of a device is computed as follows:

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

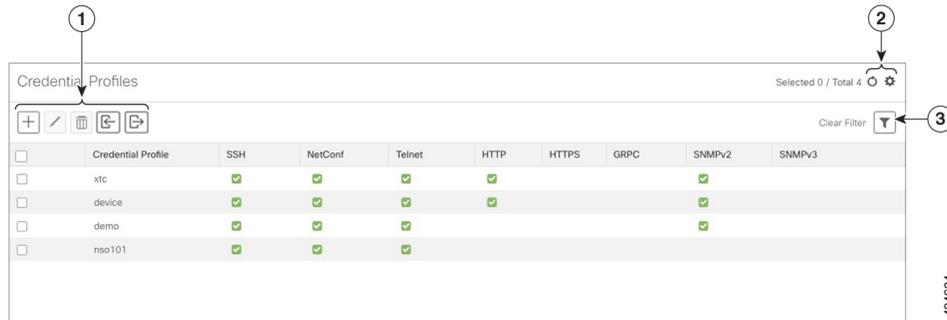
Manage Credential Profiles

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 11: Credentials Profile window



Item	Description
1	Click to add a credential profile. See Create Credential Profiles, on page 82 .
	Click to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 86 .
	Click to delete the selected credential profile. See Delete Credential Profiles, on page 87 .
	Click to import new credential profiles from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Credential Profiles, on page 84 .
	Click to export credential profiles to a CSV file. See Export Credential Profiles, on page 87 .
2	Click to refresh the Credential Profiles window.
	Click to choose the columns to make visible in the Credential Profiles window (see Set, Sort and Filter Table Data, on page 6).
3	Click to set filter criteria on one or more columns in the Credential Profiles window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Create Credential Profiles

Follow the steps below to create a new credential profile. You can then use the profile to apply credentials consistently when you add new devices or providers. You can add as many protocols and corresponding credentials to the profile as you want.

If you have many credential profiles to add, you may find it more efficient to put the information in a CSV file and import the file. See [Import Credential Profiles, on page 84](#).

When creating device credential profiles that contain SNMP credentials, Cisco recommends that the profile contain credentials for the version of SNMP actually enabled on the device, and that version only. For example: If SNMPv3 is not enabled in the device configuration, do not include SNMPv3 credentials in the device credential profile.

If you plan to use the import and export features and CSV files to create credential profiles in bulk, please note that:

- All the characters in each password or community string entry in every credential profile exported to a CSV file are replaced with asterisks ([Export Credential Profiles, on page 87](#)).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see [Import Credential Profiles, on page 84](#)).

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 86](#) to replace the asterisks with actual passwords and community strings.

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

Step 2 Click .

Step 3 In the **Profile Name** field, enter a descriptive profile name. The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.

If you will have many credential profiles, make the name as informative as possible because that information will be displayed on the Credential Profiles panel.

Step 4 Select a protocol from the **Connectivity Type** dropdown.

Step 5 Complete the credentials fields described in the following table. The required and optional fields displayed will vary with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
SSH	Enter the required User Name , Password , and Confirm Password . The Enable Password is optional.
SNMPv2	Enter the required SNMPv2 Read Community string. The Write Community string is optional.
NETCONF	Enter the required User Name , Password , and Confirm Password .
TELNET Note There may be some security limitations when using this protocol.	Enter the required User Name , Password , and Confirm Password . The Enable Password is optional.
HTTP	Enter the required User Name , Password , and Confirm Password .
HTTPS	Enter the required User Name , Password , and Confirm Password .
GRPC	Enter the required User Name , Password , and Confirm Password .

Connectivity Type	Fields
SNMPv3	<p>Choose the required Security Level and enter the User Name.</p> <p>If you chose the NO_AUTH_NO_PRIV Security Level of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional.</p> <p>If you chose the AUTH_NO_PRIV Security Level, you must choose an Auth Type and enter an Auth Password.</p> <p>If you chose the AUTH_PRIV Security Level, you must choose an Auth Type and Priv Type, and enter an Auth Password and Priv Password.</p> <p>Only the following SNMPv3 Privacy Types are supported</p> <ul style="list-style-type: none"> • CFB_AES_128 • CBC_DES_56 <p>The following Privacy Types are not supported:</p> <ul style="list-style-type: none"> • AES192 • AES256 • 3DES

Step 6 (Optional) Click + **Add Another** and repeat the above steps, as needed, for all other protocols and corresponding credentials you want to add to this credential profile.

Step 7 Click **Save**.

Import Credential Profiles

Complete the steps below to create a CSV file that specifies multiple credential profiles and then import it into Cisco Crosswork Change Automation and Health Insights.

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 86](#) to replace the asterisks with actual passwords and community strings.

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

Step 2 Click  to open the **Import CSV File** 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. Failure to do so will result in loss of device connectivity, and inability to collect certain KPI data or execute configured Playbooks on devices associated with the credential profile.
- Password and community string information associated with a user ID are stored in plain text in the CSV file you prepare. Be aware of the security implications of this, and apply appropriate safeguards.

Field	Entries	Required or Optional
Credential Profile	The name of the credential profile. For example: nso .	Required
Connectivity Type	Valid values are: SSH, SNMPv2, NETCONF, TELNET, HTTP, HTTPS, GRPC or SNMPv3	Required
User Name	For example: NSOUser	Required if Connectivity Type is SSH, NETCONF, TELNET, HTTP, HTTPS, SNMPv3 or GRPC .
Password	The password for the preceding User Name .	Required if Connectivity Type is SSH, NETCONF, TELNET, HTTP, HTTPS or GRPC
Enable Password	Use an Enable password. Valid values are: ENABLE, DISABLE	Required if Connectivity Type is SSH or TELNET . Otherwise leave blank.
Enable Password Value	Specify the Enable password to use.	Required if Connectivity Type is SSH or TELNET and Enable Password is set to ENABLE . Otherwise leave blank.
SNMPV2 Read Community	For example: readprivate	Required if Connectivity Type is SNMPv2
SNMPV2 Write Community	For example: writeprivate	Required if Connectivity Type is SNMPv2
SNMPV3 User Name	For example: DemoUser	Required if Connectivity Type is SNMPv3

Field	Entries	Required or Optional
SNMPV3 Security Level	Valid values are noAuthNoPriv , AuthNoPriv or AuthPriv	Required if Connectivity Type is SNMPv3
SNMPV3 Auth Type	Valid values are HMAC_MD5 or HMAC_SHA	Required if Connectivity Type is SNMPv3 and SnmPV3 Security Level is AuthNoPriv or AuthPriv
SNMPV3 Auth Password	The password for this authorization type.	Required if Connectivity Type is SNMPv3 and SnmPV3 Security Level is AuthNoPriv or AuthPriv
SNMPV3 Priv Type	Valid values are CFB_AES_128 or CBC_DES_56 The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	Required if Connectivity Type is SNMPv3 and SnmPV3 Security Level is AuthPriv
SNMPV3 Priv Password	The password for this privilege type.	Required if Connectivity Type is SNMPv3 and SnmPV3 Security Level is AuthPriv

Be sure to delete the sample data rows before saving the file or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

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

The credential profiles you imported should now be displayed in the **Credential Profiles** window.

Edit Credential Profiles

A credential profile can be shared by multiple devices, even hundreds of devices in a large network. Complete the following procedure to edit credential profile settings.



Warning

Changing the settings in a credential profile without first changing the settings on the device associated with the profile may result in a loss of connectivity, inability to collect certain KPI data, or an inability to execute configured playbooks on devices associated with the modified profile. For example: If the SNMP community string on the device no longer matches what is in the credential profile, SNMP-based KPIs will not function.

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 87](#)).

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**.

Note If the device is not updated within 30 seconds when you modify connectivity or credential profile information, move the device state to DOWN and then UP. The CLI reachability is triggered and the updated values are displayed.

Delete Credential Profiles

Follow the steps below to delete a credential profile.



Note You cannot delete a credential profile that is associated with one or more devices or providers.

- Step 1** Export a backup CSV file containing the credential profile you plan to delete (see [Export Credential Profiles, on page 87](#)).
- 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 **Admin** > **Providers**).
- Step 3** Reassign the devices or providers to a different credential profile (for help with this task, see [Change the Credential Profile for a Device or Provider, on page 88](#) or [Change the Credential Profile for Multiple Network Devices, on page 88](#), and [Edit Providers, on page 187](#)).
- Step 4** After all devices and providers have had their credential profiles reassigned: From the main menu, choose **Device Management** > **Credential Profiles**.
- Step 5** In the **Credential Profiles** window, choose the profile that you want to delete and then click .
-

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 86](#) to replace the asterisks with actual passwords and community strings.

- Step 1** From the main menu, choose **Device Management** > **Credential Profiles**.
- Step 2** (Optional) In the **Credential Profiles** window, filter the credential profile list as needed.
- Step 3** Check the check boxes for the profiles you want to export. Check the check box at the top of the column to select all the profiles for export.

- Step 4** Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately

Change the Credential Profile for a Device or Provider

You can edit device information, including changing the credential profile in the device record. This operation changes an existing association between a device and a credential profile.

Before you begin

You need a credential profile to complete this task. To create a credential profile, see [Create Credential Profiles, on page 82](#).



Note Make sure the profile's credential settings are correct before following this procedure.

-
- Step 1** From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.
- Step 2** (Optional) Filter the device list by entering text in the **Search** field or filtering specific columns.
- Step 3** Check the check box of the device you want to change, and click .
- Step 4** Choose a different credential profile from the **Credential Profile** drop-down list.
- Step 5** Click **Save**.

After the device record is updated, the system attempts to communicate with the device using the new profile. Confirm that the device is reachable without any errors.

Change the Credential Profile for Multiple Network Devices

If you want to change the credential profile for a large number of network devices, you may find it more efficient to make the change by editing a devices CSV file. The basic method is:

1. Export a CSV file containing the devices whose credential profiles you want to change (see [Export Network Devices, on page 103](#)).
2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist). Save the edited file.

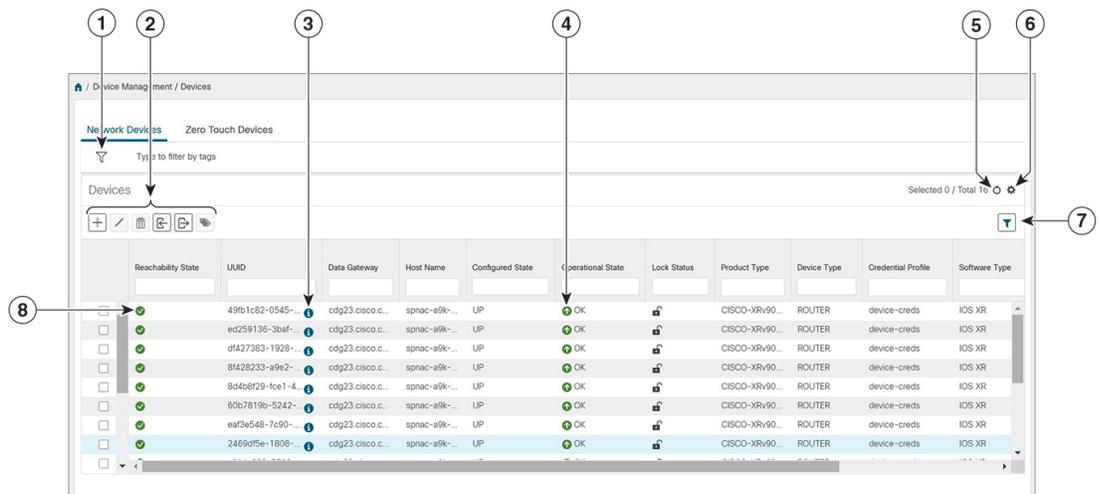
You will need to make sure that the credential profile to which you are changing already exists. If you have not yet created that credential profile, the CSV import will fail. The credential profile you associate with these devices must also have the authorization credentials for every protocol that was configured for these devices during onboarding. If any credential for a specific protocol configured on the devices is missing from or incorrect in the credential profile, then the CSV import will succeed, but reachability checks will fail for these devices.

- Step 1** From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.
- Step 2** Choose the devices whose credential profiles you want to change. Your options are:
- Click  to include all devices.
 - Filter the device list by entering text in the **Search** field or by filtering specific columns. Then click  to include only the filtered list of devices.
 - Check the boxes next to the device records you want to change. Then click  to include only the devices that have been checked.
- Step 3** Edit and save the new CSV file using the tool of your choice. Be sure to enter the correct credential profile name in the **Credential Profile** field for each device.
- Step 4** Click .
- Step 5** In the **Import** dialog box, click **Browse**, choose the new CSV file, and click **Import**.

Manage Network Devices

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

Figure 12: Devices Window



Item	Description
1	The Filter by tags field lets you filter the devices by the tags applied to them. Type the name of the tag that has been applied to the device that you are trying to find. See Filter Network Devices by Tags, on page 101 .

Item	Description
2	Click  to add a new device to the device inventory. See About Adding Devices to Inventory, on page 90 .
	Click  to edit the information for the currently selected devices. See Edit Network Devices, on page 101 .
	Click  to delete the currently selected devices. See Delete Network Devices, on page 102 .
	Click  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. See Import Network Devices, on page 94 .
	Click  to export information for selected devices to a CSV file. See Export Network Devices, on page 103 .
	Click  to modify tags applied to the selected devices. See Apply or Remove Device Tags, on page 191 .
3	Click  to open the Device Details pop-up window, where you can view important information for the selected device. See Get Network Device Details, on page 99 .
4	Icons in the Operational State column show whether a device is operational or not. See Reachability and Operational State, on page 79
5	Click  to refresh the Devices list.
6	Click  to select which columns to display in the Devices list (see Set, Sort and Filter Table Data, on page 6).
7	Click  to set filter criteria on one or more columns in the Devices list.
	Click the Clear Filter link to clear any filter criteria you may have set.
8	Icons in the Reachability State column show whether a device is reachable or not. See Reachability and Operational State, on page 79 .

About Adding Devices to Inventory

There are six ways to add devices to Cisco Crosswork Change Automation and Health Insights. Each has its own set of prerequisites, which you must fulfill if the device addition is to succeed.

In order of preference for most users, the methods and their prerequisites are:

1. **Importing devices using the Cisco Crosswork Change Automation and Health Insights APIs:** This is the fastest and most efficient of the three methods, but requires programming skills and API knowledge. For more, see the [inventory management APIs on Cisco Devnet](#).

2. **Importing devices from a Devices CSV file:** This method is explained in [Import Network Devices, on page 94](#). This method is time-consuming and error-prone, as you must create and format all of the data yourself beforehand (including not only devices, but also the providers, credential profiles and tags), and then ensure all of these items are properly associated with the devices after the CSV import. To succeed with this method, you must first:
 - Create the provider(s) that will be associated with the devices (see [Manage Providers, on page 170](#))
 - Create corresponding credential profiles for all of the devices and providers listed in the CSV file (see [Create Credential Profiles, on page 82](#))
 - Create tags for use in grouping the new devices (see [Manage Tags, on page 188](#))
 - Download the CSV template file from Cisco Crosswork Change Automation and Health Insights and populate it with all the devices you will need.
3. **Adding them via the UI:** This method is explained in [Add Network Devices Through the UI, on page 95](#). It is the least error-prone of the three methods, as all data is validated during entry, but 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.
4. **Auto-onboarding from a Cisco SR-PCE provider:** This method is explained in [Add Cisco SR-PCE Providers, on page 179](#). 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.
5. **Auto-onboarding using Zero Touch Provisioning:** This method is explained in [Manage Devices Using Zero Touch Provisioning, on page 104](#). 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.
6. **Onboard the devices on Cisco Crosswork Data Gateway:** This method is explained in [Attach a Device to a Cisco Crosswork Data Gateway Instance, on page 217](#).



Note Cisco Crosswork Change Automation and Health Insights version 3.2 supports only single stack deployment modes. Devices can be onboarded either with only IPv4 address or only IPv6 address.

Prerequisites for Onboarding Devices

Before adding devices, you must ensure that the devices themselves are configured to collect and transmit telemetry data properly and communicate successfully with Cisco Crosswork Change Automation and Health Insights. The following sections provide sample configurations for a variety of communications options. Use them as a guide to configuring the devices you plan to manage using Cisco Crosswork Change Automation and Health Insights.



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

Pre-Onboarding SNMP v2 Device Configuration

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and Telnet rate limits. The NETCONF setting is only needed if the device is MDT-capable.

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
line default
  exec-timeout 0 0
  width 107
  length 37
  absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
  server <NTPServerIPAddress>
!
service cli history size 5000
service cli interactive disable
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
  ssh
!
```

Pre-Onboarding SNMPv3 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 Change Automation and Health Insights, 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 cisco123 udp-port
1062

snmp-server community cisco123

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 cisco123 udp-port
1062
```

```
snmp-server community cisco123
```

```
snmp-server traps snmp linkup
```

```
snmp-server traps snmp linkdown
```

Please note that, for traps to be received, the snmp ip field for the device as listed in the Cisco Crosswork Change Automation and Health Insights inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork Change Automation and Health Insights will reject the traps. Also, the device needs to be in ADMIN_UP state for traps to be received.

Sample Configuration for Devices in Cisco NSO

If you plan to use Cisco NSO as a provider to configure devices managed by Cisco Crosswork Change Automation and Health Insights, be sure that the Cisco NSO device configurations observe the following guidelines.

The following example shows a Cisco NSO setup 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 remote name and password of cisco. Next, we are setting all the devices with a name that starts with Router to a device type of netconf using ned-id cisco-iosxr-nc-6.6. Finally, we are setting all of the devices with a name starting with Router to be assigned to authgroup cisco. Edit the setting to match your environment. For example:

```
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 steps unlock the devices and retrieve the ssh keys from all of the devices. NSO then synchronizes itself with the device by uploading the devices current configuration and stores the present configuration. It is important to perform these steps to ensure that the device, NSO, and Crosswork Network Automation applications are starting from a common configuration. For example:

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
commit
```

Import Network Devices

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

Importing devices from a CSV file adds any devices not already in the database, and overwrites the data in any device record with an Inventory Key Type and device key field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import). For this reason, it is a good idea to export a backup copy of all your current devices before an import (see [Export Network Devices, on page 103](#)).



Note If you plan on using a CSV file to import devices managed by Cisco Network Services Orchestrator (Cisco NSO), you must prepare the CSV following the guidelines given in [Sample Configuration for Devices in Cisco NSO, on page 93](#).

Step 1 From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.

Step 2 Click  to open the **Import CSV File** dialog box.

Step 3 If you have not already created a device CSV file to import:

- a) Click the **Download sample 'Device Management template (*.csv)' file** link and save the CSV file template to a local storage resource.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each device.

Note Confirm that the TE router ID value for each device is populated. This value is used to uniquely identify the device in the topology which is learned from SR-PCE. Without a valid TE router ID for each device, the topology will not be displayed.

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 Network Devices Through the UI, on page 95](#).

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

- c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

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

Step 6 Resolve any errors and confirm device reachability.

The device information you imported should be displayed in the **Devices** window within a few minutes (see [Manage Network Devices, on page 89](#)).

It is normal for devices to show as unreachable or not operational when they are first imported. However, if after 30 minutes they are still displayed as unreachable or not operational, there is an issue that needs to be investigated. To investigate, select **Device Management > Job History** and click on any  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 Cisco Crosswork Change Automation and Health Insights server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

Add Network 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 when adding one or a few devices only. For the bulk of your devices, add them either by synchronization with a provider (see [Add Cisco SR-PCE Providers, on page 179](#)), or by importation from a CSV file (see [Import Network Devices, on page 94](#)).

Before you begin

Be sure you have completed the planning steps and setup requirements discussed in [Get Started , on page 9](#), and that the devices themselves have been pre-configured as explained in [Prerequisites for Onboarding Devices, on page 91](#).

- Step 1** From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.
- 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 complete.)
- Step 5** (Optional) Repeat to add more devices.

Table 10: Add New Device Window (=Required)*

Field	Description
* Configured State	<p>The management state of the device. Options are</p> <ul style="list-style-type: none"> • UNMANAGED—Cisco Crosswork Change Automation and Health Insights is not monitoring the device. • DOWN—The device is being managed and is down. • UP—The device is being managed and is up.

Field	Description
* Reachability Check	<p>Determines whether Cisco Crosswork Change Automation and Health Insights performs reachability checks on the device. Options are:</p> <ul style="list-style-type: none"> • ENABLE (In CSV: REACH_CHECK_ENABLE)—Checks for reachability and then updates the Reachability State in the UI automatically. • DISABLE (In CSV: REACH_CHECK_DISABLE)—The device reachability check is disabled. <p>Cisco recommends that you always set this to ENABLE. This field is optional if Configured State is marked as UNMANAGED.</p>
* Credential Profile	<p>The name of the credential profile to be used to access the device for data collection and configuration changes. For example: nso23 or srpce123.</p> <p>This field is optional if Configured State is marked as UNMANAGED.</p>
Host Name	The hostname of the device. Cisco Crosswork Change Automation and Health Insights discovers it and updates it.
Inventory ID	Inventory ID value for the device. The value can contain a maximum of 128 alphanumeric characters, and can include dots (.), underscores ("_"), colons (":"), or hyphens ("-"). No other special characters are allowed.
Software Type	Software type of the device. For more information, see Supported Devices and Software Types, on page 311 .
Software Version	Software version of the device. For more information, see Supported Devices and Software Types, on page 311 .
UUID	Universally unique identifier (UUID) for the device.
Serial Number	Serial number for the device.
MAC Address	MAC address of the device.
* Capability	The capabilities that allow collection of device data and that are configured on the device. You must select at least SNMP as this is a required capability. The device will not be onboarded if SNMP is not configured. Other options are YANG_MDT , TL1 , YANG_CLI , and YANG-EPNM . The capabilities you select will depend on the device software type and version.
Tags	<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. For more information, see Manage Tags.</p>
Product Type	Product type of the device.
Connectivity Details	

Field	Description
Protocol	<p>The connectivity protocols used by the device. Choices are: SSH, SNMPv2, NETCONF, TELNET, HTTP, HTTPS, GRPC, and SNMPv3.</p> <p>To add more connectivity protocols for this device, click + at the end of the first row in the Connectivity Details panel. To delete a protocol you have entered, click × shown next to that row in the panel.</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 SSH and SNMP. If you do not configure SNMP, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for NETCONF. TELNET connectivity is optional.</p>
* IP Address / Subnet Mask	<p>Enter the device's IP address (IPv4 or IPv6) and subnet mask.</p> <p>Note Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues.</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 Protocol you chose. The standard port assignments for each protocol are:</p> <ul style="list-style-type: none"> • SSH: 22 • SNMP: 161 • NETCONF: 830 • TELNET: 23 • HTTP: 80 • HTTPS: 443
Timeout	<p>The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.</p>
Routing Info	
ISIS System ID	<p>The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.</p>
OSPF Router ID	<p>The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.</p>
*TE Router ID	<p>The device's OSPF Router ID or ISIS Router ID depending on the IGP used in the network topology.</p>
Streaming Telemetry Config	
Vrf	<p>Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.</p>
Source Interface	<p>The range of loopback in the device type. This field is optional.</p> <p>Note This field can be edited only when the device is in DOWN or UNMANAGED state.</p>

Field	Description
Location	
All location fields are optional, with the exception of Longitude and Latitude , which are required for the geographical view of your network topology.	
Longitude, Latitude	Longitude and latitude values are required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude and latitude in Decimal Degrees (DD) format.
Altitude	The altitude, in feet or meters, at which the device is located. For example, 123 .
Providers and Access	
Local Config: Provider and Device Key	<p>Provider type used to configure devices. Choose a provider from the list.</p> <p>If a Cisco NSO provider is chosen, the Device Key will automatically populate and the Credential Profile appears.</p> <p>For CSV entry, use <code>ROBOT_PROVIDER_LOCAL_CONFIG</code> and enter the Provider name.</p>
Compute Config: Provider	<p>Provider type used for topology computation. Choose a provider from the list.</p> <p>For CSV entry, use <code>ROBOT_PROVIDER_COMPUTE</code> and enter the Provider name.</p>

Example

Figure 13: Add New Device Window

The screenshot shows a web-based form titled "Add New Device" with a close button (X) in the top right corner. The form is organized into several sections, each with a dropdown arrow on the left:

- General:** Contains fields for Configured State (dropdown), Reachability Check (dropdown), Credential Profile (dropdown), Host Name, Inventory ID, Software Type, Software Version, UUID, Serial Number, Mac Address, Capability (dropdown), Tags (dropdown), and Product Type.
- Connectivity Details:** Includes a table for network connections with columns for Protocol (dropdown), IP Address / Subnet Mask, Port, and Timeout. There is an "+ Add Another" link and a trash icon.
- Routing Info:** Features IS-IS System ID, OSPF Router ID, and TE Router ID fields.
- Streaming Telemetry config:** Includes Vrf and Source Interface (with a dropdown menu showing "Loopback") fields.
- Location:** Contains fields for Building, Street, City, State, Country, Region, Zip, Latitude, Longitude, and Altitude.
- Providers and Access:** Includes Local Config (dropdown), Provider (dropdown), Device Key, Compute Config (dropdown), and Provider (dropdown) fields.

At the bottom right of the form, there are "Save" and "Cancel" buttons.

Get Network Device Details

Whenever you select **Device Management > Devices** and display the list of devices under the **Network Devices** tab, you can click  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 14: Details for DeviceName Window

Details for 1bce17d4-5219-4057-800a-57142388000a ✕

▼ Connectivity Details

Protocol	IP Address/Port	Timeout
<input checked="" type="checkbox"/> SSH	10.10.10.10:22	60
<input checked="" type="checkbox"/> TELNET	10.10.10.10:23	60
<input checked="" type="checkbox"/> SNMP	10.10.10.10:161	60
<input checked="" type="checkbox"/> NETCONF	10.10.10.10:830	60

▼ Identifiers

Key Type
Inventory ID
Host Name spnac-a9k-s105
UUID 1bce17d4-5219-4057-800a-57142388000a
Node IP 10.10.10.10
Serial # 256E
Mac Address 0050

▼ Hardware/Software

Product Type CISCO-XRv9000
Product Family Cisco XRv9K
Product Series Cisco XRV9000 Series Virtual Routers
Manufacturer Cisco Systems Inc.
Software Type IOS XR
Software Version 6.6.3
Capability YANG_MDT;SNMP;YANG_CLI

▼ Routing Info

ISIS System ID
OSPF Router ID
TE Router ID 10.10.10.10

▼ Streaming Telemetry config

Telemetry Interface default
Source VRF

▼ Location

Civic Address
Latitude 41.9
Longitude 12.4
Altitude

▼ Providers and Access

Local Config

Device Key cw-
Provider Name nso7
Credential Profile nso-creds

Compute Config

Provider Name
Credential Profile

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 (for help with the icons shown in this area, see [Device and Link Icons, on page 68](#)).

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

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.

For help with tagging your devices, see [Apply or Remove Device Tags, on page 191](#). For help with creating and deleting tags, see [Manage Tags, on page 188](#).

To filter devices by tags:

-
- Step 1** Display the **Network Devices** tab or the **Network Topology** map:
 - a) Display the **Network Devices** tab by choosing **Device Management > Devices**.
 - b) Display the topology map by choosing **Network Visualization > View Topology**.
 - 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.
-

Edit Network 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 (see [Export Network Devices, on page 103](#)).

-
- Step 1** From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.
 - Step 2** (Optional) Filter the list of devices by filtering specific columns.
 - Step 3** Check the check box of the device you want to change, then click
 - Step 4** Edit the values configured for the device, as needed. For a description of the fields you can update, see [Add Network Devices Through the UI](#).

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 filled in.)

Step 6 Resolve any errors and confirm device reachability.

Delete Network Devices

Complete the following procedure to delete devices.

Before you begin

- If the auto-onboard **managed** or **unmanaged** options are set for an SR-PCE provider, you should set auto-onboard for the SR-PCE(s) to **off**.
- Confirm that the device is not connected to the network or that it is powered off before deleting the device.



Note

- 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 set to **off**, and it is still functional and connected to the network, the device will be rediscovered as unmanaged as soon as it is deleted.

- Step 1** Export a backup CSV file containing the devices you plan to delete (see [Export Network Devices, on page 103](#)).
- Step 2** From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.
- 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 to edit the devices, as follows:
- Change each device's state to **DOWN** or **UNMANAGED**.
- If you want to delete devices in bulk, Cisco recommends that you change the device state in this manner in batches of 50 devices, then complete deletion of these devices before deleting another batch.
- Delete any KPIs currently running on the devices.
 - Abort any Playbooks running on or scheduled to run on the devices.
- Step 6** Click .
- Step 7** In the confirmation dialog box, click **Delete**.
- Step 8** After deleting a device from the user interface, delete any telemetry configuration objects on the router that match the regex pattern `*CW_*.*`. For example: You would find and delete router config objects like the three shown below:

```
!
destination-group CW_df5068767b68f9f0d9649cb32aca0cde917e5694
  address-family ipv4 172.16.2.31 port 31500
  encoding self-describing-gpb
  protocol tcp
!
!
sensor-group CW_df5068767b68f9f0d9649cb32aca0cde917e5694
  sensor-path Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/summary
```

```
!  
subscription CW_df5068767b68f9f0d9649cb32aca0cde917e5694  
  sensor-group-id CW_df5068767b68f9f0d9649cb32aca0cde917e5694 sample-interval 120000  
  destination-id CW_df5068767b68f9f0d9649cb32aca0cde917e5694  
!  
!
```

Export Network Devices

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.



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

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

View Device Job History

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

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

Figure 15: Job History Window With Error Details Popup

Inventory Jobs Total 48 ⌂ ⚙

Clear Filter ▼

Start Time	End Time	Status	Transaction ID	Description	User Name
Thu Jul 11 2019 00:29:45	Thu Jul 11 2019 00:29:45	✔ Completed	2df5abfb-a773-44cf-90eb-bb3...	Update 1 Provider(s)	admin
Thu Jul 11 2019 00:29:37	Thu Jul 11 2019 00:29:37	✔ Completed	a48fc525-294f-401c-931f-6ec...	Insert 1 Credential(s)	admin
Thu Jul 11 2019 00:29:06	Thu Jul 11 2019 00:29:06	✔ Completed	b2f90c2-ada7-449b-9e1c-34b...	Insert 1 Provider(s)	admin
Wed Jul 10 2019 23:54:27	Wed Jul 10 2019 23:54:27	✘ Failed ⓘ	f9bbc535-109e-4621-a1c5-c6...	Delete 7 Tag(s)	admin
Wed Jul 10 2019 23:51:51	Wed Jul 10 2019 23:51:51	✔ Completed	b6362a8a-7ff9-4d9d-9c6d-d1...	Insert 1 Tag(s)	admin
Wed Jul 10 2019 23:30:25	Wed Jul 10 2019 23:30:25	✔ Completed	b34cb396-9077-4561-a294-e...	Update 8 Node(s) Via CS...	admin
Wed Jul 10 2019 23:28:32	Wed Jul 10 2019 23:28:32	✔ Completed	2823a33e-8ce1-499d-89f1-9c...	Update 1 Node(s)	admin
Wed Jul 10 2019 23:28:32	Wed Jul 10 2019 23:28:32	✔ Completed	662ffc8c-4992-4778-a7ba-22b...	Unassign Tags	admin
Wed Jul 10 2019 23:28:26	Wed Jul 10 2019 23:28:26	✔ Completed	180a0b48-cacc-48e2-913c-5a...	Update 1 Node(s)	admin
Wed Jul 10 2019 23:22:45	Wed Jul 10 2019 23:22:45	✘ Failed ⓘ	45540994-f6f9-4a8e-953f-4d...	Insert 2 Provider(s) Via C...	admin
Wed Jul 10 2019 23:14:18	Wed Jul 10 2019 23:14:18	✘ Failed ⓘ			
Wed Jul 10 2019 23:14:10	Wed Jul 10 2019 23:14:10	✔ Completed			

Error Details

[ErrCannotDeleteProvider]: Provider xtc-CE2 is in use and cannot be deleted.

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. You can toggle between ascending and descending sort order (for more help, see [Set, Sort and Filter Table Data, on page 6](#)).

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

Error information may include `clean-up failure` events as audit messages. These messages indicate that Cisco Crosswork Network Automation configuration objects on the device could not be removed, and will explain why they could not be removed. Users will need to take manual action to remove them. This typically involves deleting any XR telemetry configuration objects with names starting with `CW_`.

Manage Devices Using Zero Touch Provisioning

Introduction

The Crosswork Zero Touch Provisioning (ZTP) application allows users to quickly and easily bring up devices using a Cisco-certified software image and a day-zero software configuration of the customer's choice. Once provisioned in this way, the new device is onboarded to the Crosswork device inventory (and, if it is configured as a Crosswork Provider, to Cisco NSO), where it can be monitored and managed like other devices.

Crosswork ZTP can connect devices to the network either out-of-band, via the management network (if your organization has established one), or in-band, over the data network. The file integrity of software images is validated before upload to Crosswork using the Cisco-supplied MD5 checksum for each image file. Both image and configuration files are stored in the Crosswork inventory, as part of the ZTP controller service, which is accessible via API. ZTP uses the secure iPXE remote boot capability, and your organization's DHCP server, to download files to each device and install or execute them.

Crosswork ZTP is especially useful when factory-reset devices have been shipped to a branch office or other remote site and then cabled to the network, with no image or configuration. Using the ZTP application, a network administrator can establish an entry for the device with a corresponding image and configuration,

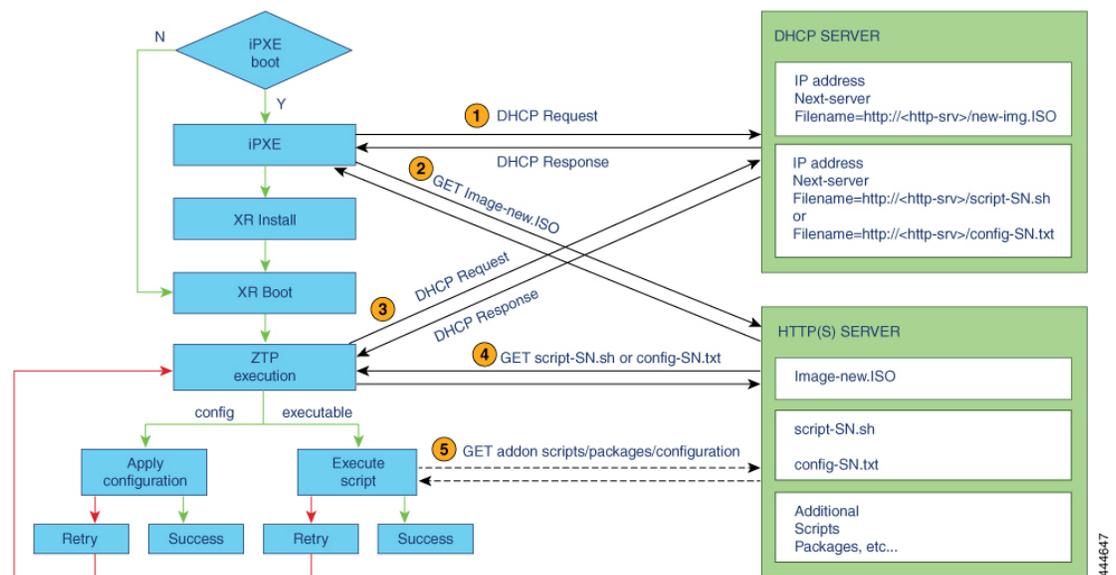
and both provision and onboard the device. The only intervention needed at the device is to press the reset button on the device chassis.

Crosswork ZTP is also useful for devices that are already in production. Users can trigger a CLI reboot of the already-imaged device, and then reload or replace the current software image, apply a Software Maintenance Update (SMU), run a day-one or later configuration script, or execute arbitrary CLI, shell or Python scripts on the device as needed.

Crosswork ZTP is fully integrated with Cisco Smart Licensing. Once provisioned and onboarded, each ZTP device's "Provisioned" status registers and activates a single Smart License for that device, based on its serial number. The license and the device are thereafter counted and tracked. Re-provisioning or configuring for the same device does not consume an additional license (see [Evaluation Licenses and ZTP](#), on page 106).

ZTP Process Logic

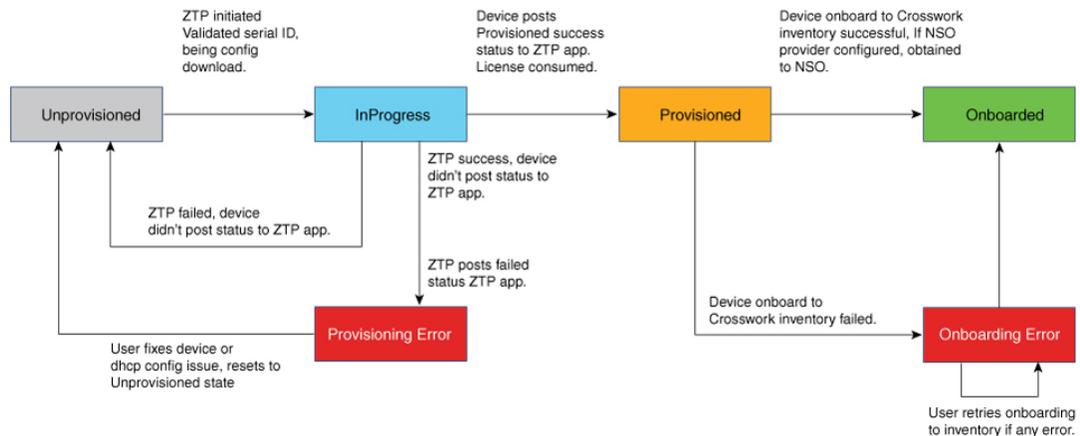
The illustration below shows the process logic that ZTP uses to provision and onboard devices.



ZTP Device State Transitions

Once initiated by a factory reset or CLI reload, the ZTP process proceeds automatically, and updates the Zero Touch Devices window with status messages indicating which stage of the process the device has reached. The figure below shows the state changes as the process proceeds. ZTP device entries start out in the **Unprovisioned** state and, after ZTP is initiated, transition to the **Provisioned** state, where they are connected to the network. If the provisioning is successful, the device will transition to the **Onboarded** state, where it becomes part of the Crosswork inventory and can be monitored and managed like any other Crosswork network device.

The ZTP process is considered successful when the ZTP device loads all of its code successfully ("code" meaning both the image plus configuration files, or the configuration file alone), establishes connectivity with Crosswork, and updates its **Status to Provisioned**. Achieving this state causes one license to be counted for that specific device's serial number. Because the license is based on the device serial number, later transition to the **Onboarded** state, or any further ZTP re-provisioning, re-imaging, or re-configuration, does not affect the license count.



Evaluation Licenses and ZTP

All licenses start with an evaluation period, typically 90 days. When the evaluation period expires, Crosswork will display a banner, warning users that evaluation licenses have expired. While this banner is displayed, some ZTP operations (such as configuration downloads) will be blocked. Users will need to purchase a valid license with an entitlement for the number of ZTP devices to be provisioned and onboarded to resume using blocked functions. The ZTP server treats licenses in a non-restrictive manner, in the sense that, even if all of the valid licenses are consumed, most ZTP functions will continue to work, but the warning banner will be displayed.

ZTP Supported Platforms

Crosswork Zero Touch Provisioning supports the following platforms:

- **Software:** Cisco IOS-XR versions 6.6.3, 7.0.1, 7.0.2, and 7.0.12.
- **Hardware:** Cisco Network Convergence Systems (NCS) 5500 Series Routers, NCS 540 Series Routers, NCS 560 Series Routers, NCS 1000-1004 Series Routers, Cisco Aggregation Services (ASR) 9000 Series Routers, and Cisco 8000 and 8800 Series Routers.



Note Customers using the following Cisco IOS-XR versions, please contact Cisco Customer Experience (CX) to source SMUs/ISOs for the following caveats:

- IOS-XR 7.0.1: [CSCvs98093](#)
- IOS-XR 7.0.2: [CSCvt30758](#)

ZTP Prerequisites

In addition to the other requirements mentioned in this section, using Crosswork ZTP to provision and onboard devices means your Crosswork installation must meet the following requirements:

- Ensure that Crosswork and your IOS XR devices are deployed in a secure network domain.

- Configure your organization's DHCP server to enable ZTP image and configuration file downloads. See [DHCP Setup for Crosswork ZTP, on page 128](#).
- The Crosswork server must be reachable from the devices, via an out-of-band management or in-band data network. See the network diagram in the "Network Requirements" topic in the *Cisco Crosswork Change Automation and Health Insights Installation Guide*.
- The Credential Profiles you plan to use to manage the ZTP devices once they have been onboarded must already exist in Crosswork. See [Manage Credential Profiles, on page 81](#).
- If you want Crosswork ZTP to onboard your devices to Cisco NSO, NSO must already be configured as a Crosswork Provider. See [Manage Providers, on page 170](#) and [Sample Configuration for Devices in Cisco NSO, on page 93](#).

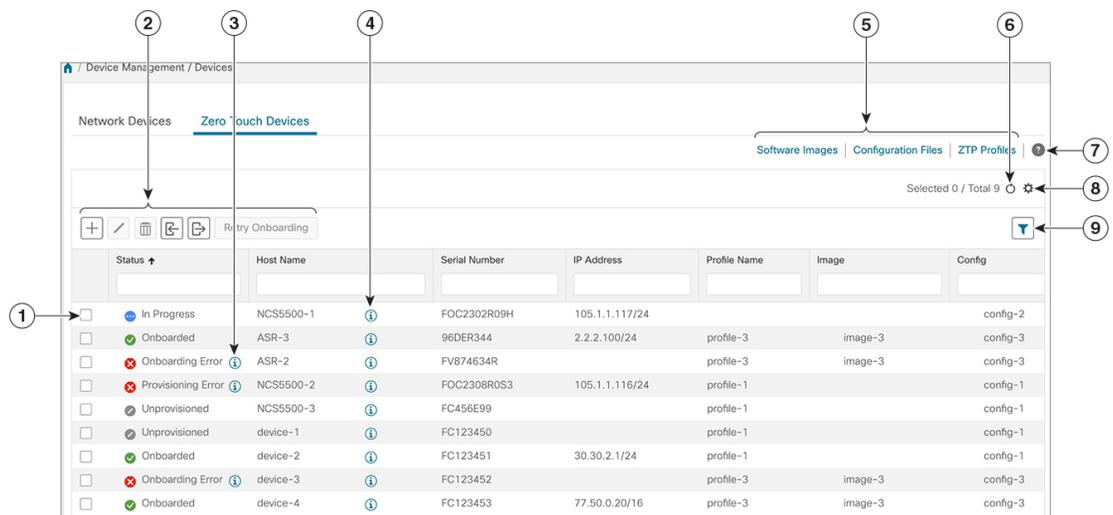
Use the Zero Touch Devices Window to Work with Devices

The **Zero Touch Devices** window (shown below) gives you a list of all of the ZTP device entries you have created and enables you to add, import, edit, and delete them. Once ZTP processing is initiated, you can use the window's **Status** column to monitor each device's progress from the initial **Unprovisioned** state to the **Provisioned** and final **Onboarded** states (see [ZTP Device State Transitions, on page 105](#)). You can also get a summary view of current ZTP device status by viewing the **Zero Touch Provisioning** dashboard on the Crosswork Home page (see [Use the Zero Touch Provisioning Tile to Monitor Progress, on page 109](#)).

The same **Status** column notifies you when a **Provisioning Error** or **Onboarding Error** occurs for a device during ZTP processing. If errors are detected, you can use this window to view possible causes of an onboarding error, edit the device's **Status** back to **Unprovisioned**, and then either **Retry Onboarding** (in the case of an onboarding error) or trigger ZTP processing again (in the case of a provisioning error).

Once ZTP devices are successfully onboarded, you can manage and monitor them using the **Network Devices** tab.

To view the **Zero Touch Devices** window, select **Device Management > Devices > Zero Touch Devices**.



Item	Description
1	Text and icons in the Status column show the current provisioning status of each ZTP device.

Item	Description
2	<p>Click  to add a new ZTP device to the ZTP repository. See Create ZTP Device Entries Using the UI, on page 122.</p> <p>Click  to edit the information for the currently selected ZTP device entry, including the device Status. See Edit ZTP Devices, on page 127.</p> <p>For devices with an error Status, such as Onboarding Error or Provisioning Error, you must always use the  to reset the device's Status to Unprovisioned before attempting to retry onboarding.</p> <p>Click  to delete the currently selected ZTP device entry. See Delete ZTP Devices, on page 128. Note that deleting a device that has successfully completed ZTP processing has no impact on the number of ZTP licenses that have been used.</p> <p>Click  to import new ZTP device entries 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. See Create ZTP Device Entries Using Import, on page 125 and Prepare ZTP Device Import Files, on page 126.</p> <p>Click  to export information for selected ZTP devices to a CSV file. See Export Devices.</p> <p>Click Retry Onboarding to attempt to onboard a selected ZTP device entry when a previous onboarding attempt failed. You must first select the device entry you want to retry. You cannot retry more than one device entry at a time.</p> <p>Before before attempting to retry onboarding for a device, you must use the  to reset the device's Status to Unprovisioned.</p> <p>You will want to review the error popup and log files, determine why the ZTP onboarding process failed (for example: bad IP address) and, where needed, update the device entry's image or configuration, or update the corresponding DHCP device entry (see DHCP Setup for Crosswork ZTP, on page 128).</p>
3	Click  in the Status column for information on the cause of any detected provisioning or onboarding errors. See Troubleshoot ZTP Issues, on page 145 .
4	Click  in the Host column for details about the host.
5	Click these links to bypass the Crosswork main menu and navigate directly to the Software Image , Configurations or ZTP Profiles window.
6	Click  to refresh the Zero Touch Devices window.
7	Click  to display the Zero Touch Provisioning Steps page. It will remind you of the ZTP process workflow steps, and help you navigate to the parts of the ZTP user interface that will enable you to complete each step. See Workflow: Zero Touch Provisioning, on page 110 .
8	Click  to select which columns to display in the Zero Touch Devices window. See Set, Sort and Filter Table Data, on page 6 .

Item	Description
9	Click  to set filter criteria on one or more columns in the Zero Touch Devices window. See Set, Sort and Filter Table Data, on page 6 .
	Click the Clear Filter link to clear any filter criteria you may have set.

Use the Zero Touch Provisioning Tile to Monitor Progress

The **Zero Touch Provisioning** tile (shown below) lets you see a summary view of your current ZTP processing status. It provides a count for all the devices, images, configuration files and profiles currently in use, as well as the number of devices in each of the possible ZTP states (see [ZTP Device State Transitions, on page 105](#)).

Until you begin using ZTP device management, the tile will have counts of zero for all of these indicators. The counts will change as you work with the application. Clicking on the **View ZTP devices** link at the bottom of the tile will navigate directly to the **Zero Touch Devices** window, where you can begin creating ZTP device entries and ZTP profiles by uploading the associated software image and configuration files (see [Use the Zero Touch Devices Window to Work with Devices, on page 107](#)).

To view the **Zero Touch Provisioning** tile, click the **Home** icon on the main menu.



Zero Touch Provisioning Concepts

Crosswork Zero Touch Provisioning (ZTP) makes use of the following basic terminology and concepts:

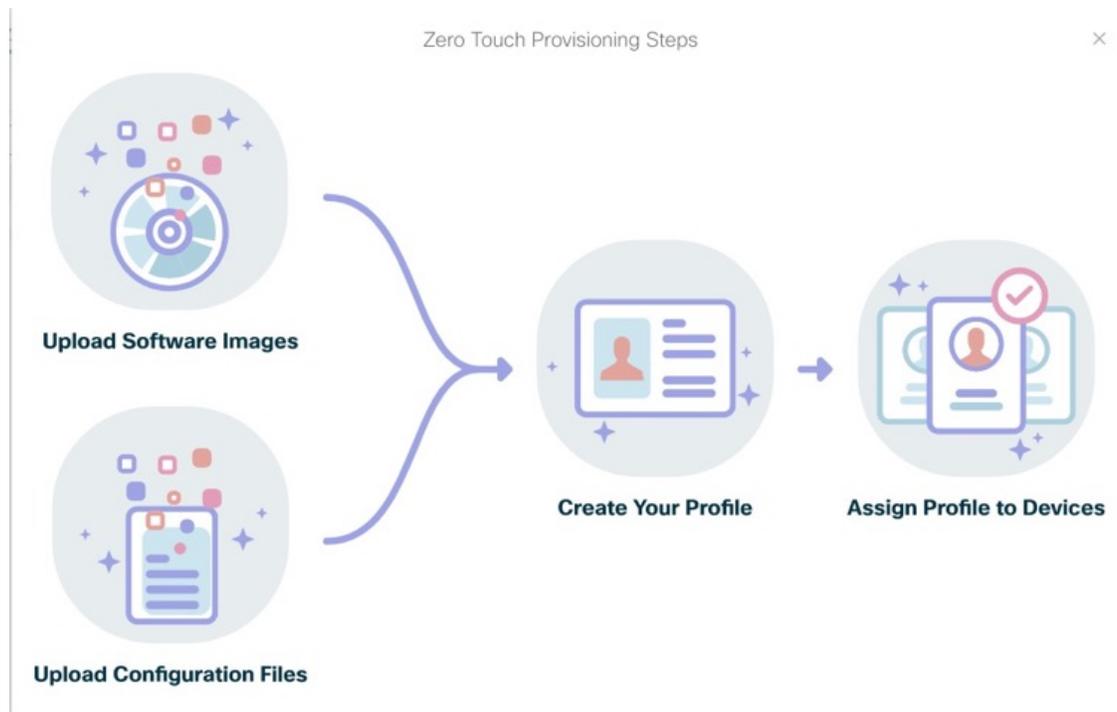
- **Image file:** A binary Cisco IOS-XR software image or Software Maintenance Update (SMU) file, used to install or maintain an installation of the Cisco Internet Operating System on a network device. The Crosswork ZTP process on the device downloads the image from Crosswork and installs the images using the [open-source boot firmware iPXE](#). If any SMU maintenance patches need to be deployed, they can be done via user script after image download via ZTP processing.
- **Configuration file:** A file used to set the operating parameters of the newly imaged or re-imaged device. This can be a Python script, Linux shell script, or a sequence of Cisco IOS CLI commands stored as an ASCII text file. The Crosswork ZTP process downloads the configuration file to the newly imaged device, which then executes it.
- **ZTP profile:** A Crosswork storage construct that combines (normally) one image and one configuration into a single unit. Crosswork uses ZTP profiles to automate imaging and configuration processes. While

optional, creating ZTP profiles is recommended as the best way to combine a single image file and configuration file based on a product or device family, such as the Cisco ASR 9000 or Cisco NCS5500. It will also help you to configure your organization's DHCP server based on device family class, and use a single set of image/configuration files for devices in that class.

- **ZTP repository:** The location where Crosswork stores ZTP image and configuration files.
- **File path:** The explicit path to a stored image, SMU, or configuration file in the ZTP repository. Better known as the bootfile name, the file path is used in DHCP (option 67 for v4) configuration and represented as an HTTP/HTTPS URL image or configuration file path in the repository. File paths must be specified when you update DHCP for your ZTP devices. You can easily copy this URL from the ZTP repository and update it in the DHCP server configuration file (see [Copy Configuration File Paths and UUIDs, on page 119](#) and [Copy Image File Paths and UUIDs, on page 114](#)).
- **UUID:** The Universal Unique Identifier (UUID) uniquely identifies an image or configuration file uploaded to Crosswork. In the DHCP bootfile URL, for any change in the configuration or image file used for ZTP, it is sufficient to copy and then update the corresponding UUID in the URL.

Workflow: Zero Touch Provisioning

For a reminder of the main steps in using Zero Touch Provisioning (ZTP) to provision and onboard your network devices, click  on any window in the ZTP application. The popup **Zero Touch Provisioning Steps** page shown below displays icons representing each major step in the process. Click on one of the icons to navigate directly to the part of the Crosswork ZTP user interface that allows you to perform that step.



The following table provides links to more detailed information on how to perform each step in the process

Step	For details, see...
1. Download from Cisco and then upload to the ZTP repository the IOS-XR device image files you want to use to image your ZTP devices.	Upload Software Image Files, on page 112
2. Create and then upload to the ZTP repository the day-zero (or later) configuration files you want to use to configure your devices.	Upload Configuration Files, on page 114 Prepare Your Custom Day-Zero Configuration Files, on page 115 Use Custom Day-Zero Configuration Files, on page 117
3. (Optional) Create one or more ZTP profiles to image and/or configure your devices. Note that specifying an image file in a ZTP profile is optional. You can also image or configure a device without a ZTP profile, by specifying the image and/or configuration file when you create the ZTP device entry.	Create Zero Touch Profiles, on page 120
4. Create ZTP device entries to be provisioned and onboarded by ZTP processing. You can specify the device image and/or configuration file to be used in ZTP processing either in the ZTP device entry itself, or by specifying a ZTP profile (if you have created one).	Create ZTP Device Entries, on page 122
5. Modify your organization's DHCP configuration, so that DHCP can properly respond to each device's request for an image and/or configuration download.	DHCP Setup for Crosswork ZTP, on page 128
6. Initiate the ZTP process, which will then provision and onboard ZTP devices. You can trigger Crosswork ZTP processing by rebooting the device.	<p>You can do this either by:</p> <ul style="list-style-type: none"> • If you have physical access to the device: Press the reset button on the device chassis. • If the device has been imaged: Connect to the device via the console, enter exec mode, and issue a <code>ztp initiate</code> command. The command will try to initiate on the management port first, then try other available ports. <p>For details and options for the <code>ztp initiate</code> command, see the examples at this link.</p>
7. Troubleshoot provisioning and onboarding issues as needed	Troubleshoot ZTP Issues, on page 145

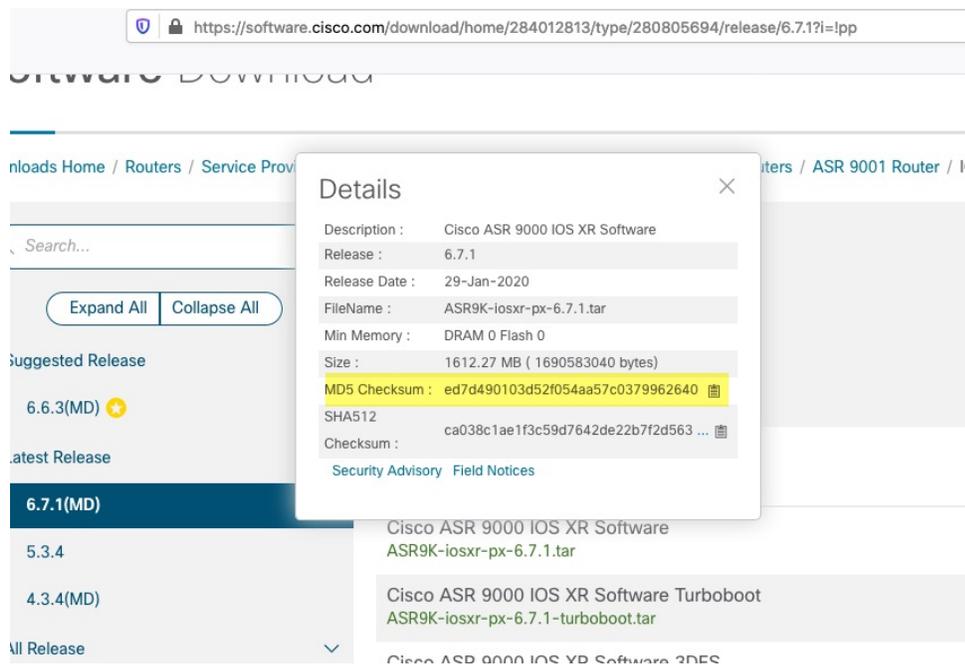
Upload Software Image Files

The ZTP repository is intended for initial onboarding of devices. You can upload as many images as you want, up to the maximum image-file storage limit of 20GB. As image files tend to be large, Cisco recommends that you restrict uploads to only those images needed for day-zero imaging.

Before you begin

Be sure to:

- Download the image files you plan to add to the ZTP repository. Licensed software images and SMU files are always available for download from the [Cisco Software Download site](#). Only image files with the filename extensions `iso`, `tar` or `rpm` can be uploaded to the ZTP repository. See [ZTP Supported Platforms, on page 106](#).
- Copy to your clipboard or record the MD5 checksum used to verify the integrity of each image file. The MD5 checksum for each image file is available on the **Details** popup window for the Cisco Software Download page from which you downloaded that file. You can quickly copy the checksum to your clipboard by clicking the clipboard icon shown on the same line as the MD5 checksum itself (highlighted in the example popup shown below).



- Step 1** From the main menu, choose **Device Management** > **Software Images**. Crosswork displays the **Image Repository** list.
- Step 2** Click . Crosswork displays the **Add Image** page.
- Step 3** Enter the values for the new file upload as shown in the table below.

Table 11: Add Image Fields (*=required)

Field	Description
Image Name *	The unique name you want to assign to the uploaded image file.
Image Type *	Select Image or SMU .
MD5 Checksum *	Enter the image's MD5 checksum.
OS Platform *	Select the IOS device software platform. Currently, the IOS-XR platform is supported.
OS Version *	Select the IOS software platform version for the image or SMU. Currently, versions 6.6.3 , 7.0.1 , 7.0.2 and 7.0.12 are supported.
Device Family *	Select the device family on which this software image or SMU will be applied (for example, CISCO ASR9000).
Software Image *	Click Browse to navigate to and select the image or SMU file to be uploaded.

- Step 4** When you have complete entries in all of the required fields, click **Add** to begin uploading the new file. Crosswork displays a progress bar during the upload. Once the upload is complete, Crosswork verifies the integrity of the image file using the MD5 checksum you entered. If these do not match, then either the checksum is incorrect or the file is corrupt. Crosswork will prompt you to either correct the checksum, or upload another version of the file.

Edit Image Files

Except for the software image file name itself, you can change any of the properties for an image you have added to the ZTP repository.

- Step 1** From the main menu, choose **Device Management > Software Images**. Crosswork displays the **Image Repository** list.
- Step 2** In the **Image Repository** list, click the selection box next to the image file whose properties you want to edit.
- Step 3** Click . Crosswork displays the **Edit Image** page.
- Step 4** Change the values in the fields as needed.
- Step 5** When you have completed your changes, click **Update** to save them.

Delete Image Files

Deleting an image associated with a ZTP profile will render that profile non-functional. A mistaken deletion cannot be undone, but the image can be uploaded again and re-associated with the ZTP profile.

As software image files tend to be very large, Cisco recommends that you restrict your ZTP repository to only those images needed for Day Zero and Day One configurations.

Before you begin

There are no checks to prevent deletion of an active image file. Be sure that any image you plan to delete from the ZTP repository is not already associated with ZTP device entries or ZTP profiles. You can check if an image file is associated with an individual ZTP device entry by checking your device entries listed on the **Zero Touch Devices** window (see [Use the Zero Touch Devices Window to Work with Devices, on page 107](#)). You can check if an image file is associated with a ZTP profile by selecting the **View Details** option for the ZTP profile with which you think it may be associated (see [View Zero Touch Profile Details, on page 122](#)).

-
- Step 1** From the main menu, choose **Device Management > Software Images**. Crosswork displays the **Image Repository** list.
- Step 2** In the **Image Repository** list, click the selection box next to the image you want to delete.
- Step 3** Click .
- Crosswork prompts you to verify that the image file is not already associated with a ZTP profile.
- Step 4** Click **Delete** to delete the image file.
-

Copy Image File Paths and UUIDs

When added to Crosswork, every image or SMU file is assigned a unique UUID and stored in the Crosswork repository. You will need to specify the unique repository file path and UUID for each device when modifying your DHCP server configuration file to permit provisioning (see [DHCP Setup for Crosswork ZTP, on page 128](#)). You can quickly copy to your clipboard the complete file path and UUID for any image or SMU file, directly from the **Software Images** list. You can also copy just the image file's UUID.

-
- Step 1** From the main menu, choose **Device Management > Software Images**. Crosswork displays the **Image Repository** list.
- Step 2** If you want to copy:
- The image's full path and UUID: Click  in the **Image/SMU Name** column.
 - The image's UUID only: Click  in the **Image UUID** column.

Crosswork copies the file path 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, be sure to replace the *IP* variable with the IP address and port of your Crosswork server.

Upload Configuration Files

You can add a maximum of 5GB of configuration files to the ZTP repository. No single configuration file can exceed 2MB in size.

Before you begin

Be sure you have prepared one or more configuration or script files to add to the ZTP repository. Only IOS-XR CLI text configuration (`.txt`), Linux shell (`.sh`) or Python script (`.py`) files, with the appropriate filename extensions, can be added.

For guidance on creating and running custom configuration files using Crosswork ZTP, see [Prepare Your Custom Day-Zero Configuration Files, on page 115](#) and [Use Custom Day-Zero Configuration Files, on page 117](#).

Step 1 From the main menu, choose **Device Management > Configuration Files**. Crosswork displays the **Configurations** window.

Step 2 Click . Crosswork displays the **Add Configuration** page.

Step 3 Enter the values for the new configuration file upload as shown in the table below.

Table 12: Add Configuration Fields (=required)*

Field	Description
Configuration Name *	The unique name you want to assign to the uploaded configuration file. This is the name that distinguishes it from all other configuration files in the repository, and is the name that will appear on the Configuration Files list.
OS Platform *	Select the IOS device software platform appropriate for this configuration. Currently, the IOS-XR platform is supported.
OS Version *	Select the IOS software platform version appropriate for this configuration. Currently, versions 6.6.3 , 7.0.1 , 7.0.2 and 7.0.12 are supported.
Device Family *	Select the family of devices to which this configuration will be applied (for example, CISCO ASR9000).
Config/Script File *	Click Browse to navigate to and select the configuration or script file to be uploaded.

Step 4 When you have complete entries in all of the required fields, click **Add** to begin uploading the new configuration file. Crosswork displays the contents of the configuration file in a popup window. Verify that it is the file you want. You can scroll the popup window to verify the contents of the file.

Step 5 When you are ready, click **OK** to continue. Then click **Add** to upload the file.

Prepare Your Custom Day-Zero Configuration Files

Configuration files vary greatly in contents, depending on the needs of the organization using the device and the device capabilities. The following topics provide guidelines to follow when preparing day-zero configuration scripts for use with Crosswork ZTP

A Sample Basic Day-Zero Configuration Script

The generic shell script does most of the work of configuring your IOS-XR devices (see [Use Custom Day-Zero Configuration Files, on page 117](#)). Your custom day-zero configuration file can be as simple as the example shown below:

```
#!/ IOS XR Configuration 7.0.1
!! Last configuration change at Wed Mar 1 10:38:34 2019 by admin
!
hostname {$HOSTNAME}
username {$SSH_USERNAME}
```

```

group root-lr
group cisco-support
secret {$SSH_PASSWORD}
!
tpa
vrf default
!
!
call-home
service active
contact smart-licensing
profile CiscoTAC-1
active
destination transport-method http
!
!
interface MgmtEth0/RP0/CPU0/0
ipv4 address dhcp

```

This example makes use of several placeholders, such as *{\$HOSTNAME}*, for which the system will insert corresponding values at runtime. See the next section for guidelines on using these placeholders in your configuration file

ZTP Placeholders in Day-Zero Configuration Files

The following table lists the placeholders you can use in your custom day-zero configuration files. At runtime, for each of these placeholders, Crosswork will substitute the appropriate values for each device. For an example of the use of these placeholders, see the sample configuration script in the preceding topic.

Table 13: ZTP Placeholders in Configuration Files

This placeholder...	...is filled using the value from the...
<i>{\$HOSTNAME}</i>	Device's host name value as specified in the ZTP device entry.
<i>{\$IP_ADDRESS}</i>	Device's IP address value, as assigned by DHCP.
<i>{\$SSH_USERNAME}</i>	Credential Profile's User Name field (where the Connectivity Type is SSH).
<i>{\$SSH_PASSWORD}</i>	Credential Profile's Password field (where the Connectivity Type is SSH).
<i>{\$SSH_ENPASSWORD}</i>	Credential Profile's Enable Password field (where the Connectivity Type is SSH).
<i>{\$SNMP_READ_COM}</i>	Credential Profile's Read Community field (where the Connectivity Type is SNMPv2).
<i>{\$SNMP_WRITE_COM}</i>	Credential Profile's Write Community field (where the Connectivity Type is SNMPv2).
<i>{\$SNMP_SEC_LEVEL}</i>	Credential Profile's Security Level field (where the Connectivity Type is SNMPv3).
<i>{\$SNMP_USERNAME}</i>	Credential Profile's User Name field (where the Connectivity Type is either SNMPv2 or SNMPv3).
<i>{\$SNMP_AUTH_TYPE}</i>	Credential Profile's User Name field (where the Connectivity Type is SNMPv3 and Security Level is AUTH_NO_PRIV or AUTH_PRIV).

This placeholder...	...is filled using the value from the...
<code>{ \$SNMP_AUTH_PASS }</code>	Credential Profile's User Name field (where the Connectivity Type is SNMPv3 and Security Level is AUTH_NO_PRIV or AUTH_PRIV).
<code>{ \$SNMP_PRIV_TYPE }</code>	Credential Profile's User Name field (where the Connectivity Type is SNMPv3 and Security Level is AUTH_PRIV).
<code>{ \$SNMP_PRIV_PASS }</code>	Credential Profile's Priv Password field (where the Connectivity Type is SNMPv3 and Security Level is AUTH_PRIV).

Use Custom Day-Zero Configuration Files

You will be applying your day-zero configuration using a generic shell script that works with all of the supported routers and does most of the work of configuring them. The modified shell script will call your own custom configuration file.

Before you begin

Be sure you have prepared your own custom day-zero configuration file as explained in [Prepare Your Custom Day-Zero Configuration Files, on page 115](#). You will also need to add it to the Crosswork ZTP repository, as explained in [Upload Configuration Files, on page 114](#).

Once you have uploaded your own custom day-zero configuration file to Crosswork, copy or record its UUID, as explained in [Copy Configuration File Paths and UUIDs, on page 119](#). You will need it when you modify the generic shell script.

-
- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Configuration Files** list.
- Step 2** Click **Download Sample Script**. Your browser will prompt you to save the generic script file on your local file system. Give the file a unique name and change the filename extension to **.sh**, to indicate that it is a Linux shell script.
- Step 3** Open the saved shell script with the editor of your choice.
- Step 4** In the saved shell script, locate and modify the values assigned to the following variables, as follows:
- **XRZTP_INTERFACE_NAME**: The interface on the device where the ZTP process will be initiated. For example: **MgmtEth0/RP0/CPU0/0**.
 - **CW_HOST_IP**: The IP address of the Crosswork server. For example: **192.168.1.1**.
 - **CW_PORT**: The Crosswork server port number on which to initiate download of your own custom configuration file. Use **30604** if this will be an HTTP download, or **30603** for an HTTPS download.
 - **CW_CONFIG_UUID**: The UUID of your own custom day-zero configuration file, previously uploaded to the Crosswork repository. For example: **30d2d77c-462a-4b4d-8960-fd94436cc0f9**.
- Step 5** (Optional) If you will be using the script to configure Cisco ASR 9000 devices: The generic script, as written, will work with all the supported device families except ASR 9000. The script contains commands that will make it work with ASR 9000, but these have been commented out. To make it work with ASR 9000, un-comment the ASR 9000 command sections and comment out the sections for other devices. These sections are clearly documented in the script.
- Step 6** Save the modified shell script.
- Step 7** Upload the modified shell script to the ZTP repository, as explained in [Upload Configuration Files, on page 114](#).

- Step 8** Create or modify ZTP device entries, or create ZTP profiles, with **Configuration** settings that point to the UUID of the modified shell script. For help with these tasks, see the topics under [Create ZTP Device Entries, on page 122](#) and [Create Zero Touch Profiles, on page 120](#).
-

Edit Configuration Files

You can change any of the stored field values for a configuration file you have uploaded to the ZTP repository. For a list of the field values you can change, see the "Add Configuration Fields" table in [Upload Configuration Files, on page 114](#).

If you change the value in the **Config/Script File** field during an edit session, you will trigger a configuration file upload to the repository, just as you do when uploading configuration files (see [Upload Configuration Files, on page 114](#)). Note that you will need to browse to and select the new configuration or script file to change the value in **Config/Script File**.

Except for uploads triggered by changes in **Config/Script File**, changing the value in these fields does not change the configuration file itself. In order to update a configuration file's contents:

1. Download the existing file, as explained in [Download Configuration Files, on page 118](#).
 2. Make your changes to the file, using your choice of editor.
 3. Upload the changed configuration file to the ZTP repository, as explained in [Upload Configuration Files, on page 114](#).
-

- Step 1** From the main menu, choose **Device Management > Configuration Files**. Crosswork displays the **Configurations** window.
- Step 2** In the **Configurations** list, click the selection box next to the configuration file you want to edit.
- Step 3** Click . Crosswork displays the **Edit Configuration** page.
- Step 4** Change the values in the fields as needed.
- Step 5** When you have completed your changes, click **Update** to save them.
-

Download Configuration Files

You can download any configuration file previously added to the ZTP repository. This is handy when you want to make changes in an existing file, or create a new configuration using an existing one as a template.

- Step 1** From the main menu, choose **Device Management > Configuration Files**. Crosswork displays the **Configurations** window.
- Step 2** In the **Configuration Files** list, in the **Configuration Name** column next to the configuration file you want to download, click [↓](#).
- Crosswork displays the file download window for your client OS. Change the file name as needed, navigate to the folder where you want to store it, and confirm that you want to save the file.
-

Delete Configuration Files

Follow the steps below to delete a configuration file.

Before you begin

Be sure that any configuration file you plan to delete from the ZTP repository is not already associated with ZTP device entries or ZTP profiles. You can check if a configuration file is associated with an individual ZTP device entry by checking your device entries listed on the **Zero Touch Devices** window (see [Use the Zero Touch Devices Window to Work with Devices, on page 107](#)). You can check if a configuration file is associated with a ZTP profile by selecting the **View Details** option for the ZTP profile with which you think it may be associated (see [View Zero Touch Profile Details, on page 122](#)).

Deleting a configuration file associated with a ZTP profile will render that profile non-functional. A mistaken deletion cannot be undone, but the configuration file can be uploaded again and re-associated with the ZTP profile.

-
- Step 1** From the main menu, choose **Device Management > Configuration Files**. Crosswork displays the **Configurations** window.
- Step 2** In the **Configurations** list, click the selection box next to the configuration file you want to delete.
- Step 3** Click .
- Crosswork prompts you to check that the file is not already associated with a device entry or ZTP profile.
- Step 4** Click **Delete** to delete the file.
-

Copy Configuration File Paths and UUIDs

When added to Crosswork, every configuration file is assigned a unique UUID and stored in the Crosswork ZTP repository. You will need to specify the unique repository file path and UUID for each device when modifying your DHCP server configuration file to permit provisioning (see [DHCP Setup for Crosswork ZTP, on page 128](#)). You can quickly copy to your clipboard the complete file path and UUID for any configuration file, directly from the **Configurations** list. You can also copy just the configuration file's UUID.

-
- Step 1** From the main menu, choose **Device Management > Configuration Files**. Crosswork displays the **Configurations** window.
- Step 2** If you want to copy:
- The configuration file's full path and UUID: Click  in the **Configuration Name** column.
 - The configuration file's UUID only: Click  in the **Config UUID** column.

Crosswork copies the file path 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, be sure to replace the `CCW_HOST_IP` variable with the IP address and port of your Crosswork server.

Create Zero Touch Profiles

You can create as many ZTP profiles as you like. However, Cisco recommends that you create one and only one day-zero ZTP profile per specific device group or device family. Each ZTP profile can have just one image file and one configuration file associated with it.

An image file is not required in every ZTP profile. You can create ZTP profiles that specify a configuration only. You can also associate image or configuration files directly with a device entry, without using a ZTP profile, by selecting a previously added image or configuration file from the dropdown menu in the ZTP device entry's **Software Image** and **Configuration File** fields (see [Create ZTP Device Entries Using the UI, on page 122](#)) or entering the file names in those columns in the CSV file you use to import device entries (see [Create ZTP Device Entries Using Import, on page 125](#)).

Before you begin

Be sure you have added to the ZTP repository:

- All of the image files you plan to use in the ZTP profiles you create. For help with this task, see [Upload Software Image Files, on page 112](#).
- All of the configuration files you plan to use in the ZTP profiles you create. For help with this task, see [Upload Configuration Files, on page 114](#).

-
- Step 1** From the main menu, choose **Device Management > Zero Touch Profiles**. Crosswork displays the **ZTP profile Management** page.
- Step 2** Click + **New Profile**. Crosswork displays the **Add Profile** page, with tiles representing your ZTP profiles.
- Step 3** Enter the values for the new ZTP profile as shown in the table below.
- Step 4** When you have completed entries in all of the required fields, click **Save** to create the new ZTP profile. Crosswork displays the **ZTP Profile Management** page, with a new tile for the new profile.

Table 14: Add Profile Fields (*=required)

Field	Description
Profile Name *	The unique name you want to assign to this ZTP profile. This is the name as it will appear in the tile representing this ZTP profile on the ZTP Profile Management page, and when adding new ZTP devices.
Description	Enter a description of the ZTP profile. This description will appear in the tile representing this ZTP profile on the ZTP Profile Management page.
OS Platform *	Select the IOS software platform for the devices to which this ZTP profile will be applied. This should be the same platform as the image and configuration files the profile uses. Currently, the IOS-XR platform is supported.
OS Version *	Select the IOS software platform version for the devices to which this ZTP profile will be applied. This should be the same version as the image and configuration files the profile uses. Currently, IOS-XR versions 6.6.3 , 7.0.1 , 7.0.2 and 7.0.12 are supported.

Field	Description
Device Family *	Select the device family for the devices to which this ZTP profile will be applied. This should be the same device family as the image and configuration files the profile uses. The device family will appear in the tile representing this ZTP profile on the ZTP Profile Management page.
Software Image	Select from the dropdown menu the image file that this profile will apply to the devices. The file must already exist in the ZTP repository. See Upload Software Image Files, on page 112 . Note that an image file is optional for ZTP profiles; you may have profiles that only apply a configuration.
Configuration File *	Select from the dropdown menu the configuration file that this profile will apply to the devices. The file must already exist in the ZTP repository. See Upload Configuration Files, on page 114 .

Edit Zero Touch Profiles

Follow the steps below to edit the stored field values for a ZTP profile.

- Step 1** From the main menu, choose **Device Management > Zero Touch Profiles**. Crosswork displays the **ZTP Profile Management** page.
- A tile icon represents each of the existing ZTP profiles.
- Step 2** (Optional) To find a specific profile: Click in the **Search Profiles** box and begin typing. The **ZTP Profile Management** page displays only the profile tiles that match the text you entered.
- Step 3** In the top right corner of the tile for the ZTP profile you want to edit, click **...**.
- Step 4** From the drop down menu, select **Edit**. Crosswork displays the **Edit Profile** page.
- Step 5** Change the values in the fields as needed.
- Crosswork will verify that any changes you make to the **OS Platform**, **OS Version** or **Device Family** field values match the same values for the software image or configuration file you associated with the ZTP profile. You cannot change the **Profile Name**.
- Step 6** When you have completed your changes, click **Update** to save them.

Delete Zero Touch Profiles

You can delete any ZTP profile as long as it is not already associated with an unprovisioned ZTP device. Deleting a ZTP profile does not affect the configuration or image files associated with it.

You can check if a ZTP profile is associated with an individual ZTP device entry by checking your device entries listed on the **Zero Touch Devices** window (see [Use the Zero Touch Devices Window to Work with Devices, on page 107](#)).

-
- Step 1** From the main menu, choose **Device Management > Zero Touch Profiles**. Crosswork displays the **ZTP profile Management** page.
- A tile icon represents each of the existing ZTP profiles.
- Step 2** (Optional) To find a specific profile: Click in the **Search Profiles** box and begin typing. The **ZTP Profile Management** page displays only the profile tiles that match the text you entered.
- Step 3** In the top right corner of the tile for the ZTP profile you want to delete, click ***.
- Step 4** From the drop down menu, select **Delete**.
- Step 5** To confirm, click **Delete** again.
-

View Zero Touch Profile Details

You can view the stored field values for any ZTP profile without editing it. Profile details include the Profile Name, Description, Device Type, OS and OS Version, and the names of the associated image and configuration files.

-
- Step 1** From the main menu, choose **Device Management > Zero Touch Profiles**. Crosswork displays the **ZTP Profile Management** page.
- A tile icon represents each of the existing ZTP profiles.
- Step 2** (Optional) To find a specific profile: Click in the **Search Profiles** box and begin typing. The **ZTP Profile Management** page displays only the profile tiles that match the text you entered.
- Step 3** In the top right corner of the tile representing the ZTP profile you want to view, click ***.
- Step 4** From the drop down menu, select **View Details**.
- Crosswork displays a popup window listing all the ZTP profile details.
-

Create ZTP Device Entries

Before you can provision and onboard ZTP devices, you must first create ZTP device entries. Crosswork uses these entries to provision and onboard the actual devices once ZTP processing is initiated.

You can create ZTP device entries one at a time, using the Crosswork user interface, or in bulk by importing a CSV file.

The following topics discuss both methods, as well as how to properly prepare CSV files, and ways to edit, delete, and export backups of your ZTP entries.

Create ZTP Device Entries Using the UI

Follow the steps below to create ZTP device entries one by one, using the GUI. Under normal circumstances, you will want to use this method when adding a few devices only. For adding device entries in bulk, import them from a CSV file (see [Create ZTP Device Entries Using Import, on page 125](#)).

Newly added ZTP device entries always appear in the **Zero Touch Devices** tab with their **Status** set to **unprovisioned**. They will remain **unprovisioned** until you initiate ZTP processing.

Before you begin

Be sure you have:

- Completed the planning steps and setup requirements discussed in [Get Started](#).
- Added the software image files you want loaded onto your ZTP devices when ZTP processing is initiated, as explained in [Upload Software Image Files](#).
- Added the configuration files you want to use to provision or configure your ZTP devices when ZTP processing is initiated, as explained in [Upload Configuration Files, on page 114](#).

As a convenience for users who may be testing a ZTP profile for a new family of devices, Crosswork provides fields for associating image and configuration files directly with a ZTP device entry, instead of via a ZTP profile. Once you have tested these files and provision/onboarding is successful, Cisco recommends that you create the ZTP profiles you want to use to provision/onboard other instances of this device family, before adding the device entries for them. This can be especially helpful if you are planning to add ZTP devices via import.

- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Devices** list.
- Step 2** Click the **Zero Touch Devices** tab.
- Step 3** Click .
- Step 4** Enter values for the new ZTP device entry, as listed in the table below.
Once devices are onboarded, additional attributes may be displayed.
- Step 5** Click **Save**. The Save button is disabled until all required fields are complete.

Table 15: Add ZTP Device Fields (*=required)

Field	Description
Host Name *	The hostname of the device. Crosswork discovers it and updates it.
Serial Number *	Serial number for the device. ZTP uses the serial number as part of the device ID.
Profile	Choose whether you want to use a Zero Touch (ZT) profile to configure this device. Select No Profile if you have not yet created a ZTP profile for the new ZTP device. No Profile is the default. If you select Use Profile , you must select the ZTP profile in the next field.
Profile Name *	Select the ZTP profile you want to use to provision this device. Required only if you selected Use Profile in the Profile field
IP Address	The IP address of the device, obtained via script from your organizations DHCP server.

Field	Description
Status	Defaults to Unprovisioned during ZTP device entry creation. You cannot select a different status while adding an entry. The Status updates automatically after ZTP processing is initiated.
MAC Address	The MAC address for the device.
Inventory ID	The inventory ID for the device.
UUID	The Universally Unique Identifier (UUID) for the device. This is assigned by the system unless you elect to enter one yourself.
OS Platform *	Select the software platform for the device. This should be the same platform as the image and configuration files you will use to provision it. Currently, the IOS-XR platform is supported. Required only if you selected No Profile in the Profile field.
OS Version *	Select the IOS software platform version for the device. This should be the same version as the image and configuration files you will use to provision it. Currently, IOS-XR versions 6.6.3 , 7.0.1 , 7.0.2 and 7.0.12 are supported. Required only if you selected No Profile in the Profile field.
Device Family *	Select the device family for the device. This should be the same device family as the image and configuration files you will use to provision it. Required only if you selected No Profile in the Profile field.
Software Image	Select from the dropdown menu the image file you will use to image the device. A software image is not required, even if you selected No Profile in the Profile field.
Configuration File *	Select from the dropdown menu the configuration file you will use to configure the device. Required only if you selected No Profile in the Profile field.
Credential Profile *	Select from the dropdown menu the Credential Profile to be assigned to the device, which will be used to access it for data collection and configuration changes. For example: nso23 .
Connectivity Details	

Field	Description
Protocol	<p>The connectivity protocols used by the device. Choices are: SSH, SNMPv2, NETCONF, TELNET, HTTP, HTTPS, GRPC, and SNMPv3.</p> <p>You can add one protocol for this device by completing the fields in the first row of the Connectivity Details panel. To add more connectivity protocols, click  at the end of the first row. To delete a protocol you have entered, click  shown next to that row in the panel. You can enter as many sets of connectivity details as you want. You must enter connectivity details for at least SSH, SNMPv2 or SNMPv3, and NETCONF. SNMP is required to onboard the device. NETCONF is required to manage IOS-XR devices. TELNET and other connectivity protocols are optional.</p> <p>Please note that the assigned IP address needs to be reachable from the Crosswork server. In some cases, this may require route creation. Consult the <i>Cisco Crosswork Change Automation and Health Insights Installation Guide</i> for additional details on network configuration.</p>
* IP Address / Subnet Mask	<p>Enter the device's IP address (IPv4 or IPv6) and subnet mask.</p> <p>Required only if you chose to set up a connectivity protocol.</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 Protocol you chose. The standard port assignments for each protocol are:</p> <ul style="list-style-type: none"> • SSH: 22 • SNMP: 161 • NETCONF: 830 • HTTP: 80 • HTTPS: 443 <p>Required only if you chose to set up a connectivity protocol.</p>
Timeout	<p>The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds; the recommended timeout value is 60 seconds.</p>
Providers and Access	
Provider Names	<p>Select the provider type used to manage devices. For ZTP, select an NSO provider only.</p>
Device Key	<p>If you choose Cisco NSO as a provider, the Device Key will automatically populate.</p>

Create ZTP Device Entries Using Import

Follow the steps below to create multiple ZTP device entries all at once by importing a CSV file.

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

Before you begin

Be sure you have:

- Completed the planning steps and setup requirements discussed in [Get Started](#).
- Uploaded to Crosswork the software files you will use to image the devices when ZTP processing is initiated, as explained in [Upload Software Image Files](#).
- Uploaded to Crosswork the configuration files you will use to configure the devices when ZTP processing is initiated, as explained in [Upload Configuration Files, on page 114](#).
- Used the template to prepare a CSV file describing the device entries you want to import. You can download the CSV template using the **Import Devices** dialog box, as explained in [Prepare ZTP Device Import Files, on page 126](#).

-
- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Devices** list.
- Step 2** Click the **Zero Touch Devices** tab.
- Step 3** Click  to open the **Import Devices** dialog box.
- Step 4** Click **Browse** to navigate to the CSV file you created and then select it.
- Step 5** With the CSV file selected, click **Import**.
-

Prepare ZTP Device Import Files

Complete the steps below to create a CSV file specifying one or more ZTP devices that you can then import into Crosswork, as explained in [Create ZTP Device Entries Using Import, on page 125](#).

Note that, if you are preparing the import file to correct device entries you have already made, the device entries must be in the **Unprovisioned** status. For instructions on how to reset the device entry's status, see [XREF](#)

-
- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Devices** list.
- Step 2** Click the **Zero Touch Devices** tab.
- Step 3** Click  to open the **Import Devices** dialog box.
- Step 4** Click the **Download 'Devices import' template (.csv) file** link and save the CSV file template to a local storage resource. Then click **Cancel** to exit the **Import Devices** dialog.
- Step 5** Open the template using your preferred tool. Begin adding rows to the file, one row for each device. As you do so, observe the following guidelines:
- Use two semicolons with no space between them to indicate that you are leaving a field blank.
 - 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. 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 mapping between the two fields will be as follows:

- SSH: 22
- SNMP: 161
- NETCONF: 830

For a list of the fields and the values you can enter, see the "Add ZTP Device Fields" table in [Create ZTP Device Entries Using the UI, on page 122](#).

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.

If you notice errors next to your device entries after the import, download the ZTP device entries as explained in [Export ZTP Devices, on page 127](#). Correct the errors in the exported CSV file. Before re-importing it, make sure the device entries with errors have their **Status** set to **Unprovisioned**.

Export ZTP Devices

When you export the ZTP device list, all of the ZTP device information is exported to a CSV file. Export is a handy way to keep a record of all the ZTP 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 (this works only for ZTP device entries with a **Status** of **Unprovisioned**).



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

-
- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Devices** list.
- Step 2** Click the **Zero Touch Devices** tab.
- Step 3** Click . Your browser will prompt you to select a path and file name to use when saving the CSV file, or to open it immediately.
-

Edit ZTP Devices

Follow the steps below to update a ZTP device entry. You can select and edit only one ZTP device entry at a time.

Before editing any device, it is always good practice to export a CSV backup of the devices you want to change (see [Export ZTP Devices, on page 127](#)).

-
- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Devices** list.
- Step 2** Click the **Zero Touch Devices** tab.

- Step 3** (Optional) Filter the list of ZTP devices by filtering specific columns (see [Set, Sort and Filter Table Data, on page 6](#)).
- Step 4** Check the check box of the device entry you want to change, then click . The **Edit Device** page appears.
- Step 5** Edit the values configured for the device entry, as needed.
- For a description of the fields you can edit, see [Create ZTP Device Entries Using the UI, on page 122](#). Some fields will be disabled, depending on the **Status** of the device entry.
- If the device entry **Status** displays an **Onboarding Error** or **Provisioning Error**, you must reset the **Status** to **Unprovisioned** before attempting to retry onboarding or importing a device entry CSV file.
- Step 6** Click **Save**. The Save button is disabled until all required fields are completed.

Delete ZTP Devices

Follow the steps below to delete an unprovisioned ZTP device. Deleting ZTP devices from the **Zero Touch Devices** tab deletes them from the ZTP repository only. Onboarded ZTP devices must be deleted from the **Network Devices** tab.

Before deleting any device, it is always good practice to export a CSV backup (see [Export ZTP Devices, on page 127](#)). Note that deleting a device that has successfully completed ZTP processing has no impact on the number of ZTP licenses that have been used.

- Step 1** From the main menu, choose **Device Management > Devices**. Crosswork displays the **Devices** list.
- Step 2** Click the **Zero Touch Devices** tab.
- Step 3** (Optional) Filter the list of ZTP devices by filtering specific columns (see [Set, Sort and Filter Table Data, on page 6](#)).
- Step 4** Check the check box for the ZTP devices you want to delete.
- Step 5** Click .
- Step 6** In the confirmation dialog box, click **Delete**.

DHCP Setup for Crosswork ZTP

Once you have uploaded your ZTP image and configuration files, (optionally) created ZTP profiles, and created your device entries, you must update your organization's DHCP server configuration file with the IDs for these device entries and the paths to the image and configuration files stored in the Crosswork ZTP repository. These entries identify each ZTP host and the corresponding file paths and UUIDs of the associated image and configuration files. This step is necessary to allow Crosswork and DHCP to identify these ZTP devices and to respond correctly to each device's requests for connection to the network, and image and configuration file downloads.

The following topics discuss how to update common DHCP server configurations to meet this requirement. Please refer to the following note on support for HTTP and HTTPS downloads.

Crosswork ZTP Device Management Support for HTTP and HTTPS

Cisco strongly recommends that you deploy ZTP over secure network domains.

As of today, Cisco devices supported by Crosswork 3.2.0 (that is, those running IOS-XR versions 6.6.3, 7.0.1, 7.0.2, and 7.0.12) 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 your organization's DHCP server configuration.

If you want to use HTTP for both image and configuration file downloads, these URLs must specify the HTTP protocol and port 30604, as shown in Example 1, below.

If you want to use HTTPS for configuration file downloads only, the URL must specify the HTTPS protocol and port 30603. You must also specify the `-k` option before the HTTPS protocol specification of the URL. See Example 2, below.

Figure 16: Example 1: HTTP Image and Configuration File Download URLs

```
if exists user-class and option user-class = "iPXE" {
filename =
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-...853a3210c581";
} else if exists user-class and option user-class = "exr-config" {
filename =
"http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/configs/device/files/...3b2c07b94cee";
}
```

Figure 17: Example 2: HTTP Image and HTTPS Configuration File Download URLs

```
if exists user-class and option user-class = "iPXE" {
filename =
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-...853a3210c581";
} else if exists user-class and option user-class = "exr-config" {
filename = "-k
https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/configs/device/files/...3b2c07b94cee";
}
```

Cisco Prime Network Registrar DHCP Setup

Below are two sets of scripts that allow you to add ZTP device, image and configuration file entries to the Cisco Prime Network Registrar (CPNR) DHCP server configuration file. There is one set of three scripts for IPv4, and a separate set of five scripts for IPv6. To use these scripts:

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

Cisco recommends that you deploy Crosswork ZTP over secure networks only. Please see the additional requirements in [#unique_123 unique_123_Connect_42_ZTPSupport4HTTPS](#).

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

```

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

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

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

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
(request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
(request get option 61)) \"-script\") (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ####
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0cb"

client <device-1-serial-num>-script create
client-policy <device-1-serial-num>-script set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"

```

```

client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config) (2
0)"

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

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

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

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

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

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

```

IPv4 Script 2 of 3: ztp-v4-option-set.txt

```

#
#
# Option Definition Set Export/Import Utility
# Version: 1
#
{
  ( name = Cisco-ZTP )
  ( id-range = 1 )
  ( vendor-option-regex = PXEClient:Arch:.* )
  ( tenant-id = 0 )
  ( desc = Cisco ZTP Suboption Definitions )
  ( option-list = [
    {
      ( id = 43 )
      ( name = Cisco-ZTP )
      ( base-type = AT_BLOB )
      ( desc = Cisco Zero Touch Provision )
      ( flags = )
      ( option-list = [
        {
          ( id = 1 )
          ( name = clientId )
          ( base-type = AT_NSTRING )
          ( desc = )
          ( flags = )
        }
        {
          ( id = 2 )
          ( name = authCode )
          ( base-type = AT_INT8 )
          ( desc = )
          ( flags = )
        }
      ]
    }
  ]
}

```

```

        ( id = 3 )
        ( name = md5sum )
        ( base-type = AT_NSTRING )
        ( desc = )
        ( flags = )
    }
] )
}
] )
}

```

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"
    )
)

```

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

```

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

```

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

```

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

```

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

```

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

```

(let (id)
  (setq id (request get option 1))
  (or
    # First try extracting the serial number from DUID
    (try (if (equali (substring id 0 6) 00:02:00:00:00:09)

```

```

        (concat (as-string (substring id 6 128)) "-script")
    )
)
# If that fails, use normal client-id (DUID) lookup
(concat (to-string id) "-script")
)
)

```

IPv6 Script 5 of 5: ztp-v6-options.txt

```

# Option Definition Set Export/Import Utility
# Version: 1
#
{
  ( name = dhcp6-cisco-custom )
  ( desc = Cisco Systems, Inc. )
  ( vendor-option-enterprise-id = 9 )
  ( id-range = 2 )
  ( option-list = [
    {
      ( name = cisco-17 )
      ( id = 17 )
      ( base-type = AT_VENDOR_OPTS )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
      ( option-list = [
        {
          ( name = clientID )
          ( id = 1 )
          ( base-type = AT_NSTRING )
          ( sepstr = , )
          ( desc = ZTP - clientID )
        }
        {
          ( name = authCode )
          ( id = 2 )
          ( base-type = AT_INT8 )
          ( sepstr = , )
          ( desc = ZTP - authCode )
        }
        {
          ( id = 3 )
          ( name = md5sum )
          ( base-type = AT_NSTRING )
          ( desc = ZTP - md5sum )
        }
      ]
    }
    {
      ( name = cnr-leasequery )
      ( id = 13 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
      ( option-list = [
        {
          ( name = oro )
          ( id = 1 )
          ( base-type = AT_SHORT )
          ( flags = AF_IMMUTABLE )
          ( repeat = ZERO_OR_MORE )
          ( sepstr = , )
        }
      ]
    }
    {
      ( name = dhcp-state )
    }
  ]
)

```

```

    ( id = 2 )
    ( base-type = AT_INT8 )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = data-source )
    ( id = 3 )
    ( base-type = AT_INT8 )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = start-time-of-state )
    ( id = 4 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = base-time )
    ( id = 5 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = query-start-time )
    ( id = 6 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = query-end-time )
    ( id = 7 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = client-class-name )
    ( id = 8 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = partner-last-transaction-time )
    ( id = 9 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = client-creation-time )
    ( id = 10 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = limitation-id )
    ( id = 11 )
}

```

```

    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = binding-start-time )
    ( id = 12 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = binding-end-time )
    ( id = 13 )
    ( base-type = AT_STIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = fwd-dns-config-name )
    ( id = 14 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = rev-dns-config-name )
    ( id = 15 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = lookup-key )
    ( id = 16 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = user-defined-data )
    ( id = 17 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = prefix-name )
    ( id = 18 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = failover-state-serial-number )
    ( id = 19 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = reservation-key )
    ( id = 20 )
    ( base-type = AT_BLOB )

```

```

        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-partner-lifetime )
        ( id = 21 )
        ( base-type = AT_STIME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-next-partner-lifetime )
        ( id = 22 )
        ( base-type = AT_STIME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-expiration-time )
        ( id = 23 )
        ( base-type = AT_STIME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = client-oro )
        ( id = 24 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( repeat = ZERO_OR_MORE )
        ( sepstr = , )
    }
] )
}
{
    ( name = failover )
    ( id = 21 )
    ( base-type = AT_BLOB )
    ( flags = AF_NO_CONFIG_OPTION,AF_SUPPORTS_ENCAP_OPTION,AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
        {
            ( name = server-state )
            ( id = 1 )
            ( base-type = AT_INT8 )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = server-flags )
            ( id = 2 )
            ( base-type = AT_INT8 )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = binding-status )
            ( id = 3 )
            ( base-type = AT_INT8 )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = binding-flags )

```

```

    ( id = 4 )
    ( base-type = AT_INT8 )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = start-time-of-state )
    ( id = 5 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = state-expiration-time )
    ( id = 6 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = failover-expiration-time )
    ( id = 7 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = bndupd-serial )
    ( id = 8 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = bndack-serial )
    ( id = 9 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = client-flags )
    ( id = 10 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = vpn-id )
    ( id = 11 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = lookup-key )
    ( id = 12 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
      {
        ( name = type )
        ( id = 0 )
      }
    ] )
  }

```

```

        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = data )
        ( id = 0 )
        ( base-type = AT_BLOB )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
] )
}
{
    ( name = user-defined-data )
    ( id = 13 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = reconfigure-data )
    ( id = 14 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
        {
            ( name = time )
            ( id = 0 )
            ( base-type = AT_DATE )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = key )
            ( id = 0 )
            ( base-type = AT_BLOB )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
    ] )
}
{
    ( name = requested-fqdn )
    ( id = 15 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
        {
            ( name = flags )
            ( id = 0 )
            ( base-type = AT_INT8 )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = domain-name )
            ( id = 0 )
            ( base-type = AT_DNSNAME )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
    ] )
}

```

```

] )
}
{
  ( name = forward-dnsupdate )
  ( id = 16 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reverse-dnsupdate )
  ( id = 17 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = partner-raw-cltt )
  ( id = 18 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-class )
  ( id = 19 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = status-code )
  ( id = 20 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = status-code )
      ( id = 0 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = status-message )
      ( id = 0 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = dns-info )
  ( id = 21 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = flags )
      ( id = 0 )
      ( base-type = AT_SHORT )

```

```

        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = host-label-count )
        ( id = 0 )
        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = name-number )
        ( id = 0 )
        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
] )
}
{
    ( name = base-time )
    ( id = 22 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = relationship-name )
    ( id = 23 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = protocol-version )
    ( id = 24 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = mclt )
    ( id = 25 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = dns-removal-info )
    ( id = 26 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
        {
            ( name = host-name )
            ( id = 1 )
            ( base-type = AT_RDNSNAME )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = zone-name )
            ( id = 2 )
        }
    ] )
}

```

```

        ( base-type = AT_DNSNAME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = flags )
        ( id = 3 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = forward-dnsupdate )
        ( id = 4 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = reverse-dnsupdate )
        ( id = 5 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    ] )
}
{
    ( name = max-unacked-bndupd )
    ( id = 27 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = receive-timer )
    ( id = 28 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = hash-bucket-assignment )
    ( id = 29 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = partner-down-time )
    ( id = 30 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = next-partner-lifetime )
    ( id = 31 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = next-partner-lifetime-sent )

```

```

        ( id = 32 )
        ( base-type = AT_DATE )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = client-oro )
        ( id = 33 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( repeat = ZERO_OR_MORE )
        ( sepstr = , )
    }
    {
        ( name = requested-prefix-length )
        ( id = 34 )
        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    ] )
}
] )
}
] )
}

```

Generic ISC DHCP Setup

Below is a sample of the type of host entry you would make for a ZTP device in the `/etc/dhcp/dhcp.conf` configuration file of an [Internet Systems Consortium \(ISC\) DHCP server](#).

While DHCP servers differ in overall implementation, most open-source DHCP servers use options and formats similar to the following ISC examples for IPv4 and IPv6.

Cisco recommends that you deploy Crosswork ZTP over secure networks only. Please see the additional requirements in [#unique_123 unique_123_Connect_42_ZTPSupport4HTTPS](#).

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

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://105.11.1.2.1:30604/crosswork/imagesvc/v1/device/files/
        cw-image-uuid-2b66f2ce-21ff-44c1-9801-d649db2a5581
    } else if exists user-class and option user-class = "exr-config" {
        filename = "http://105.1.2.1:30604/crosswork/configsvc/v1/configs/device/files/
        9cclea36-f53f-4306-959f-0fd804b32f01";
    }
}

```

ISC IPv6 DHCP Configuration Example

```

host 5501
{
    host-identifier option dhcp6.client-id
00:02:00:00:00:09:46:4f:43:32:33:30:38:52:30:53:33:00;
    fixed-address6 fc00:15:2::36;
    if exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) = "iPXE" {
        option dhcp6.bootfile-url
"http://[fc00:15:2::2]:30604/crosswork/imagesvc/v1/device/files/
    cw-image-uuid-94dc3788-e0d4-4bb0-9c17-721b23c30007";
    } else {if exists dhcp6.user-class and substring(option dhcp6.user-class, 0, 10) =
"exr-config" {
        option dhcp6.bootfile-url
"http://[fc00:15:2::2]:30604/crosswork/configsvc/v1/configs/device/files/
    2dde1691-bb9c-4e1e-919c-08fffa89611a";
    }
}
    }
}

```

IPv4 DHCP Configuration Entries and Values

The following table describes each line in the IPv4 example DHCP device entries and the source of the values used. The IPv6 entries are similar.

Table 16: IPv4 DHCP Configuration Host Entries and Values

IPv4 Entry	Description
host NCS5k-1	The device entry host name. This 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" is the serial number of the device, which can be found on the device chassis. If you do not have physical access to the device, the IOS-XR <code>show inventory</code> command will provide the serial number.
hardware ethernet 00:cc:fc:bb:be:6a	The MAC address of the device's Ethernet NIC on which you trigger the zero-touch provisioning process. This can be a management or data port, as long as it is reachable from Crosswork.
fixed-address 105.1.1.16	The IP address to be assigned to the device during configuration. This 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, which is used to image (or re-image) the device. If the request includes this option, then the device will download from the ZTP repository the image file corresponding to the UUID and on the path specified in the <code>filename =</code> parameter. To copy the complete image file path and/or UUID into your DHCP device entry, follow the steps in Copy Image File Paths and UUIDs, on page 114 .

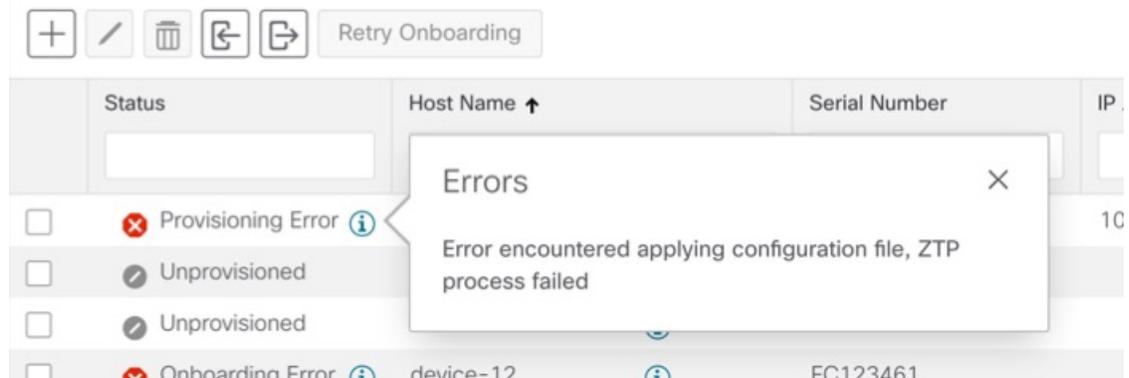
IPv4 Entry	Description
<pre>option user-class = "exr-config" and ffl filename =</pre>	<p>This line checks that the incoming ZTP request contains the "exr-config" option, which is used to configure the device. If the request includes this option, then the device will download from the Crosswork repository the configuration file corresponding to the UUID and on the path specified in the <code>filename =</code> parameter. To copy the complete configuration file path and/or UUID into your DHCP device entry, follow the steps in Copy Configuration File Paths and UUIDs, on page 119.</p>

Troubleshoot ZTP Issues

Crosswork ZTP provisioning and onboarding happen quickly and automatically, but errors and problems do occur. The following topics discuss how to remedy common problems.

Inspect Status Errors

As explained in [Use the Zero Touch Devices Window to Work with Devices](#), on page 107, the **Status** column displays the  next to every device entry whose ZTP processing finished with a **Provisioning Error** or **Onboarding Error**. Click on the icon to display a popup window with information about the error, as in the example shown below. When you are finished viewing the popup window, click **X** to close it.



Errors while uploading image files

Make sure that the image file's MD5 checksum was entered correctly. If all the information was entered correctly, image uploads to the Crosswork repository can still fail due to slow network connections. If you are running into this problem, retry the upload.

Uploaded images and configuration files are not in the drop down menu when creating ZTP device entries or ZTP profiles

The drop down menu selects images and configuration files based on the device family and release number you specify in your device entry or profile. Make sure that the release and the device family for the image or configuration files matches the release and device family specified for the device entry or profile you are creating.

Errors during import of devices

If there are any devices already present in Crosswork that have the same serial numbers as the devices you are importing, make sure these existing devices are in the **Unprovisioned** state before the import (all the devices imported using CSV files have their status set to **Unprovisioned** on import). Before importing the devices, make sure the configuration files, software images, and ZTP profiles mentioned in the CSV file are already present in Crosswork. If you are importing a previously exported CSV file in which you have made changes, and want to ensure they are associated with new image or configuration files you have uploaded, make sure to edit the UUIDs of the associated image and configuration files in the CSV file before importing.

Image file download fails

Check that there is network connectivity between 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's configuration file is correct. If you must correct the image UUID specified in the DHCP server's configuration file, make sure you restart the DHCP server before initiating ZTP processing again.

Configuration file download fails

Check that there is network connectivity between 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's configuration file is correct. If you must correct the image UUID specified in the DHCP server's configuration file, make sure you restart the DHCP server before initiating ZTP processing again. Make sure that the device serial number entered in Crosswork is correct and matches the serial number on the device's chassis. Ensure that the device's status in Crosswork is either **Unprovisioned** or **In Progress** before initiating ZTP processing. If the device is in any other state, the configuration download will fail again.

Device state is showing Onboarded and not Provisioned

This is expected behavior, as **Provisioned** is an intermediate state. As soon as the device state is changed to **Provisioned**, Crosswork will attempt to onboard the device immediately, and the status will change to **Onboarded** or **Onboarding Error**, depending on whether the onboard to DLM was successful or not.

Onboarding Error

The default Crosswork device life-cycle management (DLM) policy for identifying devices uniquely is the IP address. If your Crosswork installation is using the default DLM policy and if there is already a device in inventory with the same IP address as the ZTP device entry being processed, the device status will change first to **Provisioned**, then to **Onboarding Error**. You will get the same result if the IP address field is not populated in the device entry. These same issues apply if your Crosswork installation uses an OSPF ID, ISIS ID, or other DLM policy. All the DLM policy fields must be populated and their values must be unique for onboarding to succeed. If onboarding fails, inspect the popup error message, update the corresponding fields and retry onboarding.



CHAPTER 7

Perform Administrative Tasks

This section contains the following topics:

- [Manage Cisco Crosswork Network Automation, on page 147](#)
- [Manage Backup and Restore, on page 158](#)
- [Integration with TACACS+ and LDAP servers, on page 161](#)
- [Manage Users, on page 164](#)
- [Manage Providers, on page 170](#)
- [Manage Tags, on page 188](#)
- [Define Network Visualization Display Settings, on page 193](#)
- [Manage Certificates, on page 193](#)
- [Smart Licensing Registration, on page 196](#)
- [Security Hardening Overview, on page 202](#)

Manage Cisco Crosswork Network Automation

The **Crosswork Manager** window gives you consolidated information about the current status of each installed Cisco Crosswork Change Automation and Health Insights application and its supporting services. 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 Cisco Crosswork Change Automation and Health Insights.

Select **Admin > Crosswork Manager** to display a **Crosswork Manager** window, with information like the window shown in the following example.

The screenshot displays the Cisco Crosswork Network Automation Admin interface. The main dashboard, titled "CrossWork Applications Summary", shows the following statistics:

Category	Count
Total	5
Running	5
Down	0
Degraded	0

Below the summary, the interface lists several application details, each with a status bar and control buttons:

- Health Insights:** Status: Running (2 Services - 2 Running | 0 Down | 0 Degraded). Description: robot-nca: No Data Available. Recommendation: None at this stage.
- Change Automation:** Status: Running (2 Services - 2 Running | 0 Down | 0 Degraded). Description: robot-nca: All dependencies are reachable. Recommendation: None at this stage.
- Topology:** Status: Running (3 Services - 3 Running | 0 Down | 0 Degraded). Description: nca-d-topo-svc: nca-d DB is available at this time. Recommendation: None at this stage.
- Collection Infra:** Status: Running (9 Services - 9 Running | 0 Down | 0 Degraded). Description: dg-manager: Data Gateway Manager Service started. State: Running| magellan: magellan started up robot-dimnvmgr: Inventory Manager Service is running. Recommendation: None at this stage.
- Core Infra:** Status: Running (11 Services - 11 Running | 0 Down | 0 Degraded). Description: csw-clms: **

Each application detail includes a "Show Service Details" link and a set of control buttons: Restart, Stop, Start, Collect All, Collect Logs, and Collect Metrics.

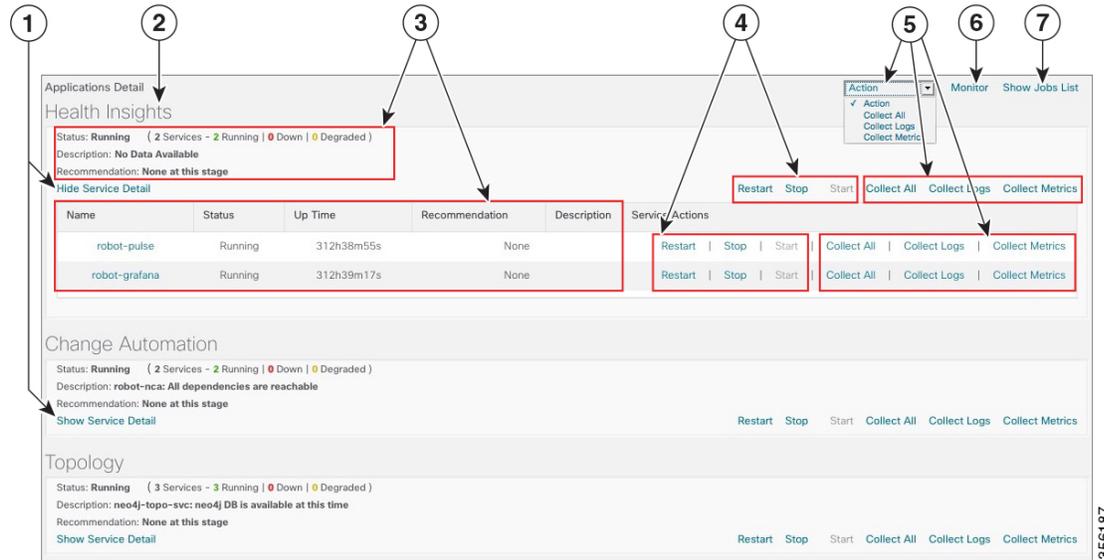
The **Crosswork Manager** window has two main views. The **Crosswork Applications Summary** view, at the top of the window, is a dashboard giving you a quick look at the overall health of the system. It displays the total number of Cisco Crosswork Change Automation and Health Insights applications currently installed in the system, and how many of that total are **Running**, **Down**, or **Degraded**.

The **Applications Detail** view, below the **Crosswork Applications Summary** view, allows you to:

- View the name and current runtime status of each installed application and its supporting services.
- Get advice about what to do when an application or one of its services has issues.
- Collect logs and metrics on any application or service, or for the system as a whole.
- Stop, start, or restart any application or service.

The **Applications Detail** view, shown in the following figure, is the best way to investigate any system health issues indicated in the **Crosswork Applications Summary**.

Figure 18: Applications Detail View



366187

Item	Description
1	Click the Show/Hide Service Detail link in each application tile to view the detailed status of the underlying services for that application.
2	An application tile like this shows the current status of the named application and a summary of the status of that application's services. This includes the total number of services, and how many of those services are Running, Down, or Degraded.
3	Both the application tile and its Service Detail table provide the name, status, description and recommendation for the respective application or service. The Service Detail table also provides service uptime, and you can click on the link in the Name column to see more details about the service, such as its process ID and pod identifier.
4	To control an application or service, click on any of the links in this section of the application tile or Service Detail table. You can click: <ul style="list-style-type: none"> • Restart to restart the application or service. • Stop to stop the application or service. • Start to start the application or service. See Control Cisco Crosswork Network Automation Applications and Services , on page 157.

Item	Description
5	<p>To gather logs and metrics for the entire system, or for any application or service, click on any of the "collect" links at the system (in the dropdown menu), application, or service level. You can choose:</p> <ul style="list-style-type: none"> • Collect All to collect both logs and metrics. • Collect Logs to collect only logs. • Collect Metrics to collect only metrics. <p>See Collect and Share Cisco Crosswork Network Automation Logs and Metrics, on page 154.</p>
6	<p>Click the Monitor link to monitor individual Cisco Crosswork Change Automation and Health Insights functions and features, using analytical dashboards and data gathered over the last 24 hours of run time.</p> <p>See Monitor Cisco Crosswork Network Automation Functions in Real Time, on page 150.</p>
7	<p>Choosing any of the control or collect actions at the system, application or service level will initiate a job. You can view each job's progress by clicking the Show Jobs List link at the top right corner of the window. You can also use the Show Jobs List to publish collected logs and metrics files, and check on the status of publish jobs you initiate.</p>

Monitor Cisco Crosswork Network Automation Functions in Real Time

You can monitor the health of Cisco Crosswork Change Automation and Health Insights and any of its functions in real time, using a set of monitoring dashboards you can access from the **Crosswork Manager** window.

Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights applications or their underlying services.

There are multiple monitor dashboards, categorized by the type of functionality they monitor and the metrics they provide, as shown in the following table.

Table 17: Monitoring Dashboard Categories

This dashboard category...	Monitors...
Change Automation	Playbook functions. Metrics include the number of MOP jobs executed, response latency, API calls, database activity, and so on.
Collection - Manager	Device-data collection functions. Metrics include telemetry collection latencies, total collection operations, memory and database activity related to telemetry, delayed collections, and so on.
Health Insights	Key Performance Indicator functions. Metrics include the number of KPI alerts, API calls, and so on.
Infra	System infrastructure messaging and database activity.

This dashboard category...	Monitors...
Inventory	Inventory manager functions. These metrics include total numbers of inventory change activities.
Platform	System hardware and communications usage and performance. Metrics include disk and CPU usage, database size, network and disk operations, and client/server communications.
ZTP	Zero Touch Provisioning functions.

To conserve disk space, Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights implementation of Grafana. For more information about Grafana itself, see <https://grafana.com> and <http://docs.grafana.org>

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

Step 2 At the right, just below the **Crosswork Applications Summary** view, click the **Monitor** link, highlighted below.



The Grafana user interface appears within the **Crosswork Manager** window, replacing the **Applications Detail** view.

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.

Home / Admin / Crosswork Manager
CrossWork Applications Summary

5 Total 5 Running 0 Down

Action ▾ St

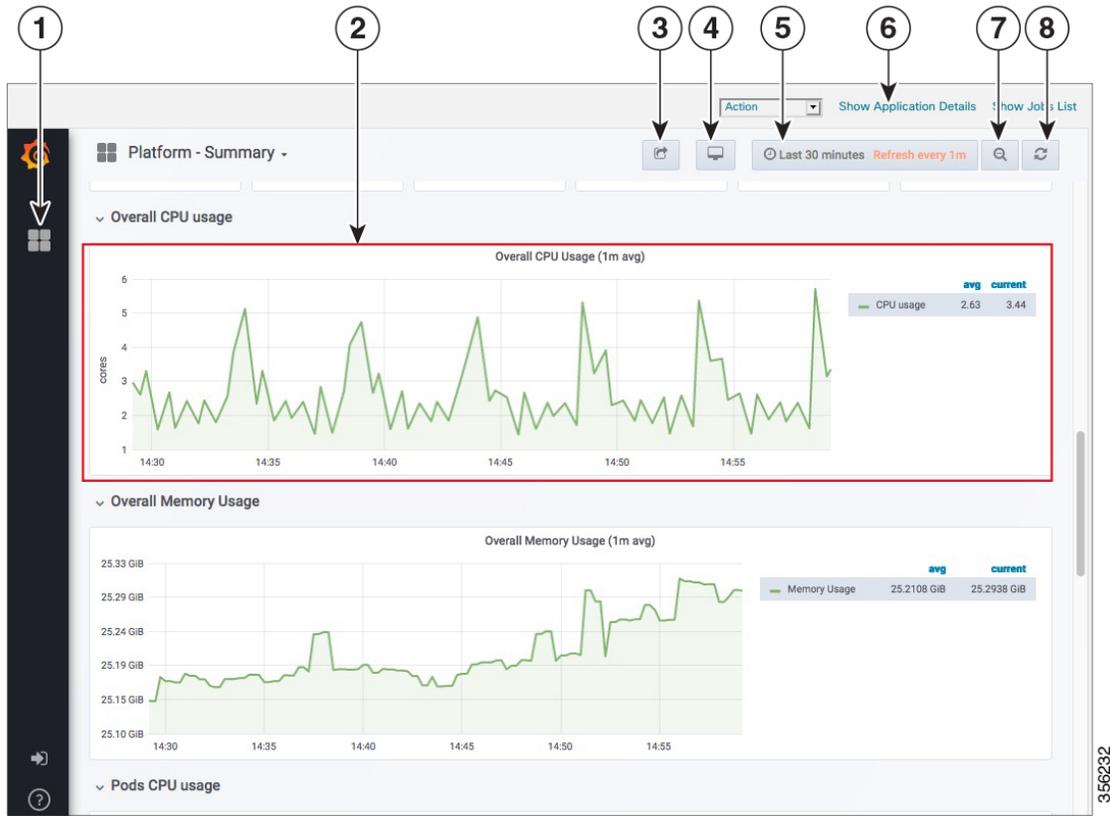
Find dashboards by name

Recent

General

- Change Automation nca
- Collection - Manager collection
- Collection - Pipeline CLI collection
- Collection - Pipeline Kafka collection
- Infra - Etcd infra
- Infra - Kafka infra
- Infra - Nats infra
- Inventory - Manager inventory
- Platform - Metrics platform
- Platform - Pods platform
- Platform - Statefulsets platform
- Platform - Summary kubernetes platform

Step 4 Click the  icon next to the dashboard you want to view. For example: Clicking on the **Platform - Summary** dashboard displays a view like the one shown in the following figure. For more information on how to use Grafana go to <https://grafana.com>.



Step 5 Scroll the dashboard as needed to display all of the metrics it provides, or select any of the functions described in the following table.

Item	Description
1	Dashboard Icon: Click the icon to re-display the dashboard list and select a different dashboard.
2	<p>Time Series Graph Zoom: 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"> Click a time-period starting point in the graph line and hold down the mouse. 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. <p>To reset a zoomed time series graph to the default, click the Zoom Out icon.</p>

Item	Description
3	<p>Share Dashboard icon: Click the icon to make the dashboard you are viewing shareable with other users. Clicking this icon displays a popup window with tabs and options to share the dashboard in your choice of these forms:</p> <ul style="list-style-type: none"> • URL Link: Click the Link tab and then click Copy to copy the dashboard's URL to your clipboard. You can also choose whether to retain the current time and template settings with the URL. • Local Snapshot File: Click the Snapshot tab and then click Local Snapshot. Grafana creates a local snapshot of the dashboard on the server. When the snapshot is ready, click Copy Link to copy the URL of the snapshot to your clipboard. • Export to JSON File: Click the Export tab and then click Save to file. You will be prompted to save or open the exported JSON file. You can also choose to turn data source names in the file into templates by selecting the Export for sharing externally checkbox before clicking Save to file. • View JSON File and Copy to Clipboard: Click the Export tab and then click View JSON (you can choose to templatzize data source names by selecting the Export for sharing externally checkbox before clicking View JSON). Grafana displays the exported JSON code in a popup window. Click Copy to Clipboard to copy the file to your clipboard.
4	<p>Cycle View Mode icon: Click this icon to toggle between the default Grafana TV view mode and the Kiosk mode. The Kiosk view hides most of the Grafana menu. Press Esc to exit the Kiosk view.</p>
5	<p>Time/Refresh Selector: Indicates the time period for the metrics displayed in the dashboard and how often the metrics are refreshed. Click the selector to choose a different time range and refresh rate.</p> <p>You can specify a custom pair of time-range start and end points, or choose from one of several predefined ranges, such as Today so far or Last three hours.</p> <p>You can choose predefined refresh rates from Off to 2 Days.</p> <p>When you have finished making changes, click Apply.</p> <p>When making selections, remember that Cisco Crosswork Change Automation and Health Insights keeps only 24 hours of data. If you select time ranges or refresh rates beyond that limit, the dashboard may be blank.</p>
6	<p>Show Application Details: Click this link to re-display the Crosswork Manager window's Applications Detail view.</p>
7	<p>Zoom Out icon: Click this icon to reset a zoomed time series graph back to the unzoomed state.</p>
8	<p>Refresh icon: Immediately refresh the data shown.</p>

Collect and Share Cisco Crosswork Network Automation Logs and Metrics

You can collect logs and metrics on multiple levels of Cisco Crosswork Change Automation and Health Insights. You can collect logs and metrics for the entire system, for any of its installed application, or for any service supporting an application. You can also choose to collect only logs, only the additional metrics, or both.



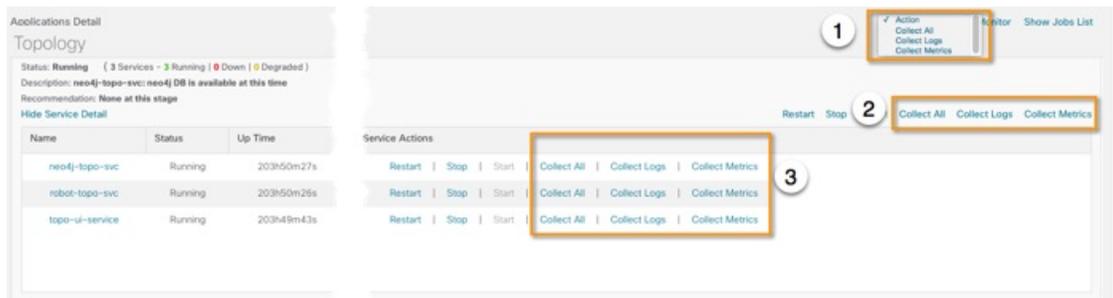
Note Collected logs include audit log files that capture user details and application-specific data. Application-specific data contains information on any CRUD (Create, Replace, Update, Delete) operation performed by the users along with the session history. For more information, see [Audit Log, on page 156](#).

Collected logs and metrics are stored in gzipped tar archive files. You can publish these archives to an HTTP or HTTPS server of your choice.

Step 1 From the main menu, choose **Admin > Crosswork Manager**. The **Crosswork Manager** window displays, with the **Application Detail** section listing all the applications.

Step 2 Click the option for the collection level and target information you want, as follows:

- To collect for the entire system: From the **Action** drop down on the right, opposite the **Applications Detail** section title, choose **Collect All**, **Collect Logs**, or **Collect Metrics**. See item 1 in the following figure.
- To collect for an application: Scroll to the **Application Detail** tile for the application you want. Then click the **Collect All**, **Collect Logs**, or **Collect Metrics** link on the right, opposite the application's name. See item 2 in the following figure.
- To collect for a service: Scroll to the **Application Detail** tile for the application whose service you want to collect. Click the **Show Service Detail** link for that application. Then click the **Collect All**, **Collect Logs**, or **Collect Metrics** link on the right, opposite the service's name. See item 3 in the following figure.



Step 3 When you click on the collection option you want, the **Crosswork Manager** window displays a popup message indicating that a job was successfully created and giving the job ID. Click on the **Show Jobs List** link at the right to view the job's progress in the **Crosswork Manager** window's **Jobs List** view, which replaces the **Applications Detail** view.

Step 4 Wait for the job to complete. When the **Jobs List** view's **Status** column for your job has changed to **JobCompleted**, the **Action** column for the job will show an enabled **Publish** link for the completed job, and the **Description** column will show the file name of the gzipped tar archive file containing the collected information.

User	Job Id	Status	Job Scope	Description	Action	Publish Status
admin	201905067	JobCreated	Health-Insights	Job in progress. Progress compl...	Publish	Details
admin	20190506	JobCompleted	All	showtech_all_20190506175107...	Publish	Details

- Step 5** (Optional) Click on the **Publish** link to publish the collected information to an HTTP or HTTPS server, as follows:
- A popup window will prompt you for the destination server host name, the storage path on the server, the port number, and the login user name and password for the server (if required). Enter the server information and click **Publish**.
 - The **Job List** view's **Publish Status** column for the job shows an enabled **Details** link. Click the **Details** link to view a popup window showing the status of the publish job.

- Step 6** When you are finished, click the **Show Application Details** link to re-display the **Applications Detail** view.

Audit Log

Audit logs map the user information in Cisco Crosswork Change Automation and Health Insights with all the critical user actions performed in the system.

User actions related to the following operations are included in the audit log:

- Manage playbooks (import, export or delete) and playbook execution



Note When a playbook execution request is sent, Change Automation prints an audit log with details like playbook name, user information, session details and execution ID of the job. When a maintenance task in this playbook is executed, an audit log is printed with details such as execution ID and commit label (if a commit is performed on NSO). All the commit labels associated with an execution ID can be identified in this manner. You can use the commit labels to perform a lookup on NCS CLI and see the exact configuration changes that were pushed to the device.

- KPIs, KPI Profiles, and Alert group creation, deletion, and configuration updates
- Enabling and disabling of KPI Profiles
- Device onboarding
- User creation, deletion, and configuration updates
- Cisco Crosswork Data Gateway management operations

- Collection job creation
- Administrative tasks (show-tech execution, topology updates, NSO-related actions)

Sample Audit Log entry

This is a sample audit log entry created when a playbook is run by a local admin user.

```
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
```

Table 18: Common Audit Log entry fields

Field	Description
time	Time when the audit log is printed.
msg	Message sent between applications.
user	Name of the user.
policyId	Role or permission of user (taken from local database, TACACS, or LDAP server).
backend	Server (local database, TACACS, or LDAP) against which user is authenticated.
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 additional fields specific to that application. For example: In the sample audit log entry above, playbook field refers to the playbook being executed in Change Automation.

Audit Log location

Logs are placed in `/var/log/robot/audit/audit.log` under the respective application pods. For example: the sample audit log mentioned above is stored in `<robot-nca>` data directory under the Change Automation pod.

In addition to the individual application audit logs, all audit log files are collected every hour as separate gzipped tar files in the following data directory:

```
/mnt/robot_datafs/<app-name>/<instance>/auditlogs/auditlogs.tar.gz
```

The audit log files are collected and circulated based on the maximum size and maximum number of backups on Cisco Crosswork Change Automation and Health Insights. For example: **MaxSize: 20 megabytes** and **MaxBackups: 5**.

Control Cisco Crosswork Network Automation Applications and Services

Users with administrator privileges can control the runtime status of any Cisco Crosswork Change Automation and Health Insights application or service. This can include:

- Stopping a running application or service
- Starting a stopped application or service
- Restarting a running or stopped application or service

Please note that stopping, starting and restarting Cisco Crosswork Change Automation and Health Insights applications and services can result in anomalous system behavior and possible data loss. Use these functions only with the supervision of Cisco TAC staff.

Step 1 From the main menu, choose **Admin > Crosswork Manager**. The **Crosswork Manager** window displays, with the **Application Detail** view listing all the applications.

Step 2 Display the application or service whose runtime status you want to control:

- To control an application: Scroll to the **Application Detail** tile for the application you want.
- To control a service: Scroll to the **Application Detail** tile for the application whose service you want to control, then click the **Show Service Detail** link for that application to show its services.

Step 3 Click on the **Start**, **Stop**, or **Restart** link shown next to the service (item 1 in the following figure) or the application whose runtime status you want to control.

The screenshot shows the 'Topology' section of the Crosswork Manager. It displays a table of services with columns for Name, Status, and Up Time. The services listed are neo4j-topo-svc, robot-topo-svc, and topo-ui-service, all with a status of 'Running'. To the right of the table, there are two callouts: '1' points to the 'Service Actions' section, which contains 'Restart', 'Stop', and 'Start' links for each service. '2' points to a larger view of the 'Restart', 'Stop', and 'Start' links for a specific service.

Name	Status	Up Time
neo4j-topo-svc	Running	204h39m46s
robot-topo-svc	Running	204h39m45s
topo-ui-service	Running	204h39m2s

Step 4 Click the **Show Jobs List** link at upper right to view the runtime control job's progress in the **Crosswork Manager** window's **Jobs List** view.

Step 5 When you are finished, click the **Show Application Details** link to re-display the **Applications Detail** view.

Manage Backup and Restore

The Backup Restore functionality is critical to prevent data loss in your Cisco Crosswork Change Automation and Health Insights VM.

Follow the steps below to create a backup for the Cisco Crosswork Change Automation and Health Insights VM and to restore a backup.

**Important**

- Cisco recommends that you perform the backup or restore operation only during a scheduled maintenance window when admin users should not access the UI. Both operations are time-consuming and stops all other applications running in the system.
- The same Cisco Crosswork Change Automation and Health Insights software image that was used to backup must also be used when doing a restore operation.
- Stay on the **Backup Restore** window until the backup/restore process completes. Otherwise, you may see incorrect content or UI errors since various services are rebooting frequently.
- Only one backup or restore operation can be running at any given time.

Before you begin, ensure that:

- You have the Host Name, Port number, and Remote path to a Secure FTP server to use as the destination for backup files.
- You have the user credentials to an account with write permissions to create files and directories in the destination server remote path.

-
- Step 1** From the main menu, choose **Admin > Backup Restore**. The **Backup Restore** window is displayed.
- Step 2** During your first login, you should configure a destination server to store the backup file. This is a one-time activity and has to be completed before taking the backup. Click **Destination** to display the **Edit Destination** dialog box. Make relevant entries in the fields provided.
- Click **Save** to confirm the server details.
- Step 3** **To create a backup:**
- a) Click **Backup**. The **Backup** dialog box is displayed with destination server details pre-filled.
 - b) Provide a relevant name in the **Job Name** field.
 - c) (Optional) Click **Verify Backup** to check if Cisco Crosswork Change Automation and Health Insights has enough resources to complete the operation. If the check is successful, a warning message is displayed about the time-consuming nature of the operation. Click **OK**.
 - d) Click **Start Backup** to start the backup operation. The corresponding backup job set is created and added to the job list. See Step 5 to view Backup progress.
- Step 4** **To restore a backup file:**
- a) Select the required backup file from the **Backup Restore Job Sets** table, and the job details are displayed on the right side.
 - b) Click the **Restore** button to display the **Restore** dialog box with destination server details pre-filled.
 - c) Provide a relevant name in the **Job Name** field.
 - d) (Optional) Click **Verify Restore** and a prompt is displayed that suggests doing the backup or restore during maintenance window owing to the time-consuming nature of the operation. Click **OK**.
 - e) Click **Start Restore** to start the restore operation. The corresponding restore job set is created and added to the job list.
- Step 5** **To view a job progress:**

- a) Enter the job details (such as Status, Job Name, or Job Type) in the search fields in **Backup Restore Job Sets** table on the left side. Click  to select which columns to display in the Job set list. The list is automatically filtered based on your search string. Click the required job set from the search results.
- b) Alternately, you can manually scroll the list and click the required job set.
- c) The **Job Details** table on the right side displays information about the selected job set such as Status, Job Type and Start time. In case of a failed job, hover the mouse pointer over the  icon near **Status** to view the error details.

Disaster Restore

Disaster Restore is a restore operation, appropriately named to be used in case of a disaster, such as VM crash. The **Disaster Restore** option is displayed if no backup jobs have been initiated in the system. After the completion of the first backup job, this button is disabled.



Note While using disaster recovery operation, please note the following:

- The new VM that you use needs to have the same IP address as the one where backup was performed. This is important as internal certificates are tied to the IP address.
- The same software image that was used to backup must also be used when doing a restore operation.
- The VM which is brought up should have same services running when the backup was performed. If the previous VM was patched/updated then the new VM also needs to be patched/updated before disaster restore is performed.
- The disaster restore operation trusts the backup file which is provided. Caution is advised while selecting the appropriate backup file.

To perform a disaster restore:

- Step 1** From the main menu, choose **Admin > Backup Restore**. The **Backup Restore** window is displayed.
- Step 2** Click **Destination** to display the **Edit Destination** dialog box. Enter the details of the remote destination server where the backup file is uploaded.
- Step 3** Click **Disaster Restore** to display the **Disaster Restore** dialog box with destination server detailed pre-filled.
- Step 4** Make relevant entry in the **Backup File Name** field.
- Step 5** Click **Start Restore** to start the disaster restore operation.

Note If disaster restore operation fails, you are recommended to bring up a new VM to retry the disaster restore operation.

Integration with TACACS+ and LDAP servers

In addition to supporting local users, Cisco Crosswork Change Automation and Health Insights supports TACACS+ and LDAP users through integration with the TACACS+ and LDAP servers. The integration process has the following steps:

- Configure the TACACS+ and LDAP server.
- Create the roles that are referenced by the TACACS+ and LDAP users.



Note If you try to login to Cisco Crosswork Change Automation and Health Insights as a TACACS+ or LDAP user before creating the required user roles, you will get an error message: "Key not authorized: no matching policy". If this occurs, close the browser. Login as a local admin user and create the missing user roles. After the roles are created, you can logout and login back as a TACACS+ or LDAP user.

Related Topics

[Manage TACACS+ Servers](#), on page 161

[Manage LDAP Servers](#), on page 163

[Create User Roles](#), on page 168

Manage TACACS+ Servers

In addition to local database authentication, Cisco Crosswork Change Automation and Health Insights can use TACACS+ servers to authenticate users. TACACS+ is a security protocol that provides centralized validation of users attempting to access your network. It allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting (AAA) services independently of one another.

Local database authorization takes precedence over authorization by TACACS+ server. When adding the TACACS+ server, you can specify the priority value for each instance. Priority field value is unique across TACACS+ and LDAP servers. Providing a duplicate value will result in an error.



- Note**
- Please note that any operation you do following the instructions in this section will affect all new logins to the Cisco Crosswork Change Automation and Health Insights user interface. To minimize session interruption, Cisco recommends that you perform all your TACACS+ changes and submit them in a single session.
 - As the AAA server page works in bulk update mode wherein all the servers are updated in a single request, it is advised to give write permission for "Remote Authentication Servers Integration api" only to users who have the relevant authorization to delete the servers. For more information, see [Create User Roles, on page 168](#).
 - AAA page operations are captured in the audit log file with generic messages that mention that the AAA servers have been updated. For more information on collecting logs, see [Collect and Share Cisco Crosswork Network Automation Logs and Metrics, on page 154](#)

Add a TACACS+ Server

Before adding a TACACS+ server, you will need to know the server's IP address, port number, shared secret, and service name.

-
- Step 1** From the main menu, choose **Admin > AAA**.
The **AAA** window opens. If it is not already displayed, click the **TACACS+ Servers** tab.
- Step 2** Click to open the **Add Server** dialog box.
- Step 3** Enter the TACACS+ server's settings, then click **Add**.
Note Only the server's IP address, port number, shared secret, and service name are required. You can leave the other values blank, as needed.
- Step 4** Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.
-

Edit a TACACS+ Server

-
- Step 1** From the main menu, choose **Admin > AAA**.
The **AAA** window opens. If it is not already displayed, click the **TACACS+ Servers** tab.
- Step 2** Click the check box next to the TACACS+ server whose settings you want to update, then click .
The **Edit Server** dialog box opens.
- Step 3** Make the necessary changes, then click **Update**.
Note You cannot change the value for the **Shared Secret** parameter.
- Step 4** Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.
-

Delete a TACACS+ Server

-
- Step 1** From the main menu, choose **Admin > AAA**.
The **AAA** window opens. If it is not already displayed, click the **TACACS+ Servers** tab.
- Step 2** Click the check box next to the TACACS+ server you want to delete.
Note You can delete only one TACACS+ server at a time.
- Step 3** Click . The **Delete *server-IP-address*** dialog box opens.

Step 4 Click **Delete** to confirm.

Manage LDAP Servers

Cisco Crosswork Change Automation and Health Insights supports the use of LDAP servers to authenticate users. Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

Like TACACS+ server, you can specify a unique priority value to assign precedence in the authentication request.



Note

- Please note that any operation you do following the instructions in this section will affect all new logins to the Cisco Crosswork Change Automation and Health Insights user interface. To minimize session interruption, Cisco recommends that you perform all your TACACS+ changes and submit them in a single session.
 - As the AAA server page works in bulk update mode wherein all the servers are updated in a single request, it is advised to give write permission for "Remote Authentication Servers Integration api" only to users who have the relevant authorization to delete the servers. For more information, see [Create User Roles, on page 168](#).
-

Add a LDAP Server

Before adding a LDAP server, you will need to know the Server name and URL, Bind DN and credential, Base DN, user filter, DN format, Principal Attribute ID, Policy ID, and connection timeout value.

Step 1 From the main menu, choose **Admin > AAA**.

The **AAA** window opens. Click on the **LDAP Servers** tab.

Step 2 Click to open the **Add Server** dialog box.

Step 3 Enter the LDAP server settings, then click **Add**.

Step 4 Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Edit a LDAP Server

Step 1 From the main menu, choose **Admin > AAA**.

The **AAA** window opens. Click on the **LDAP Servers** tab.

Step 2 Click the check box next to the LDAP server whose settings you want to update, then click .

The **Edit Server** dialog box opens.

Step 3 Make the necessary changes, then click **Update**.

Step 4 Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Delete a LDAP Server

Step 1 From the main menu, choose **Admin > AAA**.

The **AAA** window opens. Click on the **LDAP Servers** tab.

Step 2 Click the check box next to the LDAP server you want to delete.

Note You can delete only one LDAP server at a time.

Step 3 Click . The **Delete server-IP-address** dialog box opens.

Step 4 Click **Delete** to confirm.

Manage Users

From the main menu, select **Admin > Users** to display the **Users** window. Using this window, you can add a new user, edit the settings for an existing user, delete a user from the network, and create user roles.



Note Before you can create a new user that does *not* have admin-level access to Cisco Crosswork Change Automation and Health Insights functionality, you must first create a new role that limits the features they can access. See [Create User Roles](#) for more information.

Only a local admin user can add, update, and delete other local user accounts. A TACACS+ user, regardless of role assigned, will not be able to manage local users.

Administrative Users Created During Installation

During installation, Cisco Crosswork Change Automation and Health Insights 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 Cisco Crosswork Change Automation and Health Insights server.
2. The **Crosswork administrator**, with the username **admin** and the default password **admin**. Product administrators use this ID to log in to and configure the Cisco Crosswork Change Automation and Health Insights 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 Crosswork administrator password using the following methods:

- Log in as the admin user and edit the admin user password, as explained in [Edit Users, on page 165](#).
- Enter the following command: `admin(config)# username admin <password>`

Add Users

Follow the steps below to create a new user ID.

The user ID's user name must be unique. You cannot create a new user ID with the same user name as an existing user ID.

The special administrative user names **admin** (for administering Cisco Crosswork Change Automation and Health Insights) and **cw-admin** (for administering the virtual machine hosting the product) are created during installation and are reserved for those purposes (see [Administrative Users Created During Installation, on page 164](#)).

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Users** tab.

Step 2 Click  to open the **Add New User** dialog box.

Step 3 Enter the following information for the user you are adding:

- **User Name:** Enter a unique name for the user ID. User names cannot contain spaces or special characters.
- **First Name** and **Last Name:** Enter the first and last name of the person assigned to this user ID.
- From the **Role** drop-down at the bottom of the dialog box, choose the role that you want to assign to the user. See [Create User Roles](#) for more information.
- **Password** and **Confirm Password:** Enter the default password for this user ID. The user will be required to change the default password the first time they attempt to log on using it.

Note The user password must be string of minimum 8 characters without spaces and should include letters, numbers, upper-case and lower-case characters, and one of the allowed special characters ("@!\$%*?&").

Step 4 Click **Save**.

Edit Users

Users with administrator privileges can edit any user ID's User Name, First Name, Last Name, and Role.

Administrators cannot change a user's password by editing the user ID. Users can change their passwords by logging in, clicking , and selecting **Change Password**.

-
- Step 1** From the main menu, choose **Admin > Users**.
The **Users** window opens.
If it is not already displayed, click the **Users** tab.
- Step 2** Click on the check box of the user whose settings you want to update, then click  to open the **Edit User** dialog box.
- Step 3** Make the necessary updates to the user ID.
- Note** First Name, Last Name and Role can be edited for user accounts with administrative privileges.
- Step 4** Click **Update** to save your changes.
-

Delete Users

Follow the steps below to delete an existing user ID.

The administrative user IDs **admin** and **cw-admin** created during installation cannot be deleted (see [Administrative Users Created During Installation, on page 164](#)).

-
- Step 1** From the main menu, choose **Admin > Users**.
The **Users** window opens.
If it is not already displayed, click the **Users** tab.
- Step 2** Click on the check box of the user you want to delete, then click . The **Delete Username User** dialog displays.
- Step 3** Click **Delete** to confirm deletion.
-

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 Crosswork functions controlled by that API. For example: The “Health Insights” category provides access to all of the “Health Insights API” functions, such as selecting and running KPI Profiles, importing custom user-defined KPIs, deleting custom KPIs, and so on.
- 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 Change Automation and Health Insights will assume 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 Change Automation and Health Insights 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 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 Change Automation and Health Insights.
- Give read-only access to roles for users who only need to see Cisco Crosswork Change Automation and Health Insights data to help their work as system architects or planners.

The following table describes some sample custom user roles you should consider creating:

Table 19: 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
KPI Developer	Develops custom KPIs for others to use	Core Infra, Health Insights, Inventory/All	All
API Integrator	All	All	All



Note Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions. Using Zero Touch Provisioning features requires access to all ZTP APIs.

Create User Roles

Local users with administrator privileges can create new users as needed (see [Add Users, on page 165](#)).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

The local **admin** role enables access to all functionality. It is created during installation and cannot be changed or deleted. However, its privileges can be assigned to new local users. Only local users can create or update user roles; TACACS users cannot.

Follow the steps below to create a new user role.

-
- Step 1** From the main menu, choose **Admin > Users**.
- The **Users** window opens.
- If it is not already displayed, click the **Roles** tab. The **Roles** window has a **Roles** table on the left side and a corresponding **admin** table on the right side which shows the grouping of user permissions for the selected role.
- Step 2** On the **Roles** table, click to display a new role entry in the table.
- Step 3** Enter a unique name for the new role.
- Step 4** Define the user role's privilege settings:
- 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 Users, on page 165](#)).

Edit User Roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

- Step 1** From the main menu, choose **Admin > Users**.
The **Users** window opens.
If it is not already displayed, click the **Roles** tab.
- Step 2** In the **Roles** table, click on an existing role to select it. The **Admin** table on the right side displays the permission settings for the selected role.
- Step 3** Define the role's settings:
- 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** to save your changes.
-

Clone User Roles

Cloning an existing user role is the same as creating a new user role (see [Create User Roles, on page 168](#)), 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 [Edit Users, on page 165](#)). Later, you can edit the roles themselves to give users the privileges you want (see [Edit User Roles](#)).

- Step 1** From the main menu, choose **Admin > Users**.
The **Users** window opens.
If it is not already displayed, click the **Roles** tab.
- Step 2** Click on an existing role to select it.
- Step 3** Click  to create a new duplicate entry in the **Roles** table with all the permissions of the original role.
- Step 4** Enter a unique name for the cloned role.
- Step 5** (Optional) Define the role's settings:

- a) Check the check box for every API that the cloned role can access.
- b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Delete User Roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Roles** tab.

Step 2 Click on the role you want to delete, to select it.

Step 3 Click  to display the **Delete Role** dialog box.

Step 4 Click **Delete** to confirm that you want to delete the user role.

Manage Providers

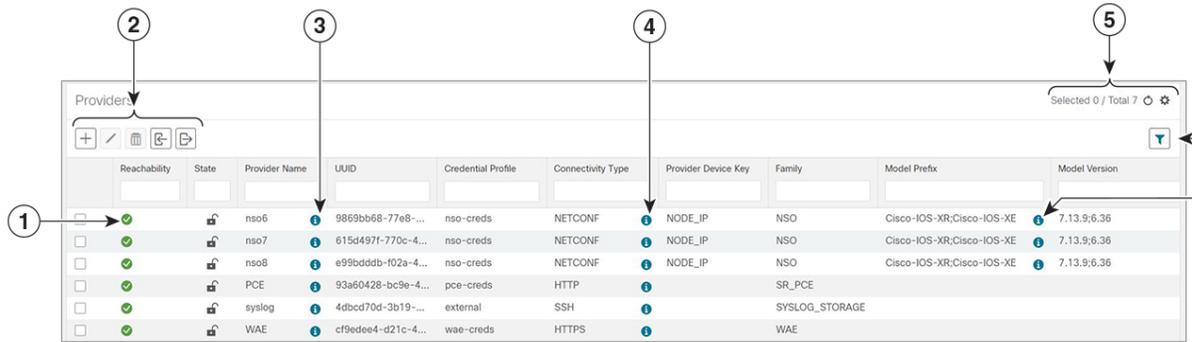
Cisco Crosswork Change Automation and Health Insights communicates with external providers. You decide which providers to use and then configure them. Cisco Crosswork Change Automation and Health Insights stores the provider connectivity details and makes that information available to applications.

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 **Admin > Providers**.



Note Wait until the application responds between performing a succession of updates. For example, adding, deleting, then readding providers in a short time. 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. See [Control Cisco Crosswork Network Automation Applications and Services, on page 157](#).

Figure 19: Providers window



Item	Description
1	The icon shown next to the provider in this column indicates the provider's Reachability . For more information, see Reachability and Operational State, on page 79 .
2	Click to add a provider. See About Adding Providers, on page 172 .
	Click to edit the settings for the selected provider. See Edit Providers, on page 187 .
	Click to delete the selected provider. See Delete Providers, on page 187 .
	Click to import new providers or update existing providers from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Providers, on page 175 .
	Click to export a provider to a CSV file. See Export Providers, on page 188 .
3	Click next to the provider in the Provider Name column to open the Properties for pop-up window, showing the details of any startup session key/value pairs for the provider.
4	Click next to the provider in the Connectivity Type column to open the Connectivity Details pop-up window, showing the protocol, IP, and other connection information for the provider.
5	Click to refresh the Providers window.
	Click to choose the columns to make visible in the Providers window (see Set, Sort and Filter Table Data, on page 6).
6	Click to set filter criteria on one or more columns in the Providers window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Item	Description
7	Click  next to the provider in the Model Prefix column to open the Supported Models pop-up window, showing a list of the model prefix names and versions in use (for Cisco NSO providers only).

About Provider Families

Cisco Crosswork Change Automation and Health Insights supports different types, or families, of providers. Each provider family supplies its own mix of special services to Cisco Crosswork Change Automation and Health Insights, and each comes with unique requirements and options.

The currently supported provider families are shown in the following table.

Table 20: Supported Provider Families

Provider Family	Description
NSO	Instances of Cisco Network Services Orchestrator (Cisco NSO), used to configure network devices. See Add Cisco NSO Providers, on page 178 .
WAE	Instances of Cisco WAN Automation Engine (Cisco WAE) provide "what if" analysis used to evaluate network changes as part of Cisco Crosswork Change Automation and Health Insights Playbooks. See Add Cisco WAE Providers, on page 182 .
SR-PCE	Instances of Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) containing the configuration information needed to allow Cisco Crosswork Change Automation and Health Insights to communicate with and retrieve segment routing information for the network. See Add Cisco SR-PCE Providers, on page 179 .
Syslog Storage	Instances of storage servers (remote or on the Cisco Crosswork Change Automation and Health Insights VM itself) where you want store syslogs and other data retrieved from devices by KPIs and Playbooks. See Add Syslog Storage Providers, on page 183 .
Alert	Instances of providers (such as Cisco Crosswork Situation Manager) to which alerts collected during KPI monitoring are to be forwarded. See Add an Alert Provider, on page 184 .
Optimization Engine	Instances of Cisco Crosswork Optimization Engine, to provide real-time network optimization allowing operators to effectively maximize network utilization as well as increase service velocity. See Add Optimization Engine Providers, on page 185 .

About Adding Providers

Cisco Crosswork Change Automation and Health Insights depends on a variety of providers to perform various functions. For example, Cisco Network Services Orchestrator provides device and routing 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. Also, not every Cisco Crosswork Change Automation and Health Insights deployment will use the same mix of providers. In any case, to access each provider's services, the provider must be added to the Cisco Crosswork Change Automation and Health Insights system configuration.

There are two ways to add providers:

1. **Adding providers via the UI:** This method is explained in [Add Providers Through the UI, on page 173](#). Although this method is the most time-consuming, it is more often used because most deployments will not need a lot of separate providers or provider instances.
2. **Importing providers from a providers CSV file:** This method is explained in [Import Providers, on page 175](#). Importing a CSV file is useful when you have a lot of separate providers or provider instances to add or update at one time.

Note that both methods require that you:

- Create a corresponding credential profile, beforehand, so that Cisco Crosswork Change Automation and Health Insights can access the provider. For help, see [Create Credential Profiles, on page 82](#).
- 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.



Note

Cisco Crosswork Change Automation and Health Insights version 3.2 only supports single stack deployment modes. You can configure multiple IP addresses (IPv4 or IPv6) for each protocol, but at least one of the IP addresses in each protocol should match the deployment type. For example, for an IPv4 deployment mode, at least one of the configured IP addresses should be IPv4. Instead, if you configure only IPv6 addresses, the request will be rejected.

Stack/Deployment mode	IPv4 deployment	IPv6 deployment
Provider IP address	<ul style="list-style-type: none"> • IPv4 address (mandatory) • IPv6 address (optional) 	<ul style="list-style-type: none"> • IPv4 address (optional) • IPv6 address (mandatory)

For help on adding the most common providers using the UI, see the following topics.

Add Providers Through the UI

Use this procedure to add a new external provider. You can then map the provider to devices.

- Step 1** From the main menu, choose **Admin > Providers**.
- 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 21: Add Provider Fields (*=required)

Field	Description
* Provider Name	The name for the provider that will be used to refer to it in Cisco Crosswork Change Automation and Health Insights. For example: MyWAE . The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.
* Credential Profile	Select the name of the credential profile that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider.
* Family	Select the provider family. Choices are: NSO , WAE , SR-PCE , ALERT and SYSLOG_STORAGE .
* Device Key	Select the method that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way Cisco Crosswork Change Automation and Health Insights maps the device in its own inventory to the device as it is stored in the Cisco NSO provider. Choices are: <ul style="list-style-type: none"> • INVENTORY_ID—Use this value if the device identifier Cisco NSO uses is the inventory ID. • HOST_NAME—If Cisco NSO uses the device hostname as the device identifier, this value must match the hostname that is specified for the device in the inventory. <p>Note that the Device Key is only required for the Cisco NSO provider. It is not needed for other providers.</p>
Connection Type(s)	
* Protocol	Select the principal protocol that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. Options include: HTTP , HTTPS , SSH , SNMP , NETCONF , TELNET , and more. <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>
* IP Address/ Subnet Mask	Enter the IP address (IPv4 or IPv6) and subnet mask of the provider's server.
* Port	Enter the port number to use to connect to the provider's server. This is the port corresponding to the protocol being configured. For example, if the protocol used to communicate with the provider server is SSH, the port number is usually 22.
Timeout	Enter the amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.
Model Prefix Info	

Field	Description
* Model	<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>Cisco-IOS-XR</p> <p>Cisco-NX-OS</p> <p>Cisco-IOS-XE</p> <p>For telemetry, only Cisco-IOS-XR 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 Model Prefix Info section. To delete a model prefix you have entered, click the  shown next to that row.</p>
* Version	<p>Required only if you are adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the NSO server.</p>
Provider Properties	
Property Key	<p>Enter the name of the key for the special provider property you want to configure.</p> <p>Provider properties control how Cisco Crosswork Change Automation and Health Insights 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 Cisco Crosswork Change Automation and Health Insights does not validate provider properties. Make sure the properties you enter are valid for the provider.</p> <p>Note In a two network interface configuration, Cisco Crosswork Change Automation and Health Insights defaults to communicating with providers using the Management Network Interface (eth0). You can change this behavior by adding Property Key and Property Value as outgoing-interface and eth1 respectively. This is most often necessary when creating the SR-PCE provider, as its management interface may reside on the data network instead of the management network.</p>
Property Value	<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 Provider Properties section. To delete a key/value pair you have entered, click  shown next to that pair.</p>

Import Providers

Complete the steps below to create a CSV file that specifies providers and then import it into Cisco Crosswork Change Automation and Health Insights.

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 188](#)).

Step 1 From the main menu, choose **Admin > Providers**.

Step 2 Click  to open the **Import CSV File** dialog box.

Step 3 If you have not already created a provider CSV file to import:

- a) Click the **Download sample 'Provider template (*.csv)' file** link and save the CSV file template to a local storage resource.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each provider.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate entries with semicolons, the order in which you enter values is important. For example, if you enter **SSH ; SNMP ; NETCONF ; TELNET** in the **connectivity_type** field and you enter **22 ; 161 ; 830 ; 23** in the **connectivity_port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830
- Telnet: port 23

Field	Description	Required or Optional
Provider Name	Enter the name for the provider that will be used in Cisco Crosswork Change Automation and Health Insights. For example: MyWAE . The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.	Required
Connectivity Type	Enter the name of the protocol that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. Valid values are: ROBOT_MSVC_TRANS_TCP, ROBOT_MSVC_TRANS_UDP, ROBOT_MSVC_TRANS_HTTP, ROBOT_MSVC_TRANS_HTTPS, ROBOT_MSVC_TRANS_GRPC, ROBOT_MSVC_TRANS_SSH, ROBOT_MSVC_TRANS_NETCONF, ROBOT_MSVC_TRANS_TELNET, ROBOT_MSVC_TRANS_SNMP, ROBOT_MSVC_TRANS_TL1, ROBOT_MSVC_TRANS_TL1_SECURE, ROBOT_MSVC_TRANS_ICMP, ROBOT_MSVC_TRANS_KAFKA, ROBOT_MSVC_TRANS_NATS.	Required
Connectivity IP	Enter the IP address (IPv4 or IPv6) of the provider.	Required
Connectivity Port	Enter the port number to use to connect to the provider's server.	Required
Connectivity Timeout	Enter the amount of time (in seconds) to wait before the connection to the provider times out. The default is 30 seconds.	Required
Credential Profile	Enter the name of the credential profile that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. This profile must already exist in the system.	Required

Field	Description	Required or Optional
Provider Device Key	<p>Enter the enum value corresponding to the key that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way Cisco Crosswork Change Automation and Health Insights maps the device to the Cisco NSO provider. Valid values are:</p> <ul style="list-style-type: none"> • ROBOT_PROVDEVKEY_HOST_NAME—If you are using the device hostname as the device ID within NSO, this value must match the hostname that is specified for the device in the inventory. • ROBOT_PROVDEVKEY_INVENTORY_ID—Use this enum value if the inventory ID is the device identifier for NSO. <p>This entry is only required if you are creating or updating a Cisco NSO provider.</p>	Required
Family	Enter the provider family. Valid entries are: WAE , SYSLOG_STORAGE , ALERT , SR_PCE , and NSO .	Required
Model Prefix	<p>If you are adding a Cisco NSO provider: Select the model prefix that matches the NED CLI used by the NSO server. Valid entries are: Cisco-IOS-XR, Cisco-NX-OS, Cisco-IOS-XE.</p> <p>For telemetry, only Cisco-IOS-XR is supported.</p>	Required for Cisco NSO providers only
Model Version	<p>If you adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the</p> <p>Required for Cisco NSO only server (should be 6.0.4).</p>	Required for Cisco NSO providers only
Properties	<p>Enter the name of the key for the special provider property you want to configure.</p> <p>See the documentation on adding individual providers for property key/value requirements. Cisco Crosswork Change Automation and Health Insights does not validate provider property key names or values. Make sure the properties you enter are valid for the provider.</p>	Required for some providers, otherwise optional

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

- c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

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

The provider information you imported should now be displayed in the **Providers** window.

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

Add Cisco NSO Providers

Cisco Network Services Orchestrator (Cisco NSO) providers supply device management and configuration maintenance services to Cisco Crosswork Change Automation and Health Insights.

Follow the steps below to add (through the UI) a Cisco NSO provider for Cisco Crosswork Change Automation and Health Insights. You can also add providers using CSV files (see [Import Providers, on page 175](#)).

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see [Create Credential Profiles, on page 82](#)).
- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology.



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

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

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

- Know the Cisco NSO server IP address and hostname.
- Confirm Cisco NSO device configurations (see [Sample Configuration for Devices in Cisco NSO, on page 93](#)).

Step 1 From the main menu, choose **Admin > Providers**.

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 that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO**.
- **Device Key:** Select the method that Cisco NSO uses to identify devices uniquely. This will serve as the way Cisco Crosswork Change Automation and Health Insights maps the device to Cisco NSO. Choices are: **NONE**, **INVENTORY_ID**, or **HOST_NAME**.
- Under Connection Type(s), **Protocol:** Select the protocol that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. **NETCONF** is usually preferred.
- **IP Address/Subnet Mask:** Enter the IP address (IPv4 or IPv6) and subnet mask of the Cisco NSO server.

- **Port:** Enter the port to use to connect to the Cisco NSO server. The default is **2022**.
- **Model:** Select the model (**Cisco-IOS-XR**, **Cisco-NX-OS**, or **Cisco-IOS-XE**) from the drop-down list and enter its associated NED driver version. Add a model for each type of device that will be used in the topology. If you have more than one, select  to add another supported model.
- **Version:** Enter the NED software version installed for the device model in NSO.

For more information on fields, see [Import Providers, on page 175](#).

b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

Step 4 When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

Add Cisco SR-PCE Providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers supply device discovery, management, configuration-maintenance and route-calculation services to Cisco Crosswork Change Automation and Health Insights. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices that are part of the topology using XR Topology Controller (XTC). 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 Change Automation and Health Insights 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 for Cisco Crosswork Change Automation and Health Insights.

Before you begin

You will need to:

- Create a credential profile for the Cisco SR-PCE provider (see [Create Credential Profiles, on page 82](#)). 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 Crosswork Change Automation and Health Insights server and Cisco SR-PCE.

- 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. Your options, set using the **Provider Properties** fields, are as follows:
 - **auto-onboard** is **off**: If you set these **Provider Properties** values, you will add or import devices manually. When Cisco SR-PCE discovers devices, the device data is recorded in the Cisco SR-PCE database, but is not registered in the Cisco Crosswork Change Automation and Health Insights Device Management database.
 - **auto-onboard** is **unmanaged**: If you set these **Provider Properties** values, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Change Automation and Health Insights Device Management database, with their configured state set to **unmanaged**. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the **managed** state later, you will need to download them as a CSV file (see [Export Network Devices, on page 103](#)), and modify the CSV file to add the SNMP and management IP address information. You can then update the auto-onboarded devices with this information by importing the modified CSV file (see [Import Network Devices, on page 94](#)). You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).
 - **auto-onboard** is **managed**: If you set these **Provider Properties** values, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Change Automation and Health Insights Device Management database, with their configured state set to **managed**. Their connectivity IP addresses will be set to their router IDs, and SNMP polling will be enabled. For successful SNMP polling, you will have to correct the connectivity IP address. You can do this by editing the device, or use the device CSV import feature to correct it. You will also need to add a second **Provider Properties** key/value pair, with the key **device-profile** and the value being the name of an SNMP credential profile for the new devices.
- If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:
 - Assign an existing credential profile for communication with the new managed devices.
 - The credential profile must be configured with an SNMP protocol.
- For high availability, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations .

Step 1 From the main menu, choose **Admin > Providers**.

Step 2 Click .

Step 3 Enter the following values for the Cisco SR-PCE provider fields:

a) Required fields:

- **Provider Name**: Name of the SR-PCE provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile**: Select the previously created Cisco SR-PCE credential profile.
- **Family**: Select **SR_PCE**. All other options should be ignored.
- **Protocol**: Select **HTTP**.

- **IP Address/ Subnet Mask:** Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Provider Properties:** Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
<code>auto-onboard</code>	<code>off</code> Note Use this option if you plan to manually (via UI or CSV import) enter all of your network devices.
<code>auto-onboard</code>	<code>unmanaged</code>
<code>auto-onboard</code>	<code>managed</code> Note This option is only supported on IPv4 deployments. If you enable this option for an IPv6 deployment, devices will still register as unmanaged in the inventory.
<code>device-profile</code>	The name of a credential profile that contains SNMP credentials for all the new devices. Note This field is necessary only if <code>auto-onboard</code> is set to <code>managed</code> or <code>unmanaged</code> .
<code>outgoing-interface</code>	<code>eth1</code> Note You have to set this only if you want to enable Cisco Crosswork Change Automation and Health Insights access to SR-PCE via the data network interface when using the two NIC configuration.

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 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 (**managed/unmanaged/off**) 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 page.
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 page.

Add Cisco WAE Providers

Cisco WAN Automation Engine (Cisco WAE) providers supply traffic and topology analysis to Cisco Crosswork Change Automation and Health Insights. 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 [About Adding Providers, on page 172](#)).

Before you begin

You will need to:

- Create a credential profile for the Cisco WAE provider (see [Create Credential Profiles, on page 82](#)). This should be a basic HTTP/HTTPS text-authentication credential (currently, MD5 authentication is not supported). If the Cisco WAE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP/HTTPS protocol.
- Know the name you want to assign to the provider. This is usually the DNS hostname of the Cisco WAE server.
- Know the Cisco WAE server IP address and port. The connection protocol will be HTTP or HTTPS.

Step 1 From the main menu, choose **Admin > Providers**.

Step 2 Click .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name:** Name of the Cisco WAE provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **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 **8083** 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 KPI monitoring, Playbook execution, and other operations (such as syslog storage).

Follow the steps below to use the UI to add one or more storage providers for Cisco Crosswork Change Automation and Health Insights. You can also add providers using CSV files (see [About Adding Providers, on page 172](#)).

Before you begin

You will need to:

- Create a credential profile for the storage provider (see [Create Credential Profiles, on page 82](#)). This should be an SSH or HTTPS credential, depending on the protocol you plan to use (SSH is recommended).
 - 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 or HTTPS.
 - Know the destination directory on the storage provider's server. You will need to specify this using the **Provider Properties** fields.
-

Step 1 From the main menu, choose **Admin > Providers**.

Step 2 Click .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name:** Name of the storage provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile:** Select the previously created storage credential profile.
- **Family:** Select **SYSLOG_STORAGE**.
- **Protocol:** Select the protocol that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. **SSH** or **HTTPS** are usually preferred.
- **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 or **443** for HTTPS).
- **Provider Properties:** Enter the following key/value pair in these fields:

Property Key	Property Value
<code>DestinationDirectory</code>	The absolute path where the collected data will be stored on the server. For example: <code>/root/cw-syslogs</code>

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 for Cisco Crosswork Change Automation and Health Insights. You can also add the alert provider by importing a CSV file (see [About Adding Providers, on page 172](#)).

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 82](#)). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the provider does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the alert provider. This is usually the DNS hostname of the server.
- Know the alert server IPv4 address and port. The connection protocol will be HTTP.
- Know the URL of the alert server endpoint. You will need to specify this using the **Property Value** field.

Step 1 From the main menu, choose **Admin > Providers**.

Step 2 Click .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name:** Name of the provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile:** Select the previously created alert provider credential profile.
- **Family:** Select **ALERT**.

- **Protocol:** **HTTP** is pre-selected.
- **IP Address/ Subnet Mask:** Enter the IP Address (IPv4 or IPv6) and subnet mask of the alert server.
- **Port:** Enter the port number (usually, 80 for HTTP).
- **Provider Properties:** The `alertEndpointUrl` property key name is pre-entered. In the Property Value field, enter the alert server endpoint only. For example, if the complete path to the endpoint is `http://aws.amazon.com:80/myendpoint/bar1/`, you would enter `/myendpoint/bar1/` only.

b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the alert server.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the alert provider.

Add Optimization Engine Providers

Follow the steps below to use the UI to add one or more instances of Optimization Engine as providers. You can also add providers using CSV files (see [About Adding Providers, on page 172](#)).

Before you begin

You will need to:

- Create a credential profile for the Optimization Engine provider (see [Create Credential Profiles, on page 82](#)). This should be a basic HTTPS text-authentication credential.
- Know the name you want to assign to the provider. This is usually the DNS hostname of the Optimization Engine server.
- Know the Optimization Engine server IP address and port. The connection protocol will be HTTPS.

Step 1 From the main menu, choose **Admin > Providers**.

Step 2 Click .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name:** Name of the Optimization Engine provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile:** Select the previously created credential profile.
- **Family:** Select **OPTIMIZATION ENGINE**.
- **Protocol:** Select **HTTPS**.
- **IP Address/ Subnet Mask:** Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port:** Enter the port number (usually, **30603** 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.

Get Provider Details

Use the **Providers** window to get details about your providers and to check on their reachability.

Step 1 From the main menu, choose **Admin > Providers**.

For each provider configured in Cisco Crosswork Change Automation and Health Insights, the **Providers** window lists information such as the provider's name, universally unique identifier (UUID), associated credential profile, device key, and more, as shown in the figure below.

Figure 20: Providers Window

Providers										
										Selected 0 / Total 4
										Clear Filter
Rea...	...	Provide...	UUID	Credenti...	Connecti...	Provider D...	Family	Model Prefix	Model Version	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="lock"/>	xtc-CE2 <i>i</i>	5841cb3d-92b6-312c-8b7...	XTC1-CE2	HTTP <i>i</i>	SR_PCE			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="lock"/>	xtc-CE4 <i>i</i>	313b3a98-36e8-3ec1-90b...	XTC1-CE2	HTTP <i>i</i>	SR_PCE			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="lock"/>	NSO179 <i>i</i>	de20c619-55e8-3f70-84f1...	NSO-Cred	NETCONF <i>i</i>	NODE_IP	NSO	Cisco-IOS-XR <i>i</i>	6.6.2
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="lock"/>	Syslog <i>i</i>	6e9a49a1-1054-3758-85c...	syslog	SSH <i>i</i>	SYSLOG_STOR...			

Step 2 The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols. For a description of each icon and its meaning, see [Reachability and Operational State, on page 79](#).

Cisco Crosswork Change Automation and Health Insights checks provider reachability immediately after a provider is added or modified. Other than these events, Cisco Crosswork Change Automation and Health Insights checks reachability every 5 minutes.

Step 3 Get additional details for any provider, as follows:

- In the **Provider Name** column, click the *i* to view provider-specific key/value properties.
- In the **Connectivity Type** column, click the *i* 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 *i* 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 **X** to close the details window.

If you are running into 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. For an SR-PCE provider, it is typically HTTP and port 8080.

The following CLI command can be used to perform this check:

```
curl -v -H "X-Subscribe: stream" "http://<ip-address>:8080/  
bwod/subscribe/json?keepalive-30&priority=5"
```

- c. Check your firewall setting and network configuration.
- d. Check the provider host or intervening devices for Access Control List settings that might limit who can connect.

Edit Providers

When editing provider settings, be aware that a provider can be mapped to many devices, even thousands of devices in a large network.



Note

- Before making any changes to a provider configuration you should be certain that you understand the full impact of the change. If you are unsure about the potential risk of making a change, contact Cisco services for guidance.
- See [Add Cisco SR-PCE Providers, on page 179](#) 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 188](#)).

-
- Step 1** From the main menu, choose **Admin > Providers**.
 - Step 2** In the **Providers** window, choose the provider you want to update and click .
 - Step 3** Make the necessary changes and then click **Save**.
 - Step 4** Resolve any errors and confirm provider reachability.

Delete Providers

Follow the steps below to delete a provider.

You are alerted when you try to delete a provider that is associated with one or more devices or credential profiles.

-
- Step 1** Export a backup CSV file containing the provider you plan to delete (see [Export Providers, on page 188](#)).
 - Step 2** (Optional) Check whether any devices are mapped to the provider and change the provider before deletion.
 - a) From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed by default.
 - b) In the **Network Devices** window, enter the obsolete provider name in the **Search** field.
 - c) Check the check box for the device that is mapped to the obsolete provider, and click .
 - d) Choose a different provider from the **Provider** drop-down list.

e) Click **Save**.

Step 3 Delete the provider as follows:

- a) From the main menu, choose **Admin > Providers**.
- b) In the **Providers** window, choose the provider(s) that you want to delete and click .
- c) In the confirmation dialog box, click **Delete**.

Export Providers

You can quickly export provider data to a CSV file. This is a handy way to keep backup copies of your provider information.



Note You cannot edit a CSV file and then re-import it to update existing providers.

Step 1 From the main menu, choose **Admin > Providers**.

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.

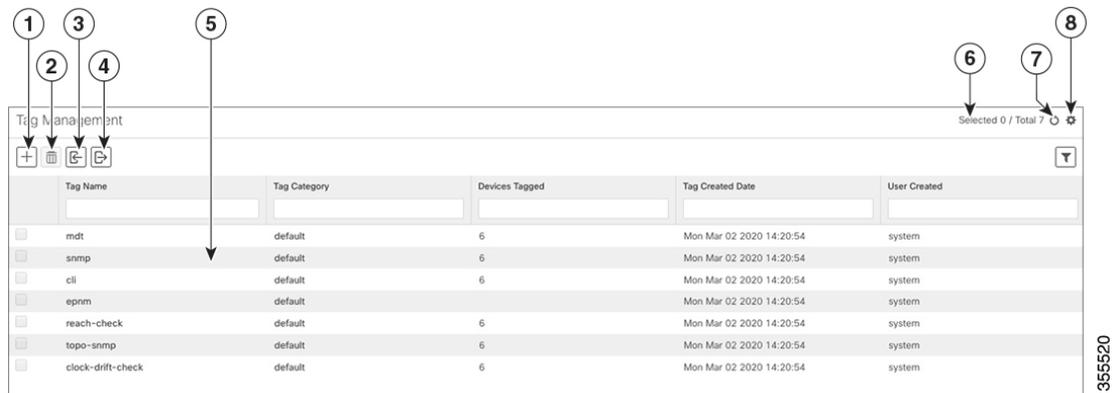
To open this window, choose **Admin > Tags** from the Cisco Crosswork Change Automation and Health Insights main window.



Note Cisco Crosswork Change Automation and Health Insights automatically creates a default set of tags and assigns them to every device it manages:

- cli
- mdt
- reach-check
- snmp
- clock-drift-check

You cannot select, edit, delete, or manually associate these default tags with any device.



Item	Description
1	Click to create new device tags. See Create Tags .
2	Click to delete currently selected device tags. See Delete Tags .
3	Click to import the device tags defined in a CSV file into Cisco Crosswork Change Automation and Health Insights. See Import Tags, on page 190 . 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 Cisco Crosswork Change Automation and Health Insights to quickly add or edit multiple tags. See Export Tags, on page 192 .
5	Displays the tags currently available in Cisco Crosswork Change Automation and Health Insights and their attributes.
6	Indicates the number of tags that are currently selected in the table.
7	Click to refresh the Tag Management window.

Item	Description
8	Click  to choose the columns to make visible in the Tag Management window (see Set, Sort and Filter Table Data, on page 6).
	Click  to set filter criteria on one or more columns in the Tag Management window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Create Tags

You can create as many tags and tag categories as you want. If you will have many tags, it might be quicker to list them in a CSV file and import the file, instead of creating each tag individually. See [Import Tags, on page 190](#).



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.

Step 1 From the main menu, choose **Admin > 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 191](#).

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 Cisco Crosswork Change Automation and Health Insights. 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 192](#)).

Step 1 From the main menu, choose **Admin > Tags**.

Step 2 Click  to open the **Import CSV File** dialog box.

Step 3 If you have not already created a CSV file to import:

- a) Click the **Download sample 'Tags template (*.csv)' file** link and save the CSV file template to a local storage resource.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each tag. Use a comma to delimit each field within a row. Use a semicolon to separate multiple entries in the same field.

Field	Description	Required or Optional
Tag Name	Enter the name of the tag. For example: SanFrancisco or Spine/Leaf .	Required
Tag Category	Enter the tag category. For example: City or Network Role .	Required

Note **Tag Name** and **Tag Category** fields are case-insensitive and can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

- c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

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

The tags and tag categories that you imported should now be displayed in the **Tag Management** window.

What to do next

Add tags to devices. See [Apply or Remove Device Tags, on page 191](#).

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 190](#)).

For efficiency, Cisco Crosswork Change Automation and Health Insights automatically updates inventory data, including topology, for all the devices in a tagged group, as a single set of inventory collection jobs. But please note that tag-group membership is static for other functions. For example, if you add or remove a device from a tagged group after applying a KPI, the KPI will monitor only the original group members. If you

change group membership and want the KPI to monitor all the members of the group, re-apply the KPI to the changed group.

You can apply a maximum of 15 tags to any one device.

To apply tags to a device or set of devices, do the following:

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

Use caution when deleting existing tags. They are used to group devices and deleting them can affect which KPIs are being monitored and the Playbooks run on them.

To delete device tags, do the following:



Note If the tag is mapped to any devices, then the tag cannot be deleted.

-
- Step 1** Export a backup CSV file containing the tags you plan to delete (see [Export Tags, on page 192](#)).
 - Step 2** From the main menu, choose **Admin > Tags**. The **Tag Management** window is displayed.
 - Step 3** Check the check box next to the tags you want to delete.
 - Step 4** From the toolbar, click .
 - Step 5** The confirmation dialog box will list the number of devices currently using the tag(s) you are about to delete. Click **Delete** to confirm deletion.
-

Export Tags

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

-
- Step 1** From the main menu, choose **Admin > 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.
-

Define Network Visualization Display Settings

Cisco Crosswork Change Automation and Health Insights administrator privileges are required to configure the display settings that are used by the Network Visualization application.

For a description of how to configure these settings, see the following topics:

- [Define Color Thresholds for Link Bandwidth Utilization](#)
- [Configure Geographical Map Settings, on page 75](#)

Manage Certificates

The Cisco Crosswork Change Automation and Health Insights VM-hosted server and its browser-based user interface communicate with each other using SSL certificates exchanged over HTTPS. For details about these protocols, see [SSL Certificates, on page 203](#) and [HTTPS, on page 203](#)

When installed, Cisco Crosswork Change Automation and Health Insights secures these interactions using a self-signed TLS certificate. This certificate has a two-year lifespan, after which it expires. If you want to continue using the expired self-signed certificate to secure server/client communications, you will need to regenerate it by following the steps in [Extend Self-Signed Certificate Expiration, on page 194](#)

If you prefer to secure these communications with a user-provided certificate, either purchased from a Certificate Authority (CA) or self-signed by your organization, you can validate and upload it by following the steps in [Substitute a User-Provided Certificate, on page 195](#).

The user-provided certificate must meet the following requirements:

- Cisco Crosswork Change Automation and Health Insights supports IP Subject Alternative Name (SAN) server certificates only. The IP address is the primary means to reach the user interface.
- The server will present your user-provided certificates to the browser, so the certificates you supply must be valid both for Cisco and for Cisco Crosswork Change Automation and Health Insights.
- It must also include the required fields and field values shown in the following table.

Table 22: Required User-Provided Certificate Fields and Values

Field	Description	Value
<NUMBER OF DAYS>	Number of days the certificate will be valid.	Must be greater than 30 days and less than 730 days (or two years)
<COUNTRY>	Country (C=)	US
<STATE>	State (ST=)	CALIFORNIA
<LOCATION>	Location (L=)	SAN JOSE
<ORGANIZATION>	Organization (O=)	CISCO SYSTEMS INC
<ORGANIZATIONAL UNIT NAME>	Organizational Unit (OU=)	CROSSWORK
<COMMON NAME>	Common Name (CN=)	The IP address of the Cisco Crosswork Change Automation and Health Insights server VM.

- The certificate must also have the SAN extension set, with both DNS and IP address keys. The following provides an example of how to generate a self-signed certificate using OpenSSL:

```

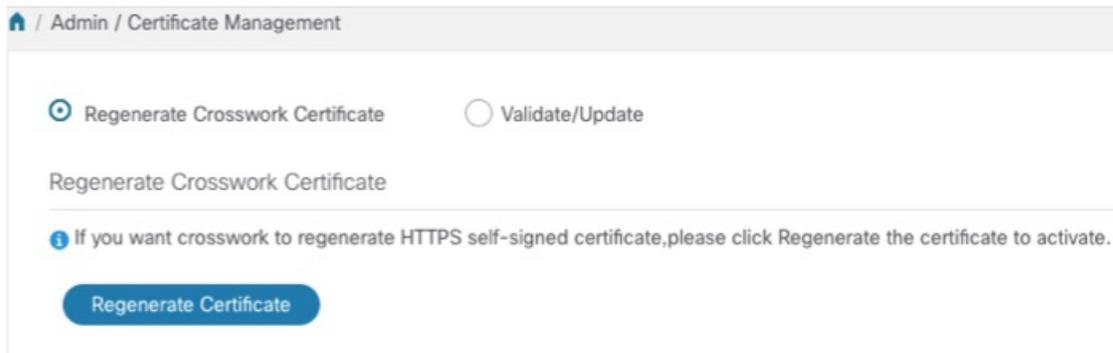
/usr/bin/openssl req \
    -x509 \
    -nodes \
    -days 730 \
    -newkey rsa:4096 \
    -keyout "filename.key" \
    -out "filename.crt" \
    -subj "/C=US/ST=CALIFORNIA/L=SAN JOSE/O=CISCO SYSTEMS
INC/OU=CROSSWORK/CN=1.1.1.1" \
    -extensions SAN \
    -config <(cat /etc/ssl/openssl.cnf \
    <(printf "\n[SAN]\nsubjectAltName=DNS:0.0.0.0,IP:1.1.1.1"))

```

Extend Self-Signed Certificate Expiration

Follow these steps to regenerate the self-signed certificate and extend its lifetime by two years.

-
- Step 1** From the main menu, select **Admin > Certificate Management**. The **Certificate Management** window appears.
- Step 2** Select the **Regenerate Crosswork Certificate** radio button.



Step 3 When you are ready, click **Regenerate Certificate**.

When Cisco Crosswork Change Automation and Health Insights has finished regenerating the certificate, it displays an alert message indicating that the regeneration operation is successful and you will be logged out. You must log in again to continue using Cisco Crosswork Change Automation and Health Insights.

Note In certain situations, your internet browser may fail to load the GUI page contents after a Cisco Crosswork Change Automation and Health Insights certificate regeneration, even if you try to log out and login again. You may also see invalid certificate errors or authentication errors. To prevent these errors, you need to refresh the browser after a certificate regeneration, specially if the browser is in incognito or private browsing mode.

Substitute a User-Provided Certificate

Follow the steps below to validate and upload a user-provided certificate. The certificate must meet the requirements explained in [Manage Certificates, on page 193](#).

Before you begin

You must know the names of the user-provided certificate and key files and their locations in your local storage.

Step 1 From the main menu, select **Admin > Certificate Management**. The **Certificate Management** window appears.

Step 2 Select the **Validate/Update** radio button.

Step 3 Use the **Browse** button next to each field to browse to and select the key and certificate files you want to validate and use.

Admin / Certificate Management

Regenerate Crosswork Certificate
 Validate/Update

Validate/Update Certificate

! You can upload new Certificate here. once you upload the files,it will be validated and updated.

Key File*

foo.key

Cert File*

foo.crt

Step 4 Click **Validate** to validate the certificate and key files.

Step 5 Click **Update** to replace the existing certificate with the user-provided certificate you have validated.

Smart Licensing Registration

This section provides an overview of the Cisco Smart Licensing feature integrated with the Cisco Crosswork Change Automation and Health Insights and describes the instructions to complete the product registration.

Overview

Smart Licensing is a software based end-to-end license platform that comprises several tools and processes that authorizes customers to use Cisco products. Smart Licensing provides a software inventory management system that provides Customers, Cisco, and selected Partners with information about Software Ownership and Software Utilization.

A **Cisco Smart Account** provides the repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage and track Cisco purchases. The **Cisco Smart Software Manager (CSSM)** enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you may create and manage multiple virtual accounts within your Smart Account to manage licenses. For more information, see <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html>

From the main menu, select **Admin > Smart Licensing Registration** to display the **Smart Software Licensing** window. Using this window, you can register your Cisco Crosswork Change Automation and Health Insights application, edit the transport settings, renew the license, and de-register your application.

Prerequisites for Smart Licensing Registration

You should have:

- A Cisco Smart Account.
- Purchased licenses for the Cisco Crosswork Change Automation and Health Insights application.

Configure Transport Settings

You can configure the transport settings to decide how Cisco Crosswork Change Automation and Health Insights communicates with the Cisco servers.

- **Direct:** The application directly connects with Cisco Smart Software Manager (CSSM).
- **Transport Gateway:** The application communicates via a Transport Gateway or CSSM on-prem, which replicates the cloud-based user experience but keeps all communication on premises.



Note For more information on the CSSM on-prem option, see the [Smart Software Manager guide](#).

- **HTTP/HTTPS Gateway:** The application connects via an intermediate proxy server. This is applicable only for Direct mode.



Note Transport Settings cannot be changed while the Cisco Crosswork Change Automation and Health Insights is in Registered mode. You have to de-register to change them.

Step 1

In the **Smart Software Licensing** window, the Transport Settings display the current transport mode selected. To modify, click **View/Edit**.

The **Transport Settings** dialog box is displayed.

Transport Settings
×

Configure how the product will communicate with Cisco. Note that this setting is shared with Smart Call Home, so any changes made here will apply to other features using this service.

Direct - product communicates directly with Cisco's licensing servers
URL :

Transport Gateway - proxy data via Transport Gateway or On Prem Smart Software Manager
URL :

HTTP/HTTPS Gateway - send data via an intermediate HTTP or HTTPS proxy
IP Address :
Port :

Step 2 Select the relevant transport mode and make relevant entries in the fields provided.

Step 3 Click **Save**.

Register Cisco Crosswork Change Automation and Health Insights

To enable licensed features, Cisco Crosswork Change Automation and Health Insights must be registered to CSSM using a registration ID token. Once registered, an Identity Certificate is saved securely in the Smart Account and used for all ongoing communications. The certificate is valid for one year and will be renewed automatically after six months to ensure continuous operation.

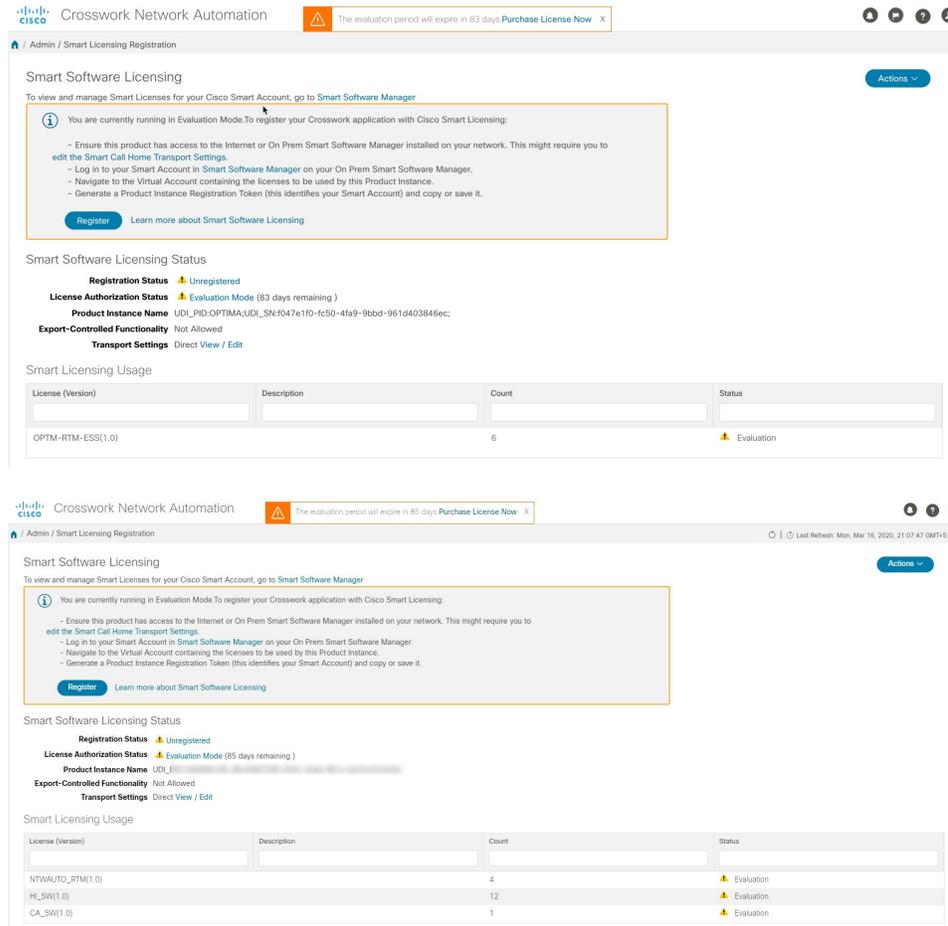


Note For information on generating the registration token, please refer to the support resources provided in the [Smart Software Manager](#) webpage.

Step 1 From the main menu, select **Admin > Smart Licensing Registration** to display the **Smart Software Licensing** window. The registration status

The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 21: Smart Software Licensing Unregistered



Step 2 In the **Smart Software Licensing** window, click **Register**.
The **Smart Software Licensing Product Registration** dialog box is displayed.

Smart Software Licensing Product Registration ×

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

Register Cancel

Step 3 In the **Product Instance Registration Token** field, enter the registration token generated from your Smart Account. Make sure the token ID is accurate and within validity period. For more information, see https://www.cisco.com/c/en_in/products/software/smart-accounts/software-licensing.html.

Step 4 (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** checkbox.

Note After a backup restore or disaster restore operation, you must manually re-register the Cisco Crosswork Change Automation and Health Insights VM to CSSM. This is applicable in case of a Cisco Crosswork Change Automation and Health Insights 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.

Admin / Smart Licensing Registration Last Refresh: Mon, Mar 16, 2020, 21:07:47 GMT+5:30

Smart Software Licensing Actions

To view and manage Smart Licenses for your Cisco Smart Account, go to Smart Software Manager

Smart Software Licensing Status

- Registration Status** ✔ Registered (Dec 17, 2019)
- License Authorization Status** ✔ Authorized (Dec 18, 2019)
- Smart Account** InternalTest1
- Virtual Account** Crosswork
- Product Instance Name** _____
- Export-Controlled Functionality** Allowed
- Transport Settings** Direct View / Edit

Smart Licensing Usage

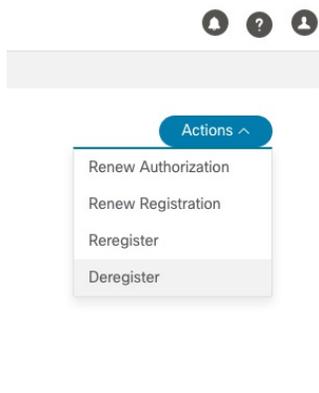
License (Version)	Description	Count	Status
Network Auto RTM(1.0)	Network Automation Right To Manage	20	✔ In_Compliance
Health Insights(1.0)	Telemetry driven KPI monitoring	45	✔ In_Compliance
Change Automation(1.0)	Playbook driven closed loop remediation	1	✔ In_Compliance

- Note**
- If you encounter a communication timeout error during registration, click **OK** in the error dialog box and the application will reattempt the registration.
 - In some cases, after successful registration, the page may need to be refreshed manually to see the updated status.

Manual Actions

The renewal of registration and authorization are automatically enabled for Cisco Crosswork Change Automation and Health Insights, by default. However, in the event of a communication failure between the application and the Cisco server, these actions can be manually initiated. You can use the **Actions** drop-down button to manually renew, re-register and de-register the application.

- Step 1** In the **Smart Software Licensing** window, click **Actions** drop-down button and select the relevant option for the following quick actions.



- Actions > Renew Authorization:** To renew the authorization manually if the automatic renewal service fails at the end of 30 days.
- Actions > Renew Registration:** To renew the registration manually if the automatic renewal service fails at the end of 6 months.
- Actions > Re-register:** Re-register the application, for example, on account of the expiry of registration tokens.
- Actions > De-register:** De-register the application, for example, when the transport settings need to be changed.

Note Once de-registered, the Cisco Crosswork Change Automation and Health Insights 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 202](#)

- Step 2** The selected action is executed successfully.
-

License Authorization Statuses

Based on the registration status of your Cisco Crosswork Change Automation and Health Insights application, you can see the following License Authorization Statuses.

Table 23: 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.

Security Hardening Overview

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- Cisco Crosswork Change Automation and Health Insights infrastructure
- Cisco Crosswork Change Automation and Health Insights storage system (local or external)

Hardening Cisco Crosswork Change Automation and Health Insights security requires completion of the following tasks:

- Shutting down insecure and unused ports
- Configuring network firewalls

- Hardening the Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights.

Authentication Throttling

Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights 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 Change Automation and Health Insights 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.

SSL Certificates

SSL 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 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 Change Automation and Health Insights server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.



Note A client might need to store multiple server certificates to enable interaction with multiple servers.



To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that

created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

Disable Insecure Ports and Services

As a general policy, any ports that are not needed should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco Crosswork Change Automation and Health Insights. You can do this by listing the ports that are open and comparing it with a list of ports needed for Cisco Crosswork Change Automation and Health Insights.

To view a list of all open listening ports:

Step 1

Log in as a Linux CLI admin user and enter the **netstat -aln** command.

The **netstat -aln** command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. The command returns output similar to the following:

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:10248         0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:10249         0.0.0.0:*               LISTEN
tcp    0      0 192.168.125.114:40764   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:48714   192.168.125.114:10250   CLOSE_WAIT
tcp    0      0 192.168.125.114:40798   192.168.125.114:2379    ESTABLISHED
tcp    0      0 127.0.0.1:33392         127.0.0.1:8080          TIME_WAIT
tcp    0      0 192.168.125.114:40814   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:40780   192.168.125.114:2379    ESTABLISHED
tcp    0      0 127.0.0.1:8080          127.0.0.1:44276         ESTABLISHED
tcp    0      0 192.168.125.114:40836   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:40768   192.168.125.114:2379    ESTABLISHED
tcp    0      0 127.0.0.1:59434         127.0.0.1:8080          ESTABLISHED
tcp    0      0 192.168.125.114:40818   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:22      192.168.125.1:45837     ESTABLISHED
tcp    0      0 127.0.0.1:8080          127.0.0.1:48174         ESTABLISHED
tcp    0      0 127.0.0.1:49150         127.0.0.1:8080          ESTABLISHED
tcp    0      0 192.168.125.114:40816   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:55444   192.168.125.114:2379    ESTABLISHED
```

Step 2

Check the *Cisco Crosswork Change Automation and Health Insights Installation Guide* for the table of ports used by Cisco Crosswork Change Automation and Health Insights, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product*.

Note If you are not sure whether you should disable a port or service, contact your Cisco representative.

Step 3

If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork Change Automation and Health Insights to operate.

Harden Your Storage

We recommend that you secure all storage elements that will participate in your Cisco Crosswork Change Automation and Health Insights installation, such as the database, backup servers, and so on.

- If you are using external storage, contact your storage vendor and your Cisco representative.
- If you are using internal storage, contact your Cisco representative.
- If you ever uninstall or remove Cisco Crosswork Change Automation and Health Insights, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted). Contact your Cisco representative for more information.



CHAPTER 8

Manage Cisco Crosswork Data Gateway

Networks maintain a large amount of data that spans thousands of devices. Cisco Crosswork Change Automation and Health Insights Collection Service collects and manages this data through its integral component - Cisco Crosswork Data Gateway.

This section contains the following topics:

- [Overview of Cisco Crosswork Data Gateway, on page 207](#)
- [Manage Cisco Crosswork Data Gateway Instances, on page 208](#)
- [Configure Cisco Crosswork Data Gateway Settings, on page 223](#)

Overview of Cisco Crosswork Data Gateway

When Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway are deployed together, Cisco Crosswork Change Automation and Health Insights acts as the **controller application** for the Cisco Crosswork Data Gateway instance. You can use the UI to add and manage additional instances of Cisco Crosswork Data Gateway no matter if they are forwarding data to Cisco Crosswork Change Automation and Health Insights or other compatible data consumers. The number of Cisco Crosswork Data Gateway you need depends on the number of devices being supported, the amount of data being processed and your network architecture.

Cisco Crosswork Data Gateway can also be deployed with other Crosswork products and in that case, will have a different controller application.



Note This chapter explains only the Cisco Crosswork Data Gateway features that can be accessed via Cisco Crosswork Change Automation and Health Insights UI.

For more information about Cisco Crosswork Data Gateway VM and how to manage it, see **Appendix B: Configure Cisco Crosswork Data Gateway Base VM, on page 279**.

We also recommended that you read about components of Cisco Crosswork Data Gateway at [Cisco Crosswork Data Gateway Components, on page 282](#) before moving further.

Manage Cisco Crosswork Data Gateway Instances

Cisco Crosswork Data Gateway is initially deployed with just a basic VM called the Base VM (containing only enough software to register itself with its controller).

It follows the instructions from Crosswork - collects data as requested and sends it to the defined output destination.

Depending on your private network's size and configuration, you may require one or more Cisco Crosswork Data Gateway instances for collection. It may be necessary to deploy multiple Cisco Crosswork Data Gateway instances to address the requirements for:

1. Geo-separated regions
2. Massive scale

Cisco recommends the simplest approach of a fixed configuration of devices to a particular instance (such as x to y for CDG1 and (y+1) to z for CDG2).



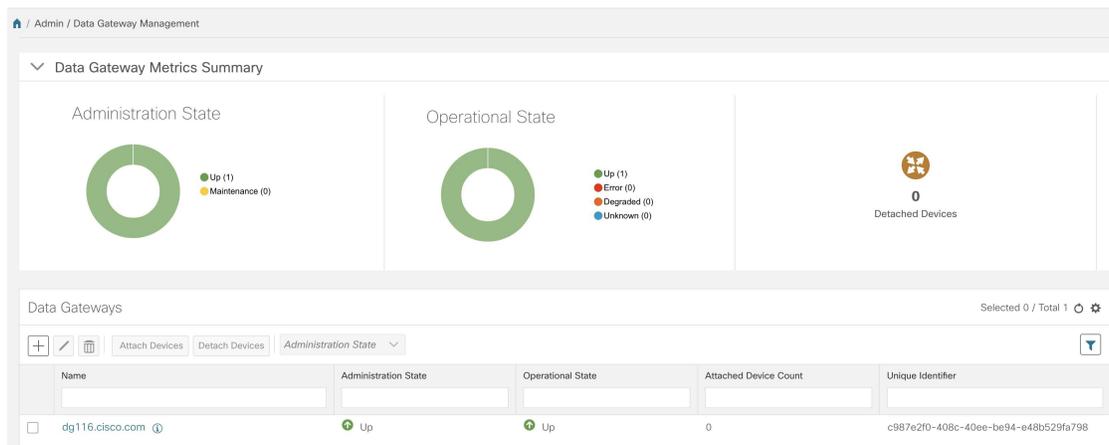
Note

More complicated approaches for resource optimization and dynamic assignment of tasks are possible and if desired, we recommend working with Cisco Customer Experience team to design the behavior.

Cisco Crosswork Data Gateway features can be accessed via Crosswork Network Automation UI.

To open Cisco Crosswork Data Gateway management view, choose **Admin > Data Gateway Management** from the left navigation bar in the Crosswork Network Automation UI.

Figure 22: Data Gateway Management View

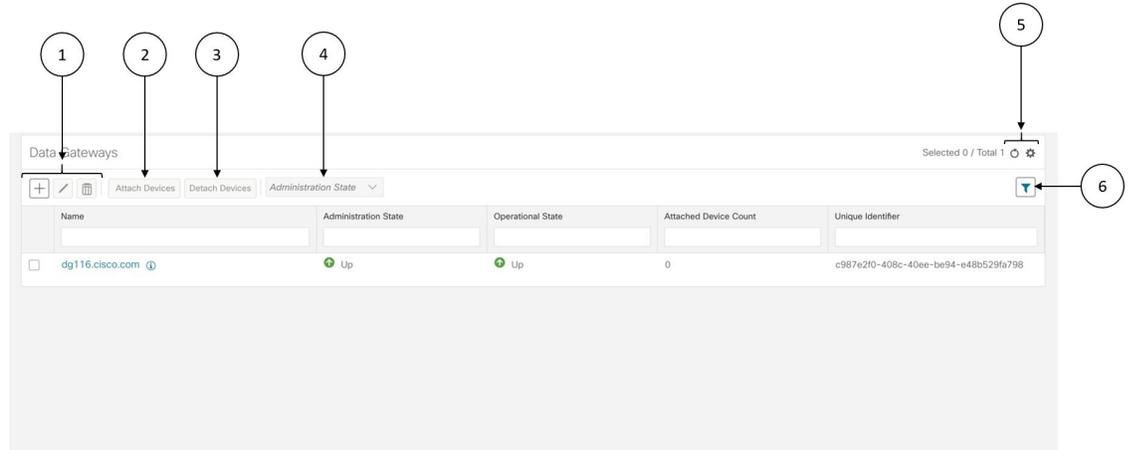


Item	Description
Data Gateway Metrics Summary Pane	<p>Summarizes the overall metrics of all Cisco Crosswork Data Gateway instances currently enrolled with Crosswork:</p> <ul style="list-style-type: none">• Administration State Tile: shows the number of Cisco Crosswork Data Gateway instances in each administration state i.e., Up and Maintenance.• Operational State Tile: shows the number of Cisco Crosswork Data Gateway instances in each operational state i.e., Up, Error, Degraded, and Unknown.• Detached Devices Tile: Shows the number of devices that are currently not attached to any Cisco Crosswork Data Gateway instance.

Item	Description
<p>Data Gateways Pane</p>	<p>Provides options to add, edit, and delete Cisco Crosswork Data Gateway VMs, attach/detach devices, change administration state, and filter options.</p> <p>It also displays the following details for the individual Cisco Crosswork Data Gateway instances:</p> <ul style="list-style-type: none"> • Name: Name of the Cisco Crosswork Data Gateway VM. • Administration State: Administration state of the Cisco Crosswork Data Gateway VM. A Cisco Crosswork Data Gateway VM has either of the two states at a time: <ul style="list-style-type: none"> •  Up: The VM is currently active. •  Maintenance: The VM is not operational ("down") and has been set to "Maintenance" mode by the user. No new jobs are submitted to Cisco Crosswork Data Gateway while it is in this mode. However, the currently running collection jobs do not stop. • Operational State: Operational state of the Cisco Crosswork Data Gateway VM. A Crosswork Data Gateway VM has either of the four states at a time: <ul style="list-style-type: none"> •  Up: The VM is operational and all individual components are "OK". •  Error: <p>The VM's operational state is in an error condition. It is either not reachable or all the critical components on the VM are "not OK".</p> •  Degraded: <p>The VM's operational state is degraded as one or more critical components on the VM are "not OK".</p> •  Unknown: <p>The VM's operational state is unknown as it has enrolled itself with Crosswork, but hasn't established a session yet.</p>

From the **Data Gateways** pane, you can add a new Cisco Crosswork Data Gateway instance, update the settings configured for an existing instance, de-enroll an instance, attach devices to an instance, detach devices from a instance, or change administration state of an instance.

Figure 23: Data Gateways Pane



Item	Description
1	Click to add a Cisco Crosswork Data Gateway VM. See Add a Cisco Crosswork Data Gateway Instance , on page 212.
	Click to edit the settings for the selected Cisco Crosswork Data Gateway VM. See Update Cisco Crosswork Data Gateway Instance Enrollment Settings , on page 212.
	Click to de-enroll the selected Cisco Crosswork Data Gateway VM. See De-enroll a Cisco Crosswork Data Gateway Instance , on page 216.
2	Click Attach Devices to attach devices to the selected Cisco Crosswork Data Gateway VM. See Attach a Device to a Cisco Crosswork Data Gateway Instance , on page 217.
3	Click Detach Devices to detach devices from the selected Cisco Crosswork Data Gateway VM. See Detach a Device From a Cisco Crosswork Data Gateway Instance , on page 219.
4	Click Administration State to switch administration state of the selected Data Gateway VM. See Change the Administration State of a Cisco Crosswork Data Gateway Instance , on page 215.
5	Click to refresh the Data Gateways window.
	Click to choose the columns to make visible in the Data Gateways window (see Set, Sort and Filter Table Data , on page 6).
6	Click to show/hide the quick filters.
	Click the Clear All Filters link to clear any filter criteria you may have set.

The **Data Gateways** pane displays the following details of the enrolled Cisco Crosswork Data Gateway instances:

Field	Description
Name	Name of the Cisco Crosswork Data Gateway.
Administration State	Administration state of the Cisco Crosswork Data Gateway instance.
Operational State	Operational state of the Cisco Crosswork Data Gateway instance.
Attached Device Count	Number of devices attached to the Cisco Crosswork Data Gateway instance.
Unique Identifier	Unique identifier of the Cisco Crosswork Data Gateway instance.

Add a Cisco Crosswork Data Gateway Instance

After installing Cisco Crosswork Data Gateway, you must enroll it with Cisco Crosswork Change Automation and Health Insights.

Steps to enroll a Cisco Crosswork Data Gateway instance is described in *Cisco Crosswork Change Automation and Health Insights 3.2 Installation Guide* in Section: **Enroll Cisco Crosswork Data Gateway With Cisco Crosswork Change Automation and Health Insights**

After enrolling, you must verify that the operational state of the Cisco Crosswork Data Gateway instance is **Up** before beginning to use it.



Note Watch out for "alerts" at the top of the **Data Gateway** page while the Cisco Crosswork Data Gateway is not operationally up.

Update Cisco Crosswork Data Gateway Instance Enrollment Settings

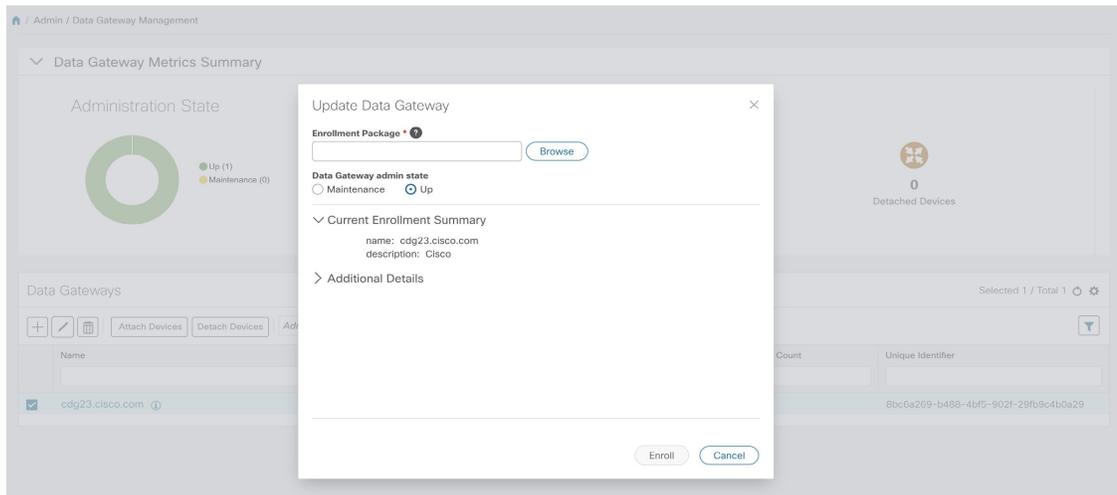
If there's an update for the Cisco Crosswork Data Gateway VM, you can regenerate a new enrollment package and upload it to Crosswork by following these steps:

Before you begin

Ensure that you have manually copied the new enrollment package to your local PC as per the procedure described in the *Cisco Crosswork Change Automation and Health Insights 3.2 Installation Guide* in Section: *Export Enrollment Package*.

-
- Step 1** From the main menu, choose **Admin > Data Gateway Management**. The **Data Gateway Management** view opens.
 - Step 2** From the **Data Gateways** window, select the Cisco Crosswork Data Gateway instance you want to update.
 - Step 3** Click  to edit the settings for the selected Cisco Crosswork Data Gateway instance.

- Step 4** In the **Update Data Gateway** pop up, click **Browse** to select the new enrollment package. Select the admin state in which you want to bring up the Cisco Crosswork Data Gateway instance.



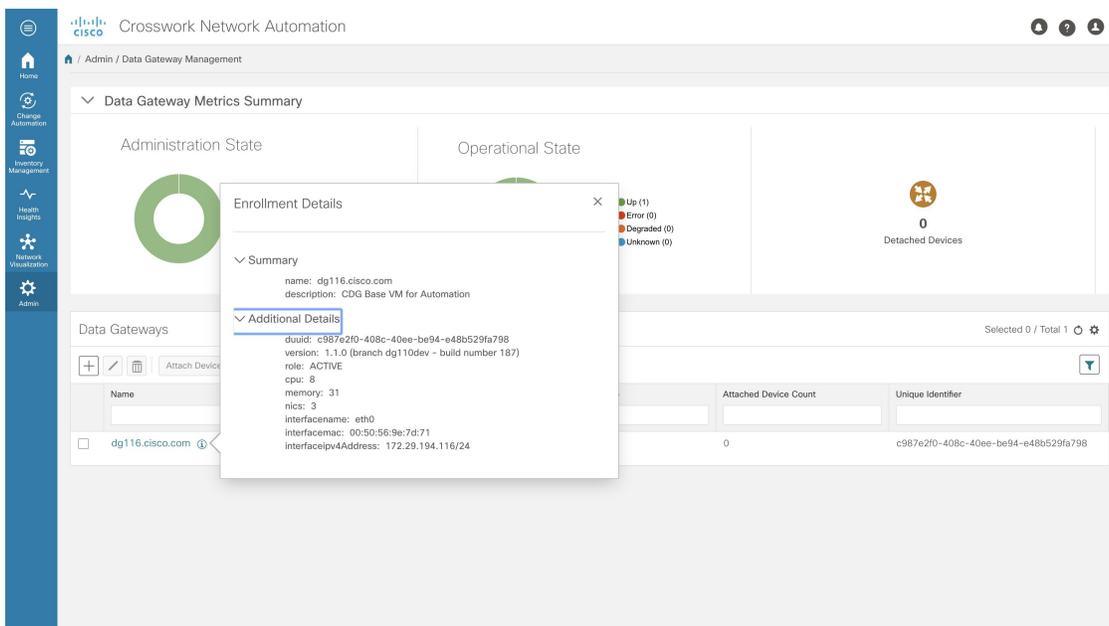
- Step 5** Click **Enroll**.

View Enrollment Details

To view enrollment details of a Cisco Crosswork Data Gateway instance, in the **Data Gateways** pane, click  icon next to the Cisco Crosswork Data Gateway name as shown in the following figure.



Note Some of these details are the OVF parameters that were configured in the OVA Template while installing Cisco Crosswork Data Gateway. For description of these parameters, see Section: **Install Crosswork Data Gateway** in *Cisco Crosswork Change Automation and Health Insights 3.2 Installation Guide*.



Following enrollment details are displayed:

Field	Description
Summary	
name	Name of the Cisco Crosswork Data Gateway instance.
description	User-friendly description to be displayed in the controller i.e., Crosswork.
Additional Details	
duuid	Unique identifier for the Cisco Crosswork Data Gateway instance.
version	Currently installed version of Cisco Crosswork Data Gateway.
role	Is the Cisco Crosswork Data Gateway instance active or in maintenance mode.
cpu	Number of vCPUs.

Field	Description
memory	Amount of total memory. Note The value shown for <i>memory</i> represents the usable amount for user processes, not the total VM amount. The Cisco Crosswork Data Gateway operating system reserves about 700MB from the total VM memory for itself, which is excluded from memory reporting tools. It is expected for the <i>memory</i> value reported here to be 1GB less than the full amount allocated to the VM due to operating system reservation and rounding.
nics	Number of NICs being used by Cisco Crosswork Data Gateway. This is 3 in case of on-premise installation i.e., for Cisco Crosswork Change Automation and Health Insights.
interfacename	Name of the interface.
interfacemac	MAC address of the interface
interfaceIPv4address/interfaceIPv6address	IPv4/IPv6 address of the interface.
cert_chain	Certificate used for handshake between Cisco Crosswork Data Gateway instance and Cisco Crosswork Change Automation and Health Insights.

Change the Administration State of a Cisco Crosswork Data Gateway Instance

You can change the administration state of a Cisco Crosswork Data Gateway instance via Crosswork UI.



Note If the maintenance activities are affecting the communication between Crosswork and Cisco Crosswork Data Gateway, the collection is interrupted and resumes when the communication is restored.

While an instance is in in **Maintenance** mode, no new jobs are submitted to it. During downtime, admin can do modifications to Cisco Crosswork Data Gateway, such as updating the certificates, changing management address, etc.

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

Follow the steps below to change the administration state of a Cisco Crosswork Data Gateway instance.

Step 1 From the main menu, choose **Admin > Data Gateway Management**. The **Data Gateway Management** view opens.

De-enroll a Cisco Crosswork Data Gateway Instance

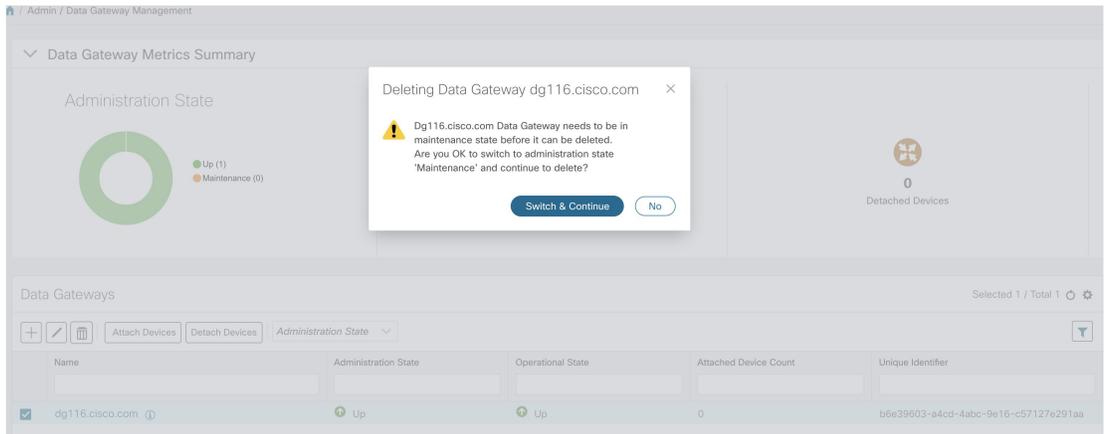
- Step 2** From the **Data Gateways** window, select the Cisco Crosswork Data Gateway instance whose administration state you want to change.
- Step 3** From the **Administration State** dropdown, select the state to which you want to switch to.

The screenshot shows the 'Data Gateway Management' interface. At the top, there is a 'Data Gateway Metrics Summary' section with three donut charts: 'Administration State' (Up: 1, Maintenance: 0), 'Operational State' (Up: 1, Error: 0, Degraded: 0, Unknown: 0), and 'Detached Devices' (0). Below this is a table of 'Data Gateways' with columns for Name, Up, State, Operational State, Attached Device Count, and Unique Identifier. The table contains one entry: 'dg116.cisco.com' with 'Up' in the Up column, 'Up' in the State column, 'Up' in the Operational State column, '0' in the Attached Device Count column, and 'c987e2f0-408c-40ee-be94-e48b529fa798' in the Unique Identifier column. The 'Administration State' dropdown menu is open, showing 'Up' and 'Maintenance' options.

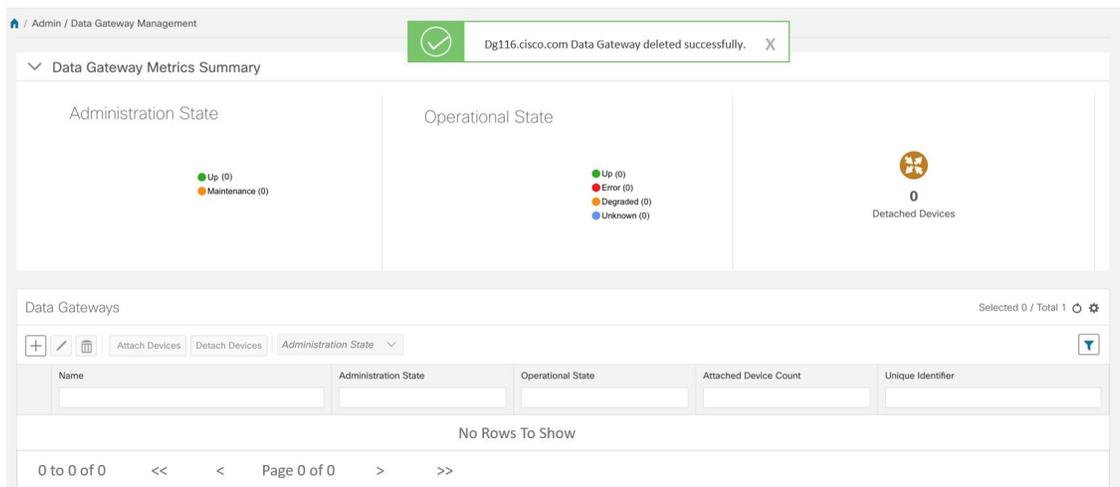
De-enroll a Cisco Crosswork Data Gateway Instance

Follow the steps below to de-enroll a Cisco Crosswork Data Gateway instance.

- Step 1** From the main menu, choose **Admin > Data Gateway Management**. The **Data Gateway Management** view opens.
- Step 2** From the **Data Gateways** window, select the Cisco Crosswork Data Gateway instance you want to delete.
- Step 3** Click .
- Step 4** A Cisco Crosswork Data Gateway instance must be in maintenance mode to be deleted. Click **Switch & Continue** when prompted to switch to **Maintenance** mode.



The selected Cisco Crosswork Data Gateway instance is deleted.



Attach a Device to a Cisco Crosswork Data Gateway Instance



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

Follow the steps below to attach a device to a Cisco Crosswork Data Gateway instance.

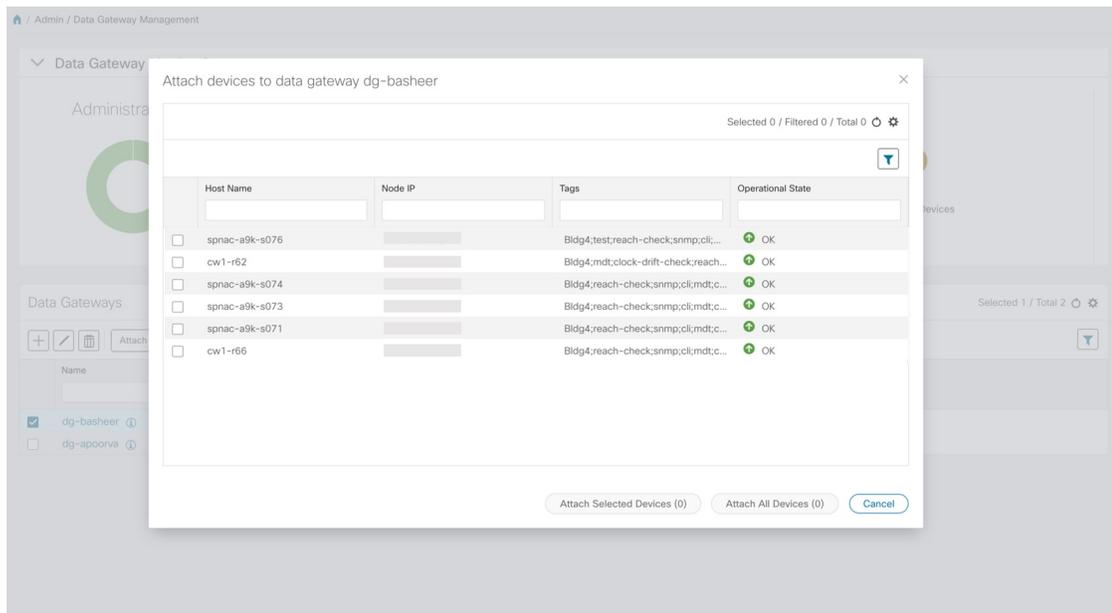
Before you begin

1. For optimal performance, it is recommended that device attaching to Cisco Crosswork Data Gateway instance should be done in batches of no more than 300 devices.

You can add more than 300 devices. However, doing so may cause a performance impact.

2. Ensure that both the administration state and operational state of the Cisco Crosswork Data Gateway instance to which you want to attach devices is "Up". Only then proceed with attaching devices.

- Step 1** From the main menu, choose **Admin > Data Gateway Management**. The **Data Gateway Management** view opens.
- Step 2** From the **Data Gateways** window, select the Cisco Crosswork Data Gateway instance to which you want to attach devices.
- Step 3** Click **Attach Devices**. The **Attach Devices** window opens. It lists all the devices available for attaching.

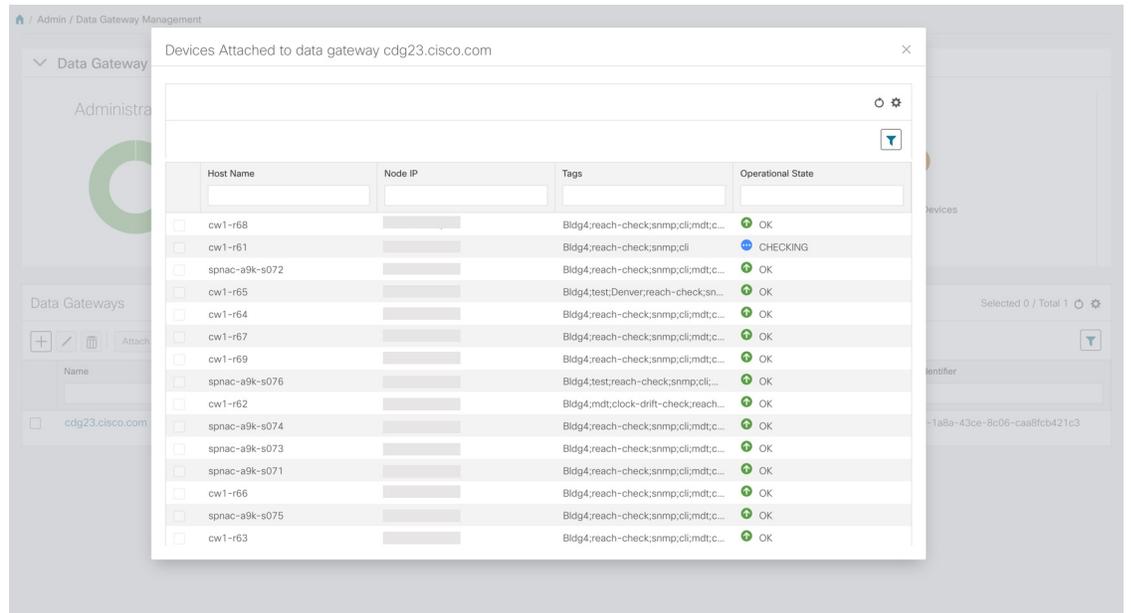


- Step 4** To attach all the devices, click **Attach All Devices**. Otherwise, select the devices you want to attach and click **Attach Selected Devices**.

What to do next

To verify if the devices were attached to the VM, check the **Attached Device Count** under the **Data Gateways** pane. The count would have increased.

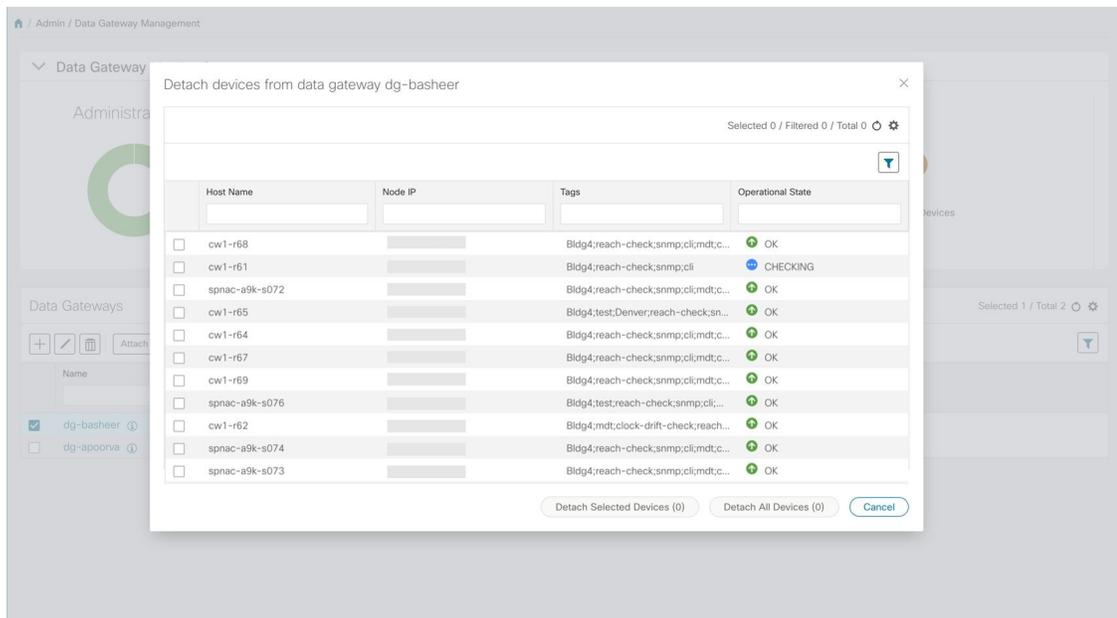
Click on the  icon next to the attached device count to see the list of all devices attached to the selected instance, as shown in the following figure.



Detach a Device From a Cisco Crosswork Data Gateway Instance

Follow the steps below to detach a device from a Cisco Crosswork Data Gateway instance.

- Step 1** From the main menu, choose **Admin > Data Gateway Management**. The **Data Gateway Management** view opens.
- Step 2** From the **Data Gateways** window, select the Cisco Crosswork Data Gateway instance from which you want to detach devices.
- Step 3** Click **Detach Devices**. The **Detach Devices** window opens. It lists all the devices attached to the selected Cisco Crosswork Data Gateway instance.



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

What to do next

To verify if the devices were detached from the VM, check the **Attached Device Count** under **Data Gateways** window. The count would have decreased.

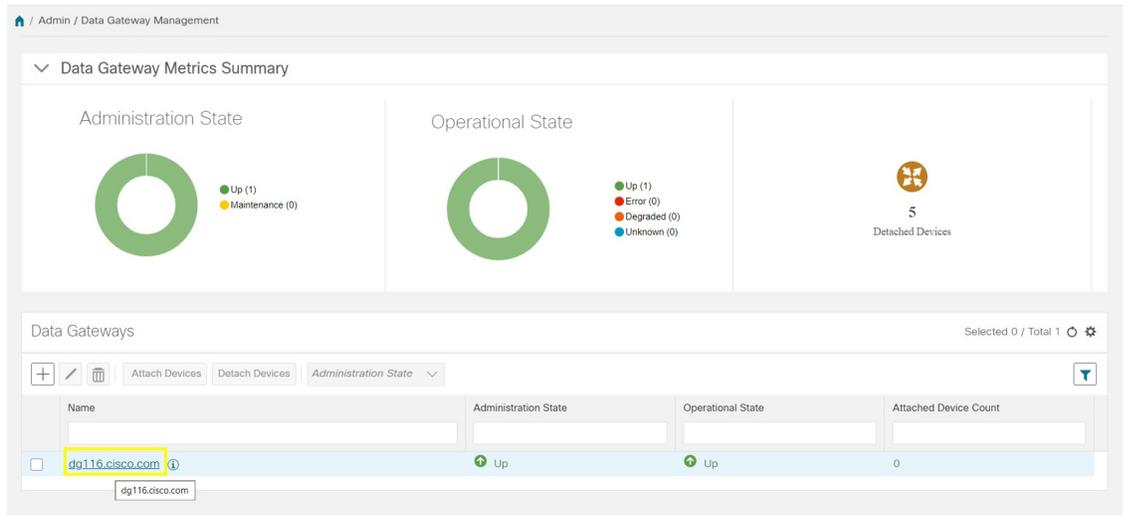
View Cisco Crosswork Data Gateway Instance Health

Cisco Crosswork Data Gateway comprises of various containerized services running on an Ubuntu VM. Its overall health depends on health of each containerized service.

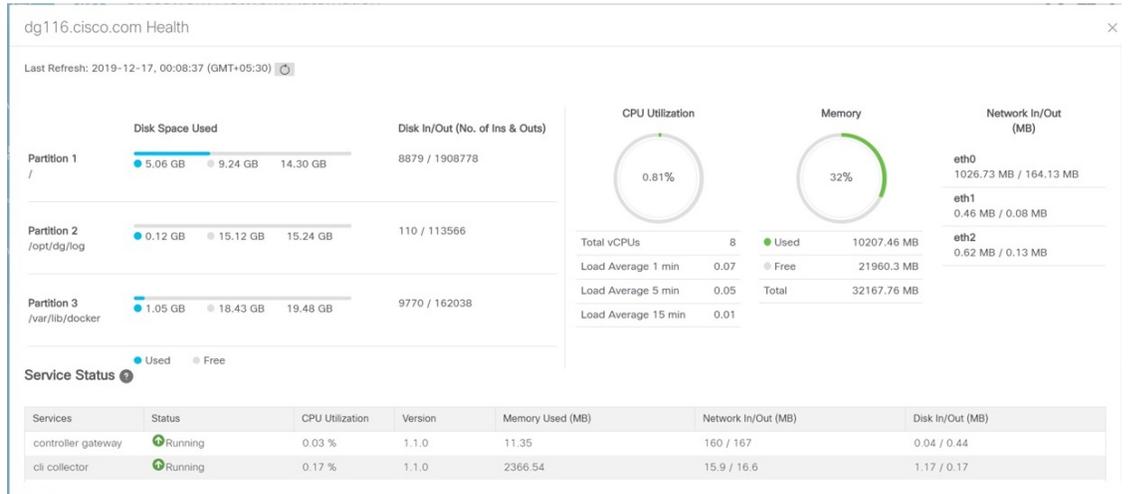
Cisco Crosswork Data Gateway collects host and container metrics and writes them to a container mounted path in vitals.json file and sends it to the Crosswork.

Vitals also contains the health information of individual container services running on the Cisco Crosswork Data Gateway instance and their resource consumption.

To view health of a Cisco Crosswork Data Gateway instance, in the **Data Gateways** window, click the name of the Cisco Crosswork Data Gateway instance whose health you want to view as shown in the following figure.



The **Health** pop up displays the following details:



Field	Description
Host VM	
Last Refresh	Date and time of the last refresh. Click to refresh the Data Gateway Health pop up.
Disk Space Used	Percentage of the disk space used for partitions: / /opt/dg/log /var/lib/docker

Field	Description
Disk In/Out	<p>Number of read/write or input/output operations involving a disk for the partitions:</p> <p>/</p> <p>/opt/dg/log</p> <p>/var/lib/docker</p> <p>Note This is a cumulative counter, not a delta time series.</p>
CPU Utilization	Amount of actively used CPU and total number of vCPUs.
Load	Load average – is the average system load over a given period of time of 1, 5, and 15 minutes.
Memory	Amount of memory used and available memory.
Network In/Out	<p>The amount of data sent/received in MB for NIC interfaces:</p> <p>eth0</p> <p>eth1</p> <p>eth2</p> <p>Note This is a cumulative counter, not a delta time series.</p>
Service Status	
Service	Name of the Cisco Crosswork Data Gateway service.
Status	<p>Status of the service:</p> <ul style="list-style-type: none"> • Running • Degraded • Error
CPU Utilization	Percentage of actively utilized CPU by the service.
Version	Version of the service deployed.
Memory Used (MB)	Amount of memory being used by the service.
Network In/Out	<p>The amount of data sent/received in MB by the service over its interface.</p> <p>Note This is a cumulative counter, not a delta time series.</p>

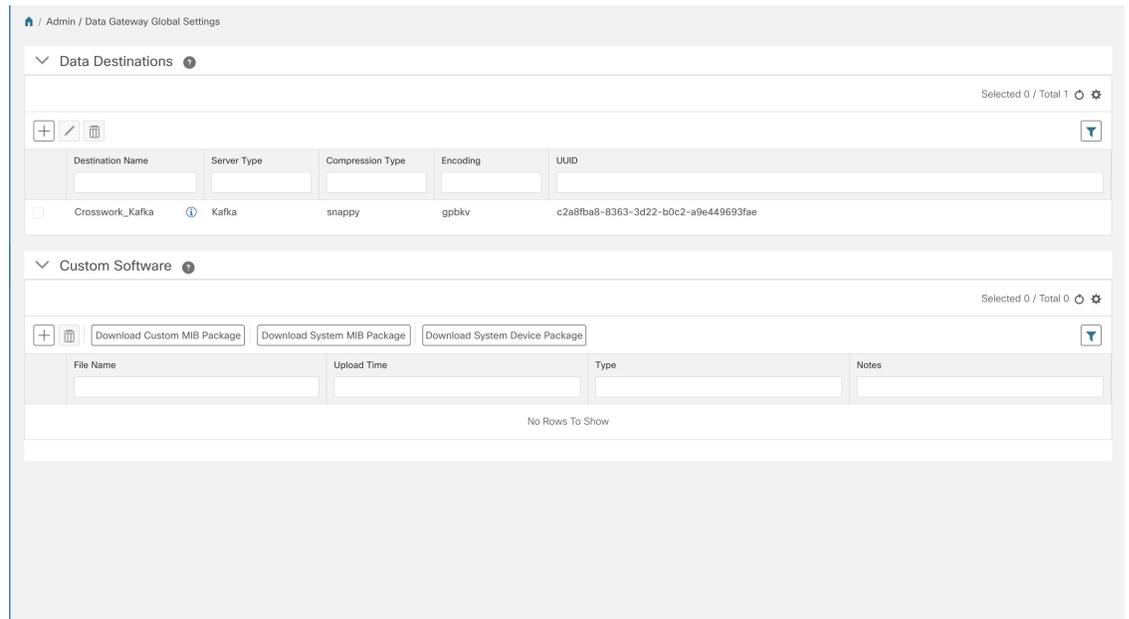
Field	Description
Disk In/Out	Number of read/write or input/output operations that the service has done involving a disk. Note This is a cumulative counter, not a delta time series.

Configure Cisco Crosswork Data Gateway Settings

This section describes how to configure global settings for Cisco Crosswork Data Gateway i.e., managing data destinations and custom software packages.

To open Cisco Crosswork Data Gateway global settings view, choose **Admin > Data Gateway Global Settings** from the left navigation bar in the Cisco Crosswork Change Automation and Health Insights window.

Figure 24: Data Gateway Global Settings View



Item	Description
Data Destinations Pane	Shows approved external data destinations that can be used by collection jobs to deposit their data and provides options to add, edit, and delete data destinations.
Custom Software Pane	Provides options to: <ul style="list-style-type: none"> • add and delete custom MIBs and device packages • download custom MIBs, system MIBs, and device packages

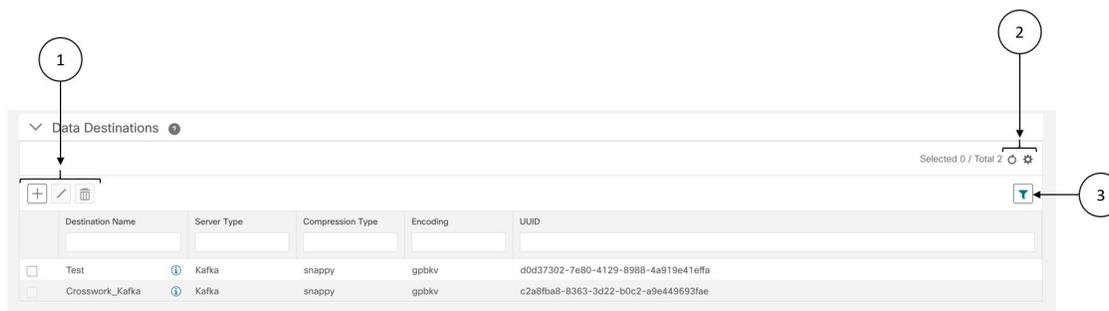
Manage Data Destinations

From the **Data Destinations** pane, you can add a new data destination, update the settings configured for an existing data destination, and delete a data destination.



Note The **Crosswork_Kafka** data destination in the below figure is Cisco Crosswork Change Automation and Health Insights's internal data destination and hence, it cannot be updated or deleted.

Figure 25: Data Destinations Pane



Item	Description
1	Click to add a data destination. See Add a Data Destination, on page 225 .
	Click to edit the settings for the selected data destination. See Update a Data Destination, on page 229 .
	Click to delete the selected data destination. See Delete a Data Destination, on page 231 .
2	Click to refresh the Data Destinations window.
	Click to choose the columns to make visible in the Data Destinations window (see Set, Sort and Filter Table Data, on page 6).
3	Click to show/hide the quick filters.
	Click the Clear All Filters link to clear any filter criteria you may have set.

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

Field	Description
Destination Name	Name of the data destination
Server Type	Server type of the data destination i.e., external Kafka or gRPC server.

Field	Description
Compression Type	Compression type being used for the data destination. Crosswork
Encoding	Encoding type being used for the data destination.
UUID	Unique identifier for the data destination. This ID is automatically generated by Crosswork when an external data destination is created and is a required parameter for collection job creation.

Add a Data Destination



Note

- If you reinstall an already existing external Kafka data destination with the same IP address, then the collectors need to be restarted for changes to take place .
- You can secure communication channel between Cisco Crosswork Data Gateway and the specified data destination i.e., either Cisco Crosswork Change Automation and Health Insights or external Kafka. **Steps 7 - 8** of the below procedure explain how to do that.

However, enabling security can impact performance.

- If your external data destination requires a TLS connection, keep the public certificate ready or if it requires client authentication, keep the client certificate and key files ready. The client key might be password-encrypted which will need to be configured as part of the data destination provisioning. Currently, Cisco 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.

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

Before you begin

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

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



Note

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

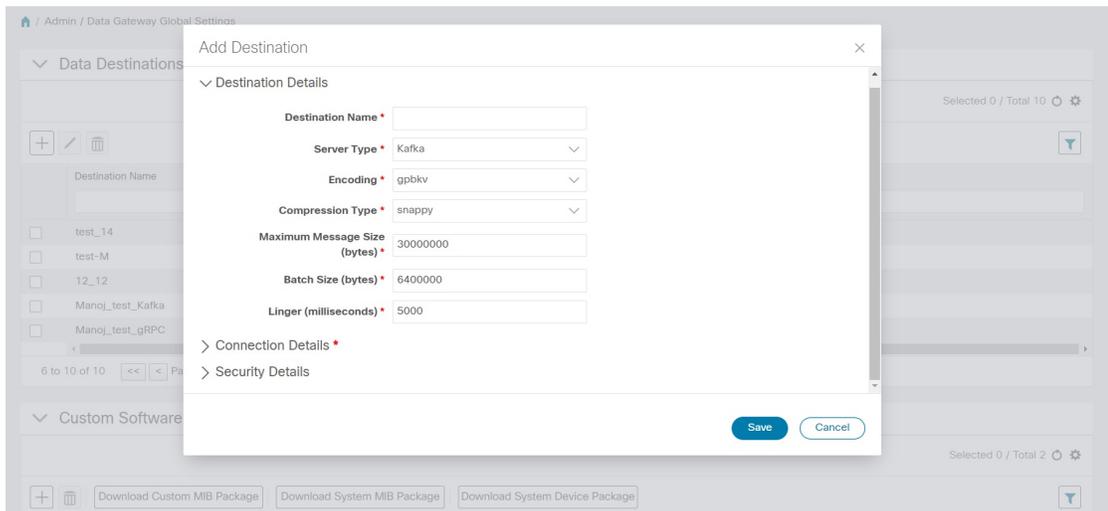
- `num.io.threads = 8`
- `num.network.threads = 3`
- `message.max.bytes= 30000000`

- Create Kafka topics that you want to be used for data collection.

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

Step 2 From **Data Destinations** pane, choose **+**.

Step 3 In the **Add Destination** pop-up, enter the **Destination Details** as per the table below:

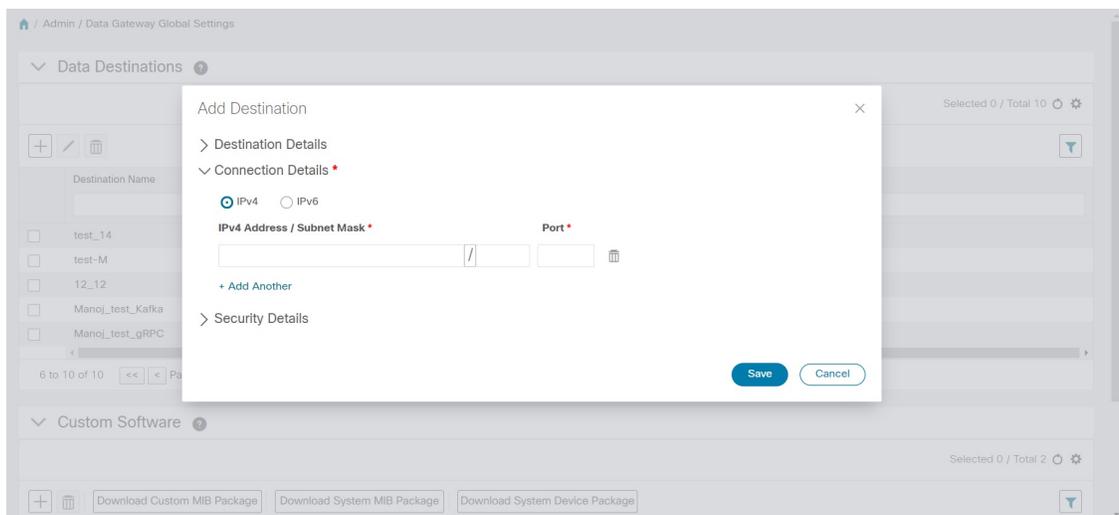


Field	Value
Destination Name	Enter a descriptive data destination name. The name can contain a maximum of 128 alphanumeric characters, plus underscores ("_") or hyphens ("-"). No other special characters are allowed. If you will have many data destinations, make the name as informative as possible to be able to distinguish later.
Server Type	From the drop down, select the server type of your data destination (Kafka/gRPC).
Encoding	From the drop down, select the encoding (json/gpbkv).
Compression Type	From the drop down, select the compression type: Compression types supported for Kafka are snappy, gzip, lz4, zstd, and none) Note zstd compression type is supported only for Kafka 2.0 or higher. Compression types supported for gRPC are snappy, gzip, and deflate.

Field	Value
Maximum Message Size (bytes) (Kafka-only)	Enter the maximum message size in bytes. <ul style="list-style-type: none"> • Default Value: 30000000 bytes/ 30 MB • Min: 1000000 bytes/1 MB • Max: 30000000 bytes/ 30 MB For <code>Maximum Message Size</code> property, you can input a value lesser than the default, but not more.
Batch Size (bytes) (Kafka-only)	Enter the required batch size in bytes. <ul style="list-style-type: none"> • Default Value: 6400000 bytes/6.4 MB • Min: 16384 bytes/ 16.38 KB • Max: 6400000 bytes/6.4 MB <p>Note For <code>Batch Size</code> property, you can input a value lesser than the default, but not more.</p>
Linger (milliseconds) (Kafka-only)	Enter the required linger time in milliseconds. <ul style="list-style-type: none"> • Default Value: 5000 ms • Min: 0 ms • Max: 5000 ms

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

Step 4 Select a protocol from the **Connection Details** options. Cisco Crosswork Data Gateway supports both IPv4 and IPv6.

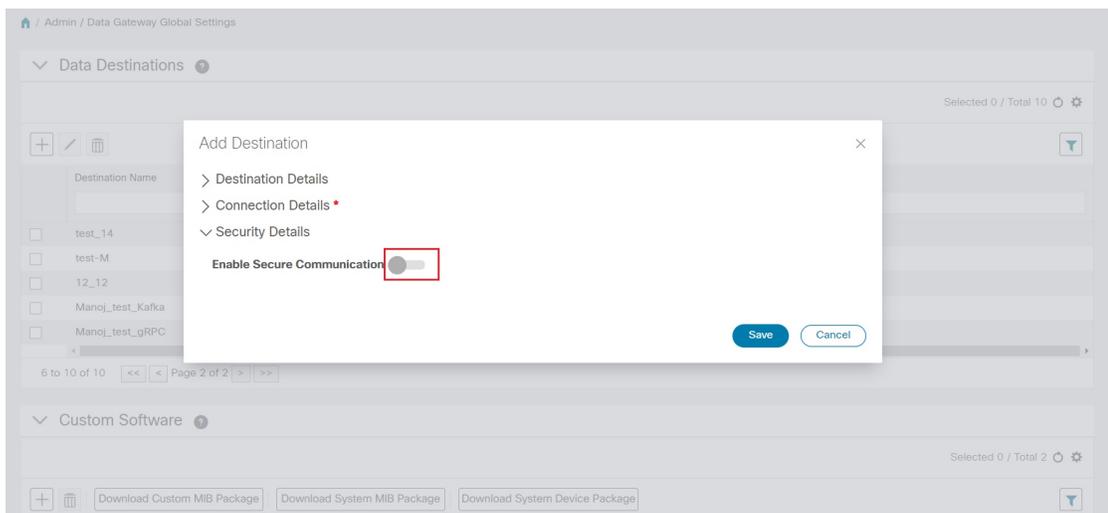


Add a Data Destination

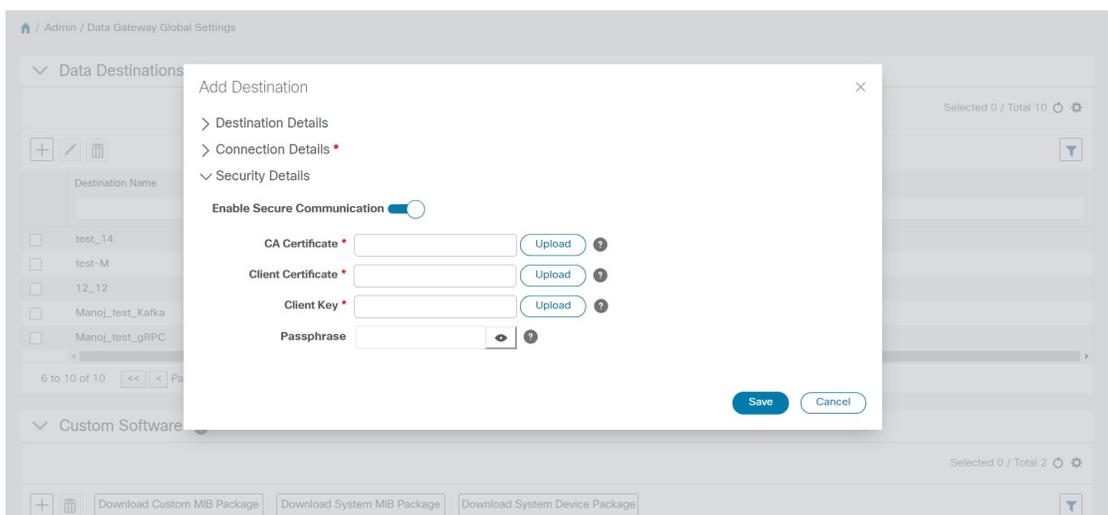
Step 5 Complete the **Connection Details** fields as described in the following table. The fields displayed will vary with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
IPv4	Enter the required IPv4 Address/ Subnet Mask , and Port . You can add multiple IPv4 addresses by clicking + Add Another
IPv6	Enter the required IPv6 Address/ Subnet Mask , and Port . You can add multiple IPv6 addresses by clicking + Add Another .

Step 6 If required, enable security by turning on **Enable Secure Communication** option under **Security Details**.



Step 7 Complete the **Security Details** fields as described in the following table.



Cisco Crosswork Data Gateway supports certificate-based authentication.

Note Currently, Cisco Crosswork Data Gateway supports IP-based certificates only. Hostname-based certificates are not supported in this release.

Field	Description
CA Certificate	Specify the PEM encoded trusted CA certificate i.e., the .PEM file to be used for secure communication between Cisco Crosswork Data Gateway and the specified data destination (Crosswork Kafka/ external Kafka/gRPC).
Client Certificate	Specify the PEM encoded client certificate i.e., .PEM, .CRT, or .CER file to be used for client authentication.
Client Key	Specify the PKCS#8 or .KEY file. This is the private key for the specified client certificate.
Passphrase	Enter the passphrase if the client key is passphrase encrypted.

Step 8 Click **Save**.

What to do next

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

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

Update a Data Destination



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

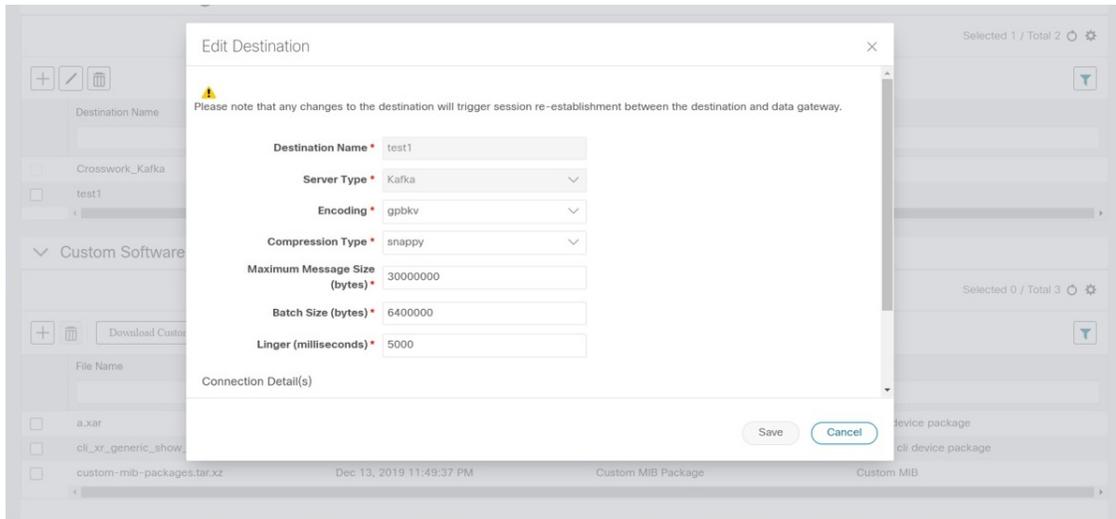
Follow the steps below to update a data destination.

Step 1 From **Data Destinations** window, select the destination you want to update.

Step 2 Click .

Step 3 In the **Edit Destination** pop up, make the required changes.

Note In **Edit** mode, you cannot update **Destination Name** and **Server Type**.



Step 4 Click **Save**.

View Data Destination Details

To view details of a data destination, in the **Data Destinations** pane, click  icon next to the data destination name whose details you want to see. Cisco Crosswork Data Gateway displays the details as shown in the following figure.

View Destination: kafka-172-ssl-withpassphrase
✕

▼ Destination Details

Destination Name * kafka-172-ssl-withpassphrase

Server Type * Kafka

Encoding * gpbkv

Compression Type * snappy

Maximum Message Size (bytes) * 30000000

Batch Size (bytes) * 6400000

Linger (milliseconds) * 5000

▼ Connection Details *

IPv4

IPv4 Address / Subnet Mask * 172.29.194.172 / 24 **Port *** 9093

▼ Security Details

Enable Secure Communication

CA Certificate *

```
-----BEGIN CERTIFICATE-----
MIIFhzCCA2+gAwIBAgIJAMxj/HMZHoRIM
A0GCSqGSIb3DQEBCwUAMEsxCzAJBgN
V
BAYTAIVTMQswCQYDVQQIDAJDQTEOMA
wGA1UECgwFQ2lzY28xETAPBgNVBACM
```

Client Certificate *

```
-----BEGIN CERTIFICATE-----
MIIFRDCCAyygAwIBAgIJAPTQSP/G6BeH
MA0GCSqGSIb3DQEBCwUAMEsxCzAJBg
NV
BAYTAIVTMQswCQYDVQQIDAJDQTEOMA
wGA1UECgwFQ2lzY28xETAPBgNVBACM
```

Client Key *

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIJcTAbBgkqhkiG9w0BBQMwDgQloHjZ5
GEJBkACAaggABIIJUFQ2I/3BiXzr9zch
1QuyI7GBn6ApAaC/0kKpXiiBK9/thUDSnv/
Ku3Q3sF8C2Nq6h22lpyNJmOL7Lw6D
```

Passphrase

Close

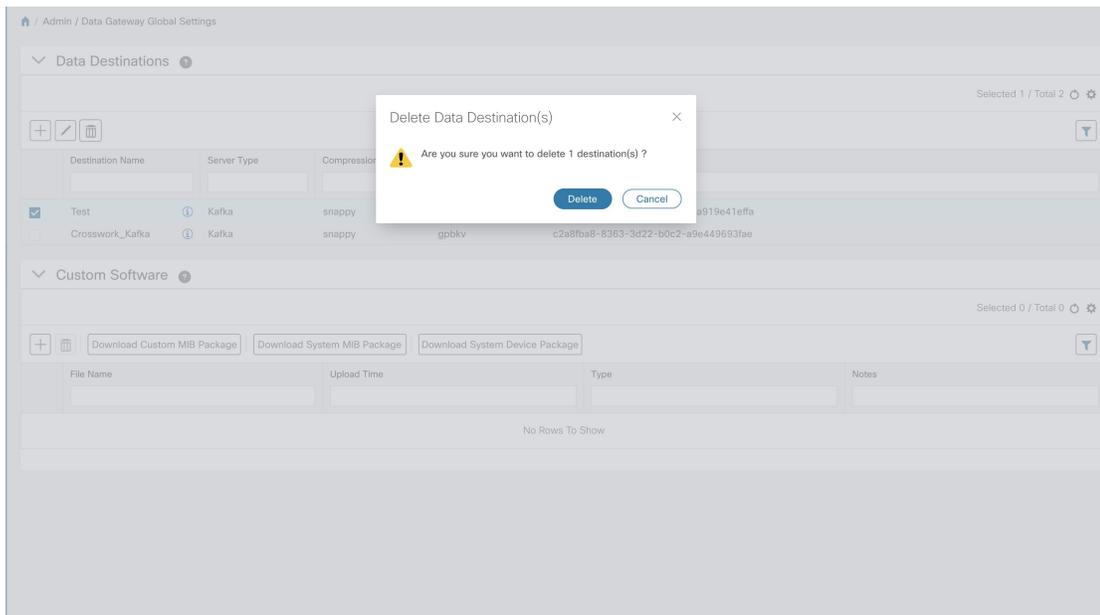
Delete a Data Destination

Follow the steps below 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. See [Monitoring Collection Jobs](#), on page 259.

- Step 1** From the main menu, choose **Admin > Data Gateway Global Settings**.
- Step 2** From the **Data Destinations** pane, select the Data destination(s) you want to delete.
- Step 3** Click .
- Step 4** In **Delete Data Destination(s)** pop up, click **Delete** to confirm.



Manage Custom Software Packages

To support third party device CLI and SNMP MIBs, Cisco Crosswork Data Gateway allows you to import the device packages and MIBs to the collectors. Device packages can be imported to allow Cisco Crosswork Data Gateway to retrieve CLI and SNMP data and convert it into xml for third party devices. You can extend the SNMP coverage of Cisco Crosswork Change Automation and Health Insights by uploading Custom MIB Packages with any additional MIB and YANG descriptions you require. If you only wish raw SNMP data, no additional files are needed, the system will fold the entire data package into the the Cisco Crosswork Data Gateway data payload.



Note MIBs are required only if the collection request references MIB TABLE names or SCALAR names. However, if the requests are OID-based, then MIBs are not required.

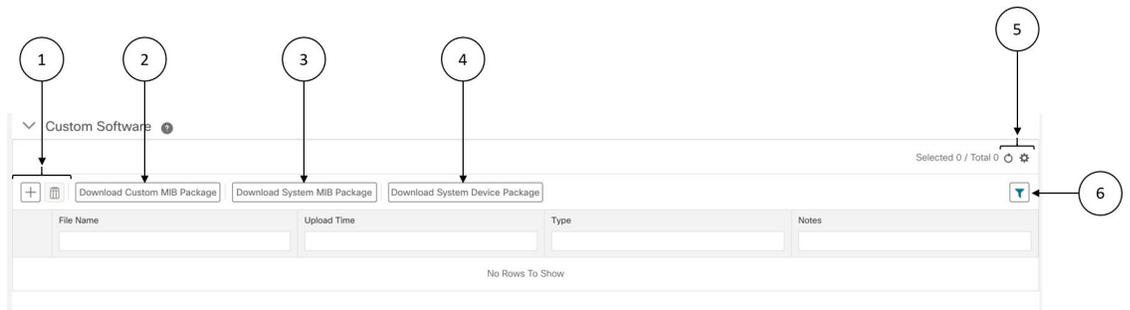
Cisco Crosswork Data Gateway allows you to register and deploy three types of custom software packages:

- 1. CLI Device Package:** provides instructions for how to speak to a device using CLI and parse the results into the desired xml.
- 2. Custom MIB Packages:** Custom MIBs and device packages can be specific to third party devices or be used to filter the collected data or format it differently for Cisco devices. These are editable by the user.
- 3. SNMP Device Package:** provides instructions for how to speak to a device using SNMP and parse the results into the desired xml.

Cisco Crosswork Data Gateway also allows you to download Custom MIB package, System MIB package, and System Device package.

System Device and MIB Packages are bundled in the Crosswork software and are automatically downloaded to the Cisco Crosswork Data Gateway instances. These are NOT modifiable by the user. Custom Device Packages can be downloaded when required for interfacing with third-party devices.

From the **Custom Software** pane, you can add a new custom package, delete a custom package, and download custom packages.



Item	Description
1	Click to add a new custom package. See Add a Custom Software Package, on page 234 .
	Click to delete a custom package. See Delete a Custom Software Package, on page 235 .
2	Click Download Custom MIB Package to download custom MIB packages. See Download Custom or System MIBs and Packages, on page 236 .
3	Click Download System MIB Package to download system MIB packages. See Download Custom or System MIBs and Packages, on page 236 .
4	Click Download System Device Package to download system device packages. See Download Custom or System MIBs and Packages, on page 236 .
5	Click to refresh the Custom Software window.
	Click to choose the columns to make visible in the Custom Software window (see Set, Sort and Filter Table Data, on page 6).

Item	Description
6	Click  to show/hide the quick filters.
	Click the Clear All Filters link to clear any filter criteria you may have set.

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

Field	Description
File Name	Name of the custom software package.
Upload Time	Time of the file upload.
Type	Type of the custom software package.
Notes	Notes related to the custom software package entered by the user while importing the package.

Add a Custom Software Package

Crosswork allows you to upload Custom Device Packages in case you want to filter/format the collected raw data differently.

There are two types of upload:

1. Custom MIB Package upload (a single file custom-mib-packages.tar.xz): which is archive of all custom MIBs/YANGs file
2. Individual Device Package Upload

When uploading new MIBs as a part of Custom MIB Package, it's required that those new MIBs files are loadable within collectors along with existing System MIB files i.e., all dependencies in the files get resolved properly. An offline tool steps are provided for you to ensure that their new MIBs gets parsed and uploaded properly. Accordingly, you can prepare the Custom MIB Package and upload.

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



Note Crosswork doesn't allow Custom MIB package files to overwrite the System MIB Package files. It results in a failed upload attempt.

Using UI, Admin can upload CLI device packages, custom MIB packages, and SNMP device packages. This gets downloaded on the Cisco Crosswork Data Gateway instance to mounted path of respective collectors.

Follow these steps to import a custom software package into Cisco Crosswork Data Gateway:

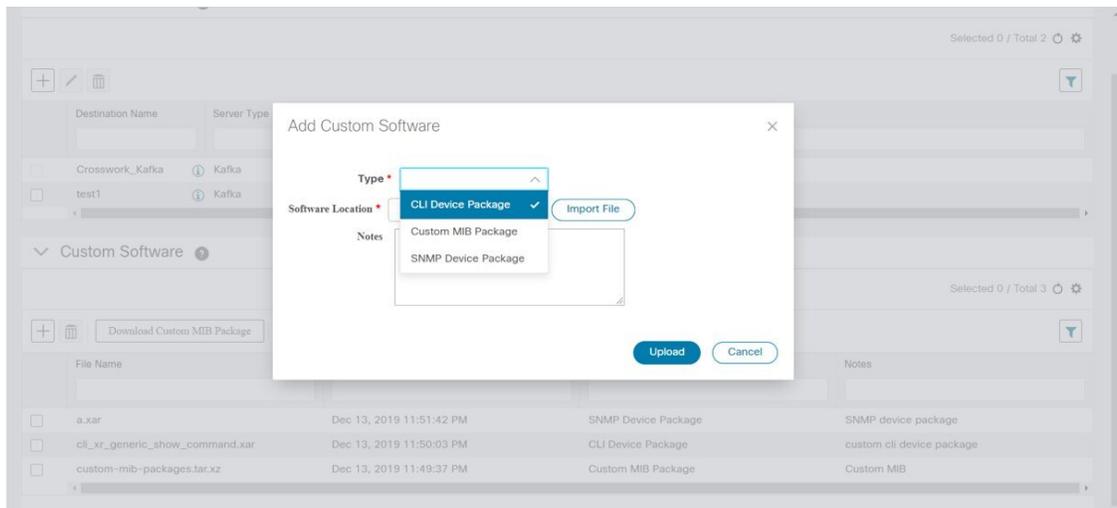
**Note**

- Ensure that the custom software package TAR file has just the device package folders and none of the parent folder or hierarchy of folders as part of the TAR file. If not imported properly, Cisco Crosswork Data Gateway throws exceptions when executing the job with custom device package.
- Crosswork does not implement any control on the files being uploaded other than checking the file extension.

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

Step 2 From **Custom Software** window, choose .

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



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

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

Step 6 Click **Upload**.

Delete a Custom Software Package

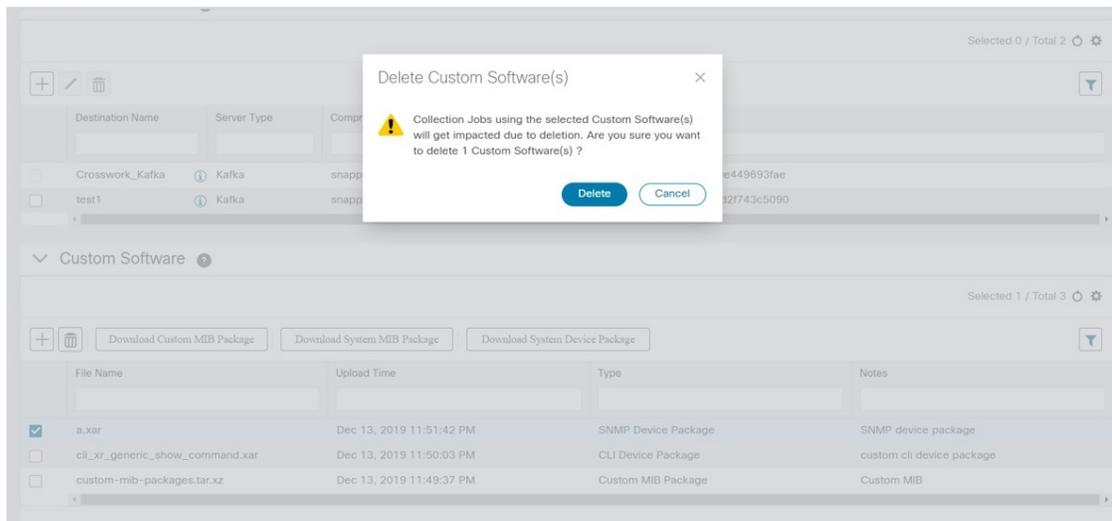
Follow the steps below to delete a custom software package.

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

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

Step 3 Click .

Step 4 In the **Delete Custom Software** pop up, click **Delete** to confirm.



Download Custom or System MIBs and Packages

Cisco Crosswork Data Gateway has some pre-loaded MIBs and device packages. You can download them to obtain a tarball of the custom MIBs and device packages from the Crosswork UI, add more custom MIBs and device packages and re-upload them to the Crosswork. See [List of Pre-loaded Traps and MIBs for SNMP Collection, on page 264](#).

System MIB Packages and System Device Packages are downloadable only. This is only if you want to know the abilities that already exists in the system. These cannot be modified.

If you have a new version, you can delete the existing one and upload the new one.

Follow the below steps to download custom software packages from Crosswork UI.

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

Step 2 From **Custom Software** pane, choose based on the following table:

If you want to download	Click...
Custom MIB Package	Download Custom MIB Package
System MIB Package	Download System MIB Package
System Device Package	Download System Device Package

Step 3 In the download window, navigate to the location where you want to download the file and click **Save**.

What to do next

To add new MIBs/Yangs, follow the steps:

1. Extract the package and add new files.

2. Run the package through the offline tool as explained at [Use Custom MIBs and Yangs on Cisco DevNet](#) to ensure that it can be uploaded to Crosswork.
3. Tar it back as custom-mib-packages.tar
4. Run XZ utility to compress it to custom-mib-packages.tar.xz
5. Upload the package back into Crosswork by following the steps described at [Add a Custom Software Package, on page 234](#).



CHAPTER 9

Configure Collection

This section contains the following topics:

- [Collection Service Overview](#), on page 239
- [Prerequisites for Device Model Driven Telemetry](#), on page 239
- [About Collection Jobs](#), on page 242
- [Collection Job Payload Model](#), on page 242
- [Create Collection Jobs](#), on page 248
- [Best Practices and Limitations for Creating Collection Jobs](#), on page 248
- [Collection Jobs](#), on page 249
- [Monitoring Collection Jobs](#), on page 259
- [List of Pre-loaded Traps and MIBs for SNMP Collection](#), on page 264
- [List of Pre-loaded YANG Modules for MDT Collection](#), on page 270

Collection Service Overview

Multiple applications requesting same data overload network devices causing outages. Cisco Crosswork Data Gateway's **Collection Optimization** feature tackles this problem by optimizing collection requests. Thereby, reducing redundant data collections.

Users with administrative privileges can monitor Collection Service status and performance, and start/stop/restart it or its underlying services, using the Cisco Crosswork Change Automation and Health Insights user interface. You can also collect logs and performance metrics for this service. For help with these tasks, see [Manage Cisco Crosswork Network Automation](#), on page 147.

Prerequisites for Device Model Driven Telemetry

The Cisco Crosswork Change Automation and Health Insights Collection Service configures telemetry as needed on the devices enrolled within the service.



Note

If an operator configures telemetry directly on the same devices either manually or through some mechanism outside of the Collection Service, the commands must not contain the keyword `cw`. The keyword `cw` is reserved for use by the Collection Service. In particular, the following commands must not contain the keyword `cw` when configured outside of the Collection Service:

```

destination-group
sensor-group
subscription
    sensor-group-id
    destination-id

```

For example (invalid telemetry configuration):

```

telemetry model-driven
destination-group CW_1b4ac245d863cf3e787d42bae97f1d18dd300d5e

```

For more information, see the telemetry configuration documentation for your particular device (for example: [Telemetry Configuration Guide for Cisco ASR 9000](#))

For collection to work, the maximum number of interfaces on a single device must be less than 8,000. The cumulative count of interfaces across all devices must be less than 30,000.

Invalid Telemetry Configuration

The following sample output shows an *invalid* telemetry configuration on a device when configured outside of the Collection Service.

```

telemetry model-driven
destination-group CW_1b4ac245d863cf3e787d42bae97f1d18dd300d5e
address-family ipv4 172.16.2.31 port 31500
encoding self-describing-gpb
protocol tcp
!
!
destination-group CW_6da4e808ed4724911f2288dbae605bb62f9617
address-family ipv4 <IP_address> port 31500
encoding self-describing-gpb
protocol tcp
!
!
destination-group CW_7ee5d52d7e513640f71417d4fcdb584c6a883f7c
address-family ipv4 <IP_address> port 31500
encoding self-describing-gpb
protocol tcp
!
!
destination-group CW_bbd6f2991d04e920fbda0f2a5ceb63d1c9f62cdf
address-family ipv4 <IP_address> port 31500
encoding self-describing-gpb
protocol tcp
!

```

Valid Telemetry Configuration

The following sample output shows a *valid* telemetry configuration on a device when configured outside of the Collection Service. Note that the *<IP_address>* referred to in this sample should not be the IP address of the Cisco Crosswork Change Automation and Health Insights server. It should be the IP address of the other data consumer.

```

telemetry model-driven
destination-group CUSTOM_X_1171424d5b08d674367318299db2f8a0d7d489e9
address family ipv4 <IP_address> port <Port>
encoding gpb

```

```

    protocol grpc no-tls
    !
!
sensor-group CUSTOM_X_1171424d5b08d674367318299db2f8a0d7d489e9
  sensor-path Cisco-IOS-XR-spirit-install-instmgr-oper:software-install/active
!
subscription CUSTOM_X_1171424d5b08d674367318299db2f8a0d7d489e9
  sensor-group-id CUSTOM_X_1171424d5b08d674367318299db2f8a0d7d489e9 sample-interval 7000
  destination-id CUSTOM_X_1171424d5b08d674367318299db2f8a0d7d489e9
!

```



Note The **sample-interval** can be changed depending on the size of your network. It is defined in milliseconds and determines how fast you want the data to be pushed out.

Confirm that all PCCs or provider edge routers have telemetry configured and report data to . For example, routers should report prefix and tunnel counters:

```

RP/0/RP0/CPU0:PE1#show traffic-collector ipv4 counters prefix
Thu Jul 11 08:32:32.993 UTC
Prefix Label Base rate TM rate State
(Bytes/sec) (Bytes/sec)
-----
192.168.0.1/32 16001 1 0 Active
192.168.0.2/32 16002 1 0 Active
192.168.0.3/32 16003 1 0 Active
192.168.0.4/32 16004 2 0 Active
192.168.0.6/32 16006 501023 501021 Active
192.168.0.7/32 16007 17320774 17320772 Active
192.168.0.8/32 16008 3737825 3737823 Active
192.168.0.9/32 16097 3 0 Active
192.168.0.10/32 16096 2 0 Active

```

```

RP/0/RP0/CPU0:PE1#show traffic-collector ipv4 counters tunnel
Thu Jul 11 08:32:20.746 UTC
Interface Base rate Base rate State
(Packet/sec) (Bytes/sec)
-----
srte_c_102_ep_192.168.0.7 0 0 Active

```

Cisco IOS XR devices that are onboarded through telemetry must have the following configuration settings on the device to ensure that NETCONF and SSH work correctly:

```

ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server rate-limit 600
ssh server session-limit 1024
netconf-yang agent ssh

```

Cisco IOS XR devices that are onboarded through SNMP must have SNMP enabled on the device. The following is an example of an SNMP configuration on a Cisco IOS XR device:

```

snmp-server community public RO

```

Please note that, currently, Cisco Crosswork Change Automation and Health Insights does not itself support execution of EXEC privilege commands, such as **enable**, on devices. These types of commands must be executed using the device console or other means.

About Collection Jobs

As mentioned earlier, Crosswork Data Gateway pulls functional images from the Crosswork. Each functional image represents a collection type. You can create multiple jobs for a given collection type. A collection job describes what task a Crosswork Data Gateway is expected to perform. Crosswork receives the data collection requests via these collection jobs and assigns to a Crosswork Data Gateway instance to serve the request.

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

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

Crosswork Data Gateway lets you create three types of collection jobs:

CLI Collection Job

Enables CLI-based data collection (such as device configuration) from the network devices. The CLI collector uses XDE/PAL to collect device data for a given CLI. Only **show** commands are supported for this type of collection job.

SNMP Collection Job

Enables SNMP-based data collection based on the OIDs supported on the devices.

Supported SNMP versions include SNMPv1, SNMPv2c, and SNMPv3 for data polling and traps.

MDT Collection Job

Collects model driven telemetry data streamed from the device to the Crosswork Data Gateway.



Note

1. Crosswork Data Gateway drops incoming southbound traffic if there is no corresponding (listening) collection job request for the same. It also drops data/SNMP traps received from an unsolicited device (i.e., not attached to Crosswork Data Gateway). Crosswork Data Gateway records this in log and notifies Crosswork.
 2. Polled data cannot be requested from the device until Crosswork Data Gateway is ready to process and transmit the data. If it cannot keep up with the amount of data, it sends an error to northbound interface indicating when the throttling began and condition cleared.
-

Collection Job Payload Model

A collection job describes the following:

- Data to be collected.
- Devices from which collection is desired and credentials to authenticate.

- Collection intervals (a periodic interval no less than 60 seconds or greater than 32 days or immediately on demand.)
- Data Destinations where the collected data is to be deposited.

A single collection job can contain either CLI commands, SNMP MIB requests, or MDT subscriptions. Crosswork Data Gateway routes the request to the appropriate collector to fetch the requested data.

A collection job has three main parts:

```
//          Device Groups(s) -- identifies the different device groups from which data is
//                               to be collected and their authentication credentials.
//          Data Destinations(s) -- identifies the different output destination the final
//          data                               is sent to
//
```



Note Without clustered setup of external Kafka, if two destination nodes are specified, one is discarded.

Shown below is a sample collection job payload:

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

```

    }
  ]
}

```

The following table explains the fields of the above payload:

Field	Type	(M)andatory or (O)ptional	Description
collection_job	json object	M	Describes collection job with application context as key.
application_context	json object	M	Unique handle to identify your application's subscription. Note Combination of application ID and Context ID must be globally unique.
application_id	String	M	Unique identifier for the application. Note The prefix "cw" is reserved for Crosswork collection jobs and must not be used for jobs of other applications.
context_id	String	M	Unique identifier for the application subscription across all the collection jobs.
collection_mode	json object	M	A json object that holds lifetime type and collector type attributes of the collection job.
lifetime_type	string	O	Type of lifetime of job: <ul style="list-style-type: none"> • UNKNOWN_TEMPORAL_TYPE (default) • APPLICATION_MANAGED • CALENDAR_MANAGED • AUTO_DELETE_AFTER_N_SAMPLES

Field	Type	(M)andatory or (O)ptional	Description
collector_type	string	M	Type of the collector: <ul style="list-style-type: none"> • UNKNOWN_COLLECTOR (default) • CLI_COLLECTOR • SNMP_COLLECTOR • TRAP_COLLECTOR • MDT_COLLECTOR
n_collections	int	M	Number of collections to run before auto-deletion. Used only when lifetime_type is AUTO_DELETE_AFTER_N_SAMPLES.
job_device_set	json object	M	A json object containing device sets information.
device_set	json object	M	Device Grouping Object. For a given request, set one of either one device grouping i.e., list of devices or a device group, but not both.
device_ids	json array	M	Array of device IDs. Corresponds to UUID of the devices in the Crosswork inventory.
sensor_input_configs	json object	M	A group of sensors and their cadences.

Field	Type	(M)andatory or (O)ptional	Description
sensor_data	json object	M	<p>Type of sensor data:</p> <ul style="list-style-type: none"> • snmp_sensor • snmp_yang_sensor • cli_yang_sensor • cli_sensor • mdt_sensor • trap_sensor • trap_yang_sensor <p>Note YANG sensors are used for Crosswork initiated collection jobs, whereas Non-YANG sensors are used for API-initiated collection jobs.</p>
cadence_in_millisecc	int	O	Optional cadence value of this sensor config in seconds. If not passed the sensor config collection is done once.
sensor_output_configs	json array	M	A group of sensors and their cadences. Sensor Output represents output of sensor to a destination for given sensor which is a topic on Kafka or gRPC server.

Field	Type	(M)andatory or (O)ptional	Description
sensor_data	json object	M	<p>Every sensor path on the input side needs to have one mapping on the output side:</p> <ul style="list-style-type: none"> • snmp_sensor • snmp_yang_sensor • cli_yang_sensor • cli_sensor • mdt_sensor • trap_sensor • trap_yang_sensor <p>Note YANG sensors are used for Crosswork initiated collection jobs, whereas Non-YANG sensors are used for API-initiated collection jobs.</p>
destination	json object	M	<p>A JSON object that holds the final data destination information. It can hold one or more type of target information. Currently supported data destinations are kafka and gRPC.</p>
destination > context_id	string	M	<p>Destination context identifier. It could be Kafka topic name if destination is external Kafka server. The combination of destination_id and context_id needs to be unique for destination.</p> <p>What context id means depends on the destination type of destination provider. If gRPC is destination type, context_id is not used and will be ignored.</p>

Field	Type	(M)andatory or (O)ptional	Description
destination_id	string	M	Unique identifier for the data destination in inventory.

Create Collection Jobs



Note Cisco Crosswork Data Gateway API access for external data collection integration is separately licensed.

You can create and delete collection jobs using the Crosswork REST APIs. To access API documentation, see [API Documentation, on page 2](#).

For reference of collection job payloads, see [Collection Jobs, on page 249](#). Once the collection job is created, Crosswork adds it to the respective collector of the Crosswork Data Gateway.

The collection job is then picked up by the Crosswork Data Gateway for execution when the Image Manager syncs with Crosswork and retrieves the latest boot-config and docker-compose.

Upon successful creation of collection job, if the data destination is up, running, and accessible, Crosswork Data Gateway starts sending data to it. In this scenario, status for per device per sensor config is shown as ACTIVE in the Crosswork UI in **Collection Jobs** view. See [Monitoring Collection Jobs, on page 259](#)



Note Sensor output and input configs can be changed post creation by using a PUT collection job API. Other collection job parameters are immutable.

However, if output server is inaccessible, Crosswork Data Gateway fails to send data to it.

If you want to delete a collection job created by a Cisco Crosswork Change Automation and Health Insights application, it must be deleted via the corresponding application only.

Best Practices and Limitations for Creating Collection Jobs

Cisco recommends that following best practices be followed while creating collection job payloads:

Limitation	Best Practices
Scale	

Limitation	Best Practices
<p>Maximum size of sensor path collected data is 10 MB. Crosswork Data Gateway collector data at the same time from N devices cannot exceed 6 GB.</p>	<ol style="list-style-type: none"> Any collected sensor path's data size should not be > 10 MB when data destination is Kafka, otherwise you will get the following error message in <code>collector.log</code> file (to access log files, see Run show-tech, on page 309): RecordTooLargeException: The message is xxxxxxxx bytes when serialized which is larger than the maximum request size you have configured with the max.request.size configuration. Crosswork Data Gateway collector data at the same time from N devices with M sensor path per device and with P average size of collected data per sensor path cannot exceed 6 GB i.e., (N = # of devices) x (M = # of sensor path) x (P= Average Message size per sensor path) < 6GB
Log Purge Policy	
<p>When total log file size for a collector reaches 2 GB, Crosswork Data Gateway starts cleaning up by removing the old log files.</p>	<p>If you would like to save the old log files, save it to any other remote server before the total log file size reaches 2 GB per collector. This can be done by running show-tech from Crosswork Data Gateway Main Menu > Troubleshooting.</p>

Collection Jobs

This section contains sample collection job payloads for the following collection profiles:

- [CLI Collection Job, on page 249](#)
- [SNMP Collection Jobs, on page 251](#)
- [MDT Collection Job, on page 257](#)

CLI Collection Job

Crosswork Data Gateway supports CLI-based data collection from the network devices. It uses XDE/PAL to collect device data for a given CLI. Only show commands are supported for this type of collection job.

**Note**

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

OR

It should be ≥ 60 (i.e. at least 1 minute) up to 2764800 seconds (i.e. at most 32 days) max, indicating how frequently configured sensor data should be collected.

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

Following is a CLI collection job sample:

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

```

    }
  }
}

```

SNMP Collection Jobs

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

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



Note MIBs are required only if the collection request references MIB TABLE names or SCALAR names. However, if the requests are OID-based, then MIBs are not required.

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

The device packages can be imported into the Crosswork Data Gateway VM as described in Section [Add a Custom Software Package, on page 234](#).

The following SNMP versions are supported:

- SNMPv1
- SNMPv2c
- SNMPv3

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

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

**Note**

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

OR

It should be ≥ 60 (i.e. at least 1 minute) up to 2764800 seconds (i.e. at most 32 days) max, indicating how frequently configured sensor data should be collected.

- When collection from a device is skipped due to previous execution still in progress, Crosswork Data Gateway raises a warning log. No alert is generated for this scenario.
- For SNMP v1/v2c, if the device details (such as host or community string) are incorrect in the payload, Crosswork Data Gateway ignores the traps received from the device and logs the a WARN message.

In case of SNMP v3, if the device details (such as auth, priv, and security name details) are incorrect in the payload, Crosswork Data Gateway filters it out and hence, does not receive the trap. Thus, no WARN message is logged.

Sample Configurations on Device:

Version	Configuration
V1	<pre>snmp-server group group1 v1 snmp-server user user1 group1 v1 snmp-server host <host_ip> traps <community_string> udp-port 1062</pre> <p>For example,</p> <pre>snmp-server host 172.29.194.78 traps test udp-port 1062</pre> <p>Note Version 1 is the default version used by the device.</p>
V2c	<pre>snmp-server group group1 v2c snmp-server user user1 group1 v2c snmp-server host 172.29.194.142 traps version 2c v2test udp-port 1062</pre>
V3	<pre>snmp-server group group1 v3 auth notify user1 read user1 write user1 snmp-server view user1 1.3 included snmp-server user user1 group1 v3 auth md5 <password> priv aes 128 <password> snmp-server host 172.23.92.193 traps version 3 priv user1 udp-port 1062</pre>

The SNMP Collector supports the following operations:

- SCALAR

- TABLE



Note For TABLE operation, you can either provide a Table OID or a Column OID.

- MIB_WALK
- TRAP
- DEVICE_PACKAGE

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



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

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

Default value is 1500 milliseconds

Minimum value is 1500 milliseconds

However, there is no limitation on the maximum value of this attribute.

Following is an SNMP collection job sample:

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

```

        "cadence_in_millisec": "60000"
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_461cb8aa-a16a-44b8-b79f-c3daf3ea925f"
        }
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic2_e7ed6300-fc8c-47ee-8445-70e543057f8a"
        }
      }
    ]
  }
}

```

SNMP Traps Collection Job

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

**Note**

- Device should have been pre-configured by the traps.
- Crosswork Data Gateway listens on UDP port 1062 for Traps.
- If the collection job is invalid, there is missing configuration on the device, or no trap is received, the status of the job remains "Unknown".
- For list of supported Traps and MIBs, see [List of Pre-loaded Traps and MIBs for SNMP Collection, on page 264](#).

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

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

Following is an SNMP-Trap collection job sample:

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "TRAP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "a9b8f43d-130b-4866-a26a-4d0f9e07562a",
            "8c4431a0-f21d-452d-95a8-84323a19e0d6",
            "eaab2647-2351-40ae-bf94-6e4a3d79af3a"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "destination": {
```

```

        "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
        "context_id": "topic1_696600ae-80ee-4a02-96cb-3a01a2415324"
    }
}
]
}
}

```

Enabling Traps forwarding to external applications

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

Therefore, it is recommended to have a single SNMP Trap collection job per device (with any OID as sensor path) as it would be enough to get all traps from that device.



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

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

Below are some sample values and a sample payload:

- Link up

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4
```

- Link Down

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3
```

- Syslog

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1
```

- Cold Start

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1
```

```

{
  "nodeIdStr": "BF5-XRV9K1.tr3.es",
  "nodeIdUuid": "C9tZ5lJoSJKf5OZ67+U5JQ==",
  "collectionId": "133",
  "collectionStartTime": "1580931985267",
  "msgTimestamp": "1580931985267",
  "dataGpbkv": [
    {
      "timestamp": "1580931985267",
      "name": "trapsensor.path",
      "snmpTrap": {
        "version": "V2c",
        "pduType": "TRAP",
        "v2v3Data": {
          "agentAddress": "172.70.39.227",
          "oidRecords": [
            {
              "oid": "1.3.6.1.2.1.1.3.0",
              "strValue": "7 days, 2:15:17.02"
            }
          ]
        }
      }
    }
  ]
}

```

```

        {
          "oid": "1.3.6.1.6.3.1.1.4.1.0", // This oid is the Object Identifier.
          "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
kind of trap.
        },
        {
          "oid": "1.3.6.1.2.1.2.2.1.1.8",
          "strValue": "8"
        },
        {
          "oid": "1.3.6.1.2.1.2.2.1.2.8",
          "strValue": "GigabitEthernet0/0/0/2"
        },
        {
          "oid": "1.3.6.1.2.1.2.2.1.3.8",
          "strValue": "6"
        },
        {
          "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
          "strValue": "down"
        }
      ]
    }
  ],
  "collectionEndTime": "1580931985267",
  "collectorUuid": "YmNjZjEzMTktZjFlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBFQ09MTEVDVE9S",
  "status": {
    "status": "SUCCESS"
  },
  "modelData": {},
  "sensorData": {
    "trapSensor": {
      "path": "1.3.6.1.6.3.1.1.5.4"
    }
  },
  "applicationContexts": [
    {
      "applicationId": "APP1",
      "contextId": "collection-job-snmp-traps"
    }
  ]
}

```

MDT Collection Job

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

**Note**

- MDT collector retains the collection ID that comes as part of the telemetry proto for the device. This behavior is different from CLI and SNMP collectors which compute the collection ID based on the sequence number of the collection.
- MDT collection jobs require some configuration to be done on the device. This configuration is automatically taken care of by NSO.
- If there is some change (delete/update) in existing MDT jobs between backup and restore operations, Crosswork does not replay the jobs for config update on the devices as it involves Provider(NSO). You have to restore configs on provider/devices. Crosswork will just restore the jobs in database.
- Before using any YANG modules, check if they are supported. See Section: [List of Pre-loaded YANG Modules for MDT Collection](#) , on page 270.

It supports data collection for the following transport mode:

- MDT TCP Dial-out Mode

Following is a sample of MDT collection payload:

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

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

```

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

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

```

Monitoring Collection Jobs

Once a device is mapped to a Cisco Crosswork Data Gateway instance, the status of all the associated collection jobs is set to 'Unknown'. A job could have status as 'Unknown' for either of the following reasons:

- Cisco Crosswork Data Gateway has not yet reported its status.
- Loss of connection between Cisco Crosswork Data Gateway and Crosswork.
- Cisco Crosswork Data Gateway received the collection job, but actual collection is still pending.

After the collection job is processed, the status changes to 'Successful' if the processing was successful or else it changes to 'Failed'.

From the **Collection Jobs** view, you can monitor the status of the collection jobs currently active on all the Cisco Crosswork Data Gateway instances enrolled with Cisco Crosswork Change Automation and Health Insights, such as system jobs and API-defined collection jobs.

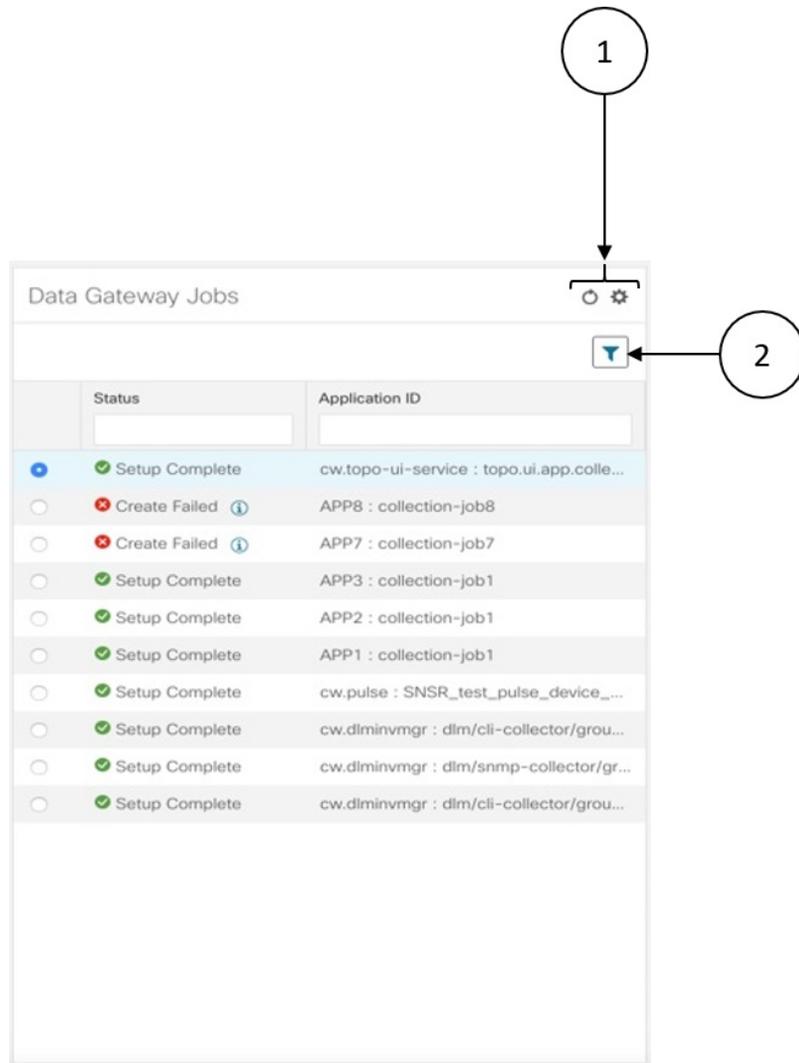
From the navigation bar, choose **Admin > Collection Jobs**.

The screenshot displays the Cisco Crosswork Network Automation interface. On the left is a navigation sidebar with icons for Home, Change Automation, Inventory Management, Health Insights, Network Visualization, and Admin. The main content area is split into two panes:

- Data Gateway Jobs Pane:** A table listing collection jobs with columns for Status and Application ID. Several jobs are listed with a status of 'Setup Complete'.
- Job Details Pane:** Shows details for a selected job: 'cw.topo-ui-service : topo.ui.app.collector.consumer'. It includes sections for Lifecycle Status (Setup Complete), Job Configuration (Config Details), Collection Type (SNMP), and Last Modified On (Fri Dec 13 2019 00:41:28 GMT+5:30). Below this is a process flow diagram showing 'Collections (4)' leading to 'Distributions (4)', with 'Data Gateways' and 'Destinations' also indicated. A table below the diagram shows 'Showing - All Collections (4) | Collection Issues (4)' with columns for Collection Status, Hostname, Sensor Data, and Last Status Change Reported Time. The table lists four entries for routers: RouterSanFrancisco, RouterFremont, RouterSFO, and RouterMilpitas, all with a status of 'Unknown' and sensor data of 'IF-MIB:IF-MIB:ifTable/ifEntry'.

Item	Description
Data Gateway Jobs Pane	Shows the list of all active collection jobs along with their status and application ID.
Job Details Pane	Shows the details of a particular job selected in the Data Gateway Jobs pane.

To view details of a collection job, select the collection job from the **Data Gateway Jobs** pane. The details of the selected job are displayed in the **Job Details** pane right next to the **Data Gateway Jobs** pane.



Item	Description
1	Click  to refresh the Data Gateway Jobs window.
	Click  to choose the columns to make visible in the Data Gateway Jobs window (see Set, Sort and Filter Table Data, on page 6).
2	Click  to show/hide the quick filters.
	Click the Clear All Filters link to clear any filter criteria you may have set.

Data Gateway Jobs pane displays only the status and application ID.



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.

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

The screenshot shows the 'Job Details' pane for a collection job. At the top, the job name and context are displayed: 'cw.topo-ui-service : topo.ui.app.collector.consumer'. Below this, there are four tabs: 'Lifecycle Status' (Setup Complete), 'Job Configuration' (Config Details), 'Collection Type' (SNMP), and 'Last Modified On' (Thu Dec 12 2019 11:11:28 PST). A navigation bar below the tabs shows 'Collections (4)' selected, with 'Distributions (4)' also visible. Below the navigation bar, there are four sections: 'Devices', 'Data Gateways', 'Destinations', and 'Collection Issues (4)'. The 'Collection Issues (4)' section contains a table with the following data:

Collection Status	Hostname	Device Id	Sensor Data	Last Status Change Reported Time
Unknown	RouterSanFrancisco	d112738f-c...	IF-MIB:IF-MIB/ifTable/IF-E...	Thu Dec 12 2019 12:13:53 PST
Unknown	RouterFremont	c700dde9-...	IF-MIB:IF-MIB/ifTable/IF-E...	Thu Dec 12 2019 12:13:53 PST
Unknown	RouterSFO	999d81a9-...	IF-MIB:IF-MIB/ifTable/IF-E...	Thu Dec 12 2019 12:13:53 PST
Unknown	RouterMilpitas	618d7e4f-2...	IF-MIB:IF-MIB/ifTable/IF-E...	Thu Dec 12 2019 12:13:53 PST

Item	Description
1	Application name and context associated with the collection job.
2	Lifecycle status of the collection job.

Item	Description
3	Job payload of the collection job that you pass in the REST API request. Click  icon next to Config Details to view the job configuration. Crosswork Data Gateway lets you view configuration in two modes: <ul style="list-style-type: none"> • View Mode • Text Mode
4	Collection Type
5	Time and date of last modification of the collection job.
6	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.
7	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.
8	Click  to refresh the Job Details window. Click  to choose the columns to make visible in the Job Details window (see Set, Sort and Filter Table Data, on page 6).
9	Click  to show/hide the quick filters. Click the Clear All Filters link to clear any filter criteria you may have set.

Job Details pane displays the following details about a collection job:

Field	Description
Collection/Distribution Status	Status of the collection/distribution. It is reported on a on change basis from Cisco 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.

Field	Description
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 Copy to Clipboard.</p> <p>and</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"> • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec <p>It shows the following metrics for a collection:</p> <ul style="list-style-type: none"> • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count
Last Status Change Reported Time	Time and date on which last status change was reported for that device sensor pair from Cisco Crosswork Data Gateway.

List of Pre-loaded Traps and MIBs for SNMP Collection

This section lists the traps and MIBs that the Collection Service 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 24: Supported Traps

Trap	OID
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
coldStart	1.3.6.1.6.3.1.1.5.1
isisAdjacencyChange	1.3.6.1.2.1.138.0.17

ADSL-LINE-MIB.mib	CISCO-LWAPP-INTERFACE-MIB.mib	IANA-ITU-ALARM-TC-MIB.mib
ADSL-TC-MIB.mib	CISCO-LWAPP-IPS-MIB.mib	IANA-LANGUAGE-MIB.mib
AGENTX-MIB.mib	CISCO-LWAPP-LINKTEST-MIB.mib	IANA-RTPROTO-MIB.mib
ALARM-MIB.mib	CISCO-LWAPP-LOCAL-AUTH-MIB.mib	IANAifType-MIB.mib
APS-MIB.mib	CISCO-LWAPP-MDNS-MIB.mib	IEEE8021-CFM-MIB.mib
ATM-FORUM-MIB.mib	CISCO-LWAPP-MESH-BATTERY-MIB.mib	IEEE8021-PAE-MIB.mib
ATM-FORUM-TC-MIB.mib	CISCO-LWAPP-MESH-LINKTEST-MIB.mib	IEEE8021-TC-MIB.mib
ATM-MIB.mib	CISCO-LWAPP-MOBILITY-EXT-MIB.mib	IEEE802171-CFM-MIB.mib
ATM-TC-MIB.mib	CISCO-LWAPP-MOBILITY-MIB.mib	IEEE8023-LAG-MIB.mib
ATM2-MIB.mib	CISCO-LWAPP-NETFLOW-MIB.mib	IEEE802dot11-MIB.mib
BGP4-MIB.mib	CISCO-LWAPP-REAP-MIB.mib	IF-INVERTED-STACK-MIB.mib
BRIDGE-MIB.mib	CISCO-LWAPP-RF-MIB.mib	IF-MIB.mib
CISCO-AAA-SERVER-MIB.mib	CISCO-LWAPP-SI-MIB.mib	IGMP-STD-MIB.mib
CISCO-AAA-SESSION-MIB.mib	CISCO-LWAPP-TC-MIB.mib	INET-ADDRESS-MIB.mib
CISCO-AAL5-MIB.mib	CISCO-LWAPP-TRUSTSEC-MIB.mib	INT-SERV-MIB.mib
CISCO-ACCESS-ENVMON-MIB.mib	CISCO-LWAPP-TSM-MIB.mib	INTEGRATED-SERVICES-MIB.mib

CISCO-ATM-EXT -MIB.mib	CISCO-LWAPP- WLAN-MIB.mib	IP-FORWARD-MIB.mib
CISCO-ATM- PVCTRAP-EXTN-MIB.mib	CISCO-LWAPP-WLAN -SECURITY-MIB.mib	IP-MIB.mib
CISCO-ATM- QOS-MIB.mib	CISCO-MEDIA- GATEWAY-MIB.mib	IPMCAST-MIB.mib
CISCO-AUTH- FRAMEWORK-MIB.mib	CISCO-MOTION-MIB.mib	IPMROUTE-MIB.mib
CISCO-BGP-POLICY -ACCOUNTING-MIB.mib	CISCO-MPLS-LSR -EXT-STD-MIB.mib	IPMROUTE-STD -MIB.mib
CISCO-BGP4-MIB.mib	CISCO-MPLS-TC -EXT-STD-MIB.mib	IPV6-FLOW-LABEL -MIB.mib
CISCO-BULK-FILE -MIB.mib	CISCO-MPLS-TE-STD -EXT-MIB.mib	IPV6-ICMP-MIB.mib
CISCO-CBP-TARGET -MIB.mib	CISCO-NAC-TC -MIB.mib	IPV6-MIB.mib
CISCO-CBP-TARGET -TC-MIB.mib	CISCO-NBAR-PROTOCOL -DISCOVERY-MIB.mib	IPV6-MLD-MIB.mib
CISCO-CBP-TC-MIB.mib	CISCO-NETSYNC -MIB.mib	IPV6-TC.mib
CISCO-CCME-MIB.mib	CISCO-NTP-MIB.mib	IPV6-TCP-MIB.mib
CISCO-CDP-MIB.mib	CISCO-OSPF- MIB.mib	IPV6-UDP-MIB.mib
CISCO-CEF-MIB.mib	CISCO-OSPF- TRAP-MIB.mib	ISDN-MIB.mib
CISCO-CEF-TC.mib	CISCO-OTN-IF-MIB.mib	ISIS-MIB.mib
CISCO-CLASS-BASED -QOS-MIB.mib	CISCO-PAE-MIB.mib	ITU-ALARM-MIB.mib
CISCO-CONFIG- COPY-MIB.mib	CISCO-PAGP-MIB.mib	ITU-ALARM-TC- MIB.mib
CISCO-CONFIG- MAN-MIB.mib	CISCO-PIM-MIB.mib	L2TP-MIB.mib
CISCO-CONTENT- ENGINE-MIB.mib	CISCO-PING-MIB.mib	LANGTAG-TC-MIB.mib
CISCO-CONTEXT- MAPPING-MIB.mib	CISCO-POLICY-GROUP -MIB.mib	LLDP-EXT-DOT1 -MIB.mib
CISCO-DATA -COLLECTION-MIB.mib	CISCO-POWER- ETHERNET-EXT-MIB.mib	LLDP-EXT-DOT3 -MIB.mib
CISCO-DEVICE-EXCEPTION -REPORTING-MIB.mib	CISCO-PRIVATE -VLAN-MIB.mib	LLDP-MIB.mib
CISCO-DIAL- CONTROL-MIB.mib	CISCO-PROCESS-MIB.mib	MAU-MIB.mib
CISCO-DOT11- ASSOCIATION-MIB.mib	CISCO-PRODUCTS- MIB.mib	MGMD-STD-MIB.mib
CISCO-DOT11-HT- PHY-MIB.mib	CISCO-PTP-MIB.mib	MPLS-FTN-STD- MIB.mib
CISCO-DOT11-IF-MIB.mib	CISCO-RADIUS- EXT-MIB.mib	MPLS-L3VPN-STD- MIB.mib

CISCO-DOT11-SSID-SECURITY-MIB.mib	CISCO-RF-MIB.mib	MPLS-LDP-ATM-STD-MIB.mib
CISCO-DOT3- OAM-MIB.mib	CISCO-RF-SUPPLEMENTAL-MIB.mib	MPLS-LDP-FRAME-RELAY-STD-MIB.mib
CISCO-DS3-MIB.mib	CISCO-RTTMON-TC -MIB.mib	MPLS-LDP-GENERIC-STD-MIB.mib
CISCO-DYNAMIC-TEMPLATE-MIB.mib	CISCO-SELECTIVE-VRF-DOWNLOAD-MIB.mib	MPLS-LDP-MIB.mib
CISCO-DYNAMIC-TEMPLATE-TC-MIB.mib	CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB.mib	MPLS-LDP-STD-MIB.mib
CISCO-EIGRP-MIB.mib	CISCO-SESS-BORDER-CTRLR-EVENT-MIB.mib	MPLS-LSR-MIB.mib
CISCO-EMBEDDED-EVENT-MGR-MIB.mib	CISCO-SESS-BORDER-CTRLR-STATS-MIB.mib	MPLS-LSR-STD-MIB.mib
CISCO-ENHANCED-IMAGE-MIB.mib	CISCO-SMI.mib	MPLS-TC-MIB.mib
CISCO-ENHANCED-MEMPOOL-MIB.mib	CISCO-SONET-MIB.mib	MPLS-TC-STD-MIB.mib
CISCO-ENTITY-ASSET -MIB.mib	CISCO-ST-TC.mib	MPLS-TE-MIB.mib
CISCO-ENTITY-EXT -MIB.mib	CISCO-STACKWISE- MIB.mib	MPLS-TE-STD-MIB.mib
CISCO-ENTITY-FRU-CONTROL-MIB.mib	CISCO-STP-EXTENSIONS-MIB.mib	MPLS-VPN-MIB.mib
CISCO-ENTITY- QFP-MIB.mib	CISCO-SUBSCRIBER-IDENTITY-TC-MIB.mib	MSDP-MIB.mib
CISCO-ENTITY-REDUNDANCY-MIB.mib	CISCO-SUBSCRIBER-SESSION-MIB.mib	NET-SNMP-AGENT-MIB.mib
CISCO-ENTITY-REDUNDANCY-TC-MIB.mib	CISCO-SUBSCRIBER-SESSION-TC-MIB.mib	NET-SNMP-EXAMPLES-MIB.mib
CISCO-ENTITY-SENSOR-MIB.mib	CISCO-SYSLOG-MIB.mib	NET-SNMP-MIB.mib
CISCO-ENTITY-VENDORTYPE-OID-MIB.mib	CISCO-SYSTEM-EXT- MIB.mib	NET-SNMP-TC.mib
CISCO-ENVMON-MIB.mib	CISCO-SYSTEM-MIB.mib	NHRP-MIB.mib
CISCO-EPM-NOTIFICATION-MIB.mib	CISCO-TAP2-MIB.mib	NOTIFICATION-LOG-MIB.mib
CISCO-ETHER-CFM- MIB.mib	CISCO-TC.mib	OLD-CISCO-CHASSIS-MIB.mib
CISCO-ETHERLIKE- EXT-MIB.mib	CISCO-TCP-MIB.mib	OLD-CISCO-INTERFACES-MIB.mib
CISCO-FABRIC- C12K-MIB.mib	CISCO-TEMP-LWAPP-DHCP-MIB.mib	OLD-CISCO-SYS- MIB.mib

CISCO-FIREWALL -TC.mib	CISCO-TRUSTSEC -SXP-MIB.mib	OLD-CISCO-SYSTEM -MIB.mib
CISCO-FLASH-MIB.mib	CISCO-TRUSTSEC -TC-MIB.mib	OPT-IF-MIB.mib
CISCO-FRAME- RELAY-MIB.mib	CISCO-UBE-MIB.mib	OSPF-MIB.mib
CISCO-FTP-CLIENT -MIB.mib	CISCO-UNIFIED- COMPUTING-ADAPTOR -MIB.mib	OSPF-TRAP-MIB.mib
CISCO-HSRP-EXT -MIB.mib	CISCO-UNIFIED- COMPUTING-COMPUTE -MIB.mib	OSPFV3-MIB.mib
CISCO-HSRP-MIB.mib	CISCO-UNIFIED- COMPUTING-ETHER -MIB.mib	P-BRIDGE-MIB.mib
CISCO-IETF-ATM2 -PVCTRAP- MIB.mib	CISCO-UNIFIED- COMPUTING-FC- MIB.mib	PIM-MIB.mib
CISCO-IETF-BFD -MIB.mib	CISCO-UNIFIED- COMPUTING-MEMORY -MIB.mib	PIM-STD-MIB.mib
CISCO-IETF-FRR -MIB.mib	CISCO-UNIFIED- COMPUTING -MIB.mib	POWER-ETHERNET -MIB.mib
CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED- COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED- COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED- COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS- TE-EXT-STD-03- MIB.mib	CISCO-VLAN- IFTABLE-RELATIONSHIP -MIB.mib	PTOPO-MIB.mib
CISCO-IETF-MPLS- TE-P2MP-STD-MIB.mib	CISCO-VLAN- MEMBERSHIP-MIB.mib	PerfHist-TC-MIB.mib
CISCO-IETF-MSDP -MIB.mib	CISCO-VOICE-COMMON -DIAL-CONTROL-MIB.mib	Q-BRIDGE-MIB.mib
CISCO-IETF-PIM-EXT -MIB.mib	CISCO-VOICE-DIAL -CONTROL-MIB.mib	RADIUS-ACC-CLIENT -MIB.mib
CISCO-IETF-PIM -MIB.mib	CISCO-VOICE-DNIS -MIB.mib	RADIUS-AUTH-CLIENT -MIB.mib
CISCO-IETF-PW- ATM-MIB.mib	CISCO-VPDN-MGMT -MIB.mib	RFC-1212.mib
CISCO-IETF-PW- ENET-MIB.mib	CISCO-VTP-MIB.mib	RFC-1215.mib
CISCO-IETF-PW-MIB.mib	CISCO-WIRELESS- NOTIFICATION-MIB.mib	RFC1155-SMI.mib

CISCO-IETF-PW- MPLS-MIB.mib	CISCO-SB-DEVICEPARAMS -MIB.mib	RFC1213-MIB.mib
CISCO-IETF-PW -TC-MIB.mib	CISCO-SB- HWENVIRONMENT.mib	RFC1315-MIB.mib
CISCO-IETF-PW -TDM-MIB.mib	CISCO-SB-MIB.mib	RFC1398-MIB.mib
CISCO-IETF-VPLS -BGP-EXT-MIB.mib	CISCO-SB-Physicaldescription -MIB.mib	RIPv2-MIB.mib
CISCO-IETF-VPLS -GENERIC-MIB.mib	DIAL-CONTROL-MIB.mib	RMON-MIB.mib
CISCO-IETF-VPLS- LDP-MIB.mib	DIFFSERV-DSCP-TC.mib	RMON2-MIB.mib
CISCO-IF-EXTENSION -MIB.mib	DIFFSERV-MIB.mib	RSTP-MIB.mib
CISCO-IGMP-FILTER -MIB.mib	DISMAN-NSLOOKUP -MIB.mib	RSVP-MIB.mib
CISCO-IMAGE-LICENSE -MGMT-MIB.mib	DISMAN-PING-MIB.mib	SMON-MIB.mib
CISCO-IMAGE-MIB.mib	DISMAN-SCHEDULE -MIB.mib	SNA-SDLC-MIB.mib
CISCO-IMAGE-TC.mib	DISMAN-SCRIPT-MIB.mib	SNMP-COMMUNITY -MIB.mib
CISCO-IP-LOCAL- POOL-MIB.mib	DISMAN-TRACEROUTE -MIB.mib	SNMP-FRAMEWORK -MIB.mib
CISCO-IP-TAP-MIB.mib	DOT3-OAM-MIB.mib	SNMP-MPD-MIB.mib
CISCO-IP-URPF-MIB.mib	DRAFT-MSDP-MIB.mib	SNMP-NOTIFICATION -MIB.mib
CISCO-IPMROUTE- MIB.mib	DS0-MIB.mib	SNMP-PROXY-MIB.mib
CISCO-IPSEC-FLOW -MONITOR-MIB.mib	DS1-MIB.mib	SNMP-REPEATER -MIB.mib
CISCO-IPSEC-MIB.mib	DS3-MIB.mib	SNMP-TARGET-MIB.mib
CISCO-IPSEC-POLICY -MAP-MIB.mib	ENTITY-MIB.mib	SNMP-USER-BASED -SM-MIB.mib
CISCO-IPSLA- AUTOMEASURE-MIB.mib	ENTITY-SENSOR-MIB.mib	SNMP-USM-AES -MIB.mib
CISCO-IPSLA- ECHO-MIB.mib	ENTITY-STATE-MIB.mib	SNMP-USM-DH- OBJECTS-MIB.mib
CISCO-IPSLA- JITTER-MIB.mib	ENTITY-STATE- TC-MIB.mib	SNMP-VIEW- BASED-ACM-MIB.mib
CISCO-IPSLA- TC-MIB.mib	ESO-CONSORTIUM -MIB.mib	SNMPv2-CONF.mib
CISCO-ISDN-MIB.mib	ETHER-WIS.mib	SNMPv2-MIB.mib
CISCO-LICENSE- MGMT-MIB.mib	EtherLike-MIB.mib	SNMPv2-SMI.mib
CISCO-LOCAL- AUTH-USER-MIB.mib	FDDI-SMT73-MIB.mib	SNMPv2-TC-v1.mib

CISCO-LWAPP- AAA-MIB.mib	FR-MFR-MIB.mib	SNMPv2-TC.mib
CISCO-LWAPP- AP-MIB.mib	FRAME-RELAY -DTE-MIB.mib	SNMPv2-TM.mib
CISCO-LWAPP- CCX-RM-MIB.mib	FRNETSERV- MIB.mib	SONET-MIB.mib
CISCO-LWAPP- CDP-MIB.mib	GMPLS-LSR- STD-MIB.mib	SYSAPPL-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-CAPABILITY.mib	GMPLS-TC-STD- MIB.mib	TCP-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-MIB.mib	GMPLS-TE-STD-MIB.mib	TOKEN-RING-RMON -MIB.mib
CISCO-LWAPP-DHCP -MIB.mib	HC-PerfHist-TC-MIB.mib	TOKENRING-MIB.mib
CISCO-LWAPP-DOT11- CLIENT-CALIB-MIB.mib	HC-RMON-MIB.mib	TRANSPORT-ADDRESS -MIB.mib
CISCO-LWAPP-DOT11- CLIENT-CCX-TC-MIB.mib	HCNUM-TC.mib	TUNNEL-MIB.mib
CISCO-LWAPP-DOT11 -LDAP-MIB.mib	HOST-RESOURCES -MIB.mib	UDP-MIB.mib
CISCO-LWAPP- DOT11-MIB.mib	HOST-RESOURCES -TYPES.mib	VPN-TC-STD-MIB.mib
CISCO-LWAPP -DOWNLOAD-MIB.mib	IANA-ADDRESS- FAMILY-NUMBERS-MIB.mib	VRRP-MIB.mib
CISCO-LWAPP- IDS-MIB.mib	IANA-GMPLS-TC-MIB.mib	

List of Pre-loaded YANG Modules for MDT Collection

This section lists the YANG modules that the Collection Service 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-ntp-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-ntp-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-perfmngmt-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-sdacc-oper.yang
Cisco-IOS-XR-controller-otu-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-npu-stats-oper.yang
Cisco-IOS-XR-subscriber-accounting-oper.yang	Cisco-IOS-XR-alarmgr-server-oper.yang
Cisco-IOS-XR-ncs5500-qos-oper.yang	Cisco-IOS-XR-fia-internal-tcam-oper.yang
Cisco-IOS-XR-skywarp-netflow-oper.yang	Cisco-IOS-XR-tty-server-oper.yang
Cisco-IOS-XR-ncs1k-mxp-lldp-oper.yang	Cisco-IOS-XR-qos-ma-oper.yang
Cisco-IOS-XR-fib-common-oper.yang	Cisco-IOS-XR-aaa-protocol-radius-oper.yang
Cisco-IOS-XR-dnx-netflow-oper.yang	Cisco-IOS-XR-platform-pifib-oper.yang
Cisco-IOS-XR-lpts-pa-oper.yang	Cisco-IOS-XR-asr9k-fsi-oper.yang
Cisco-IOS-XR-ncs1k-mxp-oper.yang	Cisco-IOS-XR-ncs5500-coherent-node-oper.yang
Cisco-IOS-XR-asr9k-sc-invmgr-oper.yang	Cisco-IOS-XR-snmp-ifmib-oper.yang
Cisco-IOS-XR-ptp-pd-oper.yang	Cisco-IOS-XR-ip-mobileip-oper.yang
Cisco-IOS-XR-ethernet-cfm-oper.yang	Cisco-IOS-XR-wdsysmon-fd-oper.yang
Cisco-IOS-XR-pbr-oper.yang	Cisco-IOS-XR-infra-objmgr-oper.yang
Cisco-IOS-XR-ip-rsvp-oper.yang	Cisco-IOS-XR-ipv6-io-oper.yang
Cisco-IOS-XR-terminal-device-oper.yang	Cisco-IOS-XR-plat-chas-invmgr-ng-oper.yang
Cisco-IOS-XR-mpls-oam-oper.yang	Cisco-IOS-XR-ncs5500-coherent-portmode-oper.yang
Cisco-IOS-XR-sse-span-oper.yang	Cisco-IOS-XR-infra-dumper-oper.yang
Cisco-IOS-XR-asr9k-sc-diag-oper.yang	Cisco-IOS-XR-mpls-io-oper.yang



APPENDIX **A**

Device and Credentials Sync With Cisco NSO

This section contains the following topics:

- [Add Devices and Credential Profiles By Synchronizing With Cisco NSO, on page 275](#)

Add Devices and Credential Profiles By Synchronizing With Cisco NSO

If you are currently using Cisco Network Services Orchestrator (Cisco NSO) to manage your network devices, you may be able to perform a bulk upload of your Cisco NSO devices to Cisco Crosswork Change Automation and Health Insights by synchronizing the two systems. Cisco strongly recommends that you undertake this synchronization only once, and only with the direct assistance of your Cisco CX account team.



Note

If you encounter NSO read timeout error while pushing configuration, increase the NSO timeout from 20 to 120 seconds by editing the `ncs.conf` file with `set devices global-settings read-timeout 120`.

Before you begin

To perform this task, you will need:

- A Cisco NSO server that is fully populated with the devices you want to add.
- The protocol, IP address, port, administrative user name and password needed to connect to the Cisco NSO server.
- Access to a text editor that you can use to edit the Cisco NSO server `ncs.conf` file.
- The parameters required to add Cisco NSO as a Cisco Crosswork Change Automation and Health Insights provider.
- The SNMP community strings and other credentials that Cisco NSO uses to access the devices you want to add to Cisco Crosswork Change Automation and Health Insights.

You will also need to ensure that you have pre-configured your devices to work with Cisco Crosswork Change Automation and Health Insights, as explained in [Prerequisites for Onboarding Devices, on page 91, Sample](#)

[Configuration for Devices in Cisco NSO, on page 93](#) and [Prerequisites for Device Model Driven Telemetry, on page 239](#).

Step 1 On the Cisco NSO server: Access and edit the `ncs.conf` file to enable port 8080 and then restart the server with a package reload:

- Access the Cisco NSO command line interface (CLI) via SSH. For example: `myname@host$:ssh NSOadmin@NSOserverIPAddress`. Supply the Cisco NSO administrator password when prompted.
- Navigate to the `ncs.conf` file, which is usually located under `./home/nso/`.
- Make a backup copy of the current `ncs.conf`. Use the date in the file name to identify it as a backup. For example: `cp ncs.conf ncs.conf-1-1-2019`.
- Edit the `ncs.conf` file's `<webui>` parameters to include the following (the critical enabling command is **highlighted**):

```
<webui>
  <enabled>true</enabled>
  <transport>
    <tcp>
      <enabled>true</enabled>
      <ip>0.0.0.0</ip>
      <port>8080</port>
    </tcp>
```

- Restart the server and its packages by running the following commands in this order:

```
[root@localhost ncs-run]# source /home/nso/nso-5.2/ncsrc
```

To start NSO:

```
[root@localhost ncs-run]# ncs
```

To stop NSO:

```
[nso@localhost ncs-run]$ ncs --stop
```

Step 2 Log into Cisco Crosswork Change Automation and Health Insights and set up Cisco NSO as a provider, with the credentials needed to connect to Cisco NSO and to the imported devices:

- Create a credential profile for the Cisco NSO devices, as explained in [Create Credential Profiles, on page 82](#). Be sure to include in the credential profile at least the SNMP credentials that Cisco NSO uses to manage these devices; you can create multiple sets of SNMP credentials in the profile, as well as credentials for other protocols.
- Create an HTTP credential profile for the Cisco NSO server.
- Add Cisco NSO as a provider, as explained in [Add Providers Through the UI, on page 173](#). Be sure to assign to the Cisco NSO provider the HTTP credential profile you just created.
- Before logging out of the Cisco Crosswork Change Automation and Health Insights user interface, take note of the names you assigned to the Cisco NSO provider. You will need them to finish the next step.

Step 3 Synchronize Cisco Crosswork Change Automation and Health Insights's Inventory Management application with Cisco NSO's inventory services, as follows:

- Access the Cisco Crosswork Change Automation and Health Insights CLI using SSH and the administrator ID. For example: `myname@host$:ssh cw-admin@CrossworkServerIPAddress`.

```
myname@host$:ssh cw-admin@CrossworkServerIPAddress
```

When prompted, enter the administrator password.

- Switch to superuser status:

```
myname@host$:sudo su
```

When prompted, enter the administrator password.

- c) Enter the following command to find the component ID for the Inventory Management Kubernetes pod container:

```
kubectl get pods | grep dlmi
```

The response will contain the component ID as a hash appended to the pod name: `robot-dlminvmgr-componentID`

- d) Enter the following command to access the Inventory Management Kubernetes container:

```
kubectl exec -it robot-dlminvmgr-componentID bash
```

Where *componentID* is the ID you retrieved in the previous step.

- e) Synchronize Cisco NSO inventory services with Inventory Management using the following command:

```
bash# syncsvc --cwhost CrossworkServerIPAddress --cwuser CrossworkAdminUser --cwpass  
'CrossworkAdminPassword' --provpass NSOAdminPassword --provider ProviderName --oper get
```

Where:

- *CrossworkServerIPAddress* is the IP address of the Cisco Crosswork Change Automation and Health Insights server.
- *CrossworkAdminUser* is the user name of the Cisco Crosswork Change Automation and Health Insights administrator (**cw-admin**).
- *CrossworkAdminPassword* is the password for the Cisco Crosswork Change Automation and Health Insights cw-admin user.
- *NSOAdminPassword* is the password for the Cisco NSO admin user.
- *ProviderName* is the name of the Cisco NSO provider you created.

Synchronization will begin as soon as connection is established. When device processing is finished, verify that the sync added all the Cisco NSO devices to Cisco Crosswork Change Automation and Health Insights successfully.



APPENDIX **B**

Configure Cisco Crosswork Data Gateway Base VM

This appendix describes how to configure a Cisco Crosswork Data Gateway Base VM.

This section contains the following topics:

- [About Cisco Crosswork Data Gateway Base VM, on page 279](#)
- [Basic Concepts, on page 282](#)
- [Manage Users, on page 283](#)
- [View Current System Settings, on page 286](#)
- [Change Current System Settings, on page 290](#)
- [Monitor Cisco Crosswork Data Gateway Health, on page 299](#)
- [Troubleshooting, on page 305](#)

About Cisco Crosswork Data Gateway Base VM

A Cisco Crosswork Data Gateway instance is created as a standalone VM and can be geographically separate from the controller application (the controller application could be Crosswork Cloud or a Crosswork On-Prem application, such as Cisco Crosswork Change Automation and Health Insights). This Base VM is capable of connecting to the controller application and enable data collection from the network.

Crosswork orchestrates the collection from the distributed Cisco Crosswork Data Gateway VM instances.

The Cisco Crosswork Data Gateway VM is delivered as an OVA file and the additional functional images are delivered as Docker images.

Base VM Contents

The Base VM (OVA) is pre-packaged with basic functionality required to reach the controller application.

The Cisco Crosswork Data Gateway VM (OVA) contains the following pre-packaged contents:

- Cisco hardened Ubuntu distribution of Linux
- Cisco Crosswork Data Gateway services:
 - Vitals Monitor - Monitors resource usage on the VM.

- Controller Gateway – Establishes trusted connection with the controller application via the Controller Gateway and downloads functional images and configuration files.
- Image Manager – Coordinates between the Cisco Crosswork Data Gateway and the controller application to download functional images and configuration files.
- Route Manager – Directs traffic to devices on different south-bound destinations and also connects to the controller application and data devices via the north-bound interface.
- Docker IPv6nat - Programs IPv6 routes for docker containers.



Note Functional images (CLI, SNMP, and MDT collectors) are not included in the Base VM. They are downloaded by Cisco Crosswork Data Gateway from the controller application after successful authentication and bootstrap.

Log In and Log Out

You can use either of the following two ways to access Cisco Crosswork Data Gateway:

- [Access Cisco Crosswork Data Gateway Through vCenter, on page 280](#)
- [Access Cisco Crosswork Data Gateway Via SSH, on page 280](#)

Access Cisco Crosswork Data Gateway Through vCenter

Follow these steps to log in via vCenter:

-
- Step 1** Locate the VM in vCenter and then right click and select **Open Console**.
The Cisco Crosswork Data Gateway flash screen comes up.
- Step 2** Enter username (`dg-admin` or `dg-oper` as per the role assigned to you) and the corresponding password (the one that you created during installation process) and press **Enter**.
-

Access Cisco Crosswork Data Gateway Via SSH



Note The SSH process is protected from brute force attacks by blocking the client IP after a number of login failures. Failures such as incorrect username or password, connection disconnect, or algorithm mismatch are counted against the IP. Up to 4 failures within a 20 minute window will cause the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures will cause the blocked time to be increased. Each client IP is tracked separately.

Follow these steps to login via SSH.

- Step 1** Run the following command:

```
ssh <username>@<ManagementNetworkIP>
```

where **ManagementNetworkIP** is the management network IP address.

For example,

To login as administrator user: `ssh dg-admin@<ManagementNetworkIP>`

To login as operator user: `ssh dg-oper@<ManagementNetworkIP>`

The Cisco Crosswork Data Gateway flash screen opens prompting for password.

Step 2 Input the corresponding password (the one that you created during installation process) and press **Enter**.

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 [Supported User Roles, on page 283](#).

```
Cisco Crosswork
Main Menu - Please Choose an Option:

 1 Export Enrollment Package
 2 Show System Settings
 3 Change Current System Settings
 4 Vitals
 5 Troubleshooting
 p Change Passphrase
 | Logout

< K >
```

The Main Menu presents the following options:

1. Export Enrollment Package
2. Show System Settings
3. Change Current System Settings

4. Vitals
 5. Troubleshooting
- p. Change Passphrase
- l. Logout

Basic Concepts

Cisco Crosswork Data Gateway makes extensive use of certain concepts. It is helpful to be familiar with them before you get started.

Cisco Crosswork Data Gateway Components

Cisco Crosswork Data Gateway has the following five main components or services:

- [Controller Gateway, on page 282](#)
- [Image Manager, on page 282](#)
- [Vitals Monitor, on page 283](#)
- [Route Manager, on page 283](#)
- [Docker IPv6nat, on page 283](#)

Controller Gateway

Controller Gateway is the component responsible for all the interaction between a Cisco Crosswork Data Gateway instance and its controller application. It manages the session creation with the controller application and makes sure all the payloads and responses are signed and verified for integrity. Components such as Image Manager, Vitals Monitor, and Route manager interact via Controller Gateway with the controller application to exchange the details those components need.



Note

When the Controller Gateway stops, any alerts are not updated in `cdg-alerts.log`. However, when it starts, it sends an alert that it has started. This is because all the alerts go through the Controller Gateway and if it is down, the controller application won't receive the alerts. To access log files, see [Run show-tech, on page 309](#).

Image Manager

The Image Manager starts up when Cisco Crosswork Data Gateway VM boots. It downloads the functional images from the repository as instructed by the controller application and brings up the services.

It has the following responsibilities:

- Periodically pull boot-config file from the controller application via Controller Gateway.
- Based on the boot-config and local images metadata cache, determine if the functional images and docker-compose file need to be downloaded.

- Send appropriate alerts to the controller application, if there are issues while processing the boot-config.
- Stop and remove any services that are no longer called for in the latest boot-config.
- Cleanup the local images metadata cache to keep it synchronized with the latest boot-config received from the controller application.
- Downloads collectors environment and other files that facilitate establishment of connection between collectors and Crosswork.
- Downloads system device packages and MIB packages required by the collectors from Crosswork.
- Downloads custom software to the collectors when uploaded via Crosswork UI.



Note Functional images are downloaded only when there is a change in boot-config response.

Vitals Monitor

The Vitals Monitor monitors the health and vitals of the Cisco Crosswork Data Gateway VM. It collects the CPU, memory, disk usage, docker containers metrics, etc. and aggregates this information in a file on the host filesystem.

For more information, see [Monitor Cisco Crosswork Data Gateway Health, on page 299](#).

Route Manager

Route Manager manages south-bound routes to devices and north-bound routes to data destinations based on add/delete requests from collector upon the updates of inventory and collection jobs.

Route manager adds/deletes the static routes by comparing the existing routes configured on the VM with the routes configuration. This configuration is pushed to the Route Manager by the controller application in case of Crosswork On-Premise deployment.

Appropriate alerts are sent to the controller application if there is any failure in processing route request.

Docker IPv6nat

docker-ipv6nat is a special process that programs ipv6 routes for docker containers.

Manage Users

This section contains the following topics:

- [Supported User Roles, on page 283](#)
- [Change Password, on page 285](#)

Supported User Roles

Cisco Crosswork Data Gateway supports only two users with the following user roles:

- **Administrator:** One default user with administrator role is created when Cisco Crosswork Data Gateway is brought up for the first time. This user cannot be deleted and has both read and write privileges such as start/shut down Cisco Crosswork Data Gateway, register an application, apply authentication certificates, configure server settings, and perform kernel upgrade.
- **Operator:** This user is also created by default during the initial VM bring up. Operator can review the state/health of the Cisco Crosswork Data Gateway, retrieve health/error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.



Note

- Both users' credentials are configured during Cisco Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

Table 25: Permissions Per Role

Permissions	Administrator	Operator
Export enrollment package	✓	✓
Show system settings		
vNIC Addresses	✓	✓
NTP		
DNS		
Proxy		
UUID		
Syslog		
Certificates		
First Boot Provisioning Log		
Change Current System Settings		
Configure NTP	✓	×
Configure DNS		
Configure Control Proxy		
Configure Static Routes		
Configure Syslog		
Create new SSH keys		
Import Certificate		
vNIC1 MTU		
Vitals		

Permissions	Administrator	Operator
Docker Containers	✓	✓
Docker Images		
Controller Reachability		
NTP Reachability		
Route Table		
ARP Table		
Network Connections		
Disk Space Usage		
Troubleshooting		
Ping a Host	✓	✓
Traceroute to a Host	✓	✓
NTP Status	✓	✓
System Uptime	✓	✓
Run show-tech	✓	✓
Remove All Collectors and Reboot VM	✓	×
Reboot VM	✓	×
Test SSH Connection	✓	✓
Change Passphrase	✓	✓

Change Password

Both Administrator and Operator users can change their own passphrases but not each others'.

Follow these steps to change your passphrase:

Step 1 From the Main Menu, select **p Change Passphrase** and click **OK**.

Step 2 Input your current password and press Enter.

```
Changing password for dg-admin.
(current) UNIX password: [ ]
```

Step 3 Enter new password and press Enter. Re-type the new password and press Enter.

```
Changing password for dg-admin.  
[(current) UNIX password:  
[Enter new UNIX password:  
[Retype new UNIX password:
```

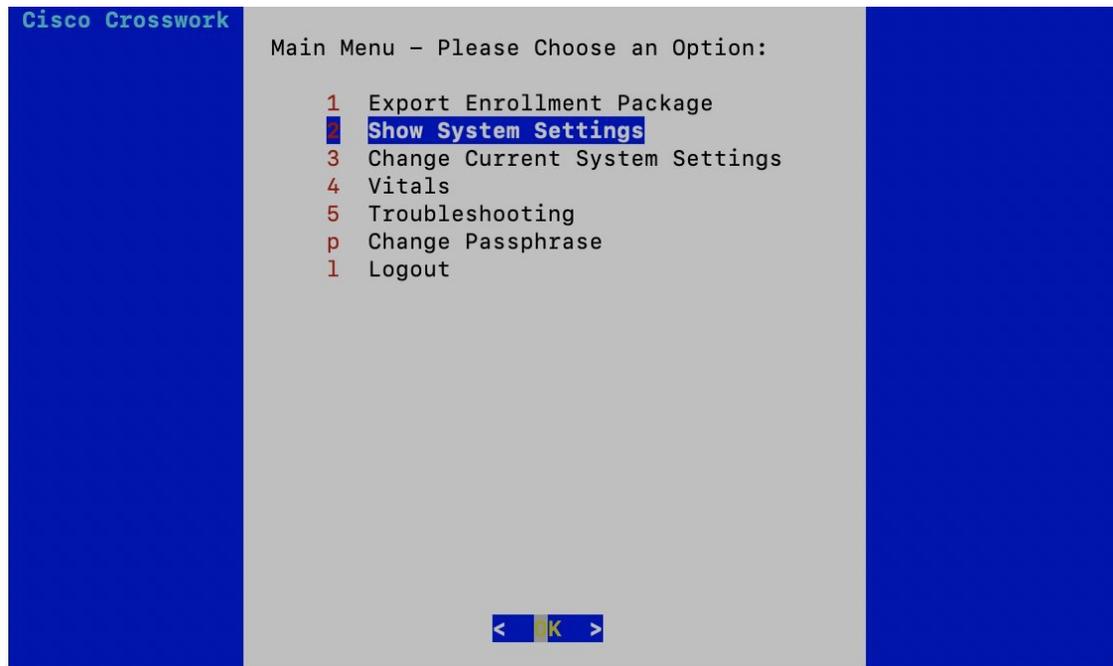
View Current System Settings

Cisco Crosswork Data Gateway allows you to view the following settings:

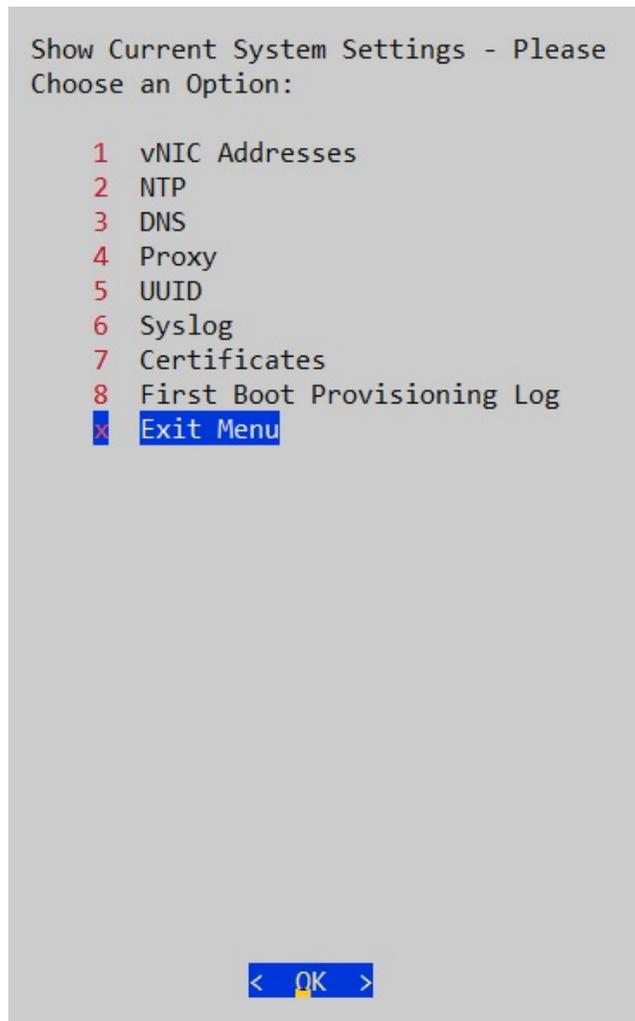
- vNIC Addresses
- NTP
- DNS
- Proxy
- UUID
- Syslog
- Certificates
- First Boot Provisioning Log

Follow these steps to view the current system settings:

Step 1 From the Main Menu, select **2 Show System Settings**, as shown in the following figure:



Step 2 Click **OK**. The **Show Current System Settings** menu opens.



Step 3 Select the setting you want to view.

Setting Option	Description
1 vNIC Addresses	Displays the addresses of the vNIC0, vNIC1, and vNIC2 interfaces.

Setting Option	Description
2 NTP	<p>Displays NTP settings.</p> <p>It is important that NTP time be synchronized with the controller application and its Cisco Crosswork Data Gateway instances.</p> <p>If not, then session handshake doesn't happen and functional images are not downloaded. In such cases, error message <code>clock time not matched and sync failed</code> is logged in <code>controller-gateway.log</code>. To access log files, see Run show-tech, on page 309.</p> <p>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 Cisco Crosswork Data Gateway instance. See View Cisco Crosswork Data Gateway Vitals, on page 299. If NTP has been set incorrectly, you will see error Session not established.</p> <p>To configure NTP settings, see Configure NTP, on page 292.</p>
3 DNS	Displays addresses of the DNS servers.
4 Proxy	Displays proxy server settings if there's any.
5 UUID	Displays the unique identifier of the Cisco Crosswork Data Gateway VM.
6 Syslog	<p>Displays syslog settings.</p> <p>The Controller Gateway doesn't send a start event to the Syslog server. Also, SNMP, MDT, and CLI events are not updated in the local syslog file, but are sent to the external syslog server. To configure syslog settings, see Configure Syslog, on page 296.</p>
7 Certificates	<p>Provides the following options to view certificate files:</p> <ul style="list-style-type: none"> • Collector certificate file • Controller signing certificate file • Controller SSL/TLS certificate file • Syslog certificate file
8 First Boot Provisioning Log	Displays the first boot provisioning log.

- Step 4** Click **OK**. Cisco Crosswork Data Gateway displays the selected setting.
- After you are done viewing the settings, press any key to return to the **Show Current System Settings** menu.

To return to the Main Menu, select **x Exit Menu** and click **OK**.

Change Current System Settings

**Note**

- Cisco Crosswork Data Gateway System settings can only be configured by the Administrator.
 - In 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
```

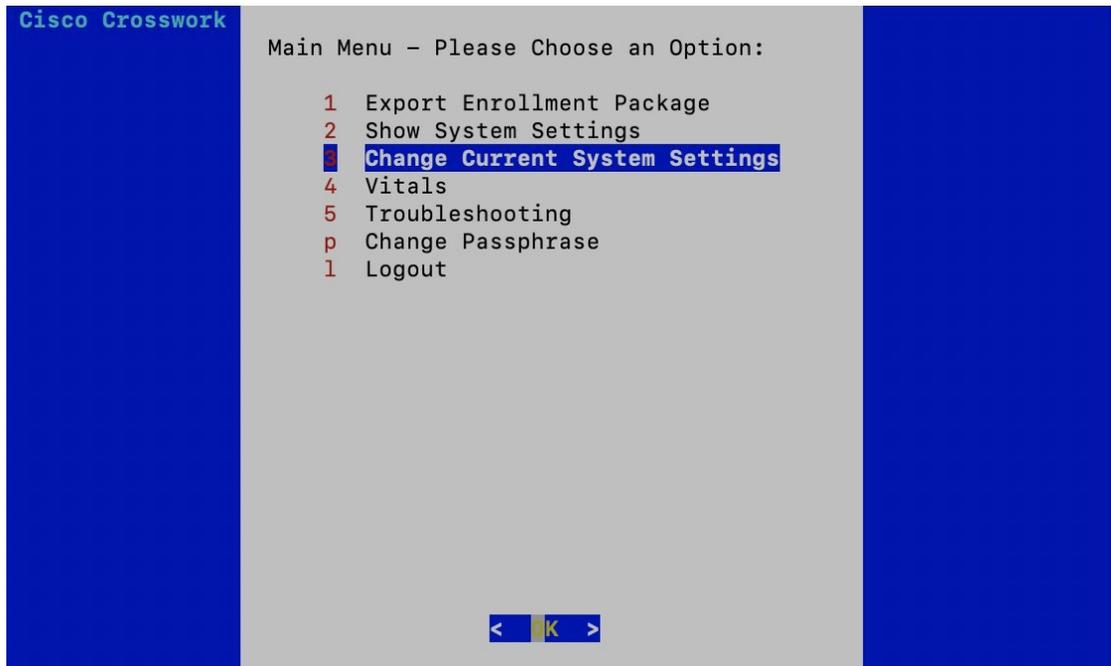
where 55 is a custom port.
-

Cisco Crosswork Data Gateway allows you to change the following settings:

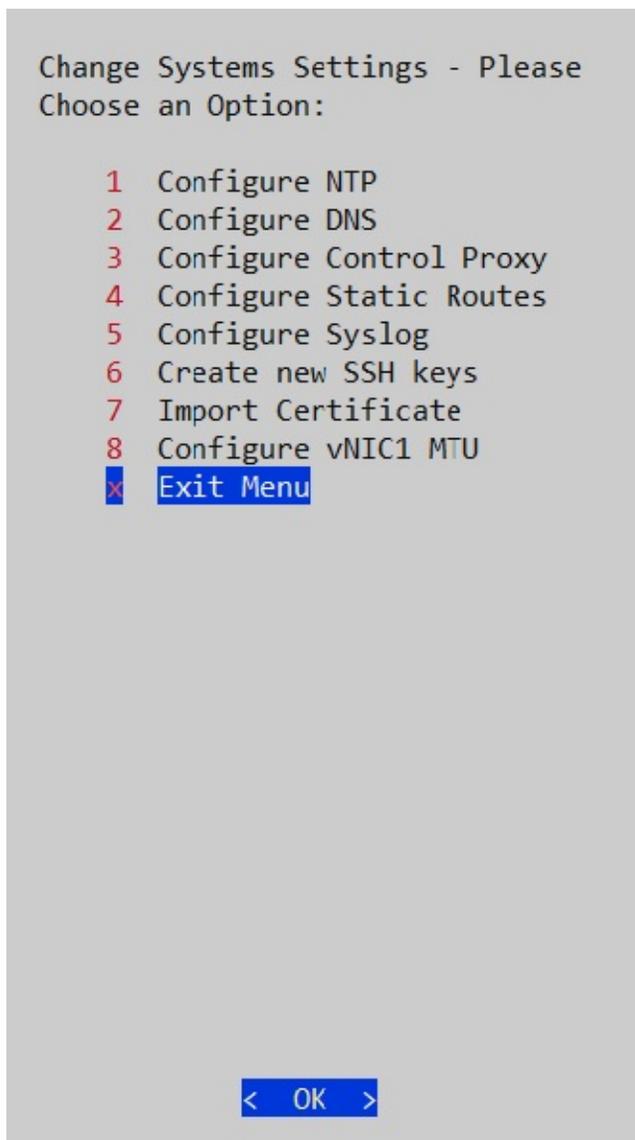
- NTP
- DNS
- Control Proxy
- Static routes
- Syslog
- SSH keys
- Certificate
- vNIC1 MTU

Follow these steps to change the current system settings:

Step 1 From the Main Menu, select **3 Change Current System Settings**, as shown in the following figure.



Step 2 Click **OK**. The **Change System Settings** menu opens.



Step 3 Select the setting you want to change.

Step 4 Click **OK**. Cisco Crosswork Data Gateway prompts you to input new value for the selected setting.

Step 5 After you have entered the new settings, click **OK** to save the settings and return to the **Change System System Settings** menu.

To return to the Main Menu, select **x Exit Menu** and click **OK**.

Configure NTP

Step 1 From the **Change Current System Settings** Menu, select **1 Configure NTP** and click **OK**.

- Step 2** Enter the new NTP server.
- Step 3** Click **OK** to save the settings.
-

Configure DNS

- Step 1** From the **Change Current System Settings** menu, select **2 Configure DNS** and click **OK**.
- Step 2** Enter the new DNS domain and server address.
- Step 3** Click **OK** to save the settings.
-

Configure Control Proxy

- Step 1** From the **Change Current System Settings** menu, select **3 Configure Control Proxy** and click **OK**.
- Step 2** Enter the new Proxy server URL and the exception list.
- Step 3** Click **OK** to save the settings.
-

Configure Static Routes

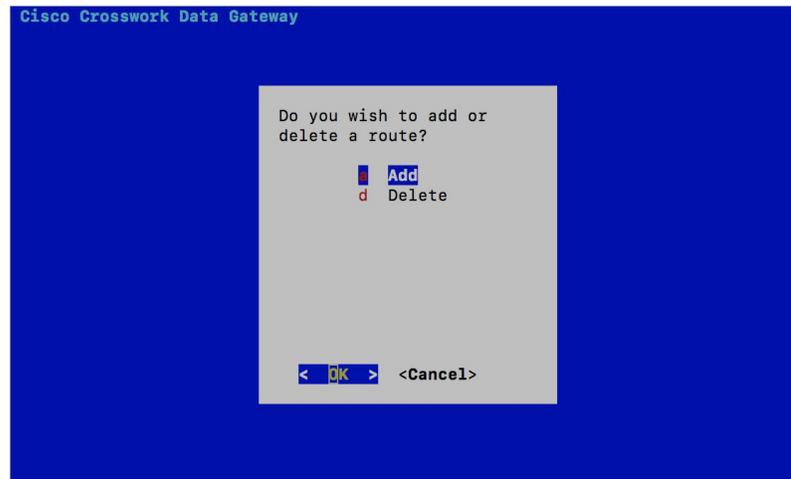
In Cisco Crosswork Data Gateway, the static routes are configured when the Route Manager receives add/delete requests from the collectors. The **Configure Static Routes** option from the main menu can be used for troubleshooting purpose.



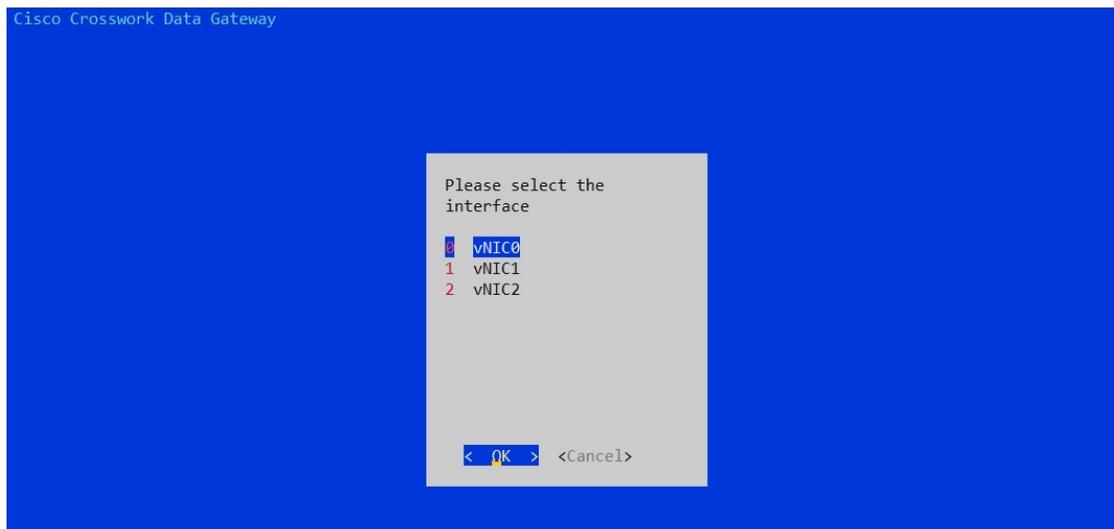
Note Static routes configured using this option are lost when the Cisco Crosswork Data Gateway reboots.

Add Static Routes

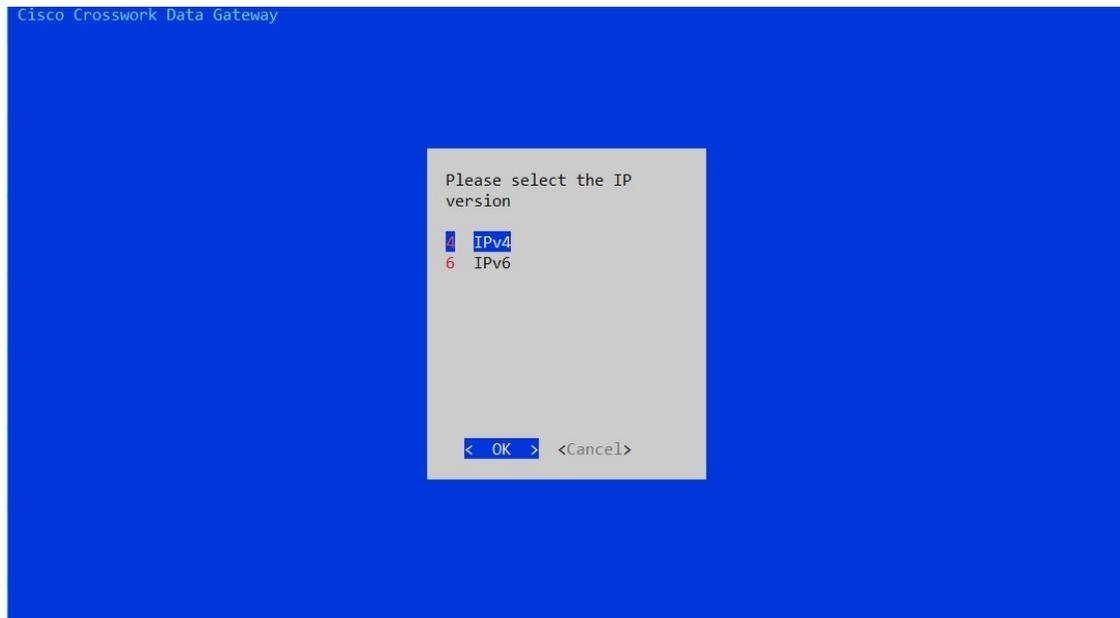
- Step 1** From the **Change Current System Settings** menu, select **4 Configure Static Routes** and click **OK**.
- Step 2** To add a static route, select **a Add** and click **OK**.



Step 3 Select the interface for which you want to add a static route and click **OK**.



Step 4 Select the IP address version for which you want to add a route and click **OK**.



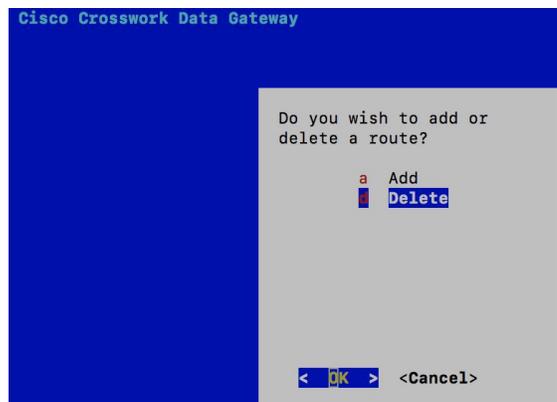
Step 5 Enter IPv4/IPv6 subnet in CIDR format when prompted.

Step 6 Click **OK** to save the settings.

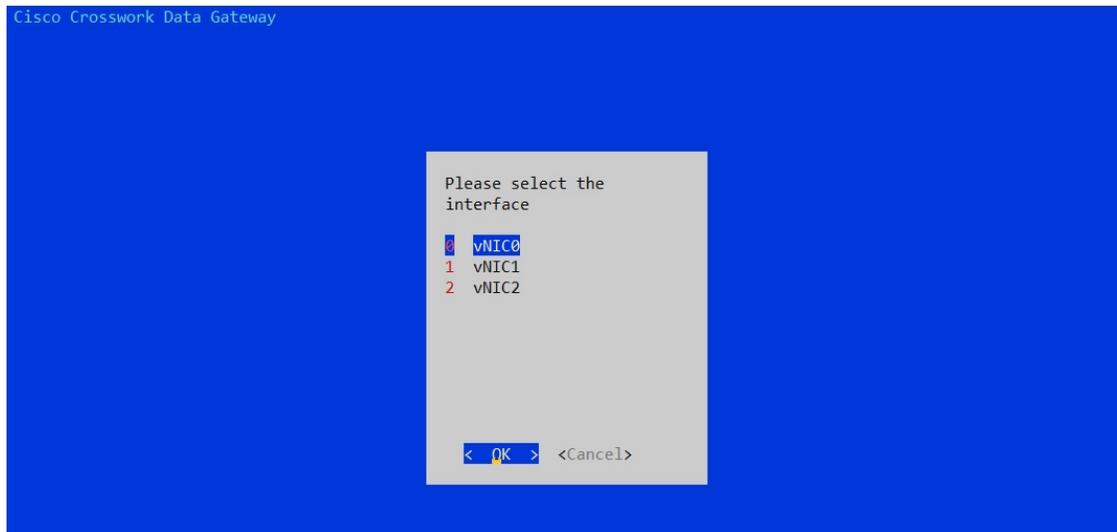
Delete Static Routes

Step 1 From the **Change Current System Settings** Menu, select **4 Configure Static Routes** and click **OK**.

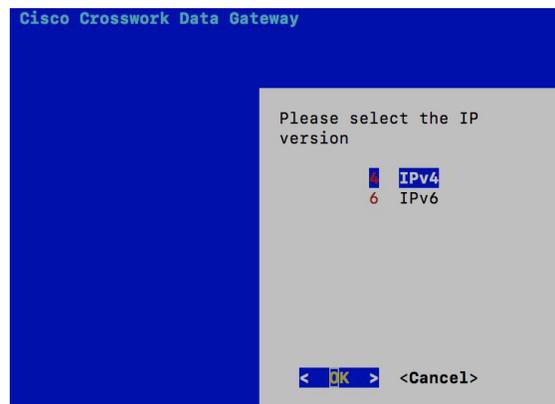
Step 2 To delete a static route, select **d Delete** and click **OK**.



Step 3 Select the interface for which you want to delete a static route and click **OK**.



Step 4 Select the IP address version for which you want to delete a route and click **OK**.



Step 5 Enter IPv4/IPv6 subnet in CIDR format.

Step 6 Click **OK** to save the settings.

Configure Syslog



Note For any Syslog server configuration with IPv4/IPv6 support for different linux distributions, please refer your system administrator and configuration guides.

Step 1 From the **Change Current System Settings** Menu, select **5 Configure Syslog** and click **OK**.

Step 2 Enter the new values for the following syslog attributes:

- Server address: IPv4 or IPv6 address of a syslog server accessible from the management interface. If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).
- Port: Port number of the syslog server
- Protocol: Use UDP, TCP, or RELP when sending syslog.
- Use Syslog over TLS?: Use TLS to encrypt syslog traffic.
- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
- Syslog Root Certificate File URI: PEM formatted root cert of syslog server retrieved using SCP.
- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

Step 3 Click **OK** to save the settings.

Create New SSH Keys

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.

Step 1 From the **Change Current System Settings** Menu, select **7 Import Certificate** and click **OK**.

Step 2 Select the certificate you want to import and click **OK**.

```

Import Certificates - Please Choose an Option:

 1 Controller Signing Certificate File
 2 Controller SSL/TLS Certificate File
 3 Syslog Certificate File
 4 Exit Menu

< OK >

```

Step 3 Enter SCP URI for the selected certificate file and click **OK**.

Step 4 Enter passphrase for the SCP URI and click **OK**.

Configure vNIC1 MTU



Note

- This procedure is not applicable to Cloud deployment.
- In case of On Premise deployment, you can change vNIC1 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 Cisco 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 [Run show-tech](#).

Step 1 From the **Change Current System Settings** menu, select **8 Configure vNIC1 MTU**.

Step 2 Enter vNIC1 MTU value.

Step 3 Click **OK** to save the settings.

Monitor Cisco Crosswork Data Gateway Health

This section contains the following topics:

- [Vitals Monitor, on page 299](#)
- [View Cisco Crosswork Data Gateway Vitals, on page 299](#)
- [collector-vitals Service, on page 302](#)

Vitals Monitor

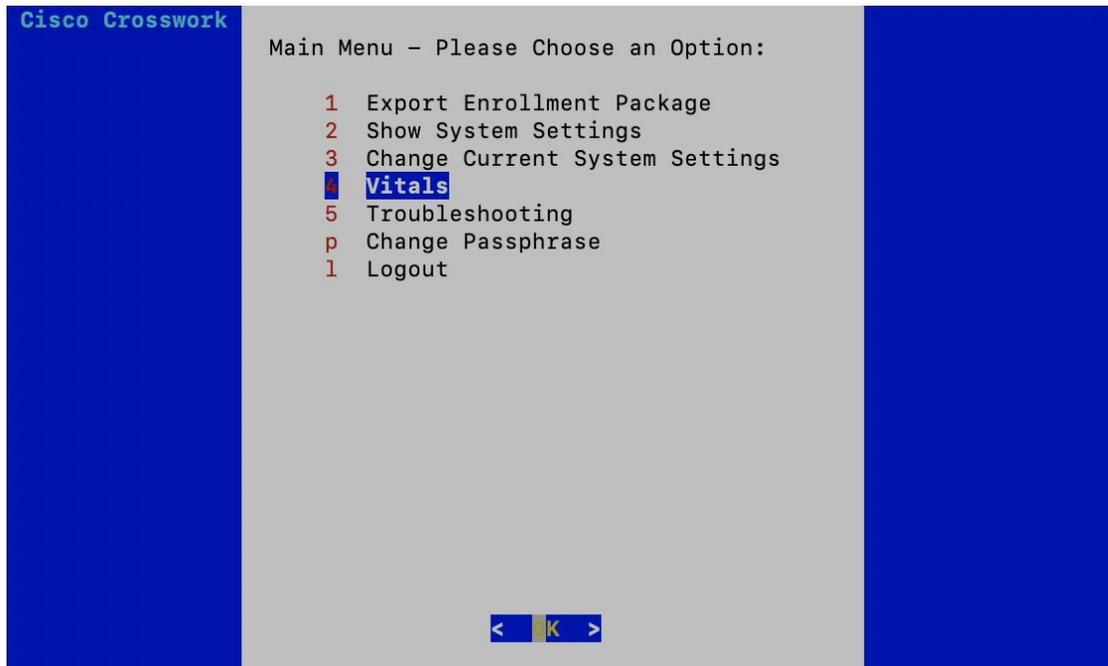
The Vitals Monitor component of Cisco Crosswork Data Gateway enables you to view vitals for the following:

1. Docker containers
2. Docker images
3. Controller reachability
4. NTP reachability
5. Route table
6. ARP table
7. Network connections
8. Disk space usage

View Cisco Crosswork Data Gateway Vitals

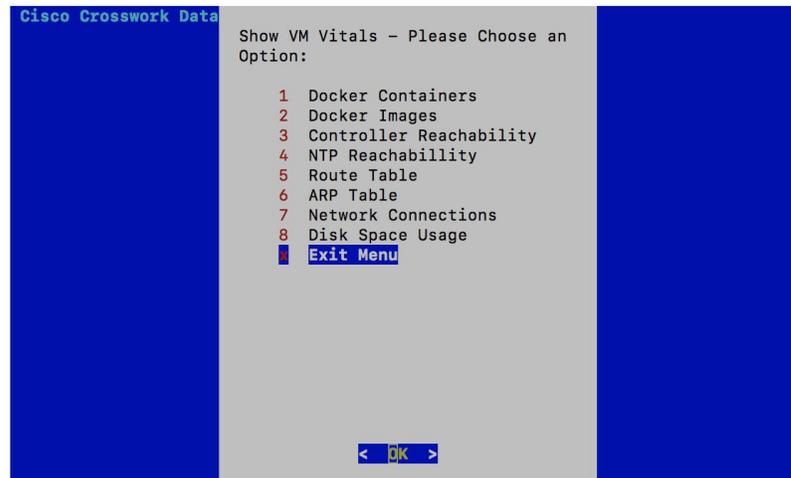
Follow these steps to view Cisco Crosswork Data Gateway vitals:

-
- Step 1** From the Main Menu, select **4 Vitals** and click **OK**.



The **Show VM Vitals** menu opens.

Step 2 Select the vital you want to view and click **OK**.



Vital	Description
<p>Docker Containers</p>	<p>Displays the following vitals for the docker containers:</p> <ul style="list-style-type: none"> • Container ID • Image • Name • Command • Created Time • Status • Port
<p>Docker Images</p>	<p>Displays the following vitals for the docker images:</p> <ul style="list-style-type: none"> • Repository • Image ID • Created Time • Size • Tag
<p>Controller Reachability</p>	<p>Displays the following vitals for controller reachability:</p> <ul style="list-style-type: none"> • Default gateway status • Reachability test details (number of packets transmitted and received, packet loss percentage, and time) • DNS server • DNS server status • Reachability test details (number of packets transmitted and received, packet loss percentage, and time) • Controller session status
<p>NTP Reachability</p>	<p>Displays the following vitals for NTP reachability:</p> <ul style="list-style-type: none"> • NTP server • Resolved IP Address • Status • Reachability test details (number of packets transmitted and received, packet loss percentage, and time) • Chrony status • Reference ID • System time
<p>Route Table</p>	<p>Displays IPv4 and IPv6 route tables.</p>

Vital	Description
ARP Table	Displays ARP tables.
Network Connections	Displays the following vitals for network connections: <ul style="list-style-type: none"> • Netid • State • Recv-Q • Send-Q • Local Address and Port • Peer Address and Port
Disk Space Usage	Displays the following vitals for disk space usage: <ul style="list-style-type: none"> • Filesystem • Size • Used space • Available space • Use percentage • Mounted on volume

Cisco Crosswork Data Gateway displays the vitals for the selected item.

After you are done viewing the vitals, press any key to return to the **ShowVM Vitals** menu.

To return to the Main Menu, select **x Exit Menu** and click **OK**.

collector-vitals Service

Cisco Crosswork Data Gateway comprises of various containerized services running on an Ubuntu VM. Its overall health depends on health of each containerized service.

As part of collector vitals, Cisco Crosswork Data Gateway collects host and container metrics and writes them to a container mounted path in vitals.json file and sends it to the Controller.

These vitals of a Cisco Crosswork Data Gateway VM can also be viewed in the Crosswork UI as described in Section: [View Cisco Crosswork Data Gateway Instance Health, on page 220](#).

It collects the following metrics:

Field	Description
Host VM	

Field	Description
Disk Space Used	Percentage of the disk space used for partitions: / /opt/dg/log /var/lib/docker
Disk In/Out	Number of read/write or input/output operations involving a disk for the partitions: / /opt/dg/log /var/lib/docker Note This is a cumulative counter, not a delta time series.
CPU Utilization	Amount of actively used CPU and total number of vCPUs.
Load	Load average – is the average system load over a given period of time of 1, 5, and 15 minutes.
Memory	Amount of memory used and available memory. Note The value shown for <i>memory</i> represents the usable amount for user processes, not the total VM amount. The Cisco Crosswork Data Gateway operating system reserves about 700MB from the total VM memory for itself, which is excluded from memory reporting tools. It is expected for the <i>memory</i> value reported here to be 1GB less than the full amount allocated to the VM due to operating system reservation and rounding.
Network In/Out	The amount of data sent/received in MB for NIC interfaces: eth0 eth1 eth2 Note This is a cumulative counter, not a delta time series.
Service Status	
Service	Name of the Cisco Crosswork Data Gateway service.

Field	Description
Status	Status of the service: <ul style="list-style-type: none"> • Running • Degraded • Error
CPU Utilization	Percentage of actively utilized CPU by the service.
Version	Version of the service deployed.
Memory Used (MB)	Amount of memory being used by the service.
Network In/Out	The amount of data sent/received in MB by the service over its interface. Note This is a cumulative counter, not a delta time series.
Disk In/Out	Number of read/write or input/output operations that the service has done involving a disk. Note This is a cumulative counter, not a delta time series.

**Note**

- When either of the following components listed below are not responsive, Cisco Crosswork Data Gateway vitals are not updated:
 - Docker Engine
 - Vitals Monitor
 - Controller Gateway

The "Collector Vitals" and "Controller Gateway" dockers must be up and running for alerts/vitals to get updated.

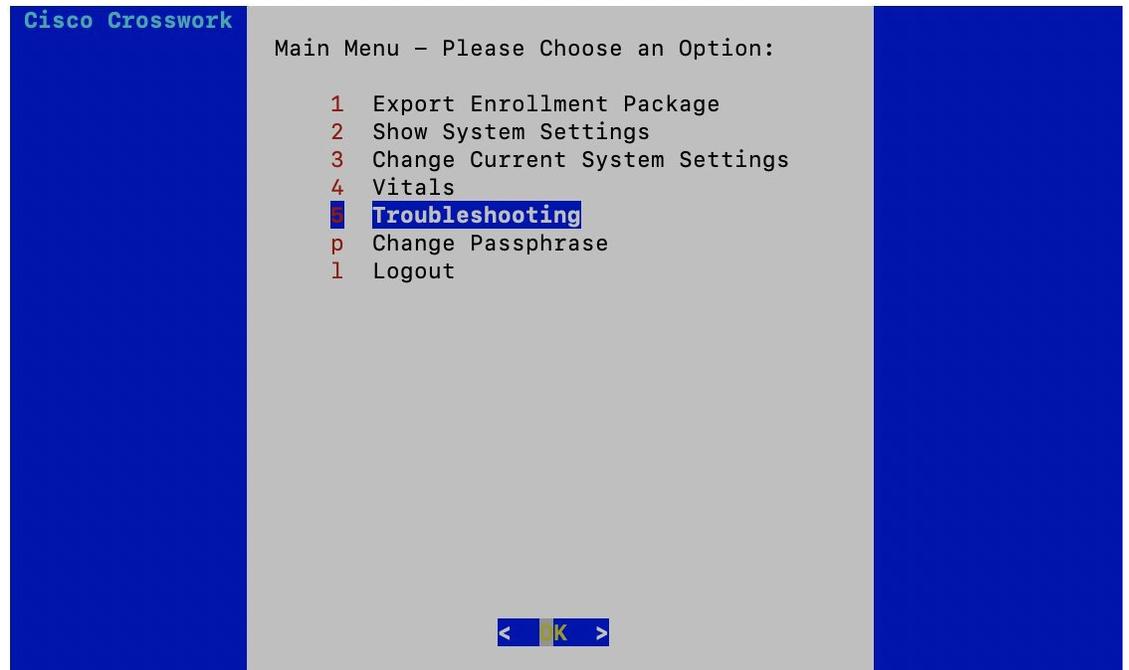
- When Vitals Monitor stops, no alerts are added to cdg-alerts.log. This is because the monitor service runs as a part of Vitals Monitors and it doesn't trigger any alerts when Vitals Monitor itself is down.
- Also, the alerts are not added to cdg-alerts.log when Vitals Monitor is running and Controller Gateway is down.

To access log files, see [Run show-tech, on page 309](#).

Troubleshooting

You can troubleshoot a Cisco Crosswork Data Gateway instance directly from the VM. Cisco Crosswork Data Gateway provides logs of errors, requests to the server, and changes made to the VM and reports any process failures/outages.

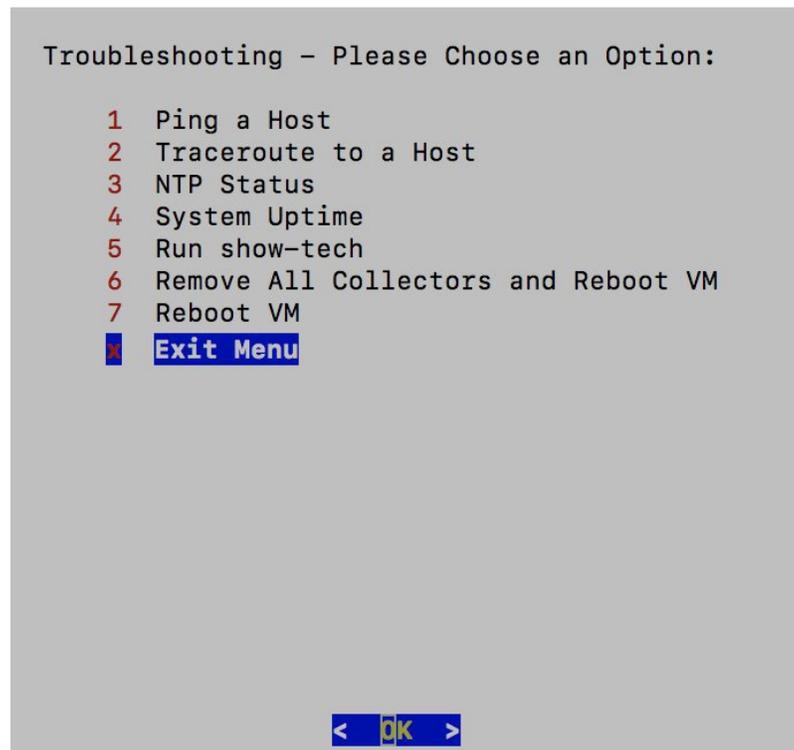
To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu and click **OK**, as shown in the following figure:



Cisco Crosswork Data Gateway opens the **Troubleshooting** menu that provides you the following options to troubleshoot your Cisco Crosswork Data Gateway instance:



Note The following figure shows the Troubleshooting Menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table [Table 25: Permissions Per Role](#), on page 284.



This section contains the following topics:

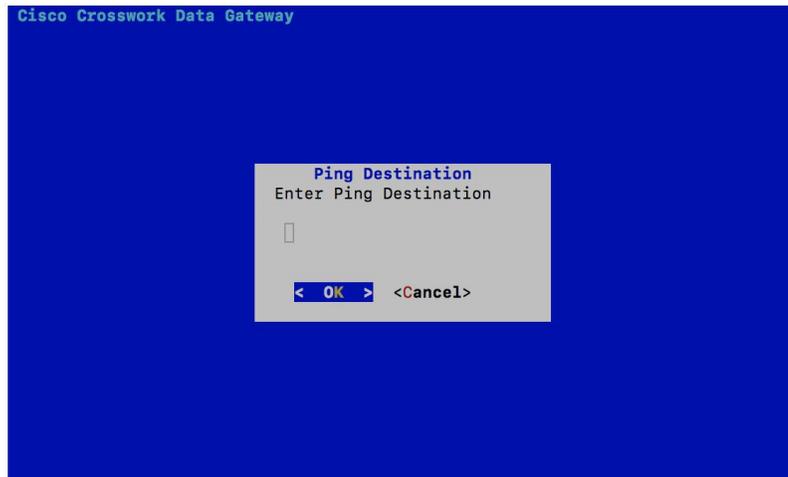
- [Ping a Host, on page 306](#)
- [Traceroute to a Host, on page 307](#)
- [Check NTP Status, on page 308](#)
- [Check System Uptime, on page 308](#)
- [Run show-tech, on page 309](#)
- [Reboot Crosswork Data Gateway VM, on page 310](#)

Ping a Host

To aid troubleshooting, Cisco Crosswork Data Gateway provides you Ping utility that can be used to check reachability to any IP address.

Step 1 From **Troubleshooting** menu, select **1 Ping a Host** and click **OK**.

Step 2 Enter the ping destination.



Step 3 Click **OK**.

Cisco Crosswork Data Gateway displays the result of the ping operation.

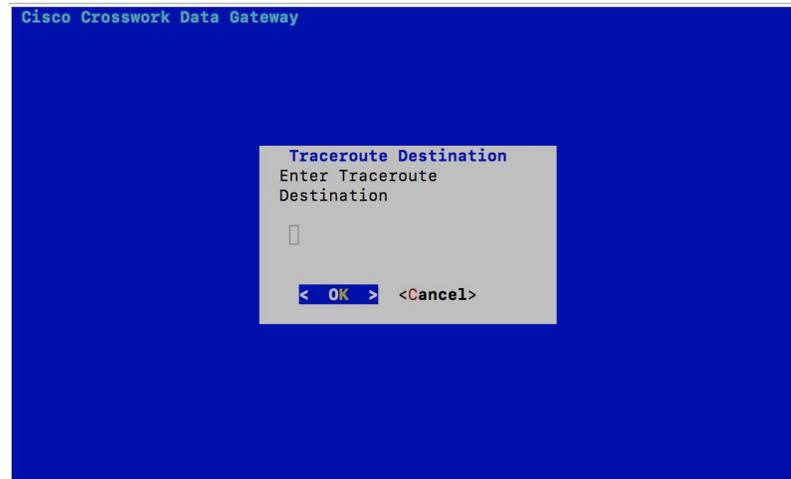
```
PING 172.23.92.143 (172.23.92.143) 56(84) bytes of data.  
64 bytes from 172.23.92.143: icmp_seq=1 ttl=64 time=0.428 ms  
64 bytes from 172.23.92.143: icmp_seq=2 ttl=64 time=0.368 ms  
64 bytes from 172.23.92.143: icmp_seq=3 ttl=64 time=0.270 ms  
  
64 bytes from 172.23.92.143: icmp_seq=4 ttl=64 time=0.574 ms  
  
64 bytes from 172.23.92.143: icmp_seq=5 ttl=64 time=0.433 ms  
64 bytes from 172.23.92.143: icmp_seq=6 ttl=64 time=0.487 ms  
^C  
--- 172.23.92.143 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5107ms  
rtt min/avg/max/mdev = 0.270/0.426/0.574/0.097 ms  
Press any key to continue
```

Traceroute to a Host

Cisco Crosswork Data Gateway provides **Traceroute to a Host** option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Cisco Crosswork Data Gateway to reach the controller application.

Step 1 From **Troubleshooting** menu, select **2 Traceroute to a Host** and click **OK**.

Step 2 Enter the traceroute destination.



Step 3 Click **OK**.

Check NTP Status

Use this option to check the status of the NTP server.

Step 1 From **Troubleshooting** menu, select **3 NTP Status**.

Step 2 Click **OK**. The Cisco Crosswork Data Gateway displays the NTP server status.

```

Reference ID   : AB442641 (mtv5-ai27-dcm10n-ntp1.cisco.com)
Stratum       : 2
Ref time (UTC) : Fri Jun 21 04:53:44 2019
System time   : 0.000044881 seconds fast of NTP time
Last offset   : +0.000057586 seconds
RMS offset    : 0.000080841 seconds
Frequency     : 21.559 ppm slow
Residual freq : +0.009 ppm
Skew          : 0.144 ppm
Root delay    : 0.002095408 seconds
Root dispersion : 0.001190380 seconds
Update interval : 2062.6 seconds
Leap status   : Normal
Press any key to continue

```

Check System Uptime

Use this option to check system uptime.

Step 1 From **Troubleshooting** menu, select **4 System Uptime**.

Step 2 Click **OK**. The Crosswork Data Gateway displays the system uptime.

```
05:11:55 up 3 days, 1:49, 1 user, load average: 0.18, 0.12, 0.10
Press any key to continue
```

Run show-tech

Cisco Crosswork Data Gateway provides the option **show_tech** to export its log files to a user-defined SCP destination.

The collected data includes the following:

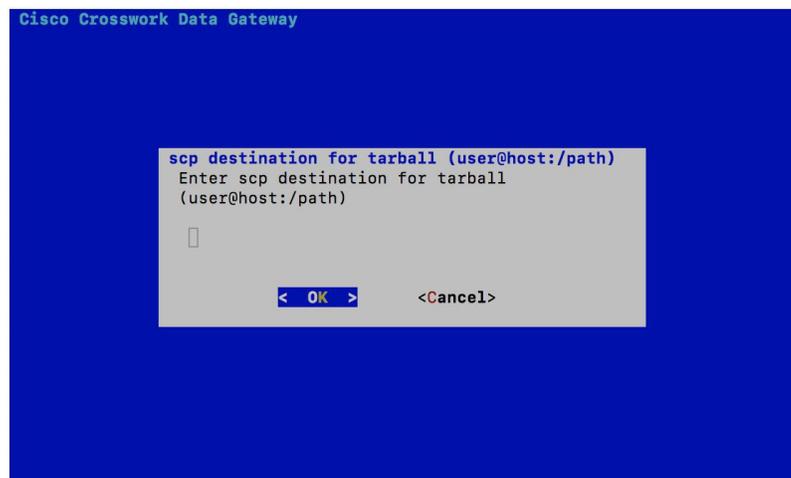
- Logs of all the Data Gateway components running on docker containers
- VM Vitals

It creates a tarball in the directory where it is executed. The output is a tarball named `CDG-<CDG-version>-year-month-day--hour-minute-second-*.tar.bz2`

The execution of this command may take several minutes depending on the state of Crosswork Data Gateway.

Step 1 From **Troubleshooting** menu, select **5 Show-tech** and click **OK**.

Step 2 Enter the destination to save the tarball containing logs and vitals.



Step 3 Enter your SCP passphrase and click **OK**.

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:

```
Cisco Crosswor
Troubleshooting - Please Choose an Option:
1 Ping a Host
2 Traceroute to a Host
3 NTP Status
4 System Uptime
5 Run show-tech
6 Remove All Collectors and Reboot VM
7 Reboot VM
  Exit Menu
< OK >
```

- **Remove All Collectors and Reboot VM:** Select this option from the **Troubleshooting** menu if you want to remove all the collectors (functional images) and reboot VM.
- **Reboot VM:** Select this option from the **Troubleshooting** menu for a normal reboot.



APPENDIX **C**

Supported Devices Information

This section contains the following topics:

- [Supported Devices and Software Types, on page 311](#)

Supported Devices and Software Types

You can configure the software type while onboarding a device to Cisco Crosswork Change Automation and Health Insights. The devices and the corresponding suggested software types are explained in the table below:

Table 26: Supported devices and software types

Device	Suggested Software Type
Alcatel-Lucent	TIMOS
Cisco ASR 5000 Device (formerly STAROS)	ASR5K STAROS
Cisco Adaptive Security Appliance (ASA)	ASASW
Cisco Application Control Engine (ACE)	ACSW
Cisco CatOS Device	CATOS
Cisco IOS Device	IOS
Cisco IOS-EXR Device	IOS XR
Cisco IOS-XR Device	IOS XR
Cisco ME1200 Device running ME1200 OS	ME1200_OS
Cisco NX-OS Device	NXOS
Cisco NX-OS Device with embedded UCSM	NXOS
Cisco Network Analysis Module (NAM)	NAM
Cisco Optical Networking System (ONS) Device	ONS

Device	Suggested Software Type
Cisco SG500 Device running SG500 OS	SG500_OS
Cisco Service Control Engine (SCE)	SCOS
Cisco Unified Communications Manager (UCM)	UCOS
Cisco WAAS Device	Wide Area Application Services
Cisco Wireless LAN Controller	WLC
Generic UNIX Device	UNIX
H3C Comware Device	Comware
Huawei VRP Device	HW_VRP
Juniper JunOS Device	JUNOS



APPENDIX **D**

Telemetry-Traffic Collector (TM-TC) Troubleshooting Procedures

This section explains the troubleshooting scenarios encountered for the Telemetry-Traffic Collector (TM-TC) service.

- [Handling Zombies, on page 313](#)
- [Handling Device Cleanup Errors, on page 315](#)

Handling Zombies

Telemetry – Traffic Collector (TM-TC) service is implemented using nano-services and Reactive FASTMAP design pattern.

There are two nano-plans in TM-TC:

- **External user facing plan:** This plan provides an interface for tracking the configuration status of each node.
- **Internal hidden plan:** This plan applies TM-TC service configuration to a node. The internal service is created for each device by a stacked service.

Zombies are the internal operational data model in NSO to store deleted service data. Zombies are helpful when performing staged deletions and RFM (RFM is the NSO version of eventual consistency). When a service deletion is triggered, NSO maintains references of the deleted services (zombies) in operational data. The zombies are deleted from the configuration database (CDB) when all the configurations for the service are removed from the devices. Zombies inform the data interface the progress of a service deletion. It also informs the stage it is waiting on, which helps to point to the problematic area. For more information, see [NSO documentation in Cisco DevNet](#).

On Cisco Crosswork Change Automation and Health Insights, when you trigger a deletion to clean up the configuration on a device (DLM ADMIN_DOWN / UNMANAGED / DELETION), depending on the connectivity of the device, deleting the configuration at once may lock down the database until the time the last configuration is removed. Once the configuration is successfully removed from the device, the TM-TC service will update the nano-plan state to communicate the deletion progress to the data interface. After the deletion process is completed, TM-TC service removes the nano-plan, zombies, and all the service-related operational data from the CDB.

In some scenarios, as mentioned below, the zombies may not be deleted even after deleting the device configuration and may require manual intervention to delete the configuration references from the devices.

In such cases, run the cleanup action on the device/service. Device and service are inter-usable terms in this context as Cisco Crosswork Change Automation and Health Insights creates services per device.

1. Device is not reachable during deletion.
2. Device is reachable, but the configuration removal fails on the device for other reasons.

If a device/service goes into the zombie state, user should delete the existing plan to enable any new telemetry collection on the device. If the data interface (Crosswork) or a CLI/NETCONF user tries to recreate the service instance before the zombie/delete is fully processed, the following error is displayed, which indicates that the deletion process is still in progress.

Aborted: Operation failed because: Service still in zombie state: 'YYY'



Note

TM-TC Funtion Pack does not support zombie resurrect and redeploy options.

The below image shows how to check if a service is in zombie state on NSO.

Figure 26: Checking if a service is in zombie state on NSO

```
admin@ncs# show zombies service
zombies service /cisco-tm-tc-fp-internal:tm-tc[name='Crosswork_cahi-192.168.124.10']
delete-path /cisco-tm-tc-fp-internal:tm-tc[name='Crosswork_cahi-192.168.124.10']
admin@ncs#
```

TYPE	NAME	BACK TRACK	GOAL	STATE	STATUS	WHEN	ref	POST ACTION STATUS
self	self	true	-	init	reached	-	-	-
				cisco-tm-tc-fp-nano-services:config-apply	reached	-	-	-
				ready	not-reached	-	-	-

```
admin@ncs#
admin@ncs#
admin@ncs#
```

The below image shows the message displayed when you try to create a new configuration on a service that is in zombie state (viewed in the **Health Insights > Job History** page).

Figure 27: Zombie state error message

Job Details

Job Set ID: 0733 | Status: Job Completed | Failures: 2 | Start Time: Thu, Jun 25, 2020, 13:05:43 GMT+5:30 | End Time: Thu, Jun 25, 2020, 13:06:46 GMT+5:30

Status	Operation	KPIs or *Alert Group	KPI Profile	Device	Message
✖	Create	RIB OSPF route count	test_2	PCE-663	Collection job failure: ErrorType:Exception,hostname 192.168.123.113 ...
✖	Create	ISIS neighbor summ...	test_2	PCE-663	Collection job failure: ErrorType:Exception,hostname 192.168.123.113 Operation failed because: Service still in zombie state: /cisco-tm-tc-fp-internal:tm-tc[name='Crosswork_cahi-192.168.124.10']

The below image shows the NSO cleanup command to remove the plan in zombie state.

Figure 28: NSO cleanup command

```

admin@ncs# tm-tc-actions cleanup service Crosswork_cahi-192.168.124.10 no-networking false
success true
detail
Cleaning up TMTC service: Crosswork_cahi-192.168.124.10
Removed all plan components
Removing service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-192.168.124.10}
Removed service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-192.168.124.10}
Removing service oper: /cisco-tm-tc-fp-internal:tm-tc-internal/tm-tc-oper-data{Crosswork_cahi-192.168.124.10 192.168.124.10}
Removed service oper
Removed side-effects
Removed side-effects
Removed kickers
Removing kicker: /kickers/data-kicker{"pre-condition: /cisco-tm-tc-fp-internal:tm-tc-internal/tm-tc-plan{Crosswork_cahi-192.168.124.10 192.168.124.10}/plan/component{ncs:self self}/state{cisco-tm-tc-fp-nano-services:config-apply}"}
Removed kickers
Cleanup Successful for Crosswork_cahi-192.168.124.10
admin@ncs#
admin@ncs#
admin@ncs# show zombies service
% No entries found.
admin@ncs#

```

Handling Device Cleanup Errors

The deletion of telemetry configuration may fail at times, and you will be notified about it in the Job History page.

Figure 29: Telemetry configuration deletion error

The screenshot shows the 'Job History' page with a table of jobs. The first job, 'Cleanup Nodes', is marked as 'Failed'. An 'Error Details' dialog box is open, showing the following error message:

```

Application:robot_collector_hellos failed to cleanup the device. Device uuid:577ca46f-461c-4985-9743-e7c83060dbc9 Device external id:scale-xrv1
Error:ErrorType:Exception,hostname 2001:420:54ff:24::650:42 Network Element Driver: device 2001:420:54ff:24::650:51: out of sync Please cleanup the device manually

```

Description	Status	Imp...	Start Time	End Time
Cleanup Nodes	Failed		Thu, Jun 25, 2020, 3:39:49 PM GMT+5:30	Thu, Jun 25, 2020
Cleanup Nodes	Failed		Thu, Jun 25, 2020, 3:39:49 PM GMT+5:30	Thu, Jun 25, 2020
Update 1 Node(s)	Completed		Thu, Jun 25, 2020, 3:37:26 PM GMT+5:30	Thu, Jun 25, 2020
Update 1 Node(s)	Completed		Thu, Jun 25, 2020, 3:37:26 PM GMT+5:30	Thu, Jun 25, 2020
Update 1 Node(s)	Completed		Thu, Jun 25, 2020, 3:37:25 PM GMT+5:30	Thu, Jun 25, 2020
Update 1 Node(s)	Completed		Thu, Jun 25, 2020, 3:13:08 PM GMT+5:30	Thu, Jun 25, 2020
Update 1 Node(s)	Completed		Thu, Jun 25, 2020, 3:12:31 PM GMT+5:30	Thu, Jun 25, 2020
Update 1 Node(s)	Completed		Thu, Jun 25, 2020, 3:12:18 PM GMT+5:30	Thu, Jun 25, 2020

The device cleanup error can occur in two scenarios:

- **Failure in deleting a specific telemetry configuration on the device**

In this scenario, user is expected to clear the failed configuration from telemetry service manually. This automatically removes the configuration from device. If the configuration is removed from the device, functional pack will restore the configuration, hence user should also remove it from the functional pack service model.

Follow these steps to remove the subscription manually from NSO CLI:

1. Browse through the Telemetry – Traffic Collector (TM-TC) configuration to find out the subscription id to be deleted.
2. Delete the subscription node found above using delete command on NSO CLI.

```

[ns0@localhost ~]$ ncs_cli -u admin
admin connected from 2001:420:54ff:24::650:40 using ssh on localhost.localdomain
admin@ncs> configure
Entering configuration mode private
[ok][2020-06-25 06:16:59]

[edit]
admin@ncs% show cisco-tm-tc-fp:tm-tc Crosswork_cahi-2001:420:54ff:24::650:51 node 2001:420:54ff:24::650:51 telemetry-model-driven-subscription subscription
subscription CW_198a375c-f3f4-407e-8663-ae67868be7cd_8ba94cfeeb43d659ec25944fe54bcb646ccc58dc {
  sensor-group CW_198a375c-f3f4-407e-8663-ae67868be7cd_8ba94cfeeb43d659ec25944fe54bcb646ccc58dc {
    sample-interval 300000;
  }
  destination-group CW_198a375c-f3f4-407e-8663-ae67868be7cd_8ba94cfeeb43d659ec25944fe54bcb646ccc58dc;
}
subscription CW_198a375c-f3f4-407e-8663-ae67868be7cd_bdb2b80d0b89e63d68643982cf8d96103c119d6 {
  sensor-group CW_198a375c-f3f4-407e-8663-ae67868be7cd_bdb2b80d0b89e63d68643982cf8d96103c119d6 {
    sample-interval 300000;
  }
  destination-group CW_198a375c-f3f4-407e-8663-ae67868be7cd_bdb2b80d0b89e63d68643982cf8d96103c119d6;
}
[ok][2020-06-25 06:16:14]

[edit]
admin@ncs% delete tm-tc Crosswork_cahi-2001:420:54ff:24::650:51 node 2001:420:54ff:24::650:51 telemetry-model-driven-subscription subscription CW_198a375c-f3f4-407e-8663-ae67868be7cd_bdb2b80d0b89e63d68643982cf8d96103c119d6
[ok][2020-06-25 06:16:56]

[edit]
admin@ncs% commit
Commit complete.
[ok][2020-06-25 06:17:07]

[edit]
admin@ncs%
System message at 2020-06-25 06:17:08...
Commit performed by admin via ssh using cli.
admin@ncs%
System message at 2020-06-25 06:17:09...
Commit performed by admin via ssh using cli.
admin@ncs%
System message at 2020-06-25 06:17:09...
Commit performed by admin via ssh using cli.

```

• Failure in deleting the telemetry service on NSO for a device

When ADMIN_DOWN/UNMANAGED is set on a device in DLM, or if device is removed from DLM, Cisco Crosswork Change Automation and Health Insights will remove the telemetry service associated with that device on NSO. If this fails, it would be reported as device cleanup failure. In this case, user is expected to run the cleanup command on NSO CLI. The cleanup command has a “match” option using which all the services whose name is matching with a particular string can be removed at one go.

Below are some examples:

The name of a service for a specific device would be *Crosswork_cahi-<node key in NSO>*

To remove one service: **request tm-tc-actions cleanup service <service-name> no-networking false**

```

admin@ncs>
admin@ncs> request tm-tc-actions cleanup service Crosswork_cahi-2001:420:54ff:24::650:51 no-networking false
success true
detail
Cleaning up TMTc service: Crosswork_cahi-2001:420:54ff:24::650:51
Removed all plan components
Removing service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-2001:420:54ff:24::650:51}
Removed service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-2001:420:54ff:24::650:51}
Removing service oper: /cisco-tm-tc-fp-internal:tm-tc-internal/tm-tc-oper-data{Crosswork_cahi-2001:420:54ff:24::650:51 2001:420:54ff:24::650:51}
Removed service oper
Removed side-effects
Removed side-effects
Removed kickers
Removed kickers
Cleanup Successful for Crosswork_cahi-2001:420:54ff:24::650:51
[ok][2020-06-25 06:31:00]
admin@ncs>
admin@ncs>

```

To remove all services whose name matches with the string "Crosswork": **request tm-tc-actions cleanup service Crosswork match true no-networking false**

```

admin@ncs>
admin@ncs> request tm-tc-actions cleanup service Crosswork match true no-networking false
success true
detail
Cleaning up TMTc service: Crosswork_cahi-2001:420:54ff:24::650:51
Removed all plan components
Removing service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-2001:420:54ff:24::650:51}
Removed service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-2001:420:54ff:24::650:51}
Removing service oper: /cisco-tm-tc-fp-internal:tm-tc-internal/tm-tc-oper-data{Crosswork_cahi-2001:420:54ff:24::650:51 2001:420:54ff:24::650:51}
Removed service oper
Removed side-effects
Removed side-effects
Removed kickers
Removed kickers
Cleanup Successful for Crosswork_cahi-2001:420:54ff:24::650:51
Cleaning up TMTc service: Crosswork_cahi-2001:420:54ff:24::650:52
Removed all plan components
Removing service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-2001:420:54ff:24::650:52}
Removed service /cisco-tm-tc-fp:tm-tc{Crosswork_cahi-2001:420:54ff:24::650:52}
Removing service oper: /cisco-tm-tc-fp-internal:tm-tc-internal/tm-tc-oper-data{Crosswork_cahi-2001:420:54ff:24::650:52 2001:420:54ff:24::650:52}
Removed service oper
Removed side-effects
Removed side-effects
Removed kickers
Removed kickers
Cleanup Successful for Crosswork_cahi-2001:420:54ff:24::650:52
[ok][2020-06-25 06:24:44]
admin@ncs>

```