Cisco Crosswork Planning 7.0 Collection Setup and Administration

First Published: 2024-08-30

Last Modified: 2025-05-21

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.

CONTENTS

CHAPTER 1

CHAPTER 2

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 the following topics:

Introducing Cisco Crosswork Planning

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

Cisco Crosswork Planning provides tools to create and maintain a model of the current network through the continual monitoring and analysis of the network, and the traffic demands that are placed on it. At a 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.

These are some of the important features of Cisco Crosswork Planning.

- 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.

Cisco Crosswork Planning comprises the following two components. These components run independently of each other and you can enable/disable them based on your requirements.

- **Cisco Crosswork Planning Collector**

  Cisco Crosswork Planning Collector consists of a set of services that create, maintain, and archive a model of the current network through continual monitoring and analysis of the network, and the traffic demands that are placed on it.

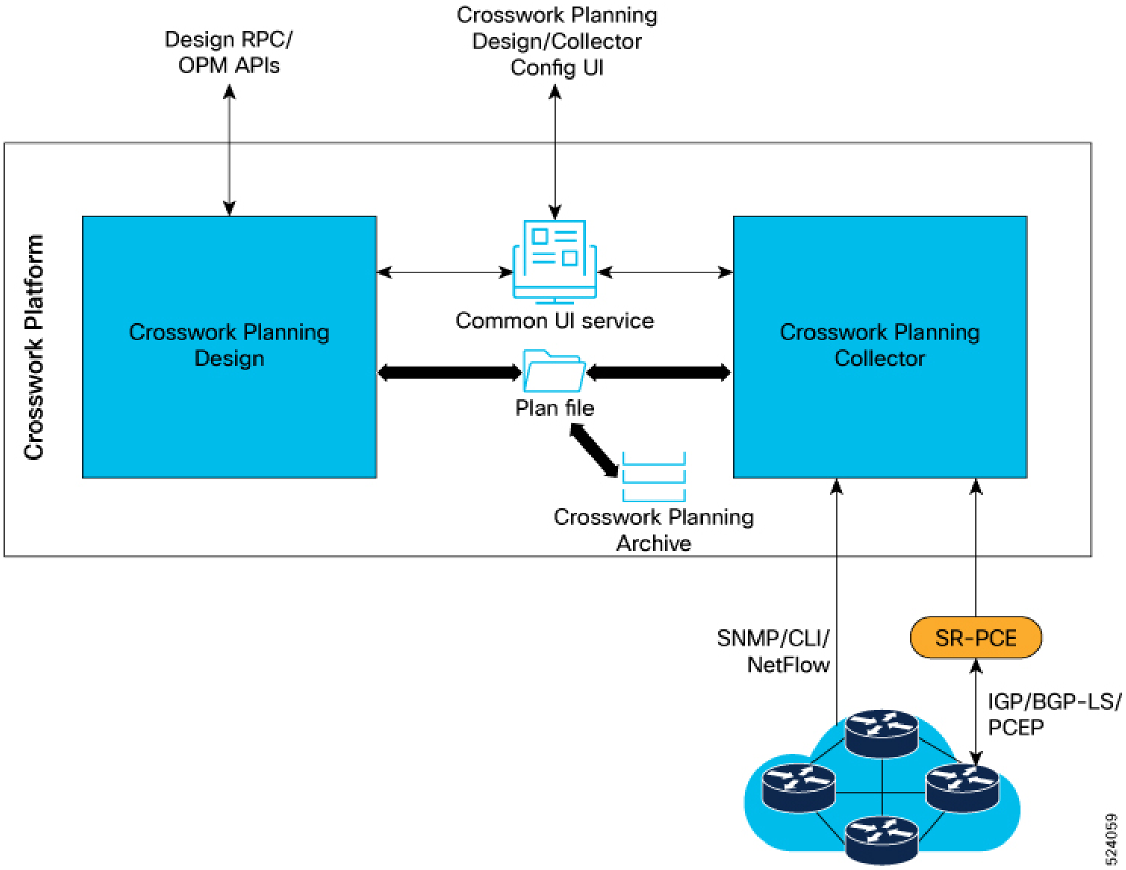
- **Cisco Crosswork Planning Design**

  Cisco Crosswork Planning Design is a network design and planning tool that 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 Crosswork infrastructure. The Cisco Crosswork Planning Design and Cisco Crosswork Planning Collector applications are packaged as separate components and can be enabled/disabled as per your requirements. 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 in Cisco Crosswork Planning

A *Collector* is a package that populates parts of the abstract network model, querying the network to do so. Most collectors operate as follows:

1. They read a *source network model* (or simply, a *source model*).
2. They augment the source model with information obtained from the actual network.
3. They produce a *destination network model* (or simply, a *destination model*) with the resulting model.

Cisco Crosswork Planning includes several different collectors, such as:

- **Topology Collectors**—Populates a basic network model with topology information (nodes, interfaces, circuits) based on the discovered IGP database augmented by SNMP queries and SR-PCE. The topology collectors do not have a source model.
- **LSP Collector**—Augments a source model with LSP information, producing a destination model with the extra information.
- **Traffic Collector**—Augments a source model with traffic statistics polled from the network, producing a new destination model with extra information.

- **Layout Collector**—Adds layout properties to a source model to improve visualization. It produces a new destination model with the extra layout information. The collector records changes to the layout properties, so when the source model changes and the destination model is updated, the layout properties in the destination model are updated accordingly.

For a comprehensive list of all the collectors supported in Cisco Crosswork Planning, see Collector Descriptions, on page 47.

Network Models and Plan File

Cisco Crosswork Planning Collector application produces *network models*, which can be built from an actual network by combining information from different collectors. A *model building chain* is an arrangement of collectors organized in such a way as to produce a network model with the desired information. The network model is saved in a *plan file* (.pln format) which can be viewed or downloaded from the Cisco Crosswork Planning Design application.

Aggregation of Collectors

In Cisco Crosswork Planning, two levels of data aggregation (consolidation) happens with the help of following aggregators:

- Delta Aggregation Rules Engine (DARE), on page 4
- Simple Aggregation Engine (SAgE), on page 4

For more details, see the following topics:

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. Primarily DARE consolidates all topology collectors' data.

Simple Aggregation Engine (SAgE)

Simple Aggregation Engine (SAgE) 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. The network information from all the collectors is written into plan files. The network changes can be archived from SAgE.

SAgE aggregator enables to run 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 38.

Generation of Network Models

Network models are generated on completion of each level of aggregation. First model is generated as the output of DARE aggregation (see Delta Aggregation Rules Engine (DARE), on page 4). This file is used by the components such as traffic, inventory, layout, netflow, demands as data source. Once the SAgE aggregation completes (see Simple Aggregation Engine (SAgE), on page 4), it generates the second file, the final network model, which is the final output of the aggregated collected data.

Log In and Log Out

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 7.0 Installation Guide*.

After installing Cisco Crosswork Planning, you can access the Cisco Crosswork Planning UI using the following steps.

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

Step 2 The Cisco Crosswork Planning's browser-based user interface displays the login window. Enter your username and password. The default administrator user name and password is **admin**. This account is created automatically at installation. The initial password for this account must be changed during installation verification. Cisco strongly recommends that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user roles with appropriate privileges and assign new users to those roles. At least one of the users you create should be assigned the "administrator" role.

Step 3 Click **Login**.

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

Note
Logging out while working on a plan file does not result in closing of the file; it remains open.

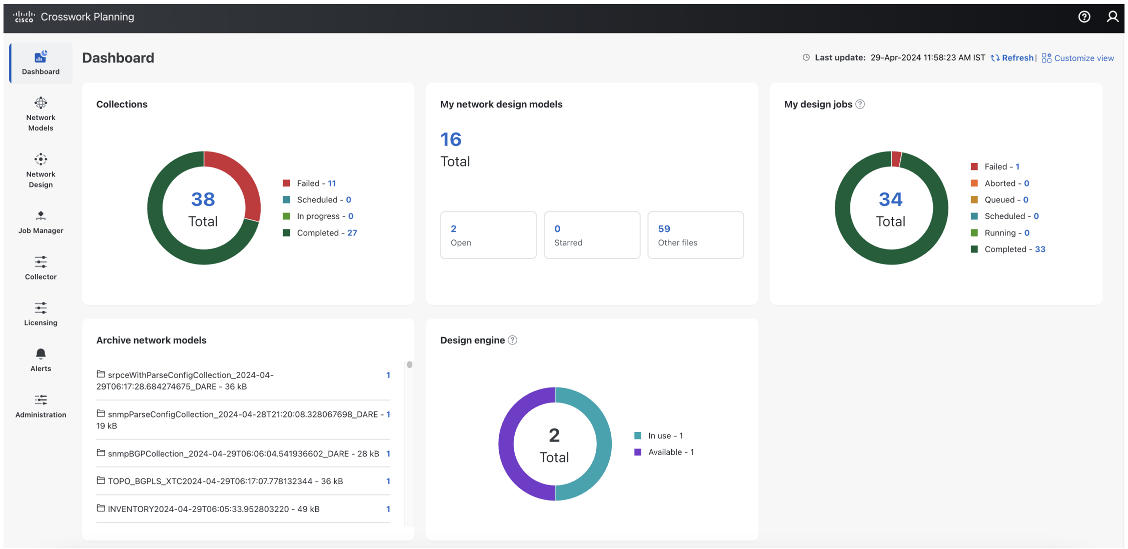
Dashboard

After successful login, the Dashboard page opens. The Dashboard page provides an at-a-glance operational summary of Cisco Crosswork Planning. The dashboard is made up of a series of dashlets. The dashlets included in your dashboard depend on which Cisco Crosswork Planning application is installed. For example, the **Collections** and **Archive network models** dashlets are displayed only if you have installed the Cisco Crosswork

Planning Collector application. The **My network design models**, **My design jobs**, and **Design engine** dashlets are displayed only if you have installed the Cisco Crosswork Planning Design application.

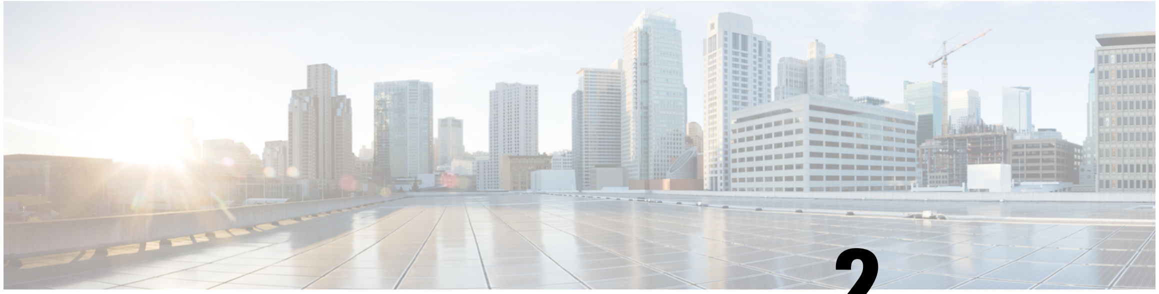
Links in each dashlet allow you to explore further details. This helps to navigate to the desired pages easily.

Figure 2: Dashboard View



srpceWithParseConfigCollection_2024-04-29T06:17:28.684274675_DARE - 36 kB	1
snmpParseConfigCollection_2024-04-28T21:20:08.328067698_DARE - 19 kB	1
snmpBGPCollection_2024-04-29T06:06:04.541936602_DARE - 28 kB	1
TOPO_BGPLS_XTC2024-04-29T06:17:07.778132344 - 36 kB	1
INVENTORY2024-04-29T06:05:33.952803220 - 49 kB	1

Use the **Customize view** button at the top right corner to customize how the dashlets appear. For details, see the *Customize the View of the Dashboard topic in the Cisco Crosswork Planning Design 7.0 User Guide*.



CHAPTER 2

Configure Network Models

This section contains the following topics:

Workflow: Network Model Creation

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 device and network access configuration, network model creation, user management, agent configuration, and so on.

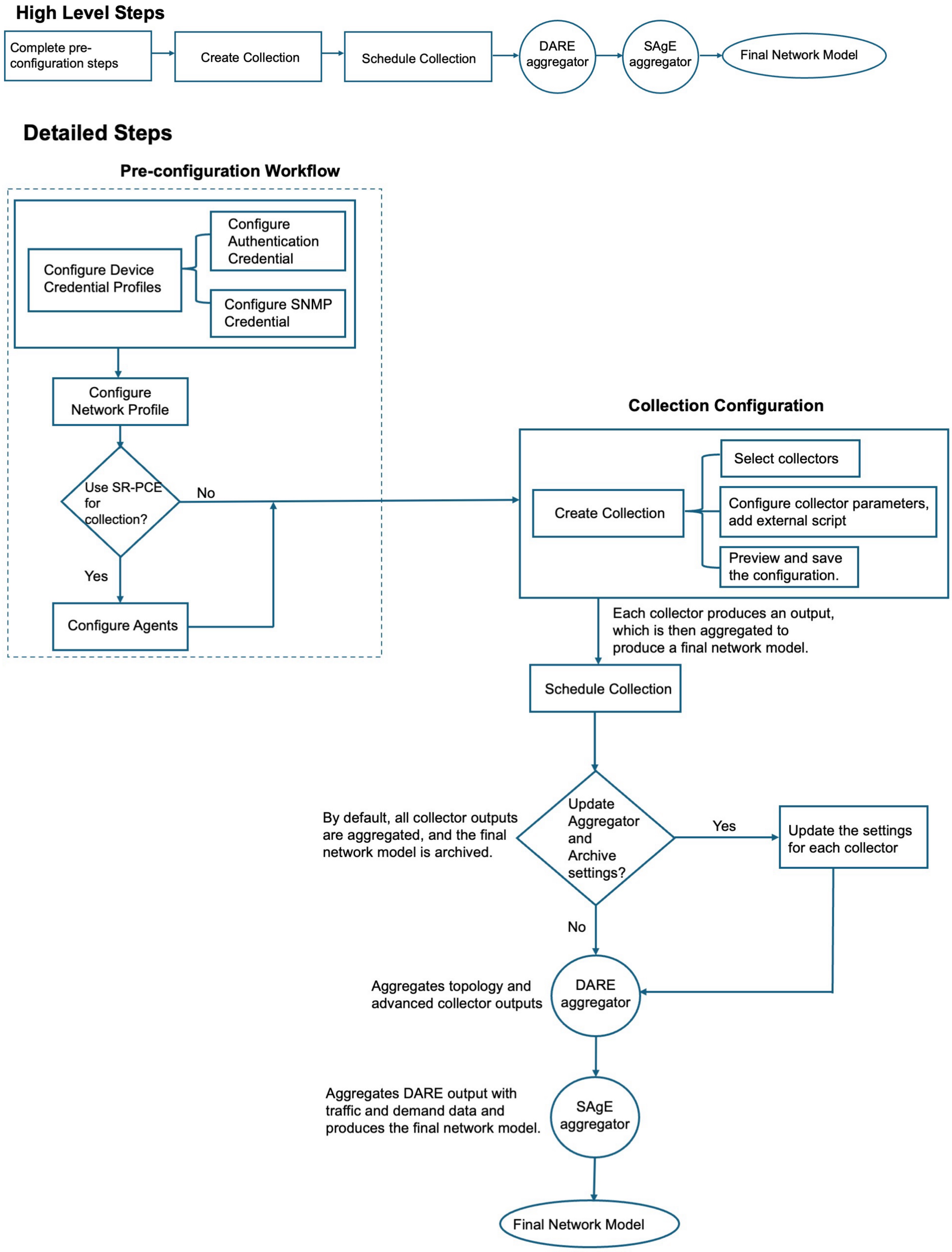
The following table and image show a high-level workflow for configuring individual network models:

Table 1: Network Model Creation Workflow

Step	Action
1. Configure device authgroups, SNMP groups, and network profile access.	See Workflow: Preconfiguration Steps, on page 10.
2. (Optional) Configure agents. This step is required only for collecting SR-PCE or NetFlow information.	See Configure Agents, on page 24.
3. Configure the collections (basic and advanced configurations).	See Workflow: Collection Configuration, on page 10.

Step	Action
4. Schedule when to run the collections.	See Add Schedules, on page 34.
5. (Optional) Manage the aggregation and archive of network model as per your requirement.	See • Aggregate Collector Outputs, on page 38 • Configure Archive, on page 40
6. View or download the plan files in the Cisco Crosswork Planning Design application.	See View or Download Plan Files, on page 42.

Figure 3: Network Model Creation Workflow


High Level Steps
Complete pre-configuration steps
Create Collection
Schedule Collection
DARE aggregator
SAgE aggregator
Final Network Model
Detailed Steps
Pre-configuration Workflow
Configure Device Credential Profiles
Configure Authentication Credential
Configure SNMP Credential
Configure Network Profile
Use SR-PCE for collection?
No
Yes
Configure Agents
Collection Configuration
Create Collection
Select collectors
Configure collector parameters, add external script
Preview and save the configuration.
Each collector produces an output, which is then aggregated to produce a final network model.
Schedule Collection
By default, all collector outputs are aggregated, and the final network model is archived.
Update Aggregator and Archive settings?
Yes
Update the settings for each collector
No
Aggregates topology and advanced collector outputs
DARE aggregator
Aggregates DARE output with traffic and demand data and produces the final network model.
SAgE aggregator
Final Network Model

Workflow: Preconfiguration Steps

The following 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.

Table 2: Preconfiguration Workflow

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 Profile, 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 24.

Workflow: Collection Configuration

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.

The high-level workflow involved in the collection configuration process is as follows:

Table 3: Collection Configuration Workflow

Step	Description
1. Complete all the steps mentioned in the preconfiguration workflow.	See Workflow: Preconfiguration Steps, 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.

Step	Description
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.
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 External Scripts Against a Network Model, on page 83.
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 34.
7. (Optional) Update the aggregation and archive settings, as required.	See: • Aggregate Collector Outputs, on page 38 • Configure Archive, on page 40

Migrate Collector Configurations

In Cisco Crosswork Planning, you can migrate the collector configurations from Cisco WAE 7.5.x/7.6.x, as well as from one Cisco Crosswork Planning instance to the other.

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 importing the configuration, the server restores only the file name and not the actual file. If the correct file is not used, then the collection fails.

Migrate Collector Configuration from Cisco WAE

Follow these steps to migrate the collector configurations from Cisco WAE 7.5.x/7.6.x to Cisco Crosswork Planning.

Before you begin

- Download the upgrade script from Cisco Software Download page.

Procedure

Step 1 If you have not backed up the configuration, use the following 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 the following 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
```

Step 2 If you already have the backed-up configuration, use the following 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 the following 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.
```

Step 3 Import the Cisco Crosswork Planning compatible configuration file to Cisco Crosswork Planning using the following steps:

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

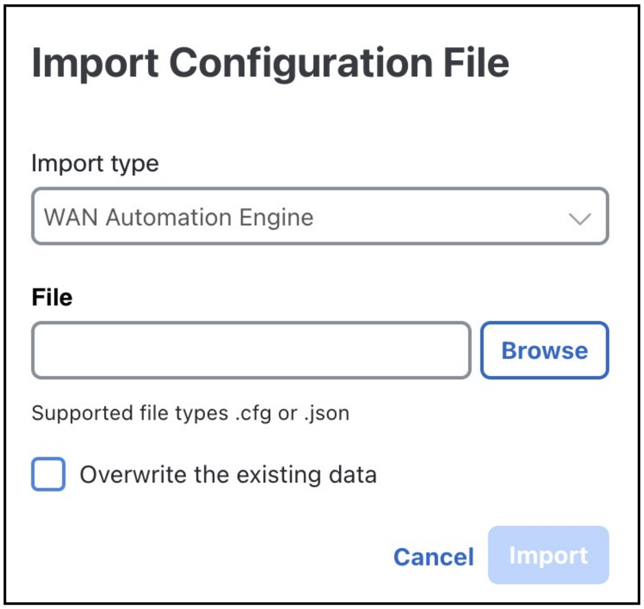
a) Log in to the Cisco Crosswork Planning UI.

b) From the main menu, choose **Collector** > **Migration**.

c) Click **Actions** and choose **Configuration migration**.

The Import configuration file window appears.

Figure 4: Import Configuration File Window



Import Configuration File

Import type

WAN Automation Engine

File

Supported file types .cfg or .json

□ Overwrite the existing data

d) From the **Import type** drop-down, choose **WAN Automation Engine**.

e) Click **Browse** and select the Cisco WAE collector configuration file which is compatible with Cisco Crosswork Planning compatible.

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.

You can monitor status of the import in the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays the status of the task as **Success**.

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 Configuration between Cisco Crosswork Planning Instances

Note If you are 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.

Follow these steps to migrate the collector configuration from one Cisco Crosswork Planning instance (source) to the other (target).

Procedure

Step 1 Download the collector configuration file from the source machine you want to migrate the configuration from:

a) Log into 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 choose **Configuration backup**.

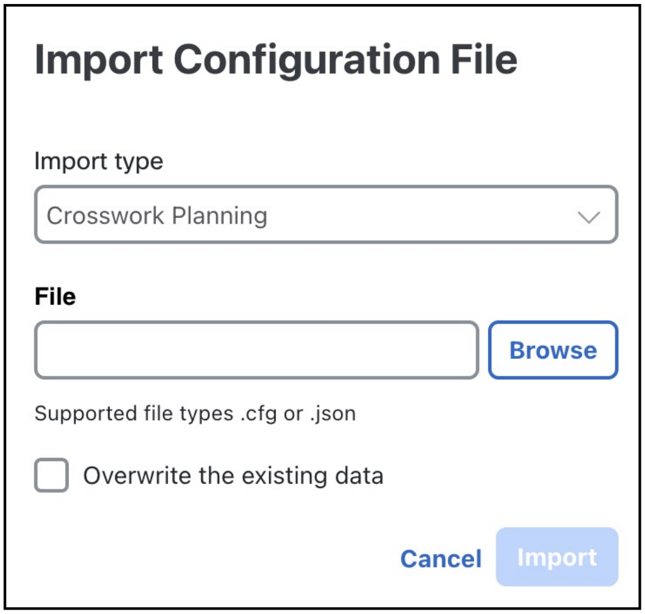
The collector configuration file is downloaded to your local machine.

Step 2 Import the collector configuration file to the target machine where you want to migrate it to:

a) Log into 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 choose **Configuration migration**.

The Import configuration file window appears.

Figure 5: Import Configuration File Window



Import Configuration File

Import type: Crosswork Planning

Supported file types .cfg or .json

d) From the **Import type** drop-down, choose **Crosswork planning**.

e) Click **Browse** and select the collector configuration file that you downloaded in the Step 1 (c).

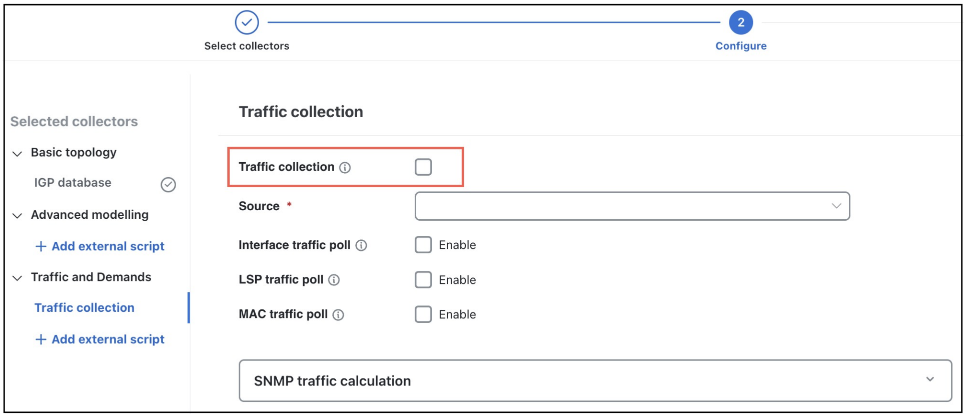
f) (Optional) If you want to overwrite the existing collector configuration, check the **Overwrite the existing data** check box.

g) Click **Import** to import the collector configuration file.

You can monitor status of the import in the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays the status of the task as **Success**.

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 on the Collections (**Collector** > **Collections**) page:

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



Traffic collection □
Source *
Interface traffic poll □ Enable
LSP traffic poll □ Enable
MAC traffic poll □ Enable

For details on configuring the **Traffic and Demands** collector, see Collect Traffic Statistics, on page 75.

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.

The following workflow describes the steps to create the credential profiles:

Table 4: Credential Profiles Configuration Workflow

Step	Action
1. Set up device authentication credentials to access devices.	See Configure Authentication Credentials, on page 17.

Step	Action
2. Set up SNMP credentials to access the network server.	See Configure SNMP Credentials, on page 18.

Configure Authentication Credentials

If you are accessing the Collections page (**Collector** > **Collections**) for the first time, then a Welcome screen appears. Click **Get Started** to see the preconfiguration steps, which are listed in the stepper pane on the left. The first step guides you to complete the creation of authentication credentials.

Or

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

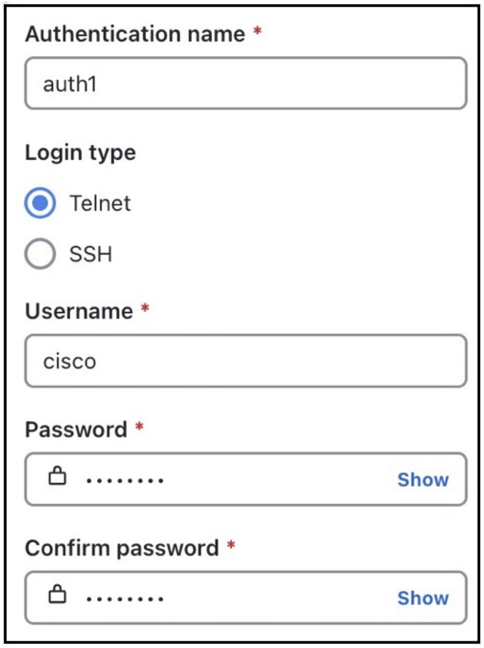
Procedure

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

Step 2 In the **Authentication** tab, click the **+ Create new** button.

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

Figure 6: Configure Authentication Credentials



Authentication name *
auth1

Login type
● Telnet
○ SSH

Username *
cisco

Password *
········

Confirm password *
········

Step 3 Enter the values in the following fields:

- **Authentication name**—Enter a descriptive name.
- **Login type**—Choose which login protocol to use: **SSH** or **Telnet**. 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**.

Configure SNMP Credentials

If you are accessing the Collections page (**Collector** > **Collections**) for the first time, then 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 first step, the second one guides you to complete the creation of SNMP credentials.

Or

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

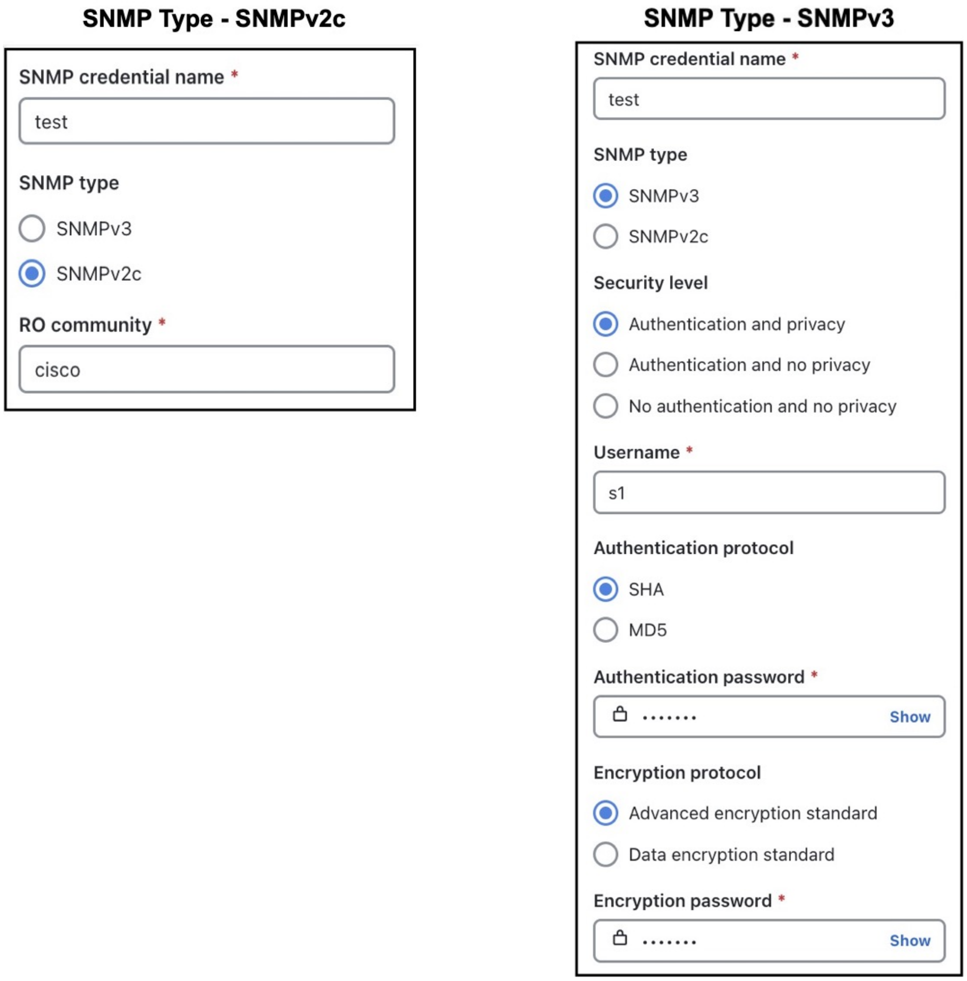
Procedure

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

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

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

Figure 7: Configure SNMP Credentials



SNMP Type - SNMPv2c

SNMP credential name *

test

SNMP type

○ SNMPv3

● SNMPv2c

RO community *

cisco

SNMP Type - SNMPv3

SNMP credential name *

test

SNMP type

● SNMPv3

○ SNMPv2c

Security level

● Authentication and privacy

○ Authentication and no privacy

○ No authentication and no privacy

Username *

s1

Authentication protocol

● SHA

○ MD5

Authentication password *

••••••• Show

Encryption protocol

● Advanced encryption standard

○ Data encryption standard

Encryption password *

••••••• Show

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

Step 4 Under **SNMP type**, choose which SNMP protocol to use: **SNMPv2c** or **SNMPv3**.

- If you choose **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.
- If you choose **SNMPv3**, enter the following default credentials:
  - **Security level**—Select one of the following:
    - **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 the following:

  - **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**.

Configure Network Profile

Define a network profile to gather the data from the network. This network profile is made up of network nodes and their credentials. You can also apply filter criteria to include or exclude a few nodes during discovery.

If you are accessing the Collections page (**Collector** > **Collections**) for the first time, then 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.

Or

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.

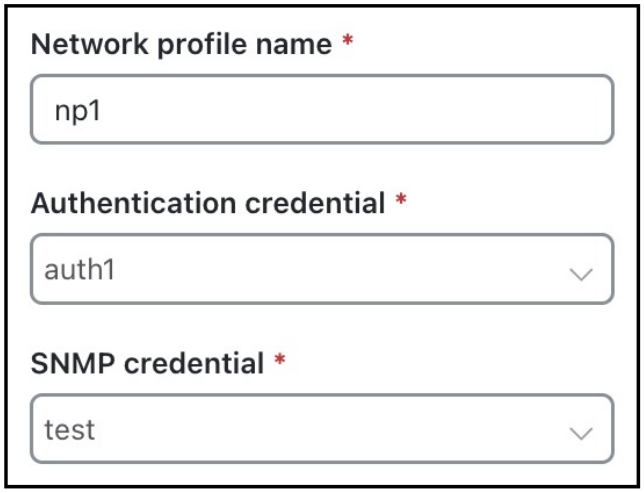
Procedure

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



Network profile name *

np1

Authentication credential *

auth1

SNMP credential *

test

Step 3 Enter the following information:

- **Network profile name**—Enter a name for the network access profile.
- **Authentication credential**—Choose 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**—Choose 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 21.

Step 6 (Optional) To include or exclude individual nodes from the collection, see Configure the Node Filter, on page 22.

Step 7 Click **Save**.

Add or Edit Nodes

Follow these steps to add or edit nodes associated with network access credentials created in the previous topic.

Procedure

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

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

Step 3 Under **Node list**, click the **Edit nodes** button and do one of the following:

- If you are adding the nodes manually for the first time, then click the **+ Add node** button. Enter the node details in the **Add Node** window and click **Save**. The newly added node appears in the Node List page.

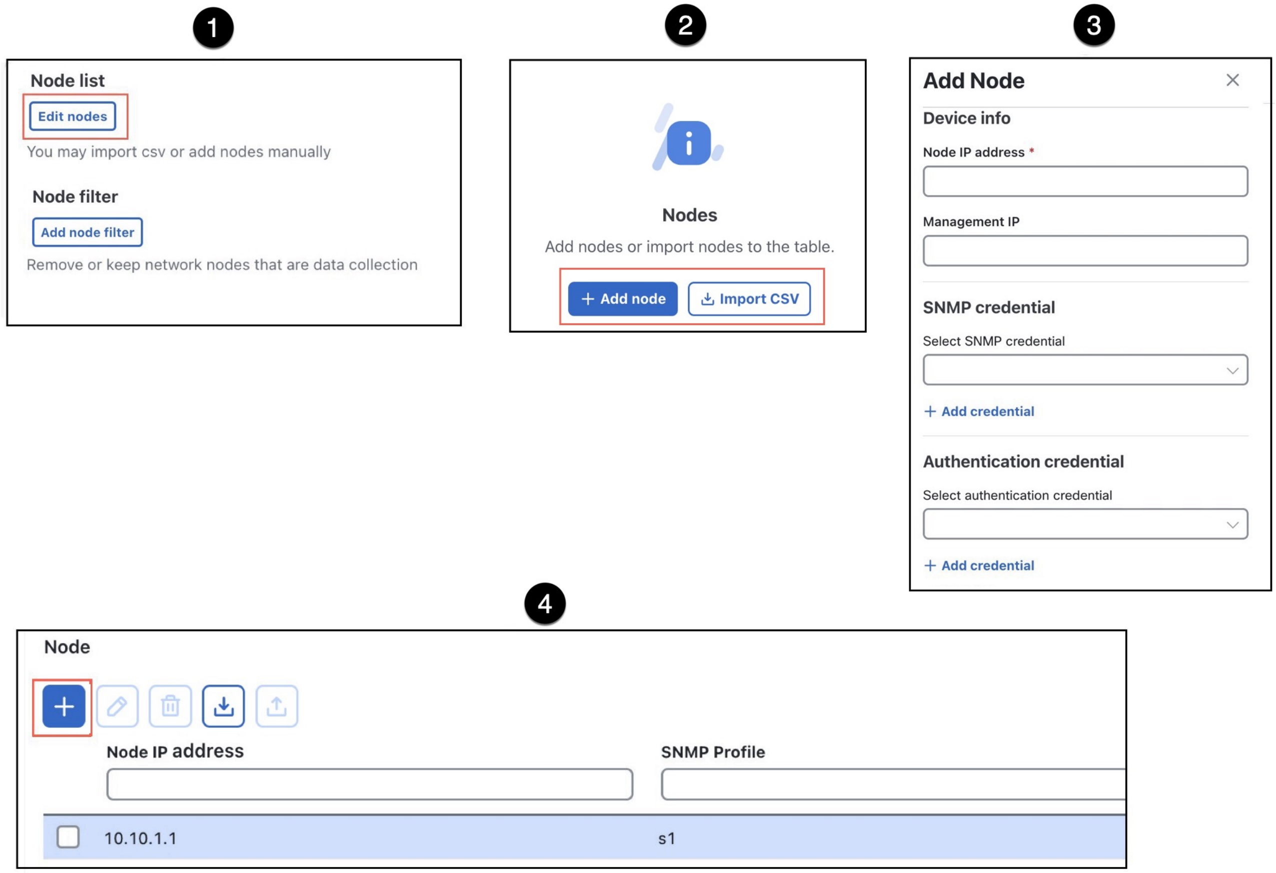
  If you want to add more nodes, then click + and enter the details.

- If there are no nodes added and if you want to import the node list, click the ⭳ Import CSV button. Click **Browse** and enter the CSV file path, and click **Import**. The newly imported nodes appear in the Node List page.

  If you want to import a different node list, then click ⭳ and import the CSV file.

  Click the **sample file** link to download a sample file containing node list.

Figure 9: Add Nodes Pages



Node list

You may import csv or add nodes manually

Node filter

Remove or keep network nodes that are data collection

Nodes

Add nodes or import nodes to the table.

Add Node

Device info

Node IP address *

Management IP

SNMP credential

Select SNMP credential

Authentication credential

Select authentication credential

Node

	Node IP address	SNMP Profile
☐	10.10.1.1	s1

- To Export a node list, click ⭱.

- To edit a node, select the node, click ✎, and enter the node details.

- To delete the nodes, select the nodes and click 🗑.

Step 4 Click **Done**.

Configure the Node Filter

Cisco Crosswork Planning enables you to include or exclude individual nodes from the data collection.

Note

- Node/Host name or loopback IP can be added for 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 only by IP address.
- Node filter does not support Segment List hops.

Procedure

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

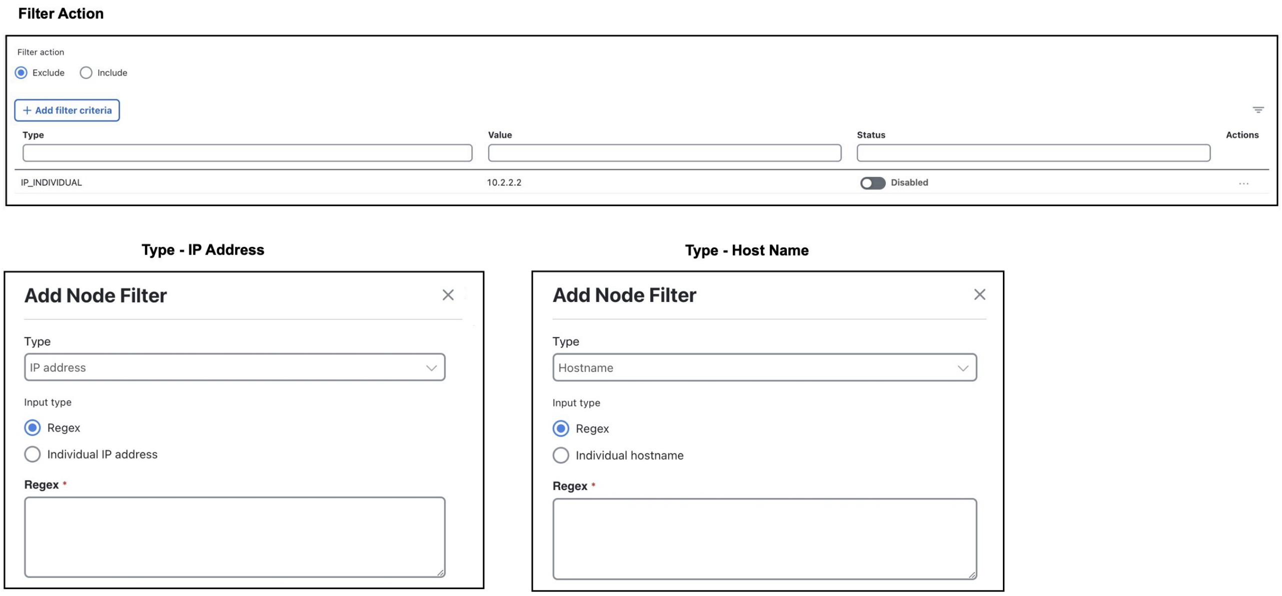
Step 2 Choose the required network profile and click **Save & Proceed**.

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



Filter Action

Filter action
● Exclude ○ Include

Type	Value	Status	Actions
IP_INDIVIDUAL	10.2.2.2	Disabled	...

Type - IP Address

Add Node Filter
Type: IP address
Input type: ● Regex ○ Individual IP address
Regex *

Type - Host Name

Add Node Filter
Type: Hostname
Input type: ● Regex ○ Individual hostname
Regex *

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**. Based on the type you selected in the previous step, you get different options.

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

Use the **Regex** option when multiple nodes are to be included/excluded with a single expression. Enter the **Regex** expression in the Regex field.

Use the **Individual IP address** option to add IP address of each node. Enter the IP address in the **IP address** field.

Use the **Individual hostname** option to add hostname of each node. Enter the hostname in the **Hostname** field.

Step 8 Click **Save**.

Step 9 (Optional) Repeat steps 4–8 to add more filter criteria.

Step 10 Slide the toggle in the **Status** column to the Enabled position to consider the entries in the filter.

Step 11 Click **Save**.

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

Configure Agents

Agents perform information-gathering tasks and should be configured before certain network collection operations. This section describes how to configure agents using the Cisco Crosswork Planning UI.

Note This task is required only for collecting SR-PCE or NetFlow information.

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.

If you are accessing the Collections page (**Collector** > **Collections**) for the first time, then 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.

Or

Follow these steps to configure agents from the **Collector** > **Agents** page.

Procedure

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

Step 2 Click **+ Create new**.

Note
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 Choose the required Collector types. The options are **SR-PCE** or **NetFlow**.

- The SR-PCE agent periodically collects information from the SR-PCE server, 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
  SR-PCE agents must be configured for any networks that use SR-PCE before you can perform a network collection.

- The NetFlow collector is 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 types** you choose.

- If you choose **SR-PCE** as the collector type, then enter the applicable configuration details mentioned in Table 5: SR-PCE Agent Configuration Options, on page 25.
- If you choose **NetFlow** as the collector type, then enter the applicable configuration details mentioned in Table 6: NetFlow Agent Configuration Options, on page 27.

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 Create Collections, on page 29.

SR-PCE and NetFlow Agent Configuration Options

This topic describes options available when configuring SR-PCE and NetFlow agents:

Table 5: SR-PCE Agent Configuration Options

Option	Description
Enabled	Enables the SR-PCE agent. Default is enabled.
SR-PCE host IP	Indicates the host IP address of the SR-PCE router.
SR-PCE REST port	Indicates the port number to connect to the SR-PCE host. The default is 8080.

Option	Description
Authentication type	Indicates the authentication type to be used for connecting to the SR-PCE host. The available options are: • 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	Indicates the username for connecting to the SR-PCE host.
Password	Indicates the password for connecting to the SR-PCE host.
Connection retry count	Indicates the maximum number of retry counts for connecting to the SR-PCE host.
Topology collection	Specifies whether to collect topology data and to have subscription for network changes. The options are: Collection only, Collection and Subscription, and Off. Default is Collection and Subscription.
LSP collection	Specifies whether to collect LSP data and to have subscription for network changes. The options are: Collection only, Collection and Subscription, and Off. Default is Collection and Subscription.
Connection timeout interval	Specifies the connection timeout in seconds. Default is 50 seconds.
Pool size	Indicates the number of threads processing SR-PCE data in parallel.
Keep alive interval	Indicates the interval in seconds to send keep-alive messages. Default is 10.
Batch size	Indicates the number of nodes to send in each message. Default is 1000.
Keep alive threshold	Specifies 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	Indicates the time to buffer SR-PCE events before sending to collectors, in seconds.
Playback events delay	Indicates the delay in SR-PCE events playback to mimic real events, in seconds (0 = no delay).

Option	Description
Max LSP history	Indicates the 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.

Table 6: 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	Indicates the node name.
Sampling rate	Indicates the 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	Indicates the IPv4 source address of flow export packets.
BGP source IP	Indicates the IPv4 or IPv6 source address of iBGP update messages.
BGP password	Indicates the BGP peering password for MD5 authentication.
Interval	Indicates the interval time for writing the output file, in seconds. Enter the value that is greater than zero and multiple of 60. Default is 900 seconds.
Flow size	Indicates the flow collection deployment size, based on network-wide aggregated flow export traffic rate. The values are: • 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	Allows you to choose the 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.

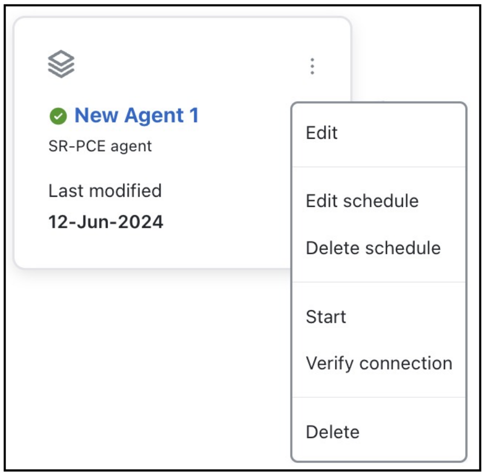
- **Delete schedule**—Use this option to delete the data refresh frequency set for the agents.

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



New Agent 1
SR-PCE agent
Last modified
12-Jun-2024

Configure Collections

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

Create Collections

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.

Before you begin

Ensure that you have completed the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to create collections.

Procedure

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

Step 2 Click **Add collection** at the top-right corner. The Add Collection modal window appears.

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

Step 3 In the **Collection name** field, enter the name of the collection.

Step 4 From the **Node profile** drop-down list, choose the required node profile. If you want to create any new node profile, then click **+ Add new profile**.

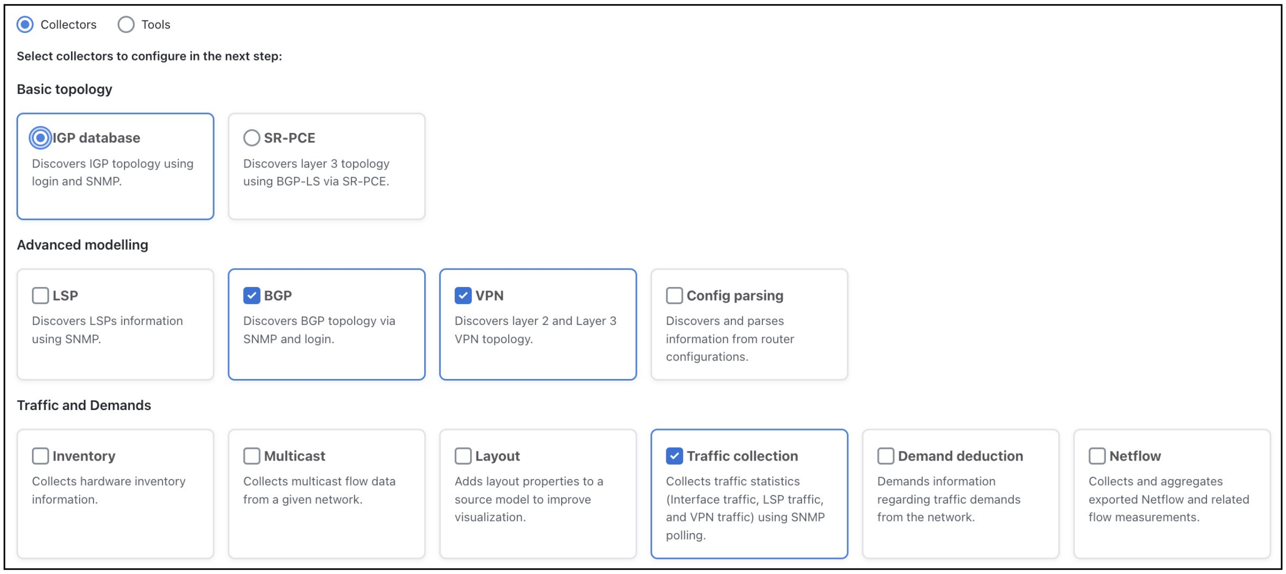
Step 5 Click **Continue**.

The collection configuration page appears with a numbered navigation bar at the top.

Step 6 Verify that the **Collectors** radio button is clicked at the top. This option is selected by default.

Step 7 Select the required collectors. You must choose one of the Basic topology collectors to start the network collection. Then, select the collectors from the other sections.

Figure 12: Select Collectors Page



● Collectors ○ Tools

Select collectors to configure in the next step:

Basic topology

● IGP database
Discovers IGP topology using login and SNMP.

○ SR-PCE
Discovers layer 3 topology using BGP-LS via SR-PCE.

Advanced modelling

□ LSP
Discovers LSPs information using SNMP.

☑ BGP
Discovers BGP topology via SNMP and login.

☑ VPN
Discovers layer 2 and Layer 3 VPN topology.

□ Config parsing
Discovers and parses information from router configurations.

Traffic and Demands

□ Inventory
Collects hardware inventory information.

□ Multicast
Collects multicast flow data from a given network.

□ Layout
Adds layout properties to a source model to improve visualization.

☑ Traffic collection
Collects traffic statistics (Interface traffic, LSP traffic, and VPN traffic) using SNMP polling.

□ Demand deduction
Demands information regarding traffic demands from the network.

□ Netflow
Collects and aggregates exported Netflow and related flow measurements.

The collectors are categorized under the following sections. Choose the collectors from all these sections as per your requirement. For descriptions of all the collectors, see Collector Descriptions, on page 47.

- **Basic topology**—Choose the required basic topology collector. The supported basic topology collectors are: IGP database and SR-PCE. You can choose only one topology collector.
- **Advanced modeling**—Choose 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 choose multiple advanced collectors.
- **Traffic and Demands**—Choose the required collectors for traffic collection. The supported traffic and demands collectors are: Inventory, Multicast, Layout, Traffic collection, Demand deduction, and NetFlow. You can choose multiple traffic and demand collectors.

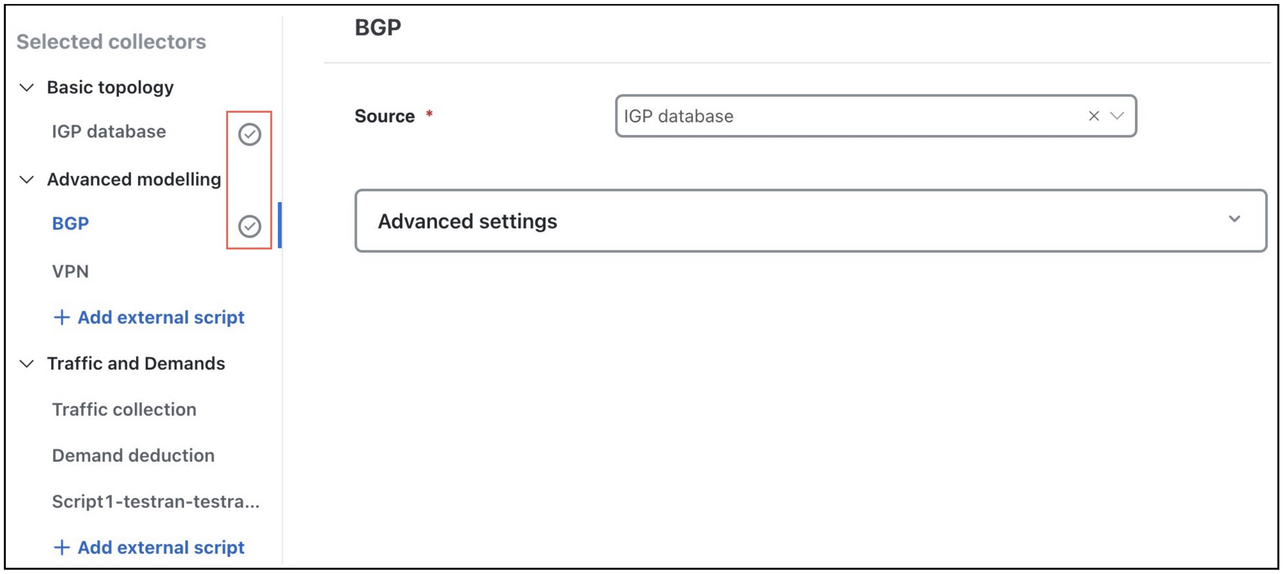
Step 8 In the second step of configuration, enter the configuration parameters for the selected collectors. Note the following:

- 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, choose 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 each collector that you selected. Otherwise, the **Next** button is not enabled and you will not be able to proceed further.

Figure 13: Configure Collection Parameters



BGP

Source * IGP database

Step 9 (Optional) If you want to use a customized script against a collection model, use the **+ Add external script** link. For details, see Run External Scripts Against a Network Model, on page 83.

Step 10 Once the configuration parameters are entered for all the collectors, click **Next**.

Step 11 The final step of collection configuration is to preview the order in which the collectors are added. In the preview diagram, you can observe which collector output is being used as the input for the other collector.

If you are satisfied with the configuration, then click **Create** to proceed with the creation of the collection. The Collection creation successful message appears.

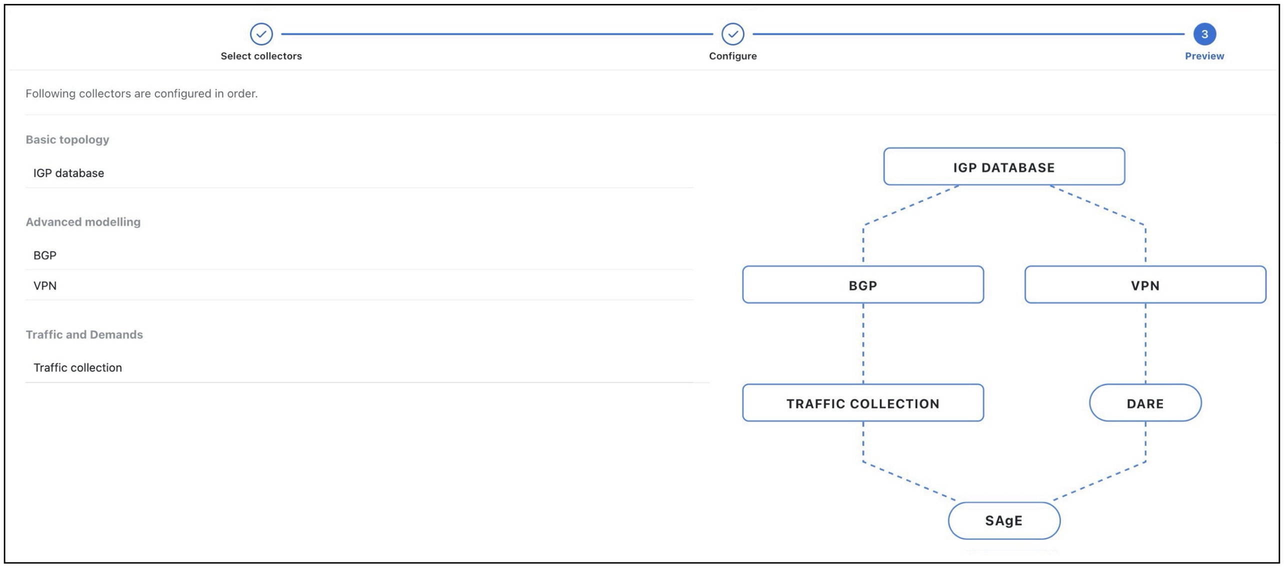
If you want to make any changes to the configuration, then click **Back** to go back to the previous page. You can also click the step numbers at the top to navigate to the required configuration step.

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.

Figure 14: Preview Page



Following collectors are configured in order.

Basic topology

IGP database

Advanced modelling

BGP

VPN

Traffic and Demands

Traffic collection

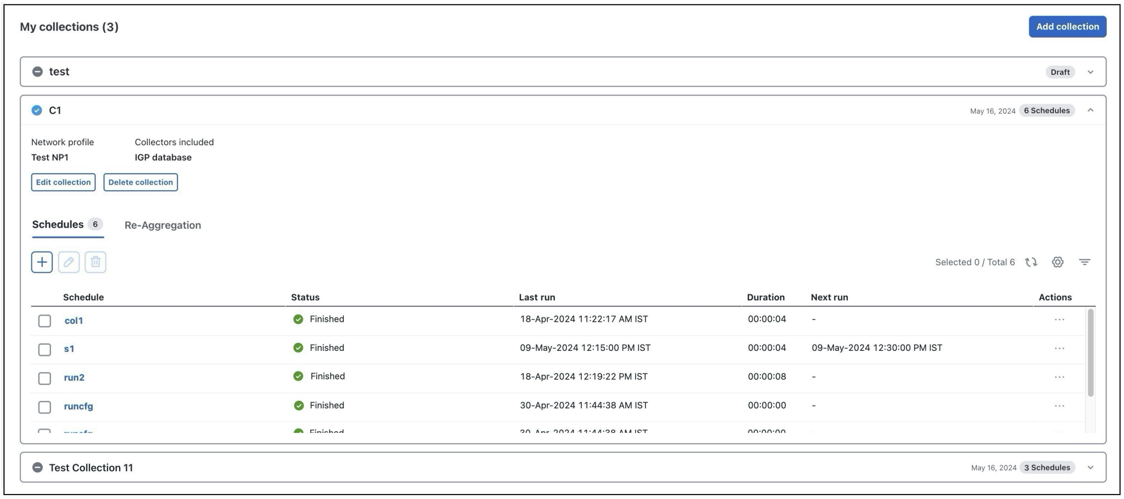
Step 12 (Optional) If you want to configure the schedules immediately, click **Add schedule** in the dialog box and proceed with the schedule configuration. For details, see Add Schedules, on page 34.

Step 13 Click **Done** in the successful message box to complete the collection creation process.

The newly added collection appears in the **Collector** > **Collections** page.

The following image shows a sample Collections page with three collections. Expand each collection panel to view its details.

Figure 15: List of Available Collections



My collections (3)

test

C1 May 16, 2024

Network profile: Test NP1

Collectors included: IGP database

Selected 0 / Total 6

	Schedule	Status	Last run	Duration	Next run	Actions
□	col1	✓ Finished	18-Apr-2024 11:22:17 AM IST	00:00:04	-	···
□	s1	✓ Finished	09-May-2024 12:15:00 PM IST	00:00:04	09-May-2024 12:30:00 PM IST	···
□	run2	✓ Finished	18-Apr-2024 12:19:22 PM IST	00:00:08	-	···
□	runcfg	✓ Finished	30-Apr-2024 11:44:38 AM IST	00:00:00	-	···
□	runcfg	✓ Finished	30-Apr-2024 11:44:38 AM IST	00:00:00		

Test Collection 11 May 16, 2024

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 34.

Edit Collections

Follow these steps to edit collections.

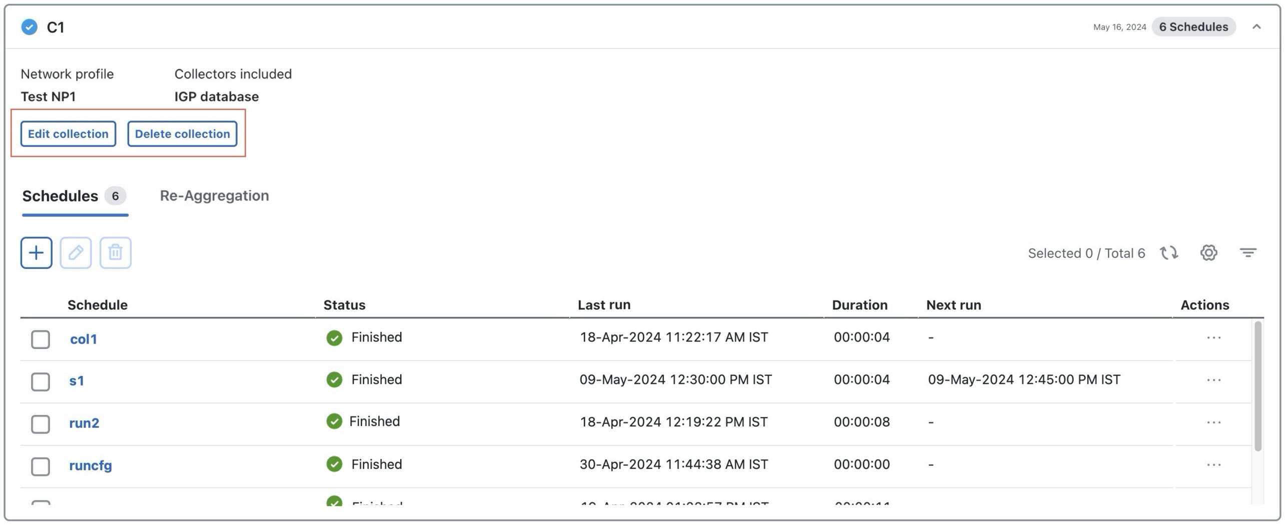
Procedure

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 32).

Step 2 Expand the Collection panel you want to edit.

Step 3 Click **Edit collection**.

Figure 16: Collection Actions



Network profile: Test NP1

Collectors included: IGP database

	Schedule	Status	Last run	Duration	Next run	Actions
□	col1	✓ Finished	18-Apr-2024 11:22:17 AM IST	00:00:04	-	···
□	s1	✓ Finished	09-May-2024 12:30:00 PM IST	00:00:04	09-May-2024 12:45:00 PM IST	···
□	run2	✓ Finished	18-Apr-2024 12:19:22 PM IST	00:00:08	-	···
□	runcfg	✓ Finished	30-Apr-2024 11:44:38 AM IST	00:00:00	-	···

Step 4 Make the required changes in the **Select collectors** and **Configure** pages as required. For reference, see Create Collections, on page 29. Preview the changes and ensure that the updated configuration meets your requirements.

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 Add Schedules, on page 34.

Delete Collections

Follow these steps to delete collections.

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 32).

Step 2 Expand the Collection panel you want to delete.

Step 3 Click **Delete collection** (for reference, see Figure 16: Collection Actions, on page 33).

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

The collection deletion successful message 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. Also, you can create multiple schedules for the same collection with different time intervals and different collector settings.

Add Schedules

Before you begin

- Ensure that you have created the required collections. For details, see Create Collections, on page 29.
- Be familiar with using cron expressions.

Follow these steps to add schedules.

Procedure

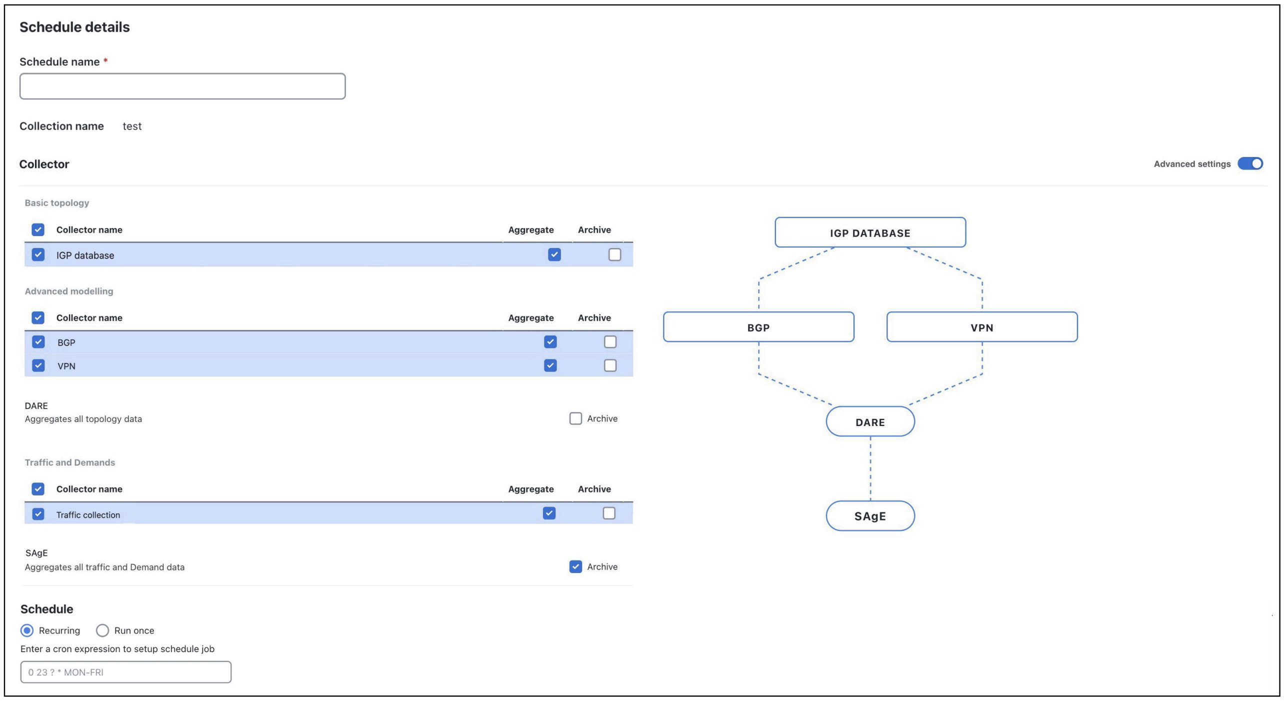
Step 1 From the main menu, choose **Collector** > **Collections**. The list of already created collections appears (for reference, see Figure 15: List of Available Collections, on page 32).

Step 2 Expand the collection panel for which you want to add the schedule and use any of the following 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 36).

The Schedule details page appears.

Figure 17: Schedule Details



Schedule details

Schedule name *

Collection name test

Collector

Advanced settings

Basic topology

☑ Collector name	Aggregate	Archive
☑ IGP database	☑	□

Advanced modelling

☑ Collector name	Aggregate	Archive
☑ BGP	☑	□
☑ VPN	☑	□

DARE
Aggregates all topology data □ Archive

Traffic and Demands

☑ Collector name	Aggregate	Archive
☑ Traffic collection	☑	□

SAgE
Aggregates all traffic and Demand data ☑ Archive

Schedule

● Recurring ○ Run once

Enter a cron expression to setup schedule job

0 23 ? * MON-FRI

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

Step 4 In the **Collector** section:

- If you want to exclude any collector from 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 38.
- 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 40.

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

- If you choose 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 choose the **Recurring** option, enter 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.

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

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

Edit Schedules

Follow these steps to edit schedules.

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 32).

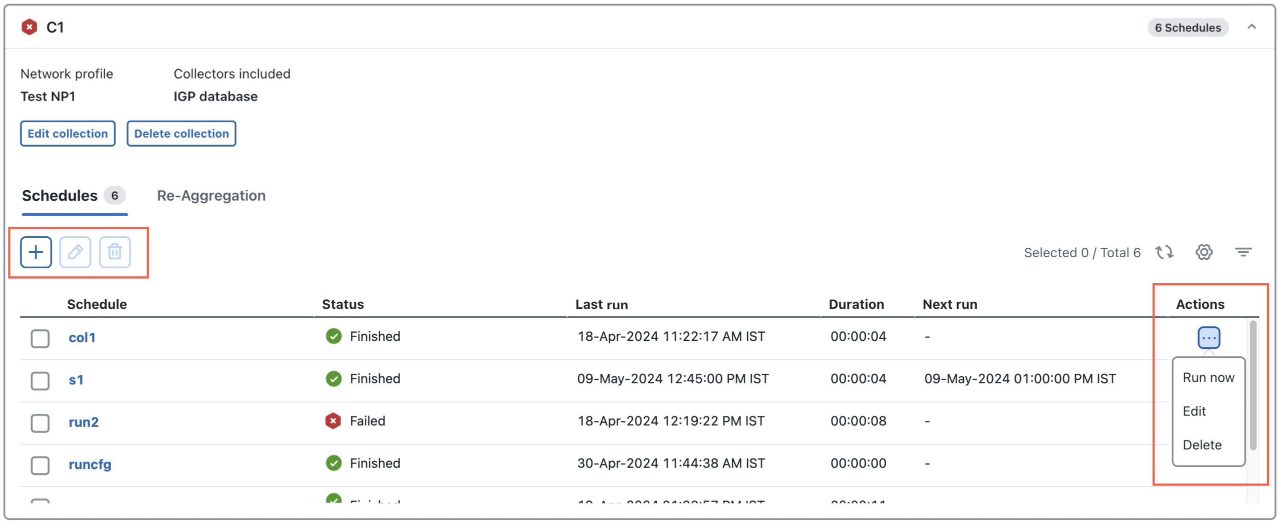
Step 2 Expand the collection panel for which you want to edit the schedule.

Step 3 Under the **Schedules** tab, edit the schedules in any of the following ways:

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

Note
You can edit only one schedule at a time.

Figure 18: Schedule Actions



C1

6 Schedules

Network profile: Test NP1

Collectors included: IGP database

Schedules 6 | Re-Aggregation

Selected 0 / Total 6

	Schedule	Status	Last run	Duration	Next run	Actions
□	col1	✓ Finished	18-Apr-2024 11:22:17 AM IST	00:00:04	-	•••
□	s1	✓ Finished	09-May-2024 12:45:00 PM IST	00:00:04	09-May-2024 01:00:00 PM IST	
□	run2	✕ Failed	18-Apr-2024 12:19:22 PM IST	00:00:08	-	
□	runcfg	✓ Finished	30-Apr-2024 11:44:38 AM IST	00:00:00	-	

Step 4 Make the required changes in the **Edit Schedule** page. Then, click **Run now** to run the job immediately or **Schedule** to run the job at the specified interval. For details, see Add Schedules, on page 34.

Delete Schedules

Follow these steps to delete schedules.

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 32).

Step 2 Expand the collection panel for which you want to delete the schedule.

Step 3 Under the **Schedules** tab, delete the schedules in any of the following ways (see Figure 18: Schedule Actions, on page 36):

- Select the schedule that you want to delete and click 🗑.
- From 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 schedule deletion successful message appears.

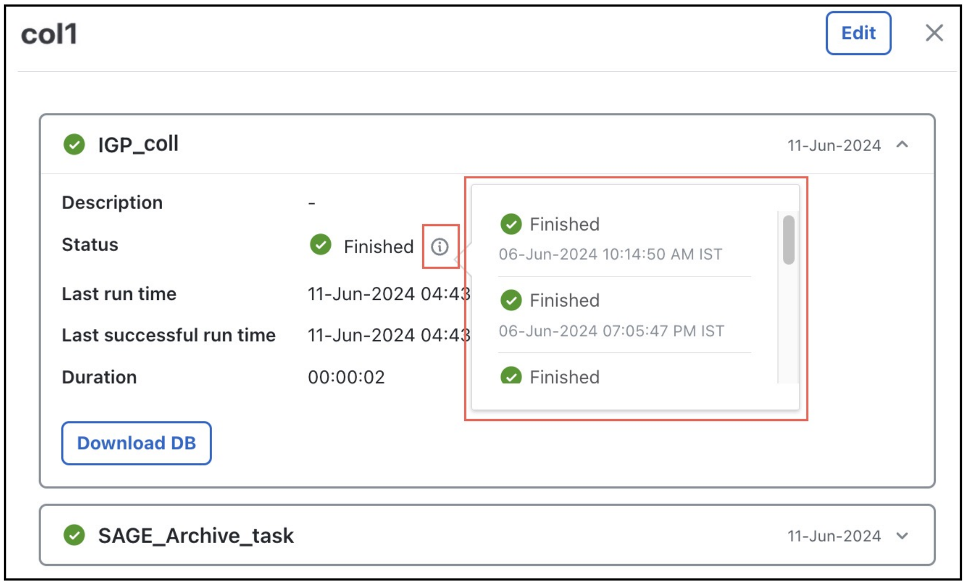
View Schedule Task Status and History

After a schedule is configured for a collection, you can view the current status and last 10 statuses of the tasks involved.

To do this:

1. Expand the collection panel.
2. Click the name of the schedule in the **Schedules** tab.

   The page that opens displays the statuses of all the tasks involved in the scheduled collection, along with timestamps of the recent task execution, the duration of the task, and the description (if there is a task failure).



col1

IGP_coll — 11-Jun-2024

Description	-
Status	✓ Finished ⓘ
Last run time	11-Jun-2024 04:43
Last successful run time	11-Jun-2024 04:43
Duration	00:00:02

✓ Finished
06-Jun-2024 10:14:50 AM IST

✓ Finished
06-Jun-2024 07:05:47 PM IST

✓ Finished

SAGE_Archive_task — 11-Jun-2024

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

Click **Download DB** to download the collected data from the collector.

Aggregate Collector Outputs

Each collector produces an output, which are 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, and helps 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 Create Collections, on page 29.

Follow these steps to exclude any collector output from aggregation.

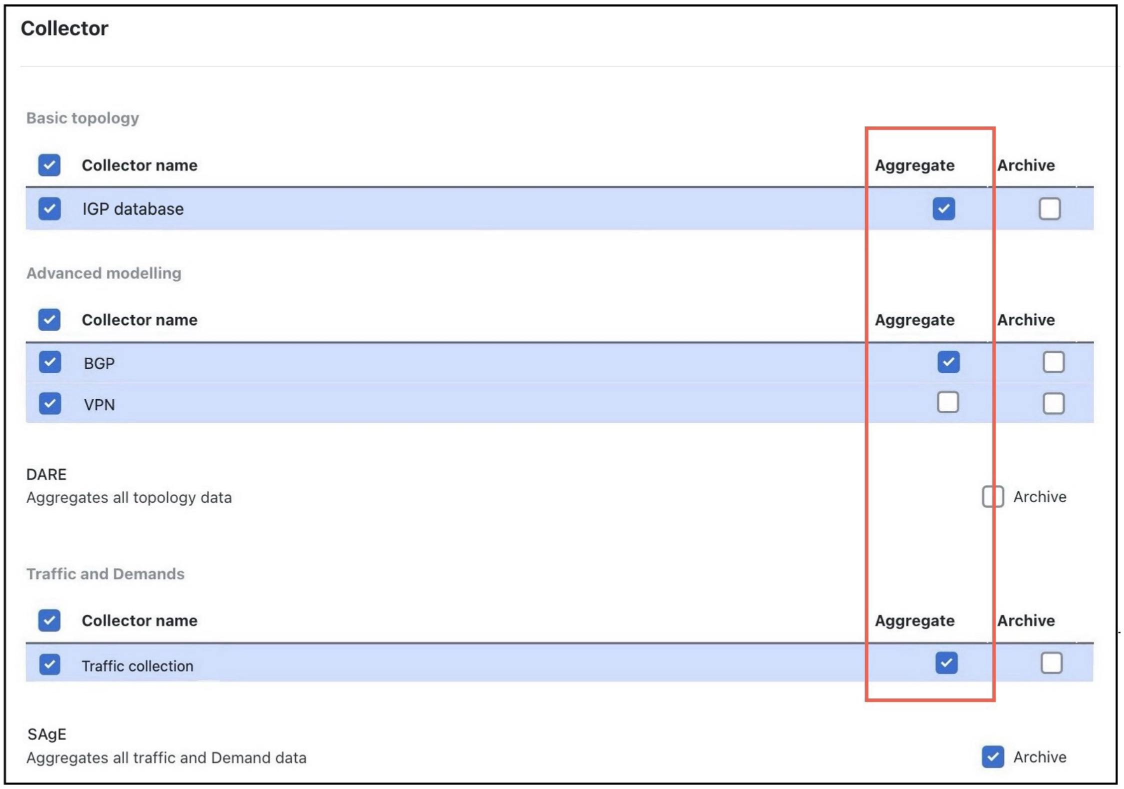
Procedure

Step 1 Open the Add or Edit Schedule page for the collection you want to edit. For details, see Add Schedules, on page 34 or Edit Schedules, on page 36.

Step 2 (Optional) Notice that the **Advanced Settings** toggle button is turned on by default. If it is not, then 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



Collector

Basic topology

☑	Collector name	Aggregate	Archive
☑	IGP database	☑	□

Advanced modelling

☑	Collector name	Aggregate	Archive
☑	BGP	☑	□
☑	VPN	□	□

DARE
Aggregates all topology data
□ Archive

Traffic and Demands

☑	Collector name	Aggregate	Archive
☑	Traffic collection	☑	□

SAgE
Aggregates all traffic and Demand data
☑ Archive

Step 4 (Optional) Update the schedule settings. For details, see Add Schedules, on page 34.

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

Once you uncheck the **Aggregate** check box for any 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.

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. When you use this option, the data collection will not occur, but the aggregated model created so far will be discarded and a fresh aggregation process will begin.

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.

Follow these steps to reaggregate collector outputs.

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 32).

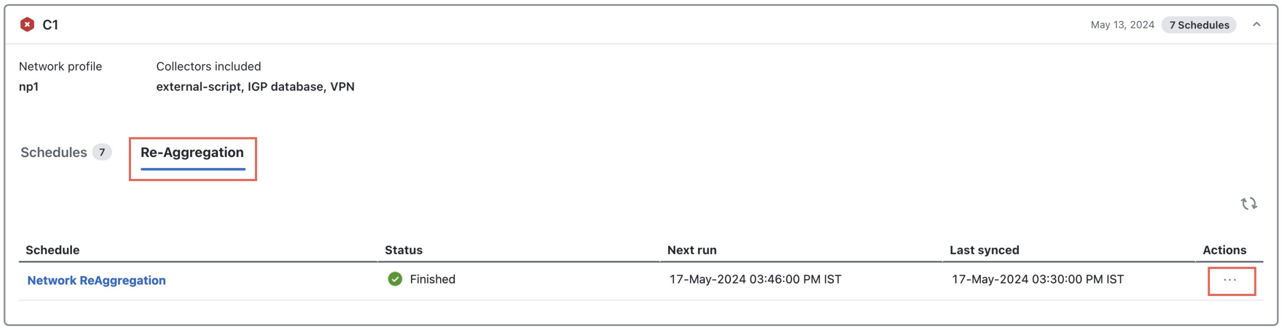
Step 2 Expand the collection panel in which you want to reaggregate the collector outputs.

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

Step 4 If you are performing the reaggregation for the first time, click the **Schedule** or **Run once** button. If this is not the first time, then update the schedule or re run the aggregation using the options mentioned in the next step.

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

Figure 20: Reaggregation of Collection



C1

May 13, 2024 · 7 Schedules

Network profile: np1

Collectors included: external-script, IGP database, VPN

Schedules 7 · Re-Aggregation

Schedule	Status	Next run	Last synced	Actions
Network ReAggregation	Finished	17-May-2024 03:46:00 PM IST	17-May-2024 03:30:00 PM IST	⋯

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

Step 5 Update the schedule or run the reaggregation once more using ⋯ under the **Actions** column, if required. Based on the option you selected in the previous step, the options displayed under this button differ slightly.

If you have selected the **Schedule** option in the previous step, then this button displays: Run now, Edit schedule, Pause, and Delete. If you have selected the **Run once** option, then it displays: Run now, Add schedule, and Delete.

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

Configure Archive

The Archive is a repository for plan files. 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.

If you have the Cisco Crosswork Planning Design application installed on the same machine, the archived network models appear under **Network Models** > **Local archive**.

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.

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 Create Collections, on page 29.

Procedure

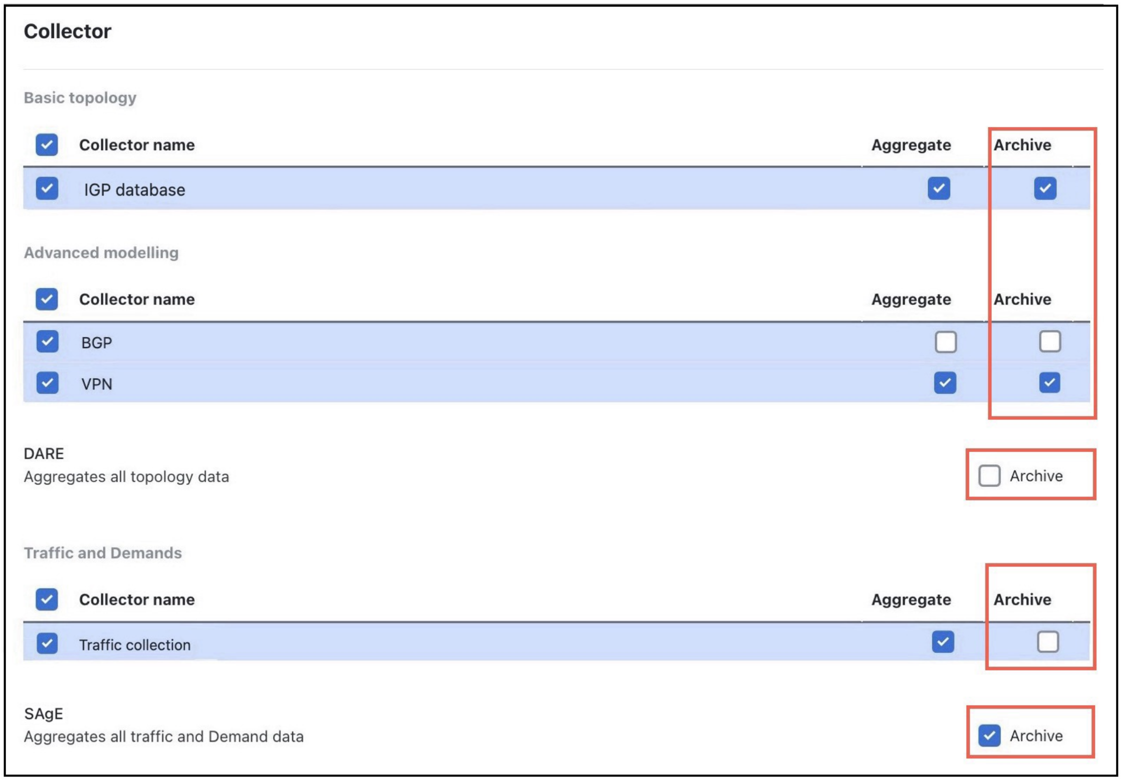
Step 1 Open the Add or Edit Schedule page for the collection that you want to edit. For details, see Add Schedules, on page 34 or Edit Schedules, on page 36.

Step 2 (Optional) Notice that the **Advanced settings** toggle button is turned on by default. If it is not, then turn it on.

Step 3 Under the **Collector** section:

- If you want to archive network models at a collection level, check the check box under the **Archive** column of the corresponding collection.
- If you do not want to archive a final network model, uncheck the **Archive** check box next to SAgE.

Figure 21: Archive Settings



Collector

Basic topology

☑	Collector name	Aggregate	Archive
☑	IGP database	☑	☑

Advanced modelling

☑	Collector name	Aggregate	Archive
☑	BGP	□	□
☑	VPN	☑	☑

DARE
Aggregates all topology data
□ Archive

Traffic and Demands

☑	Collector name	Aggregate	Archive
☑	Traffic collection	☑	□

SAgE
Aggregates all traffic and Demand data
☑ Archive

Step 4 (Optional) Update the schedule settings. For details, see Add Schedules, on page 34.

Step 5 If you selected **Run once** in the previous step, click **Run now** to run the job immediately. If you selected **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 sections of the **Network Models** page.

What to do next

Access the plan files from the Cisco Crosswork Planning Design application. For more details, see View or Download Plan Files, on page 42.

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

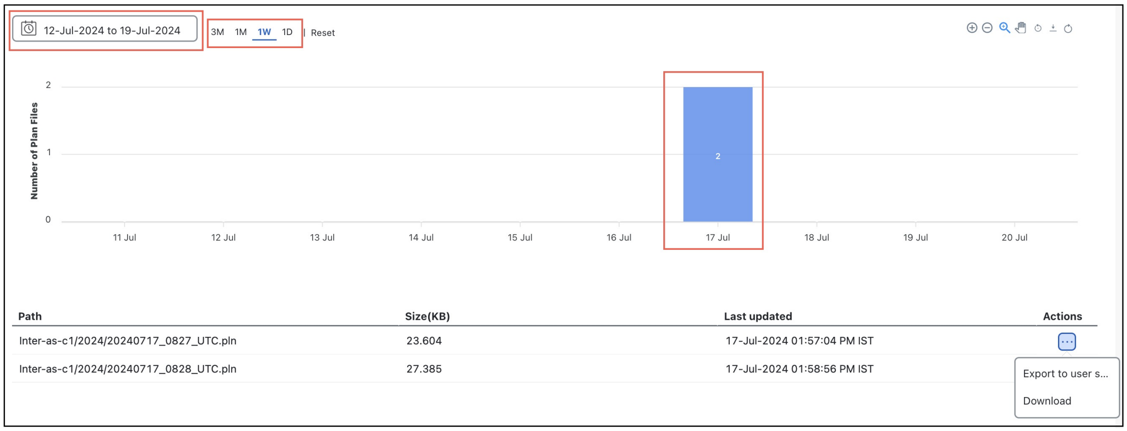
- Make sure that the network model has been archived. For details, see Configure Archive, on page 40.

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



Path	Size(KB)	Last updated	Actions
Inter-as-c1/2024/20240717_0827_UTC.pln	23.604	17-Jul-2024 01:57:04 PM IST	⋯
Inter-as-c1/2024/20240717_0828_UTC.pln	27.385	17-Jul-2024 01:58:56 PM IST	

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 7.0 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.

The following high-level workflow describes how to access the network models from the external collector:

Table 7: Workflow: Access 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 40.
2. Connect to the machine where Cisco Crosswork Planning Collector application is installed (external collector).	See Connect to the External Collector, on page 44.
3. Access the network models from the Remote archive.	See View or Download Plan Files from Remote Archive, on page 45.

Connect to the External Collector

Follow these steps 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 the IP address of the machine where the Cisco Crosswork Planning Collector application is installed (external collector).

Step 4 Enter the Port, Username, and Password details of the machine.

Step 5 Click **Save**.

Step 6 From the main menu, choose **Network Models** and verify that the **Remote archive** option is displayed in the left pane. Notice that the collections archived in the external collector are displayed here.

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 45.

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 43):

- 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.

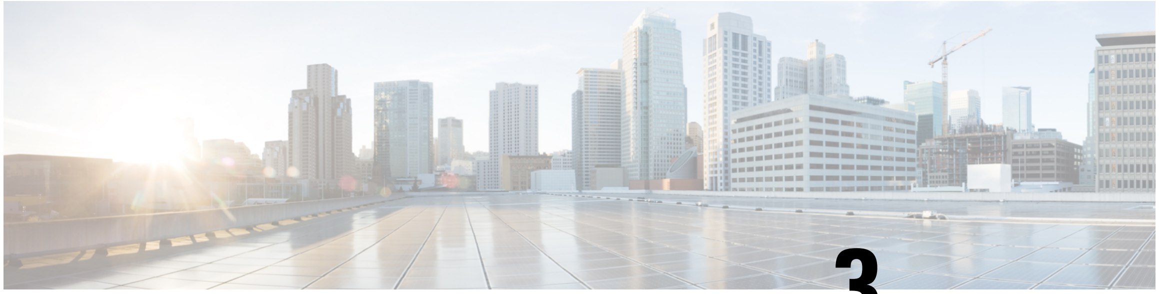
Step 6 (Optional) Select the required tags from the list (if available) or create new tags.

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 7.0 User Guide*.



CHAPTER 3

Supported Collectors and Tools

This section contains the following topics:

Collector Descriptions

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

Table 8: Collector Descriptions

Collector	Description	Prerequisite/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 50

Collector	Description	Prerequisite/Notes	Configuration Steps
SR-PCE	Discovers Layer 3 topology using SR-PCE. It uses raw SR-PCE data as the source for the topology. Node and interface/port properties are discovered using SNMP.	• The SR-PCE agents must be configured before running this collection. For details, see Configure Agents, on page 24. • 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 51
Advanced Modeling Collection			
LSP	Discovers LSP information using SNMP.	• A network model with basic topology collection must exist. • If using SR-PCE, the Collect Topology Information Using the SR-PCE Collector, on page 51 must be completed before running this collection.	See Collect LSP Information, on page 55
PCEP LSP	(Accessible only when SR-PCE collector is selected as the basic topology collector) Discovers PCEP LSPs using SR-PCE.	The Collect Topology Information Using the SR-PCE Collector, on page 51 must be completed before running this collection.	See Collect PCEP LSP Information Using SR-PCE, on page 56
BGP	Discovers BGP peering using login and SNMP.	A network model with basic topology collection must exist.	See Discover BGP Topology, on page 60
VPN	Discovers Layer 2 and Layer 3 VPN topology.	A network model with basic topology collection must exist.	See Discover VPN Topology, on page 63
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 70
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 64
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 58

Collector	Description	Prerequisite/Notes	Configuration Steps
Layout	Adds layout properties to a source model to improve visualization.	• An aggregated network model. • After the Layout collector is configured, a plan file containing layout properties must be imported back into the Layout model.	See Improve Network Model Visualization, on page 73
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 55. • If collecting VPN traffic, a network model with VPN collection must exist. See Discover VPN Topology, on page 63.	See Collect Traffic Statistics, on page 75
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 79
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 81
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 External Scripts Against a Network Model, on page 83

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**. 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 50 and Collect Topology Information Using the SR-PCE Collector, on page 51.

Collect Topology Information Using the IGP Database Collector

In Cisco Crosswork Planning, there are two topology collectors: IGP database and SR-PCE. In a single collection, you can choose any one of these collectors for collecting information related to topology. Selecting both collectors is not permitted.

To use the SR-PCE collector for topology collection, see Collect Topology Information Using the SR-PCE Collector, on page 51.

The **IGP database** collector discovers network topology using IGP database with the collection of node properties and interface and port discovery using SNMP. This is typically the first collector that is configured before other collectors, because it provides the basic data collection needed. This collector provides full topology discovery. Collection of multi instances of OSPF and IS-IS is also supported. All links collected from routers will have an associated IGP process ID.

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.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the IGP database collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Select **IGP database** from the **Basic topology** section and click **Next**.

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

- **Index**—Index number for the seed router.
- **Router IP**—Management IP address of the seed router.
- **Protocol type**—Select the IGP protocol that is running on the network. The options are: ospf, ospfv3, isis, and isisv6.

  If you choose either **ospf** or **ospfv3** as the Protocol type, enter the value for **OSPF area** in the Advanced page (click ⚙). The OSPF area option specifies the area ID or all. The default is area 0.

  If you choose either **isis** or **isisv6** as the Protocol type, enter the value for **ISIS level** (1, 2, or BOTH) in the Advanced page (click ⚙).
- **Collect interfaces**—Check this check box to discover full network topology. By default, this option is enabled.

Step 4 (Optional) To add more seed routers, click **+ Add router** and repeat Step 3 for each seed router. Ensure that the index number is unique for each seed router.

Step 5 (Optional) To exclude or include individual QoS information from the nodes, under **Advanced settings** > **QoS Node Filter** section, click **+ Add node filter** and enter the values as required.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see IGP and SR-PCE Collection Advanced Options, on page 53.

Step 7 Click **Next**.

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

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 34.
- 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 32.

Collect Topology Information Using the SR-PCE Collector

Note In Cisco Crosswork Planning, there are two topology collectors: IGP database and SR-PCE. In a single collection, you can choose any one of these collectors for collecting information related to topology. Selecting both collectors is not permitted.

To use the IGP database collector for topology collection, see Collect Topology Information Using the IGP Database Collector, on page 50.

The **SR-PCE** collector discovers Layer 3 topology using SR-PCE. An SR-PCE agent is a Cisco Crosswork Planning component which will connect to SR-PCE server and process the telemetry data sent by server. SR-PCE agent uses two different REST connections with SR-PCE, one for LSP and the other for Topology data collection. After topology and LSP data collection, SR-PCE agent will (optionally) subscribe to SR-PCE and listen to further network change events.

Node and interface/port properties are discovered using SNMP. For testing purposes, you can also use the SR-PCE topology discovery using SR-PCE only (the Extended discovery field disabled) when no SNMP access is available. 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 also 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 as the loopback address associated with SRv6 is not obtained using SR-PCE. To populate the SRv6NodeSIDPrefixLoopbacks details, you must 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 External Scripts Against a Network Model, on page 83.

Note

- The default ISIS level is set to level2 for NodePrefixLoopbacks. The same is also populated for an OSPF network.
- Cisco Crosswork Planning does not reflect the update of non-null to null value in the FlexAlgo columns. The values will start reflecting after a DARE re-sync.

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

Note

- Dual stack support (capability to handle both IPv4 and IPv6 simultaneously), and the configuration of OSPF or ISIS on an interface are populated correctly as part of data collection. However, during SR-PCE collection, 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.
- 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.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.
- An SR-PCE agent must be configured and running. For more information, see Configure Agents, on page 24.

Follow these steps to configure the SR-PCE collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Select **SR-PCE** from the **Basic topology** section and click **Next**.

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

- **SR-PCE host**—Choose an SR-PCE agent.
- **Backup SR-PCE host**—Choose a backup SR-PCE agent. You can enter the same SR-PCE agent if you do not have a backup.
- **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**—Choose 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 enter the details in the relevant fields. For descriptions of these advanced options, see IGP and SR-PCE Collection Advanced Options, on page 53.

Step 5 Click **Next**.

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

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 34.
- 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 32.

IGP and SR-PCE Collection Advanced Options

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

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	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
QoS node filter	Indicates the filter for determining the nodes for which the QoS data is obtained.
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 is used when IS-IS TE extensions are not enabled.) • OFF—Performs no guessing. • Safe—Chooses guesses that have 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 to interfaces. Circuit removal is sometimes required with IS-IS databases to fix IS-IS advertising inconsistencies.
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.
Minimum IP guessing	Indicates the minimum IP guessing prefix length. All interfaces with equal or larger prefix lengths are considered.
Minimum prefix length	Indicates the minimum prefix length to allow when finding parallel links. All interfaces with equal or larger prefix lengths (but less than 32) are considered.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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 only have a single link end (not common).

Collect LSP Information

The **LSP** collector collects the RSVP LSP information in the network using SNMP.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the LSP collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **LSP** from the **Advanced modeling** section 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 as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Get FRR LSPs**—Check the **Enabled** check box to discover Multiprotocol Label Switching (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 55.

Step 7 Click **Next**.

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

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 34.
- 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 32.

LSP Collection Advanced Options

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

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 the LSPs.
Get extras	Collects additional LSP properties.
Use signaled name	Uses the LSP tunnel signaled name instead of LSP tunnel name (IOS-XR).
Auto bandwidth	Discovers auto bandwidth.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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

The **PCEP LSP** collector uses the data collected from the SR-PCE collector and appends LSP information, thus creating a new network model.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.
- Confirm that BGP-LS topology collection using SR-PCE (SR-PCE collector) has been completed for a network. You will need to use this model as the source network for collecting LSPs. For more information, see Collect Topology Information Using the SR-PCE Collector, on page 51.

Follow these steps to configure the PCEP LSP collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Select **SR-PCE** from the **Basic topology** section.

Step 3 Select **PCEP LSP** from the **Advanced modeling** section 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 as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Agents**—Choose the relevant SR-PCE agents from the drop-down list. For information on creating agents, see Configure Agents, on page 24.
- **Reactive network**—Check the **Enabled** check box to subscribe to notifications from SR-PCE to update LSPs based on addition or deletion. This option is enabled by default.

Step 6 (Optional) Expand the **Advanced settings** panel and enter the following 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**—Enter the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.

Step 7 Click **Next**.

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

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 34.
- 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 32.

Collect Multicast Flow Data from a Network

The **Multicast** collector collects multicast flow data from a given network. It is a collection of the following collectors:

- **Login find multicast**—Log in to the router to fetch or parse multicast flow data.
- **Login poll multicast**—Log in to the router to get multicast traffic rate
- **SNMP find multicast**—Collect multicast data for multicast flows using SNMP.
- **SNMP poll multicast**—Collect traffic data rate for multicast flows using SNMP.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the Multicast collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Multicast** from the **Traffic and Demands** section 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 as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose the source collector whose output serves as the input for this collector.
- **Data collection source**—Choose the collector using which you want 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. Based on the collectors that you selected in the previous step, the options differ. For descriptions of these advanced options, see Multicast Collection Advanced Options, on page 59.

Step 7 Click **Next**.

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

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 34.

- 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 32.

Multicast Collection Advanced Options

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

Option	Description
Login find multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
Use existing config	Uses existing collected multicast configurations from cache.
Force config update	Updates multicast configuration files even if they exist in the data directory.
Save configs	Specifies whether the multicast configurations are to be saved in the cache or discarded.
Overwrite files	Specifies if the existing files are to be overwritten.
Login poll multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
No of samples	Indicates the number of samples that will be taken.
Polling interval	Indicates the time delay between the login rate readings (in seconds).
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Specifies how to filter multicast traffic from multiple sources for each S|G group.
Use existing config	Uses existing collected multicast configurations from cache.
Force config update	Updates multicast configuration files even if they exist in the data directory.
Save configs	Specifies whether the multicast configurations are to be saved in the cache or discarded.
Overwrite files	Specifies if the existing files are to be overwritten.
SNMP find multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.

Option	Description
SNMP poll multicast settings	
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
No of samples	Indicates the number of samples that will be taken.
Polling interval	Indicates the time delay between the login rate readings (in seconds).
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Specifies how to filter multicast traffic from multiple sources for each S|G group.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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 Topology

The **BGP** collector discovers BGP topology via SNMP and login. It 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 Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the BGP collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **BGP** from the **Advanced modeling** section 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 as per your needs. Update the parameters, if required.

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

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see BGP Topology Advanced Options, on page 61.

Step 7 Click **Next**.

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

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 34.
- 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 32.

BGP Topology Advanced Options

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

Option	Description
ASN include	Allows you to enter the ASNs to include. By default, all ASNs are included.
Internal ASNs	Allows you to enter the internal ASNs.
Protocol	Specifies the Internet Protocol (IP) versions. The options are: IPv4 and IPv6.
Min IPv4 prefix length	Indicates the minimum prefix length to control how restrictive IPv4 subnet matching is in discovering interfaces as BGP links.
Min IPv6 prefix length	Indicates the minimum IPv6 prefix length to control how restrictive IPv6 subnet matching is in discovering interfaces as BGP links.
Login multi hop	Indicates whether to log in to routers that potentially contain multi-hop peers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values: cisco, juniper, alu, huawei.
Fallback login platform	Indicates the fallback vendor in case platform detection fails. Valid values: cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router.
Telnet username prompt	Indicates the alternative custom username prompt.

Option	Description
Telnet password prompt	Indicates the alternative custom password prompt.
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	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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	Description
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

The **VPN** collector discovers Layer 2 and Layer 3 VPN topology.

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

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the VPN collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **VPN** from the **Advanced modeling** section 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 as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

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

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

- **Data collection timeout**—Maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
- **Verbosity**—Log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 1 to 60.
- **Net recorder**—Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. If set to 'Record', SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. If set to '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.

Step 7 Click **Next**.

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

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 34.
- 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 32.

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.

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

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the Inventory collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Inventory** from the **Traffic and Demands** section 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 as per your needs. Update the parameters, if required.

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

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see Inventory Collection Advanced Options, on page 69.

Step 7 Click **Next**.

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

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 34.
- 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 32.

Inventory Collection Advanced Options

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

Option	Description
Get inventory options	
Login allowed	Allows logging in to the router to collect inventory data.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 30 minutes.
Build inventory options	
Exclude file	Indicates the file containing ExcludeHWList table that defines hardware characteristics to match against for exclusion in the output. Click the **Download sample file** link to download a sample file containing ExcludeHWList table.

Option	Description
Guess template	Indicates whether to broaden the search when processing raw inventory data.
Template file	Indicates the hardware template file containing HWInventory Templates and HWNameFormatRules tables. Click the **Download sample file** link to download a sample template file.
Hardware spec file	Indicates the file containing HardwareSpec table that 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 containing HardwareSpec table.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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 Port, LSP, SRLG, and VPN Information Using Configuration Parsing

Note The **Config parsing** collector is not a base topology collector. It must only be used to augment details missing from other methods of collection like SNMP and SR-PCE.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the Config parsing collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Config parsing** from the **Advanced modeling** section 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 as per your needs. Update the parameters, if required.

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

Step 6 Expand the **Get config** and **Parse config** panels, and enter the details in the relevant fields. For field descriptions, see Configuration Parsing Advanced Options, on page 71.

Note

- L2VPN config parse is not supported.
- When L3VPN information is collected by Config Parsing collector, it is assumed that all VPNs are connected to each other.
- If the Config Parsing collector is collecting VPN information and VPN collector is also being run, make sure that VPN collector is before Config Parsing collector in the collector chain.
- Single ended SRLGs with other end missing will be collected via SR-PCE. SRLGSCircuits table is not updated for the same though.

Step 7 Click **Next**.

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

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 34.
- 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 32.

Configuration Parsing Advanced Options

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

Option	Description
Get config options	

Option	Description
Collect configuration	Collects configuration from devices or routers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values: cisco, juniper, alu, huawei.
Fallback login platform	Indicates the fallback vendor in case platform detection fails. Valid values: cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router.
Telnet username prompt	Indicates the alternative custom username prompt.
Telnet password prompt	Indicates the alternative custom password prompt.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Parse config options	
Protocol type	Allows you to choose 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 Level 1 and Level 2 metrics. If both are selected, the agent combines both levels into a single network. Level 2 metrics take precedence.
OSPF area	Indicates whether to collect a single OSPF area or all areas. This option specifies the area ID or all. The default is area 0.
ASN	Indicates the Autonomous System Number (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, VPN, FRR, SR LSPS, LMP, and SR Policies.
Circuit match	Indicates the criteria to use to form circuits.
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. • None—Does not create port circuits.
OSPF process ID	Indicates the OSPF process ID to use when there are multiple OSPF processes.

Option	Description
IS-IS instance ID	Indicates the IS-IS instance ID to use when there are multiple IS-IS instances.
Loopback interface	Indicates the loopback interface number to use for the router IP.
Resolve references	Resolves IP address references, if enabled.
Multithreading	Indicates whether to use multithreading.
Filter showcommands	Filters multiple show commands.
Build topology	Builds network topology after parsing the configuration.
Shared media	Creates pseudonodes for shared media.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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.

Improve Network Model Visualization

The **Layout** collector adds layout properties to a source network model to improve visualization when importing 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 simply 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 Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the Layout collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Layout** from the **Traffic and Demands** section 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 as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

- **Source**—Choose 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**—Maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.

Step 7 Click **Next**.

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

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 34.
- 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 32.

Collect Traffic Statistics

The **Traffic collection** collector collects traffic statistics (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's name is the same as that of the collection.

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

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.
- If collecting VPN traffic, a VPN network model must exist. See Discover VPN Topology, on page 63.
- If collecting LSP traffic, an LSP network model must exist. See Collect LSP Information, on page 55.

Follow these steps to configure the Traffic collection collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Traffic collection** from the **Traffic and Demands** section 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 as per your needs. Update the parameters, if required.

Step 5 Check the **Traffic collection** check box to enable the traffic poller.

Step 6 From the **Source** drop-down list, choose the source collector whose output serves as the input for this collector.

Step 7 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.

Step 8 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.

Step 9 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.

Step 10 (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 76.

Step 11 Click **Next**.

Step 12 Preview the configuration and then click **Create** to create the collection.

You need to configure a schedule to populate the collected traffic data in the plan files. 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.

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 34.
- 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 32.

Traffic Collection Advanced Options

You can configure several advanced options when using Traffic collection.

Option	Description
Minimum window length	Indicates the minimum window length for traffic calculation, in seconds. The default is 300 seconds.
Maximum window length	Indicates the maximum window length for traffic calculation, in seconds. The default is 450 seconds.
Raw counter TTL	Indicates how long to keep raw counters (in minutes). The default is 15 minutes.
Discard over capacity	Discards traffic rates that are higher than capacity.
Net recorder file max size	Indicates the maximum size for the net record file.
Data collection timeout	Indicates the maximum time allowed for data collection (in minutes). The internal tools used for data collection will time out and exit if the specified limit is exceeded. The default is 60 minutes.
Debug	

Option	Description
Verbosity	Indicates the log verbosity level. It refers to the degree of detail and information provided in log messages. The default is 30, and the valid range is 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.

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

The **Demand deduction** collector collects information regarding traffic demands from the network.

Before you begin

Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Follow these steps to configure the Demand deduction collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **Demand deduction** from the **Traffic and Demands** section 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 as per your needs. Update the parameters, if required.

Step 5 From the **Source** drop-down list, choose 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. In the **Add Mesh Step** window, enter the following details:

a) In the **Name** field, enter the name for the step.

b) In the **Step number** field, enter the order in which this step must be performed.

c) From the **Tool** drop-down list, choose the required tool. The available tools are: Demands for P2MP LSPs, Demand deduction, External executable script, Copy demands, Demands for LSPs, and 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. Based on the tool you selected, the options differ in this section.
f) (Optional) Expand the **Advanced** panel and enter the 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 in the Mesh Step window.

Step 7 Click **Next**.

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

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 34.
- 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 32.

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

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.
- Configure NetFlow agents to operate in single mode.

Follow these steps to configure the NetFlow collector.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

Step 3 Select **NetFlow** from the **Traffic and Demands** section 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 as per your needs. Update the parameters, if required.

Step 5 Enter the following configuration parameters:

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

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

(Optional) Enter the information in the other fields. For field descriptions, see NetFlow Collection Advanced Options, on page 82.

Step 7 (Optional) Expand the **IAS flows** and **Demands** panels, and enter the details in the relevant fields. For descriptions of these options, see NetFlow Collection Advanced Options, on page 82.

Step 8 Click **Next**.

Step 9 Preview the configuration and then click **Create** to create the collection.

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 34.
- 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 32.

NetFlow Collection Advanced Options

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

Option	Description
Common config settings	
Split AS flows on ingress	Indicates the traffic aggregation strategy for external ASNs.
ASN	Indicates the ASN of the internal AS in the network.
Address family	Indicates the protocol version to include in IAS flows and demands computation.
Ext node tags	Allows you to enter one or more node tags. Click + to enter a list of one or more node tags.
Split AS flows on egress	Splits Inter AS flows on egress through all the interfaces connecting to the egress AS.
Extra aggregation	Allows you to select the list of aggregation keys from the drop-down list.
Log level	Indicates the log level of the tool. The options are: Off, Fatal, Error, Warn, Notice, Info, Debug, and Trace.
Number of threads	Indicates the maximum number of threads to be used in parallel computation.
IAS flows settings	
Trim inter AS flows	Indicates the value in MBits/sec below which the Inter AS flows for traffic is strictly discarded.

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

Run External Scripts Against a Network Model

The external scripts let you run a customized script against a selected network model. You might want to do this when you want specific data from your network that existing Cisco Crosswork Planning collectors do not 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 want.

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.

Before you begin

- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.
- The custom script must be available.

Follow these steps to run external scripts against a network model.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 and Edit Collections, on page 32.

Step 2 Choose one of the basic topology collectors, as per your requirement.

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

Step 4 Enter the following details:

- **Collector name**—Enter 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 have selected this option, then 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, then 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 any supporting file that is required for the custom script to execute successfully.
- **Executable script**—Enter the custom script details.
- **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 specify 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.

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 34.

Merge AS Plan Files

The **Merge AS** tool helps to merge plan files from different Autonomous Systems (AS). The **Merge AS** tool resolves any conflicts across the plan files. Plan files in native format are also supported.

Each AS can be on a different Cisco Crosswork Planning server.

Note

- Only Autonomous Systems (AS), Circuits, Nodes, Interfaces, External Endpoints, External Endpoint Members with virtual nodes and unresolved interfaces are resolved.
- The following demands are resolved:
    - Source or Destination associated with virtual node that are resolved with real node.
    - Source or Destination associated with the interface in a specific format.
    - Source or Destination associated with the External Endpoints.
- The following demands are not resolved:
    - Source or Destination associated with ASN number only.
- For a given plan file, the internal AS number must match what other plan files see as an external AS number, and all the Autonomous Systems that are going to be merged need to be discovered in all the plan files.

Before you begin

- Collect topology and traffic information for different Autonomous Systems (AS).
- The plan files from different AS have to be present on the same Cisco Crosswork Planning server and the path to the plan files must be mentioned.
- Complete the steps mentioned in Workflow: Preconfiguration Steps, on page 10.

Procedure

Step 1 Determine if you want to create a new collection or edit an existing one. For details, see Create Collections, on page 29 or Edit Collections, on page 32.

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

Step 3 Select **Merge AS** from the **Tools** section and click **Next**.

Step 4 Enter the following 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 the tag name for rows that are modified.

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

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

Note

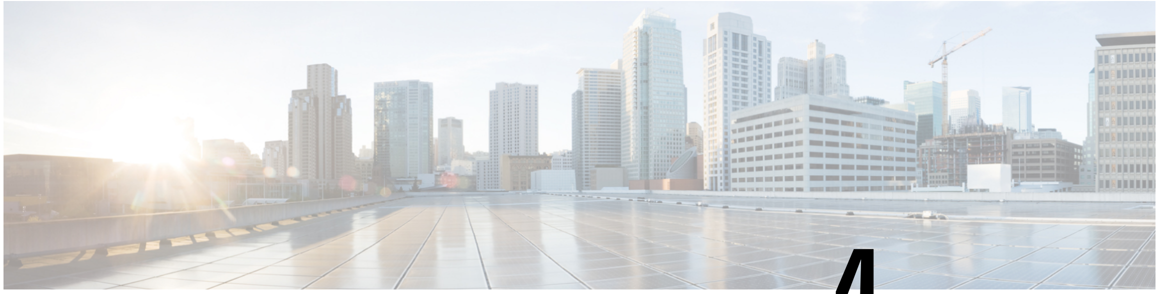
If you are migrating the configuration either from Cisco WAE or from another Cisco Crosswork Planning instance, ensure that the **DB file** field is updated with the correct file after importing the configuration. This is necessary because, after importing the configuration, the server restores only 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.

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 34.
- 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 32.



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 Overview

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it’s secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

Workflow: Smart Licensing Configuration

The high-level steps involved in configuring Cisco Smart Licensing are as follows:

Table 9: Smart Licensing Configuration Workflow

Step	Action
1. Set up a Smart Account on Cisco Software Central (software.cisco.com).	Go to Smart Account Request and follow the instructions on the website.
2. (Optional) Configure transport settings.	Configure the Transport Mode Between Cisco Crosswork Planning and CSSM, on page 88.
3. Register Cisco Crosswork Planning with the Cisco Smart Software Manager (CSSM).	See: • Register Cisco Crosswork Planning via Token, on page 89 • Register Cisco Crosswork Planning via Offline Reservation, on page 92

A **Cisco Smart Account** provides the repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage and track Cisco purchases. The **Cisco Smart Software Manager (CSSM)** enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you may create and manage multiple virtual accounts within your Smart Account to manage licenses. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

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

Configure the Transport Mode Between Cisco Crosswork Planning and CSSM

You can configure the transport settings to decide how Cisco Crosswork Planning communicates with CSSM.

- **Direct**: Cisco Crosswork Planning directly connects with CSSM.
- **Transport Gateway**: Cisco Crosswork Planning communicates via a Transport Gateway or CSSM On-prem, which replicates the cloud-based user experience but keeps all communication on premises. For more information on the CSSM On-prem option, see the Smart Software Manager guide.

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

- **HTTP/HTTPS Proxy**: Cisco Crosswork Planning communicates to the direct mode end point via the configured proxy, if proxy is configured.

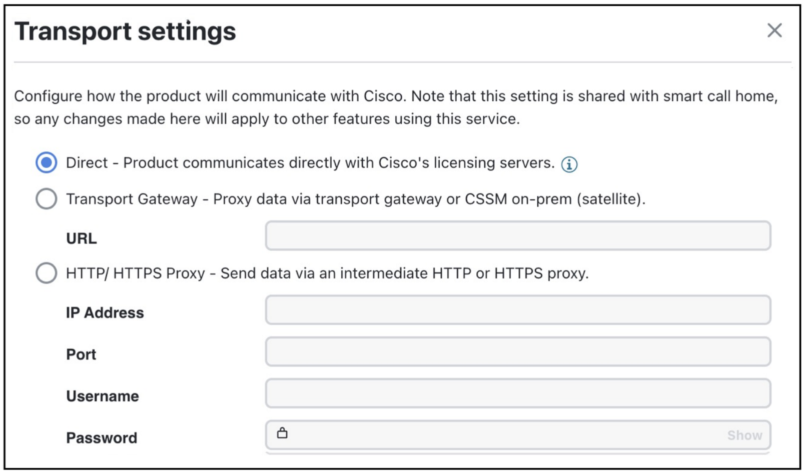
Note Transport settings cannot be changed while the Cisco Crosswork Planning product is in Registered mode. You have to de-register to change them.

Procedure

Step 1 From the main menu, choose **Licensing**. The Smart License page opens.

Step 2 The **Transport settings** field displays the current transport mode selected. To modify, click **View / Edit**. The Transport settings dialog box is displayed.

Figure 23: Transport Settings Dialog Box



Transport settings

Configure how the product will communicate with Cisco. Note that this setting is shared with smart call home, so any changes made here will apply to other features using this service.

● Direct - Product communicates directly with Cisco's licensing servers.

○ Transport Gateway - Proxy data via transport gateway or CSSM on-prem (satellite).

URL

○ HTTP/ HTTPS Proxy - Send data via an intermediate HTTP or HTTPS proxy.

IP Address

Port

Username

Password

Step 3 Select the relevant transport mode and make relevant entries in the fields provided.

Step 4 Click **Save**.

Register Cisco Crosswork Planning via Token

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

Note For information on generating the registration token, please refer to the support resources provided in the Cisco Software Central web page.

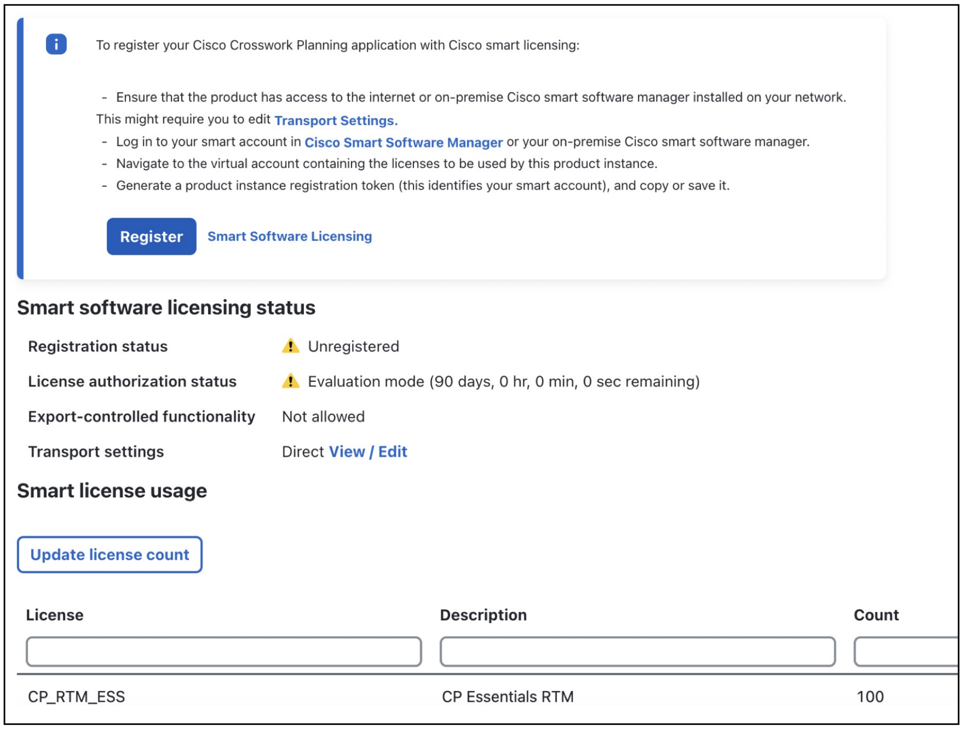
Before you begin

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

Procedure

Step 1 From the main menu, choose **Licensing**. The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 24: Smart Software Licensing Unregistered Example



To register your Cisco Crosswork Planning application with Cisco smart licensing:

- Ensure that the product has access to the internet or on-premise Cisco smart software manager installed on your network. This might require you to edit **Transport Settings**.
- Log in to your smart account in **Cisco Smart Software Manager** or your on-premise Cisco smart software manager.
- Navigate to the virtual account containing the licenses to be used by this product instance.
- Generate a product instance registration token (this identifies your smart account), and copy or save it.

Smart software licensing status

Registration status	⚠ Unregistered
License authorization status	⚠ Evaluation mode (90 days, 0 hr, 0 min, 0 sec remaining)
Export-controlled functionality	Not allowed
Transport settings	Direct **View / Edit**

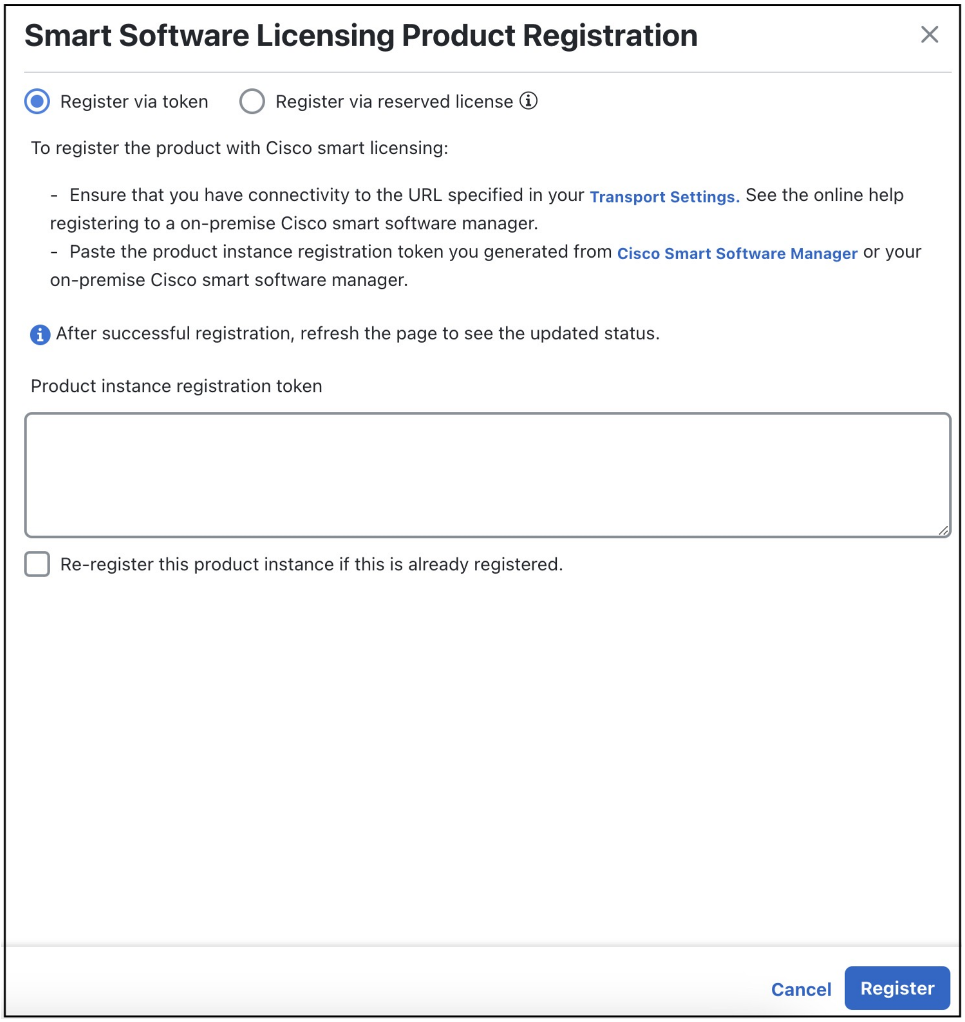
Smart license usage

License	Description	Count
CP_RTM_ESS	CP Essentials RTM	100

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

The Smart Software Licensing Product Registration dialog box is displayed.

Figure 25: Smart Software Licensing Product Registration Dialog Box



Smart Software Licensing Product Registration

● Register via token ○ Register via reserved license ⓘ

To register the product with Cisco smart licensing:

- Ensure that you have connectivity to the URL specified in your Transport Settings. See the online help registering to a on-premise Cisco smart software manager.
- Paste the product instance registration token you generated from Cisco Smart Software Manager or your on-premise Cisco smart software manager.

ⓘ After successful registration, refresh the page to see the updated status.

Product instance registration token

□ Re-register this product instance if this is already registered.

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

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**. It may take a few minutes to process the registration. If successful, the 'Product Registration completed successfully' message is displayed.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Note

- It will take a minimum of 20 seconds for the request to succeed. If you do not get the correct response from the backend within the first 20 seconds, the UI will continue to check every 10 seconds for up to five minutes. If no response is obtained after five minutes, the system will display a generic error message.
- If you encounter a registration error (for example, `"Communication send error"` or `"Invalid response from licensing cloud"`), wait for some time and retry the registration. If the error persists after multiple attempts, contact the Cisco Customer Experience team.

- In some cases, after successful registration, the page may need to be refreshed manually to see the updated status.

Manually Perform Licensing Actions

The renewal of registration and authorization is automatically enabled for Cisco Crosswork Planning, by default. However, in the event of a communication failure between the application and the Cisco server, these actions can be manually initiated. You can use the **Actions** drop-down button to manually renew, re-register and de-register the application.

Before you begin

Make sure that the 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 and select the relevant option for the following quick actions.

a) **Actions** > **Renew Authorization**: To renew the authorization manually if the automatic renewal service fails at the end of 30 days.

b) **Actions** > **Renew Registration**: To renew the registration manually if the automatic renewal service fails at the end of 6 months.

c) **Actions** > **Re-register**: Re-register the application, for example, on account of the expiry of registration tokens.

d) **Actions** > **De-register**: De-register the application, for example, when the transport settings need to be changed.

Note
Once de-registered, the application will be moved to **Evaluation** mode (if evaluation period is available) or **Evaluation Expired** mode. For more information, see License Authorization Statuses, on page 96.

Register Cisco Crosswork Planning via Offline Reservation

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

Before you begin

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

Procedure

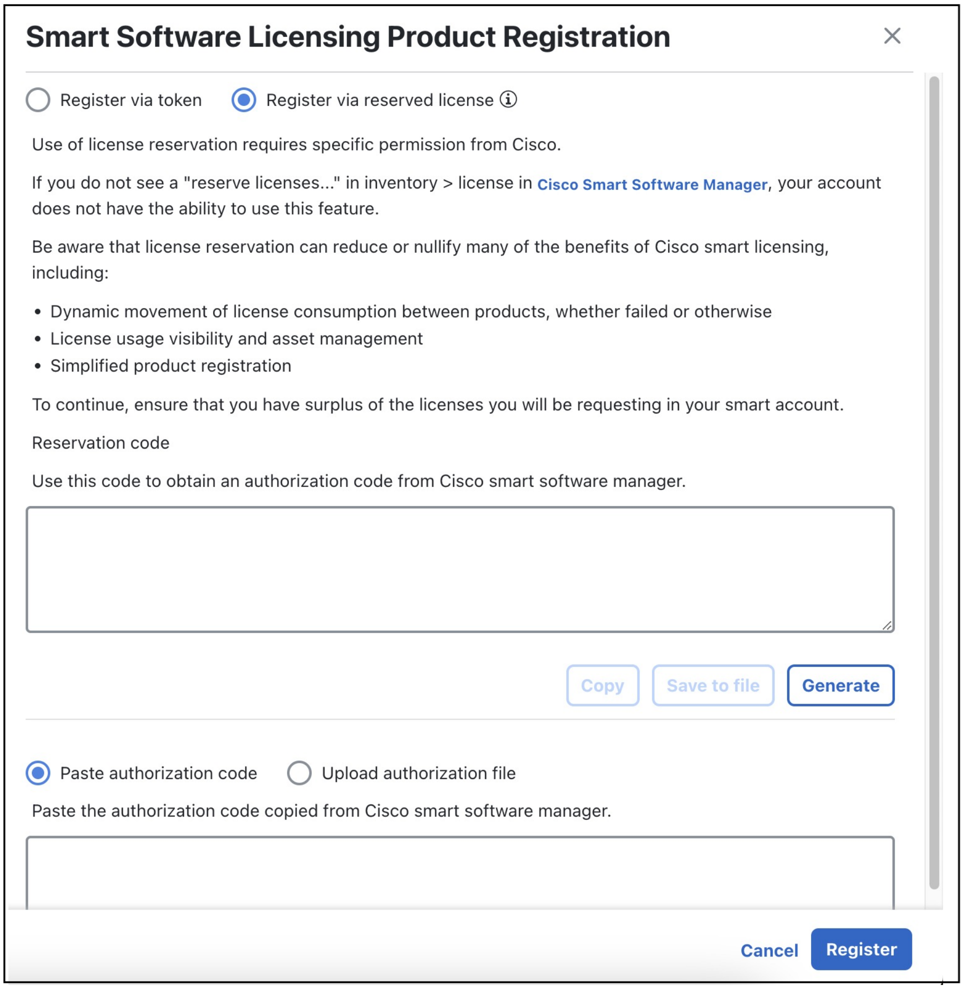
Step 1 From the main menu, choose **Licensing**.

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

The Smart Software Licensing Product Registration dialog box is displayed.

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

Figure 26: Smart Software Licensing Product Registration Dialog Box



Smart Software Licensing Product Registration

○ Register via token ● Register via reserved license ⓘ

Use of license reservation requires specific permission from Cisco.

If you do not see a "reserve licenses..." in inventory > license in Cisco Smart Software Manager, your account does not have the ability to use this feature.

Be aware that license reservation can reduce or nullify many of the benefits of Cisco smart licensing, including:

- Dynamic movement of license consumption between products, whether failed or otherwise
- License usage visibility and asset management
- Simplified product registration

To continue, ensure that you have surplus of the licenses you will be requesting in your smart account.

Reservation code

Use this code to obtain an authorization code from Cisco smart software manager.

● Paste authorization code ○ Upload authorization file

Paste the authorization code copied from Cisco smart software manager.

Step 4 Click the **Generate** button under the Reservation code section. Your Reservation Request Code is generated and populated in the text field. Copy this code using **Copy** button.

Step 5 Go to CSSM and select the appropriate Virtual Account.

Step 6 Click the **Licenses** tab, then click **License Reservation**. Paste the Reservation Request Code that you generated in Step 3 and click **Next**.

Step 7 On the Select Licenses page, select the type of reservation you need. Then, click **Next**.

Step 8 On the Review and Confirm page, click **Generate Authorization Code**. Copy the code using the **Copy to Clipboard** button.

Step 9 Navigate back to the Smart Software Licensing Product Registration page in the Cisco Crosswork Planning UI. Select the **Paste authorization code** radio button and paste the authorization code in the text field.

Step 10 Click **Register**. It may take a few minutes to process the registration.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Update Offline Reservation

Use the **Update Reservation** option to update the license counts reserved via offline reservation.

Procedure

Step 1 From the main menu, choose **Licensing**. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2 Go to CSSM and select the appropriate virtual account.

Step 3 Click the name of the product instance that matches your Product Instance Name.

Step 4 For this product instance, click the **Actions** drop-down button and choose **Update Reservation**.

Step 5 In the Select Licenses screen, select the **Reserve a Specific License** radio button, update the count of the necessary licenses from the list and click **Next**.

Step 6 In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using **Copy to Clipboard** button.

Step 7 Navigate back to the Smart License page on the Cisco Crosswork Planning UI. Click the **Actions** drop-down button and choose **Update Reservation**. Paste the Authorization Code that you generated in the previous step and click **Update**.

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

Step 8 Navigate back to CSSM. Click the required product instance name.

Step 9 Click the **Actions** drop-down button and choose **Enter Confirmation Code**.

Step 10 Enter/paste the Reservation Confirmation Code that was generated in Step 7 and click **OK**.

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

Disable Offline Reservation

Use the **Return Reservation** option to release the reserved licenses. Once the licenses are released, the application will be moved to **Evaluation** mode (if evaluation period is available), or **Evaluation Expired** mode. For more information, see License Authorization Statuses, on page 96.

Procedure

Step 1 From the main menu, choose **Licensing**. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2 Click the **Actions** drop-down button and choose **Return Reservation**.

Step 3 In the Confirm Return Reservation window, click **Confirm**.

A Release Code (Reservation Return Code) is generated. Copy this code using the **Copy** button.

Step 4 Navigate to CSSM and select the appropriate virtual account.

Step 5 Click the name of the product instance that matches your Product Instance Name.

Step 6 For this product instance, click the **Actions** drop-down button and choose **Remove**.

Step 7 In the Remove Reservation pop-up, paste the Reservation Return Code that you generated in Step 3 and click **Remove Reservation**.

The Registration status will be updated to **Unregistered** in the Smart License page of the Cisco Crosswork Planning UI.

Step 8 Navigate back to the Smart License page in the Cisco Crosswork Planning UI. Click the **Actions** drop-down button and choose **Disable License Reservation**.

Update License Counts

In Cisco Crosswork Planning, you can enter number of licenses for usage as per your requirement. Ensure that you have a sufficient number of licenses in the Virtual Account; otherwise, it will be out of compliance.

For the tools in the Cisco Crosswork Planning Design application to function correctly, you must have the appropriate number of licenses. Follow these steps to update the license counts.

Procedure

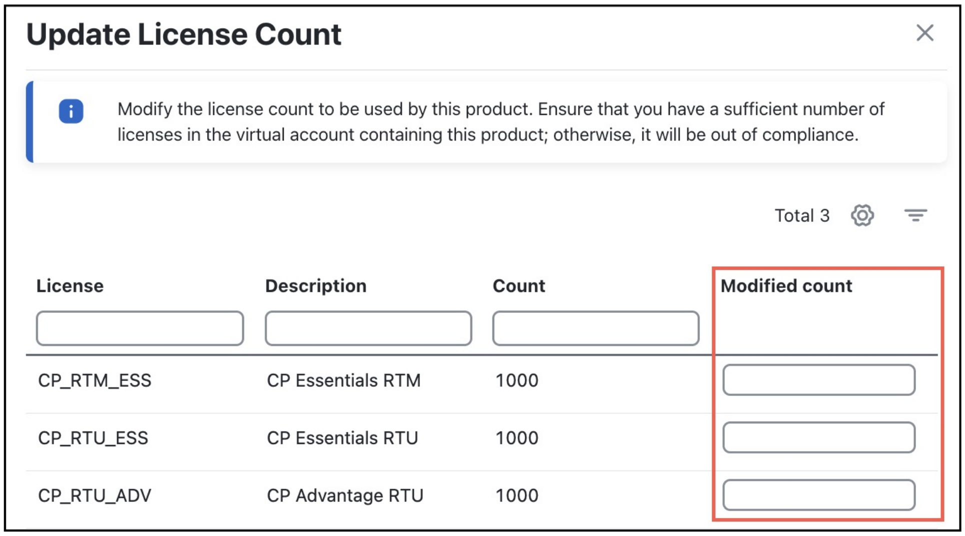
Step 1 From the main menu, choose **Licensing**.

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

The Update License Count window appears.

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

Figure 27: Update License Count



Update License Count

Modify the license count to be used by this product. Ensure that you have a sufficient number of licenses in the virtual account containing this product; otherwise, it will be out of compliance.

License	Description	Count	Modified count
CP_RTM_ESS	CP Essentials RTM	1000	
CP_RTU_ESS	CP Essentials RTU	1000	
CP_RTU_ADV	CP Advantage RTU	1000	

There are three types of licenses in Cisco Crosswork Planning:

- CP_RTM_ESS—You can choose to have either 1 license or a number of licenses equal to the number of nodes in the network. Cisco Crosswork Planning Collector application functions even if only one license is available. 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—You can have a count of 1 for both Cisco Crosswork Planning Collector and Design applications to function correctly.
- CP_RTU_ADV—You can have a count of 1 for both Cisco Crosswork Planning Collector and Design applications to function correctly.

Step 4 Click **Save**.

License Authorization Statuses

Based on the registration status, you can see the following License Authorization Statuses.

Table 10: License Authorization Statuses

Registration Status	License Authorization Status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which the licensed features of the application can be freely used. This state is initiated when you use the application for the first time.
	Evaluation Expired	The application has not been successfully registered at the end of the evaluation period. During this state, the application features are disabled, and you must register to continue using the application.
	Registered Expired	The application is unable to contact the CSSM before the expiration of Identity Certificates and has returned to the unregistered state. The application resumes the remaining evaluation period, if available. At this stage, new registration ID token is required to reregister the application.
Registered	Authorized (In Compliance)	The application has been fully authorized to use the reserved licensed features. The authorization is automatically renewed every 30 days.
	Out of Compliance	The associated Virtual Account does not have enough licenses to reserve for the application's current feature use. You must renew the entitlement/usage limit registered with the token to continue using the application.
	Authorization Expired	The application is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

CHAPTER 5

Manage Administrative Tasks

This chapter contains the following topics:

Manage Certificates

What is a Certificate?

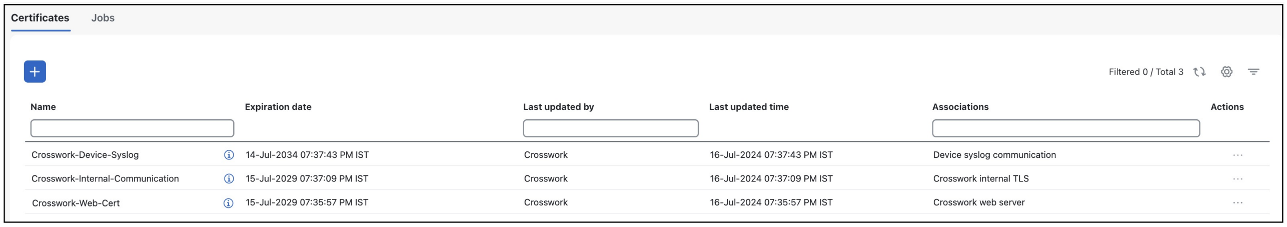
A certificate is an electronic document that identifies an individual, a server, a company, or another entity, and associates that entity with a public key. When a certificate is created with a public key, a matching private key is also generated. In TLS, the public key is used to encrypt data being sent to the entity and the private key is used to decrypt. A certificate is signed by an issuer or a "parent" certificate (Certificate Authority), that is, signed by the parent's private key. Certificates can also be self-signed. In a TLS exchange, a hierarchy of certificates is used to verify the validity of the certificate's issuer. This hierarchy is called a trust-chain and consists of three types of entities: a root CA certificate (self-signed), possibly multiple levels of intermediate CA certificates, and a server (or client) certificate (end-entity). The intermediate certificates act as a “link of trust” linking the server certificates to the CA’s root certificate and providing additional layers of security. Starting from the root certificate's private key, the private key for each certificate in the trust chain signs and issues the next certificate in the chain until finally signing an end entity certificate. The end-entity certificate is the last certificate in the chain and is used as a client or server certificate.

How are Certificates Used in Cisco Crosswork Planning?

Communication between Cisco Crosswork Planning applications and devices as well as between various Cisco Crosswork components are secured using the TLS protocol. TLS uses X.509 certificates to securely authenticate devices and encrypt data to ensure its integrity from source to destination. Crosswork uses a mix of generated and client uploaded certificates. Uploaded certificates can be purchased from Certificate authorities (CA) or can be self-signed. For example, the Cisco Crosswork VM-hosted web server and the client browser-based user interface communicate with each other using Crosswork generated X.509 certificates exchanged over TLS.

The Crosswork Cert Manager is a proxy for multiple microservices and services within the distributed framework and manages all the Crosswork certificates. The Certificate Management UI (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates. The following figure displays the default certificates provided by Cisco Crosswork Planning.

Figure 28: Certificate Management Window



Name	Expiration date	Last updated by	Last updated time	Associations	Actions
Crosswork-Device-Syslog	14-Jul-2034 07:37:43 PM IST	Crosswork	16-Jul-2024 07:37:43 PM IST	Device syslog communication	···
Crosswork-Internal-Communication	15-Jul-2029 07:37:09 PM IST	Crosswork	16-Jul-2024 07:37:09 PM IST	Crosswork internal TLS	···
Crosswork-Web-Cert	15-Jul-2029 07:35:57 PM IST	Crosswork	16-Jul-2024 07:35:57 PM IST	Crosswork web server	···

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 a New Certificate

You can add certificates for the following role:

- **Secure LDAP Communication**: The user uploads the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork, the user can add the LDAP server (see Manage LDAP Servers, on page 115) and associate the certificate.

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

Before you begin

- For information on certificate types and usage, see Certificate Types and Usage, on page 100.
- 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 7.0.

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**. and check the certificate that you want to modify.

Step 2 Click ⋯ on the certificate that you want to modify and select **Update certificate**.

Step 3 Update the necessary options.

Note
While updating a Crosswork Web Server Certificate, provide relevant values for the following fields:

- **Crosswork web CA**: Trust chain file (in PEM format) containing the root CA certificate and zero or more intermediate certificates.
- **Crosswork web intermediate**: An intermediate CA certificate signed with the root CA certificate.
- **Crosswork web intermediate key**: The key associated with the intermediate CA certificate.

- **Crosswork web passphrase**: This is an optional field.

Upon successful validation, the Certificate Management UI logs out automatically and applies the certificate to the Web Gateway.

Step 4 Click **Save**.

Download Certificates

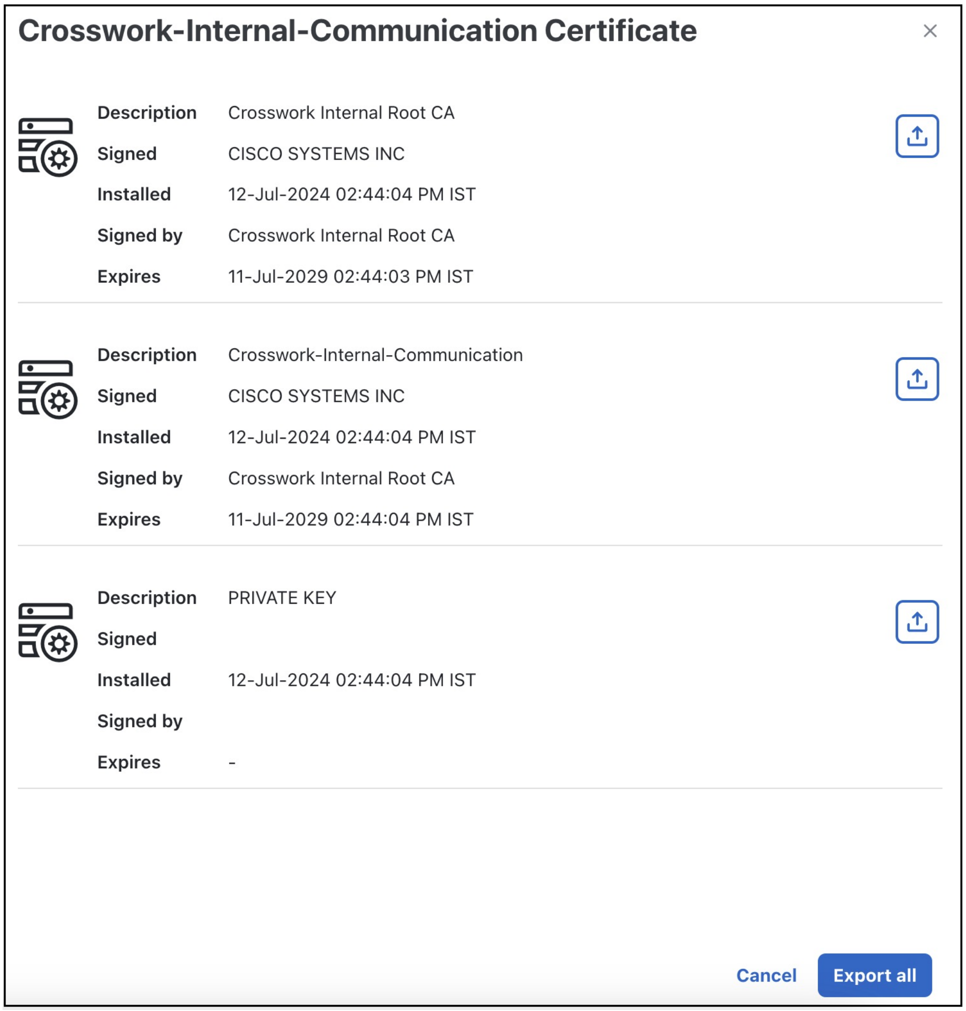
To export certificates, do the following:

Procedure

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

Step 2 Click ⓘ for the certificate you want to download.

Figure 29: Export Certificates



Crosswork-Internal-Communication Certificate

Description	Crosswork Internal Root CA
Signed	CISCO SYSTEMS INC
Installed	12-Jul-2024 02:44:04 PM IST
Signed by	Crosswork Internal Root CA
Expires	11-Jul-2029 02:44:03 PM IST

Description	Crosswork-Internal-Communication
Signed	CISCO SYSTEMS INC
Installed	12-Jul-2024 02:44:04 PM IST
Signed by	Crosswork Internal Root CA
Expires	11-Jul-2029 02:44:04 PM IST

Description	PRIVATE KEY
Signed	
Installed	12-Jul-2024 02:44:04 PM IST
Signed by	
Expires	-

Step 3 To separately download the root certificate, intermediate certificate, and the private key, click ⇪. To download the certificates and private key all at once, click **Export all**.

Manage 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 107).

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 129.

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 11: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager	All	Read, Write
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 104).

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 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 108).

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 104). Later, you can edit the roles themselves to give users the privileges you want (see Edit User Roles, on page 108).

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 on an existing role.

Step 3 Click ⧉ to create a new duplicate entry in the **Roles** table with all the permissions of the original role.

Step 4 Enter a unique name for the cloned role.

Step 5 (Optional) Define the role's settings:

a) Check the check box for every API that the cloned role can access.

b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Edit User Roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

Follow these steps toe 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 12: 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 in Cisco Crosswork Planning 7.0
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 129.

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 118.

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 107.
- 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 **AdministrationAAAServersTACACS+** 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 13: 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.
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 a New Certificate, on page 101.

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 14: 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
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.

Field	Description
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 a LDAP user before creating the required user role, you will get the error message: "`Login failed, policy not found. Please contact the Network Administrator for assistance.`". To avoid this error, ensure to create the relevant user roles in the LDAP server, before setting up a new LDAP server in Cisco Crosswork Planning.
Connection timeout	Enter the timeout value. Maximum timeout is 30 seconds.

See the example at the end of this topic for more details.

c) Click **Add**.

d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Step 3 **To edit a LDAP server**:

a) Select the LDAP server and click ✎.

b) After making changes, click **Update**.

Step 4 **To delete a LDAP server**:

a) Select the LDAP server and click 🗑.

b) Click **Delete** to confirm.

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 **AdministrationAAAServersRADIUS** 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 15: RADIUS field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS name	Only IPv4 DNS name is supported (if DNS name is selected).
Port	The default RADIUS port number is 1645.
Shared secret format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active RADIUS server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For 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.
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 113 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 Cisco Crosswork Planning is re-installed, you must ensure that the latest IDP metadata from Cisco Crosswork Planning 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 a relevant values in the **Number of parallel sessions** and **Number of parallel sessions per user** fields.

Note
Crosswork supports between 5 to 200 parallel session for concurrent users. If the number of parallel sessions are exceeded, an error is displayed while logging in to Crosswork.

Note
Crosswork supports 50 simultaneous NBI sessions up to 400 sessions.

Step 5 Check the **Enable source IP for auditing** check box to log the IP address of the user (source IP) for auditing and accounting. This check box is disabled by default. Once you enable this option and relogin to Cisco Crosswork 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 is enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

Note
Local password policy allows administrators to configure the number of unsuccessful login attempts a user can make before they are locked out of 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.

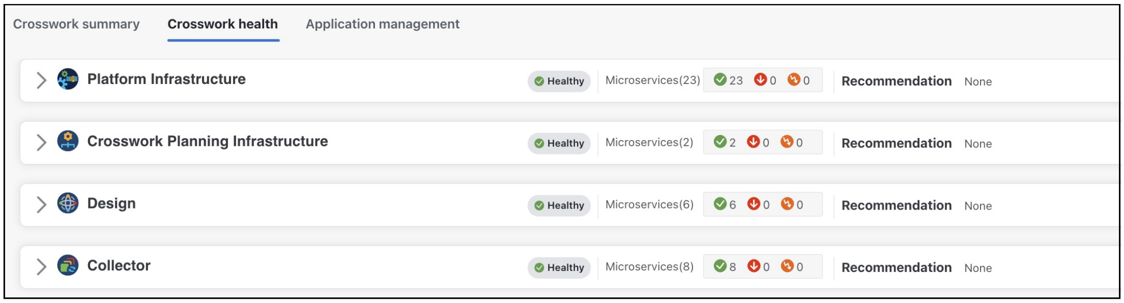
From the main menu, choose **Administration** > **Crosswork Manager** to access the **Crosswork summary** and **Crosswork health** windows. Each window provides various views to monitor system and application health. It also supplies tools and information that, with support and guidance from your Cisco 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.

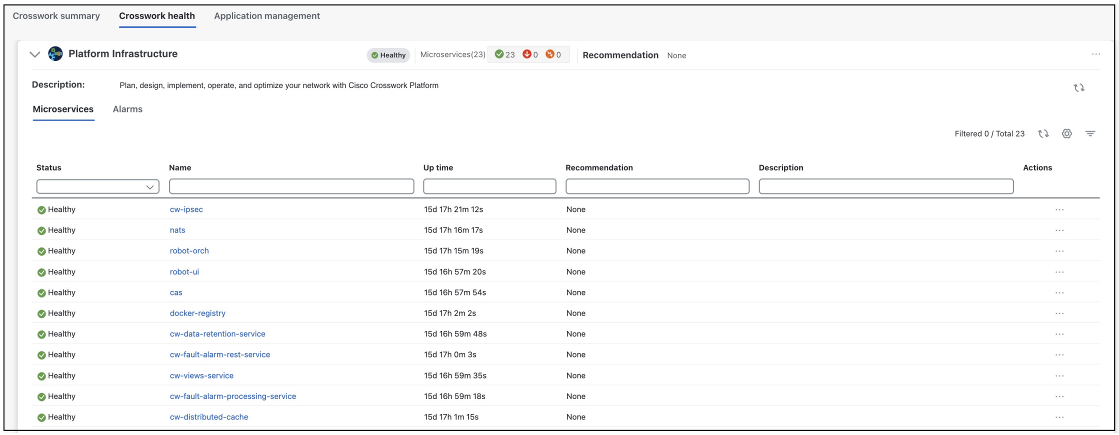
Figure 30: Crosswork Health tab



Platform Infrastructure	Healthy	Microservices(23)	✓ 23	0	0	Recommendation	None
Crosswork Planning Infrastructure	Healthy	Microservices(2)	✓ 2	0	0	Recommendation	None
Design	Healthy	Microservices(6)	✓ 6	0	0	Recommendation	None
Collector	Healthy	Microservices(8)	✓ 8	0	0	Recommendation	None

Within this window, expand an application row to view Microservice and Alarm information.

Figure 31: Microservices Tab



Description: Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Status	Name	Up time	Recommendation	Description	Actions
Healthy	cw-ipsec	15d 17h 21m 12s	None		···
Healthy	nats	15d 17h 16m 17s	None		···
Healthy	robot-orch	15d 17h 15m 19s	None		···
Healthy	robot-ui	15d 16h 57m 20s	None		···
Healthy	cas	15d 16h 57m 54s	None		···
Healthy	docker-registry	15d 17h 2m 2s	None		···
Healthy	cw-data-retention-service	15d 16h 59m 48s	None		···
Healthy	cw-fault-alarm-rest-service	15d 17h 0m 3s	None		···
Healthy	cw-views-service	15d 16h 59m 35s	None		···
Healthy	cw-fault-alarm-processing-service	15d 16h 59m 18s	None		···
Healthy	cw-distributed-cache	15d 17h 1m 15s	None		···

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.

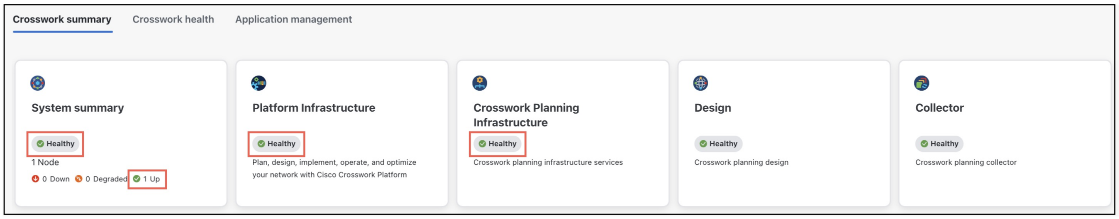
Procedure

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 32: Crosswork Summary



System summary
✓ Healthy
1 Node
0 Down 0 Degraded ✓ 1 Up

Platform Infrastructure
✓ Healthy
Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Crosswork Planning Infrastructure
✓ Healthy
Crosswork planning infrastructure services

Design
✓ Healthy
Crosswork planning design

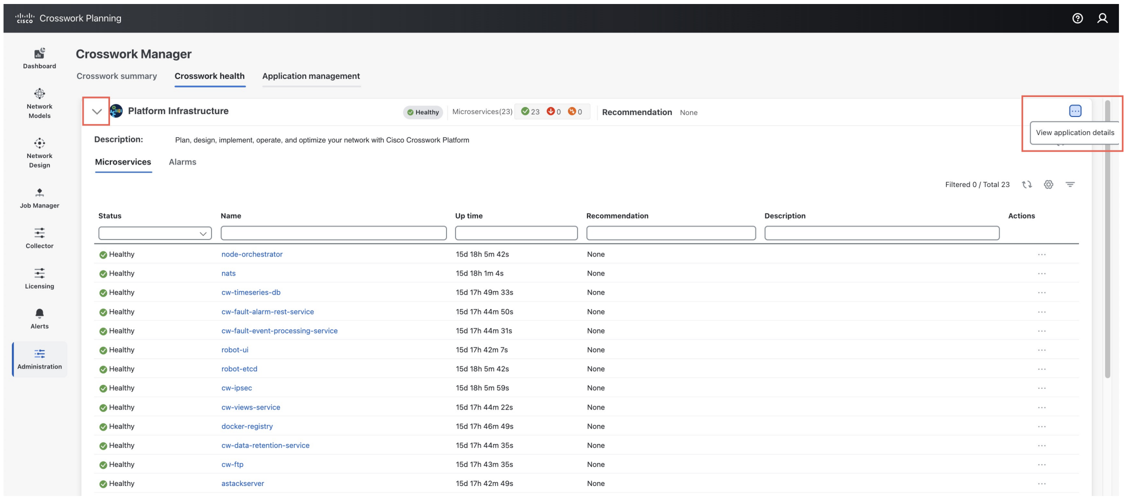
Collector
✓ Healthy
Crosswork planning collector

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 33: Crosswork Health



Crosswork Manager

Platform Infrastructure ✓ Healthy Microservices(23) ✓ 23 0 0 **Recommendation** None

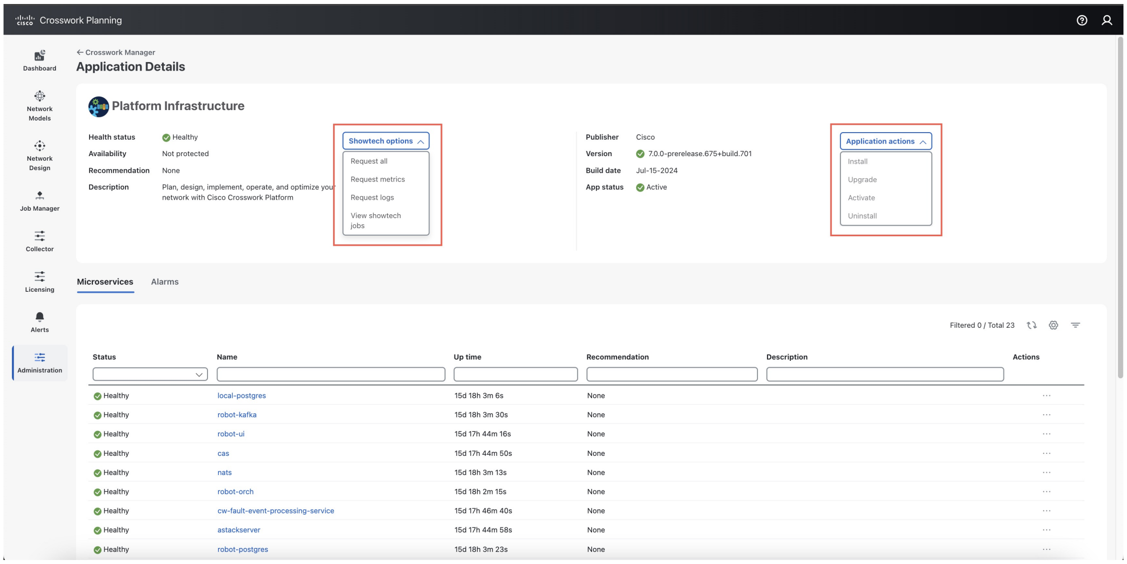
Description: Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Filtered 0 / Total 23

Status	Name	Up time	Recommendation	Description	Actions
✓ Healthy	node-orchestrator	15d 18h 5m 42s	None		...
✓ Healthy	nats	15d 18h 1m 4s	None		...
✓ Healthy	cw-timeseries-db	15d 17h 49m 33s	None		...
✓ Healthy	cw-fault-alarm-rest-service	15d 17h 44m 50s	None		...
✓ Healthy	cw-fault-event-processing-service	15d 17h 44m 31s	None		...
✓ Healthy	robot-ui	15d 17h 42m 7s	None		...
✓ Healthy	robot-etcd	15d 18h 5m 42s	None		...
✓ Healthy	cw-ipsec	15d 18h 5m 59s	None		...
✓ Healthy	cw-views-service	15d 17h 44m 22s	None		...
✓ Healthy	docker-registry	15d 17h 46m 49s	None		...
✓ Healthy	cw-data-retention-service	15d 17h 44m 35s	None		...
✓ Healthy	cw-ftp	15d 17h 43m 35s	None		...
✓ Healthy	astackserver	15d 17h 42m 49s	None		...

c) From the Application Details window, you can check and review microservice details, restart microservices, and collect showtech information. You can also perform installation-related tasks from this window.

Figure 34: Application Details



Application Details

Platform Infrastructure

Health status: Healthy
Availability: Not protected
Recommendation: None
Description: Plan, design, implement, operate, and optimize you network with Cisco Crosswork Platform

Publisher: Cisco
Version: 7.0.0-prerelease.675+build.701
Build date: Jul-15-2024
App status: Active

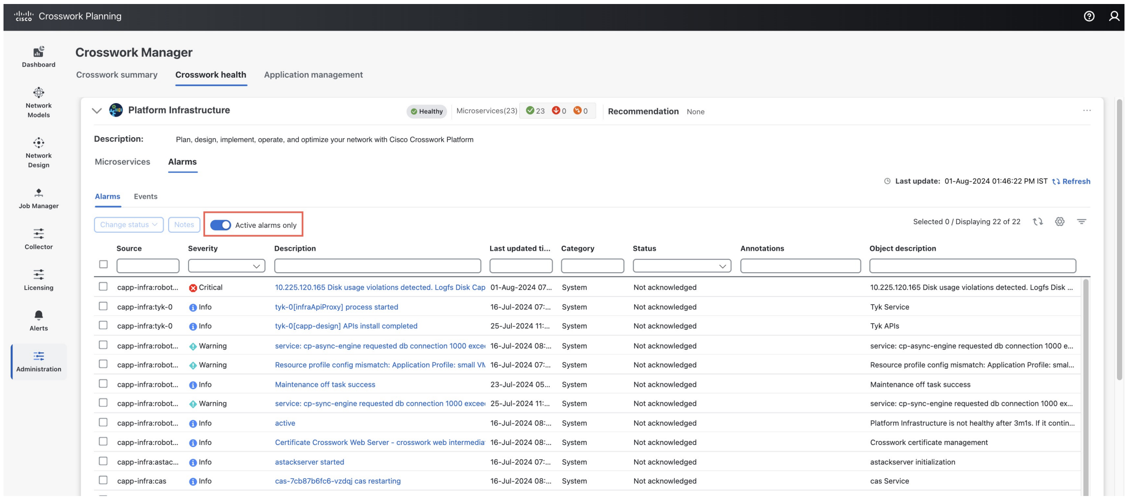
Filtered 0 / Total 23

Status	Name	Up time	Recommendation	Description	Actions
Healthy	local-postgres	15d 18h 3m 6s	None		···
Healthy	robot-kafka	15d 18h 3m 30s	None		···
Healthy	robot-ui	15d 17h 44m 16s	None		···
Healthy	cas	15d 17h 44m 50s	None		···
Healthy	nats	15d 18h 3m 13s	None		···
Healthy	robot-orch	15d 18h 2m 15s	None		···
Healthy	cw-fault-event-processing-service	15d 17h 46m 40s	None		···
Healthy	astackserver	15d 17h 44m 58s	None		···
Healthy	robot-postgres	15d 18h 3m 23s	None		···

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 35: Alarms



Crosswork Manager

Platform Infrastructure Healthy Microservices(23) 23 0 0 Recommendation None

Description: Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Last update: 01-Aug-2024 01:46:22 PM IST

Active alarms only

Selected 0 / Displaying 22 of 22

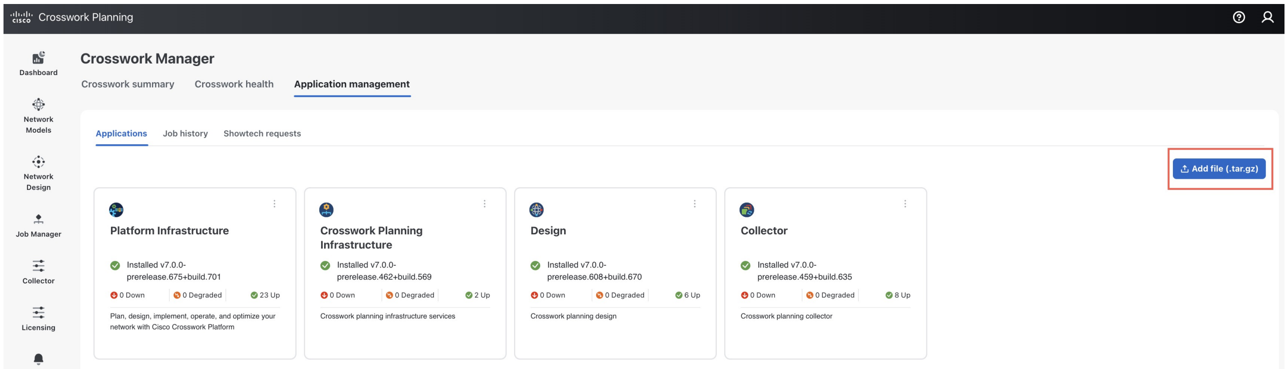
	Source	Severity	Description	Last updated ti...	Category	Status	Annotations	Object description
□	capp-infra:robot...	Critical	10.225.120.165 Disk usage violations detected. Logfs Disk Cap	01-Aug-2024 07...	System	Not acknowledged		10.225.120.165 Disk usage violations detected. Logfs Disk ...
□	capp-infra:tyk-0	Info	tyk-0[infraApiProxy] process started	16-Jul-2024 07:...	System	Not acknowledged		Tyk Service
□	capp-infra:tyk-0	Info	tyk-0[capp-design] APIs install completed	25-Jul-2024 11:...	System	Not acknowledged		Tyk APIs
□	capp-infra:robot...	Warning	service: cp-async-engine requested db connection 1000 excee	16-Jul-2024 08:...	System	Not acknowledged		service: cp-async-engine requested db connection 1000 e...
□	capp-infra:robot...	Warning	Resource profile config mismatch: Application Profile: small VN	16-Jul-2024 07:...	System	Not acknowledged		Resource profile config mismatch: Application Profile: smal...
□	capp-infra:robot...	Info	Maintenance off task success	23-Jul-2024 05...	System	Not acknowledged		Maintenance off task success
□	capp-infra:robot...	Warning	service: cp-sync-engine requested db connection 1000 excee	25-Jul-2024 11:...	System	Not acknowledged		service: cp-sync-engine requested db connection 1000 ex...
□	capp-infra:robot...	Info	active	16-Jul-2024 08:...	System	Not acknowledged		Platform Infrastructure is not healthy after 3m1s. If it contin...
□	capp-infra:robot...	Info	Certificate Crosswork Web Server - crosswork web intermedia	16-Jul-2024 08:...	System	Not acknowledged		Crosswork certificate management
□	capp-infra:astac...	Info	astackserver started	16-Jul-2024 07:...	System	Not acknowledged		astackserver initialization
□	capp-infra:cas	Info	cas-7cb87b6fc6-vzdqj cas restarting	16-Jul-2024 08:...	System	Not acknowledged		cas Service

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 window displays all applications that have been installed. You can also click **Add File (.tar.gz)** to install more applications.

Figure 36: Application Management Window


Crosswork Planning
Dashboard
Network Models
Network Design
Job Manager
Collector
Licensing
Crosswork Manager
Crosswork summary
Crosswork health
Application management
Applications
Job history
Showtech requests
Add file (.tar.gz)
Platform Infrastructure
Installed v7.0.0-prerelease.675+build.701
0 Down
0 Degraded
23 Up
Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform
Crosswork Planning Infrastructure
Installed v7.0.0-prerelease.462+build.569
0 Down
0 Degraded
2 Up
Crosswork planning infrastructure services
Design
Installed v7.0.0-prerelease.608+build.670
0 Down
0 Degraded
6 Up
Crosswork planning design
Collector
Installed v7.0.0-prerelease.459+build.635
0 Down
0 Degraded
8 Up
Crosswork planning collector

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 16: Backup and Restore options

Menu option	Description
Actions > Data backup (See Manage Cisco Crosswork Planning Backup and Restore, on page 126 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 128) to recover from a serious outage.
Actions > Data disaster restore (See Restore Cisco Crosswork Planning After a Disaster, on page 128 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 **Note** This option is not supported in Cisco Crosswork Planning 7.0.	

Manage Cisco Crosswork Planning 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.
- Crosswork does not manage the backups. It is up to the operator to periodically delete old backups from the target server to make room for future backups.
- 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.

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 **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) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data backup** to display the **Data Backup** dialog box with the destination server details pre-filled.
c) Provide a relevant name for the backup in the **Job name** field.
d) If you want to create the backup despite any microservice issues, check the **Force** check box.
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 **Remote path** 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.
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.

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

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

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

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

After the restore process completes, ensure these actions are performed to resume normal system operations:

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 27.
- 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 75.

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 7.0 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.

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 activites - login, logout, login failure due to maximum active session limit, and account locked due to maximum login failures.
- Source IP - IP address of the machine from where the action was performed. This column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork 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 provide 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 comma.

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

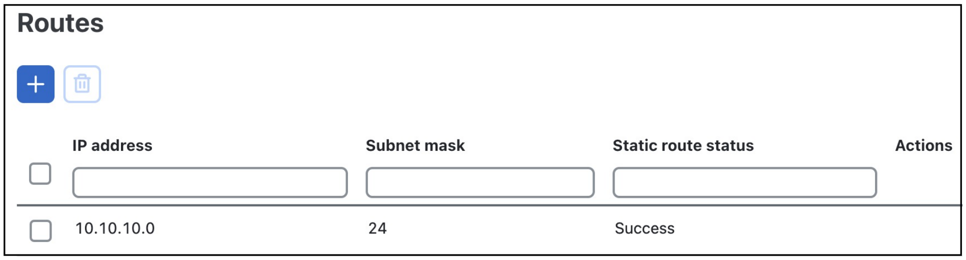
Static routes are used to reach the devices in a different subset.

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**.



Routes

	IP address	Subnet mask	Static route status	Actions
□				
□	10.10.10.0	24	Success	

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.