

Cisco Crosswork Planning 7.1 Collection Setup and Administration

First Published: 2025-06-25

Last Modified: 2025-12-22

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview** 1

Core capabilities of Cisco Crosswork Planning 1

System overview 2

Collectors 3

Network models and plan files 4

Aggregation components 4

Log in to and log out of Cisco Crosswork Planning 5

Dashboard 5

CHAPTER 2 **Configure Network Models** 7

Network model creation workflow 7

Preconfiguration workflow 10

Collection configuration workflow 10

Collector configuration migration 11

Migrate collector configurations from Cisco WAE 11

Configurations excluded during migration 13

Migrate collector configurations between Cisco Crosswork Planning instances 14

Configure credential profiles 16

Configure authentication credentials 17

Configure SNMP credentials 18

Configure network profiles 20

Add or edit nodes 22

Configure node filter 23

Regex-based filtering criteria for node selection 25

Configure agents 26

SR-PCE and NetFlow agent configuration options 27

Agent operations 29
Configure collections 30
Edit collections 34
Delete collections 35
Schedule collections 36
Edit schedules 38
Delete schedules 39
View scheduled task status and history 39
Aggregate collector outputs 40
Reaggregate collector outputs 42
Configure archive 43
View or download plan files 44
Scenario 1: When the Cisco Crosswork Planning Design and Collector applications are installed on the same machine 45
Scenario 2: When the Cisco Crosswork Planning Design and Collector applications are installed on different machines 46
Connect to the external collector 46
View or download plan files from remote archive 47

CHAPTER 3 **Supported Collectors and Tools** 49
Collector descriptions 49
Collect basic topology information 51
Collect topology information using the IGP database collector 52
Collect topology information using the SR-PCE collector 53
IGP and SR-PCE collection advanced options 55
Collect LSP information 57
LSP collection advanced options 57
Collect PCEP LSP information using SR-PCE 58
Collect multicast flow data from a network 60
Multicast collection advanced options 61
Discover BGP peers 62
BGP topology advanced options 63
Discover VPN topology 65
Collect hardware inventory information 66

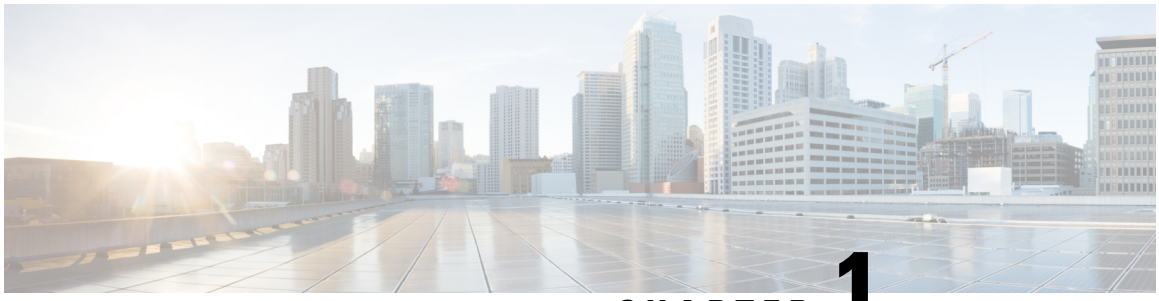
Configure inventory collection 71
Inventory collection advanced options 72
Collect port, LSP, SRLG, and VPN information using configuration parsing 73
Configuration parsing advanced options 74
Collect Circuit Style RSVP-TE information 76
Configure the Layout collector for improved network model visualization 77
Collect traffic statistics 78
Traffic collection advanced options 80
Tuning traffic polling 81
Collect traffic demands information 83
NetFlow data collection 84
NetFlow collection configuration 85
Configure the NetFlow collection 85
NetFlow collection advanced options 86
Run an external script against a network model 87
Sample script for updating interface descriptions 89
How data is collected from third-party devices 90
Collectors with support module configurations 90
Collect data from third-party devices 90
Merge AS plan files 92

CHAPTER 4 **Manage Licenses** 95
Cisco Smart Licensing 95
Configuring Smart Licensing 96
Configure the transport mode between Cisco Crosswork Planning and CSSM 96
Register Cisco Crosswork Planning via token 98
Manually perform licensing actions 101
Register Cisco Crosswork Planning via offline reservation 101
Update offline reservation 103
Disable offline reservation 104
Update license counts 104
License authorization statuses 106

CHAPTER 5 **Manage Administrative Tasks** 107

Manage certificates 107
Certificate types and usage 108
Add new certificates 109
Edit certificates 110
Download certificates 111
Update web certificate using certificate signing request 112
Manage users 114
Administrative users created during installation 115
User roles, functional categories and permissions 115
Create user roles 117
Clone user roles 118
Edit user roles 118
Delete user roles 119
Global API permissions 119
Manage active sessions 121
Set up user authentication (TACACS+, LDAP, and RADIUS) 122
Manage TACACS+ servers 123
Manage LDAP servers 125
Example 127
Manage RADIUS servers 131
Enable Single Sign-on (SSO) 133
Configure AAA settings 134
Monitor system and application health 135
Monitor platform infrastructure and application health 135
Check system health example 136
Manage backups 139
Backup and restore overview 139
Manage backup and restore 140
Recommendation: Post-restore actions 142
Restore Cisco Crosswork Planning after a disaster 143
Migrate data using backup and restore 144
View system and network alarms 145
View audit log 146
Set the pre-login disclaimer 146

Manage maintenance mode settings 147
Update network access configuration 148
Update collector capability 148
Configure aging 149
Configure purging of archived plan files 150
Configure static routes 150
Add static routes 150
Delete static routes 151



CHAPTER 1

Overview

This is a post-installation document intended to cover the steps required to get up and running with the Cisco Crosswork Planning Collector application. It provides instructions on how to configure the collectors to generate network models according to your specifications.

This chapter contains these topics:

- Core capabilities of Cisco Crosswork Planning , on page 1
- System overview, on page 2
- Collectors, on page 3
- Network models and plan files, on page 4
- Aggregation components, on page 4
- Log in to and log out of Cisco Crosswork Planning , on page 5
- Dashboard, on page 5

Core capabilities of Cisco Crosswork Planning

Cisco Crosswork Planning provides tools to create a model of the existing network by continuously monitoring the network and its traffic demands. At any given time, this network model contains all relevant information about a network, including topology, configuration, and traffic information. You can use this information as a basis for analyzing the impact on the network due to changes in traffic demands, paths, node and link failures, network optimizations, or other changes.

Key features

Some important features of Cisco Crosswork Planning include:

- Traffic engineering and network optimization: Compute TE LSP configuration to meet service level requirements, perform capacity management, and perform local or global optimization in order to maximize efficiency of deployed network resources.
- Demand engineering: Examine the impact on network traffic flow of adding, removing, or modifying traffic demands on the network.
- Topology and predictive analysis: Observe the impact to network performance of changes in the network topology, which is driven either by design or by network failures.
- TE tunnel programming: Examine the impact of modifying tunnel parameters, such as the tunnel path and reserved bandwidth.

- Class of service (CoS)-aware bandwidth on demand: Examine existing network traffic and demands, and admit a set of service-class-specific demands between routers.

Components

Cisco Crosswork Planning comprises two primary components:

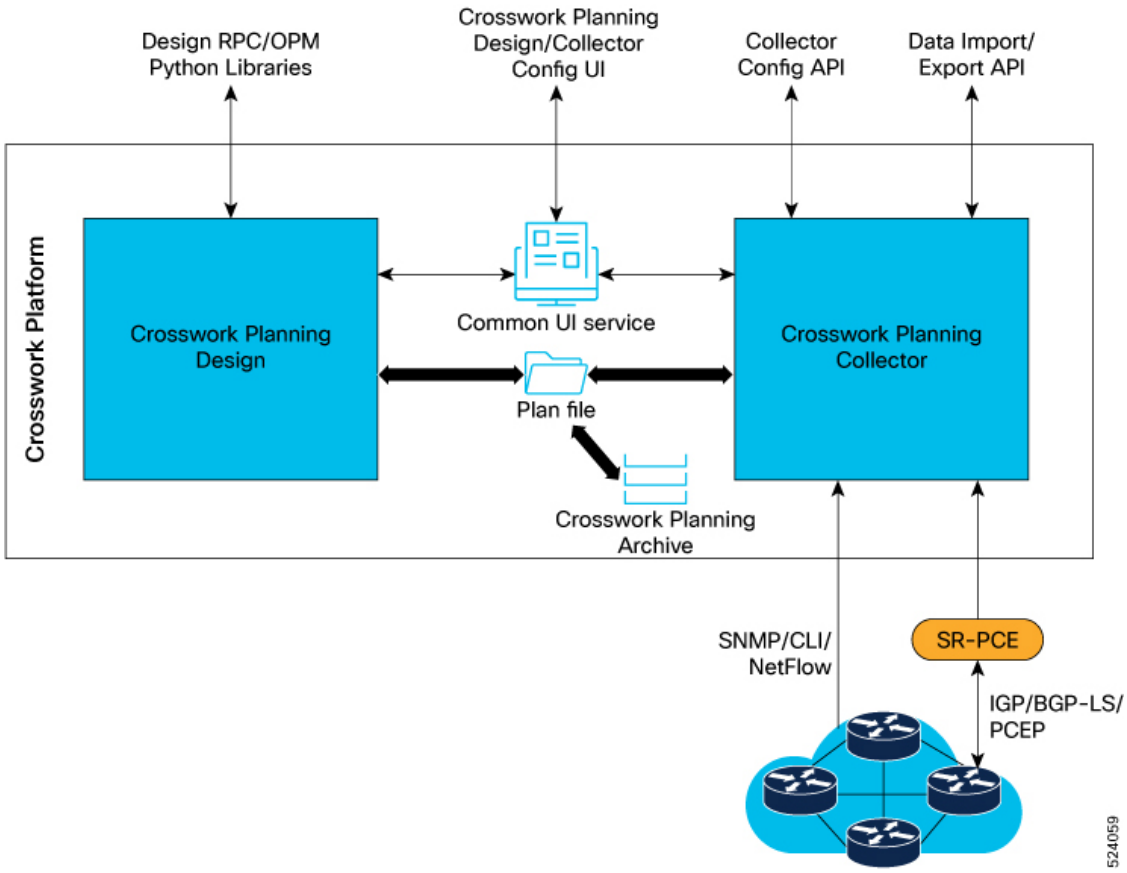
- Cisco Crosswork Planning Collector: This component consists of a set of services that create, maintain, and archive a model of the current network. It achieves this through continual monitoring and analysis of the network and the traffic demands placed on it.
- Cisco Crosswork Planning Design: This component helps network engineers and operators predict growth in their network, simulate failures, and optimize the network design to meet performance objectives while minimizing cost.

System overview

Cisco Crosswork Planning runs on the Cisco Crosswork infrastructure and is part of the Cisco Crosswork Network Automation suite of products.

The Cisco Crosswork Planning Design and Cisco Crosswork Planning Collector applications are packaged as separate components and can be enabled or disabled as per your needs. These two applications run independently of each other. The communication between Cisco Crosswork Planning Design and the archive on the Cisco Crosswork Planning Collector to import network models happens over well-defined APIs.

Figure 1: System overview



Collectors

A *Collector* is a package that populates parts of the abstract network model by querying the network.

Typically, collectors operate in this manner:

1. They read a *source network model*, also known as a *source model*.
2. They augment this source model with information obtained from the actual network.
3. They produce a *destination network model* with the resulting model. This is also known as a *destination model*.

Types of collectors

Cisco Crosswork Planning includes several different collectors, including:

- Topology collectors: These collectors populate a basic network model with topology information, such as nodes, interfaces, and circuits. This is based on the discovered IGP database augmented by SNMP queries and SR-PCE. The topology collectors do not have a source model.

- LSP collector: This collector augments a source model with LSP information, producing a destination model with the extra information.
- Traffic collector: This collector augments a source model with traffic statistics polled from the network, producing a new destination model with extra information.
- Layout collector: This collector adds layout properties to a source model to improve visualization. It produces a new destination model with these additional layout information. As the source model changes, the collector updates the layout properties of the destination model accordingly.

For a complete list of all the collectors supported in Cisco Crosswork Planning, see Collector descriptions, on page 49.

Network models and plan files

Network models are the outputs generated by the Cisco Crosswork Planning Collector application. These are built from a real network by combining information from various collectors.

A *model building chain* refers to an arrangement of these collectors organized in such a way as to produce a network model with the desired information. You can view or download the resulting network model, saved in a *plan file* (.pln format), from the Cisco Crosswork Planning Design application.

Aggregation components

The aggregation engines consolidate network data collected from various sources to generate comprehensive network models.

This section describes the roles and functions of the Delta Aggregation Rules Engine (DARE) and the Simple Aggregation Engine (SAgE) in Cisco Crosswork Planning.

Delta Aggregation Rules Engine (DARE)

The DARE aggregator is a Cisco Crosswork Planning component that brings together various collectors, selects model information from each of them, and consolidates the information into a single model. It primarily consolidates all topology collectors' data.

Simple Aggregation Engine (SAgE)

The SAgE aggregator is a Cisco Crosswork Planning component which consolidates all the network information such as traffic, inventory, layout, multicast, NetFlow, and demands. It aggregates these changes along with the topology changes from DARE network into the final network.

SAgE aggregator enables running traffic collection, inventory collection, layout, and so on in parallel.

By default, all collectors are included in the aggregation during collection configuration. You can choose to exclude any collector from aggregation while scheduling the collection. For details, see Aggregate collector outputs, on page 40.

Generation of network models

Network models are generated on completion of each level of aggregation. The first model is generated as the output of DARE aggregation. This file serves as a data source for components such as traffic, inventory,

layout, NetFlow, and demands. Once the SAgE aggregation is complete, it generates the second file, the network model, which is the final output of the aggregated data collected.

Log in to and log out of Cisco Crosswork Planning

Cisco Crosswork Planning is a browser-based application. For details on supported browser versions, see the *"Supported web browsers" section in the Cisco Crosswork Planning 7.1 Installation Guide*.

After installing Cisco Crosswork Planning, follow these steps to access the Cisco Crosswork Planning UI.

Procedure

Step 1 Open a web browser and enter `https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`

When you access Cisco Crosswork Planning from your browser for the first time, you may see 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 Planning server as a trusted site in all subsequent logins.

Step 2 Enter your username and password. The default administrator username and password is **admin**. This account is created automatically at installation. You must change the initial password for this account during installation verification. We strongly recommend that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user roles with appropriate privileges and assign new users to those roles. At least one of the users you create should be assigned the "administrator" role.

Step 3 Click **Login**.

Step 4 To log out, at the top right of the main window, click  > **Logout**.

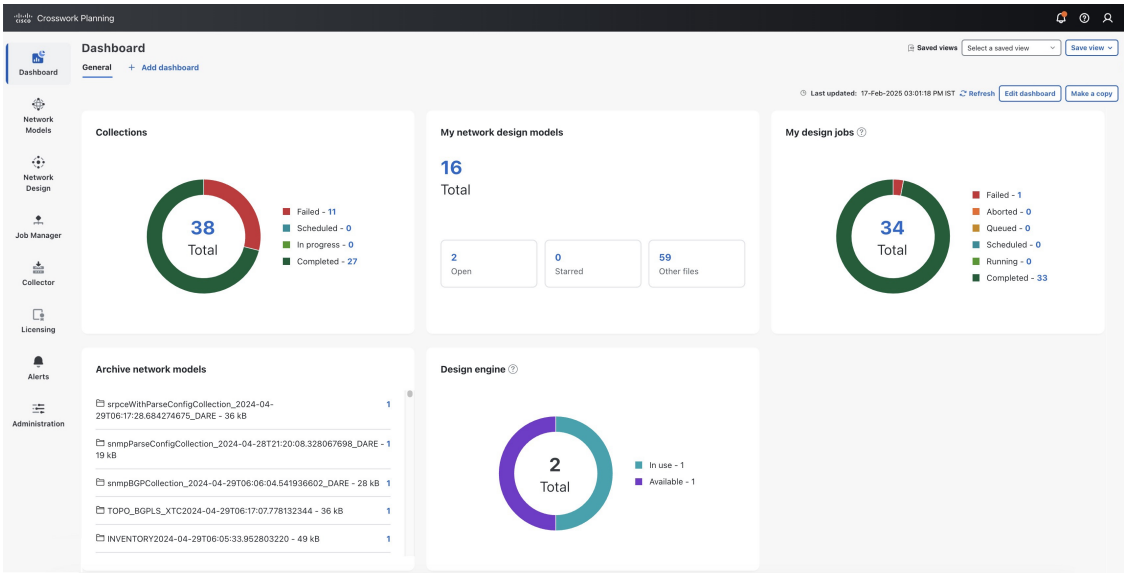
Note
Logging out does not close the plan file you are working on. It remains open.

Dashboard

The **Dashboard** page provides a quick operational summary of Cisco Crosswork Planning. This page consists of various dashlets, which vary based on the Cisco Crosswork Planning application installed.

For example, the **Collections** and **Archive network models** dashlets appear only if you have installed the Cisco Crosswork Planning Collector application. Similarly, the **My network design models**, **My design jobs**, and **Design engine** dashlets appear only if you have installed the Cisco Crosswork Planning Design application.

Figure 2: Dashboard view

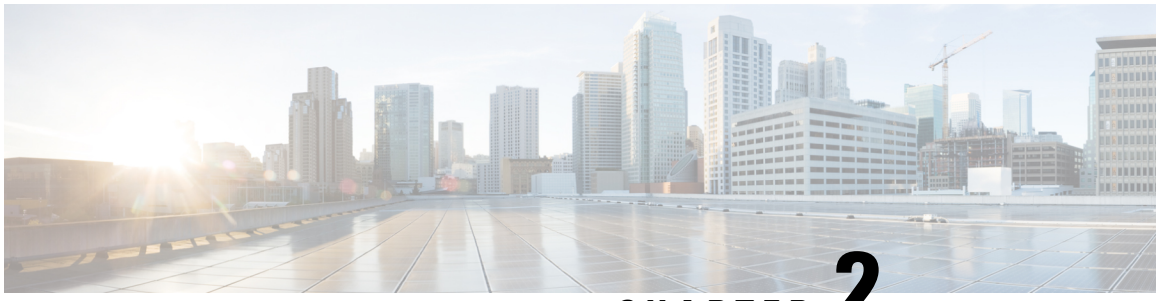


Dashlet navigation

Links in each dashlet allow you to navigate to the desired pages easily.

Dashlet customization

Use the **Edit dashboard** button at the top right corner to customize how the dashlets appear. For details, see the *Customize dashlets* topic in the *Cisco Crosswork Planning Design 7.1 User Guide*.



CHAPTER 2

Configure Network Models

This section contains the following topics:

- Network model creation workflow, on page 7
- Preconfiguration workflow, on page 10
- Collection configuration workflow, on page 10
- Collector configuration migration, on page 11
- Configure credential profiles, on page 16
- Configure network profiles, on page 20
- Configure agents, on page 26
- Configure collections, on page 30
- Schedule collections, on page 36
- Aggregate collector outputs, on page 40
- Configure archive, on page 43
- View or download plan files, on page 44

Network model creation workflow

The Cisco Crosswork Planning UI provides an easy-to-use interface that hides the complexity of creating a model building chain for a network. It combines the configuration of multiple data collectors under one network (collection) and can produce a single network model that contains the consolidated data. Use the Cisco Crosswork Planning UI for configuring device and network access, creating network models, managing users, and configuring agents.

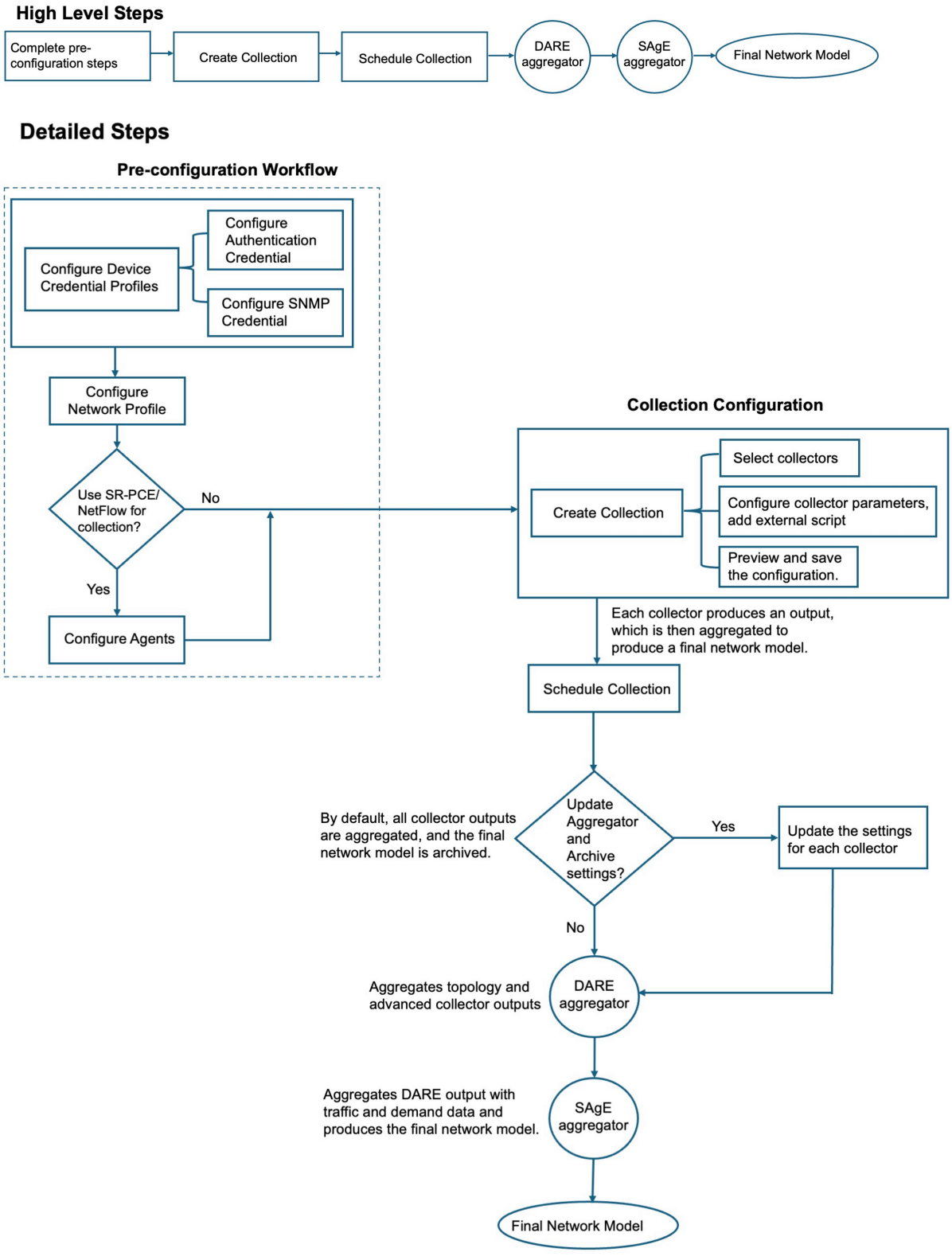
The Table 1: Network model creation workflow, on page 7 and Figure 3: Network model creation workflow, on page 9 illustrate how you can configure individual network models.

Table 1: Network model creation workflow

Step	Action
1. Configure device authgroups, SNMP groups, and network profile access.	See Preconfiguration workflow, on page 10.
2. (Optional) Configure agents only if you need to collect SR-PCE or NetFlow information.	See Configure agents, on page 26.

Step	Action
3. Configure the collections (basic and advanced configurations).	See Collection configuration workflow, on page 10.
4. Schedule when to run the collections.	See Schedule collections, on page 36.
5. (Optional) Manage aggregation and archiving of network model as per your requirement.	See • Aggregate collector outputs, on page 40 • Configure archive, on page 43
6. View or download the plan files in the Cisco Crosswork Planning Design application.	See View or download plan files, on page 44.

Figure 3: Network model creation workflow



Preconfiguration workflow

This workflow describes the steps that you must complete before creating a network model. This preconfiguration workflow involves the creation of credential profiles to access the devices, the device mappings, and the agents.

Step	Action
1. Configure the device credential profiles (Authentication profiles and SNMP profiles).	See Configure credential profiles, on page 16.
2. Configure the network profile access.	See Configure network profiles, on page 20.
3. (Optional) Create agents to collect specific information. This step is required only for collecting SR-PCE or NetFlow information.	See Configure agents, on page 26.

Collection configuration workflow

The initial step in creating a network model is to create a new network (Collection) with topology collection. Use the **Collections** page (from the main menu, choose **Collector** > **Collections**) to configure different collectors. You can choose the network elements that you want to collect. You can also indicate if an SR-PCE is used for collection or not. Based on the selection of collectors, a chain of collectors is derived and displayed. Each collector produces an output, which are aggregated to produce a final network model. The numbered navigation at the top of the page displays where you are in the network model configuration process.

This high-level workflow describes the process involved in collection configuration.

Step	Description
1. Complete all the steps mentioned in the preconfiguration workflow.	See Preconfiguration workflow, on page 10.
2. Select the required collectors.	**1.** As a first step, choose a Basic Topology collector, which will be the source for additional network collections. **2.** Choose the additional collectors, as per your requirement. The collectors are categorized under the **Basic topology**, **Advanced modeling**, and **Traffic and Demands** sections.
3. Configure collection parameters.	Based on the collectors you selected in the previous step, the configuration parameters differ. The left pane displays the selected collectors and the right pane displays the configuration parameters associated with the selected collector. Enter all the required details.

Step	Description
4. (Optional) Run external scripts against a collection model.	If you want specific data from your network that existing Cisco Crosswork Planning collectors do not provide, you can run a customized script against a selected network model. For details, see Run an external script against a network model, on page 87.
5. Preview the order in which you have configured the collectors.	Preview the order in which you have configured the collectors. If you are satisfied with the configuration, then proceed with the creation of the collection.
6. Schedule the collections.	You can run the collection jobs immediately or you can schedule them to run periodically at a specific time or at intervals. You can also set multiple schedules for a collection. For details, see Schedule collections, on page 36.
7. (Optional) Update the aggregation and archive settings, as required.	See: • Aggregate collector outputs, on page 40 • Configure archive, on page 43

Collector configuration migration

A collector configuration migration is a process that enables you to migrate collector configurations from Cisco WAE 7.5.x/7.6.x or between different Cisco Crosswork Planning instances.

Note When using collectors that have file upload options, ensure to upload the correct files after importing the collector configuration. This is necessary because, after you import the configuration, the server restores only the file name and not the actual file. If you do not use the correct file, the collection will fail.

Migrate collector configurations from Cisco WAE

This section explains how to migrate collector configurations from Cisco WAE 7.5.x/7.6.x to Cisco Crosswork Planning.

Before you begin

- Download the upgrade script from the Cisco Software Download page.

Procedure

Step 1 If you have not backed up the configuration, use these steps to back up and migrate it to a configuration compatible with Cisco Crosswork Planning:

a) Log in to the machine where Cisco WAE 7.x is installed.
b) Enter this command:

```
# ./wae_upgrade --export --install-dir <WAE_7.x_INSTALL_DIR> --cfg-dir
<dir_to_save_exported_config>
Where:
     --install-dir   indicates the directory where 7.x WAE is installed.
     --cfg-dir       indicates the folder where the backup of 7.x configuration
                     must reside. The migrated configurations are saved as
                     wae_networks.cfg in the provided directory.
```

Step 2 If you already have the backed-up configuration, use these steps to convert the file into a format compatible with Cisco Crosswork Planning:

a) Log in to the machine where the Cisco WAE 7.x configuration is backed up.
b) Enter this command:

```
# ./wae_upgrade --migrate --cfg-dir <dir_containing_7.x_config>

Where:
      --cfg-dir   indicates the folder where the 7.x configuation is backed up.
                  This configuration will be migrated to Cisco Crosswork Planning
                  compatible configuration. The migrated configurations are saved as
                  wae_networks.cfg in the provided directory.
```

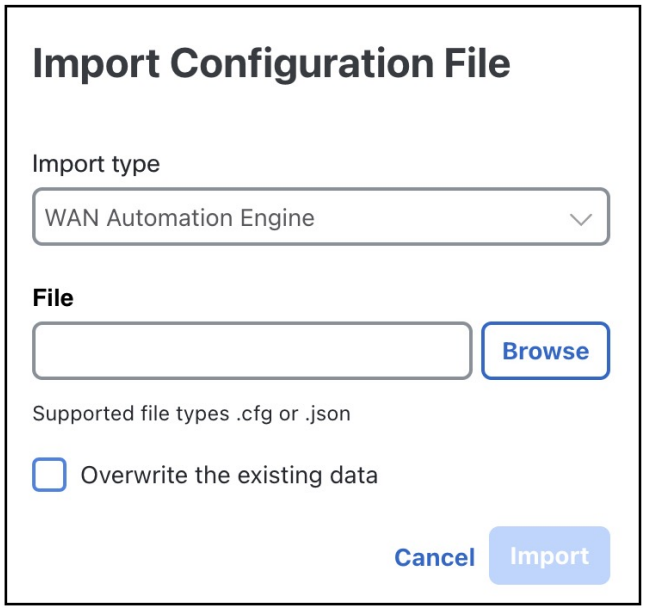
Step 3 Import the migrated configurations (**wae_networks.cfg**) to Cisco Crosswork Planning using these steps:

Note
Before migration, ensure that configurations are backed up using the upgrade scripts. Otherwise, the migration will fail.

a) Log in to the Cisco Crosswork Planning UI.
b) From the main menu, choose **Collector** > **Migration**.
c) Click **Actions** and select **Configuration migration**.

The Import Configuration File page appears.

Figure 4: Import Configuration File page



d) Select **WAN Automation Engine** from the **Import type** drop-down list.
e) Click **Browse** and select the **wae_networks.cfg** file.
f) (Optional) To overwrite the existing collector configuration, check the **Overwrite the existing data** check box.
g) Click **Import**.

The system proceeds with the import using your configuration. You can monitor the progress on the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays **Success**.

What to do next

Note After migrating from Cisco WAE to Cisco Crosswork Planning, the Telnet and SSH settings are not preserved. You need to manually verify and update these settings, if required.

Configurations excluded during migration

The following configurations are NOT migrated while moving from Cisco WAE to Cisco Crosswork Planning:

- HA, LDAP, and User Management configurations
- Smart Licensing configurations
- WMD configurations
- All optical/L1 related configurations, for example, optical agents, optical NIMO, L1-L3 Mapping, Feasibility Limit Margin, Central Frequency Exclude List, and so on. This is because, Cisco Crosswork Planning collection does not support optical features in this release. However, the optical configurations are collected as part of the upgrade script and can be used in future.

- Inter AS NIMO configurations
- Source collector details in the Copy demands step of Demand deduction collector, as these fields are different in Cisco WAE and Cisco Crosswork Planning. You have to manually configure it after migration.
- The networks which are not part of the Composer workflow
- The External executable script configurations, as these scripts may require some changes and testing before deploying to Cisco Crosswork Planning.
- The configured device credentials. A default credential is imported and you must re-enter the credentials.
- Certain resource files, for example, updated network access file, advanced Aggregator configurations such as sql-capabilities, sql-source-capabilities, and so on.
- Nodeflow configuration (BGP details) in case of NetFlow agents. You have to configure it manually post migration.
- Network record plan files

Migrate collector configurations between Cisco Crosswork Planning instances

This section explains how to migrate collector configurations from one Cisco Crosswork Planning instance (source) to the other (target).



Note If using the SR-PCE collector in your configurations, ensure to update the **SR-PCE host** and **Backup SR-PCE host** fields manually after migration. This is necessary because, these fields are not updated while migrating the collector configurations between Cisco Crosswork Planning instances.

Procedure

Step 1 Download the collector configuration file from the source machine.

a) Log in to the Cisco Crosswork Planning instance from which you want to migrate the configuration.
b) From the main menu, choose **Collector** > **Migration**.
c) Click **Actions** and select **Configuration backup**.

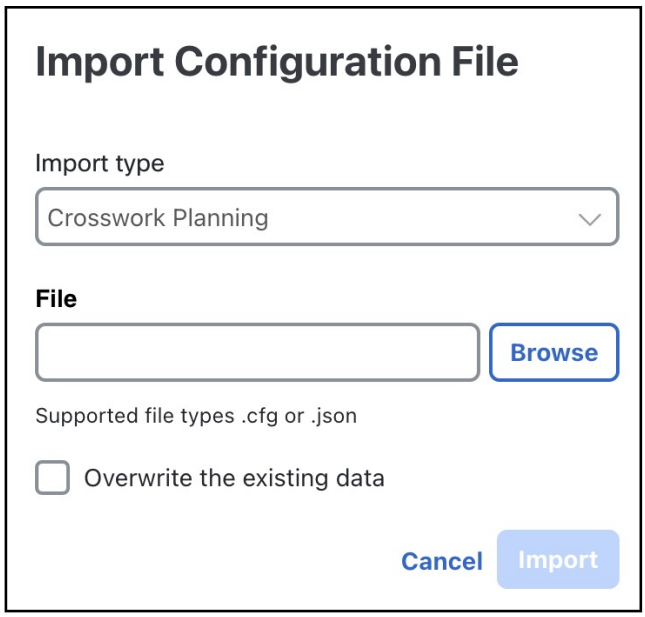
The collector configuration file is downloaded to your local machine.

Step 2 Import the collector configuration file to the target machine.

a) Log in to the Cisco Crosswork Planning instance to which you want to migrate the configuration.
b) From the main menu, choose **Collector** > **Migration**.
c) Click **Actions** and select **Configuration migration**.

The Import Configuration File page appears.

Figure 5: Import Configuration File page



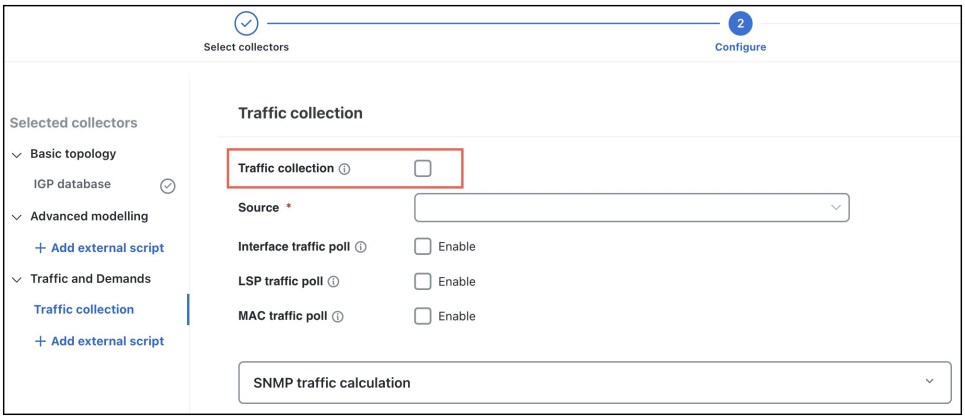
d) Select **Crosswork planning** from the **Import type** drop-down list.
e) Click **Browse** and select the collector configuration file downloaded earlier in the Step 1 (c).
f) (Optional) If you want to overwrite the existing collector configuration, check the **Overwrite the existing data** check box.
g) Click **Import** to import the collector configuration file.

The system proceeds with the import using your configuration. You can monitor the progress on the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays **Success**.

What to do next

Note In case of traffic collection, if the traffic poller agent status is displayed as down on the Agent page after migration, even though traffic collection has run successfully, follow these steps:

1. On the Collections page, click **Edit collection** for the collection corresponding to the agent.
2. On the Traffic collection configuration page, uncheck the **Traffic collection** check box and save the configuration.
3. Re-enable the **Traffic collection** check box and save the configuration again.



For details on configuring the **Traffic and Demands** collector, see Collect traffic statistics, on page 78.

Configure credential profiles

You must define credential profiles to access the devices. 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 Planning to access and manage them.

Before creating a credential profile, you must gather access credentials and supported protocols that you will use to monitor and manage your devices. For devices, it includes user IDs, passwords, and connection protocols. You will also need additional data such as the SNMPv2 read and write community strings, and SNMPv3 auth and privilege types.

This workflow describes the steps to create the credential profiles.

Step	Action
1. Set up device authentication credentials to access devices.	See Configure authentication credentials, on page 17.
2. Set up SNMP credentials to access the network server.	See Configure SNMP credentials, on page 18.

Configure authentication credentials

This section explains how to configure authentication credentials for accessing devices using SSH or Telnet.

Configure authentication credentials when setting up device access in the system for the first time or when adding new credentials for future device connections. These credentials enable secure connectivity of network devices via SSH (recommended for security) or Telnet.

You can configure authentication credentials during the initial setup via the **Collector** > **Collections** page or at any time from the **Credentials** page.

Follow these steps to set up authentication credentials from the **Collector** > **Credentials** page.

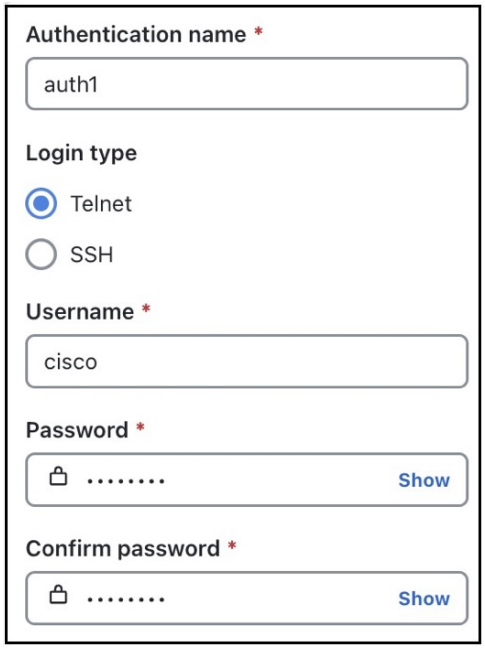
Procedure

Step 1 From the main menu, choose **Collector** > **Credentials**.

Step 2 Click **+ Create new** in the **Authentication** tab.

Note
If you are creating the authentication credentials for the first time, then click **Setup credentials**.

Figure 6: Configure authentication credentials



Step 3 Enter the values in these fields:

- Authentication name: Enter a descriptive name.
- Login type: Select either **SSH** or **Telnet** according to your requirement. The SSH protocol is more secure. The Telnet protocol does not encrypt the username and password.
- Credential fields: Enter the values in the **Username**, **Password**, and **Confirm password** fields.

Step 4 Click **Save**.

The system saves the new authentication credentials, making them available for device access through SSH or Telnet as configured.

Configure SNMP credentials

This section explains how to set up SNMP credentials to enable secure communication between the node and the seed router.

SNMP credentials are required for authenticating and encrypting messages exchanged between the node and the seed router. You can configure SNMP credentials during the initial setup via the **Collector** > **Collections** page or at any time from the **Credentials** page.

Follow these steps to configure SNMP credentials from the **Collector** > **Credentials** page.

Before you begin

Determine in advance whether you require SNMPv2c or SNMPv3, and gather any required authentication or encryption details.

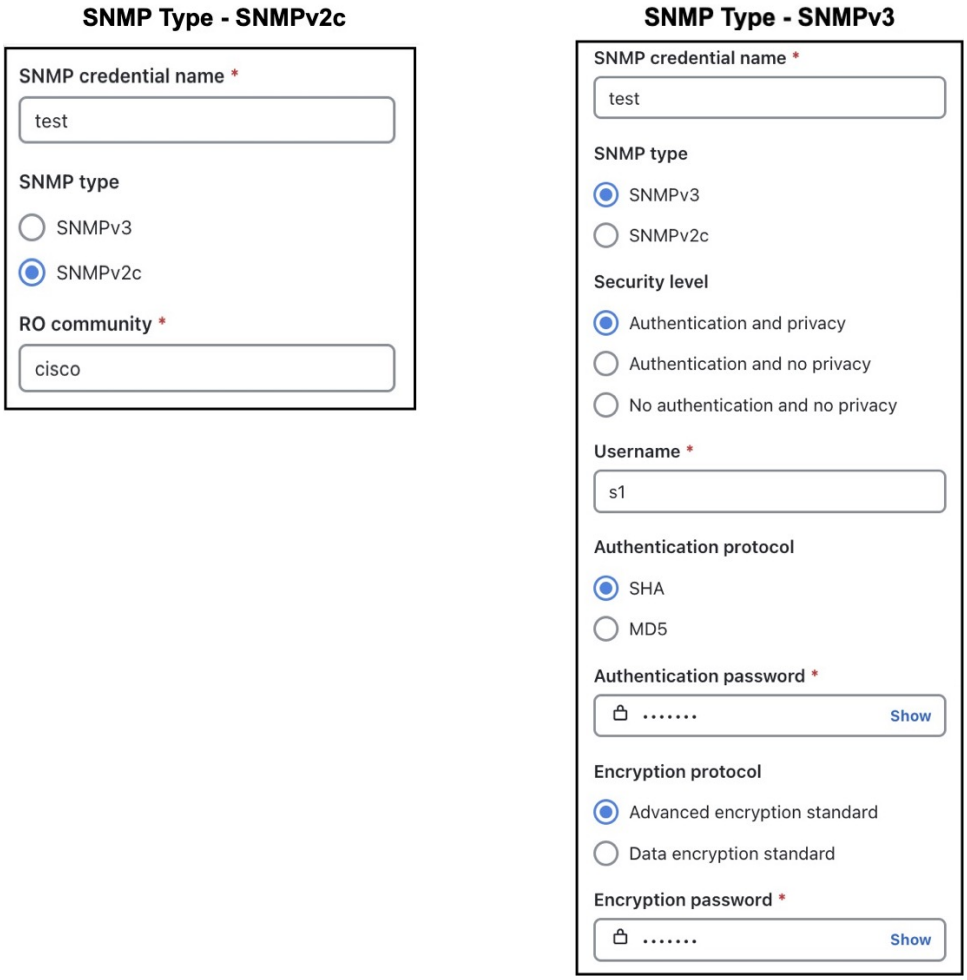
Procedure

Step 1 From the main menu, choose **Collector** > **Credentials**.

Step 2 Click the **SNMP** tab and then click **+ Create new**.

Note
If you are creating the authentication credentials for the first time, then click **Setup credentials**.

Figure 7: Configure SNMP credentials



Step 3 In the **SNMP credential name** field, enter a descriptive name for the SNMP profile.

Step 4 In the **SNMP type** section, select which SNMP protocol to use. The options are **SNMPv3** and **SNMPv2c**.

- SNMPv2c: Enter the SNMP RO community string that acts as a password. It is used to authenticate messages sent between the node and the seed router.
- SNMPv3: Enter the values in the fields mentioned in Table 1: SNMPv3 fields.

Table 2: SNMPv3 fields

Field	Action
Security level	Select one of these options: • Authentication and privacy: security level that provides both authentication and encryption. • Authentication and no privacy: security level that provides authentication but does not provide encryption. • No Authentication and no privacy: security level that does not provide authentication or encryption.
Username	Enter the user name.
Authentication protocol	Select one of these options: • SHA: HMAC-SHA-96 authentication protocol • MD5: HMAC-MD5-96 authentication protocol
Authentication password	Enter the authentication password.
Encryption protocol and Encryption password	The encryption option offers a choice of Data Encryption Standard (DES) or 128-bit Advanced Encryption Standard (AES) encryption for SNMP security encryption. The AES-128 token indicates that this privacy password is for generating a 128-bit AES key #. The AES encryption password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters. If you use the localized key, you can specify a maximum of 130 characters.

Step 5 Click **Save**.

The new SNMP credential is saved and available for secure device discovery or communication between your node and the seed router.

Configure network profiles

A network profile is made up of network nodes and their credentials. This section explains how to define a network profile to gather the data from the network.

When accessing the Collections page (**Collector** > **Collections**) for the first time, a Welcome screen appears. Click **Get Started** to see the preconfiguration steps, which are listed in the stepper pane on the left. After you complete the initial two steps, the third one guides you to complete the creation of network profiles.

Alternatively, follow these steps to set up network profiles from the **Collector** > **Network Profiles** page.

Before you begin

Configure device credential profiles (Authentication profiles and SNMP profiles). For details, see Configure authentication credentials, on page 17 and Configure SNMP credentials, on page 18.

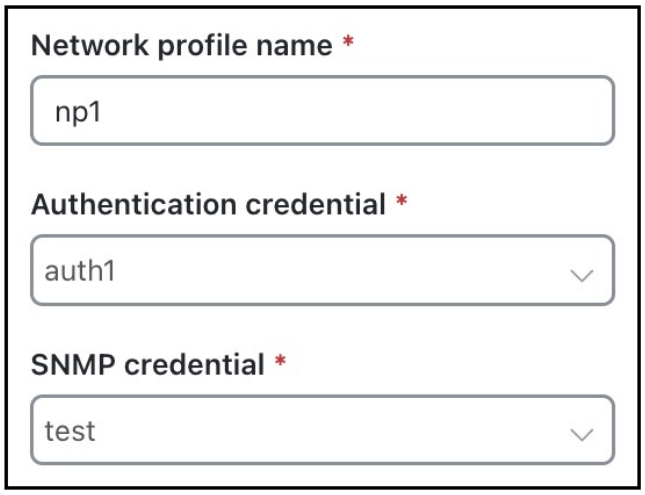
Procedure

Step 1 From the main menu, choose **Collector** > **Network Profiles**.

Step 2 Click the **+ Create new** button.

Note
If you are creating the network profile for the first time, then click **Setup network profile**.

Figure 8: Create network profile



Step 3 Enter the required values in each of these fields.

- Network profile name: Enter a name for the network access profile.
- Authentication credential: Select the applicable authentication credential from the drop-down list. If you don't have any authentication credential created, create one using the steps mentioned in Configure authentication credentials, on page 17.
- SNMP credential: Select the applicable SNMP credential from the drop-down list. If you don't have any SNMP credential created, create one using the steps mentioned in Configure SNMP credentials, on page 18.

Step 4 Click **Create & Proceed**.

Step 5 (Optional) To add or edit nodes associated with these network access credentials, see Add or edit nodes, on page 22.

Step 6 (Optional) To include or exclude individual nodes from the collection, see Configure node filter, on page 23.

Step 7 Click **Save**.

The network profile is created successfully and ready for use in gathering data from the network.

Add or edit nodes

This section explains how to add or edit nodes to update the network profile with correct node details.

Procedure

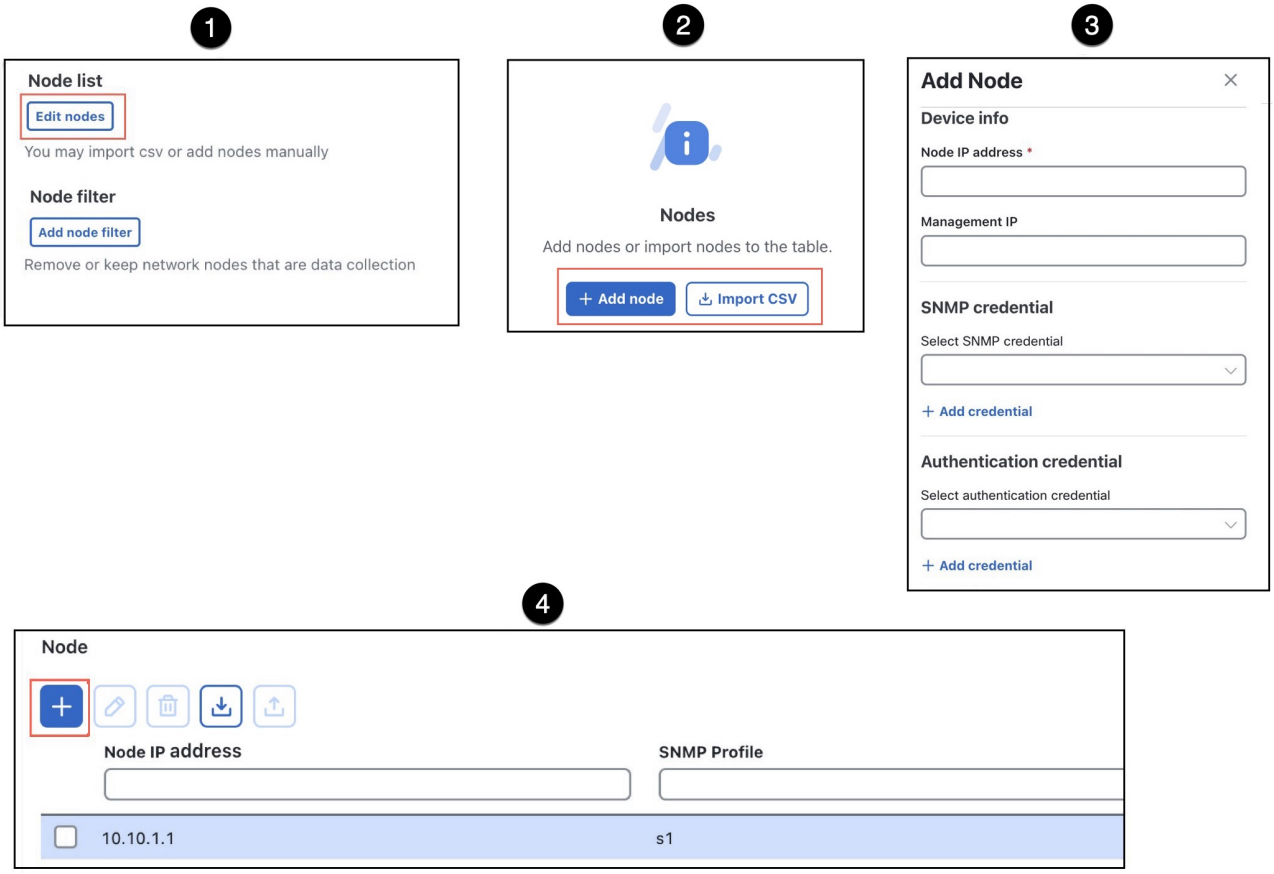
Step 1 From the main menu, choose **Collector** > **Network Profiles**.

Step 2 Select the required network profile and click **Save & Proceed**.

Step 3 Under **Node list**, click **Edit nodes** and decide how you want to add nodes.

If you decide to ...	Then ...
When there are no nodes:	
add nodes manually for the first time	**a.** Click + **Add node**. **b.** Enter the node details in the Add Node window. **c.** Click **Save**. The newly added node appears on the Node List page.
import the node list	**a.** Click Import CSV. **b.** Click **Browse** and enter the CSV file path. **c.** Click **Import**. The newly imported nodes appear on the Node List page.
When nodes exist:	
add more nodes	click + and enter the details.
import a different node list	Click and import the CSV file. Click the **sample file** link to download a sample file containing the node list.
export a node list	click .
edit a node	**a.** Select the node you want to edit. **b.** Click . **c.** Enter the node details.
delete nodes	Select the nodes and click .

Figure 9: Edit nodes pages



Step 4 Click **Done**.

Configure node filter

This section explains how to include or exclude individual nodes from the data collection.

Note

- You can add Node/Host name or loopback IP in the node filter list. Management IP must not be added in node filter IPs.
- Node/Host name works with ISIS.
- The OSPF database does not have node names, so filtering works by only IP address.
- Node filter does not support Segment List hops.

Procedure

Step 1 From the main menu, choose **Collector** > **Network Profiles**.

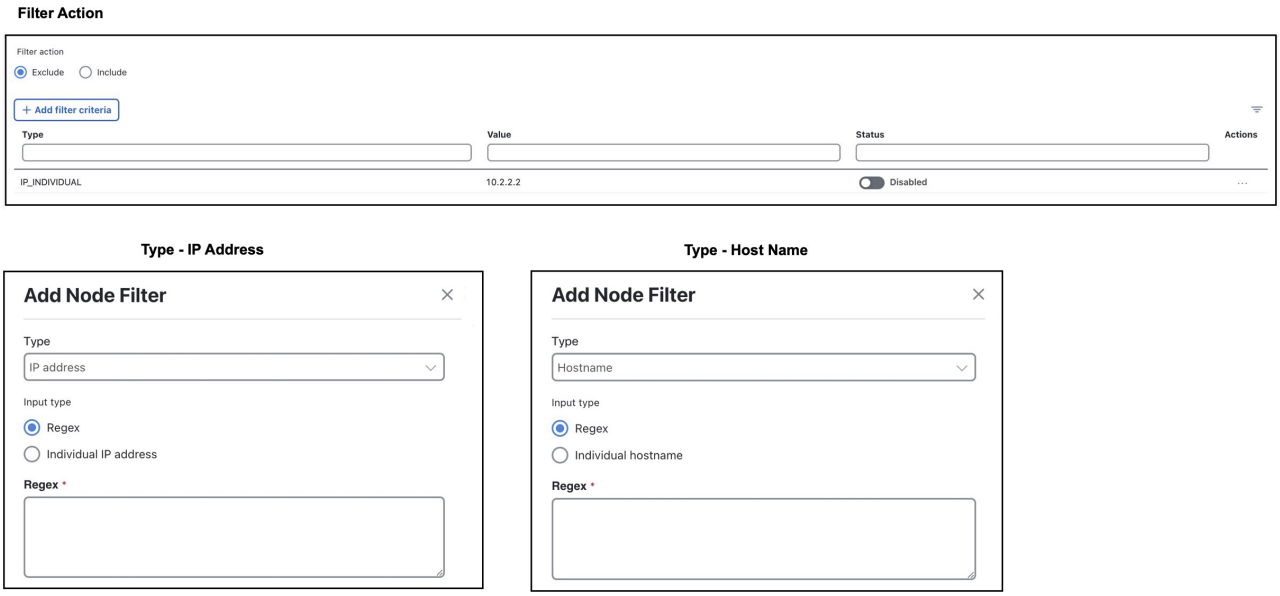
Step 2 Choose the required network profile and click **Save & Proceed**.

Step 3 Click **Add node filter**.

Step 4 Under **Filter action**, choose either **Exclude** or **Include** to exclude or include individual nodes, respectively.

Step 5 Click + **Add filter criteria**. The Add Node Filter page appears.

Figure 10: Node filter pages



Step 6 From the **Type** drop-down list, choose the type using which you want to filter. The options are: **IP address** and **Hostname**.

Step 7 Select the required option under **Input type** and click **Save**. The options depend on the type you selected in the previous step.

- If you selected **IP address**, the options are: **Regex** and **Individual IP address**.
- If you selected **Hostname**, the options are: **Regex** and **Individual hostname**.

If you decide to ...	Then ...
include or exclude multiple nodes with a regular expression	**a.** Select the **Regex** option. **b.** Enter the Regex expression in the **Regex** field. **Note** If you configure multiple regex filters (for example, one for IP and one for Hostname), the system combines them into a single pattern using the logical OR operator (|). A node is filtered if it matches either the IP pattern or the Hostname pattern. For an example of how regex-based criteria are used to filter nodes, see Regex-based filtering criteria for node selection, on page 25.
add each node's IP address	**a.** Select the **Individual IP address** option. **b.** Enter the IP address in the **IP address** field.
add each node's hostname	**a.** Select the **Individual hostname** option. **b.** Enter the hostname in the **Hostname** field.

Step 8 Optionally, you can repeat steps 4 to 7 to add more filter criteria.

Step 9 Set the toggle in the **Status** column to Enabled to consider the entries in the filter. Then, click **Save**.

What to do next

To edit or delete nodes, use the ••• > **Edit** or ••• > **Delete** options under the **Actions** column.

Regex-based filtering criteria for node selection

When you use regex expressions for IP address and Hostname, the collector service evaluates the patterns against specific fields in the plan database:

- Regex in IP address: Matched against the "Node.IPAddress" field.
- Regex in Hostname: Matched against the "Node.Name" field.

Example

To include nodes from a specific subnet or nodes with a specific pattern, you can add two separate filter criteria:

- **Type**: IP address, **Input type**: Regex, **Value**: 10\.1\..*
- **Type**: Hostname, **Input type**: Regex, **Value**: .*-lab$

The system processes these as a combined expression: **10\.1\..*|.*-lab$**. This will match:

- 10.1.50.1 (matches the IP address pattern)

- router1-lab (matches the hostname pattern)
- 10.1.1.5 (matches the IP address pattern)

Configure agents

This section describes how to configure agents to enable network collection operations in Cisco Crosswork Planning.

Agents perform information-gathering tasks and should be configured before certain network collection operations. This task is required only for collecting SR-PCE or NetFlow information.

When accessing the Collections page (**Collector** > **Collections**) for the first time, a Welcome screen appears. Click **Get Started** to see the preconfiguration steps, which are listed in the stepper pane on the left. After you complete the initial three steps, the fourth one guides you to complete the creation of agents.

Alternatively, follow these steps to configure agents from the **Collector** > **Agents** page.

Procedure

Step 1 From the main menu, choose **Collector** > **Agents**.

Note
If a collection includes the **Traffic collection** collector, the **Collector** > **Agents** page displays the traffic poller agent details as well. The agent's name is the same as that of the collection.

Step 2 Click **+ Create new**.

If you are creating agents for the first time, then click **Setup agent**.

Step 3 Enter a name for the agent in the **Agent name** field.

Step 4 Select the required Collector type.

- SR-PCE: Collects information from the SR-PCE server periodically, and processes the topology and LSP data and notifications sent by SR-PCE. The agent connects to the REST interface of SR-PCE and retrieves the PCE topology.

  Note
  You must configure the SR-PCE agents for any networks that use SR-PCE before you can perform a network collection.

- NetFlow: Responsible for receiving, processing, and storing the flow records. This data helps to analyze and gain insights into the traffic patterns and behavior of the network.

Step 5 The configuration options vary depending on the Collector type you select.

- If you select **SR-PCE**, then enter the applicable configuration details mentioned in SR-PCE agent configuration options, on page 27.
- If you select **NetFlow**, then enter the applicable configuration details mentioned in NetFlow agent configuration options, on page 28.

Step 6 Click **Save**.

The newly created agent appears on the **Collector** > **Agents** page.

- The SR-PCE and NetFlow agents restart when the configuration parameters are edited after saving.
- The SR-PCE agent
  - starts right away after configuration or when Cisco Crosswork Planning starts, as long as the **Enabled** option is selected, and
  - stops when (a) the configuration is removed, (b) Cisco Crosswork Planning has stopped, or (c) the **Enabled** option is deselected.

What to do next

Use the **Collections** page (**Collector** > **Collections**) to configure the collectors to build a network model. For more information, see Configure collections, on page 30.

SR-PCE and NetFlow agent configuration options

This topic describes the options available for configuring SR-PCE and NetFlow agents.

SR-PCE agent configuration options

This table provides the configuration options for SR-PCE agents.

Table 3: SR-PCE agent configuration options

Option	Description
Enabled	Enables the SR-PCE agent. Default is enabled.
SR-PCE host IP	Host IP address of the SR-PCE router.
SR-PCE REST port	Port number to connect to the SR-PCE host. The default is 8080.
Authentication type	Authentication type to be used for connecting to the SR-PCE host. • Basic: Use HTTP Basic authentication (plaintext). • Digest: Use HTTP Digest authentication (MD5). • None: Use no authentication. This is applicable only for old IOS XR versions.
Username	Username for connecting to the SR-PCE host.
Password	Password for connecting to the SR-PCE host.
Connection retry count	Maximum number of retry counts for connecting to the SR-PCE host.

Option	Description
Topology collection	Specifies whether to collect topology data and to have subscription for network changes. These are the options: • Collection only • Collection and Subscription (default) • Off
LSP collection	Specifies whether to collect LSP data and to have subscription for network changes. These are the options: • Collection only • Collection and Subscription (default) • Off
Connection timeout interval	Connection timeout in seconds. Default is 50 seconds.
Pool size	Number of threads processing SR-PCE data in parallel.
Keep alive interval	Interval in seconds to send keep-alive messages. Default is 10.
Batch size	Number of nodes to send in each message. Default is 1000.
Keep alive threshold	Threshold of missed keep-alive messages. Default is 2.
Event buffer enabled	Enables you to add buffer time to process notifications in an SR-PCE agent. The SR-PCE agent processes the notification, and only after the buffered time (specified in the **Events buffer time** field), the consolidated notification is sent to SR-PCE and PCEP LSP collectors. This feature is helpful if there are too many back to back notifications like link flapping, etc. The SR-PCE agent can be configured to collect only Topology information or LSP information using the **Topology collection** and **LSP collection** fields.
Events buffer time	Time to buffer SR-PCE events before sending to collectors, in seconds.
Playback events delay	Delay in SR-PCE events playback to mimic real events, in seconds (0 = no delay).
Max LSP history	Number of LSP entries to send. Default is 0.
Net recorder mode	Records SNMP messages. You can select Off, Record, or Playback. Default is Off.

NetFlow agent configuration options

This table provides the configuration options for NetFlow agents.

Table 4: NetFlow agent configuration options

Option	Description
BGP	Enables passive BGP peering. Cisco Crosswork Planning tries to set up a BGP session with the router. Enter the BGP details in the table listed below the BGP check box.
Name	Node name.
Sampling rate	Sampling rate of the packets in exported flows from the node. For example, if the value is 1,024, then one packet out of 1,024 is selected in a deterministic or random manner.
Flow source IP	IPv4 source address of flow export packets.
BGP source IP	IPv4 or IPv6 source address of iBGP update messages.
BGP password	BGP peering password for MD5 authentication.
Interval	Interval in seconds for writing the output file. Enter the value that is greater than zero and multiple of 60. Default is 900 seconds.
Flow size	Flow collection deployment size, based on network-wide aggregated flow export traffic rate. • Small: Recommended when flow traffic rate is less than 10 Mbps. • Medium: Recommended when flow traffic rate is between 10 Mbps and 50 Mbps. • Large: Recommended when flow traffic rate is more than 50 Mbps. • Lab: Not for customer use. Default is Medium.
Extra aggregation	Choose aggregation keys from the list.

Agent operations

There are several operations you can perform on the agents created:

- **Edit**—Use this option to edit the agent parameters.
- **Start**, **Restart**, and **Stop**—Use these options to start, restart, and stop the agents, respectively.
- **Verify connection**—Use this option to check the status of the agents.
- **Delete**—Use this option to delete the agents.
- **Add schedule** and **Edit schedule**—Use these options to set up and edit the data refresh frequency for the agents, respectively. Enter the schedule using a cron expression.

Note This option is available only for SR-PCE agents. You can only add or edit schedules, but you cannot view the schedule details such as Status, Duration, and so on.

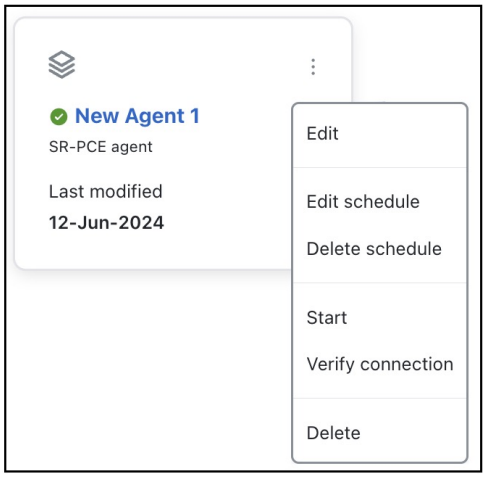
- **Delete schedule**—Use this option to delete the data refresh frequency set for the agents.

Note This option is available only for SR-PCE agents.

Follow these steps to access these options.

1. From the main menu, choose **Collector** > **Agents**. The list of already created agents appears.
2. Click ⋮ in the agent that you want to edit and choose the relevant option. Note that the options differ based on the type of agent.

Figure 11: Agent operations - example



Configure collections

This topic describes how to create collections using the Cisco Crosswork Planning UI.

The Collections page provides a visual workflow to guide you from creating a network model using various collectors to setting up a schedule to run collections and archiving the network models.

Important When configuring collections in Cisco Crosswork Planning, it is important to understand how collections and network devices impact the system's capacity. The scale numbers (for example, 6,000 or 3,000 nodes) represent the total capacity across all collections combined. For example, you can create a 6,000-node configuration using either a single collection containing all nodes or multiple collections, such as six collections with 1,000 nodes each. However, exceeding the system's defined scale limits can result in performance issues. These include collectors and aggregators running out of memory. Ensure the total number of devices or interfaces across all collections remains within the defined scale limits to maintain optimal system performance. For details on scale numbers, see the *"Profile specifications"* section in the *Cisco Crosswork Planning 7.1 Installation Guide*.

Before you begin

Ensure that you have completed the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 From the main menu, choose **Collector** > **Collections**. The list of already created collections appears.

Step 2 Begin the process of creating collections.

a) Click **Add collection** at the top right corner. The Add Collection page appears.

If you are creating the collection for the first time, then click **Add collection** in the Create collection page.

b) In the **Collection name** field, enter the name of the collection.

c) From the **Node profile** drop-down list, select the required node profile.

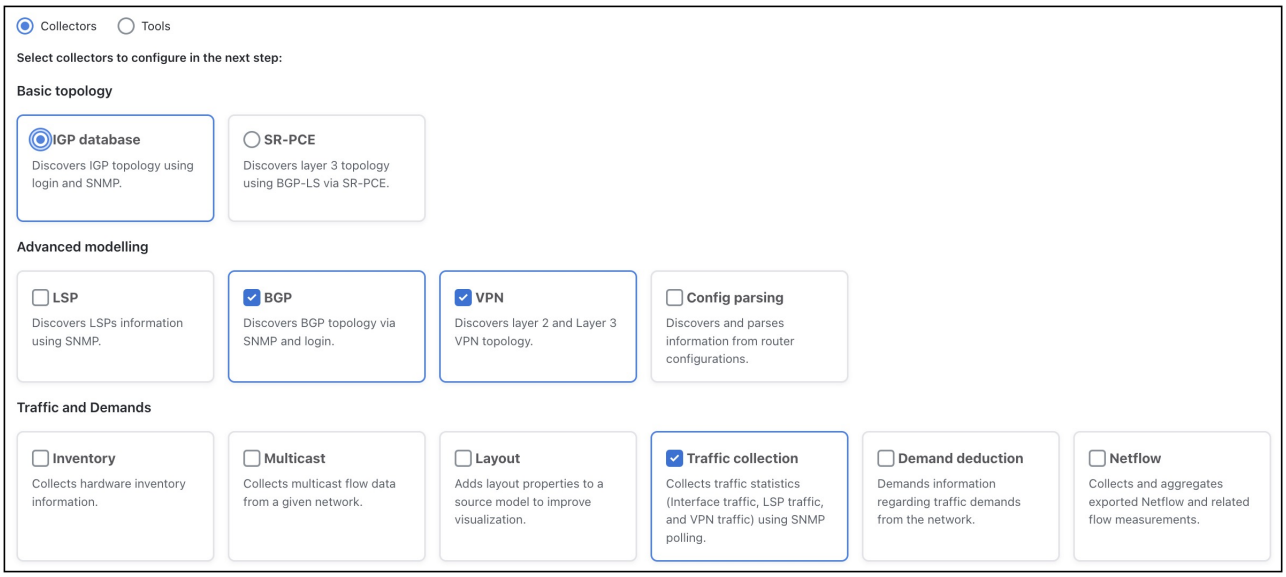
To create a new node profile, click **+ Add new profile**.

d) Click **Continue** to proceed to the collection configuration page.

Step 3 Select the required collectors. For descriptions of all the collectors, see Collector descriptions, on page 49.

a) Verify that **Collectors** is selected at the top. This option is selected by default.

Figure 12: Select collectors page



b) Select one of the Basic topology collectors to initiate the network collection. Supported collectors include: IGP database and SR-PCE.

Note that you can select only one topology collector.

c) Select additional collectors as needed from these sections.

- Advanced modeling: Select the required advanced network data collectors to configure additional data collections. The supported advanced modeling collectors are: LSP, BGP, VPN, and Config parsing. You can select multiple advanced collectors.
- Traffic and Demands: Select the required collectors for traffic collection. The supported traffic and demands collectors are: Inventory, Multicast, Layout, Traffic collection, Demand deduction, and NetFlow. You can select multiple traffic and demand collectors.

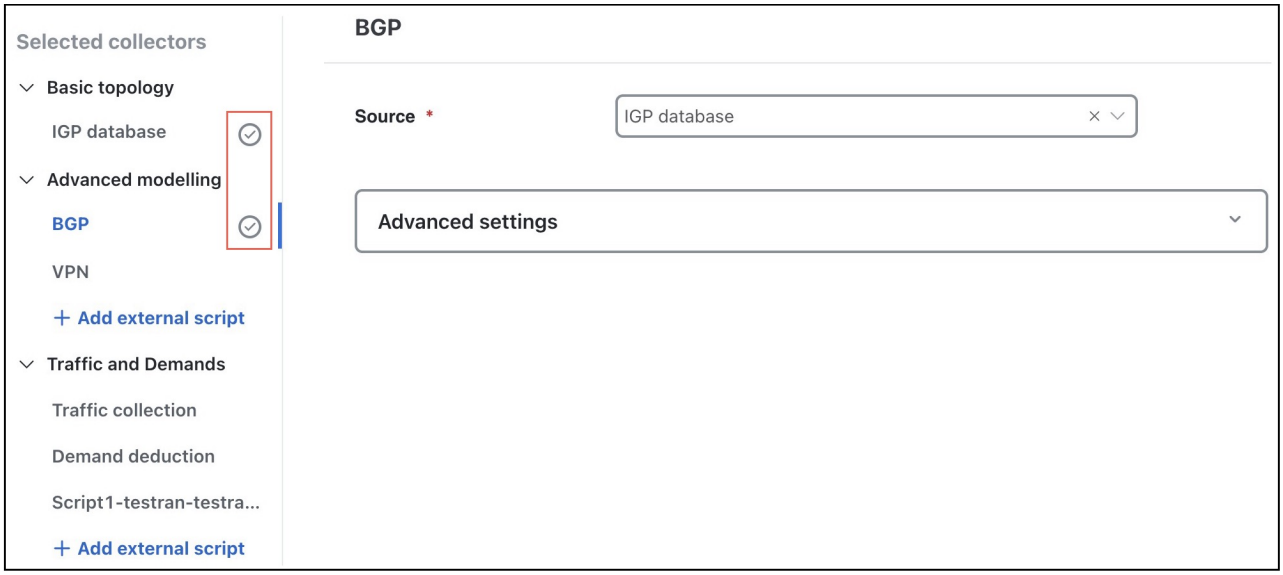
Step 4 Configure collectors.

a) Enter the configuration parameters for the selected collectors.

- The **Selected collectors** pane on the left displays the collectors that you selected in the previous step. Click the collector name in this pane to enter the configuration details.
- From the **Source** drop-down, select the collector whose output will serve as the source (input) for the currently selected collector.
- A tick mark appears next to the collector name once you enter all the required configuration parameters for that specific collector.
- To exclude a selected collector during the configuration process, click Remove.

Note
You must enter the configuration details for all selected collectors. Otherwise, the **Next** button is not enabled and you will not be able to proceed further.

Figure 13: Configure collection parameters



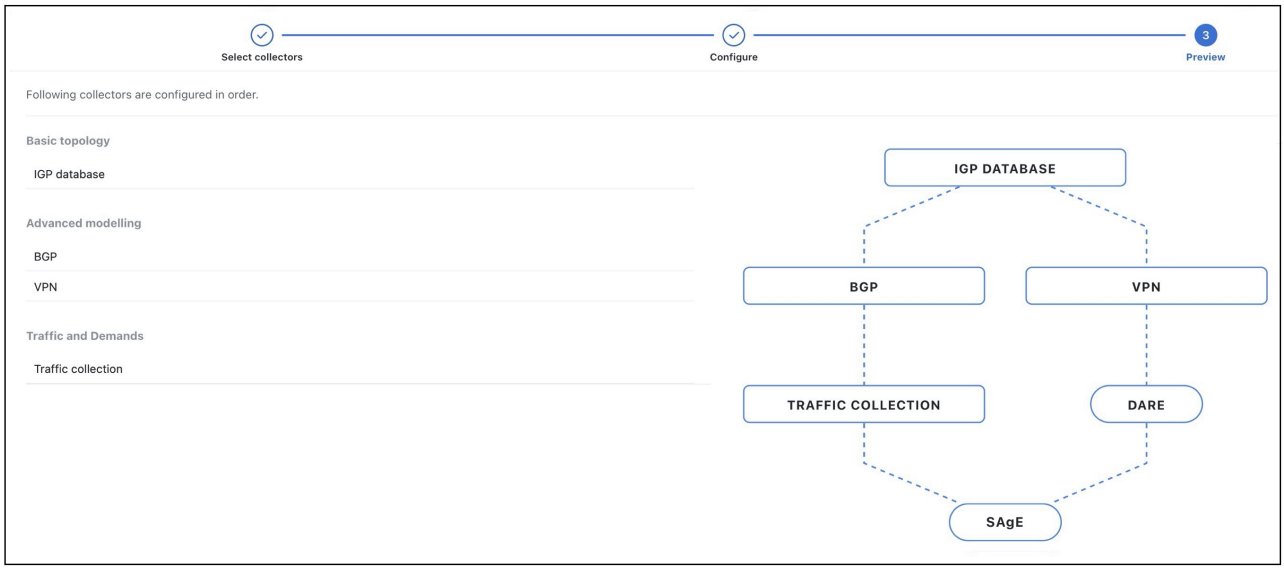
b) (Optional) To use a customized script against a collection model, click the **+ Add external script** link. For details, see Run an external script against a network model, on page 87.

c) Once the configuration parameters are entered for all the collectors, click **Next**.

Step 5 Preview the order in which the collectors are added and complete collection creation.

a) Review the preview diagram to verify the order in which collectors are added. You can observe which collector output is being used as the input for the other collector.

Figure 14: Preview page



b) If you are satisfied with the configuration, click **Create** to proceed with the creation of the collection.

- A confirmation message appears indicating that the collection has been successfully created.

- To make any changes to the configuration, click **Back** to go back to the previous page. You can also click the step numbers at the top to navigate to the required configuration step.

Note

- By default, all changes are auto saved as you make them. Until you click the **Create** button, these changes are saved as **Draft**.
- Auto-saving is enabled only when creating a new collection or if the collection is in the Draft state. If you are editing an existing collection, the changes are not auto-saved.

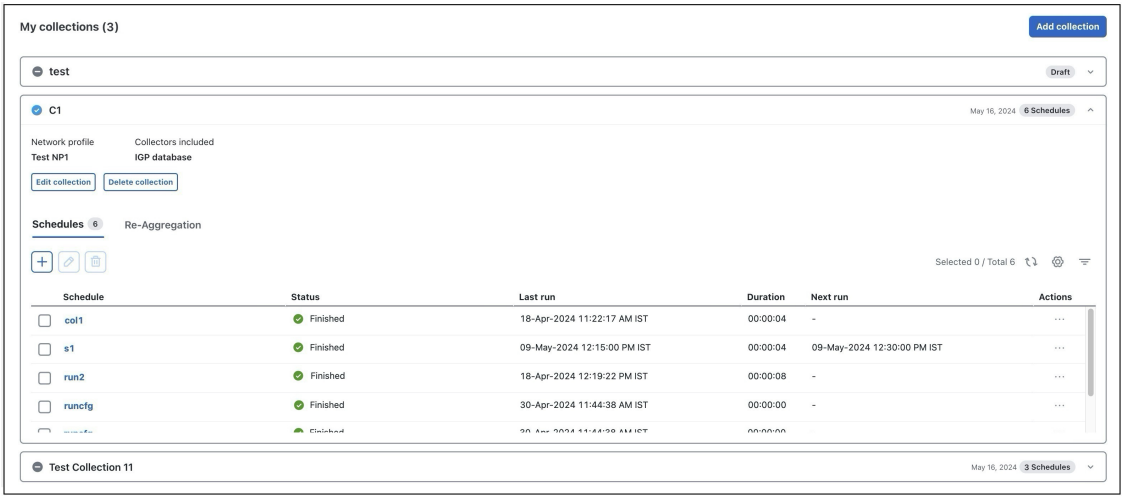
Step 6 (Optional) If you want to configure the schedules immediately, click **Add schedule** in the dialog box and proceed with the schedule configuration. For details, see Schedule collections, on page 36.

Step 7 Click **Done** in the successful message box to complete the collection creation process.

The newly added collection appears in the **Collector** > **Collections** page. Expand each collection panel to view its details.

This image shows a sample Collections page with three collections.

Figure 15: List of available collections



What to do next

Schedule collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule collections, on page 36.

Edit collections

This topic describes how to edit existing collections.

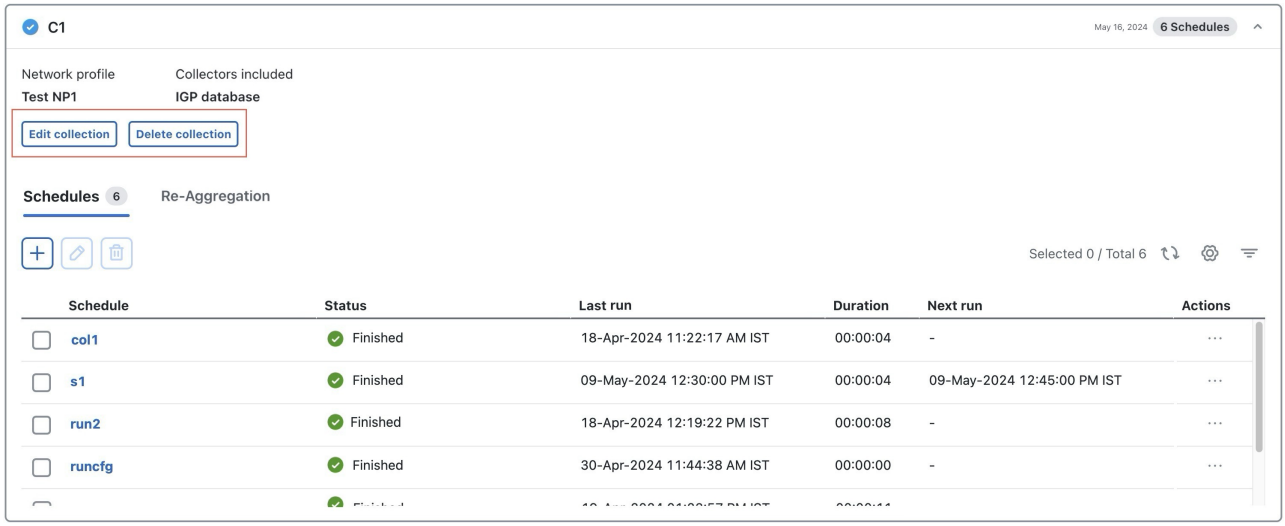
Procedure

Step 1 From the main menu, choose **Collector** > **Collections**. The list of existing collections appears.

Step 2 Expand the Collection area you want to edit.

Step 3 Click **Edit collection**.

Figure 16: Collection actions



Step 4 Make the required changes in the **Select collectors** and **Configure** pages. Preview the changes and ensure that the updated configuration meets your requirements. For more information, see Configure collections, on page 30.

Step 5 Click **Save**.

What to do next

Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule collections, on page 36.

Delete collections

This topic describes how to delete existing collections.

Procedure

Step 1 From the main menu, choose **Collector** > **Collections**. The list of existing collections appears.

Step 2 Expand the Collection area you want to delete.

Step 3 Click **Delete collection** (for reference, see Figure 16: Collection actions, on page 35).

Step 4 Click **Yes** in the confirmation dialog box.

A message confirming the successful deletion of the collection appears.

Schedule collections

This topic describes how to schedule different network collections to run using the Cisco Crosswork Planning UI.

You can schedule jobs to run at a specific date and time, or at regular intervals. You can also create multiple schedules for the same collection with different time intervals and collector settings.

Before you begin

- Ensure that you have created the required collections. For details, see Configure collections, on page 30.
- Be familiar with using cron expressions.

Procedure

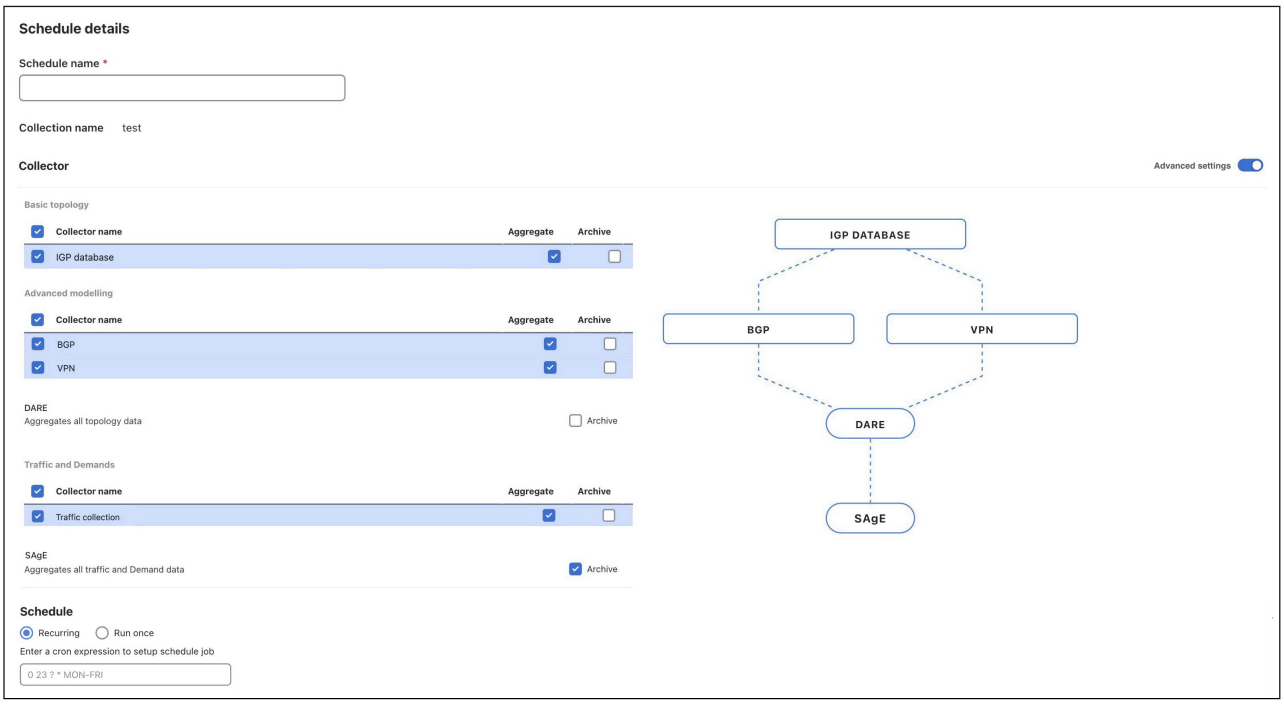
Step 1 From the main menu, choose **Collector** > **Collections**. The list of already created collections appears (for reference, see Figure 15: List of available collections, on page 34).

Step 2 Expand the collection panel for which you want to add the schedule. Use one of these options to create the schedule:

- If this is the first time you are creating the schedule, then click the **Add schedule** button while creating the collection or in the collection panel.
- If there are already other schedules available, click the  icon under the **Schedule** tab to create additional schedules (see Figure 18: Schedule actions, on page 38).

The Schedule details page appears.

Figure 17: Schedule details



Step 3 In the **Schedule name** field, enter the name for the schedule.

Step 4 In the **Collector** section:

- If you want to exclude any collector from data collection, uncheck the check box next to the collector name.
- If you want to exclude any collector from aggregation, uncheck the check box under the **Aggregate** column of the corresponding collector. For details, see Aggregate collector outputs, on page 40.
- If you want to archive any collection, check the check box under the **Archive** column of the corresponding collector. For details, see Configure archive, on page 43.

Step 5 In the **Schedule** section, specify whether you want to run this collection once or as a recurring job.

- If you select the **Run once** option, the collection runs immediately and only once. After selecting this option, the **Schedule** button at the bottom changes to **Run now**. Click it to run the collection immediately.
- If you select the **Recurring** option, specify the time interval using a cron expression. The **Recurring** option is selected by default. After entering the cron expression, click **Schedule** to run the job at the time interval you specified.

Step 6 (Optional) Repeat steps 2 through 5 if you want to create more schedules.

The configured schedule appears in the corresponding Collection panel in the **Collector** > **Collections** page. Click the schedule name under the **Schedule name** column to view its details.

Edit schedules

This topic describes how to change the execution timing or parameters of existing schedules within a collection..

Use this task to update the schedule associated with a collection in the system. Editing a schedule lets you control when collections run, ensuring alignment with operational requirements or maintenance windows.

Procedure

Step 1 From the main menu, choose **Collector** > **Collections**. The list of existing collections appears.

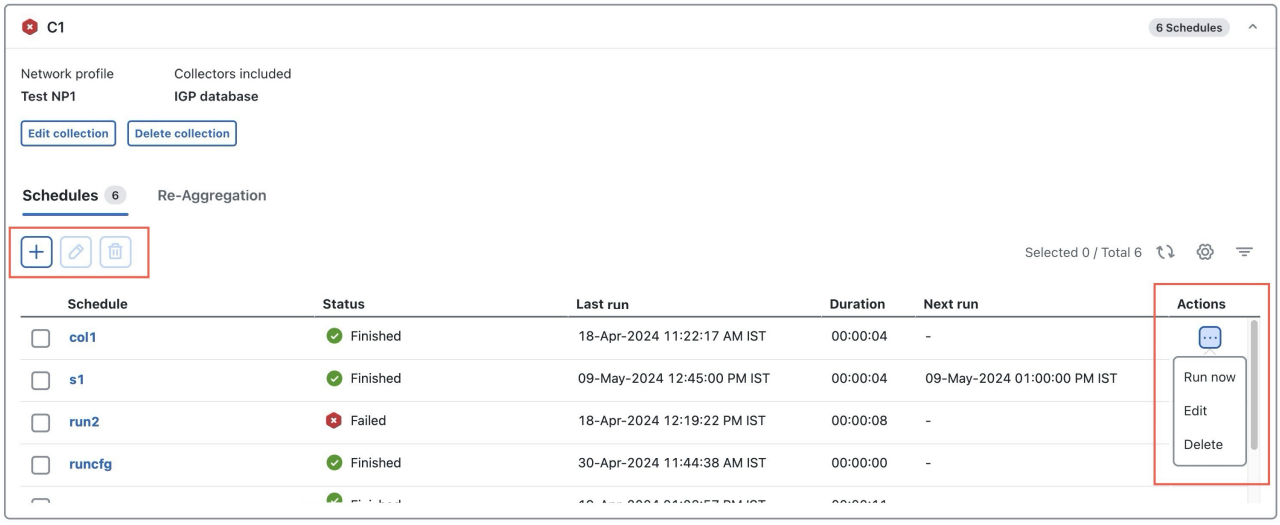
Step 2 Expand the collection panel that contains the schedule you want to edit.

Step 3 Under the **Schedules** tab, edit the schedules using any of these options:

- Select the schedule you want to edit and click .
- In the **Actions** column, click ••• > **Edit** for the schedule you want to edit.
- Click the schedule name (under the **Schedule** column) and then click **Edit**.

Note
You can edit only one schedule at a time.

Figure 18: Schedule actions



Step 4 In the **Edit Schedule** page, make the required changes.

Step 5 Click **Run now** to execute the job immediately, or click **Schedule** to set the job to run at a specified interval. For details, see Schedule collections, on page 36.

The selected schedule is updated. The collection will run immediately or at the newly specified intervals, depending on the option you chose.

Delete schedules

This topic describes how to remove unwanted collection schedules from the system.

Use this task when you need to clean up scheduled data collection activities to ensure only relevant schedules are active in your environment.

Procedure

Step 1 From the main menu, choose **Collector** > **Collections**. The list of existing collections appears.

Step 2 Expand the collection panel that contains the schedule you want to delete.

Step 3 Under the **Schedules** tab, delete the schedules using any of these options:

- Select the schedule you want to delete and click .
- In the **Actions** column, click ••• > **Delete** for the schedule you want to delete.

Note
You can delete only one schedule at a time.

Step 4 Click **Yes** in the confirmation dialog box.

The selected schedule is removed from the collection, and a confirmation message appears indicating successful deletion.

View scheduled task status and history

This topic describes how to view the statuses and recent histories of scheduled tasks for a collection.

After a schedule is configured for a collection, you can view the current task status and last 10 statuses of the tasks involved. This helps you track execution outcomes, troubleshoot failures, and download collected data when needed.

Follow these steps to view scheduled task statuses and histories.

Before you begin

Confirm that a schedule has been configured for the collection.

Procedure

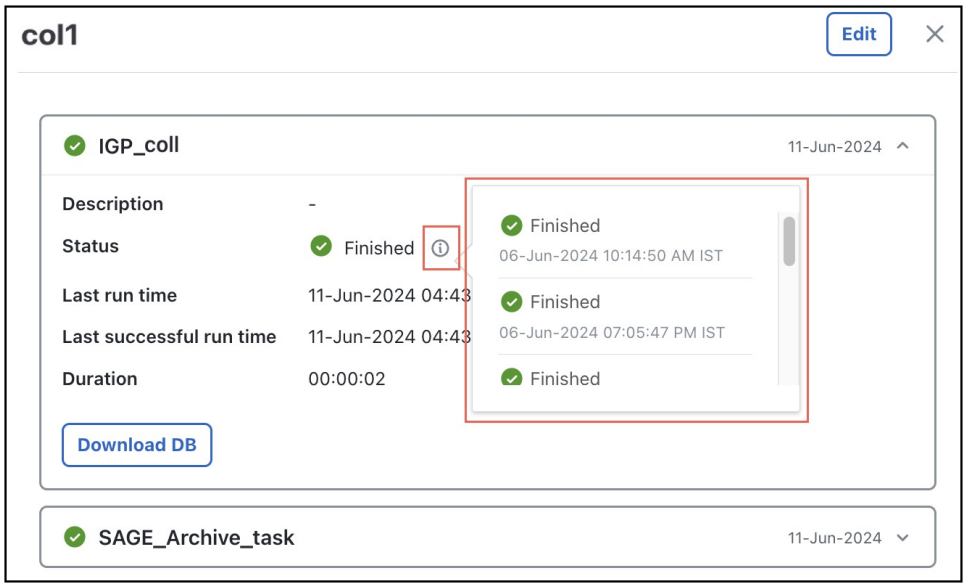
Step 1 Expand the desired collection panel.

Step 2 In the **Schedules** tab, click the name of the schedule.

The page that opens displays the statuses of all the tasks involved in the scheduled collection, including:

- timestamps of the recent task execution

- duration of each task, and
- description if the task has failed.



Step 3 Click the ⓘ icon in the **Status** field to display the last 10 task statuses.

Step 4 To download the collected data from the collector, click **Download DB**.

What to do next

If you identify any failed tasks, review the descriptions provided and take further troubleshooting or corrective action as needed.

Aggregate collector outputs

This topic describes how to exclude specific collector outputs from the network model aggregation process.

Each collector produces an output, which is aggregated (consolidated) to build a complete network model. Cisco Crosswork Planning uses the Delta Aggregation Rules Engine (DARE) to aggregate basic and advanced topology collector outputs. Simple Aggregation Engine (SAgE) consolidates all traffic and demand data, along with the topology changes from DARE, to create a final network model.

By default, all the selected collectors are included in the aggregation during collection configuration. You can choose to exclude any collector from aggregation while scheduling the collection. By doing so, even though the data is collected from the excluded collector, it will not be aggregated.

Note It is assumed that you are in the middle of creating a network model when performing the steps described in this topic. For more information, see Configure collections, on page 30.

Follow these steps to exclude a collector output from aggregation.

Procedure

Step 1 Open the Add or Edit Schedule page for the collection you want to edit. For more information, see Schedule collections, on page 36 or Edit schedules, on page 38.

Step 2 (Optional) Notice that the **Advanced Settings** toggle button is turned on by default. If it is off, turn it on.

Step 3 Under the **Collector** section, uncheck the **Aggregate** check box for the collector you want to exclude from aggregation.

Figure 19: Aggregation settings



Step 4 (Optional) Update the schedule settings. For more information, see Schedule collections, on page 36.

Step 5 If you select **Run once** in the previous step, click **Run now** to run the job immediately. If you select **Recurring**, click **Schedule** to run the job at the specified time interval.

After you uncheck the **Aggregate** check box for a collector, the subsequent data collected from that collector will not be aggregated. However, the data previously collected from the unchecked collector will still be available in the aggregator output.

Data from excluded collectors is no longer included in aggregation, ensuring only selected collector outputs contribute to the final network model.

Reaggregate collector outputs

This topic describes how to reaggregate collector outputs.

At any point during the collection process, you can perform reaggregation of all the collectors and populate the DARE and SAgE network afresh. This process does not trigger new data collection, but removes the previous aggregation results and starts a new aggregation.

Note In a collection

- only one scheduler can be used for reaggregation and
- only those collectors which are part of aggregation are considered for reaggregation.

Procedure

Step 1 From the main menu, choose **Collector** > **Collections**. The list of existing collections appears.

Step 2 Expand the collection panel in which you want to reaggregate the collector outputs.

Step 3 Click the **Re-Aggregation** tab.

Step 4 If re-aggregating for the first time, click **Schedule** or **Run once**.

- If you click **Run once**, the reaggregation happens immediately and only once.
- If you click **Schedule**, enter the data refresh frequency using a cron expression and click **Save**. The data resync occurs at the specified interval.

The **Network ReAggregation** entry appears in the table providing status and details of the job.

Figure 20: Reaggregation of collection



Step 5 To update the schedule or perform reaggregation again, click ••• under the **Actions** column. Based on the option you selected in the previous step, the options displayed under this button differ slightly.

- If you selected **Schedule**, these options appear: Run now, Edit schedule, Pause, and Delete.
- If you selected **Run once**, these options appear: Run now, Add schedule, and Delete.

Step 6 (Optional) Click the **Netwok ReAggregation** link in the table to view the details of aggregation.

The system discards the previous aggregation and initiates a new aggregation process for the selected collectors.

Configure archive

This topic describes how to configure archive settings in a collection.

After creating a network model and running collections, you can retrieve and view the plan files. Plan files capture all relevant information about a network at a given time, and can include topology, traffic, routing, and related information. The archive is a repository for plan files.

By default, the final network model is archived after running the collection. However, from the Add or Edit Schedules page, you can

- choose not to archive a final network model
- choose to archive models at a collection level, and
- schedule the archiving of network models.

Before you begin

It is assumed that you are in the middle of creating a network model when performing the steps described in this topic. For more information, see Configure collections, on page 30.

Procedure

Step 1 Open the Add or Edit Schedule page for the collection that you want to edit. For more information, see Schedule collections, on page 36 or Edit schedules, on page 38.

Step 2 (Optional) Check that the **Advanced settings** toggle button is turned on by default. If it is enabled, turn it on.

Step 3 Under the **Collector** section:

- To archive network models at a collection level, check the box under the **Archive** column for the corresponding collection.
- To prevent archiving of a final network model, uncheck the **Archive** check box next to SAgE.

Figure 21: Archive settings



Step 4 (Optional) Update the schedule settings. For more information, see Schedule collections, on page 36.

Step 5 If you select **Run once** in the previous step, click **Run now** to run the job immediately. If you select **Recurring**, click **Schedule** to run the job at the specified time interval.

In the final network model, the data collected from the unchecked collector will not be available.

The archived network model is saved in a plan file format (.pln) in the Archive section of the **Network Models** page.

What to do next

Access the plan files from the Cisco Crosswork Planning Design application. For more information, see View or download plan files, on page 44.

View or download plan files

The archived network model is saved in a plan file format (.pln), which can be downloaded or viewed from the **Network Models** page of the Cisco Crosswork Planning Design application. The archive locations vary based on whether the Cisco Crosswork Planning Design and Collector applications are installed on the same machine or on different machines. For more details, see the following sections.

Scenario 1: When the Cisco Crosswork Planning Design and Collector applications are installed on the same machine

If the Cisco Crosswork Planning Design and Collector applications are installed on the same machine, the archived network models appear under **Network Models** > **Local archive**.

Follow these steps to view or download the plan files from the Local archive.

Before you begin

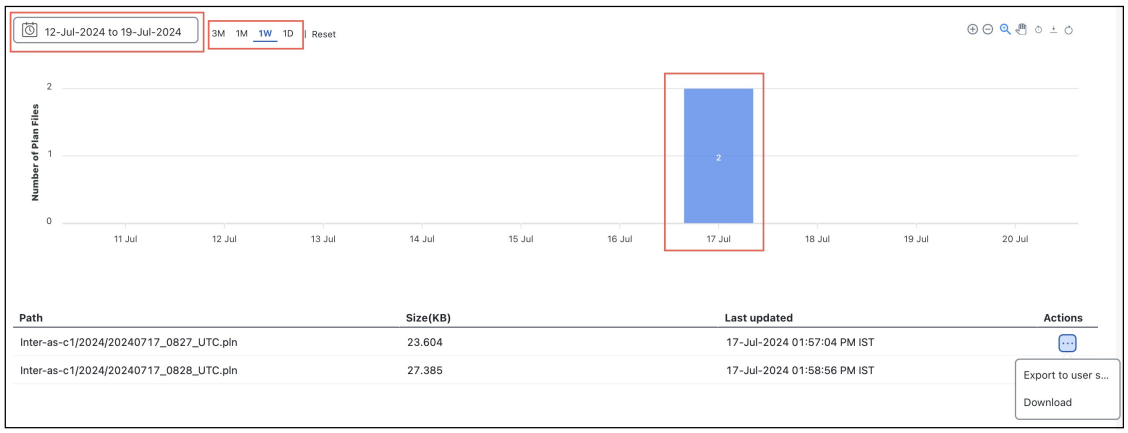
- Make sure that the network model has been archived. For details, see Configure archive, on page 43.

Procedure

Step 1 From the main menu, choose **Network Models**.

Step 2 On the left pane, under **Local archive**, a list of archived collections are displayed. Select the required collection name from the list. The right panel displays the list of plan files created under this collection at various scheduled times. The **Last updated** column displays the time at which the plan file was created.

Figure 22: Archived plan files



You can filter the plan files in several ways:

- Use the date range selection field at the top to select the required start and end dates. The plan files generated during the selected date range is displayed at the bottom.
- Use the links next to the date range selection field to view the plan files generated during last three months (3M), last one month (1M), last one week (1W), or last day (1D).
- Click the bars in the graph to view the plan files generated during a specific date or time. Continue clicking the relevant bar segment to drill down to the exact timestamp.

Step 3 Select the required plan file from the right panel and click ••• > **Export to user space** under the **Actions** column.

The Export plan to User Space window appears.

Note

To download the plan file to your local machine, click ••• > **Download** under the **Actions** column.

Step 4 (Optional) In the **Save as** field, enter a new name for the plan file.

Step 5 (Optional) Select the required tags from the list (if available) or create new tags.

To create new tags, click **Add new tag**, enter the tag name, and then click the + icon next to the field.

Step 6 Click **Save**.

The plan file is imported into the **User space** > **My network models** page.

Step 7 In the **User space** > **My network models** page, click the name of the file to visualize the network model in the **Network Design** page. For more information, see *Cisco Crosswork Planning Design 7.1 User Guide*.

Scenario 2: When the Cisco Crosswork Planning Design and Collector applications are installed on different machines

If the Cisco Crosswork Planning Design and Collector applications are installed on different machines, the archived network models appear under **Network Models** > **Remote archive** of the Cisco Crosswork Planning Design application.

This high-level workflow describes how to access the network models from the external collector.

Step	Action
1. Make sure that the network model has been archived in the machine where the Cisco Crosswork Planning Collector application is installed.	See Configure archive, on page 43.
2. Connect to the machine where Cisco Crosswork Planning Collector application is installed (external collector).	See Connect to the external collector, on page 46.
3. Access the network models from the Remote archive.	See View or download plan files from remote archive, on page 47.

Connect to the external collector

This topic describes how to connect to the Cisco Crosswork Planning Collector instance (external collector) on a different machine.

Procedure

Step 1 Log in to the machine where the Cisco Crosswork Planning Design application is installed.

Step 2 From the main menu, choose **Administration** > **Settings** > **Design settings** > **External collector collection**.

Step 3 In the **Host name/IP address** field, enter the host name or IP address of the machine where the Cisco Crosswork Planning Collector application is installed (external collector).

Step 4 Enter the port, username, and password for the external collector machine.

Step 5 Click **Save**.

Step 6 From the main menu, choose **Network Models** and verify that the **Remote archive** option appears in the left pane.

The Cisco Crosswork Planning Design application is now connected to the external collector.

What to do next

View or download the archived network models from the Remote archive. For details, see View or download plan files from remote archive, on page 47.

View or download plan files from remote archive

Follow these steps to view or download the plan files from the Remote archive.

Procedure

Step 1 Log in to the machine where the Cisco Crosswork Planning Design application is installed.

Step 2 From the main menu, choose **Network Models**.

Step 3 On the left pane, under **Remote archive**, list of collections archived in the external collector are displayed. Select the required collection name from the list. The right panel displays the list of plan files created under this collection at various scheduled times. Use the **Last updated** column to know the time at which the plan file was created.

You can filter the plan files in several ways (see Figure 22: Archived plan files, on page 45):

- Use the date range selection field at the top to select the required start and end dates. The plan files generated during the selected date range is displayed at the bottom.
- Use the links next to the date range selection field to view the plan files generated during last three months (3M), last one month (1M), last one week (1W), or last day (1D).
- Click the bars in the graph to view the plan files generated during a specific date or time. Continue clicking the relevant bar segment to drill down to the exact timestamp.

Step 4 Select the required plan file from the right panel and click ••• > **Export to user space** under the **Actions** column.

The Export Plan to User Space window appears.

Note
To download the plan file to your local machine, click ••• > **Download** under the **Actions** column.

Step 5 (Optional) In the **Save as** field, enter a new name for the plan file.

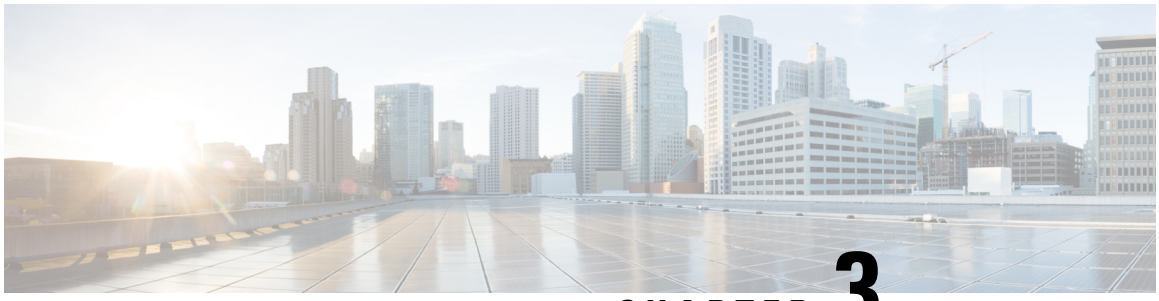
Step 6 (Optional) Select the required tags from the list (if available) or create new tags.

To create new tags, click **Add new tag**, enter the tag name, and then click the + icon next to the field.

Step 7 Click **Save**.

The plan file is imported into the **User space** > **My network models** page.

Step 8 In the **User space** > **My network models** page, click the name of the file to visualize the network model in the **Network Design** page. For more information, see *Cisco Crosswork Planning Design 7.1 User Guide*.



CHAPTER 3

Supported Collectors and Tools

This section contains the following topics:

- Collector descriptions, on page 49
- Collect basic topology information, on page 51
- Collect LSP information, on page 57
- Collect PCEP LSP information using SR-PCE, on page 58
- Collect multicast flow data from a network, on page 60
- Discover BGP peers, on page 62
- Discover VPN topology, on page 65
- Collect hardware inventory information, on page 66
- Collect port, LSP, SRLG, and VPN information using configuration parsing, on page 73
- Collect Circuit Style RSVP-TE information, on page 76
- Configure the Layout collector for improved network model visualization, on page 77
- Collect traffic statistics, on page 78
- Collect traffic demands information, on page 83
- NetFlow data collection, on page 84
- Run an external script against a network model, on page 87
- How data is collected from third-party devices, on page 90
- Merge AS plan files, on page 92

Collector descriptions

Each collector in Cisco Crosswork Planning has capabilities that determine what it collects or deploys.

This table summarizes the collectors and their functions.

Table 5: Collector descriptions

Collector	Description	Prerequisites and notes	Configuration steps
Basic Topology Collection			
IGP database	Discovers IGP topology using login and SNMP.	This is a basic topology collection. The resulting network model is used as the source network for other collectors.	See Collect topology information using the IGP database collector, on page 52

Collector	Description	Prerequisites and notes	Configuration steps
SR-PCE	• Discovers Layer 3 topology using SR-PCE. • Uses raw SR-PCE data as the source for the topology. • Discovers node, interface, and port properties using SNMP.	• Configure SR-PCE agents before running this collection. For details, see Configure agents, on page 26. • This is a basic topology collection for networks using SR-PCE. The resulting network model is used as the source network for other collectors.	See Collect topology information using the SR-PCE collector, on page 53
Advanced Modeling Collection			
LSP	Discovers LSP information using SNMP.	• A network model with basic topology collection must exist. • If using SR-PCE, collect the topology information using the SR-PCE collector, before running this collection. For details, see Collect topology information using the SR-PCE collector, on page 53.	See Collect LSP information, on page 57
PCEP LSP	Discovers PCEP LSPs using SR-PCE. **Note** This collector is accessible only when SR-PCE collector is selected as the basic topology collector.	Collect the topology information using the SR-PCE collector before running this collection. For details, see Collect topology information using the SR-PCE collector, on page 53.	See Collect PCEP LSP information using SR-PCE, on page 58
BGP	Discovers BGP peering using login and SNMP.	A network model with basic topology collection must exist.	See Discover BGP peers, on page 62
VPN	Discovers Layer 2 and Layer 3 VPN topology.	A network model with basic topology collection must exist.	See Discover VPN topology, on page 65
Config parsing	Discovers and parses information from router configurations in the network.	A network model with basic topology collection must exist.	See Collect port, LSP, SRLG, and VPN information using configuration parsing, on page 73
Traffic and Demands Collection			
Inventory	Collects hardware inventory information.	A network model with basic topology collection must exist.	See Collect hardware inventory information, on page 66
Multicast	Collects multicast flow data from a given network.	A network model with basic topology collection must exist.	See Collect multicast flow data from a network, on page 60

Collector	Description	Prerequisites and notes	Configuration steps
Layout	Adds layout properties to a source model to improve visualization.	• An aggregated network model. • After you configure the Layout collector, import a plan file containing layout properties into the Layout model.	See Configure the Layout collector for improved network model visualization, on page 77
Traffic collection	Collects traffic statistics (interface traffic, LSP traffic, MAC traffic, and VPN traffic) using SNMP polling.	• A network model with basic topology collection must exist. • If collecting LSP traffic, a network model with LSP collection must exist. See Collect LSP information, on page 57. • If collecting VPN traffic, a network model with VPN collection must exist. See Discover VPN topology, on page 65.	See Collect traffic statistics, on page 78
Demand deduction	Collects information regarding traffic demands from the network.	Source DARE network containing traffic data must exist.	See Collect traffic demands information, on page 83
NetFlow	Collects and aggregates exported NetFlow and related flow measurements.	A network model with basic topology collection must exist.	See Configure the NetFlow collection, on page 85
Custom Scripts			
External script	Runs customized scripts to append additional data to a source network model.	A source network model and a custom script must exist.	See Run an external script against a network model, on page 87

Collect basic topology information

The network model resulting from basic topology collectors is used as the source network for additional data collections. There are two collectors in Cisco Crosswork Planning which are used for this purpose, **IGP database** and **SR-PCE**. You can select only one collector per collection to gather topology information. You cannot select both collectors at the same time.

For detailed information on how to configure these collectors to collect the topology information, see Collect topology information using the IGP database collector, on page 52 and Collect topology information using the SR-PCE collector, on page 53.

Collect topology information using the IGP database collector

This topic describes how to configure the **IGP database** collector to discover complete network topology using IGP database.

The **IGP database** collector discovers network topology by leveraging the IGP database for node properties and SNMP for interface and port discovery. It is typically the first collector you configure because it provides the foundational network data required by other collectors. It supports multiple OSPF and IS-IS instances. All links collected from routers will have an associated IGP process ID. The resulting network model is used as the source network for additional collections, because it provides the core node, circuit, and interface information used by other collectors.

Follow these steps to collect topology information using the IGP database collector.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- Ensure you have network credentials and access for routers to be used as seed routers.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 In the **Basic topology** section, select **IGP database** and click **Next**.

Step 3 On the Configure page, under **Seed router**, enter these configuration parameters:

- **Index**: Enter a unique index number for the seed router.
- **Router IP**: Enter the management IP address for the seed router.
- **Protocol type**: Select the IGP protocol running on the network. The options are: ospf, ospfv3, isis, and isisv6.

If you select ...	Then ...
ospf or **ospfv3**	Enter the value for **OSPF area** on the **Advanced** page (click ⚙). The OSPF area option specifies the area ID or all. The default is area 0.
isis or **isisv6**	Enter the value for **ISIS level** (1, 2, or BOTH) on the **Advanced** page (click ⚙). The default is level 2.

- **Collect interfaces**: Ensure this box this checked to discover the full network topology. This option is enabled by default.

Step 4 (Optional) To add more seed routers, click **+ Add router** and repeat Step 3 for each seed router. Assign a unique index number to every seed router.

Step 5 (Optional) To include or exclude specific QoS node information, expand **Advanced settings** > **QoS Node Filter**, then click **+ Add node filter** and enter the required values.

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see IGP and SR-PCE collection advanced options, on page 55.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The IGP database collector begins the topology discovery process, building a network model using the specified seed routers and advanced configuration options.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Collect topology information using the SR-PCE collector

This topic describes how to configure the **SR-PCE** collector to collect Layer 3 topology information using SR-PCE.

An SR-PCE agent is a Cisco Crosswork Planning component that connects to the SR-PCE server and processes the telemetry data sent by the server. It uses two different REST connections with SR-PCE: one for LSP data collection and another for topology data collection. After collecting topology and LSP data, the SR-PCE agent can optionally subscribe to SR-PCE and listen to further network change events.

Node and interface/port properties are discovered using SNMP. For testing, you can also use the SR-PCE topology discovery using SR-PCE only (the Extended discovery field disabled) when SNMP access is unavailable. The network model resulting from topology discovery is used as the source network for additional collections because it provides the core node, circuit, and interface information used by other collectors.

The SR-PCE collector captures network updates for any changes in IGP Metric, Delay, and Node Overload. It populates the FlexAlgoAffinities, FlexAlgorithms, SRv6NodeSIDs, SRv6InterfaceSIDs, NodePrefixLoopbacks, and NodeSIDPrefixLoopbacks tables. It does not populate the SRv6NodeSIDPrefixLoopbacks table because the loopback address associated with SRv6 is not obtained using SR-PCE. To populate the SRv6NodeSIDPrefixLoopbacks details, add an external script while configuring the collector. Otherwise, the cross-table filter from SRv6NodeSIDs to NodePrefixLoopbacks will not display any results in the Cisco Crosswork Planning Design application. For details on running the external scripts, see Run an external script against a network model, on page 87.

The SR-PCE collector reads the LocalDomainIdentifier column of NetIntXtcLinks and populates the IGP Process ID in the Interfaces table.

Important notes on SR-PCE topology collection

- The default ISIS level is set to level 2 for NodePrefixLoopbacks. The same value is also populated for an OSPF network.
- Cisco Crosswork Planning does not reflect changes from a non-null value to a null value in the FlexAlgo columns. The updated values start reflecting after a DARE re-sync.
- Dual stack support (ability to handle both IPv4 and IPv6 simultaneously) and the configuration of OSPF or ISIS on an interface are populated correctly during data collection. However, when the dual protocol

(OSPF and ISIS) is enabled on a single interface for data collection, dual stack and its interface resolution are not supported during SR-PCE collection.

- The IPv4 metric value is populated in IGP metric table and the IPv6 value is populated in IPv6-IGP metric table. The TE metric values will also be updated similarly.

Follow these steps to configure the SR-PCE collector.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- Ensure an SR-PCE agent is configured and running. For details on agent setup, see Configure agents, on page 26.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 In the **Basic topology** section, select **SR-PCE** and click **Next**.

Step 3 On the Configure page, enter these configuration parameters:

- **SR-PCE host**: Select an SR-PCE agent.
- **Backup SR-PCE host**: Select a backup SR-PCE agent. If you do not have a backup, leave this field empty. Ensure you do not use the same SR-PCE agent as both the **SR-PCE host** and the **Backup SR-PCE host**.
- **ASN**: Enter 0 to collect information from all autonomous systems in the network, or enter the autonomous system number (ASN) to collect information only from a particular ASN. For example, if the SR-PCE agent has visibility to ASN 64010 and ASN 64020, enter 64020 to collect information only from ASN 64020.
- **IGP protocol**: Select the IGP protocol that is running on the network.
- **Extend discovery**: Check the **Enabled** check box to discover the full network topology (nodes and interfaces).
- **Reactive network**: Check the **Enabled** check box to subscribe to notifications from SR-PCE to update the addition or deletion of nodes or links.
- **Trigger collection**: Check the **Enabled** check box to collect topology collection on new topology additions (nodes or links).

Step 4 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see IGP and SR-PCE collection advanced options, on page 55.

Step 5 Click **Next**.

Step 6 Preview the configuration and then click **Create** to create the collection.

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The SR-PCE collector initiates topology discovery, gathers Layer 3 topology information, and updates the network model with the collected data.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

IGP and SR-PCE collection advanced options

You can configure several advanced options when using the IGP database and SR-PCE collectors.

Table 6: IGP and SR-PCE collection advanced options

Option	Description
Options applicable for both IGP and SR-PCE collection:	
Nodes	
Node performance collection	Collects node performance data if enabled.
Remove node suffix	Removes node suffixes from node names if the node contains the specified suffix. For example, 'company.net' removes the domain name for the network.
QoS queues	Allows interfaces (configured with QoS in the router) to display QoS information.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
QoS node filter	Defines a filter to determine the nodes for which the QoS data is collected.
Interfaces	
Find parallel links	Finds parallel links that are not in the IGP database when IS-IS TE extensions are not enabled.
IP guessing	Indicates the level of IP address guessing to perform for interfaces that are not present in the topology database. This setting is used when IS-IS TE extensions are not enabled. • OFF: Performs no guessing. • Safe: Makes guesses only when there is no ambiguity. • FULL: Makes best-guess decisions when there is ambiguity.
Port LAG discovery	Enables LAG discovery of port members.

Option	Description
LAG port match	Determines how to match local and remote ports in port circuits. • Guess: Creates port circuits to match as many ports as possible. • Exact: Matches based on LACP. • Complete: Matches based on LACP first, and then tries to match as many as possible. • None: Does not create port circuits.
Cleanup circuits	Removes circuits that do not have IP addresses associated with interfaces. Circuit removal is sometimes required when there are IS-IS advertising inconsistencies in the IS-IS database.
Copy description	Copies physical interface descriptions to logical interfaces if there is only one logical interface and its description is blank.
Physical ports	Collects L3 physical ports for Cisco devices.
Minimum IP guessing	Specifies the minimum prefix length for IP guessing. All interfaces with equal or larger prefix lengths are considered.
Minimum prefix length	Specifies the minimum prefix length allowed when finding parallel links. All interfaces with equal or larger prefix lengths (but less than 32) are considered.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.
Option applicable only for SR-PCE collection:	
Single-ended eBGP discovery	Discovers eBGP links that have only a single link end. This scenario is not common.

Collect LSP information

This topic describes how to configure the **LSP** collector to collect the RSVP LSP information in the network using SNMP.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Advanced modeling** section, select **LSP** and click **Next**.

Step 4 On the Configure page, click **LSP** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.
- **Get FRR LSPs**: Check the **Enabled** check box to discover MPLS Fast Reroute (FRR) LSP (backup and bypass) information.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see LSP collection advanced options, on page 57.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The LSP collector is set up and scheduled according to your configuration.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

LSP collection advanced options

You can configure several advanced options when using the LSP collector.

Table 7: LSP collection advanced options

Option	Description
Use calculated hops	Uses the calculated path hops table instead of the actual path hops table when discovering path hops.
Find actual path	Discovers actual paths for LSPs.
Get extras	Collects additional LSP properties.
Use signaled name	Uses the LSP tunnel signaled name instead of the LSP tunnel name (IOS-XR). **Note** To retrieve the signaled name when using Config parsing with the LSP collector, ensure the LSP collector executes before the Config parsing collector. If you do not follow this order, the LSP tunnel name collected by Config parsing will overwrite the signaled name value collected by the LSP collector.
Auto bandwidth	Discovers auto bandwidth.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Collect PCEP LSP information using SR-PCE

This topic describes how to configure the **PCEP LSP** collector.

The PCEP LSP collector uses the data collected from the SR-PCE collector and appends LSP information, allowing you to generate a new and enhanced network model.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.

- Complete the BGP-LS topology collection for your network using the SR-PCE collector. You need to use this model as the source network for collecting LSP information. For more information, see Collect topology information using the SR-PCE collector, on page 53.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 In the **Basic topology** section, select **SR-PCE**.

Step 3 In the **Advanced modeling** section, select **PCEP LSP** and click **Next**.

Step 4 On the Configure page, click **PCEP LSP** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.
- **Agents**: Select the SR-PCE agents from the drop-down list. For information on creating agents, see Configure agents, on page 26.

  Note
  When using multiple SR-PCE agents, note that each additional agent may increase the overall execution time, depending on the data volume the collector has to process for each agent. Consider this aspect to ensure optimal performance when selecting multiple agents.

- **Reactive network**: Check the **Enabled** check box to subscribe to notifications from SR-PCE for real-time LSP updates. This option is enabled by default.

Step 6 (Optional) Expand the **Advanced settings** panel and enter these information:

- **RSVP use signaled name**: Check the **Enabled** check box to use the RSVP LSP tunnel signaled-name instead of LSP tunnel name (IOS-XR).
- **SR use signaled name**: Check the **Enabled** check box to use the SR LSP tunnel signaled-name instead of LSP tunnel name (IOS-XR).
- **SR add index**: Check the **Enabled** check box to add indexes to SR LSP tunnels from associated interfaces (IOS-XR).
- **Data collection timeout**: Set the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

PCEP LSP information is collected and appended to the existing SR-PCE topology, generating an updated network model that includes detailed LSP data.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Collect multicast flow data from a network

This topic describes how to configure the **Multicast** collector to collect multicast flow data from your network.

The Multicast collector includes these collectors:

- Login find multicast: Logs in to the router to fetch or parse multicast flow data.
- Login poll multicast: Logs in to the router to get multicast traffic rate.
- SNMP find multicast: Collects multicast flow information using SNMP.
- SNMP poll multicast: Collects traffic rate data for multicast flows using SNMP.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Traffic and Demands** section, select **Multicast** and click **Next**.

Step 4 On the Configure page, click **Multicast** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.
- **Data collection source**: Select the collector you want to use to collect the multicast data. The options are Login find multicast, Login poll multicast, SNMP find multicast, and SNMP poll multicast.

Step 6 (Optional) Expand the ***Collector* settings** panel and enter the details in the relevant fields. Depending on the collectors you selected in the previous step, the options differ. For descriptions of these advanced options, see Multicast collection advanced options, on page 61.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The Multicast collector is configured and begins collecting multicast flow data from your network as specified.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Multicast collection advanced options

You can configure several advanced options when using the Multicast collectors.

Table 8: Multicast collection advanced options

Option	Description
Login find settings	
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 30 minutes.
Use existing config	Uses existing multicast configuration data stored in the cache.
Force config update	Updates multicast configuration files even if they exist in the cache.
Save configs	Saves multicast configurations in the cache or discards them if not selected.
Overwrite files	Overwrites existing configuration files.
Login poll settings	
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 30 minutes.
No of samples	Sets the number of data samples to collect during polling.
Polling interval	Sets the interval, in seconds, between the login rate readings.
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Defines the filtering criteria for multicast traffic from multiple sources for each S|G group.
Use existing config	Uses existing multicast configuration data stored in the cache.
Force config update	Updates multicast configuration files even if they exist in the cache.
Save configs	Saves multicast configurations in the cache or discards them if not selected.

Option	Description
Overwrite files	Overwrites existing configuration files.
SNMP find settings	
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 30 minutes.
SNMP poll settings	
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 30 minutes.
No of samples	Sets the number of data samples to collect during polling.
Polling interval	Sets the interval, in seconds, between the login rate readings.
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Defines the filtering criteria for multicast traffic from multiple sources for each S|G group.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Discover BGP peers

This topic describes how to configure the **BGP** collector to discover BGP topology using SNMP and login.

The BGP collector uses a topology network, typically an IGP topology collector output, as its source network and adds BGP links to external ASN nodes.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Advanced modeling** section, select **BGP** and click **Next**.

Step 4 On the Configure page, click **BGP** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 From the **Source** drop-down list, select the source collector whose output serves as the input for this collector.

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see BGP topology advanced options, on page 63.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The BGP collector is now configured and able to discover BGP topology using SNMP and login.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

BGP topology advanced options

You can configure several advanced options when using the BGP collector.

Table 9: BGP topology collection advanced options

Option	Description
ASN include	Specifies ASNs to include. By default, includes all ASNs.
Internal ASNs	Specifies internal ASNs.
Protocol	Specifies the Internet Protocol (IP) versions. The options are IPv4 and IPv6.
Min IPv4 prefix length	Specifies the minimum IPv4 prefix length to control how strictly subnet matching occurs when discovering interfaces as BGP links.
Min IPv6 prefix length	Specifies the minimum IPv6 prefix length to control how strictly subnet matching occurs when discovering interfaces as BGP links.
Login multi hop	Specifies whether to log in to routers that potentially contain multi-hop peers.

Option	Description
Force login platform	Overrides platform detection and uses the specified platform. Valid values are cisco, juniper, alu, huawei.
Fallback login platform	Sets the fallback vendor if platform detection fails. Valid values are cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router. This grants higher-level access required to retrieve or modify configuration on devices that require a secondary “enable password”
Telnet username prompt	Specifies an alternative username prompt for Telnet.
Telnet password prompt	Specifies an alternative password prompt for Telnet.
Find internal ASN links	Finds links between two or more internal ASNs. Normally, this action is not required because IGP discovers these links.
Find non IP exit interface	Searches for exit interfaces that are not represented as next-hop IP addresses, but rather as interfaces (which are rare). **Note** This action increases the amount of SNMP requests for BGP discovery, which affects performance.
Internal exit interface	Discovers BGP links to internal ASNs.
Get MAC address	Collects source MAC addresses of BGP peers connected to an Internet Exchange public peering switch. This action is required only for MAC accounting.
Use DNS	Indicates whether to use DNS to resolve BGP IP addresses.
Force check all	Indicates whether to check all routers even if there is no indication of potential multi-hop peers. This action could be slow.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.

Option	Description
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.
Login record mode	Records the discovery process. The options are Off, Record, and Playback. The default is Off. • Record: The messages to and from the live network are recorded internally as the tool runs. It is used for debugging. • Playback: The recorded messages are played back through the tool as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Discover VPN topology

This topic describes how to configure the **VPN** collector to discover Layer 2 and Layer 3 VPN topology.

Note Currently, only P2P-VPWS xconnect discovery is supported for Layer 2 VPNs.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Advanced modeling** section, select **VPN** and click **Next**.

Step 4 On the Configure page, click **VPN** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.
- **VPN type**: Select at least one VPN type.
  - **VPWS**: Select this type when Virtual Private Wire Service (VPWS) is being used in the network.
  - **L3VPN**: Select this type when Layer 3 VPN is being used in the network.

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed:

Table 10: VPN collection advanced options

Option	Description
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The VPN collector is now configured.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Collect hardware inventory information

The Inventory collector collects hardware inventory information.

Collected Hardware

The **Inventory** collector creates a series of NetIntHardware* tables that store the collected hardware information based on hardware type. Each of the following objects are defined by node IP address and SNMP ID.

- NetIntHardwareChassis—Router chassis objects identified by node IP address and SNMP ID.
- NetIntHardwareContainer—Each entry represents a slot in a router (anything that can have a field replaceable unit (FRU) type device installed into it). Examples include chassis slots, module slots, and port slots.
- NetIntHardwareModule—Hardware devices that can be installed into other hardware devices. Generally, these devices directly support traffic such as line cards, modules, and route processors, and do not fall into one of the other function-specific hardware tables.
- NetIntHardwarePort—Physical ports on the router.

Hardware Hierarchy

The hardware has a parent-child relationship based on where the object resides within the router. The chassis has no parent and is considered as the *root object*. Other than the chassis, each object has one parent and can have one or more child objects. Objects with no children are called *leaf objects*, such as ports and empty containers. This hierarchy generally reflects how hardware objects are installed within other objects. For example, a module representing a line card might have a parent object that is a container representing a slot.

The parent is identifiable in the NetIntHardware* tables by the ParentTable and ParentId columns. Using these two columns along with the Node (node IP address) column, you can find the parent object for any hardware object.

Example: This NetIntHardwareContainer entry identifies that container 172.23.123.456 has a chassis as a parent. In the NetIntHardwareChassis, there is an SnmpID entry that matches the container's ParentId of 2512347.

Table 11:

NetIntHardwareContainer							
Node	**SnmpID**	**ParentID**	**Model**	**Name**	**NumChildren**	**ParentTable**	**SlotNumber**
172.23.123.456	2503733	2512347		slot mau 0/0/0/5	0	NetIntHardware Chassis	0

Tracing the hierarchy from each leaf object to its corresponding root object based on the parent-child relationships results in a series of object types that form its hardware hierarchy. It is this trace that the Inventory collector uses to determine how to process the hardware devices. This is also the process you must use if adding an entry to the HWInventoryTemplates table.

Example: Chassis-Container-Module-Module-Container-Port

Tables for Processing Inventory

The Inventory collector constructs the NetIntNodeInventory table by processing the NetIntHardware* tables. The collector requires two configuration files and can additionally use an optional one.

- Template file (required)—This file contains these tables.
  - HWInventoryTemplates—Contains entries that categorize the devices in the final NetIntNodeInventory table, as well as prune from inclusion.

- HWNameFormatRules—Contains entries that format the hardware object names to make them more usable, as well as correct unexpected SNMP results.

- Exclude file (required)—Contains the ExcludeHWList table that prevents (blocked lists) hardware objects from being included in the final NetIntNodeInventory table. This can be useful when for excluding hardware that does not forward or carry traffic.
- Hardware spec file (optional)—Contains the HardwareSpec table that can be used to adjust collected data in terms of the number of slots in a specified device when the slots returned by SNMP is inaccurate.

If you modify the template or choose to exclude files, ensure these changes persist across software upgrades.

Configure Hardware Templates

The **Template file** option under the **Build inventory options** section calls a file containing both the HWInventoryTemplates and the HWNameFormatRules tables.

HWInventoryTemplates Table

The HWInventoryTemplates table tells the Inventory collector how to interpret hardware referenced by the NetIntHardware* tables. It enables the Inventory collector to categorize objects into common, vendor-neutral hardware types, such as chassis, linecards, and slots, as well as to remove hardware types that are not of interest.

Inventory hardware is categorized as a chassis, slot, line card, module slot, module, port slot, port, or transceiver. A container is categorized as either a slot, module slot, or port slot. A module is categorized as either a module or a line card. All other hardware objects are categorized by their same name. For instance, a chassis is categorized as a chassis.

The Inventory collector looks at the following columns of the HWInventoryTemplates table for matches in the NetIntHardware* tables in this order.

- DiscoveredHWHierarchy, Vendor, Model
- DiscoveredHWHierarchy, Vendor, * (where * means all entries in the Model column)

You can further enhance the search using the **Guess template** option. In this instance, if no matches are found using the first two criteria, Cisco Crosswork Planning collector then looks for matches only for DiscoveredHWHierarchy and Vendor, and does not consider Model.

If a match is found, the subsequent columns after DiscoveredHWHierarchy tell the Inventory collector how to categorize the hardware. These latter columns identify hardware object types: chassis, slot, line card, module slot, module, port slot, port, or transceiver. Each column entry has the *Type,Identifier,Name* format.

- Type is the discovered hardware type, such as “container.”
- Identifier specifies which object (of one or more of the same type) in the hierarchy is referenced (0, 1, ...).
- Name specifies a column heading in the NetIntHardware* table. This is the name that appears in for that object in the NetIntNodeInventory table.

Example: Module,0,Model. "Model" is a column heading in the NetIntHardwareModule table)

Multiple name source columns can be specified with a colon.

Example: Container,0,Model:Name

If a hardware category does not exist or is empty, the Inventory collector does not include it in the final NetIntNodeInventory table.

Example:

Using the first row of the default Template file, the Cisco Crosswork Planning collector searches the NetIntHardware* tables for ones that have entries that match the Vendor, Model, and DiscoveredHWHierarchy columns as Cisco ASR9K Chassis-Container-Module-Port-Container-Module.

Thereafter, it categorizes each entry in the hardware hierarchy (DiscoveredHWHierarchy column), and defines its location in the hardware types columns.

The first Module entry is defined as a line card, it is identified as #0, and the name that appears in the NetIntNodeInventory table is the one appearing in the Model column of the NetIntHardwareModule table. The second module is defined as a transceiver object and is identified as #1. It uses the same name format.

Notice that there are two containers in the hierarchy, but there is only one defined as a Type. This means that the second container would not appear in the NetIntNodeInventory table.

Add HWInventoryTemplates Entries

If the Cisco Crosswork Planning collector encounters an inventory device that is not in the HWInventoryTemplates table, it generates a warning that specifies pieces of the hardware hierarchy, including the SNMP ID of the leaf object and the IP address of the router. You can use this information to manually trace the objects from the leaf to the root and derive an appropriate entry in the HWInventoryTemplates table. For information on tracing hardware hierarchies, see Hardware Hierarchy.

1. Copy the warning message for reference, and use it for Step 2.
2. Using the router's IP address, as well as the SNMP ID, name, and model of the leaf object, find the leaf object referenced in the warning in either the NetIntHardwarePort or the NetIntHardwareContainer table.
3. Use the leaf object's ParentTable and ParentId columns to trace the leaf back to its parent. For each successive parent, use its ParentTable and ParentId columns until you reach the root object (chassis) in the NetIntHardwareChassis table.
4. Once each object in the hardware hierarchy is found, add it to the DiscoveredHWHierarchy column of the HWInventoryTemplates table. Complete the Vendor and Model columns.
5. For each object in the hardware hierarchy (DiscoveredHWHierarchy column), classify it into one of the standard hardware types, which are the columns listed after the DiscoveredHWHierarchy column.

HWNameFormatRules Table

The HWNameFormatRules table specifies how to format the names in the NetIntNodeInventory table. This is useful for converting long or meaningless names to ones that are easier to read and clearer for users to understand.

For each entry in the HWInventoryTemplates table, the HWNameFormatRules table is searched for a matching vendor, hardware type (HWType), name (PatternMatchExpression). Then, rather than using the name specified in the HWInventoryTemplates table, the NetIntNodeInventory table is updated with the name identified in the ReplacementExpression column.

If multiple matches apply, the first match found is used. Both the PatternMatchExpression and the ReplacementExpression can be defined as a literal string in single quotes or as a regular expression.

Example:

HWNameFormatRules			
Vendor	**HWType**	**PatternMatchExpression**	**ReplacementExpression**
Cisco	Chassis	\A4\Z	‘7507’
Cisco	Linecard	800-20017-.*	‘1X10GE-LR-SC’
Juniper	Chassis	Juniper (MX960) Internet Backbone Router	$1

The entries in the table work as follows:

- Replaces all Cisco chassis name with 7507 if the name has four characters where A is the beginning of the string and Z is the end of the string.
- Replaces all Cisco linecard names that match 800-20017-.* with 1X10GE-LR-SC.
- Replaces all Juniper chassis named “Juniper (MX960) Internet Backbone Router” with MX960.

Note SNMP returns many slot names as text, rather than integers. It is a best practice to remove all text from slot numbers for optimal use.

Exclude Hardware by Model or Name

The **Exclude file** option under the **Build inventory options** section option calls a file containing the ExcludeHWList table. This table enables you to identify hardware objects to exclude from the NetIntNodeInventory table based on model, name, or both. This is useful, for instance, when excluding management ports and route processors. The model and names can be specified using regular expressions or they can be literals.

Example:

ExcludeHWList			
HWTable	**Vendor**	**Model**	**Name**
NetIntHardwarePort	Cisco		\/CPU0\/129$
NetIntHardwareModule	Cisco	800-12308-02	
NetIntHardwarePort	Cisco		Mgmt

The entries in the table work as follows:

- Exclude all objects in the NetIntHardwarePort table where the vendor is Cisco and the name ends with CPU0/129.
- Exclude all objects in the NetIntHardwareModule table where the vendor is Cisco and the model is 800-12308-02.
- Exclude all objects in the NetIntHardwarePort table where the vendor is Cisco and the name is Mgmt.

HardwareSpec

The **Hardware spec file** option under the **Build inventory options** section calls a file containing the HardwareSpec table. This table enables you to adjust data returned from SNMP. You can adjust both the total number of slots (TotSlot) and the slot numbering range (SlotNum). For instance, SNMP might return 7 slots for a chassis when there are actually 9, including route processors.

This table looks only for hardware that contains slots, module slots, or port slots, and thus, the hardware type (HWType column) must be chassis, line card, or module. SlotNum indicates the slot number range. For instance, some routers start with slot 0, whereas others start with slot 1.

Example:

HardwareSpec				
Vendor	**HWType**	**Model**	**TotSlot**	**SlotNum**
Cisco	Chassis	7609	9	1-9

This table entry sets the Cisco 7609 chassis to have a total of 9 slots and to start the slot numbering with 9.

Configure inventory collection

This topic describes how to configure the **Inventory** collector.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Traffic and Demands** section, select **Inventory** and click **Next**.

Step 4 On the Configure page, click **Inventory** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 From the **Source** drop-down list, select the source collector whose output serves as the input for this collector.

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see Inventory collection advanced options, on page 72.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The Inventory collector is now configured according to your settings.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Inventory collection advanced options

You can configure several advanced options when using the Inventory collector.

Table 12: Inventory collection advanced options

Option	Description
Get inventory options	
Login allowed	Allows logging in to the router to collect inventory data.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 30 minutes.
Build inventory options	
Exclude file	Allows you to select the file that contains the ExcludeHWList table. This table defines hardware characteristics to match against for exclusion in the output. Click the **Download sample file** link to download a sample file that contains the ExcludeHWList table.
Guess template	Broadens the search when processing raw inventory data.
Template file	Allows you to select the hardware template file that contains the HWInventory Templates and HWNameFormatRules tables. Click the **Download sample file** link to download a sample template file.
Hardware spec file	Allows you to select the file that contains the HardwareSpec table. This table defines slot counts for specific types of hardware to verify SNMP data returned from routers. Click the **Download sample file** link to download a sample file that contains the HardwareSpec table.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.

Option	Description
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Collect port, LSP, SRLG, and VPN information using configuration parsing

This topic describes how to configure the **Config parsing** collector to collect port, LSP, SRLG, and VPN information.

Note The **Config parsing** collector is not a base topology collector. Use it only to augment details that are missing from other methods of collection, such as SNMP and SR-PCE.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Advanced modeling** section, select **Config parsing** and click **Next**.

Step 4 On the Configure page, click **Config parsing** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 From the **Source** drop-down list, select the source collector whose output serves as the input for this collector.

Step 6 Expand the **Get config** and **Parse config** panels. Enter the details in the relevant fields. For field descriptions, see Configuration parsing advanced options, on page 74.

Note
- L2VPN config parse is not supported.

- When L3VPN information is collected by the Config Parsing collector, all VPNs are assumed to be connected to each other.
- If both the Config Parsing collector and the VPN collector are collecting VPN information, ensure that the VPN collector runs before the Config Parsing collector in the collector chain.
- Single-ended SRLGs with a missing end are collected via SR-PCE. The SRLGSCircuits table is not updated for these entries.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Configuration parsing advanced options

You can configure several advanced options when using the Config parsing collector.

Table 13: Configuration parsing advanced options

Option	Description
Get config options	
Collect configuration	Retrieves configuration details from devices or routers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values are cisco, juniper, alu, huawei.
Fallback login platform	Sets the fallback vendor in case platform detection fails. Valid values are cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router. This grants higher-level access required to retrieve or modify configuration on devices that require a secondary “enable password”.
Telnet username prompt	Specifies an alternative username prompt for Telnet.
Telnet password prompt	Specifies an alternative password prompt for Telnet.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Parse config options	

Option	Description
Protocol type	Allows you to select the IGP protocol running in the network. The options are isis, ospf, and None. The default is **isis**.
ISIS level	Indicates the ISIS level to use. The agent can read IS-IS Level 1, Level 2, or both. If you select both, the agent combines both levels into a single network and Level 2 metrics take precedence.
OSPF area	Specifies whether to collect a single OSPF area or all areas. This option specifies the area ID or all. The default is area 0.
ASN	Specifies the ASN to collect. ASN is ignored by default. However, for networks that span multiple BGP ASNs, use this option to read information from more than one IGP process ID or instance ID in an ASN.
Include objects	Allows you to select the configuration objects that you want to parse. The available options are LAG, SRLG, RSVP and CS RSVP, VPN, FRR, SR LSPS, LMP, and SR Policies.
Circuit match	Indicates the criteria to use to form circuits.
LAG port match	Controls how to match local and remote ports in port circuits. • Guess: Creates port circuits to match as many ports as possible. • None: Does not create port circuits.
OSPF process ID	Specifies which OSPF process ID to use when there are multiple OSPF processes.
IS-IS instance ID	Specifies which IS-IS instance ID to use when there are multiple IS-IS instances.
Loopback interface	Specifies the loopback interface number to use for the router IP.
Resolve references	Enables resolution of IP address references during parsing.
Multithreading	Enables multithreaded processing of configuration files to speed up parsing.
Filter showcommands	Filters multiple show commands.
Build topology	Constructs network topology after parsing the configuration.
Shared media	Creates pseudonodes for shared media.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.

Option	Description
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Collect Circuit Style RSVP-TE information

This topic describes how to collect Circuit Style RSVP (CS-RSVP) LSP information from network devices.

Circuit Style RSVP (CS-RSVP) LSPs are logical entities that bundle two unidirectional RSVP LSPs with the same endpoints to form bidirectional RSVP LSPs. This allows traffic to consistently travel in both directions between the endpoints.

To collect CS RSVP-TE data, you must configure the **LSP** and **Config parsing** collectors. The Config parsing collector is required to collect the configuration data from each device in the network and parse the CS-RSVP data out of it. After the collection is run successfully, the aggregated plan file includes the CS-RSVP LSP details collected from the devices.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- Ensure that the devices have these configurations:
  - RSVP configuration with **bidirectional** enabled.
  - The **bidirectional** configuration includes the same **association id**, **source-address**, and **global-id** in both directions.
  - The **bidirectional** configuration specifies the **association type** as **co-routed**.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Advanced modeling** section, select the **LSP** and **Config parsing** collectors. Then, click **Next**.

Step 4 Configure both the **LSP** and **Config parsing** collectors. Ensure to select the **RSVP and CS RSVP** option from the **Include objects** drop-down list. This option is available in the **Parse config** section of the **Config parsing** page.

For details on the other LSP and Config parsing options, see Collect LSP information, on page 57 and Collect port, LSP, SRLG, and VPN information using configuration parsing, on page 73.

Note
To retrieve the signaled name, ensure the LSP collector executes before the Config parsing collector. If this order is not followed, LSP tunnel name collected by Config parsing will overwrite the signaled name value collected by the LSP collector.

Step 5 (Optional) Expand the **Advanced settings** panel and configure any other relevant fields. For descriptions of these advanced options, see LSP collection advanced options, on page 57.

Step 6 Click **Next**.

Step 7 Preview the configuration and then click **Create** to create the collection.

Step 8 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The resulting network model includes the CS-RSVP LSP details.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Configure the Layout collector for improved network model visualization

This topic describes how to configure the **Layout** collector.

The **Layout** collector adds layout properties to a source network model. This improves visualization when you import the plan file into Cisco Crosswork Planning. The collector automatically records changes to the layout properties. When the source network model changes, the layout of the destination model is updated.

The layout in the destination network serves as a template that is applied to the source network. The resulting network is saved as the new destination network. If the source layout contains no layout information, the layout from the destination network is added to the source network. If the source network contains layout information, that layout is maintained unless there is a conflict with the layout in the destination network. If a conflict exists, the layout information in the destination network takes precedence over the information in the source network.

Note The Layout collector saves only the node and site mappings. It does not save the node's coordinates.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Traffic and Demands** section, select **Layout** and click **Next**.

Step 4 On the Configure page, click **Layout** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.
- **Template file**: Enter the template plan file path from where the layout details are copied.

  Note
  If you are migrating the collector configuration either from Cisco WAE or from another Cisco Crosswork Planning instance, ensure that the **Template file** field is updated with the correct file after importing the collector configuration. This is necessary because, after importing the configuration, the server restores only the file name and not the actual file. If the field is not updated with the correct file, then the collection fails.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the following information:

- **Timeout**: Enter the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The Layout collector is now configured.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Collect traffic statistics

This topic describes how to configure the **Traffic collection** collector.

The **Traffic collection** collector collects traffic statistics, such as interface traffic, LSP traffic, MAC traffic, and VPN traffic using SNMP polling. After configuring the **Traffic collection** collector, you can view the traffic poller agent details in the **Collector** > **Agents** page. The agent name matches the collection name.

Note During the first traffic collection run, the traffic data is not populated in the plan file due to insufficient data to compute traffic details. Beginning with the second or third run, depending on the schedule duration and the configuration of minimum and maximum window lengths, traffic data begins to populate in the plan file.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- To collect VPN traffic, you must have a VPN network model. For details, see Discover VPN topology, on page 65.
- To collect LSP traffic, you must have an LSP network model. For details, see Collect LSP information, on page 57.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Traffic and Demands** section, select **Traffic collection** and click **Next**.

Step 4 On the Configure page, click **Traffic collection** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

a) Check the **Traffic collection** check box to enable the traffic poller.
b) From the **Source** drop-down list, select the source collector whose output serves as the input for this collector.
c) To run continuous traffic collection for interfaces, enable **Interface traffic poll** and then enter the following:
   - **Polling period**: Enter the polling period in seconds. We recommend starting with 60 seconds.
   - **QoS**: Check the **Enable** check box if you want to enable queues traffic collection.
   - **VPN**: Check the **Enable** check box if you want to enable VPN traffic collection. If enabled, confirm that the source network model has VPNs enabled.

d) To run continuous traffic collection for LSPs, enable **LSP traffic poll** and then enter the following:
   - **Polling period**: Enter the polling period in seconds. We recommend starting with 60 seconds.

   Note
   If **LSP traffic poll** is enabled, make sure that the source network model has all the LSP details.

e) To run continuous traffic collection for MAC accounting, enable **MAC traffic poll** and then enter the following:
   - **Polling period**: Enter the polling period in seconds. We recommend starting with 60 seconds.

   Note
   If **MAC traffic poll** is enabled, make sure that the source network model has MAC addresses.

f) (Optional) Expand the **SNMP traffic computation** panel and enter the details in the relevant fields. For field descriptions, see Traffic collection advanced options, on page 80.

Step 5 Click **Next**.

Step 6 Preview the configuration and then click **Create** to create the collection.

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The traffic details are updated in the plan files only on running the scheduled jobs. If a job is not executed, the traffic data is not updated in the plan files.

Traffic statistics are collected and available in the resulting plan file on execution of the subsequent scheduled jobs.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

Traffic collection advanced options

You can configure several advanced options when using Traffic collection.

Table 14: Traffic collection advanced options

Option	Description
Minimum window length	Specifies the minimum window length for traffic calculation, in seconds. The default is 300 seconds.
Maximum window length	Specifies the maximum window length for traffic calculation, in seconds. The default is 450 seconds.
Raw counter TTL	Determines how long raw counter data is kept, measured in minutes. The default is 15 minutes.
Discard over capacity	Discards traffic rates that are higher than capacity.
Net recorder file max size	Specifies the maximum size for the net record file.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.

Option	Description
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Tuning traffic polling

Traffic poller collects raw traffic counters from the network. Collection time depends on network size, network latency, and response time from individual nodes.

To run traffic polling efficiently, do the following:

1. Set the traffic poller verbosity to 40 in the **Traffic collection** configuration page.
2. Start with the default options and run continuous collection for several hours. The default values are:

```
Interface traffic poll > Polling period = 60
LSP traffic poll > Polling period = 60
Minimum window length = 300
Maximum window length = 450
Raw counter TTL = 15
```

3. Configure the Traffic collection scheduler to run every 300 seconds.
4. Download the `continuous_poller_out.log` file using the showtech option.
   a. From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Health** > **Collector**.
   b. Click the **Microservices** tab.
   c. Click ••• for the **collection-service** and choose **Request logs**.
   d. Download the resulting tar file to view the log file.
5. Search for actual collection times. For example:

```
Info [40]: LSP Traffic Poller: Collection complete. Duration: 43.3 sec
Info [40]: Interface Traffic Poller: Collection complete. Duration: 42.7 sec
```

   The fastest pace at which the poller can poll network in the example above is around 40-50 secs. This is the minimum value for `Interface traffic poll > Polling period` and `LSP traffic poll > Polling period`. Since traffic poller populates traffic for both interfaces and LSPs at the same time, it is recommended to set both values to the same value.

   Traffic Poller calculates traffic by collecting raw traffic counters c1, c2, ..., cn. It requires at least two counters to calculate traffic.

```
(c2.counter - c1.counter)/(c2.timestamp - c1.timestamp)
```

Note the following:

- A sliding window namely `Minimum window length` is used to sample two counters. It looks for two counters which are farthest apart, that is, latest and earliest for a specified period. The average traffic is calculated for this period. Since the poller requires at least two counters, the smallest value for `Minimum window length` is 2 * `polling period`. To accommodate for variations, add 25% or more.

  In case `Minimum window length` fails to find counters for the specified period due to increased network latency or node response time, it will report traffic as `N/A`. To avoid empty traffic, there is an insurance window, namely `Maximum window length` which has a minimum value equal to 2 * `polling period`. To accommodate for longer polling period, add 50% or more. For unresponsive nodes, add 100% or more.

- Traffic poller stores raw counters in memory for traffic calculation. This takes up RAM space. Once in a while traffic poller cleans up old counters stored in memory. Anything older than `Raw counter TTL` (mins) is cleaned up. Therefore, given above constraints, minimum value for `Raw counter TTL` is `Maximum window length` or more.

- Traffic population in traffic poller is the process of calculating traffic in the network and populating the plan file. The duration it takes depends on network size. The actual time it takes to populate traffic can be found in the `snmp-traffic-poller-service.log` file.

  For example:

  ```
  TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 379976
  TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 391953
  TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 388853
  ```

  In the above example, the fastest rate at which traffic can be populated (and consumed by other tools) is about 400 secs.

- Sometimes in the `snmp-traffic-poller-service.log` file, you can also see `Invalid counter` warnings to indicate that counter values do not make sense, for example, `c1.counter` is greater than `c2.counter` (which would result in negative traffic). This happens when counters reset or overflow. It is common for 32-bit counters. If there are a lot of them seen, increase the sliding window sizes to process more counters and reduce chances of failure.

- However, it is not recommended to poll network at a faster rate than populating traffic. In the example above, the most aggressive setting for traffic polling is 50 secs, but population takes around 400 secs. This amounts to 8 network polls which are wasted. Therefore, traffic polling period can be increased (along with sliding window sizes and `Raw counter TTL`).

  Here is the configuration recommended for the above network:

  1. Set the following values:

     ```
     Interface traffic poll > Polling period 180
     LSP traffic poll enabled
     LSP traffic poll > Polling period 180
     Minimum window length 400
     Maximum window length 800
     Raw counter TTL 15
     Data collection timeout 60
     ```

  2. Configure Traffic collection scheduler to run every 400 seconds.

Note Data collection timeout is adjusted to 60 mins for traffic population. This timeout is not used generally and should be just high enough.

Sample configuration above is the most aggressive in terms of traffic polling and population. These numbers can be adjusted to be less aggressive to save CPU resources and network bandwidth. For example:

1. Set the following values:

```
Interface traffic poll > Polling period 240
LSP traffic poll enabled
LSP traffic poll > Polling period 240
Minimum window length 600
Maximum window length 1200
Raw counter TTL 20
Data collection timeout 60
```

2. Configure Traffic collection scheduler to run every 600 seconds.

Collect traffic demands information

This topic describes how to configure the **Demand deduction** collector to collect information about traffic demands from the network.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Traffic and Demands** section, select **Demand deduction** and click **Next**.

Step 4 On the Configure page, click **Demand deduction** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 From the **Source** drop-down list, select the source collector whose output model serves as the input for this collector.

Step 6 Under **Demand mesh steps**, click **+ Add step** to add a step.

On the Add Mesh Step page, enter these details:

a) In the **Name** field, enter the name for the step.
b) In the **Step number** field, enter the execution order for this step.
c) From the **Tool** drop-down list, select the required tool. The available tools include Demands for P2MP LSPs, Demand deduction, External executable script, Copy demands, Demands for LSPs, or Demand mesh creator.
d) Check the **Enable** check box to run the selected tools.

e) Update or enter the details in the **Tool configuration** section. The options differ based on the selected tool.
f) (Optional) Expand the **Advanced** panel and enter the relevant details.
g) Click **Continue**.

Repeat this step to add more steps to the configuration.

To remove any of the steps added, select the step and click the **Delete** button at the bottom of the Add Mesh Step page.

Step 7 Click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The Demand deduction collector is configured to collect information about traffic demands from the network.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

NetFlow data collection

Cisco Crosswork Planning can collect and aggregate exported NetFlow and related flow measurements. These measurements can be used to construct accurate demand traffic data for Cisco Crosswork Planning Design. Flow collection provides an alternative to the estimation of demand traffic from interfaces, LSPs, and other statistics using Demand deduction. NetFlow gathers information about the traffic flow and helps to build traffic and demand matrix. Importing flow measurements is particularly useful when there is full or nearly full flow coverage of a network's edge routers. Additionally, it is beneficial when accuracy of individual demands between external autonomous systems (ASes) is of interest.

Network data collected separately by collectors, including topology, BGP neighbors, and interface statistics, is combined with the flow measurements to scale flows and provide a complete demand mesh between both external autonomous systems and internal nodes.



Note If the NetFlow collector is part of multiple collections, you cannot execute those collections at the same time. Each collection must be run individually, as the NetFlow collector does not support simultaneous execution of collections.

Cisco Crosswork Planning gathers the following types of data to build a network model with flows and their traffic measurements aggregated over time:

- Flow traffic using NetFlow, JFlow, CFlowd, IPFIX, and Netstream flows
- Interface traffic and BGP peers over SNMP
- BGP path attributes over peering sessions

NetFlow collection configuration

The flow collection process supports IPv4 and IPv6 flows captured and exported by routers in the ingress direction. It also supports IPv4 and IPv6 iBGP peering.

Routers must be configured to export flows to and establish BGP peering with the flow collection server. Note the following recommendations:

- NetFlow v5, v9, and IPFIX datagram export to the UDP port number of the flow collection server, which has a default setting of 2100. Export of IPv6 flows requires NetFlow v9 or IPFIX.
- Define a BGP session on the routers configured as iBGP Route Reflector Client for the flow collector server. If configuring this in the router itself is not feasible, then a BGP Route Reflector Server with a complete view of all relevant routing tables can be used instead.
- Configure the source IPv4 address of flow export datagrams to be the same as the source IPv4 address of iBGP messages if they are in the same network address space.
- Explicitly configure the BGP router ID.
- If receiving BGP routes, the maximum length of the BGP `AS path` attribute is limited to three hops. The reason is to prevent excessive server memory consumption, considering that the total length of BGP attributes, including `AS path`, attached to a single IP prefix can be very large (up to 64 KB).

Configure the NetFlow collection

This topic describes how to configure the **NetFlow** collector.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- Ensure all NetFlow agents are configured to operate in single mode.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Traffic and Demands** section, select **NetFlow**, and click **Next**.

Step 4 On the Configure page, click **NetFlow** in the **Selected collectors** pane on the left.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.
- **Agents**: Select the applicable agents from the drop-down list.

Step 6 In the **Common config** section, from the **Split AS flows on ingress** drop-down list, select the traffic aggregation strategy for external ASNs.

(Optional) Enter information in the other fields. For field descriptions, see NetFlow collection advanced options, on page 86.

Step 7 (Optional) Expand the **IAS flows** and **Demands** panels, and configure any other relevant advanced fields as needed. For descriptions of these options, see NetFlow collection advanced options, on page 86. Then, click **Next**.

Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The NetFlow collection configuration is now complete.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.

NetFlow collection advanced options

You can configure several advanced options when using the NetFlow collector.

Table 15: NetFlow collection advanced options

Option	Description
Common config	
Split AS flows on ingress	Specifies the traffic aggregation strategy for external ASNs. When multiple external ASNs are connected to an IXP switch, it determines whether to aggregate traffic data from all ASNs or to distribute it proportionally to MAC accounting ingress traffic.
ASN	Specifies the ASN of the internal AS in the network.
Address family	Specifies the list of protocol versions to include. Enter the versions as a comma-separated list.
Ext node tags	Allows you to enter one or more node tags. Click + to add multiple node tags.
Split AS flows on egress	Splits Inter AS flows as they exit the network through all the interfaces connected to the egress AS.
Extra aggregation	Allows you to select additional aggregation keys from the drop-down list.
Log level	Specifies the log level of the tool. The options are Off, Fatal, Error, Warn, Notice, Info, Debug, and Trace.
Number of threads	Specifies the maximum number of threads to be used in parallel computation.

Option	Description
IAS flows	
Trim inter AS flows	Specifies the value in MBits/sec below which the Inter AS flows for traffic is strictly discarded.
Match BGP external info	Specifies whether to match egress IP addresses in the BGP peer relation.
Ingress interface filter	Specifies a filter of node and interface in the form Node:InterfaceName that will be applied while reading the flow matrix to filter only those ingress interfaces.
Egress interface filter	Specifies a filter of node and interface in the form Node:InterfaceName that will be applied while reading the flow matrix to filter only those egress interfaces.
Back track micro flows	Specifies whether to generate files showing a relationship between micro flows from the input file and those demands or Inter AS flows that aggregate them.
Flow import IDs	Allows you enter comma separated flow IDs to import data from.
IAS computation timeout	Specifies the timeout for IAS flows computation, in minutes. The valid range is 1 to 1440. The default is 60 minutes.
Demands	
Demand name	Specifies the name for any new demands.
Demand tag	Specifies the tag for any new demands, or to append to the existing demands.
Trim demands	Discards demands below a set threshold (in Mbits/sec).
Demand service class	Specifies the service class for demands.
Demand traffic level	Specifies the traffic level for demands.
Missing flows	Specifies the path where the file with interfaces that are missing flows is generated.

Run an external script against a network model

This topic describes how to run an external script against a network model.

The external scripts let you run a customized script against a selected network model. Use this feature when you need specific data from your network that the existing collectors cannot provide. In this case, you take an existing collection model created in Cisco Crosswork Planning and append information from a custom script to create a final network model that contains the data you need.

For an example of a custom script, see Sample script for updating interface descriptions, on page 89.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- Have the custom script and any supporting files ready in one of the accepted file formats or compressed archives.

Note If you are using a script from Cisco WAE and intend to use it within Cisco Crosswork Planning, it may not function as expected without modifications. This is due to architectural differences between Cisco WAE and Cisco Crosswork Planning, including variations in how the files are referenced. You must adjust the script appropriately for use in Cisco Crosswork Planning.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed. Optionally, select other advanced collectors according to your needs.

Step 3 On the Configure page, click **+ Add external script** under the Advanced Modeling or Traffic and Demands section.

Step 4 Enter these details:

- **Collector name**: Specify the name for this collection.
- **Is source a plan file?**: Check this check box if you want to run the script on a plan file. If you select this option, enter the plan file details in the **Input plan file** field.
- **Source**: Select the collector on which you want to run the external script. For example, if you select BGP as the Source, the custom script is executed on the BGP collector. The output model from the BGP collection is updated based on the specifications mentioned in the custom script.
- **Input file**: Upload your custom script along with any supporting files necessary for its successful execution. If multiple files are required, compress them into a single archive before uploading. Valid file formats are .py, .sh, .pl, .zip, .tar, .gz, and .tar.gz.

  Note
  Each time a file is uploaded, the input file option is overwritten.

- **Executable script**: Enter the name of the file that initiates the script execution process. This is one of the files you uploaded in the **Input file** field.

  The external script executor provides command line arguments that enable custom scripts to access specific files and the home directory. The arguments are predefined and follow a specific order. Understanding what each argument represents is important to ensure proper usage. The argument details are listed here.

  - argv[1]: Source plan file
  - argv[2]: Output plan file
  - argv[3]: Device access authentication file
  - argv[4]: Global network access configuration file

- argv[5]: Home directory

Example:

The Sample script for updating interface descriptions, on page 89 appends a description to every interface in the network with "My IGP metric is *value*" based on the data from an Excel file named "description.xlsx". The argv[5] parameter in the script specifies the home directory path of the "description.xlsx" file. For the script to run successfully, note that you must include this Excel file in the compressed file before uploading via the **Input file** field.

- **Script language**: Select the language of the custom script. The valid script languages are Python, Shell, and Perl.
- **Aggregator properties**: If you want to specify any tables or columns to be aggregated, then list them in a .properties file and upload the file using this field. By default, all columns and tables are aggregated.
- **Timeout**: Specify the action timeout. The default is 30 minutes.

Step 5 Click **Next**.

Step 6 Preview the configuration and then click **Create** to create the collection.

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The custom script executes against the selected network model.

Sample script for updating interface descriptions

This sample Python script, read-from-excel.py, appends a description to every interface in the network with "My IGP metric is <*value*>" using data from the Excel file, description.xlsx.

Script content

```
import sys
import openpyxl
import os
from com.cisco.wae.opm.network import Network

src = sys.argv[1]
dest = sys.argv[2]
home = sys.argv[5]
srcNet = Network(src)
excel_file = os.path.join(home, "description.xlsx")
wb = openpyxl.load_workbook(excel_file)
sheet = wb.active

row_count = 1
for node in srcNet.model.nodes:
    for iface in node.interfaces:
        cell_obj = sheet.cell(row=row_count, column=1)
        iface.description = 'My IGP metric is ' + str(cell_obj.value)
        row_count = row_count + 1
        print(iface.description)

srcNet.write(dest)
```

How data is collected from third-party devices

Summary

The support modules are executable programs that take arguments to determine what and how to collect. The collected data is used to augment the given plan file and produce an output plan file.

The support modules must

- include capabilities for data collection, such as SNMP
- allow for the input of an auth file to authenticate access to the devices it will poll
- allow for the input of a network access configuration file to manage specifics of collection, such as timeouts, retries, maximum request per device, and so on
- read and write to a plan file

All these constitute the support module framework, which is provided as a template of Python libraries, simplifying the process of data collection from third-party devices.

Workflow

These stages describe how data is collected from third-party devices using support modules.

1. Once the support modules are written, integrate them into the collectors using support module configurations.
2. Specify the type of support module, executable script. The simplest is to use an executable that can be written in Python). Then, provide the script's path.
3. The collectors reorganize the execution to run the support module.

Collectors with support module configurations

Third-party support module configurations are available in these collectors:

- IGP database (Nodes and Interfaces)
- SR-PCE (Nodes and Interfaces)
- LSP
- BGP
- VPN
- Multicast (all the collectors)

Collect data from third-party devices

This topic describes how to collect data from third-party devices using the support module.

Before you begin

- Ensure you have the required support module.
- Complete the steps mentioned in Preconfiguration workflow, on page 10.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Select one of the basic topology collectors, as needed.

Step 3 In the **Advanced modeling** section, select any of the required collectors listed in Collectors with support module configurations, on page 90. Then, click **Next**.

Step 4 In the **Selected collectors** pane on the left, choose the collectors you selected in Step 3 and make all the necessary configuration changes. For more information, refer to the appropriate collector topics.

Note
Ensure that the basic topology parameters are updated to meet your needs. Update the parameters if necessary.

Step 5 To collect data from third-party devices:

a) Check the **Enabled** check box next to the **3rd party support module** parameter.

All support module configuration options appear.

b) Enter the details for these parameters:

- **Execute using**: Select the language you want to use to run the support module. The valid languages are PYTHON, SHELL, and PERL.
- **Executable script**: Enter the full path of the start-up script. This file includes the options for retrieving the start-up script name in the support module file.

  Note
  Ensure you provide the full path of the script. For example, features/src/supportmodule.py. Use only forward slashes (/) in the path and do not start the path with "./" or "/".

- **Support module**: Click **Browse** and select the support module. Ensure that the support module is in .zip or .tar format.

c) (Optional) In the **Optional Arguments** section, enter the relevant arguments as key-value pairs. This is required if you want to collect data from devices based on a specific configuration parameter in the support module.

Step 6 After entering the required configuration parameters in all the selected collectors, click **Next**.

Step 7 Preview the configuration and then click **Create** to create the collection.

Step 8 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The system begins collecting data from the specified third-party devices using your provided support module and parameters.

Merge AS plan files

This topic describes how to configure the **Merge AS** tool to merge plan files from different Autonomous Systems (ASes).

This tool resolves any conflicts across plan files. It supports plan files in native format.

Important notes on the Merge AS tool

- Each AS can be on a different Cisco Crosswork Planning server.
- Only AS, Circuits, Nodes, Interfaces, External Endpoints, and External Endpoint Members with virtual nodes and unresolved interfaces are resolved.
- These demands are resolved:
  - Source or Destination associated with a virtual node that is resolved with a real node
  - Source or Destination associated with the interface in a specific format
  - Source or Destination associated with the External Endpoints
- These demands are not resolved:
  - Source or Destination associated with ASN number only
- For a given plan file, the internal ASN must match what other plan files identify as an external ASN, and all ASes to be merged must be discovered in every plan file.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 10.
- Collect topology and traffic information for different ASes.
- Ensure that the plan files from different ASes are present on the same Cisco Crosswork Planning server, and their file paths are specified.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure collections, on page 30 or Edit collections, on page 34.

Step 2 Click the **Tools** radio button at the top.

Step 3 Select **Merge AS** and click **Next**.

Step 4 Enter these configuration parameters:

- **Retain demands**: Check the **Enabled** check box to merge the demands.
- **Tag name**: Enter a tag name to help identify the updated rows in the .pln file. The tag column in the .pln file gets updated with this tag name for modified rows.

Step 5 In the **Source collector** section, click **+ Add source collector**, and select the relevant Collection and Collector names.

Step 6 In the **Source DB** section, click **+ Add source DB**, click **Browse**, and select the source plan file located on your system.

Note
If you are migrating the configuration either from Cisco WAE or from another Cisco Crosswork Planning instance, ensure that the **DB file** field is updated with the correct file after importing the configuration. This is necessary because, after importing the configuration, the server restores only the file name and not the actual file. If the field is not updated with the correct file, then the collection fails.

Step 7 Click **Next**.

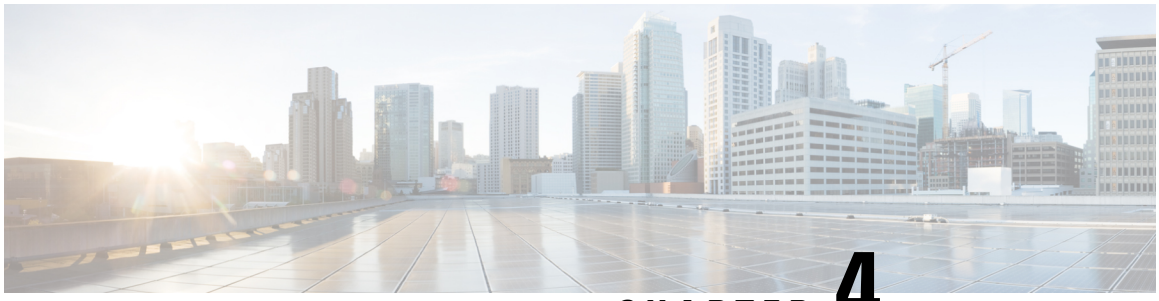
Step 8 Preview the configuration and then click **Create** to create the collection.

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule collections, on page 36.

The resulting plan file consolidates data from different ASes.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit collections, on page 34.



CHAPTER 4

Manage Licenses

Cisco Crosswork Planning supports Cisco Smart Licensing. A license is required to use all the features in Cisco Crosswork Planning. If you have questions about obtaining a license, contact your Cisco support representative or system administrator.

This chapter contains the following topics:

- Cisco Smart Licensing, on page 95
- Configuring Smart Licensing, on page 96
- Configure the transport mode between Cisco Crosswork Planning and CSSM, on page 96
- Register Cisco Crosswork Planning via token, on page 98
- Register Cisco Crosswork Planning via offline reservation, on page 101
- Update license counts, on page 104
- License authorization statuses, on page 106

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that

- provides an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization
- enables centralized control over license usage and access
- is secure, allowing you to control what users can access.

Benefits of Smart Licensing

Key benefits of Smart Licensing include:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization, eliminating the need for Product Activation Keys (PAKs).
- Unified Management: Offers a complete view into all of your Cisco products and services in an easy-to-use portal, helping you always know what you have and use.
- License Flexibility: Your software is not node-locked to hardware, allowing you to easily use and transfer licenses as needed.

Configuring Smart Licensing

Summary

Cisco Crosswork Planning integrates with Cisco Smart Accounts to simplify license management.

Smart Accounts provide a centralized, organized, and simple-to-use solution for managing Cisco software licenses across an entire organization. They act as a container that holds all Cisco software assets, allowing customers to view, store, manage, and move these assets as needed. Smart Accounts enable full visibility into license entitlements and usage, helping optimize software management. Smart Accounts support license pooling, portability, and provide compliance reporting.

Virtual Accounts are customizable subaccounts within a Smart Account used to organize and optimize Cisco licenses. They can be structured to reflect business units, product types, or geographic locations, allowing better planning and utilization of assets.

The Cisco Smart Software Manager (CSSM) enables you to manage all your Cisco Smart software licenses from one centralized website. With CSSM, you can create and manage multiple virtual accounts within your Smart Account to manage licenses. For details on Cisco Licensing, go to cisco.com/go/licensingguide.

In the Cisco Crosswork Planning UI, from the main menu, choose **Licensing**. The Smart License page opens. You can register Cisco Crosswork Planning, edit the transport settings, renew the license, and deregister the application on this page.

Workflow

These are the stages of configuring Cisco Smart Licensing in Cisco Crosswork Planning.

1. Set up a Smart Account on Cisco Software Central (software.cisco.com).
   a. Go to Smart Account Request.
   b. Follow the instructions on the website.
2. (Optional) Configure transport settings. For details, see Configure the transport mode between Cisco Crosswork Planning and CSSM, on page 96.
3. Register Cisco Crosswork Planning with CSSM. For details, see Register Cisco Crosswork Planning via token, on page 98 or Register Cisco Crosswork Planning via offline reservation, on page 101.

Configure the transport mode between Cisco Crosswork Planning and CSSM

This topic describes how to configure the transport settings to control how Cisco Crosswork Planning communicates with CSSM.

Cisco Crosswork Planning supports multiple transport modes to connect with CSSM:

- **Direct**: Cisco Crosswork Planning directly connects with CSSM.

- **Transport Gateway**: Cisco Crosswork Planning communicates via a Transport Gateway or CSSM On-prem. This approach replicates a cloud-based user experience while keeping all communication on premises. For details on the CSSM On-prem option, see the Smart Software Manager guide.

Note Cisco Crosswork Planning supports only SmartTransport URL. The URL format is: http://*SSM-ONPREM-IP*/SmartTransport.

- **HTTP/HTTPS Proxy**: Cisco Crosswork Planning connects to the direct mode end point through the configured proxy, if a proxy exists.

Follow these steps to configure the transport mode between Cisco Crosswork Planning and CSSM.

Before you begin

If Cisco Crosswork Planning is in Registered mode, you cannot change the transport settings. To modify transport settings, you must first deregister the product.

Procedure

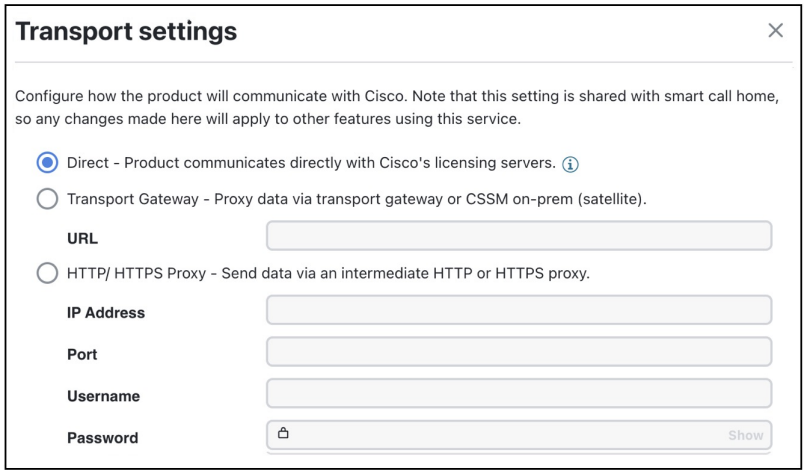
Step 1 From the main menu, choose **Licensing**.

The Smart License page opens.

Step 2 In the **Transport settings** field, view the current transport mode. To modify it, click **View / Edit**.

The Transport settings page appears.

Figure 23: Transport settings page



Step 3 Select the appropriate transport mode. Enter values in all the required fields.

Step 4 Click **Save**.

The selected transport mode and settings are saved. Cisco Crosswork Planning will use the configured transport mode for communication with CSSM.

Register Cisco Crosswork Planning via token

This topic describes how to register Cisco Crosswork Planning with CSSM using a registration token.

To enable the licensed features, you must register the Cisco Crosswork Planning application with CSSM using a registration token. Once registered, an Identity Certificate is saved securely in your Smart Account and used for all ongoing communications. The certificate is valid for one year and is renewed automatically after six months to ensure continuous operation.

Before you begin

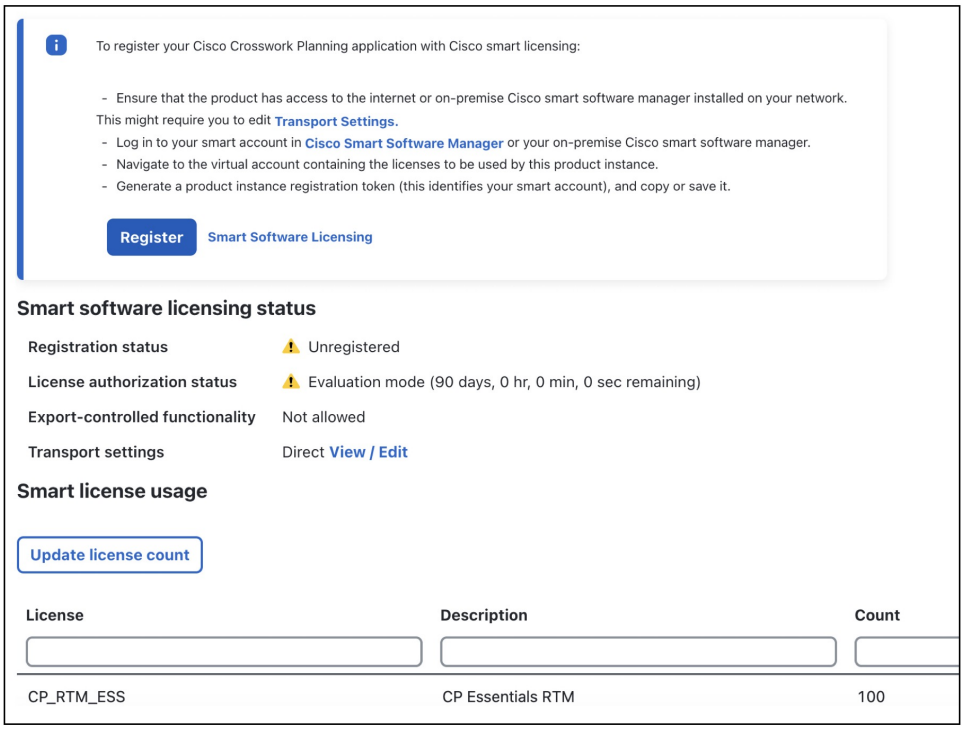
- Confirm that you have a Smart Account. If not, go to Smart Account Request and follow the instructions to create one.
- Ensure you have a valid product instance registration token. For guidance on generating the token, see the support resources in Cisco Software Central.

Procedure

Step 1 From the main menu, choose **Licensing**.

The registration status and license authorization status display as **Unregistered** and **Evaluation mode**, respectively.

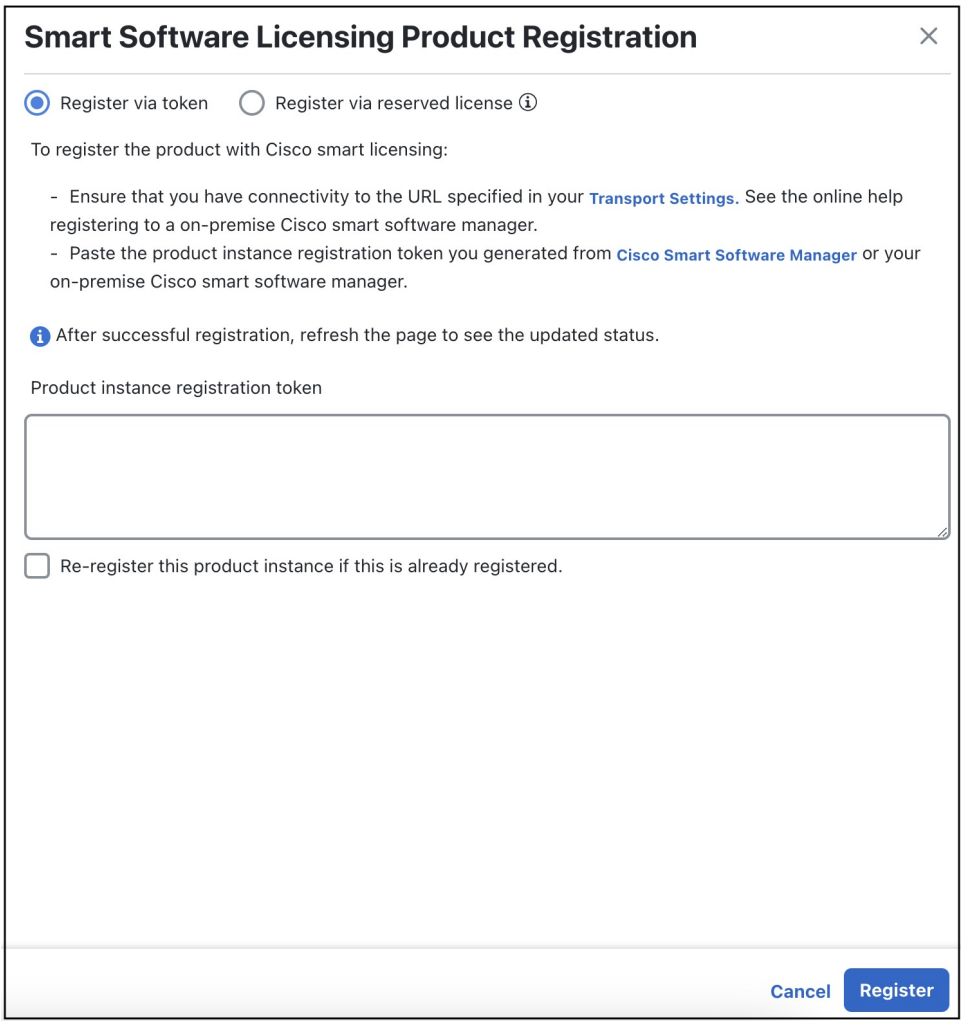
Figure 24: Smart software licensing unregistered example



Step 2 In the Smart Software Licensing area at the top, click **Register**.

The Smart Software Licensing Product Registration page opens.

Figure 25: Smart software licensing product registration page



Step 3 In the **Product instance registration token** field, enter the registration token generated from your Smart Account. Ensure the token ID is accurate and within its validity period.

Step 4 (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** check box.

Step 5 Click **Register**.

Note

- The request takes at least 20 seconds to succeed. If you do not receive a correct response from the backend within 20 seconds, the UI continues to check every 10 seconds for up to 5 minutes. If you do not receive any response after 5 minutes, a generic error message appears.
- If you see a registration error (such as "Communication send error" or "Invalid response from licensing cloud"), wait for some time and then retry the registration. If the error persists after multiple attempts, contact the Cisco Customer Experience team.
- In some cases, after successful registration, you may need to refresh the page manually to see the updated status.

After the registration is successful, a "Product Registration completed successfully" message appears.

Cisco Crosswork Planning is now registered with CSSM using a registration token. The registration and license authorization statuses are change to **Registered** and **Authorized**, respectively.

Manually perform licensing actions

This topic describes how to manually renew, register, or de-register licenses in Cisco Crosswork Planning.

By default, Cisco Crosswork Planning automatically handles registration and authorization renewals. However, if communication between the application and the Cisco server fails, manually initiate specific licensing actions using the **Actions** drop-down menu.

Before you begin

Ensure the Cisco Crosswork Planning application is in Registered mode.

Procedure

Step 1 From the main menu, choose **Licensing**.

The Smart License page appears.

Step 2 Click the **Actions** drop-down button.

Step 3 Select one of these options as required.

a) **Renew Authorization**: manually renews authorization if automatic renewal fails after 30 days.
b) **Renew Registration**: manually renews registration if automatic renewal fails after six months.
c) **Re-register**: re-registers the application, for example, if registration token has expired.
d) **De-register**: de-registers the application, for example, when you need to change the transport settings.

Note
After you de-register the application, it enters the **Evaluation** mode if evaluation period is available. Otherwise, it enters the **Evaluation Expired** mode. For more information, see License authorization statuses, on page 106.

The selected manual licensing action completes, and the application's license status is updated accordingly.

Register Cisco Crosswork Planning via offline reservation

This topic describes how to register Cisco Crosswork Planning with CSSM using offline reservation.

When you use Smart Licensing, Cisco Crosswork Planning shares usage information with CSSM at regular intervals. If you do not want to connect with CSSM regularly, Cisco Smart Licensing provides an option of offline reservation.

Before you begin

Confirm that you have a Smart Account. If not, go to Smart Account Request and follow the instructions to create one.

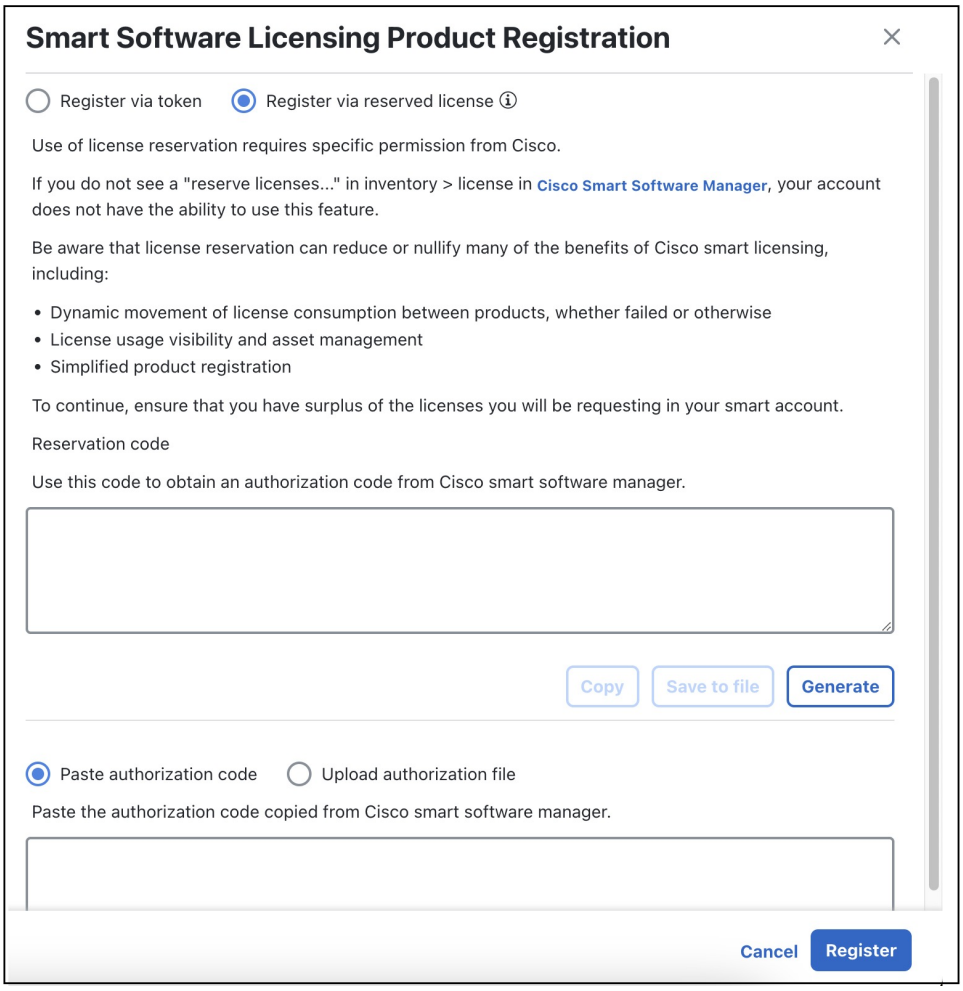
Procedure

Step 1 From the main menu, choose **Licensing**.

Step 2 In the Smart Software Licensing information box at the top, click **Register**.

The Smart Software Licensing Product Registration page opens.

Figure 26: Smart software licensing product registration page



Step 3 Select the **Register via reserved license** option.

Step 4 Generate a Reservation Request Code.

a) Click **Generate** in the Reservation code section. The Reservation Request Code appears in the text field.

b) Click the **Copy** button to copy the generated code.

Step 5 Generate the Authorization Code in CSSM.

a) Log in to CSSM and select the appropriate Virtual Account.
b) Click the **Licenses** tab and then click **License Reservation**.
c) Paste the Reservation Request Code you generated in Step 4 and click **Next**.
d) On the Select Licenses page, select the type of reservation you need and click **Next**.
e) On the Review and Confirm page, click **Generate Authorization Code**.
f) Copy the generated code using the **Copy to Clipboard** button.

Step 6 Navigate back to the Smart Software Licensing Product Registration page in Cisco Crosswork Planning.

Step 7 Select the **Paste authorization code** option and paste the authorization code in the text field.

Step 8 Click **Register**.

It may take a few minutes to process the registration.

Cisco Crosswork Planning is now registered with CSSM using the offline reservation method. The registration and license authorization statuses change to **Registered** and **Authorized**, respectively.

Update offline reservation

This topic describes how to update the license counts associated with a product instance that uses offline reservation.

Procedure

Step 1 From the main menu, choose **Licensing**. Note the Product Instance Name under the Smart Software Licensing Status section.

Step 2 Generate the Authorization Code in CSSM.

a) Log in to CSSM and select the appropriate Virtual Account.
b) Click the name of the product instance that matches your Product Instance Name.
c) For this product instance, click **Actions** > **Update Reservation**.
d) On the Select Licenses page, select the type of reservation you need, update the count of the necessary licenses from the list, and then click **Next**.
e) On the Review and Confirm page, click **Generate Authorization Code**.
f) Copy the generated Authorization Code using **Copy to Clipboard**.

Step 3 Navigate back to the Smart License page on the Cisco Crosswork Planning UI.

Step 4 Click **Actions** > **Update Reservation**.

Step 5 Paste the Authorization Code generated in Step 2 and click **Update**.

A Confirmation Code is generated. You can find it under the Smart Software Licensing Status section. Copy this code.

Step 6 Enter the Confirmation Code in CSSM.

a) Navigate back to CSSM and click the required product instance name.
b) Click **Actions** > **Enter Confirmation Code**.
c) Enter or paste the Reservation Confirmation Code generated in Step 5.

d) Click **OK**.

The license count is updated on the Smart License page of the Cisco Crosswork Planning UI.

Disable offline reservation

This topic describes how to release reserved licenses in Cisco Crosswork Planning.

Releasing the reserved licenses returns them to the pool and stops the application from consuming reserved licenses. After you release the licenses, the application enters the **Evaluation** mode if an evaluation period is available. Otherwise, it enters the **Evaluation Expired** mode.

Procedure

Step 1 From the main menu, choose **Licensing**. Note the Product Instance Name under the Smart Software Licensing Status section.

Step 2 Click **Actions** > **Return Reservation**.

Step 3 On the Confirm Return Reservation page, click **Confirm**.

The system generates a Release Code (Reservation Return Code). Use the **Copy** button to copy this code .

Step 4 Enter the Reservation Request Code in CSSM.

a) Log in to CSSM and select the appropriate virtual account.
b) Click the name of the product instance that matches your Product Instance Name.
c) For this product instance, click **Actions** > **Remove**.
d) In the Remove Reservation page, paste the Reservation Return Code that you generated in Step 3 and click **Remove Reservation**.

Step 5 Navigate back to the Smart License page in the Cisco Crosswork Planning UI. Notice that the Registration status has changed to **Unregistered**.

Step 6 Click **Actions** > **Disable License Reservation**.

The reserved licenses are released. The application enters Evaluation mode if available, or enters Evaluation Expired mode.

Update license counts

This topic describes how to update license counts in Cisco Crosswork Planning to ensure compliance and proper operation of the tools in the Cisco Crosswork Planning Design application.

Before you begin

Ensure you have a sufficient number of licenses in your Virtual Account in CSSM. Otherwise, the licenses will be out of compliance.

Procedure

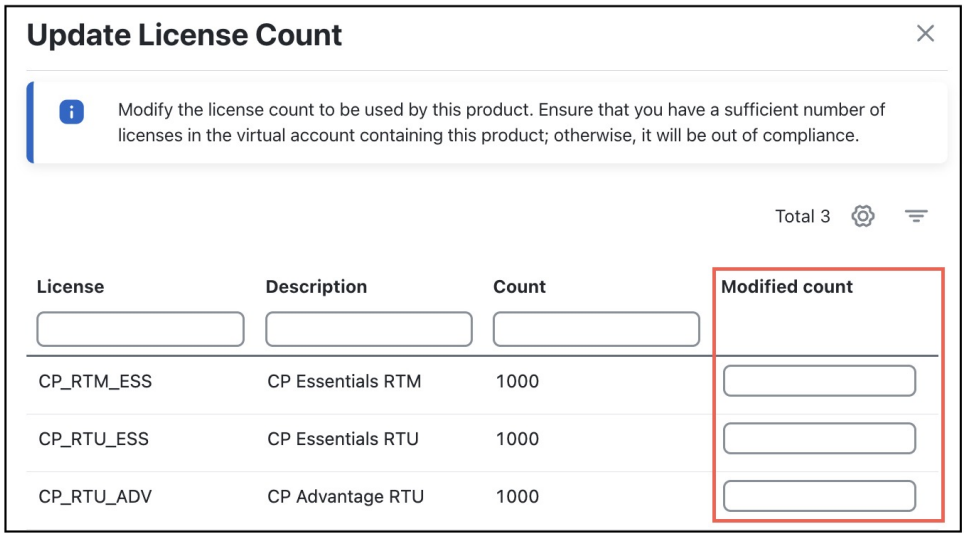
Step 1 From the main menu, choose **Licensing**.

Step 2 In the **License usage** section, click **Update license count**.

The Update License Count page appears.

Step 3 Enter the required license count in the **Modified count** column.

Figure 27: Update license count page



There are three types of licenses in Cisco Crosswork Planning:

- **CP_RTM_ESS**: You can choose to have either one license or a number of licenses equal to the number of nodes in the network. Cisco Crosswork Planning Collector application functions even if there is only one license. However, for Cisco Crosswork Planning Design application, the count must match the number of nodes in the network. This is necessary for the tools and initializers to function correctly.
- **CP_RTU_ESS**: A count of 1 is sufficient for both Cisco Crosswork Planning Collector and Design applications to function correctly.
- **CP_RTU_ADV**: A count of 1 is sufficient for both Cisco Crosswork Planning Collector and Design applications to function correctly.

Step 4 Click **Save**.

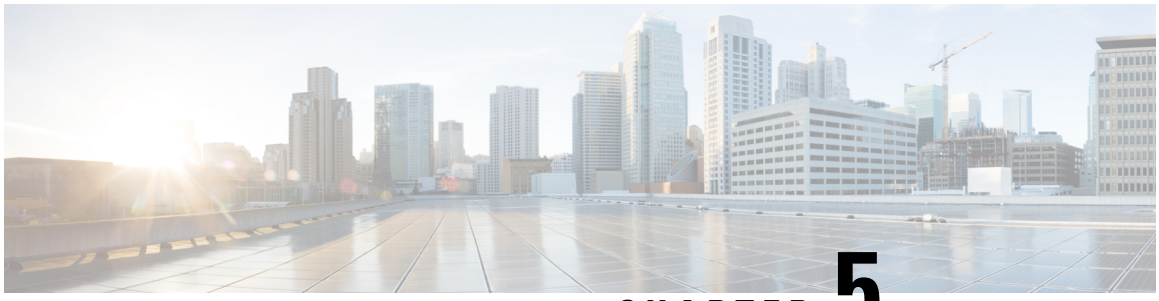
The system updates and applies the number of licenses.

License authorization statuses

Based on the system registration status, the application displays several distinct license authorization statuses. Table 16: License authorization statuses, on page 106 describes each possible combination of registration status and license authorization status and explains what each means for application usage.

Table 16: License authorization statuses

Registration status	License authorization status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which all 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 cannot contact the CSSM before its Identity Certificates expire, causing it to return to the unregistered state. The application resumes the remaining evaluation period, if available. At this stage, a new registration ID token is required to reregister the application.
Registered	Authorized (In Compliance)	The application is 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 or 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.



CHAPTER 5

Manage Administrative Tasks

This chapter contains the following topics:

- Manage certificates, on page 107
- Manage users, on page 114
- Set up user authentication (TACACS+, LDAP, and RADIUS), on page 122
- Monitor system and application health, on page 135
- Manage backups, on page 139
- View system and network alarms, on page 145
- View audit log, on page 146
- Set the pre-login disclaimer, on page 146
- Manage maintenance mode settings, on page 147
- Update network access configuration, on page 148
- Update collector capability, on page 148
- Configure aging, on page 149
- Configure purging of archived plan files, on page 150
- Configure static routes, on page 150

Manage certificates

What is a certificate?

A certificate is an electronic document that identifies an entity such as a person, server, or company and links it to a public key. When a certificate is created, both a public key and a matching private key are generated. In the TLS protocol, the public key encrypts data, while the private key decrypts it.

Certificates are signed by an issuer, often a Certificate Authority (CA), which acts as a "parent" certificate. This process can also be self-signed. In a TLS exchange, a trust chain of certificates verifies the issuer's validity. This chain includes three types of entities: a self-signed root CA certificate, possibly several intermediate CA certificates, and an end-entity certificate. Intermediate certificates connect the server certificates to the root CA, adding security. Starting with the root certificate's private key, each certificate in the chain signs and issues the next one, ending with the end-entity certificate used for server or client authentication.

Certificates in Cisco Crosswork Planning

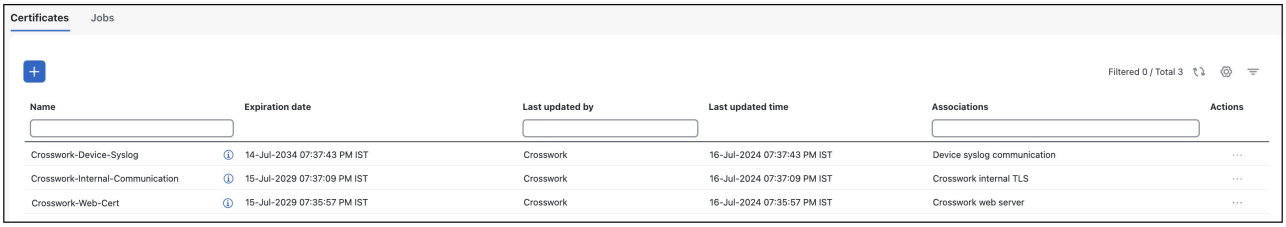
Cisco Crosswork Planning uses the TLS protocol for secure communication between devices and components. TLS utilizes X.509 certificates to authenticate devices and encrypt data, ensuring its integrity. The system

employs a combination of generated certificates and those uploaded by clients. Uploaded certificates might be purchased from Certificate Authorities or be self-signed. For instance, the system's VM-hosted web server and the client browser interface use the system-generated X.509 certificates exchanged over TLS for secure communication.

The Crosswork Cert Manager is a proxy for multiple microservices and services within the distributed framework and manages all the Crosswork certificates. The Certificate Management page (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates.

Figure 28: Certificate management page, on page 108 displays the default certificates provided by Cisco Crosswork Planning.

Figure 28: Certificate management page



Certificate types and usage

These certificates are classified into various roles with different properties depending on their use case as shown in the following table.

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork Internal TLS	Crosswork-Internal-Communication	• Generated and provided by Crosswork. • This trust-chain is available in the UI (including the server and client leaf certificates) and is created by Crosswork during initialization. • Allows mutual and server authentication.	Crosswork	Crosswork	Download	5 years	—

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork Web Server	Crosswork-Web-Cert Server Authentication	• Generated and provided by Crosswork. • Provides communication between the user browser and Crosswork. • Allows server authentication.	Crosswork Web Server	User Browser or API Client	• Upload • Download	5 years	30 days to 5 years
Crosswork Device Syslog	Crosswork-Device-Syslog	• Generated and provided by Crosswork. • Allows server authentication.		Device	Download	5 years	—

There are two category roles in Crosswork:

- Roles which allow you to upload or download trust chains only.
- Roles that allow upload or download of both the trust chain and an intermediate certificate and key.

Add new certificates

You can add certificates for the following role:

- **Secure LDAP communication**: You upload the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork, the user can add the LDAP server (see Manage LDAP servers, on page 125) and associate the certificate.



Note Cisco Crosswork Planning does not receive a web certificate directly. It accepts an intermediate CA and intermediate Key to create a new web certificate, and apply it to the Web Gateway.

Before you begin

- For information on certificate types and usage, see Certificate types and usage, on page 108.
- All certificates that are uploaded must be in Privacy Enhanced Mail (PEM) format. Note where these certificates are in the system so that you can navigate to them easily.

- Trust chain files that are uploaded may contain the entire hierarchy (root CA and intermediate certificates) in the same file. In some cases, multiple chains are also allowed in the same file.
- Intermediate Keys need to be either PKCS1 or PKCS8 format.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management** and click +.

Step 2 Enter a unique name for the certificate.

Step 3 From the **Certificate Role** drop-down menu, select the purpose for which the certificate is to be used.

Note
Only the **Secure LDAP communication** option is applicable for Cisco Crosswork Planning.

Step 4 Click **Browse**, and navigate to the certificate trustchain.

Step 5 Click **Save**.

Note
Once uploaded, the Crosswork Cert manager accepts, validates, and generates the server certificate. Upon successful validation, an alarm ("Crosswork Web Server Restart") indicates that the certificate is about to be applied. The Certificate Management UI then logs out automatically and applies the certificate to the Web Gateway. The new certificate can be checked by clicking the lock <Not Secure>/<secure> icon next to the https://<crosswork_ip>:30603.

Edit certificates

You can edit a certificate to add or remove connection destinations, upload, and replace expired or misconfigured certificates. User provided certificates and web certificates can be edited. Other system certificates that are provided by Cisco Crosswork cannot be modified and will not be available for selection.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**.

Step 2 To update a certificate:

a) Under the **Actions** column, click ••• on the certificate that you want to modify, and select **Update certificate**.

b) Fill in the appropriate values for the fields based on the certificate you wish to update. Click the ⓘ icon next to the field for more information.

c) Click **Save** to save the changes.

Step 3 To enable the client certificate authentication of a web certificate:

a) Under the **Actions** column, click ••• on the Crosswork web certificate that you want to modify, and select **Configure client certificate authentication**.

The **Configure Client Authentication** page is displayed.

b) Check the **Enable** checkbox.

The **Certificate schema** and **OCSP** settings are displayed.

The **OCSP** settings are enabled by default, but you can disable it if desired. If enabled, you can check the certificate revocation status using the Online Certificate Status Protocol (OCSP).

c) Choose the **Certificate schema** value.

- **Automatic**—Searches for the user principal name (UPN) in the alternate subject name area. If a UPN is not found, the system will use the common name value. This is the default selection.
- **Manual**—Searches for the username in the subject area based on the user identity source and the specified regular expression.

d) (Optional) Choose the **OCSP** value:

- **Automatic**—Extracts the responder URL from the certificate and uses it to perform OCSP validation.
- **Manual**—You must provide the OCSP responder URL.

e) Click **Save** to save the changes.

Step 4 To update certificate and configure client authentication in a single step:

a) Click ••• on the Crosswork web certificate that you want to modify, and select **Update certificate & configure client certificate authentication**.

The **Update Certificate and Configure Client Authentication** page is displayed.

Note
Choosing the combined option to update the certificate and configure client authentication minimizes downtime during the Crosswork server restart, as it occurs only once instead of twice if these actions are performed separately.

b) Provide the data as per the instructions in step 2 and step 3.

c) Click **Save** to save the changes.

Download certificates

Follow these steps to download certificates.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**.

Step 2 Click ⓘ for the certificate you want to download.

Step 3 To separately download the root certificate and the intermediate certificate, click ⬆ next to the certificate. To download the certificates at once, click **Export all**.

Update web certificate using certificate signing request

Cisco Crosswork Planning enables the updating of web certificates by importing an intermediate Certificate Authority (CA) certificate. Starting with version 7.0.1, it also supports updating web certificates through a Certificate Signing Request (CSR).

This approach allows you to obtain a certificate signed by an Enterprise or Commercial CA without exposing the private key outside of Cisco Crosswork Planning.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- This process requires the Crosswork server to be restarted, which will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**

Step 2 Click ••• on the web certificate (`Crosswork-Web-Cert`) and select **Update certificate**.

The **Certificate Update Method** page is displayed.

Step 3 Create a CSR to submit to the Certificate Authority.

a) Select **Create a certificate signing request (CSR)** radio button and click **Update certificate**.

The **Certificate Signing Request (CSR)** page is displayed.

b) Click **Create CSR**.

The **Create Certificate Signing Request (CSR)** page is displayed.

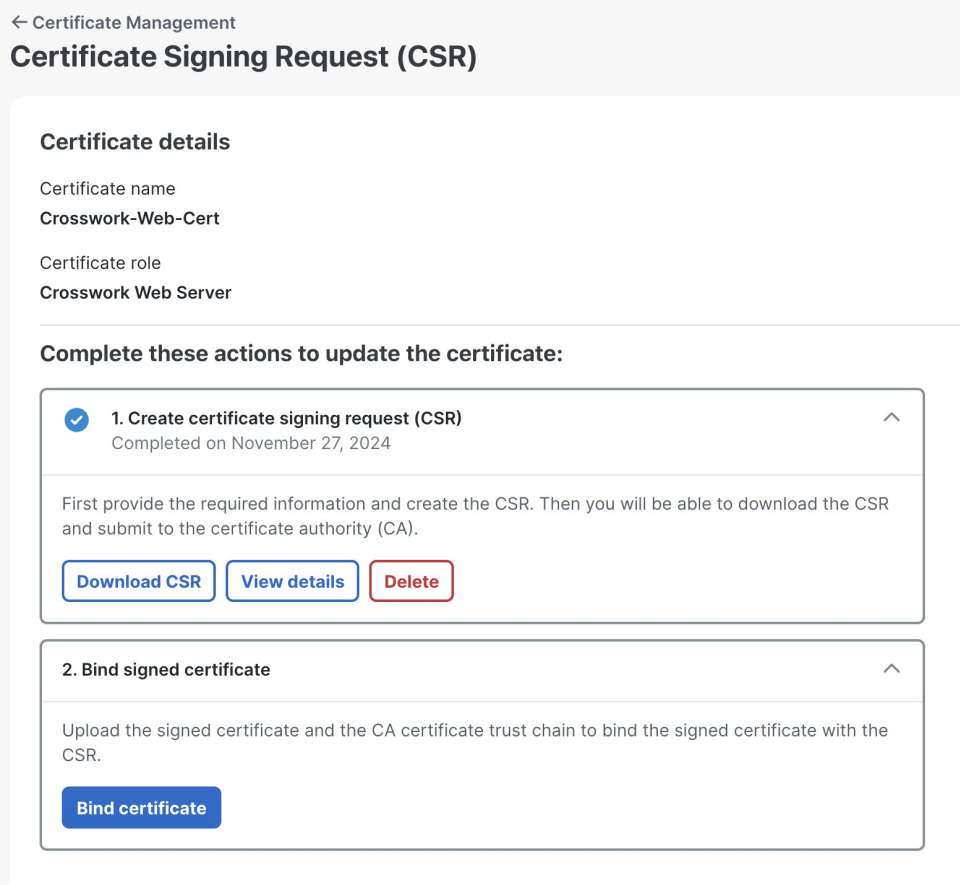
c) Provide relevant values for the fields provided. Click the ⓘ icon next to the field for more information. The mandatory fields are:

- **Common name (CN):** By default, this is the fully qualified domain name (FQDN) of the server, but it can be any unique name that identifies the server. The length should not exceed 64 characters.
- **IP address:** This is the Crosswork VIP address utilized in this deployment. Additional IP addresses should only be added if necessary for certificate validation.
- **Key Type:** The options are RSA and ECDSA. By default, RSA is selected.
- **Key Size (in bits):** The options are 2048, 3072, and 4096. By default, 2048 is selected.
- **Key Digest:** The options are SHA-256, SHA-384, SHA-224, and SHA-512. By default, SHA-256 is selected.

d) Click **Create CSR** to complete the action.

Step 4 After generating the CSR, click **Download** to download it and use the CSR to get a signed certificate from your CA.

Figure 29: Certificate Signing Request (CSR) page

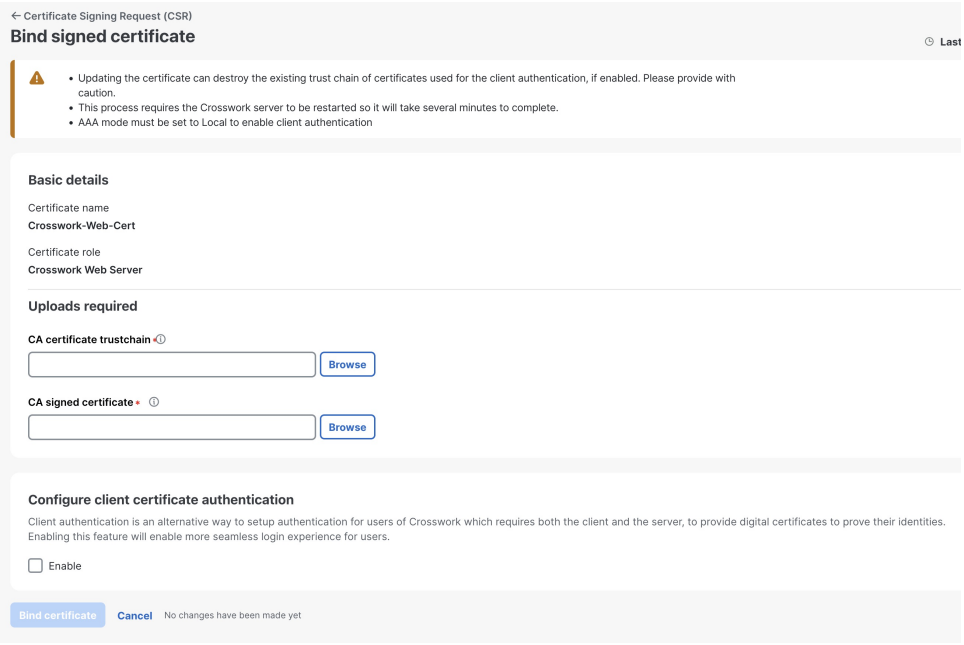


Step 5 Upload the CA-signed certificate and CA certificate trustchain to bind the certificate.

a) In the **Certificate Signing Request (CSR)** window, click **Bind certificate**.

The **Bind signed certificate** window is displayed.

Figure 30: Bind signed certificate



b) Upload the relevant data for the fields provided. Click the ⓘ icon next to the field for more information.

- **CA certificate trustchain:** This is the certificate trust chain for the web server certificate obtained from the CA.
- **CA signed certificate:** This is the final signed certificate for the web server obtained from the CA.

c) (Optional) Click the **Enable** checkbox to configure client certificate authentication.

d) Click **Bind certificate** to complete the operation.

After the bind action is completed, the web certificate is updated, and Tyk will restart with the new web certificate.

Manage users

As a best practice, administrators should create separate accounts for all users. Prepare a list of the people who will use Cisco Crosswork Planning. Decide on their user names and preliminary passwords, and create user profiles for them. During the creation of a user account, you assign a user role to determine the functionality to which the user will have access. If you will be using user roles other than "admin", create the user roles before you add your users (see Create user roles, on page 117).

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To add a new user:

a) Click  and enter the required user details.
b) Click **Save**.

Step 3 To edit a user:

a) Click the checkbox next to the User and click .
b) After making changes, click **Save**.

Step 4 To delete a user:

a) Click the checkbox next to the User and click .
b) In the **Confirm Deletion** window, click **Delete**.

Step 5 To view the audit log for a user:

a) Click the ••• icon under the **Actions** column, and select **Audit log**.

The **Audit Log** window is displayed for the selected user name. For more information, see View audit log, on page 146.

Administrative users created during installation

During installation, Cisco Crosswork Planning creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **`cw-admin`**, and the default password **`admin`**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Crosswork server.
2. The **Cisco Crosswork administrator**, with the username **`admin`** and the default password **`admin`**. Product administrators use this ID to log in to and configure the user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used.

User roles, functional categories and permissions

The **Roles** window lets users with the appropriate privileges define custom user roles. As with the default *admin* role, a custom user role consists of:

- A unique name, such as “Operator” or “admin”.
- One or more selected, named functional categories, which control whether or not a user with that role has access to the APIs needed to perform specific Cisco Crosswork functions controlled by that API.
- One or more selected permissions, which control the scope of what a user with that role can do in the functional category.

For a user role to have access to a functional category, that category and its underlying API must show as selected on the **Roles** page for that role. If the user role shows a functional category as unselected, then users with this role assigned will have no access to that functional area at all.

Some functional categories group multiple APIs under one category name. For example: The “AAA” category controls access to the Password Change, Remote Authentication Servers Integration, and Users and Role Management APIs. With this type of category, you can deny access to some of the APIs by leaving them unselected, while providing access to other APIs under the category by selecting them . For example: If you want to create an “Operator” role who is able to change his own password, but not see or change the settings for your installation’s integration with remote AAA servers, or create new users and roles, you would select the “AAA” category name, but uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” checkboxes.

For each role with a selected category, the **Roles** page also lets you define permissions to each underlying functional API:

- **Read** permission lets the user see and interact with the objects controlled by that API, but not change or delete them.
- **Write** permission lets the user see and change the objects controlled by that API, but not delete them.
- **Delete** permission gives the user role delete privileges over the objects controlled by that API. It is useful to remember that delete permission does not override basic limitations set by the Crosswork platform and it applications.

Although you can mix permissions as you wish:

- If you select an API for user access, you must provide at least “Read” permission to that API.
- When you select an API for user access, Cisco Crosswork assumes that you want the user to have all permissions on that API, and will select all three permissions for you, automatically.
- If you uncheck all of the permissions, including “Read”, Cisco Crosswork will assume that you want to deny access to the API, and unselect it for you.

Best Practices:

Cisco recommends that you follow these best practices when creating custom user roles:

- Restrict **Delete** permissions in roles for *admin* users with explicit administrative responsibility for maintenance and management of the Crosswork deployment as a whole.
- Roles for developers working with all the Cisco Crosswork APIs will need the same permissions as *admin* users.
- Apply at least **Read** and **Write** permissions in roles for users who are actively engaged in managing the network using Cisco Crosswork.
- Give read-only access to roles for users who only need to see the data to help their work as system architects or planners.

The following table describes some sample custom user roles you should consider creating:

Table 17: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager	All	Read, Write

Role	Description	Categories/API	Privileges
Monitor	Monitors alerts only	Cisco Crosswork Planning Design and Collector	Read only
API Integrator	All	All	All

Note Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions.

Create user roles

Local users with administrator privileges can create new users as needed (see Manage users, on page 114).

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, RADIUS and LDAP users cannot.

Follow these steps to create a new user role.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

The **Roles** window has a **Roles** table on the left side and a corresponding **Global API Permissions** tab on the right side which shows the grouping of user permissions for the selected role.

Step 2 On the **Roles** table, click  to display a new role entry in the table.

Step 3 Enter a unique name for the new role.

Step 4 To define the user role's privilege settings, select the **Global API Permissions** tab and perform the following:

a) Check the check box for every API that users with this role can access. The APIs are grouped logically based on their corresponding application.

b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 5 Click **Save** to create the new role.

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (see Edit user roles, on page 118).

Clone user roles

Cloning an existing user role is the same as creating a new user role, except that you need not set privileges for it. If you like, you can let the cloned user role inherit all the privileges of the original user role.

Cloning user roles is a handy way to create and assign many new user roles quickly. Following the steps below, you can clone an existing role multiple times. Defining the cloned user role's privileges is an optional step; you are only required to give the cloned role a new name. If you like, you can assign it a name that indicates the role you want a group of users to perform. You can then edit the user IDs of that group of users to assign them their new role (see Manage users, on page 114). Later, you can edit the roles themselves to give users the privileges you want (see Edit user roles, on page 118).



Note Some API permissions are predefined in the system admin role and remain unchanged in the cloned role. For example, the system admin role includes the default **Read** and **Write** permissions for the **Alarms & Events** API. These permissions are not configurable for both, original, and cloned admin roles.

Follow these steps to clone user roles.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click an existing role.

Step 3 Click  to create a new duplicate entry in the **Roles** table with all the permissions of the original role.

Step 4 Enter a unique name for the cloned role.

Step 5 (Optional) Define the role's settings:

a) Check the check box for every API that the cloned role can access.

b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Edit user roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

Follow these steps to edit user roles.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click and select on an existing role from the left side table. The **Global API Permissions** tab on the right side displays the permission settings for the selected role.

Step 3 Define the role's settings:

a) Check the check box for every API that the role can access.

b) For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write**, and **Delete** permissions pre-selected.

Step 4 When you are finished, click **Save**.

Delete user roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

Follow these steps to delete user roles.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click on the role you want to delete.

Step 3 Click .

Step 4 Click **Delete** to confirm that you want to delete the user role.

Global API permissions

The **Roles** window lets users with the appropriate privileges define custom user roles.

The following table is an overview of the various **Global API Permissions** in Cisco Crosswork Planning.

Table 18: Global API permission categories

Category	Global API permissions	Description
AAA	Password Change APIs	Provides permission to manage passwords. The READ and WRITE permissions are automatically enabled by default. The DELETE permission is not applicable to the password change operation. You cannot delete a password, you can only change it.
	Remote Authentication Servers Integration APIs	Provides permission to manage remote authentication server configurations in Cisco Crosswork Planning. You must have READ permission to view/read configuration, and WRITE permission to add/update the configuration of any external authentication server (for example, LDAP, TACACS) into Cisco Crosswork Planning. The Delete permissions are not applicable for these APIs.
	Users and Roles Management APIs	Provides permission to manage users, roles, sessions, and password policies. Supported operations include "Create new user/role", "Update user/role", "Delete a user/role", "Update task details for a user/role", "Session management (Idle-timeout, max session)", "update password policy", "get password tooltip help text", "get active sessions", and so on. The READ permission allows you to view the content, the WRITE permission allows you to create and update, and the DELETE permission allows you to delete a user or role.
Administrative Operations	Diagnostic Information APIs	
Alarms and Events	Alarms and Events APIs	Allows you to manage system alarms. **Note** The alarms and events associated with the Cisco Crosswork Planning applications are not supported.
Crosswork Planning		

Category	Global API permissions	Description
Platform	Platform APIs	The READ permission allows you to fetch the server status, Cisco Crosswork Planning node information, application health status, collection job status, certificate information, backup and restore job status, and so on. The WRITE permission allows you to • Enable/disable the xFTP server • Manage node information (set the login banner, restart a microservice, and so on) • Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, and so on) • Perform normal/data-only backup and restore operations. • Manage applications (activate, deactivate, uninstall, add package, and so on) The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.
	View APIs	Views Management in Cisco Crosswork Planning Design. The READ permission allows you to see views, the WRITE permission allows you to create/update views, and the DELETE permission will enable delete capabilities.

Manage active sessions

As an administrator, you can monitor and manage the active sessions in the Cisco Crosswork Planning UI, and perform the following actions:

- Terminate a user session
- View user audit log

Attention

- Non-admin users with permission to terminate can terminate their own sessions.
- Non-admin users with read-only permission can only collect the audit log for their sessions.
- Non-admin users without read permissions can't view the Active sessions window.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Active sessions** tab.

The Active sessions tab displays all the active sessions in the Cisco Crosswork Planning with details such as user name, login time, and login method.

Note
The **Source IP** column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork Planning. This option is available in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.

Step 2 To terminate a user session, click the ••• icon under the **Actions** column, and select **Terminate**. A dialog box is displayed to confirm your action. Select **Terminate** to terminate the session.

Attention
- You are recommended to use caution while terminating a session. A user whose session is terminated will not receive any prior warning and will lose any unsaved work.
- Any user whose session is terminated will see the following error message: `"Your session has ended. Log into the system again to continue"`.

Step 3 To view audit log for a user, click the ••• icon under the **Actions** column, and select **Audit log**.

The Audit Log window is displayed for the selected user name. For more information on the Audit Logs, see View audit log, on page 146.

Set up user authentication (TACACS+, LDAP, and RADIUS)

In addition to supporting local users, Cisco Crosswork Planning supports TACACS+, LDAP, and RADIUS users through integration with the TACACS+, LDAP, and RADIUS servers.



Caution Please note that any operation you do following the instructions in this section will affect all new logins to the Crosswork user interface. To minimize session interruption, Cisco recommends that you perform all your external server authentication changes and submit them in a single session.

The integration process has these steps:

- Configure the TACACS+, LDAP, and RADIUS servers.
- Create the roles that are referenced by the TACACS+, LDAP, and RADIUS users.
- Configure AAA settings.
- You can also enable Single Sign-on (SSO) for authentication of TACACS+, LDAP, and RADIUS users. For more information, see Enable Single Sign-on (SSO), on page 133.

Note

- The AAA server page works in bulk update mode wherein all the servers are updated in a single request. It is advised to give write permission for "Remote Authentication Servers Integration API" only to users who have the relevant authorization to delete the servers.
- A user with only Read and Write permissions (without 'Delete' permission) can delete the AAA server details from Cisco Crosswork since delete operations are part of 'Write' permissions. For more information, see Create user roles, on page 117.
- While making changes to AAA servers (create/edit/delete), you are recommended to wait for few minutes between each change. Frequent AAA changes without adequate intervals can result in external login failures.

Manage TACACS+ servers

Cisco Crosswork Planning supports the use of TACACS+ servers to authenticate users.

You can integrate Crosswork with a standalone server (open TACACS+) or with an application such as Cisco ISE (Identity Service Engine) to authenticate using the TACACS+ protocols.

Before you begin

- Configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the TACACS+ server (standalone or Cisco ISE), before configuring the AAA server in Cisco Crosswork Planning. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **TACACS+** tab. From this window, you can add, edit, and delete a new TACACS+ server.

Step 2 **To add a new TACACS+ server**:

a) Click the + icon.

b) Enter the required TACACS+ server information.

Table 19: TACACS+ field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS name	Enter the DNS name (if DNS name is selected). Only IPv4 DNS name is supported.

Field	Description
Port	The default TACACS+ port number is 49.
Shared secret format	Shared secret for the active TACACS+ server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active TACACS+ server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the TACACS+ server.
Service	Enter value of the service that you are attempting to gain access to. For example, "`raccess`". This field is verified only for standalone TACACS+. In case of Cisco ISE, you can enter a junk value. Do not leave the field blank.
Policy ID	Enter the user role that you created in the TACACS+ server. **Note** If you try to log in to Cisco Crosswork Planning as a TACACS+ user before creating the required user role, you will get the error message: "`Key not authorized: no matching policy`". If this occurs, close the browser. Log in as a local admin user and create the missing user roles in the TACACS+ server, and log in back to Cisco Crosswork Planning using the TACACS+ user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the (ISE/Standalone) TACACS+ server attributes. These values can be one or more comma-separated entries. In the TACACS+ context, the Device Access Group attribute is typically a custom or authorization attribute that the TACACS+ server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for TACACS+: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

See the example at the end of this topic for more details.

c) After you enter all the relevant details, click **Add**.

d) Click **Save all changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save changes** to confirm.

Step 3 **To edit a TACACS+ server**:

a) Click the check box next to the TACACS+ server and click .
b) After making changes, click **Update**.

Step 4 **To delete a TACACS+ server**:

a) Click the check box next to the TACACS+ server and click . The Delete *server-IP-address* dialog box opens.
b) Click **Delete** to confirm.

Manage LDAP servers

Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. Cisco Crosswork Planning supports the use of LDAP servers (OpenLDAP, Active Directory, and secure LDAP) to authenticate users. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

To use secure LDAP protocol, you must add **Secure LDAP Communication** certificate before adding the LDAP server. For more details on adding certificates, see Add new certificates, on page 109.

Before you begin

- Configure the relevant parameters (Bind DN, Policy baseDN, Policy ID, and so on) in the LDAP server before configuring the AAA server in Cisco Crosswork Planning.

Procedure

Step 1 From the main menu, choose the **Administration** > **AAA** > **Servers** > **LDAP** tab. Using this window, you can add, edit, and delete a new LDAP server.

Step 2 **To add a new LDAP server**:

a) Click the icon.
b) Enter the required LDAP server details.

Table 20: LDAP field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
Name	Name of the LDAP handler.
IP address/ Host name	LDAP server IP address or host name

Field	Description
Secure connection	Enable the **Secure Connection** toggle button if you want to connect to the LDAP server via the SSL communication. When enabled, select the secure LDAP certificate from the **Certificate** drop-down list. **Note** The secure LDAP certificate must be added in the Certificate Management screen prior to configuring the secure LDAP server. This field is disabled by default.
Port	The default LDAP port number is 389. If Secure Connection SSL is enabled, the default LDAP port number is 636.
Bind DN	Enter the login access details to the database. Bind DN allows user to log in to the LDAP server.
Bind credential / Confirm bind credential	Username and password to login to the LDAP server.
Base DN	Base DN is the starting point used by the LDAP server to search for user authentication within your directory.
User filter	The filter for user search.
DN format	The format used to identify the user in base DN.
Principal l ID	This value represents the UID attribute in the LDAP server user profile under which a particular username is organized.
Policy baseDN	This value represents the role mapping for user roles within your directory.
Policy map attribute	This helps in identifying the user under the policy base DN. This value maps to the `userFilter` parameter in your LDAP server attributes.
Policy ID	The **Policy ID** field corresponds to the user role that you created in the LDAP server. **Note** If you try to log in to Cisco Crosswork Planning as an LDAP user before creating the required user role, you will get the error message: `"Login failed, policy not found. Please contact the Network Administrator for assistance."`. To avoid this error, ensure to create the relevant user roles in the LDAP server, before setting up a new LDAP server in Cisco Crosswork Planning.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the LDAP server attributes. These values can be one or more comma-separated entries. In the LDAP context, the Device Access Group attribute is typically a custom or authorization attribute that the LDAP server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.

Field	Description
Connection timeout	Enter the timeout value. Maximum timeout is 30 seconds.

See the example at the end of this topic for more details.

c) Click **Add**.
d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Step 3 **To edit an LDAP server**:

a) Select the LDAP server and click .
b) After making changes, click **Update**.

Step 4 **To delete an LDAP server**:

a) Select the LDAP server and click .
b) Click **Delete** to confirm.

Example

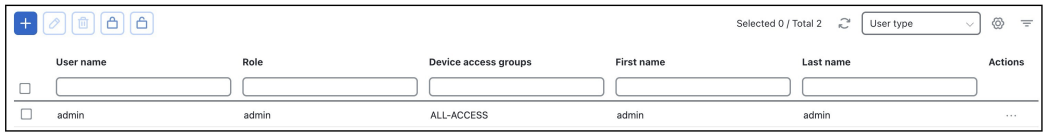
This example shows the parameters that are entered for secure LDAP configuration in Cisco Crosswork Planning. The relevant parameters are configured in the LDAP server.

These are some of the key points:

User settings in the Cisco Crosswork Planning UI

In this example, the existing default user role **admin** is used. You can find this setting on the **Administration** > **Users and Roles** > **Users** page.

- The user name, user role, first name, and last name are set to `admin`.
- The device access group is configured in the LDAP server as `description='ALL-ACCESS'`.



LDAP server details

This section describes the user's LDAP server configuration details.

1. System base DN: ou=system
2. The admin user ‘admin’ has these attributes:
   a. DN: uid=admin,ou=system
   b. password: secret
3. Users group with DN: ou=users,ou=system

4. The admin user John belongs to the ‘users’ group and has these attributes:
   a. DN: uid=john,ou=users,ou=system
   b. password: john
   c. mail: John@test.com
   d. display name: John
   e. description: ALL-ACCESS



Important The description must be equal to the **Device access groups** value for the 'admin' user in Cisco Crosswork Planning (see User settings in the Cisco Crosswork Planning UI, on page 127).

5. The group ‘CpAdmins’ has these attributes:
   a. DN: cn=CpAdmins,ou=groups,ou=system
   b. uniqueMember=uid=john,ou=users,ou=system

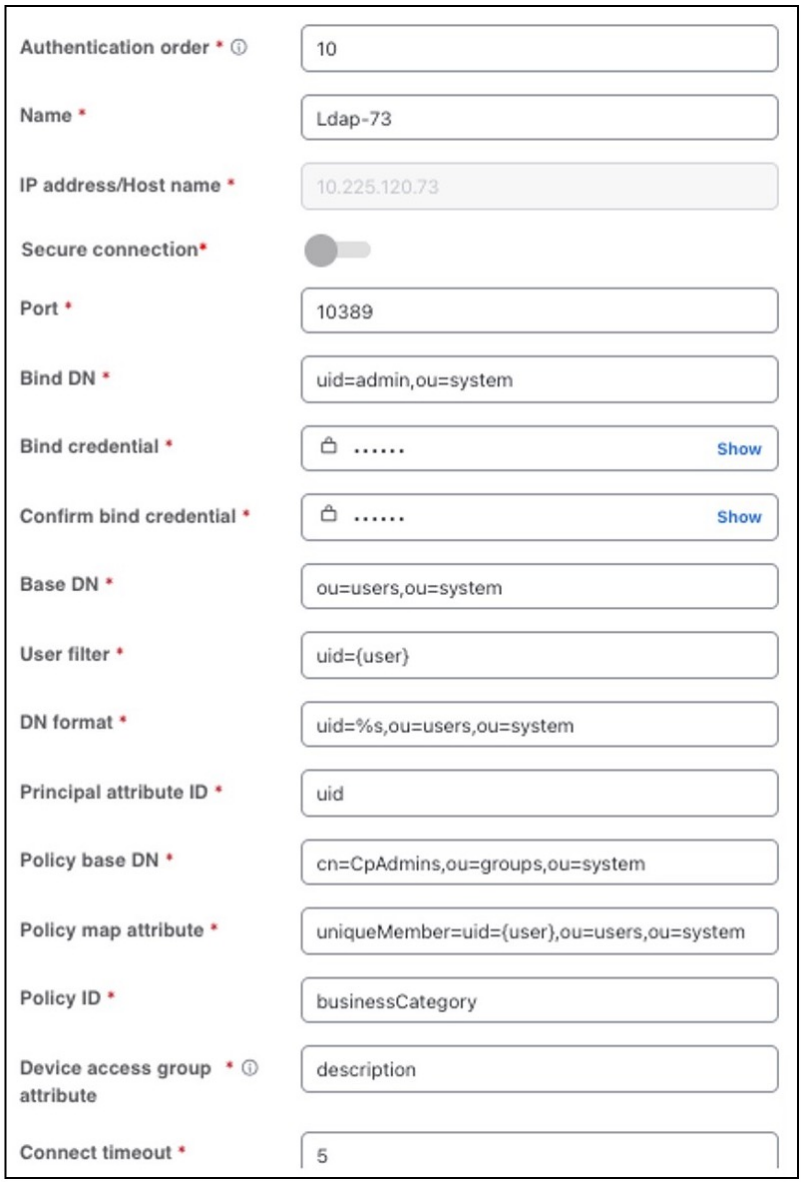
      This indicates the user’s group membership. This value must match with admin user’s DN (see Section 4(a)).
   c. businessCategory: admin

      This indicates the role that needs to be assigned to all users belonging to this group. This value must match with the **Role** value for the admin user in Cisco Crosswork Planning (see User settings in the Cisco Crosswork Planning UI, on page 127).

Corresponding LDAP configuration in the UI

This section describes the corresponding LDAP configuration in the Cisco Crosswork Planning UI.

Figure 31: LDAP configuration in the Cisco Crosswork Planning UI



Parameter	Value
Authentication order	10 (default)
Name	Ldap-73 Custom name for the LDAP configuration of a server.
IP Address/Host name	10.225.120.73 LDAP server IP address.

Parameter	Value
Port	10389 LDAP server port.
Bind DN	uid=admin,ou=system Admin user DN, as described in Section 2(a).
Bind credential	secret Admin user password, as described in Section 2(b).
Confirm bind credential	secret Admin user password, as described in Section 2(b).
Base DN	ou=users,ou=system The user's group DN for *authentication* from where the users must be searched, as described in Section 3.
User filter	uid={user} User search filter attribute 'uid', as described in Section 4.
DN format	uid=%s,ou=users,ou=system User's DN format, as described in Section 4.
Principal attribute ID	uid As described in Section 4.
Policy base DN	cn=CpAdmins,ou=groups,ou=system The group that has the role mapping attribute (admin) and under which the users will have group membership, as described in Section 5(a).
Policy map attribute	uniqueMember=uid={user},ou=users,ou=system The user's group membership attribute under the 'CpAdmins' user group (Policy base DN), as described in Section 5(b).
Policy ID	businessCategory The user role attribute (admin) under the 'CpAdmins' group (Policy base DN), as described in Section 5(c). This value must match with the CpAdmins group's attribute having 'admin' value.
Device access group attribute	description The device group attribute under the user DN, as described in Section 4(e). This value must match with the user DN attribute having value 'ALL-ACCESS'.

Manage RADIUS servers

Crosswork supports the use of RADIUS (Remote Authentication Dial-In User Service) servers to authenticate users. You can also integrate Crosswork with an application such as Cisco ISE (Identity Service Engine) to authenticate using the RADIUS protocols.

Before you begin

- Similar to TACACS+ server, you must configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the RADIUS server before configuring the AAA server in Cisco Crosswork Planning. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **RADIUS** tab. From this window, you can add, edit, and delete a new RADIUS server.

Step 2 **To add a new RADIUS server**:

a) Click the + icon.

b) Enter the required RADIUS server information.

Table 21: RADIUS field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the RADIUS server (if IP address is selected).
DNS name	Only IPv4 DNS name is supported (if DNS name is selected).
Port	The default RADIUS port number is 1645.
Shared secret format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active RADIUS server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Cisco Crosswork Planning to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the RADIUS server.
Service	Enter value of the service that you are attempting to gain access to. For example, "`raccess`".

Field	Description
Policy ID	The **Policy Id** field corresponds to the user role that you created in the RADIUS server. **Note** If you try to login to Cisco Crosswork Planning as a RADIUS user before creating the required user role, you will get the error message: `"Key not authorized: no matching policy"`. If this occurs, close the browser. Log in as a local admin user and create the missing user roles in the RADIUS server, and log in back to Cisco Crosswork Planning using the RADIUS user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the RADIUS server attributes. These values can be one or more comma-separated entries. In the RADIUS context, the Device Access Group attribute is typically a custom or authorization attribute that the RADIUS server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for RADIUS: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

As RADIUS configuration is very similar to TACACS+, please refer to the detailed example in the Manage TACACS+ servers, on page 123 for more information.

c) After you enter all the relevant details, click **Add**.
d) Click **Save all changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save changes** to confirm.

Step 3 **To edit a RADIUS server**:

a) Click the checkbox next to the RADIUS server and click .
b) After making changes, click **Update**.

Step 4 **To delete a RADIUS server**:

a) Click the checkbox next to the RADIUS server and click . The Delete *server-IP-address* dialog box opens.
b) Click **Delete** to confirm.

Enable Single Sign-on (SSO)

Single Sign-on (SSO) is an authentication method that allows you to log in with a single ID and password to any of several related, yet independent, software systems. It allows you to log in once and access the services without reentering authentication factors. Cisco Crosswork acts as Identity Provider (IDP) and provides authentication support for the relying service providers. You can also enable SSO for authentication of TACACS+, LDAP, and RADIUS users.

Crosswork supports SSO cross-launch to enable easier navigation with the service provider. Once configured, the URL can be launched using the launch icon ( ) located at the top right corner of the window.

Attention

- When Crosswork is re-installed or migrated, you must ensure that the latest IDP metadata from Crosswork is updated to the service provider applications. Failing to do this will result in authentication failure due to mismatched metadata information.
- First-time login users cannot switch to using a different username before mandatorily changing the password. The only workaround is for the administrator to terminate the session.

Note The Cisco Crosswork Planning login page is not rendered when the Central Authentication Service (CAS) pod is restarting or not running.

Before you begin

Ensure that the **Enable source IP for auditing** check box is selected in the **Administration** > **AAA** > **Settings** page.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **SSO**. The **Identity Provider** window is displayed. Using this window, you can add, edit settings, and delete service providers.

Step 2 **To add a new service provider**:

a) Click the icon.

b) In the **Service Provider** window, enter the values in the following fields:

- **Name**: Enter the name of the service provider entity.

  Note
  If a URL is provided, the **Service name** column entry in the **Identity Provider** window becomes a hyperlink.

- **Evaluation Order**: Enter a unique number which indicates the order in which the service definition should be considered.
- **Metadata**: Click the field, or click **Browse** to navigate to the metadata XML document that describes a SAML client deployment. You can also enter the service provider URL here for cross-launch.

Step 3 Click **Add** to finish adding the service provider.

Step 4 Click **Save all changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save changes** to confirm.

After the settings are saved, when you log into the integrated service provider application for the first time, the application gets redirected to the Cisco Crosswork server. After providing the Crosswork credentials, the service provider application logs in automatically. For all the subsequent application logins, you do not have to enter any authentication details.

Step 5 **To edit a service provider:**

a) Click the check box next to the service provider and click . You can update the Evaluation Order and Metadata values as required.
b) After making changes, click **Update**.

Step 6 **To delete a service provider**:

a) Click the check box next to the service provider and click .
b) Click **Delete** to confirm.

Configure AAA settings

Users with relevant AAA permissions can configure the AAA settings.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **Settings**.

Step 2 Select the relevant setting for **Fallback to Local**. By default, Cisco Crosswork Planning prefers external authentication servers over local database authentication.

Note
Admin users are always authenticated locally.

Step 3 Select the relevant value for the **Logout all idle users after** field. Any user who remains idle beyond the specified limit will be automatically logged out.

Note
The default timeout value is 30 minutes. If the timeout value is adjusted, the page will refresh to apply the change.

Step 4 Enter relevant values in the **Number of parallel sessions** and **Number of parallel sessions per user** fields.

Note
Crosswork supports between 5 to 200 parallel sessions for concurrent users. If the number of parallel sessions is exceeded, an error is displayed while logging in to Crosswork.

Note
Crosswork supports 50 simultaneous NBI sessions up to 400 sessions.

Step 5 Check the **Enable source IP for auditing** check box to log the IP address of the user (source IP) for auditing and accounting. This check box is disabled by default. Once you enable this option and relogin to Cisco Crosswork Planning, you will see the **Source IP** column on the **Audit Log** and **Active Sessions** pages.

Step 6 Select the relevant settings for the **Local password policy**. Certain password settings are enabled by default and cannot be disabled (for example, Change password on first login).

Note
Any changes in the password policy are enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

Note
Local password policy allows administrators to configure the number of unsuccessful login attempts a user can make before they are locked out of Cisco Crosswork Planning, and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

Monitor system and application health

The Cisco Crosswork Platform is built on an architecture consisting of microservices. Due to the nature of these microservices, there are dependencies across various services within the Crosswork system. The system and applications are considered Healthy if all services are up and running. If one or more services are down, then the health is considered Degraded. If all services are down, then the health status is Down.

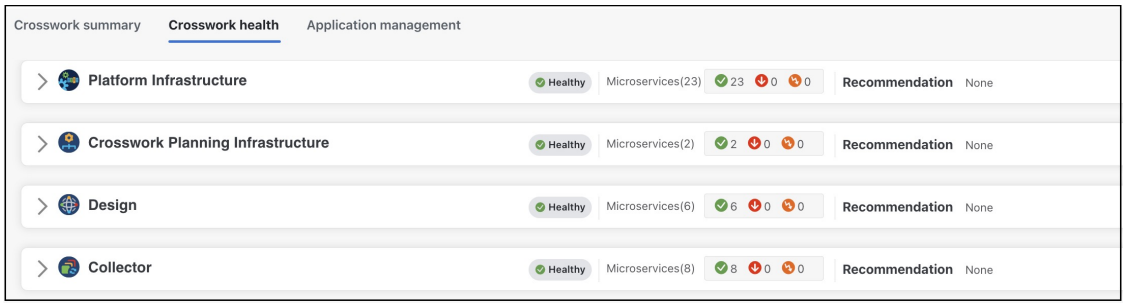
From the main menu, choose **Administration** > **Crosswork Manager** to access the **Crosswork summary** and **Crosswork health** windows. Each window provides various views to monitor system and application health. It also supplies tools and information that, with support and guidance from your Cisco Customer Experience account team, you can use to identify, diagnose, and fix issues with the Cisco Crosswork, Platform Infrastructure, and installed applications.

While both windows can give you access to the same type of information, the purpose of each summary and view is different.

Monitor platform infrastructure and application health

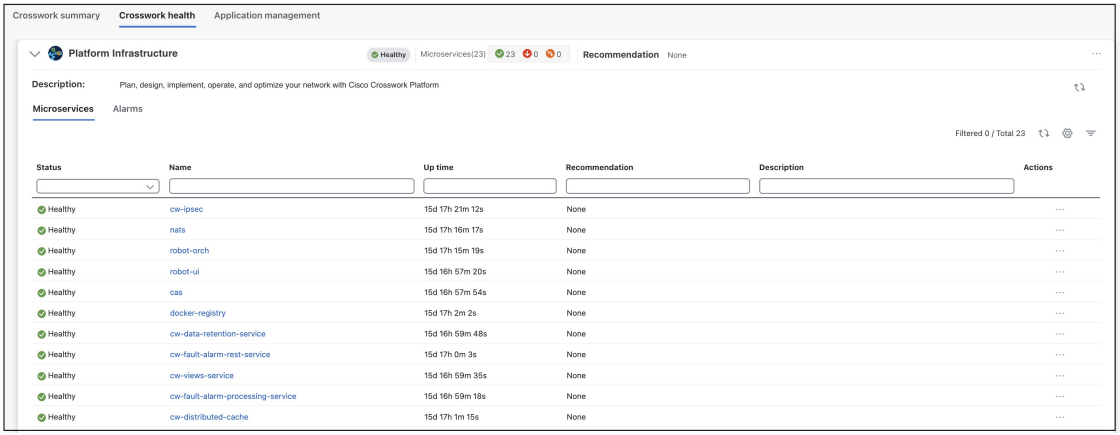
The **Crosswork health** window (**Administration** > **Crosswork Manager** > **Crosswork health** tab) provides health summaries for the Cisco Crosswork Platform Infrastructure and installed applications with the addition of microservice status details.

Figure 32: Crosswork health tab



Within this window, expand an application row to view Microservice and Alarm information.

Figure 33: Microservices tab



From the **Microservices** tab:

- View the list of microservices and, if applicable, associated microservices by clicking on the microservice name.
- Click ••• to restart or obtain Showtech data and logs per microservice.

Note Showtech logs must be collected separately for each application.

From the **Alarms** tab, you can:

- Filter the active alarms.
- Click the alarm description to drill down on alarm details.
- Change status of the alarms (Acknowledge, Unacknowledge, Clear).
- Add notes to alarms.
- View list of events in the product.
- View the correlated alarm for each event.

Check system health example

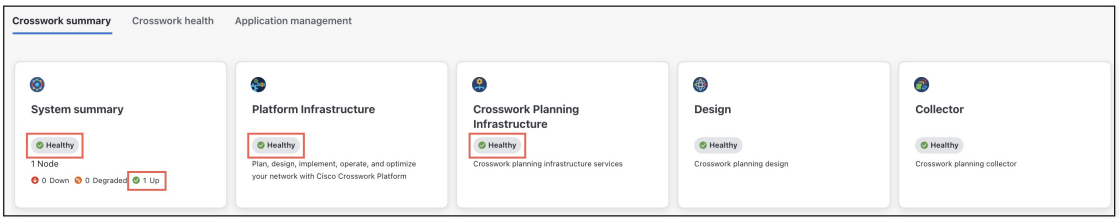
In this example, we navigate through the various windows and what areas should be checked for a healthy Crosswork system.

Procedure

Step 1 Check overall system health.

a) From the main menu, choose the **Administration** > **Crosswork Manager** > **Crosswork summary** tab.
b) Check that all the nodes are in Operational state (Up) and that the System Summary, Platform Infrastructure, and Crosswork Planning Infrastructure are Healthy.

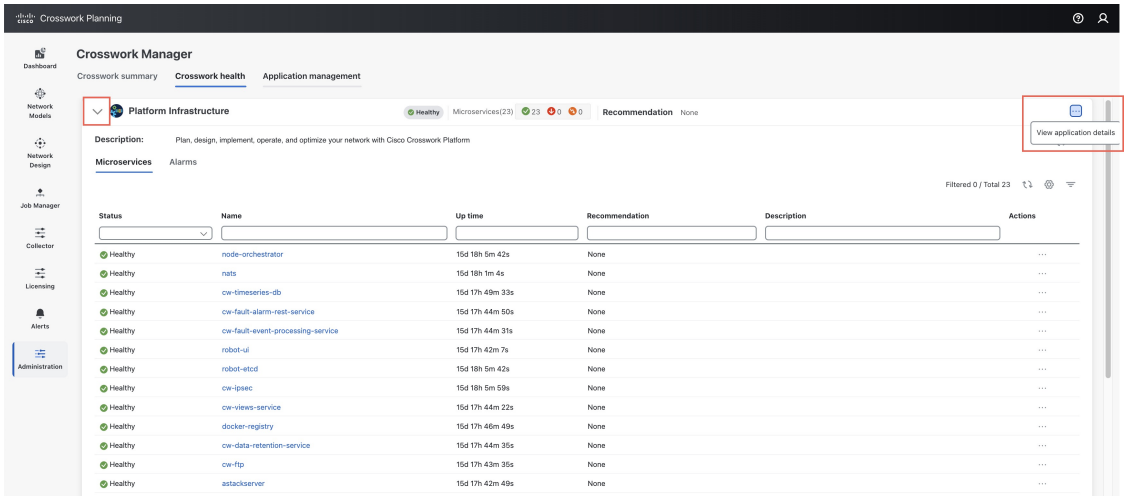
Figure 34: Crosswork summary tab



Step 2 Check and view detailed information about the microservices that are running as part of the Crosswork Platform Infrastructure.

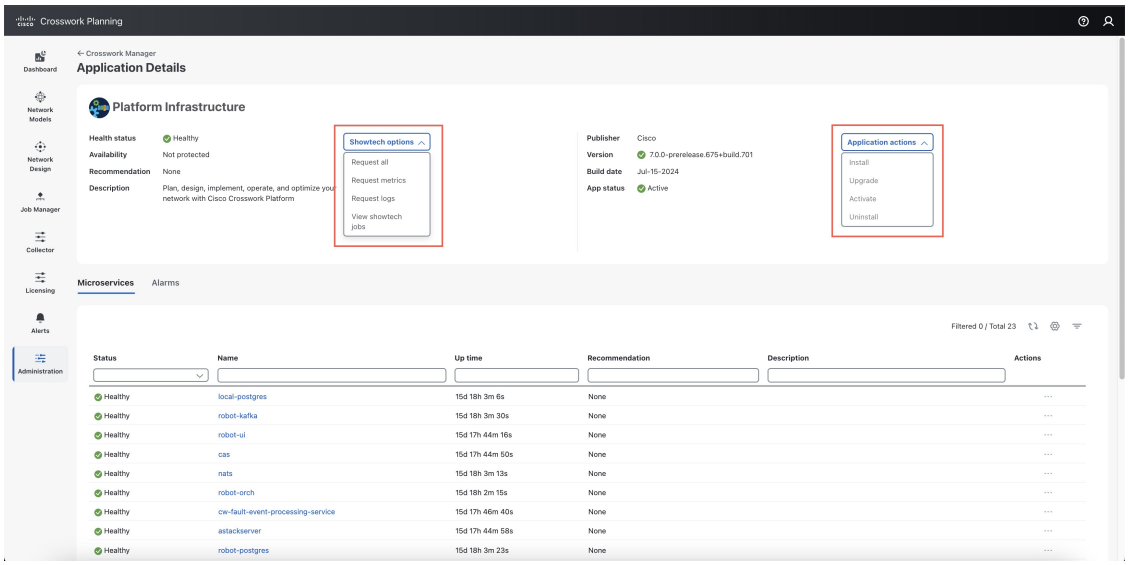
a) Click the **Crosswork health** tab.
b) Expand the Crosswork Platform Infrastructure row, click ***, and select **View application details**.

Figure 35: Crosswork health tab



c) From the Application Details page, you can check and review microservice details, restart microservices, and collect showtech information. You can also perform installation-related tasks from this window.

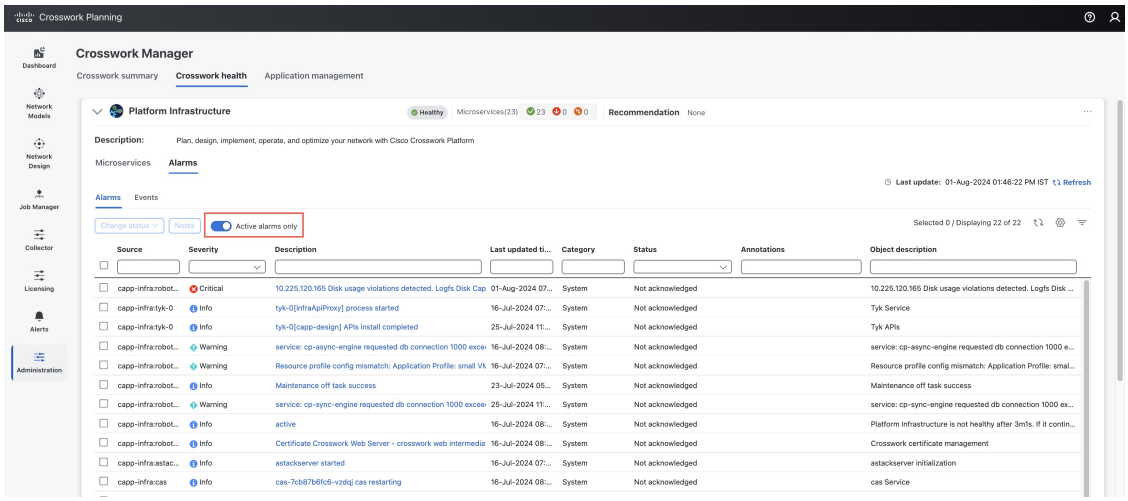
Figure 36: Application Details page



Step 3 Check and view the alarms and events related to the microservices.

a) Click the **Alarms** tab. The list only displays Crosswork Platform Infrastructure alarms. You can further filter the list by viewing only active alarms.

Figure 37: Alarms tab

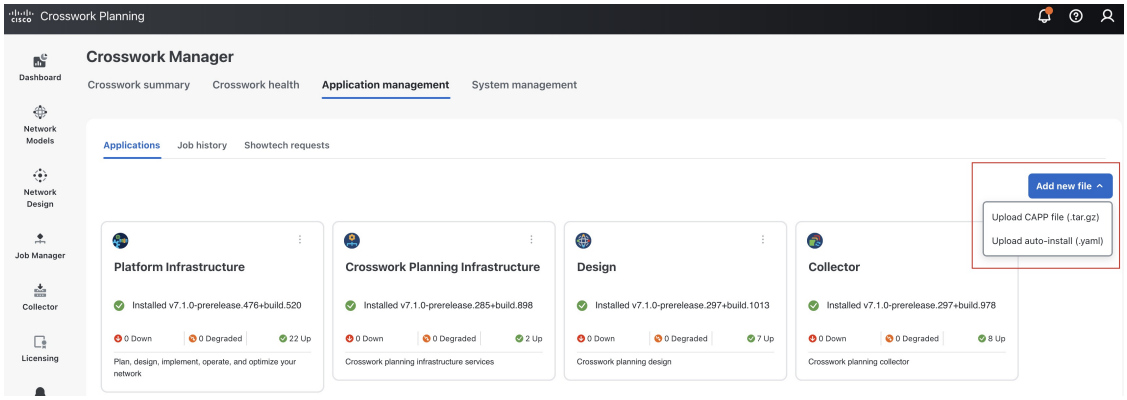


b) Click the **Events** tab. The list displays all Crosswork Platform Infrastructure events, and their correlated alarms.

Step 4 View which Crosswork applications are installed.

a) From the main menu, choose **Administration** > **Crosswork Manager** > **Application management** tab and click **Applications**. This page displays all applications that have been installed. You can also click **Add new file** to install more applications by uploading another application bundle or an auto-install file.

Figure 38: Application management window



Step 5 View the status of jobs.

a) Click the **Job History** tab. This window provides the information regarding the status of jobs and the sequence of events that have been executed as part of the job process.

Manage backups

Backup and restore overview

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

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

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

Table 22: Backup and restore options

Menu option	Description
Actions > Data backup (See Manage backup and restore, on page 140 for details)	Preserves the Cisco Crosswork Planning configuration data. The backup file can be used with the data disaster restore (Restore Cisco Crosswork Planning after a disaster, on page 143) to recover from a serious outage.
Actions > Data disaster restore (See Restore Cisco Crosswork Planning after a disaster, on page 143 for details)	Restores the Cisco Crosswork Planning configuration data after a natural or human-caused disaster has required you to rebuild a Cisco Crosswork Planning server.

Menu option	Description
Actions > Data migration (see Migrate data using backup and restore, on page 144 for details)	Migrates data from an older version of Cisco Crosswork Planning to a newer version.

Manage backup and restore

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



Attention

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

When creating or restoring backups for Cisco Crosswork Planning, follow these guidelines:

- Configure a destination SCP server for storing backup files during your first login. This is a one-time setup and must be completed before taking backups or initiating restore operations.
- Perform backup or restore operations during a scheduled maintenance window. You should not access the system during these operations. Backups will take the system offline for about 10 minutes, while restore operations can be lengthy and pause other applications, affecting data-collection jobs.
- Use the same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- Use the dashboard to monitor the progress of backup or restore processes. Avoid using the system during these processes to prevent errors or incorrect content.
- Only one backup or restore operation can run at a time.
- Ensure both Cisco Crosswork Planning and the SCP server are in the same IP environment (for example, both using IPv6).
- Delete older backups to save space on the backup server, though they may still appear in the job list.
- Operators making frequent changes should back up more often (possibly daily), while others might back up weekly or before major system upgrades.

- By default, backups are not allowed if the system is not considered healthy, but this can be overridden for troubleshooting purposes.
- If using collector agents, manually restart them, as they may remain in a stopped state after the backup and restore operation.

Before you begin

Before you begin, ensure that you have:

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

Procedure

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

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

Step 2 **Create a backup:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data backup** to display the **Data Backup** drawer panel with the destination server details pre-filled.
c) Provide a relevant name for the backup in the **Job name** field.
d) If the VM or any of the applications are not in Healthy state, but you want to create the backup, check the **Force** check box.

Note
The **Force** option must be used only after consultation with the Cisco Customer Experience team.

e) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host name**, **Port**, **Username**, **Password** and **Server path/Location** fields to specify a different destination.

f) (Optional) Click **Verify backup readiness** to verify that Cisco Crosswork Planning has enough free resources to complete the backup. If the check is successful, Cisco Crosswork Planning displays a warning about the time-consuming nature of the operation. Click **OK** to continue.

If the verification is unsuccessful, contact the Cisco Customer Experience team for assistance.

g) Click **Backup** to start the backup operation. Cisco Crosswork Planning creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.

h) To view the progress of a backup job, enter the job details (such as Status or Job Type) in the search fields in the **Backup restore job sets** table. Then, click on the job set you want.

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

Note
After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.

Note
If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

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

Note
Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task `uploadBackupToRemote`). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

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

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

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

Recommendation: Post-restore actions

After the restore process completes, ensure these actions are performed to resume normal system operations:

Editing collections

After restoring the backup, navigate to the **Collector** > **Collections** page and perform the Edit collection operation on each listed collection. Save the collections without making any changes. This ensures that the configuration data is properly updated.

Restarting agents

The restore process only copies the database and file system data. Once the restore process completes, all agents will be in a stopped state, and you must restart them manually from the Cisco Crosswork Planning UI.

- Restart the NetFlow and SR-PCE agents using the **Start** option for the respective agent in the **Setup Agent** page (**Collector** > **Agents**). For more information, see Agent operations, on page 29.
- Restart the traffic poller agent by disabling and then enabling the **Traffic collection** option on the Traffic collector configuration page. For more information, see Collect traffic statistics, on page 78.

Executing schedulers

- If using a "Run now" scheduler, execute the scheduler manually.
- If the scheduler has a CRON job configured, then the scheduler triggers automatically based on the CRON job configuration.

Restore Cisco Crosswork Planning after a disaster

A disaster recovery is a restore operation that you use after a natural or human-caused disaster has destroyed a Cisco Crosswork Planning server. You must deploy a new server first, following the instructions in *Cisco Crosswork Planning 7.1 Installation Guide*.

To perform a disaster recovery:

Before you begin

- Obtain the full name of the backup file you want to use in your disaster recovery from the SCP backup server. Typically, this will be the most recent backup file you have created. Cisco Crosswork Planning backup file names typically follow this format:

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

  Where:

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

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

- Install the exact versions of the applications that were present in your old Cisco Crosswork Planning server when the data backup was made. Any version mismatch can lead to data loss and restore job failure.
- Use the same Cisco Crosswork Planning software image that was used when creating the backup. You cannot restore the cluster using a backup created with a different software version.
- Keep your backups up-to-date to ensure you can recover the system's true state as it existed before the disaster. If you have installed new applications or patches since your last backup, take another backup.
- If the disaster recovery fails, contact Cisco Customer Experience.
- Smart Licensing registration for Crosswork applications are not restored during a disaster restore operation, and must be registered again.

Procedure

Step 1 From the main menu of the newly deployed Cisco Crosswork Planning server, choose **Administration** > **Backup and Restore**.

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

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

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

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

Migrate data using backup and restore

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

Follow these guidelines whenever you create a data migration backup:

- Ensure that you have configured a destination SCP server to store the data migration files. This configuration is a one-time activity.
- Both the Cisco Crosswork Planning and the SCP server must be in the same IP environment. For example, if Cisco Crosswork Planning is communicating over IPv6, so must the backup server.
- We recommend that you create a data migration backup only when upgrading your Cisco Crosswork Planning installation, and that you do so during a scheduled upgrade window only. Users shouldn't attempt to access Cisco Crosswork Planning while the data migration backup or restore operations are running.

Before you begin

Ensure that you have

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

Procedure

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

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

Step 2 **Create a backup:**

a) Log in as an administrator to the Cisco Crosswork Planning installation whose data you want to migrate to another installation.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data backup** to display the **Data Backup** dialog box with the destination server details prefilled.

d) Provide a relevant name for the backup in the **Job Name** field.
e) If you want to create the backup despite any microservice issues, check the **Force** check box.
f) Complete the remaining fields as needed.

   If you want to specify a different remote server upload destination: Edit the pre-filled **Host name**, **Port**, **Username**, **Password** and **Server path/Location** fields to specify a different destination.

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

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

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

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

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

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

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

View system and network alarms

You can view alarms by navigating to one of the following:

- From the main menu, choose **Alerts** > **Alarms and Events**.
- For application specific alarms, choose **Administration** > **Crosswork Manager** > **Crosswork Health** tab. Expand one of the applications and select the **Alarms** tab.

  From the **Alarms** tab, you can:

  - Click the alarm description to drill down on alarm details.
  - Change the status of the alarms (Acknowledge, Unacknowledge, Clear). Select the alarm and select the required status from the **Change status** drop-down.
  - Add notes to alarms. Select the alarm and click the **Notes** button.

View audit log

The **Audit Log** window tracks the following AAA-related events:

- Create, update, and delete users
- Create, update, and delete roles
- User login activities - login, logout, login failure due to maximum active session limit, and account locked due to maximum login failures.
- Source IP - IP address of the machine from where the action was performed. This column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork Planning. This check box is available in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.
- Password modification by user

To view the audit log, perform the following steps:

Procedure

Step 1 From the main menu, choose **Administration** > **Audit Log**.

The Audit Log window is displayed.

Step 2 Click to filter the results based on your query.

Using the export icon ( ), you can export the log in the CSV format. When exporting the CSV, you have the option to use the default file name or enter a unique name.

Set the pre-login disclaimer

Many organizations require that their systems display a disclaimer message in a banner before users login. The banner reminds the authorized users of their obligations when using the system, or provides warnings to unauthorized users. You can enable such a banner for Cisco Crosswork Planning users, and customize the disclaimer message as needed.

Procedure

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

Step 2 Under **Notifications**, click the **Pre-login disclaimer** option.

Step 3 To enable the disclaimer and customize the banner:

a) Check the **Enable** check box.

b) Customize the banner **Title**, the **Icon**, and the **Disclaimer text** as needed.

c) (Optional) Check the **Enable** check box under **Require user consent** to prompt the user to agree to the disclaimer before they log in.
d) (Optional) While editing the disclaimer, you can:
   - Click **Preview** to see how your changes look when displayed before the Crosswork login prompt.
   - Click **Discard changes** to revert to the last saved version of the banner.
   - Click **Reset to default** to revert to the original, default version of the banner.
e) When you are satisfied with your changes, click **Save** to save them and enable display of the custom disclaimer to all users.

Step 4 To turn off the disclaimer display, select **Administration** > **Settings** > **Pre-login disclaimer**, then uncheck the **Enable** check box.

Manage maintenance mode settings

The maintenance mode provides a means for shutting down the Cisco Crosswork Planning system temporarily. Cisco Crosswork Planning synchronizes all application data before the shutdown. It can take several minutes for the system to enter maintenance mode and to restart when maintenance mode is turned off. During these periods, you should not attempt to log in or use the Cisco Crosswork Planning applications.

⚠

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

Procedure

Step 1 To put Crosswork in maintenance mode:
a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.
b) Drag the **Turn on/off maintenance** slider to the right, or On position.
c) You will receive a warning message that the system is about to enter maintenance mode. Click **Continue** to confirm your choice.

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

Step 2 To restart from maintenance mode:
a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.
b) Drag the **Turn on/off maintenance** slider to the left, or Off position.

Note

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

Update network access configuration

The **Network access configuration** section specifies the parameters used for network access through SNMP, Login, and the SAM interface. These parameters can be modified to meet your specific requirements. For example, you can update the SNMP timeout value according to your needs.

Caution Before you edit, be aware that your changes will be applied globally and will affect all collections, jobs, and plan files.

To edit the network access configuration, do the following:

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Collection settings** > **Network access configuration**.

Step 2 Click the **Edit** button. An alert window appears informing that modifying the configuration to disable the required service results in collection failure. If you are changing only the timeout and other parameters, click **Confirm**.

The page turns editable.

Step 3 Edit the file as per your requirement.

Step 4 Click **Save** to save the changes.

Download the network access configuration file:

To download the network access configuration file to your local machine, click .

Update collector capability

Each collector's data source and the tables/columns into which they are populating the data are available in the **Collector capability** page. In Cisco Crosswork Planning, you can update these configurations as per your requirement.

Caution Before you update, be aware that your changes will be applied globally and will affect all collections, jobs, and plan files.

The collector's table and column details are configured using the following format:

Collector.table.table-name=ALL/Column list

where ALL indicates that the collector populates all columns in that table. If the collector populates only a subset of columns, then it is specified as a list of column names separated by commas.

Follow these steps to update the default configurations.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Collection settings** > **Collector capability**.

Step 2 Click the **Edit** button.

The page turns editable.

Step 3 Edit the .txt file as per your requirement.

Step 4 Click **Save** to save the changes.

Download the collector capability configurations

To download the collector capability configurations to your local machine, click .

Reset to default configurations

To reset the configurations to the default values, click **Reset default config** button at the top right.

Configure aging

By default, when a circuit, port, node, or link disappears from a network, it is permanently removed and must be rediscovered. To configure how long Cisco Crosswork Planning retains these elements that have disappeared before they are permanently removed from the network, complete the following steps.



Caution Before you configure, be aware that your changes will be applied globally and will affect all collections, jobs, and plan files.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** > **Collection Settings** > **Purge delay**.

Step 2 Check the **Enable** check box to enable aging.

Step 3 Enter the values in the relevant fields:

- **L3 port**—Enter the time duration for which an L3 port must be kept in the network after it becomes inactive.
- **L3 node**—Enter the time duration for which an L3 node must be kept in the network after it becomes inactive.

- **L3 circuit**—Enter the time duration for which an L3 circuit must be kept in the network after it becomes inactive.

Note
The value of **L3 node** must be greater than or equal to **L3 port** which in turn must be greater than or equal to **L3 circuit**.

Configure purging of archived plan files

The archived plan files are periodically deleted in Cisco Crosswork Planning to conserve storage space. By default, the files are retained for 30 days.

Follow these steps to configure the retention period (in days) as per your requirement.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Collection settings** > **Archive purge**.

Step 2 In the **Archive retention** field, enter the number of days after which the files can be deleted.

For example, if you enter 40 in this field, the plan files older than 40 are deleted.

Step 3 Click **Save** to save the changes.

Note Uncheck the **Enable** check box to disable the purging of archived plan files. Be aware that if you disable it, storage space will eventually run out.

Configure static routes

Static routes are used to reach the devices in a different subset reachable via the data interface.

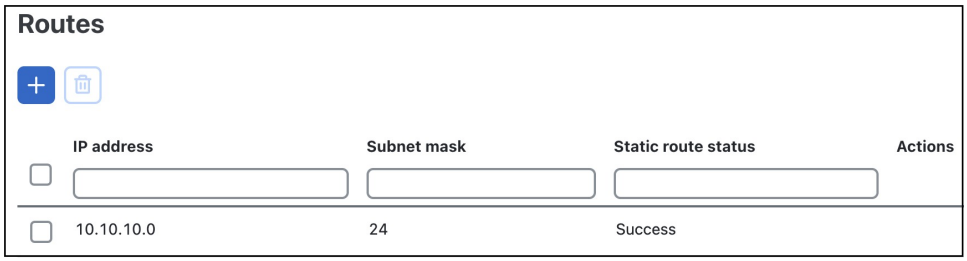
Note After static routes are applied, their corresponding entries will appear when you run the **ip rule list** command at the Crosswork shell prompt.

Add static routes

Follow these steps to add static routes.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Device connectivity management** > **Routes**.



Step 2 Click . The Add Route IP window appears.

Step 3 Enter the valid IPv4 or IPv6 subnet in CIDR format.

Step 4 Click **Add**.

Delete static routes

Follow these steps to delete static routes.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Device connectivity management** > **Routes**.

Step 2 Select the static route you want to delete and click .

Step 3 Click **Delete** in the confirmation window.