Cisco Crosswork Planning 7.2 Collection Setup and Administration

First Published: 2026-01-30

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

CONTENTS

CHAPTER 1

Getting Started

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

This chapter contains these topics:

Core capabilities of Cisco Crosswork Planning

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

Key features

Some important features of Cisco Crosswork Planning include:

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

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

Components

Cisco Crosswork Planning comprises two primary components:

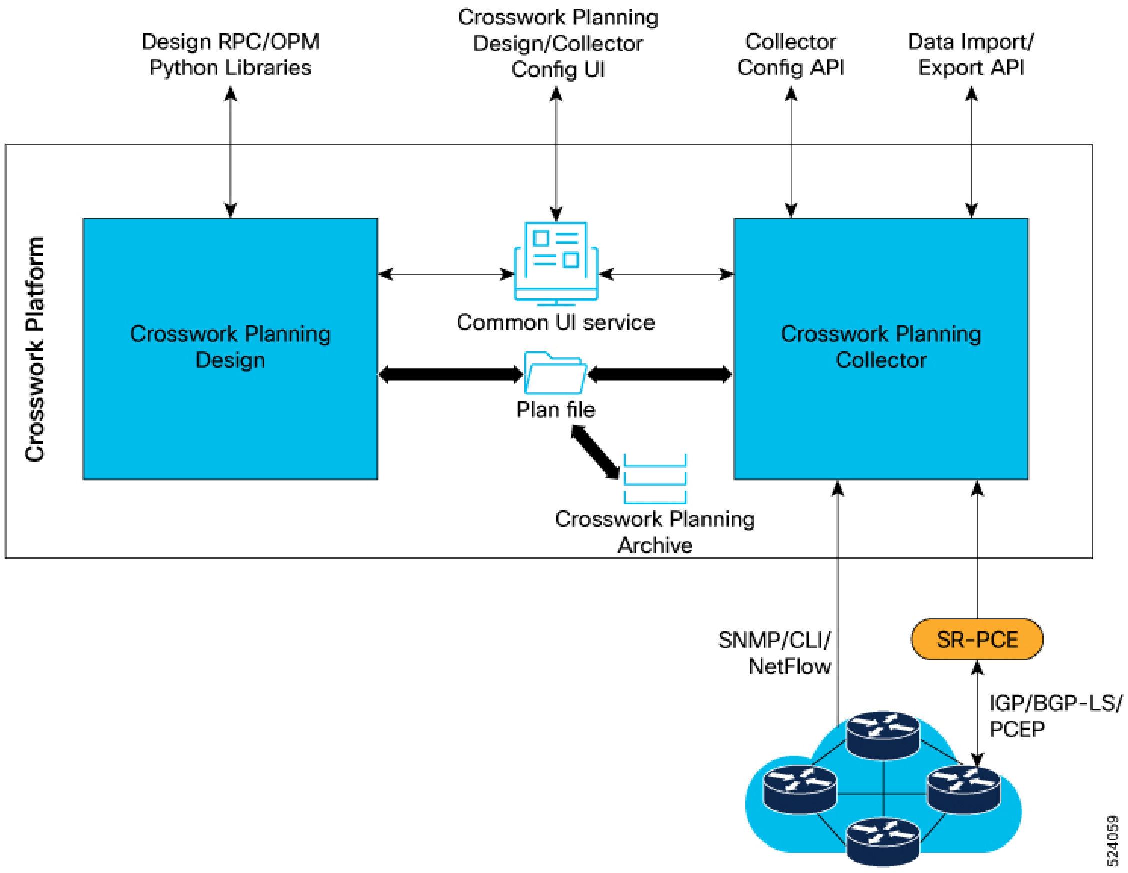
- Cisco Crosswork Planning Collector: This component consists of a set of services that create, maintain, and archive a model of the current network. It achieves this through continual monitoring and analysis of the network and the traffic demands placed on it.
- Cisco Crosswork Planning Design: This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

Cisco Crosswork Planning system

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

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

Figure 1: System overview



Collectors

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

Typically, collectors operate in this manner:

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

Types of collectors

Cisco Crosswork Planning includes several different collectors, including:

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

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

For a complete list of all the collectors supported in Cisco Crosswork Planning, see Collector descriptions, on page 51.

Network models and plan files

A *network model* is an output that

- is generated by the Cisco Crosswork Planning Collector application
- combines information from various collectors, and
- reflects the configuration and topology of a real network.

A *model building chain* refers to an arrangement of collectors organized in such a way as to produce a network model with the desired information.

The system saves the resulting network model in a plan file format (.pln), which you can view or download from the Cisco Crosswork Planning Design application.

Aggregation components

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

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

Delta Aggregation Rules Engine (DARE)

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

Simple Aggregation Engine (SAgE)

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

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

By default, all collectors are included in the aggregation during collection configuration. You can choose to exclude any collector from aggregation while scheduling the collection. For details, see Aggregate collector outputs, on page 37.

Generation of network models

Network models are generated on completion of each level of aggregation. The first model is generated as the output of DARE aggregation. This file serves as a data source for components such as traffic, inventory, layout, NetFlow, and demands. Once the SAgE aggregation is complete, it generates the second file, the network model, which is the final output of the aggregated data collected.

Log in to Cisco Crosswork Planning

This topic describes how to access the UI after installing Cisco Crosswork Planning.

Cisco Crosswork Planning is a browser-based application. For details on supported browser versions, see the *"Supported web browsers" section in the Cisco Crosswork Planning 7.2 Installation Guide*.

Procedure

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

When you access Cisco Crosswork Planning from your browser for the first time, you may see a warning that the site is untrusted. If this occurs, 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 Log in to Cisco Crosswork Planning.

a) Enter the administrator username **admin** and the default password **admin**.
b) Click **Login**.
c) When prompted to change the administrator's default password, enter the new password in the fields provided and then click **OK**.

Note
Use a strong VM password (a minimum of eight characters, including uppercase and lowercase letters, numbers, and at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words.

The **Crosswork Manager** page appears.

Step 3 Click the **Crosswork Health** tab, and click the **Crosswork Platform Infrastructure** tab to view the health status of the microservices running on Cisco Crosswork Planning.

Step 4 (Optional) Change the name assigned to the admin account to something more relevant.

You gain access to Cisco Crosswork Planning and you can begin planning or managing tasks as needed.

What to do next

To log out, in the top-right corner of the main page, click 👤 > **Logout**.

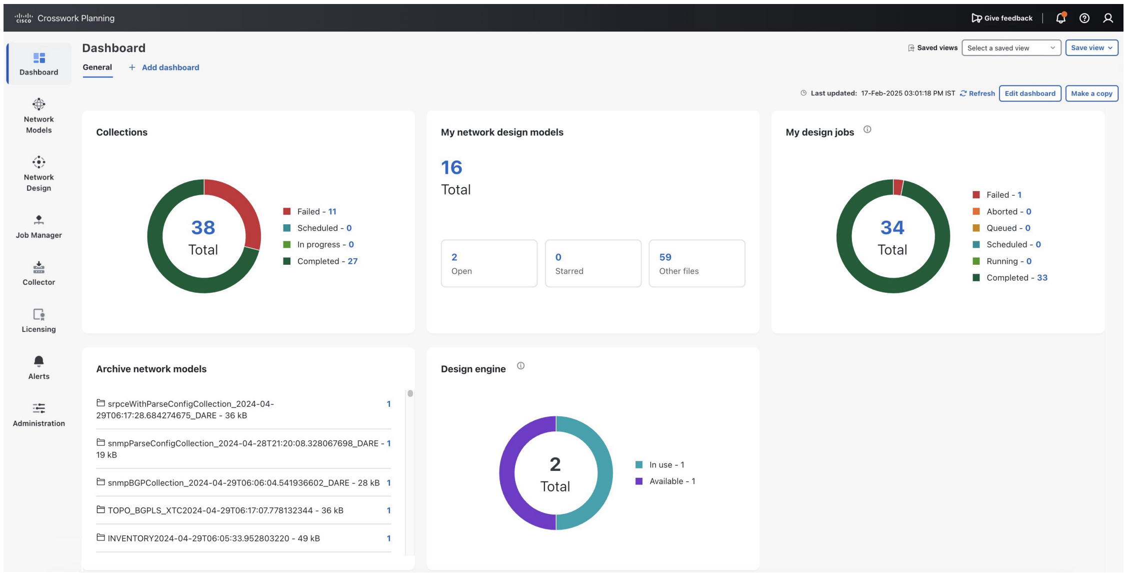
Note Logging out does not close the plan file you are working on; the file remains open.

Dashboard

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

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

Figure 2: Dashboard view



Dashlet navigation

Links in each dashlet allow you to navigate to the desired pages easily. For example, in Figure 2: Dashboard view, on page 6, link **2** in the **Open** tab in the **My network design models** dashlet indicates that there are two network models open in the UI. If you click this number **2**, the two opened network models are displayed in the **Network Design** page.

Dashlet customization

Use the **Edit dashboard** button at the top right corner to customize how the dashlets appear. For details, see Customize dashlets For details, see the *Customize dashlets* topic in the *Cisco Crosswork Planning Design 7.2 User Guide*.

CHAPTER 2

Configure Network Models

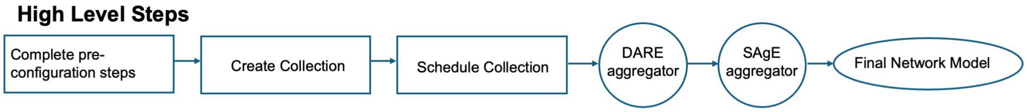
Network model creation workflow

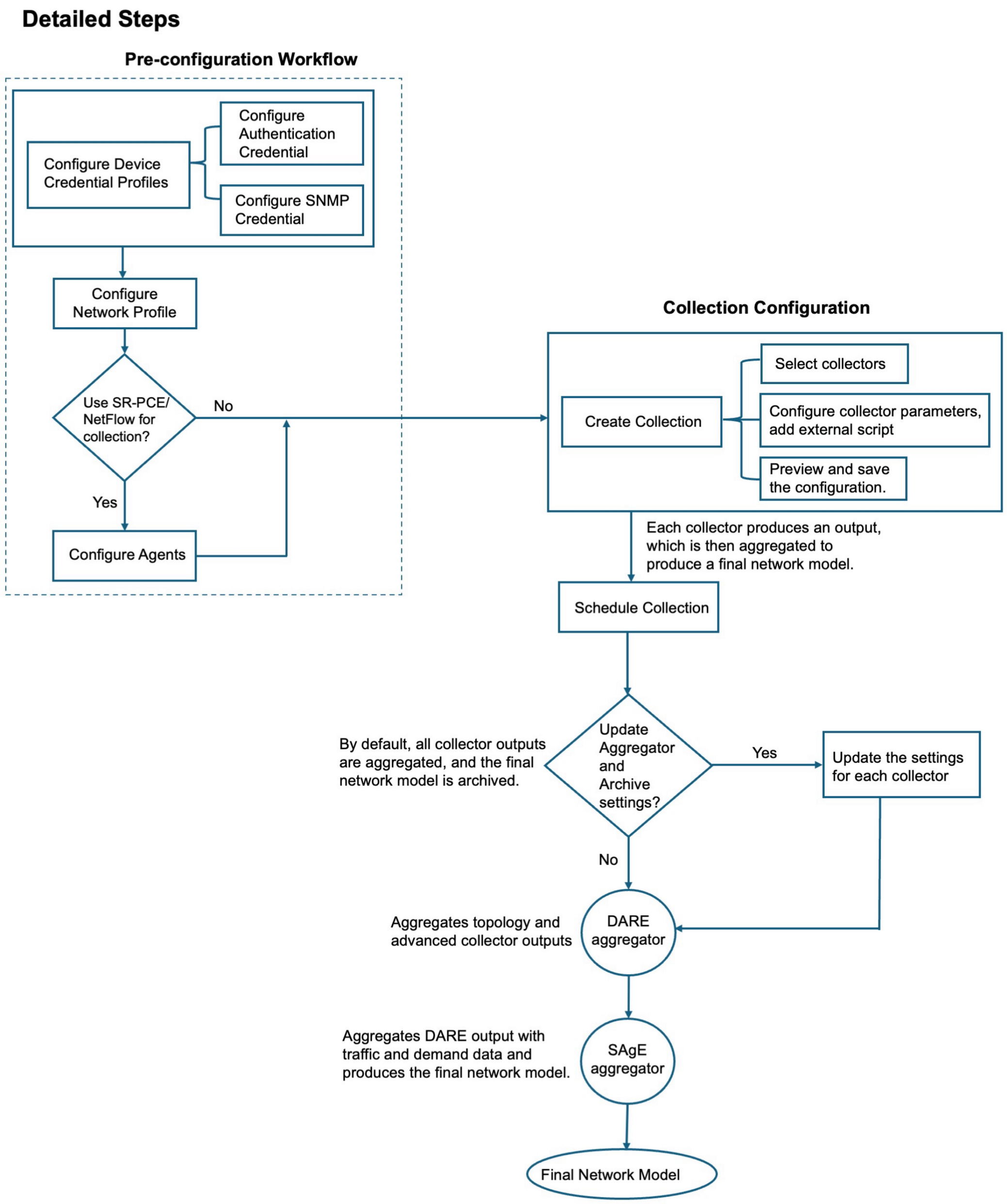
Summary

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

Workflow

Figure 3: Network model creation workflow




Detailed Steps
Pre-configuration Workflow
Configure Device Credential Profiles
Configure Authentication Credential
Configure SNMP Credential
Configure Network Profile
Use SR-PCE/ NetFlow 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

These are the stages of network model creation.

1. Configure device authgroups, SNMP groups, and network profile access. For details, see Preconfiguration workflow, on page 9.
2. (Optional) Configure agents only if you need to collect SR-PCE or NetFlow information. For details, see Configure agents, on page 18.
3. Configure the collections (basic and advanced configurations). For details, see Setting up collections, on page 23.
4. Schedule when to run the collections. See Schedule a collection, on page 30.

5. (Optional) Manage aggregation and archiving of network model according to your requirement. For details, see Aggregate collector outputs, on page 37 and Configure archive, on page 40.

6. View or download the plan files in the Cisco Crosswork Planning Design application. For details, see View or download plan files.

Preconfiguration workflow

Summary

This preconfiguration workflow outlines the preliminary steps required to create a network model. This involves setting up credential profiles to access the devices, configuring network access, and optionally creating agents to collect specific information.

Workflow

These are the stages of the preconfiguration workflow.

1. Configure the device credential profiles (Authentication profiles and SNMP profiles). For details, see Configuring credential profiles, on page 9.

2. Configure the network profile access. For details, see Configure a network profile, on page 13.

3. (Optional) Create agents to collect specific information. This step is required only for collecting SR-PCE or NetFlow information. For details, see Configure agents, on page 18.

Configuring credential profiles

Summary

Credential profiles are a method to securely store and manage device credentials for accessing network 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 bundling 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, gather access credentials and supported protocols 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.

Workflow

These are the stages of configuring credential profiles.

1. Set up device authentication credentials to access devices. For details, see Configure authentication credentials, on page 10.

2. Set up SNMP credentials to access the network server. For details, see Configure SNMP credentials, on page 11.

Configure authentication credentials

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

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

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

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

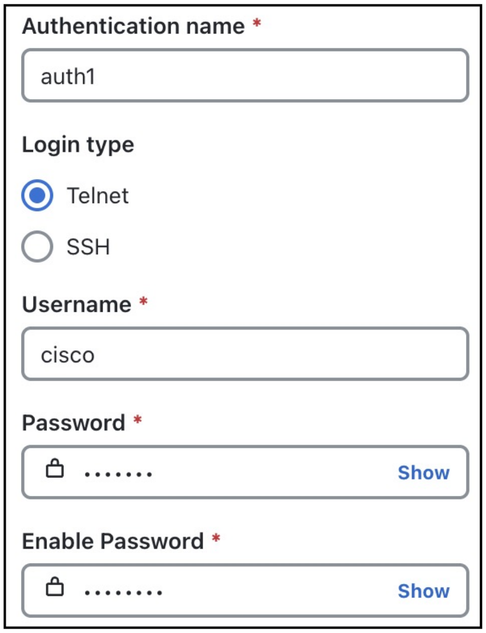
Procedure

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

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

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

Figure 4: Configure authentication credentials



Authentication name *

auth1

Login type

● Telnet

○ SSH

Username *

cisco

Password *

•••••••

Enable Password *

••••••••

Step 3 Enter values in these fields:

- Authentication name: Enter a descriptive name.

- Login type: Select either **SSH** or **Telnet** according to your requirement. The SSH protocol is more secure. The Telnet protocol does not encrypt the username and password.
- Credential fields: Enter values in **Username**, **Password**, and **Enable password**. For **Enable password**, provide a password required to access the enable mode (also known as privileged EXEC mode) on Cisco IOS routers. This password controls access to the enable mode, preventing unauthorized configuration changes on the router. If your device does not support enable mode, use the same password for both the **Password** and **Enable password** fields.

Step 4 Save the changes.

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

Configure SNMP credentials

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

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

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

Before you begin

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

Procedure

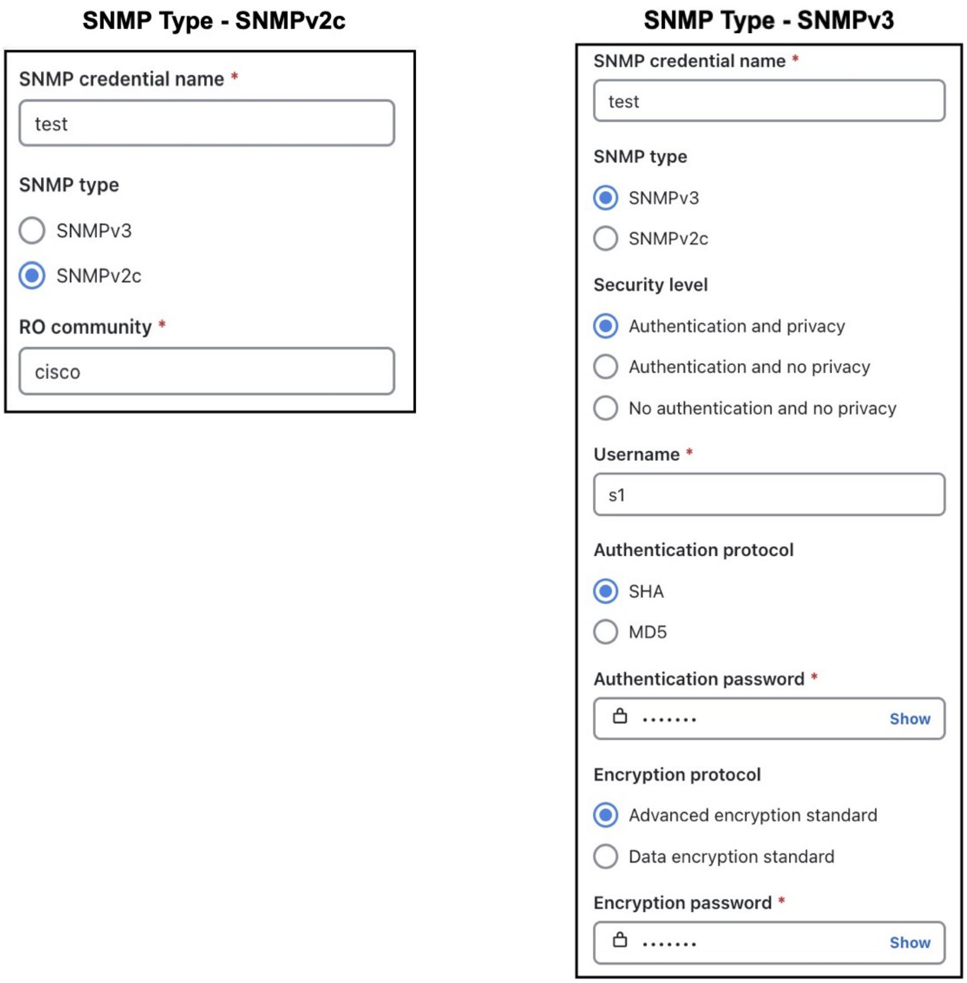
Step 1 From the main menu, choose **Collector** > **Credentials**.

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

Note

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

Figure 5: 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 In the **SNMP type** section, select which SNMP protocol to use. The options are **SNMPv3** and **SNMPv2c**.

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

Table 1: SNMPv3 fields

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

Step 5 Click **Save**.

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

Configure a network profile

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

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

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

Before you begin

Configure device credential profiles (Authentication profiles and SNMP profiles). For details, see Configure authentication credentials, on page 10 and Configure SNMP credentials, on page 11.

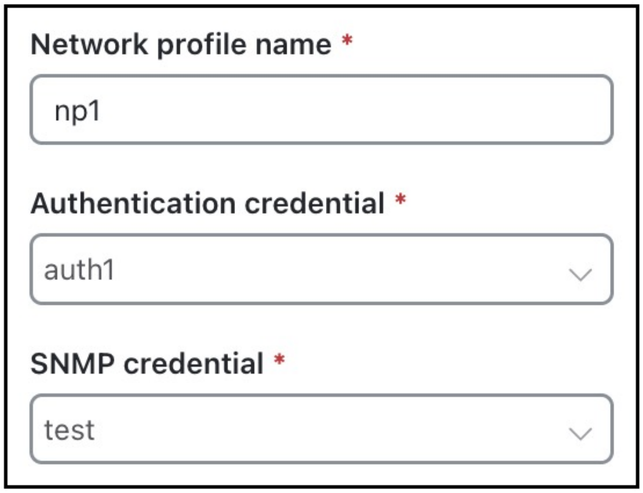
Procedure

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

Step 2 Click **+ Create new**.

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

Figure 6: Create network profile



Network profile name *
np1
Authentication credential *
auth1
SNMP credential *
test

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

- Network profile name: Enter a name for the network access profile.
- Authentication credential: Select the applicable authentication credential from the drop-down list. If you don't have any authentication credential created, create one using the steps mentioned in Configure authentication credentials, on page 10.
- SNMP credential: Select the applicable SNMP credential from the drop-down list. If you don't have any SNMP credential created, create one using the steps mentioned in Configure SNMP credentials, on page 11.

Step 4 Click **Create & Proceed**.

Step 5 (Optional) To add or edit nodes associated with these network access credentials, see Add or edit nodes in a network profile, on page 14.

Step 6 (Optional) To include or exclude individual nodes from the collection, see Configure a node filter, on page 16.

Step 7 Save the changes.

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

Add or edit nodes in a network profile

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

Procedure

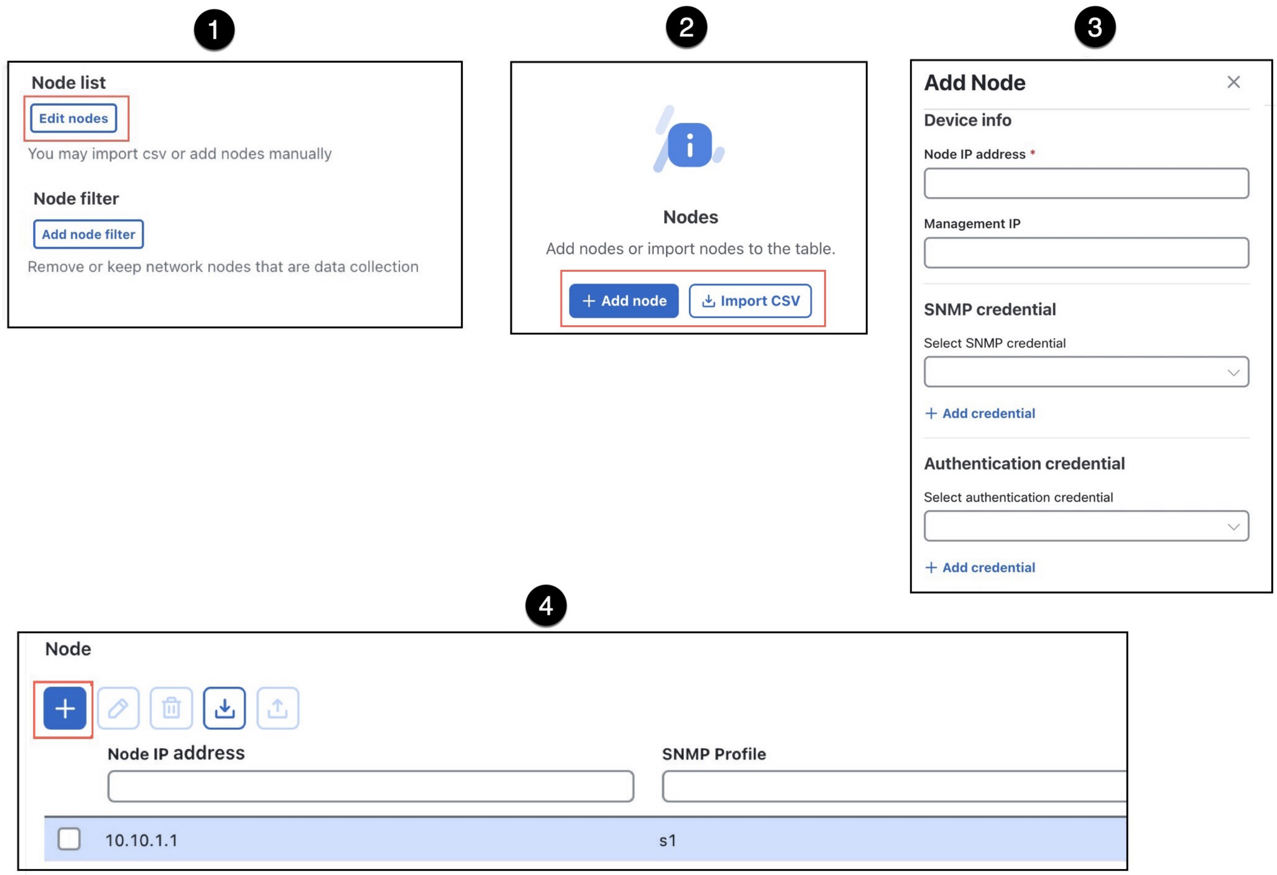
Step 1 From the main menu, choose **Collector** > **Network Profiles**.

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

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

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

Figure 7: Edit nodes pages



You may import csv or add nodes manually

Remove or keep network nodes that are data collection

Add nodes or import nodes to the table.

Node IP address	SNMP Profile
10.10.1.1	s1

Step 4 Click **Done**.

Configure a node filter

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

Node filters allow you to control which nodes are included or excluded from data collection based on defined criteria. You can either define the filter criteria manually for each node or upload a CSV file that contains the nodes and their respective filter conditions.

Note

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

Before you begin

If you use a CSV file, the first row must contain three columns: Type, Value, and Enabled.

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 whether to exclude or include individual nodes.

Step 5 Follow these steps to specify the filter criteria manually for each node:

a) Click **+ Add filter criteria**.

b) Select the type using which you want to filter. The options are: **IP address** and **Hostname**.

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

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

If you decide to ...	Then ...
include or exclude multiple nodes with a regular expression	**1.** Select the **Regex** option. **2.** Enter the Regex expression in the **Regex** field. **Note** If you configure multiple regex filters (for example, one for IP and one for Hostname), the system combines them into a single pattern using the logical OR operator (|). A node is filtered if it matches either the IP pattern or the Hostname pattern. For an example of how regex-based criteria are used to filter nodes, see Regex-based filtering criteria for node selection, on page 18.
add each node's IP address	**1.** Select the **Individual IP address** option. **2.** Enter the IP address in the **IP address** field.
add each node's hostname	**1.** Select the **Individual hostname** option. **2.** Enter the hostname in the **Hostname** field.

d) Optionally, repeat steps 5(a) to 5(c) to add more filter criteria.

Step 6 Follow these steps to import a CSV file with the list of nodes to be filtered:

a) Click **Import**.

b) Upload the CSV file containing nodes and their filter conditions. To ensure the file is formatted correctly, download and refer to the sample CSV file.

c) Import the CSV file.
The nodes listed in the CSV file appear on the Nodes Filter page.

Step 7 To consider an entry in the filter, it must be enabled. The **Status** column shows this information. To change the status, select the entry, click **Update status**, and select the required status option.

The required nodes are included or excluded from data collection according to your settings.

What to do next

To edit, delete, or export nodes, select the nodes and click **Edit**, **Delete**, or **Export**. You can sort and filter the entries using any column.

Regex-based filtering criteria for node selection

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

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

Example

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

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

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

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

Configure agents

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

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

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

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

Procedure

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

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

Step 2 Click **+ Create new**.

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

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

Step 4 Select the required Collector type.

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

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

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

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

- If you select **SR-PCE**, then enter the applicable configuration details mentioned in Table 2: SR-PCE agent configuration options, on page 20.
- If you select **NetFlow**, then enter the applicable configuration details mentioned in Table 3: NetFlow agent configuration options, on page 21.

Step 6 Click **Save**.

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

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

What to do next

Use the **Collections** page (**Collector** > **Collections**) to configure the collectors to build a network model. For more information, see Configure a collection, on page 24.

SR-PCE and NetFlow agent configuration options

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

SR-PCE agent configuration options

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

Table 2: SR-PCE agent configuration options

Option	Description
Enabled	Enables the SR-PCE agent. Default is enabled.
SR-PCE host IP	Host IP address of the SR-PCE router.
SR-PCE REST port	Port number to connect to the SR-PCE host. The default is 8080.
Authentication type	Authentication type to be used for connecting to the SR-PCE host. • Basic: Use HTTP Basic authentication (plaintext). • Digest: Use HTTP Digest authentication (MD5). • None: Use no authentication. This is applicable only for old IOS XR versions.
Username	Username for connecting to the SR-PCE host.
Password	Password for connecting to the SR-PCE host.
Connection retry count	Maximum number of retry counts for connecting to the SR-PCE host.
Topology collection	Specifies whether to collect topology data and to have subscription for network changes. These are the options: • Collection only • Collection and Subscription (default) • Off
LSP collection	Specifies whether to collect LSP data and to have subscription for network changes. These are the options: • Collection only • Collection and Subscription (default) • Off
Connection timeout interval	Connection timeout in seconds. Default is 50 seconds.
Pool size	Number of threads processing SR-PCE data in parallel.

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

NetFlow agent configuration options

This table provides the configuration options for NetFlow agents.

Table 3: NetFlow agent configuration options

Option	Description
BGP	Enables passive BGP peering. Cisco Crosswork Planning tries to set up a BGP session with the router. Enter the BGP details in the table listed below the BGP check box.
Name	Node name.
Sampling rate	Sampling rate of the packets in exported flows from the node. For example, if the value is 1,024, then one packet out of 1,024 is selected in a deterministic or random manner.
Flow source IP	IPv4 source address of flow export packets.
BGP source IP	IPv4 or IPv6 source address of iBGP update messages.
BGP password	BGP peering password for MD5 authentication.
Interval	Interval in seconds for writing the output file. Enter the value that is greater than zero and multiple of 60. Default is 900 seconds.

Option	Description
Flow size	Flow collection deployment size, based on network-wide aggregated flow export traffic rate. • Small: Recommended when flow traffic rate is less than 10 Mbps. • Medium: Recommended when flow traffic rate is between 10 Mbps and 50 Mbps. • Large: Recommended when flow traffic rate is more than 50 Mbps. • Lab: Not for customer use. Default is Medium.
Extra aggregation	Choose aggregation keys from the list.

Edit agent settings

This section explains how to perform various operations on agents, such as editing parameters, managing schedules, verifying connections, and so on.

Procedure

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

Step 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.

Option	Description
Edit	Modify the agent's parameters.
• Start • Restart • Stop	Start, restart, and stop the agents, respectively.
Verify connection	Check the status of the agents. To view the detailed status of a NetFlow agent, click **More details**.
Delete	Delete the agents.
• Add schedule • Edit schedule	Set up and edit the data refresh frequency for the agents, respectively. **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.

Option	Description
Delete schedule	Remove the data refresh frequency set for the agents. **Note** This option is available only for SR-PCE agents.

Step 3 After selecting the desired operation for an agent, proceed with any subsequent on-screen option to complete the task.

Setting up collections

This section outlines how to set up collectors and configure their parameters to create a network model.

Summary

The key components involved in the process are:

- Collections page: Used to configure different collectors and manage collection tasks.
- Collectors: Tools categorized under Startup script, Basic topology, Advanced modeling, and Traffic and Demands to gather network data.
- Configuration parameters: Settings associated with each collector that need to be adjusted based on requirements.

Use the **Collections** page (from the main menu, choose **Collector** > **Collections**) to configure different collectors. Depending on the selected 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.

Workflow

These are the stages of setting up collections.

Step	Description
1. Complete all the steps mentioned in the preconfiguration workflow.	See Preconfiguration workflow, on page 9.
2. Select the required collectors.	**1.** To use an external script as a first step in the collection configuration chain, select **Script**. **2.** Choose a Basic topology collector. If you are not using the start-up script, then this step is mandatory. You must choose one of the basic topology collectors, which will be the source for additional network collections. **3.** Choose the additional collectors, as needed. The collectors are categorized under the **Advanced modeling** and **Traffic and Demands** sections.

Step	Description
3. Configure collection parameters.	The configuration parameters differ based on the collectors you selected in the previous step. 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 an external script against a network model, on page 92.
5. Preview the order in which you have configured the collectors.	Review the order of the collectors you configured. If you are satisfied with the configuration, proceed to create the collection.
6. Set up the collection schedules.	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 a collection, on page 30.
7. (Optional) Update the aggregation and archive settings, as required.	See: • Aggregate collector outputs, on page 37 • Configure archive, on page 40

Configure a collection

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

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

Important When configuring collections in Cisco Crosswork Planning, it is important to understand how collections and network devices impact the system's capacity. The scale numbers (for example, 6,000 or 3,000 nodes) represent the total capacity across all collections combined. For example, you can create a 6,000-node configuration using either a single collection containing all nodes or multiple collections, such as six collections with 1,000 nodes each. However, exceeding the system's defined scale limits can result in performance issues. These include collectors and aggregators running out of memory. Ensure the total number of devices or interfaces across all collections remains within the defined scale limits to maintain optimal system performance. For details on scale numbers, see the *"Profile specifications"* section in the *Cisco Crosswork Planning 7.2 Installation Guide*.

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

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

Step 2 Begin the process of creating collections.

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

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

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

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

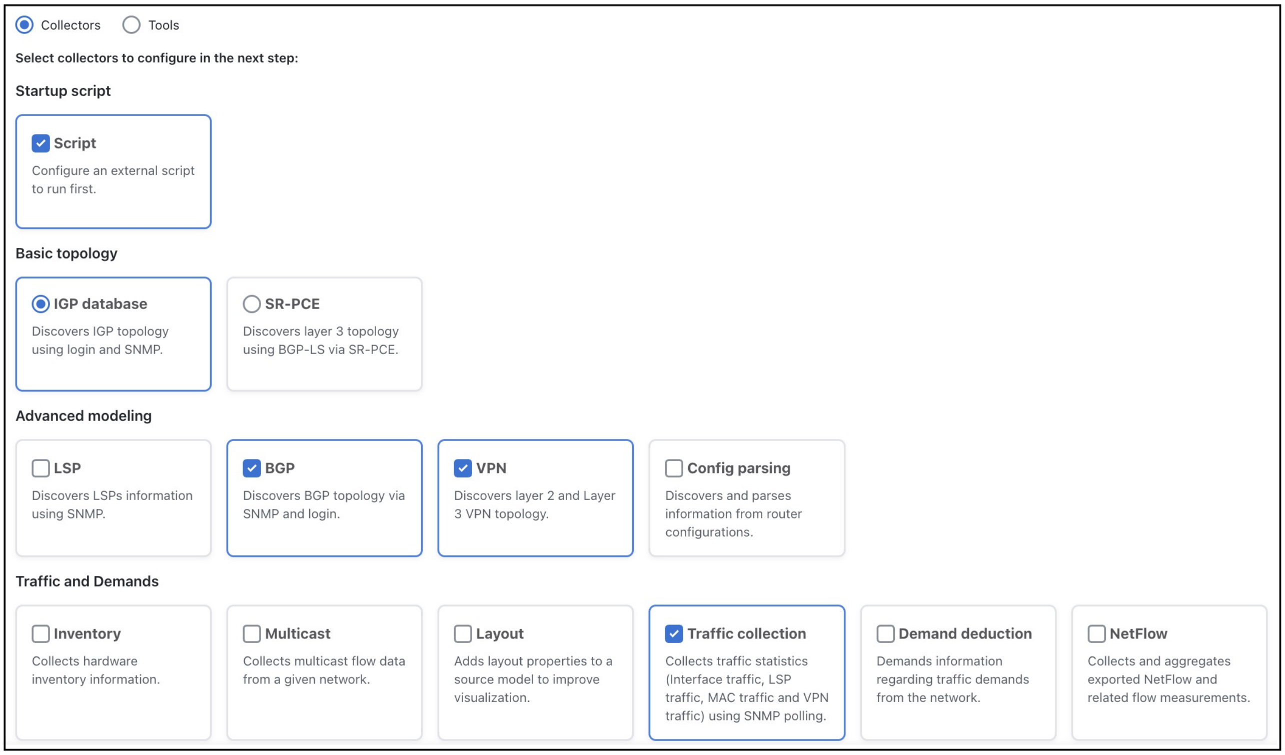
To create a new node profile, click **+ Add new profile**.

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

Step 3 Select the required collectors. For descriptions of all the collectors, see Collector descriptions, on page 51.

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

Figure 8: Select collectors page



● Collectors ○ Tools

Select collectors to configure in the next step:

Startup script

☑ Script
Configure an external script to run first.

Basic topology

● IGP database
Discovers IGP topology using login and SNMP.

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

Advanced modeling

□ 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, MAC 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.

b) To use any external script as a first step in the collection configuration chain, select **Script**.

You can select only one start-up script in a collection.

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

Note that you can select only one topology collector.

d) Select additional collectors as needed from these sections.

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

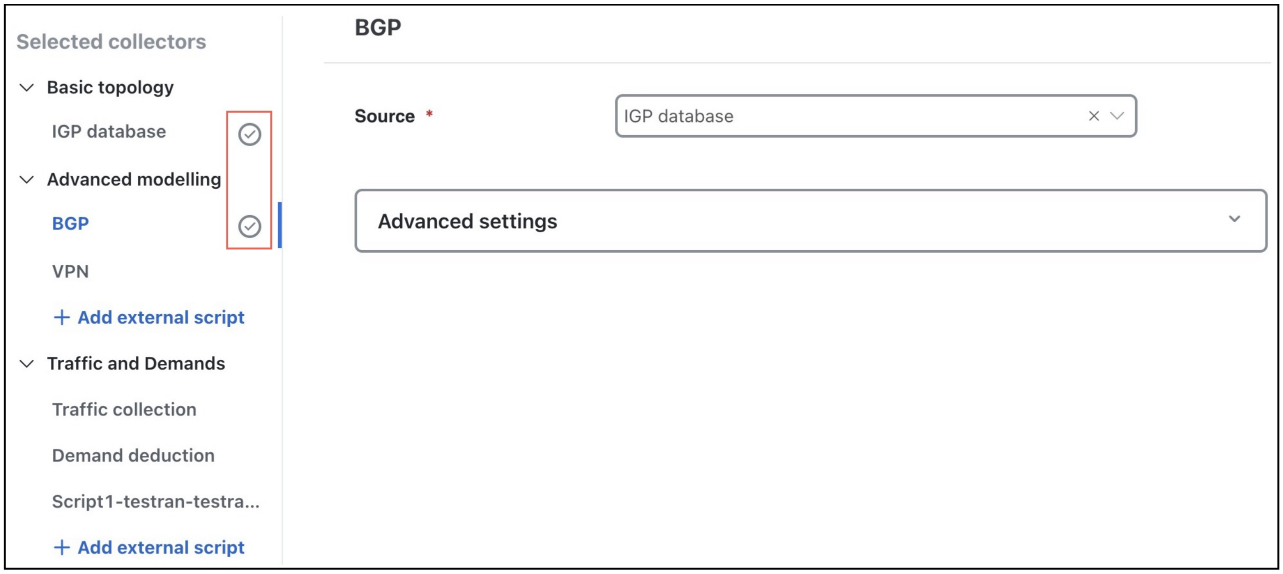
Step 4 Configure collectors.

a) Enter the configuration parameters for the selected collectors.

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

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

Figure 9: Configure collection parameters



Source * IGP database

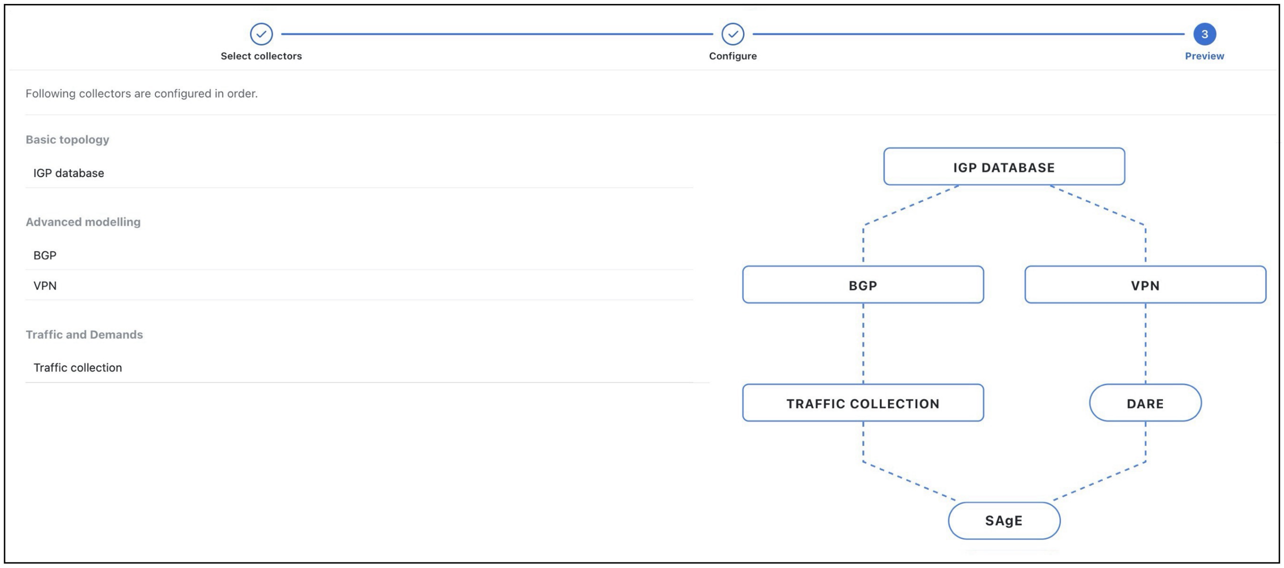
b) (Optional) To use a customized script against a collection model, click the **+ Add external script** link. For details, see Run an external script against a network model, on page 92.

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

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

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

Figure 10: Preview page



Following collectors are configured in order.

Basic topology

IGP database

Advanced modelling

BGP

VPN

Traffic and Demands

Traffic collection

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

- A confirmation message appears indicating that the collection has been successfully created.
- To make any changes to the configuration, click **Back** to go back to the previous page. You can also click the step numbers at the top to navigate to the required configuration step.

Note

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

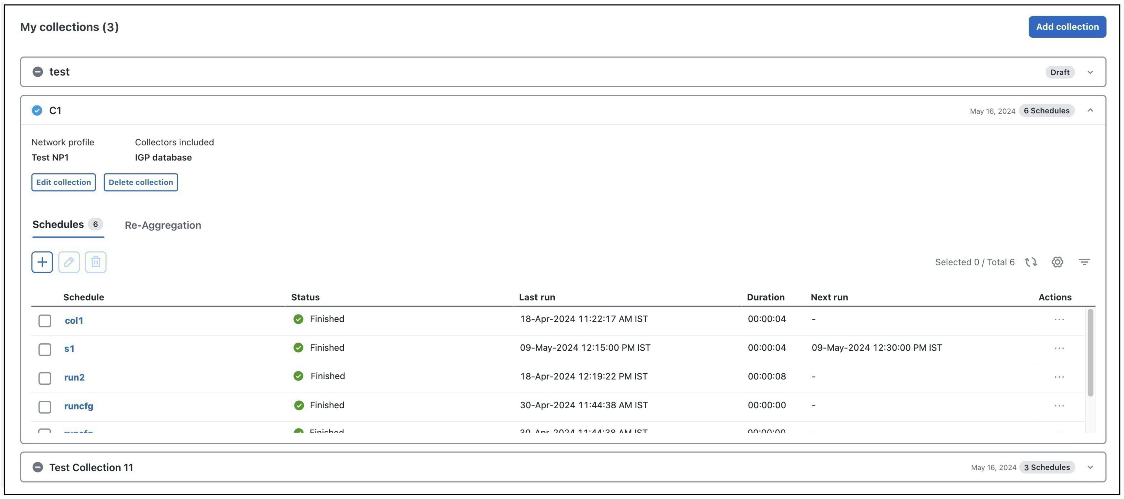
Step 6 (Optional) If you want to configure the schedules immediately, click **Add schedule** in the dialog box and proceed with the schedule configuration. For details, see Schedule a collection, on page 30.

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

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

This image shows a sample Collections page with three collections.

Figure 11: List of available collections



My collections (3)

test

C1

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 12:15:00 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

What to do next

Schedule collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule a collection, on page 30.

Edit a collection

This topic describes how to edit an existing collection.

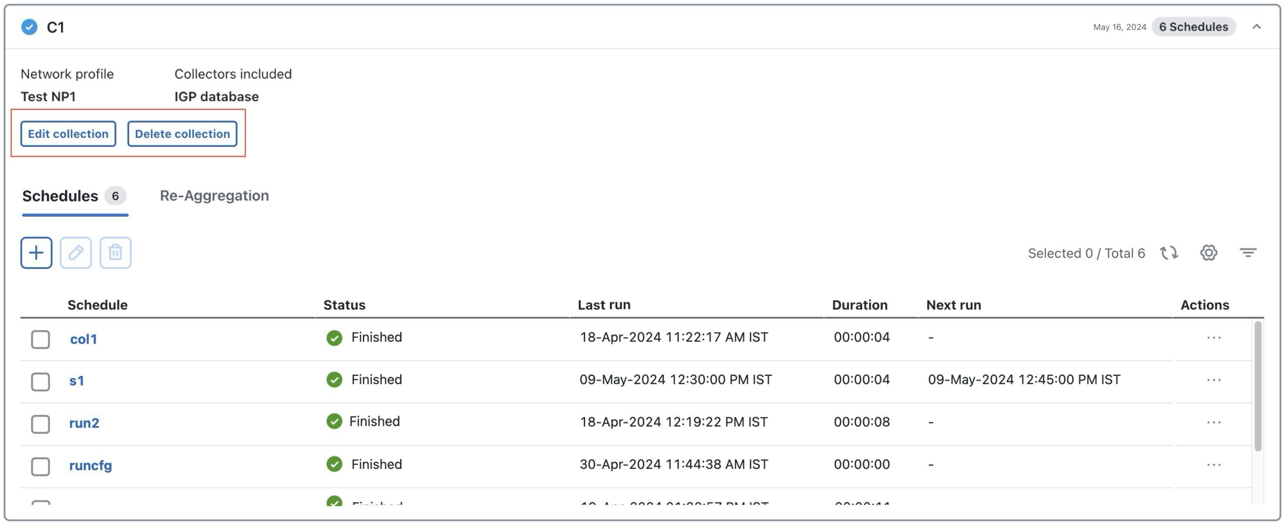
Procedure

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

Step 2 Expand the Collection area you want to edit.

Step 3 Click **Edit collection**.

Figure 12: Collection actions



C1

May 16, 2024 · 6 Schedules

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	-	···
□		✓ Finished	10-Apr-2024 01:38:57 PM IST	00:00:11		

Step 4 Make the required changes in the **Select collectors** and **Configure** pages. Preview the changes and ensure that the updated configuration meets your requirements. For more information, see Configure a collection, on page 24.

Note
When editing the collection, if you delete any collector or change the order of collectors, we strongly recommend that you reaggregate the collection. If you do not reaggregate, data from the original collection setup may be retained. For details about reaggregating collector outputs, see Reaggregate collector outputs, on page 38.

Step 5 Click **Save**.

What to do next

Configure schedules for the collection job. You can schedule the collection job to run immediately or schedule it to run at specific intervals. For details, see Schedule a collection, on page 30.

Delete a collection

This topic describes how to delete an existing collection.

Procedure

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

Step 2 Expand the Collection area you want to delete.

Step 3 Click **Delete collection** (for reference, see Figure 12: Collection actions, on page 29).

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

A message confirming the successful deletion of the collection appears.

Schedule a collection

This topic describes how to enable automated data collection by scheduling collections in the Cisco Crosswork Planning UI.

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

Before you begin

- Ensure that you have created the required collections. For details, see Configure a collection, on page 24.
- Be familiar with using cron expressions.

Procedure

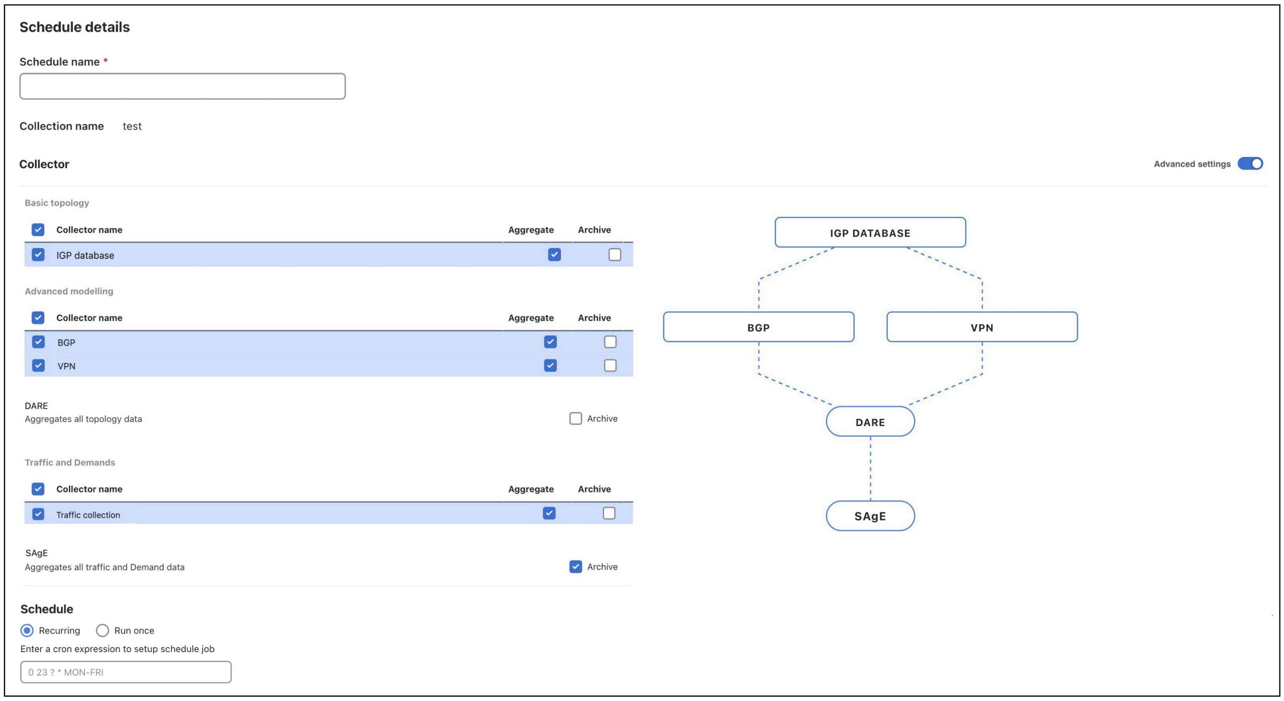
Step 1 From the main menu, choose **Collector** > **Collections**. The list of already created collections appears (for reference, see Figure 11: List of available collections, on page 28).

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

- If this is the first time you are creating the schedule, then click the **Add schedule** button while creating the collection or in the collection panel.
- If there are already other schedules available, click the ⊞ icon under the **Schedule** tab to create additional schedules (see Figure 14: Schedule actions, on page 32).

The Schedule details page appears.

Figure 13: 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 schedule.

Step 4 In the **Collector** section:

- If you want to exclude any collector from data collection, uncheck the check box next to the collector name.
- If you want to exclude any collector from aggregation, uncheck the check box under the **Aggregate** column of the corresponding collector. For details, see Aggregate collector outputs, on page 37.
- 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 select the **Run once** option, the collection runs immediately and only once. After selecting this option, the **Schedule** button at the bottom changes to **Run now**. Click it to run the collection immediately.
- If you select the **Recurring** option, specify the time interval using a cron expression. The **Recurring** option is selected by default. After entering the cron expression, click **Schedule** to run the job at the time interval you specified.

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

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

Edit a schedule

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

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

Procedure

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

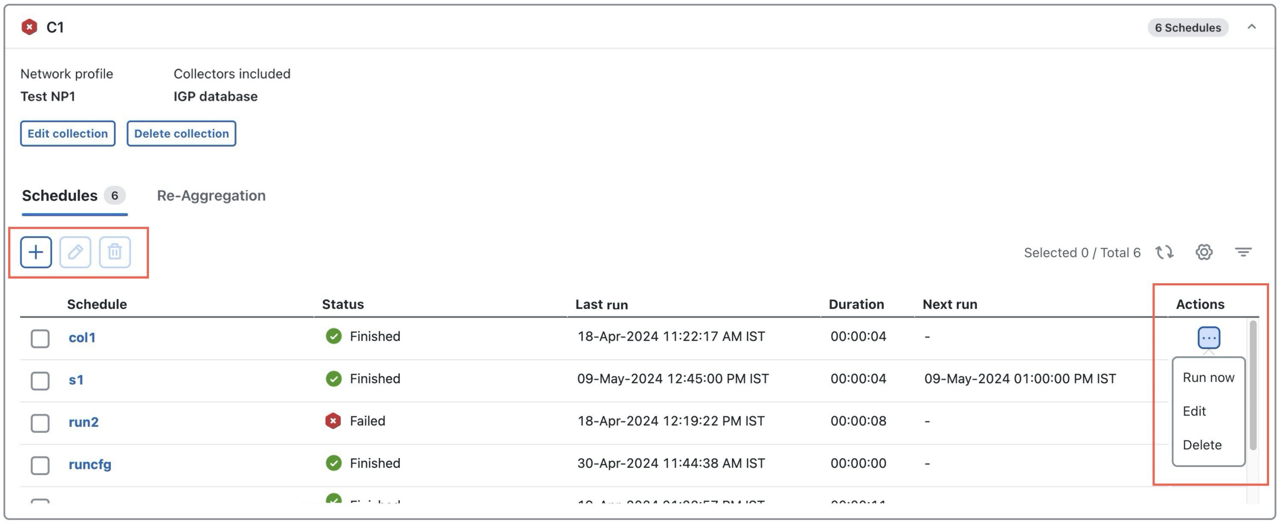
Step 2 Expand the collection panel that contains the schedule you want to edit.

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

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

Note
You can edit only one schedule at a time.

Figure 14: Schedule actions



C1 — 6 Schedules

Network profile: Test NP1
Collectors included: IGP database

Edit collection | Delete collection

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

Step 5 Click **Run now** to execute the job immediately, or click **Schedule** to set the job to run at a specified interval. For details, see Schedule a collection, on page 30.

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

Delete a schedule

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

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

Procedure

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

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

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

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

Note
You can delete only one schedule at a time.

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

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

View scheduled task status and history

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

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

Before you begin

Confirm that a schedule has been configured for the collection.

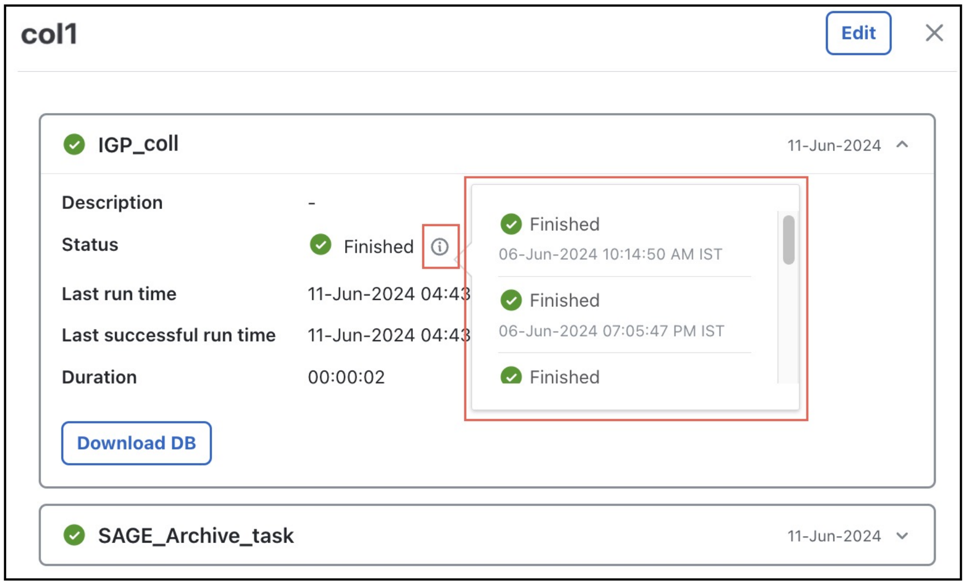
Procedure

Step 1 Expand the desired collection panel.

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

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

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



col1

Edit

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

Download DB

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

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

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

What to do next

To download the collected data, logs, or record files, see Download data, logs, and record files, on page 34.

Download data, logs, and record files

This topic describes how to download the database, logs, and the record files generated by a specific collector. These files are useful for troubleshooting issues or analyzing data.

Before you begin

- Ensure the collector has executed successfully.
- Review the limitations described in Note: Limitations for logs, database, and record file downloads, on page 35.

Procedure

Step 1 Expand the desired collection panel.

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

The page that opens displays the statuses of all the tasks involved in the scheduled collection.

Step 3 Click **Download** and select one of the options to download the data.

- **DB**: Downloads the collected network model to your local machine as a .db file.
- **Logs**: Downloads the log files as a .tar file that contains one or more logs generated by the CLI tools executed as part of the collector. Typically, this includes sysout CLI tool logs and the associated database.
- **Record files**: Downloads a .tar file that contains all the record files with collected network data from the CLI tools executed as part of the collector.

  Note
  In the traffic collector, the poller runs continuously. As a result, data is appended to the record file for as long as the poller is running. To download the record file, you must first stop the poller by disabling it in the collector configuration and saving the changes. After doing this, the record file will be available for download.

- **Debug files**: Downloads the files required for debugging. This option is available only for NetFlow collection. By default, it includes **missing-flows.txt** and **interas-file.txt** files. If you enable the **Back track micro flows** option during NetFlow collection configuration, additional files are included in the debug files. For details on NetFlow data collection, see NetFlow data collection, on page 89.

The selected database file, logs, or record files are downloaded to your local machine.

What to do next

Extract and review the data using standard archive tools.

Note: Limitations for logs, database, and record file downloads

Consider these limitations before downloading logs, database, and record files:

- Only one set of logs, database, and record files from the last execution is available at any given time.
- During traffic collection, since the traffic poller runs continuously and its logs are rolled back, the downloaded .tar file contains all rolled back logs.
- The option to download logs and record files is disabled or hidden for any collector that does not have logs or record files. For a list of collectors that support downloading logs and record files, see Collectors and tools that support downloading logs and record files, on page 35.
- Downloaded logs do not include any of the Cisco Crosswork Planning service logs.
- To log information in your custom script, use standard output. Any logs written to standard output (console) will be collected as script logs and made available for download. Logs written to the files you specify will not be available for download.

Collectors and tools that support downloading logs and record files

This table lists the collectors and tools that allow you to download logs or record files.

Table 4: Collectors or tools that support downloading logs and record files

Collector or tool	Download logs	Download record files
IGP database	✓	✓

Collector or tool	Download logs	Download record files
SR-PCE	✓	✓
BGP	✓	✓
LSP	✓	✓
PCEP LSP	✗	✗
VPN	✓	✓
Config parsing	✓	✓
Inventory	✓	✓
Multicast	✗	✗
Multicast collectors: • Login find multicast • Login poll multicast • SNMP find multicast • SNMP poll multicast	✓	✓
Layout	✓	✗
Traffic collection	✓	✓
Demand deduction	✗	✗
Demand deduction tools: • Demands for LSPs • Demands for P2MP LSPs • Demand deduction • Copy demands • Demand mesh creator	✓	✗
NetFlow	✗	✗
External script	✓	✗
DARE aggregation	✗	✗

Collector or tool	Download logs	Download record files
SAgE aggregation	✗	✗
Merge AS	✗	✗
Create representative plan	✓	✗

Aggregate collector outputs

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

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

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

Note It is assumed that you are in the middle of creating a network model when performing the steps described in this topic. For more information, see Configure a collection, on page 24.

Follow these steps to exclude a collector output from aggregation.

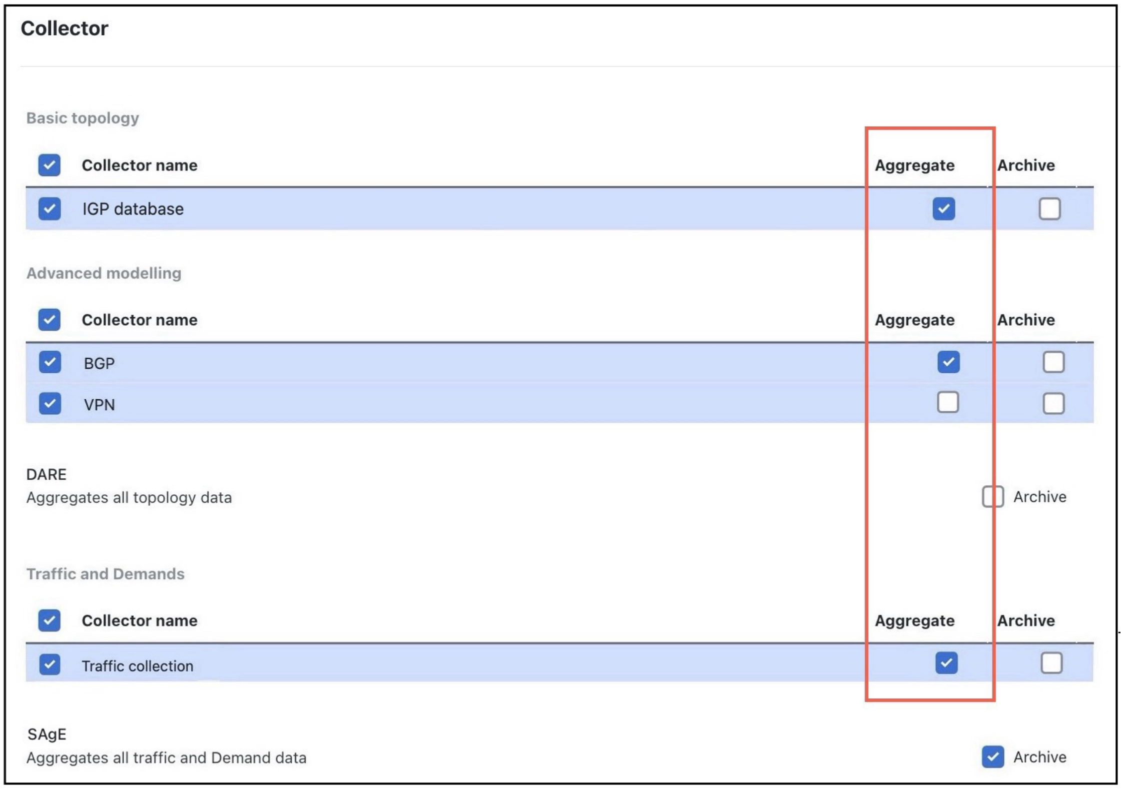
Procedure

Step 1 Open the Add or Edit Schedule page for the collection you want to edit. For more information, see Schedule a collection, on page 30 or Edit a schedule, on page 32.

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

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

Figure 15: 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 more information, see Schedule a collection, on page 30.

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

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

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

Reaggregate collector outputs

This topic describes how to reaggregate collector outputs.

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

Note

In a collection,

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

Procedure

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

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

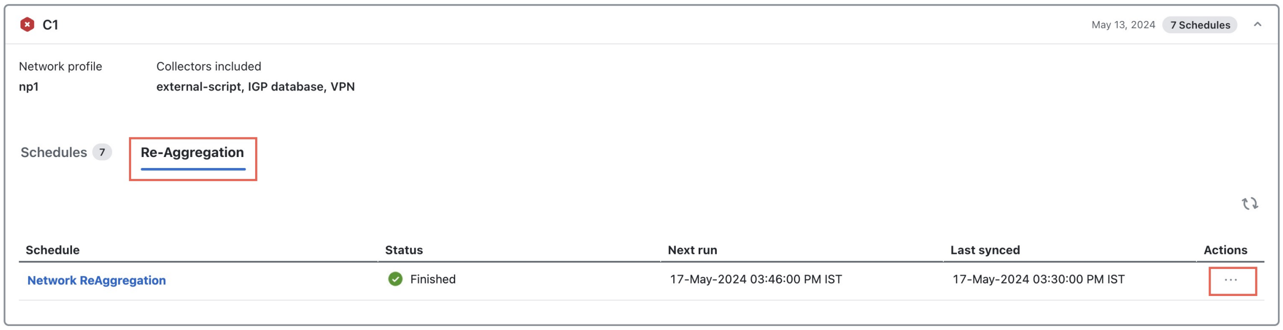
Step 3 Click the **Re-Aggregation** tab.

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

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

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

Figure 16: Reaggregation of a 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	···

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

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

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

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

Configure archive

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

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

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

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

Before you begin

It is assumed that you are in the middle of creating a network model when performing the steps described in this topic. For more information, see Configure a collection, on page 24.

Procedure

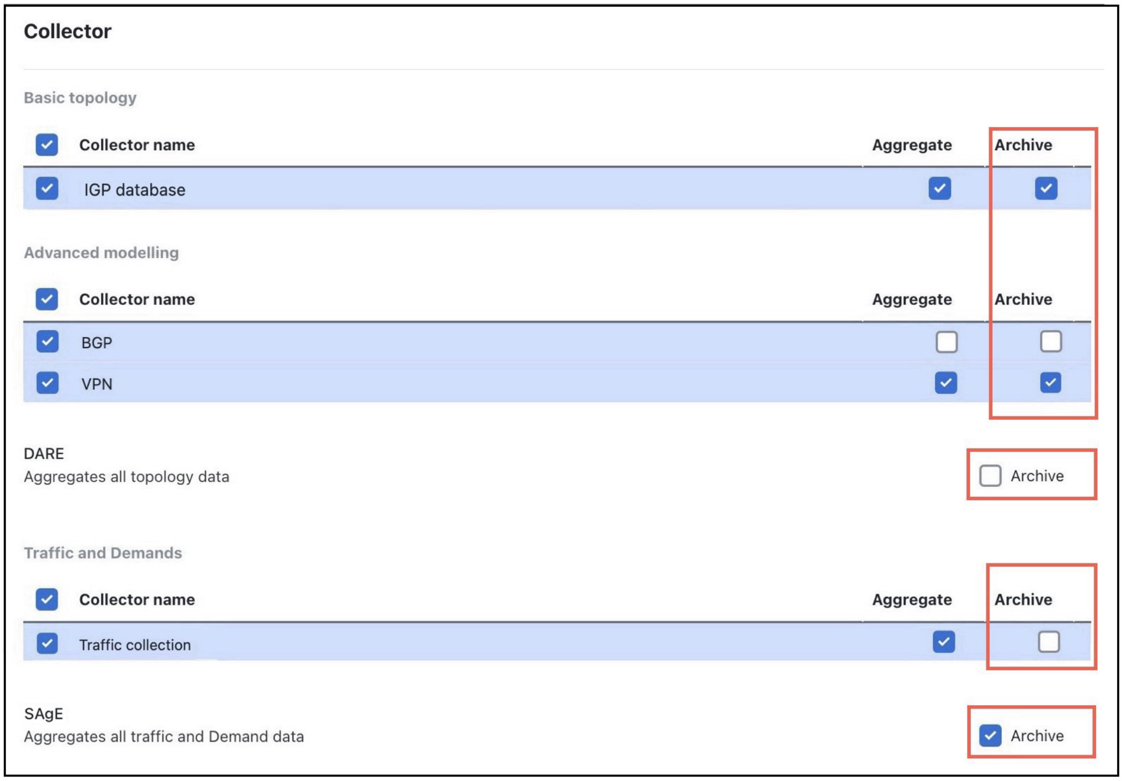
Step 1 Open the Add or Edit Schedule page for the collection that you want to edit. For more information, see Schedule a collection, on page 30 or Edit a schedule, on page 32.

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

Step 3 Under the **Collector** section:

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

Figure 17: 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 more information, see Schedule a collection, on page 30.

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

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

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

What to do next

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

View or download plan files

The archived network models are saved in a plan file format (.pln). You can access them 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.

When the applications are installed…	Then the archived network models…
on the same machine	appear under **Network Models** > **Local archive**.
on different machines	appear under **Network Models** > **Remote archive** of the Cisco Crosswork Planning Design application.

For details, refer to View or download a plan file from the local archive, on page 42 and Accessing plan files from remote archive, on page 43.

View or download a plan file from the local archive

This topic describes how to view or download a plan file from the Local archive.

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

Before you begin

Make sure that the network model has been archived. For more information, see Configure archive, on page 40.

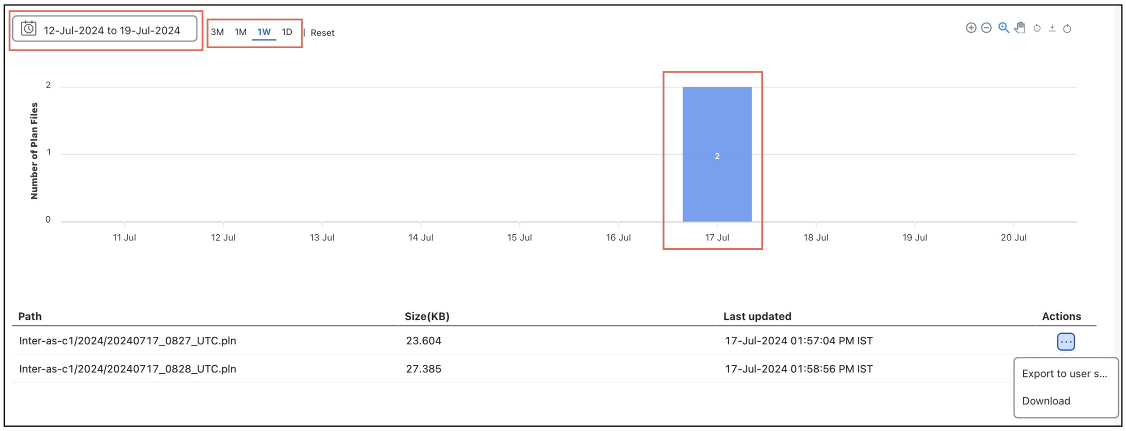
Procedure

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

Step 2 In the left pane, under **Local archive**, select the desired collection name from the list of archived collections.

The right panel displays a list of plan files created under this collection at various scheduled times. Use the **Last updated** column to find out when the plan file was created.

Figure 18: 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. Plan files generated during the selected date range appear at the bottom.

- Use the links next to the date range selection field to view the plan files generated during the last three months (3M), the last month (1M), the last week (1W), or the last day (1D).
- Click a bar graph segment 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** in the **Actions** column.

The Export plan to User Space page appears.

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

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

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 now available on the **User space** > **My network models** page.

Step 7 (Optional) To download the plan file to your local machine, click ⋯ > **Download** under the **Actions** column.

The plan file is exported to user space or downloaded to your local machine. You can now use, analyze, or visualize the plan file as needed.

What to do next

To visualize the network model, go to **User space** > **My network models** and click the file name. The network model opens in the **Network Design** page. For more information, see *Cisco Crosswork Planning Design 7.2 User Guide*.

Accessing plan files from remote archive

Summary

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

Workflow

These stages describe how to access plan files from remote archive.

1. Ensure that the network model is archived on the machine where the Cisco Crosswork Planning Collector application is installed. For details, see Configure archive, on page 40.
2. From the Cisco Crosswork Planning Design application, connect to the machine where the Collector application is installed (external collector). For details, see Connect to the external collector, on page 44.
3. Access network models from the Remote archive section of the Cisco Crosswork Planning Design application. For details, see View or download a plan file from remote archive, on page 44.

Connect to the external collector

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

Procedure

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

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

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

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

Step 5 Click **Save**.

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

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

What to do next

View or download the archived network models from the Remote archive. For details, see View or download a plan file from remote archive, on page 44.

View or download a plan file from remote archive

This topic describes how to view or download a plan file 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 In the left pane, under **Remote archive**, select the required collection name from the list of archived collections.

The right panel displays a list of plan files created under this collection at various scheduled times. Use the **Last updated** column to find out when the plan file was created.

You can filter the plan files in several ways (see Figure 18: Archived plan files, on page 42):

- Use the date range selection field at the top to select the required start and end dates. Plan files generated during the selected date range appear at the bottom.
- Use the links next to the date range selection field to view the plan files generated during the last three months (3M), the last month (1M), the last week (1W), or the last day (1D).
- Click a bar graph segment 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** in the **Actions** column.

The Export plan to User Space page appears.

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

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

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

Step 7 Click **Save**.

The plan file is now available on the **User space** > **My network models** page.

Step 8 (Optional) To download the plan file to your local machine, click ··· > **Download** under the **Actions** column.

The plan file is exported to user space or downloaded to your local machine. You can now use, analyze, or visualize the plan file as needed.

What to do next

To visualize the network model, go to **User space** > **My network models** and click the file name. The network model opens in the **Network Design** page. For more information, see *Cisco Crosswork Planning Design 7.2 User Guide*.

Collector configuration migration

Collector configuration migration is a process that

- transfers collector configurations from Cisco WAE 7.5.x/7.6.x or between different Cisco Crosswork Planning instances
- preserves existing collector settings, and
- facilitates continued operation on the target platform.

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

Migrate collector configurations from Cisco WAE

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

Note If using the Layout collector, 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.

Before you begin

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

Procedure

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

a) Log in to the machine where Cisco WAE 7.x is installed.

b) Enter this command:

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

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

a) Log in to the machine where the Cisco WAE 7.x configuration is backed up.

b) Enter this command:

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

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

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

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

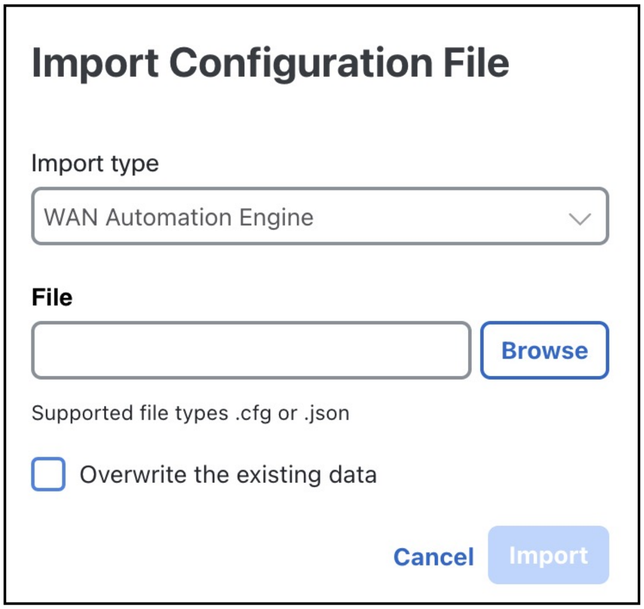
a) Log in to the Cisco Crosswork Planning UI.

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

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

The Import Configuration File page appears.

Figure 19: Import Configuration File page



Import Configuration File

Import type: WAN Automation Engine

File

Supported file types .cfg or .json

□ Overwrite the existing data

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

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

What to do next

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

Configurations excluded during migration

These configurations are not migrated while moving from Cisco WAE to Cisco Crosswork Planning.

Core system and credential configurations

- HA, LDAP, and user management configurations
- Smart Licensing configurations
- WMD configurations
- Networks that are not part of the Composer workflow

- The configured device credentials. A default credential is imported and you must re-enter the credentials.
- Network record plan files

Feature-specific configurations

- All optical/L1 related configurations such as 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 the 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 External executable script configurations, as these scripts may require some changes and testing before deploying to Cisco Crosswork Planning.
- 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.

Migrate collector configurations between two instances

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

Note

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

Procedure

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

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

The collector configuration file is downloaded to your local machine.

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

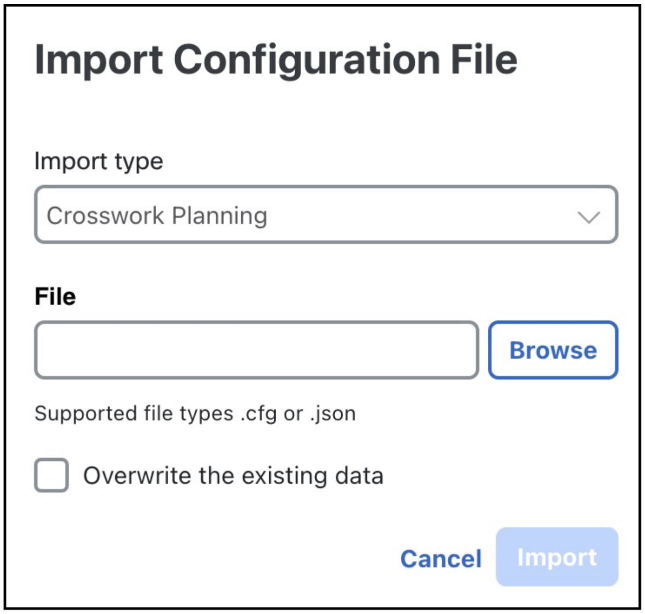
a) Log in to the Cisco Crosswork Planning instance to which you want to migrate the configuration.

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

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

The Import Configuration File page appears.

Figure 20: Import Configuration File page



Import Configuration File

Import type: Crosswork Planning

Supported file types .cfg or .json

d) Select **Crosswork planning** from the **Import type** drop-down list.

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

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

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

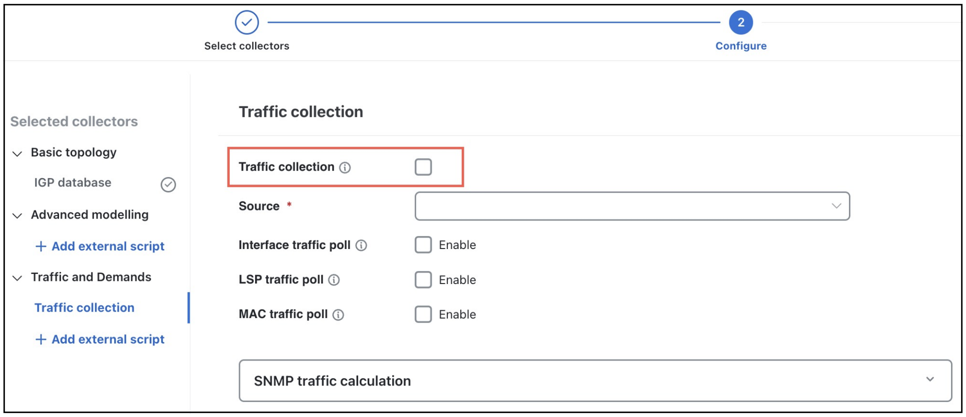
The system proceeds with the import using your configuration. You can monitor the progress on the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays **Success**.

What to do next

Note

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

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



Traffic collection

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 83.

CHAPTER 3

Supported Collectors and Tools

Collector descriptions

Each collector in Cisco Crosswork Planning has capabilities that determine what it collects or deploys. This table summarizes the collectors and their functions.

Table 5: Collector descriptions

Collector	Description	Prerequisites and notes	Configuration steps
Basic Topology Collection			
IGP database	Discovers IGP topology using login and SNMP.	This is a basic topology collection. The resulting network model is used as the source network for other collectors.	See Collect topology information using the IGP database collector, on page 56

Collector	Description	Prerequisites and notes	Configuration steps
SR-PCE	• Discovers Layer 3 topology using SR-PCE. • Uses raw SR-PCE data as the source for the topology. • Discovers node, interface, and port properties using SNMP.	• Configure SR-PCE agents before running this collection. For details, see Configure agents, on page 18. • 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 Configure the SR-PCE collector to collect topology information, on page 58
Advanced Modeling Collection			
LSP	Discovers LSP information using SNMP.	• A network model with basic topology collection must exist. • If using SR-PCE, collect the topology information using the SR-PCE collector, before running this collection. For details, see Configure the SR-PCE collector to collect topology information, on page 58.	See Collect LSP information, on page 61
PCEP LSP	Discovers PCEP LSPs using SR-PCE. **Note** This collector is accessible only when SR-PCE collector is selected as the basic topology collector.	Collect the topology information using the SR-PCE collector before running this collection. For details, see Configure the SR-PCE collector to collect topology information, on page 58.	See Collect PCEP LSP information using SR-PCE, on page 63
BGP	Discovers BGP peering using login and SNMP.	A network model with basic topology collection must exist.	See Discover BGP peers, on page 67
VPN	Discovers Layer 2 and Layer 3 VPN topology.	A network model with basic topology collection must exist.	See Discover VPN topology, on page 70
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 78
Traffic and Demands Collection			
Inventory	Collects hardware inventory information.	A network model with basic topology collection must exist.	See Collect hardware inventory information
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 64

Collector	Description	Prerequisites and notes	Configuration steps
Layout	Adds layout properties to a source model to improve visualization.	• An aggregated network model. • After you configure the Layout collector, import a plan file containing layout properties into the Layout model.	See Configure the Layout collector for improved network model visualization, on page 82
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 61. • If collecting VPN traffic, a network model with VPN collection must exist. See Discover VPN topology, on page 70.	See Collect traffic statistics, on page 83
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 88
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 90
Custom Scripts			
External script	Runs customized scripts to append additional data to a source network model.	A source network model and a custom script must exist.	See Run an external script against a network model, on page 92

Run an external script as a startup script

This topic describes how to run an external script as a first step in a collection configuration chain.

You can provide an external script as the initial step in a data collection chain. When enabled, the startup script is executed before any other collectors in the chain. This feature allows greater flexibility in how data is gathered and processed during collection.

If a startup script is used as the first step, the IGP database or SR-PCE collector becomes optional. Its configuration section will have a Source drop-down list enabled. This source is not used by the basic topology collectors for data collection. It is used to determine the order of execution of these collectors after the startup script and other external scripts in basic topology.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Review Important notes on custom startup scripts, on page 55.
- Have the custom script and any supporting files ready in one of the accepted file formats or compressed archives.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 In the **Startup script** section, select **Script**.

Step 3 (Optional) If you choose a startup script, you may skip the Basic topology collector, or configure it with the startup script as its source. Select any additional collectors as needed.

Step 4 On the Configure page, enter the script details. The startup script configuration is similar to that of other external scripts except that it does not require a source.

Option	Description
Collector name	Specify the name for the collection.
Is source a plan file?	Check this check box if you want to run the script on a plan file. If you select this option, enter the plan file details in the **Input plan file** field.
Input file	Upload your custom script and any supporting files necessary for its successful execution. If multiple files are required, compress them into a single archive before uploading. Valid file formats are .py, .sh, .pl, .zip, .tar, .gz, and .tar.gz. **Note** Each time a file is uploaded, the input file option is overwritten.
Executable script	Enter the name of the file that initiates the script execution process. This is one of the files you uploaded in the **Input file** field. For more information, see Run an external script against a network model, on page 92.
Script language	Select the language of the custom script. The valid script languages are Python, Shell, and Perl.
Aggregator properties	If you want to specify any tables or columns to be aggregated, then list them in a .properties file and upload the file using this field. By default, all columns and tables are aggregated.
Timeout	Specify the action timeout. The default is 30 minutes.

Step 5 (Optional) If you selected other collectors in Step 3, configure their parameters as needed.

To use the startup script as a source for any of the collectors, while configuring the collector parameters, select the startup script name from the **Source** drop-down list.

Step 6 Click **Next**.

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

Step 8 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

Your custom script executes as a first step in the collection configuration chain.

Important notes on custom startup scripts

Review these points when using custom startup scripts in your collections:

- Only one startup script is allowed per collection chain.
- The aggregation of any database file produced by the startup script depends on the aggregator properties set in the collector configuration.
- If you configure a collector to use a startup script as its source and the script does not produce a valid database file, the collector execution will fail.
- When migrating or restoring configurations from earlier releases, ensure that all required startup script options are available and properly populated.
- 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.

Collecting basic topology information

Summary

Collecting basic topology information involves selecting and configuring a basic topology collector to build an initial network model that serves as the source for further data collections in Cisco Crosswork Planning. Selecting the appropriate topology collector determines which data sources are included.

Two key collectors involved in the process are:

- **IGP database**: Discovers IGP topology using login and SNMP.
- **SR-PCE**: Discovers Layer 3 topology using BGP-LS via SR-PCE.

You can select only one collector per collection to gather topology information. Selecting both collectors at the same time is not allowed.

Workflow

These are the stages of collecting basic topology information.

1. Select either the **IGP database** or the **SR-PCE** collector to gather topology information for a given collection.
2. Configure the chosen collector based on your requirements.
3. Generate a network model from the collected data, which becomes the source for additional data collections.

For step-by-step instructions on configuring the **IGP database** and **SR-PCE** collectors, see Collect topology information using the IGP database collector, on page 56 and Configure the SR-PCE collector to collect topology information, on page 58.

Collect topology information using the IGP database collector

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

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

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

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Ensure you have network credentials and access for routers to be used as seed routers.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

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

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

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

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

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

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

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

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see IGP and SR-PCE collection advanced options, on page 59.

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

SR-PCE agent and collector

The SR-PCE agent and SR-PCE collector are Cisco Crosswork Planning components that enable communication and telemetry data collection between SR-PCE servers and the network.

SR-PCE agent

An SR-PCE agent is a Cisco Crosswork Planning component that

- connects to the SR-PCE server and processes the telemetry data sent by the server
- uses two different REST connections with SR-PCE: one for LSP data collection and another for topology data collection, and
- can optionally subscribe to SR-PCE and listen to further network change events after collecting topology and LSP data.

SR-PCE collector

An SR-PCE collector is a Cisco Crosswork Planning component that

- captures network updates for any changes in IGP Metric, Delay, and Node Overload
- populates the FlexAlgoAffinities, FlexAlgorithms, SRv6NodeSIDs, SRv6InterfaceSIDs, NodePrefixLoopbacks, and NodeSIDPrefixLoopbacks tables, and
- reads the LocalDomainIdentifier column of NetIntXtcLinks and populates the IGP Process ID in the Interfaces table.

The SR-PCE collector does not populate the SRv6NodeSIDPrefixLoopbacks table because the loopback address associated with SRv6 is not obtained using SR-PCE. To populate the SRv6NodeSIDPrefixLoopbacks details, add an external script while configuring the collector. Otherwise, the cross-table filter from SRv6NodeSIDs to NodePrefixLoopbacks will not display any results in the Cisco Crosswork Planning Design application. For details on running the external scripts, see Run an external script against a network model, on page 92.

Methods for topology discovery

The network model resulting from topology discovery is used as the source network for additional collections. It provides the core node, circuit, and interface information used by other collectors.

Topology and interface or port properties can be discovered in two ways.

- Using SNMP: Preferred for network discovery, as it retrieves detailed node and interface or port properties.
- Using SR-PCE only (the Extended discovery field disabled): Useful for testing, or if SNMP is unavailable.

Important notes on SR-PCE topology collection

- The default ISIS level is set to level 2 for NodePrefixLoopbacks. The OSPF network uses the same value.
- Cisco Crosswork Planning does not reflect changes from a non-null value to a null value in the FlexAlgo columns. The updated values start reflecting after a DARE re-sync.
- During data collection, dual stack support (the ability to handle both IPv4 and IPv6 simultaneously) and configuration of OSPF or ISIS on an interface are populated correctly. However, if both OSPF and ISIS are enabled on a single interface for data collection, dual stack and its interface resolution are not supported during SR-PCE collection.
- The IPv4 metric value is populated in the IGP metric table and the IPv6 value is populated in the IPv6-IGP metric table. The TE metric values are updated in the same way.
- The SR-PCE collector can collect Application-Specific Link Attribute (ASLA) delay information for interfaces and typically updates this information in the database in real time. However, if the collector receives several consecutive topology update events from SR-PCE within one minute, it may record the changes only during the next collection. In rare cases, the update may take effect only after manually restarting the SR-PCE agent.

Configure the SR-PCE collector to collect topology information

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

Follow these steps to configure the SR-PCE collector.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Ensure an SR-PCE agent is configured and running. For details on agent setup, see Configure agents, on page 18.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

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

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

- **SR-PCE host**: Select an SR-PCE agent.

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

Step 4 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see IGP and SR-PCE collection advanced options, on page 59.

Step 5 Click **Next** to continue.

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

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

IGP and SR-PCE collection advanced options

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

Table 6: IGP and SR-PCE collection advanced options

Option	Description
Options applicable for both IGP and SR-PCE collection:	
Nodes	
Node performance collection	Collects node performance data if enabled.
Remove node suffix	Removes node suffixes from node names if the node contains the specified suffix. For example, 'company.net' removes the domain name for the network.

Option	Description
QoS queues	Allows interfaces (configured with QoS in the router) to display QoS information.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
QoS node filter	Defines a filter to determine the nodes for which the QoS data is collected.
Interfaces	
Find parallel links	Finds parallel links that are not in the IGP database when IS-IS TE extensions are not enabled.
IP guessing	Indicates the level of IP address guessing to perform for interfaces that are not present in the topology database. This setting is used when IS-IS TE extensions are not enabled. • OFF: Performs no guessing. • Safe: Makes guesses only when there is no ambiguity. • FULL: Makes best-guess decisions when there is ambiguity.
Port LAG discovery	Enables LAG discovery of port members.
LAG port match	Determines how to match local and remote ports in port circuits. • Guess: Creates port circuits to match as many ports as possible. • Exact: Matches based on LACP. • Complete: Matches based on LACP first, and then tries to match as many as possible. • None: Does not create port circuits.
Cleanup circuits	Removes circuits that do not have IP addresses associated with interfaces. Circuit removal is sometimes required when there are IS-IS advertising inconsistencies in the IS-IS database.
Copy description	Copies physical interface descriptions to logical interfaces if there is only one logical interface and its description is blank.
Physical ports	Collects L3 physical ports for Cisco devices.
Minimum IP guessing	Specifies the minimum prefix length for IP guessing. All interfaces with equal or larger prefix lengths are considered.
Minimum prefix length	Specifies the minimum prefix length allowed when finding parallel links. All interfaces with equal or larger prefix lengths (but less than 32) are considered.

Option	Description
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.
Option applicable only for SR-PCE collection:	
Single-ended eBGP discovery	Discovers eBGP links that have only a single link end. This scenario is not common.

Collect LSP information

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

Note

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

Step 5 Enter these configuration parameters:

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

Step 6 (Optional) Expand the **Advanced settings** panel and enter the details in the relevant fields. For descriptions of these advanced options, see LSP collection advanced options, on page 62.

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

LSP collection advanced options

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

Table 7: LSP collection advanced options

Option	Description
Use calculated hops	Uses the calculated path hops table instead of the actual path hops table when discovering path hops.
Find actual path	Discovers actual paths for LSPs.
Get extras	Collects additional LSP properties.
Use signaled name	Uses the LSP tunnel signaled name instead of the LSP tunnel name (IOS-XR). **Note** To retrieve the signaled name when using Config parsing with the LSP collector, ensure the LSP collector executes before the Config parsing collector. If you do not follow this order, the LSP tunnel name collected by Config parsing will overwrite the signaled name value collected by the LSP collector.
Auto bandwidth	Discovers auto bandwidth.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.

Option	Description
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Collect PCEP LSP information using SR-PCE

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

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

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Complete the BGP-LS topology collection for your network using the SR-PCE collector. You need to use this model as the source network for collecting LSP information. For more information, see Configure the SR-PCE collector to collect topology information, on page 58.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

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

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

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

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

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.

- **Agents**: Select the SR-PCE agents from the drop-down list. For information on creating agents, see Configure agents, on page 18.

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

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

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

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

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Collect multicast flow data from a network

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

The Multicast collector includes these collectors:

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

Step 5 Enter these configuration parameters:

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

Step 6 (Optional) Expand the ***Collector* settings** panel and enter the details in the relevant fields. Depending on the collectors you selected in the previous step, the options differ. For descriptions of these advanced options, see Multicast collection advanced options, on page 65.

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Multicast collection advanced options

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

Table 8: Multicast collection advanced options

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

Option	Description
Traffic level name	Indicates the name of traffic level.
Traffic filtering	Defines the filtering criteria for multicast traffic from multiple sources for each S|G group.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Discover BGP peers

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

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

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

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see BGP topology advanced options, on page 68.

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

BGP topology advanced options

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

Table 9: BGP topology collection advanced options

Option	Description
ASN include	Specifies ASNs to include. By default, includes all ASNs.
Internal ASNs	Specifies internal ASNs.
Protocol	Specifies the Internet Protocol (IP) versions. The options are IPv4 and IPv6.
Min IPv4 prefix length	Specifies the minimum IPv4 prefix length to control how strictly subnet matching occurs when discovering interfaces as BGP links.
Min IPv6 prefix length	Specifies the minimum IPv6 prefix length to control how strictly subnet matching occurs when discovering interfaces as BGP links.
Login multi hop	Specifies whether to log in to routers that potentially contain multi-hop peers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values are cisco, juniper, alu, huawei.
Fallback login platform	Sets the fallback vendor if platform detection fails. Valid values are cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router. This grants higher-level access required to retrieve or modify configuration on devices that require a secondary “enable password”
Telnet username prompt	Specifies an alternative username prompt for Telnet.
Telnet password prompt	Specifies an alternative password prompt for Telnet.

Option	Description
Find internal ASN links	Finds links between two or more internal ASNs. Normally, this action is not required because IGP discovers these links.
Find non IP exit interface	Searches for exit interfaces that are not represented as next-hop IP addresses, but rather as interfaces (which are rare). **Note** This action increases the amount of SNMP requests for BGP discovery, which affects performance.
Internal exit interface	Discovers BGP links to internal ASNs.
Get MAC address	Collects source MAC addresses of BGP peers connected to an Internet Exchange public peering switch. This action is required only for MAC accounting.
Use DNS	Indicates whether to use DNS to resolve BGP IP addresses.
Force check all	Indicates whether to check all routers even if there is no indication of potential multi-hop peers. This action could be slow.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.
Login record mode	Records the discovery process. The options are Off, Record, and Playback. The default is Off. • Record: The messages to and from the live network are recorded internally as the tool runs. It is used for debugging. • Playback: The recorded messages are played back through the tool as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Discover VPN topology

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

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

Step 5 Enter these configuration parameters:

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

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

Table 10: VPN collection advanced options

Option	Description
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.

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

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

The VPN collector is now configured.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Inventory collector and hardware tables

An **Inventory** collector is a Cisco Crosswork Planning component that

- collects hardware inventory information from network devices and
- stores the collected data in structured tables (NetIntHardware*) based on hardware type.

These sections describe the process, components, configuration tables, and best practices for collecting and organizing hardware inventory information using the Inventory collector.

NetIntHardware tables

NetIntHardware* tables store the collected hardware information based on hardware type.

These are a few examples of NetIntHardware tables:

- NetIntHardwareChassis: stores router chassis objects identified by node IP address and SNMP ID.
- NetIntHardwareContainer: stores slot entries 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: stores information about 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: stores physical ports on routers.

Hardware hierarchy

A hardware has a parent-child relationship based on where the object resides within the router. The chassis, considered as the *root object*, has no parent. Except chassis, every object has one parent and can have multiple child objects. Objects without children, such as ports and empty containers, are called *leaf objects*. Hardware hierarchy generally reflects how hardware objects are installed within other objects. For instance, a module representing a line card can have as its parent a container that represents 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 of 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	NetIntHardware Chassis	0

Tracing the hierarchy from each leaf object to its corresponding root object based on the parent-child relationships results in a series of object types that form its hardware hierarchy. Using this trace, the Inventory collector determines how to process the hardware devices. You must use this process when adding an entry to the HWInventoryTemplates table.

NetIntNodeInventory table

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.

HWInventoryTemplates and HWNameFormatRules tables

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 these 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.

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

You can specify multiple name source columns using a colon. For example, Container,0,Model:Name

If a hardware category does not exist or is empty, the Inventory collector excludes it from 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:

1. 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.

2. Replaces all Cisco linecard names that match 800-20017-.* with 1X10GE-LR-SC.
3. 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

Table entries function as described::

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

HardwareSpec				
Cisco	Chassis	7609	9	1–9

Configure inventory collection

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

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

Step 6 (Optional) Expand the **Advanced settings** panel and configure any other relevant advanced fields as needed. For descriptions of these advanced options, see Inventory collection advanced options, on page 76.

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

The Inventory collector is now configured according to your settings.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Inventory collection advanced options

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

Table 11: Inventory collection advanced options

Option	Description
Get inventory options	
Login allowed	Allows logging in to the router to collect inventory data.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 30 minutes.
Build inventory options	
Exclude file	Allows you to select the file that contains the ExcludeHWList table. This table defines hardware characteristics to match against for exclusion in the output. Click the **Download sample file** link to download a sample file that contains the ExcludeHWList table.
Guess template	Broadens the search when processing raw inventory data.
Template file	Allows you to select the hardware template file that contains the HWInventory Templates and HWNameFormatRules tables. Click the **Download sample file** link to download a sample template file.
Hardware spec file	Allows you to select the file that contains the HardwareSpec table. This table defines slot counts for specific types of hardware to verify SNMP data returned from routers. Click the **Download sample file** link to download a sample file that contains the HardwareSpec table.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are: Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

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

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

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

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

Step 6 Expand the **Get config** and **Parse config** panels. Enter the details in the relevant fields. For field descriptions, see Configuration parsing advanced options, on page 79.

Note

- L2VPN config parse is not supported.
- When L3VPN information is collected by the Config Parsing collector, all VPNs are assumed to be connected to each other.
- If both the Config Parsing collector and the VPN collector are collecting VPN information, ensure that the VPN collector runs before the Config Parsing collector in the collector chain.
- Single-ended SRLGs with a missing end are collected via SR-PCE. The SRLGSCircuits table is not updated for these entries.

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Configuration parsing advanced options

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

Table 12: Configuration parsing advanced options

Option	Description
Get config options	
Collect configuration	Retrieves configuration details from devices or routers.
Force login platform	Overrides platform detection and uses the specified platform. Valid values are cisco, juniper, alu, huawei.
Fallback login platform	Sets the fallback vendor in case platform detection fails. Valid values are cisco, juniper, alu, huawei.
Try send enable	Sends an enable password if the platform type is not detected when logging in to a router. This grants higher-level access required to retrieve or modify configuration on devices that require a secondary “enable password”.
Telnet username prompt	Specifies an alternative username prompt for Telnet.
Telnet password prompt	Specifies an alternative password prompt for Telnet.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Parse config options	
Protocol type	Allows you to select the IGP protocol running in the network. The options are isis, ospf, and None. The default is **isis**.
ISIS level	Indicates the ISIS level to use. The agent can read IS-IS Level 1, Level 2, or both. If you select both, the agent combines both levels into a single network and Level 2 metrics take precedence.
OSPF area	Specifies whether to collect a single OSPF area or all areas. This option specifies the area ID or all. The default is area 0.

Option	Description
ASN	Specifies the ASN to collect. ASN is ignored by default. However, for networks that span multiple BGP ASNs, use this option to read information from more than one IGP process ID or instance ID in an ASN.
Include objects	Allows you to select the configuration objects that you want to parse. The available options are LAG, SRLG, RSVP and CS RSVP, VPN, FRR, SR LSPS, LMP, and SR Policies.
Circuit match	Indicates the criteria to use to form circuits.
LAG port match	Controls how to match local and remote ports in port circuits. • Guess: Creates port circuits to match as many ports as possible. • None: Does not create port circuits.
OSPF process ID	Specifies which OSPF process ID to use when there are multiple OSPF processes.
IS-IS instance ID	Specifies which IS-IS instance ID to use when there are multiple IS-IS instances.
Loopback interface	Specifies the loopback interface number to use for the router IP.
Resolve references	Enables resolution of IP address references during parsing.
Multithreading	Enables multithreaded processing of configuration files to speed up parsing.
Filter showcommands	Filters multiple show commands.
Build topology	Constructs network topology after parsing the configuration.
Shared media	Creates pseudonodes for shared media.
Data collection timeout	Sets the maximum time allowed for data collection, in minutes. If the specified limit is exceeded, the internal tools used for data collection will time out and exit. The default is 60 minutes.
Debug	
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.
Net recorder	Records SNMP messages. The options are Off, Record, and Playback. The default is Off. • Record: The SNMP messages to and from the live network are recorded internally as discovery runs. It is used for debugging. • Playback: The recorded messages are played back through the collector as if they came from the live network, thus providing offline debugging of network collection. • Off: No recording or playback is performed.

Collect Circuit Style RSVP-TE information

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

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

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

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Ensure that the devices have these configurations:
  - RSVP configuration with **bidirectional** enabled.
  - The **bidirectional** configuration includes the same **association id**, **source-address**, and **global-id** in both directions.
  - The **bidirectional** configuration specifies the **association type** as **co-routed**.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

For details on the other LSP and Config parsing options, see Collect LSP information, on page 61 and Collect port, LSP, SRLG, and VPN information using configuration parsing, on page 78.

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

Step 5 (Optional) Expand the **Advanced settings** panel and configure any other relevant fields. For descriptions of these advanced options, see LSP collection advanced options, on page 62.

Step 6 Click **Next**.

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

Step 8 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Configure the Layout collector for improved network model visualization

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

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

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

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

Step 5 Enter these configuration parameters:

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

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

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

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

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

The Layout collector is now configured.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Collect traffic statistics

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

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

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

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- To collect VPN traffic, you must have a VPN network model. For details, see Discover VPN topology, on page 70.

- To collect LSP traffic, you must have an LSP network model. For details, see Collect LSP information, on page 61.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

a) Check the **Traffic collection** check box to enable the traffic poller.

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

c) To run continuous traffic collection for interfaces, enable **Interface traffic poll** and then enter the following:

- **Polling period**: Enter the polling period in seconds. We recommend starting with 60 seconds.
- **QoS**: Check the **Enable** check box if you want to enable queues traffic collection.
- **VPN**: Check the **Enable** check box if you want to enable VPN traffic collection. If enabled, confirm that the source network model has VPNs enabled.

d) To run continuous traffic collection for LSPs, enable **LSP traffic poll** and then enter the following:

- **Polling period**: Enter the polling period in seconds. We recommend starting with 60 seconds.

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

e) To run continuous traffic collection for MAC accounting, enable **MAC traffic poll** and then enter the following:

- **Polling period**: Enter the polling period in seconds. We recommend starting with 60 seconds.

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

f) (Optional) Expand the **SNMP traffic computation** panel and enter the details in the relevant fields. For field descriptions, see Traffic collection advanced options, on page 85.

Step 5 Click **Next**.

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

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Traffic collection advanced options

You can configure several advanced options when using Traffic collection.

Table 13: Traffic collection advanced options

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

Tune the traffic poller settings

This topic describes the efficient way to run traffic polling.

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

Procedure

Step 1 Set the traffic poller verbosity to 40 in the **Traffic collection** configuration page.

Step 2 Start with the default options and run continuous collection for several hours. The default values include:

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

Step 3 Configure the Traffic collection scheduler to run every 300 seconds.

Step 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.

Step 5 Search for actual collection times.

Example:

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

In this example, the fastest pace at which the poller can poll the network is around 40 to 50 seconds. This value represents the minimum polling period for both Interface traffic poll and LSP traffic poll. Since the traffic poller populates traffic for both interfaces and LSPs at the same time, set both values to the same number.

The traffic poller calculates traffic by collecting raw traffic counters, such as c1, c2, and so on. It requires at least two counters to calculate traffic.

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

Best practices for poller configuration

Follow these best practices to optimize poller configuration and ensure reliable traffic data collection:

- Set **Minimum window length** to at least **2 * polling period**, because the poller requires at least two counters. Increase the window length by 25% or more to accommodate network variations.

  Minimum window length is a sliding window that is used to sample two counters. It looks for two counters which are farthest apart, that is, the latest and earliest within a specified period. The average traffic is calculated for this period. Since the poller requires at least two counters, the smallest value must be at least twice the polling period.

- Set **Maximum window length** to at least **2 * polling period**. Increase the window length by 50% or more to accommodate network variations. For unresponsive nodes, increase by 100% or more.

  If the Minimum window length does not find enough counters for the specified period due to increased network latency or node response time, the poller reports traffic as N/A. To avoid empty traffic data, use an insurance window called **Maximum window length**.

- Set **Raw counter TTL** to be equal to or greater than **Maximum window length**.

  The traffic poller stores raw counters in memory for traffic calculation, which uses RAM space. The traffic poller periodically cleans up old counters stored in memory. The system deletes any counter data older than Raw counter TTL (minutes).

- Monitor the poller memory usage and the time taken to populate traffic. Traffic population in traffic poller is the process of calculating traffic in the network and updating the plan file. The duration depends on network size. The system logs the actual time taken to populate traffic in the snmp-traffic-poller-service.log file.

  Lines from an example log file:

  ```
  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 this example, the fastest rate for populating traffic, and consumed by other tools, is about 400 seconds.

- If you see "Invalid counter" warnings in the snmp-traffic-poller-service.log file, for example, c1.counter is greater than c2.counter resulting in negative traffic, recognize that counters might have reset or overflowed. This issue commonly occurs with 32-bit counters. If you see many such errors, increase the sliding window sizes to process more counters and reduce chance of failure.

- Do not poll network at a faster rate than populating traffic. In the example above, the most aggressive polling setting is 50 seconds, whereas traffic population takes around 400 seconds. This results in eight wasted network polls. To resolve this, increase the traffic polling period, sliding window sizes, and Raw counter TTL.

  - Here is the recommended configuration for this example:

    1. Set these 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 minutes for traffic population. This timeout is not used generally and should be set only as high as necessary.

  - You can adjust these numbers to be less aggressive to save CPU resources and network bandwidth. To do this:

    1. Set these values:

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

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

Collect traffic demands information

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

Before you begin

Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

Note

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

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

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

On the Add Mesh Step page, enter these details:

a) In the **Name** field, enter the name for the step.
b) In the **Step number** field, enter the execution order for this step.
c) From the **Tool** drop-down list, select the required tool. The available tools include Demands for P2MP LSPs, Demand deduction, External executable script, Copy demands, Demands for LSPs, or Demand mesh creator.
d) Check the **Enable** check box to run the selected tools.
e) Update or enter the details in the **Tool configuration** section. The options differ based on the selected tool.
f) (Optional) Expand the **Advanced** panel and enter the relevant details.
g) Click **Continue**.

Repeat this step to add more steps to the configuration.

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

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

NetFlow data collection

NetFlow data collection is a process where Cisco Crosswork Planning

- collects NetFlow and related flow measurements from the network devices
- aggregates these measurements to construct accurate demand traffic data for Cisco Crosswork Planning Design, and
- provides an alternative to estimating the demand traffic from interfaces, LSPs, and other statistics using Demand deduction.

A NetFlow collector gathers information about traffic flow and helps build a traffic and demand matrix.

Importing flow measurements is useful when there is full or nearly complete flow coverage at a network's edge routers. In addition, it is beneficial when accuracy of individual demands between external autonomous systems (ASes) is of interest.

Data collected separately by the collectors, such as topology, BGP neighbors, and interface statistics, combines with flow measurements to scale flows and provide a complete demand mesh between both external ASes and internal nodes.

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

Types of data collected

Cisco Crosswork Planning gathers these 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 peer information collected over SNMP
- BGP path attributes over peering sessions

NetFlow collection configuration requirements

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.

The configuration requirements include:

- Configure routers to export flows and establish BGP peering with the flow collection server.
- Export NetFlow v5, v9, and IPFIX datagrams to the UDP port 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.
- Limit the maximum length of the BGP AS path attribute to three hops when receiving BGP routes. This helps to prevent excessive server memory consumption. The total length of BGP attributes attached to a single IP prefix, including AS path, can be very large, up to 64 KB.

Configure the NetFlow collection

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

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Ensure all NetFlow agents are configured to operate in single mode.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

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

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

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

Step 5 Enter these configuration parameters:

- **Source**: Select the source collector whose output serves as the input for this collector.

- **Agents**: Select the applicable agents from the drop-down list.

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

(Optional) Enter information in the other fields. For field descriptions, see NetFlow collection advanced options, on page 91.

Step 7 (Optional) Expand the **IAS flows** and **Demands** panels, and configure any other relevant advanced fields as needed. For descriptions of these options, see NetFlow collection advanced options, on page 91. Then, click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

The NetFlow collection configuration is now complete.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

NetFlow collection advanced options

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

Table 14: NetFlow collection advanced options

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

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

Run an external script against a network model

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

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

For an example of a custom script, see Sample script for updating interface descriptions, on page 95.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Have the custom script and any supporting files ready in one of the accepted file formats or compressed archives.

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

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

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

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

Step 4 Enter these details:

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

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

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

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

  These are the details of the arguments:

  - argv[1]: Source plan file

- argv[2]: Output plan file
- argv[3]: Device access authentication file
- argv[4]: Global network access configuration file
- argv[5]: Home directory
- argv[6]: Path where user uploaded external files are available
- argv[7]: Path to access archive root directory

Example:

The Sample script for updating interface descriptions, on page 95 appends a description to every interface in the network with "My IGP metric is *value*" based on the data from an Excel file named "description.xlsx". The argv[5] parameter in the script specifies the home directory path of the "description.xlsx" file. For the script to run successfully, note that you must include this Excel file in the compressed file before uploading via the **Input file** field.

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

Step 5 Click **Next**.

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

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

The custom script executes against the selected network model.

Accessing dynamic data files through external scripts

Summary

Cisco Crosswork Planning allows you to upload data files directly to the Cisco Crosswork Planning Collector. External scripts can access these files at run time, without requiring script repackaging or redeployment. This enables scripts in the Cisco Crosswork Planning Collector to use up-to-date, user-uploaded files during execution, supporting more efficient customization.

The key components involved in the process are:

- Data file uploader: Uploads updated data files to the collector.
- Upload directory: Directory where the data file is uploaded.
- External script: Reads the uploaded data files during execution.

Workflow

These are the stages of accessing dynamic data files through external scripts.

1. Upload the updated data file to the Cisco Crosswork Planning Collector’s upload directory using the REST API (https://{{server-ip:port}}/cp/collection-service/api/v1/file-gateway).
2. Run the external script, specifying the path to the data file in the upload directory as a command-line argument. argv[6] represents the path of the upload directory. For details on running an external script, see Run an external script against a network model, on page 92.

Note Uploading the same file multiple times overwrites the existing one.

3. The script reads the latest version of the data file at run time, ensuring that it processes current data.

Sample script for updating interface descriptions

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

Script content

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

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

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

srcNet.write(dest)
```

How data is collected from third-party devices

Summary

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

The support modules must

- include capabilities for data collection, such as SNMP
- allow for the input of an auth file to authenticate access to the devices it will poll

- allow for the input of a network access configuration file to manage specifics of collection, such as timeouts, retries, maximum request per device, and so on
- read and write to a plan file

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

Workflow

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

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

Collectors with support module configurations

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

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

Collect data from third-party devices

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

Before you begin

- Ensure you have the required support module.
- Complete the steps mentioned in Preconfiguration workflow, on page 9.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 To use an external script as a first step of the collection configuration chain, select the startup script option. When using a startup script, you can either skip the basic topology collector or configure it to use the startup script as its source. If you do not use a startup script, you must select one of the basic topology collectors as needed.

Step 3 In the **Advanced modeling** section, select any of the required collectors listed in Collectors with support module configurations, on page 96. Then, click **Next**.

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

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

Step 5 To collect data from third-party devices:

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

All support module configuration options appear.

b) Enter the details for these parameters:

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

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

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

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

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

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

Step 8 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

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

Merge AS plan files

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

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

Important notes on the Merge AS tool

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

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

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Collect topology and traffic information for different ASes.
- Ensure that the plan files from different ASes are present on the same Cisco Crosswork Planning server, and their file paths are specified.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

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

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

Step 4 Enter these configuration parameters:

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

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

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

Note

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

Step 7 Click **Next**.

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

Step 9 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

The resulting plan file consolidates data from different ASes.

What to do next

Use this collection as the source network to configure additional collections. For details on configuring different collectors, see the relevant topics in this chapter. For details on editing the collection, see Edit a collection, on page 28.

Representative plan files

A representative plan file is a network plan that

- provides a view that better represents the general network state
- is generated using multiple snapshots from an archive, and
- includes multiple traffic levels, each corresponding to a specified time interval.

Plan files are snapshots of a network state at a point in time. Transitory events, such as failures, are captured in the snapshot if they occur during the collection window. The traffic collected is the specific traffic that occurred during that collection window, which can be five minutes or less. As such, a snapshot usually does not represent the network state over the course of a typical day or week of network operation, and thus, is inadequate to use as the basis for long-term design and planning tasks. To address these needs, the **Create representative plan** tool uses multiple snapshots from an archive to construct a single plan that is more representative of the general network state.

You can use an external script to create a representative plan. Use the **argv[7]** argument in your script to access the archive root directory where all archives are available.

A representative plan file is particularly useful when planning networks where peak utilization occurs at unknown or different times of the day across different interfaces. A simulation analysis performed over all traffic levels identifies the time intervals when peaks occur.

Features of a representative plan

- The topology is extracted from a base plan, which by default is the most recent snapshot. However, you can specify any plan file as the base plan.
- The representative plan contains multiple traffic levels, one for each specified time interval. For example, there could be one traffic level per hour.
- Demands are extracted from snapshots that are selected from each of these time intervals. A single demand in the representative plan file contains a range of traffic values that represent the different amounts of traffic for that demand over the course of the specified time period.
- Interface, LSP, and node measurements are extracted from snapshots that are selected from each of these time intervals.

How the Create representative plan tool works

Summary

The **Create representative plan** tool creates a single plan file from snapshot plans in the archive. It creates traffic levels in the plan, each representative of demand traffic in a given time interval during a day or week.

Workflow

These stages describe how the tool creates a representative plan:

1. The tool examines all snapshots that fall into the specified time interval during the sample time range. Of these snapshots, Cisco Crosswork Planning selects the one with the least number of failed circuits and the most number of active interfaces in the common base plan. If there is a tie, the snapshot with the highest amount of demand traffic is selected. Only snapshots with single traffic levels are used.

2. The tool removes all traffic intervals from the base plan.

3. The tool creates new traffic intervals in the base plan, using the format HHmm-HHmm or dddHHmm-dddHHmm, depending on whether the time period is a day or a week.

   For example, 03:00-04:00 and Fri17:00-Fri18:00.

4. The tool imports all demands from the corresponding snapshot for the time interval.

   - If a snapshot demand matches the one existing in the base plan, then Cisco Crosswork Planning uses that demand and the snapshot demand traffic for it.
   - If there is no matching demand, Cisco Crosswork Planning Design creates the demand with 0 traffic.
   - If a demands exists in the base plan, but not in the snapshot, the demand is used with 0 traffic.
   - The tool also imports multicast demands with the required multicast flows and multicast destinations.

5. The tool imports measured traffic for interfaces, LSPs, and nodes that exist in both the base plan and the snapshot.

Result

Each resulting representative plan file includes a report section where each traffic level is defined per row.

Create a representative plan using the tool

This topic describes how to generate a network plan file that represents typical network conditions using multiple archived network snapshots.

Use this task when you need a plan file that reflects the overall network state, rather than a single moment in time. This is helpful for long-term network design and planning.

Before you begin

- Complete the steps mentioned in Preconfiguration workflow, on page 9.
- Ensure you have the archived plan files.

Procedure

Step 1 Decide whether to create a new collection or edit an existing one. For details, see Configure a collection, on page 24 or Edit a collection, on page 28.

Step 2 Click **Tools** at the top of the collection page.

Step 3 Select **Create representative plan** and click **Next**.

Step 4 From the **Archive** drop-down, select the archive from which you want to create the representative plan. The tool uses the snapshots from this archive and generates the final representative plan.

Step 5 Enter the relevant configuration parameters. For descriptions of these parameters, see Representative plan configuration parameters, on page 101.

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

Step 7 Configure schedules for the collection job. You can schedule the collection job to run immediately or at specific intervals. For details, see Schedule a collection, on page 30.

A representative plan file is generated based on the parameters you configured.

What to do next

You can:

- Access the resultant plan file from the Cisco Crosswork Planning Design application. For details, see View or download plan files.
- View the report from the Cisco Crosswork Planning Design application. From the visualization toolbar, select **Actions** > **Reports** > **Generated reports**. Click the **Representative Plan** link to view the report.

Representative plan configuration parameters

You can fine-tune the results to include specified snapshots for multiple traffic levels across specific intervals. This topic describes the representative plan configuration parameters.

Time interval parameters

These parameters define time intervals during a day or during a week (defined by **Time period**) that are created for the resulting plan file.

Parameter	Description
Time period	Defines whether the time intervals are for a day or a week.
Time interval length	Specifies the length of time intervals for each traffic level, in minutes. The default is 60 minutes. For time period "Day", the maximum limit is 60*24=1,440 minutes. For time period "Week", the maximum limit is 60*24*7=10,080 minutes.

Parameter	Description
Time interval starts	Defines the starting times for time intervals in the UTC time period. For example, 1600 for 4 PM, Mon1600 for Monday 4 PM. For a time period of one day, the format is "HHmm". For a time period of one week, the format is "dddHHmm". For example, 1600 for 4 PM, Mon1600 for Monday 4 PM. The default is all time intervals in the period, starting at "0000" (day) or "Mon0000" (week).

Sample time range parameters

These parameters define which periods of data in the archive are used to populate the specified time intervals.

Parameter	Description
Sample time end	Specifies the end time for the sample. The format is YYYYMMDD_HHmm. The default is the last inserted date in the archive.
Sample time length	Specifies the length of sample, in days. The default is 1 for time period "Day" and 7 for time period "Week".

Other parameters

These parameters define which periods of data in the archive are used to populate the specified time intervals.

Parameter	Description
Archive	The archive from which you want to create the representative plan. The tool uses the snapshots from this archive and generates the final representative plan.
Archive base time	Specifies the snapshot in the archive at this time as the base plan to augment with traffic levels from other snapshots in the archive. The format is YYYYMMDD_HHmm). Default is the most recent snapshot in the sample period.
Base plan	Specifies the plan file to augment with traffic levels from the archive. If provided, this will override the value specified in **Archive base time**.
Verbosity	Sets the level of detail in log messages. The default is 30, with a valid range from 1 to 60.

Sample parameters and outputs of representative plans

This topic provides sample parameters and outputs of representative plans.

Example 1

In this example, the network peak time is between 4 PM and 7 PM daily. To better understand this peak traffic, we could create a representative traffic level for each hour within this range: 4 PM, 5 PM, and 6 PM. For weekly forecast purposes, we use samples from the last five days to construct the traffic levels. We use the latest snapshot in the time period, 110502_0347_UTC.pln, as the base plan. This plan is located in the archive named “backbone”.

Parameters used:

- Archive: backbone
- Base plan: 110502_0347_UTC.pln
- Time interval length: 60
- Sample time length: 1
- Time interval starts: 1600, 1700, 1800

Output:

Traffic level	Snapshot	Matching interfaces	Total demand traffic	Total demands	Demands not imported
16:00-17:00	110502_0347_UTC.pln	25	43534.32	453	4
17:00-18:00	110502_0347_UTC.pln	25	47583.23	454	3
18:00-19:00	110502_0347_UTC.pln	25	50771.49	454	3

Example 2

In this example, we know the network peak times are around 4 PM daily, as well as 8 PM on Fridays. We need to get a representative traffic level for each of these six periods for the last two weeks. Because today is Tuesday, yesterday’s 4-5 PM range and last week’s Monday 4-5 PM range are used to construct the 4 PM traffic level. The base plan, 110407_0423_UTC.pln, is in the "acme" directory.

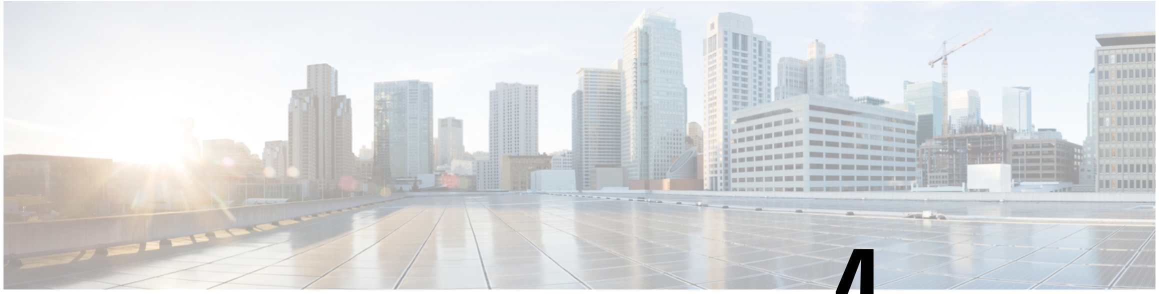
Parameters used:

- Base plan: 110407_0423_UTC.pln
- Time period: week
- Time interval length: 60
- Sample time length: 14
- Time interval starts: Mon1600, Tue1600, Wed1600, Thu1600, Fri1600, Fri2000

Output:

Traffic level	Snapshot	Matching interfaces	Total demand traffic	Total demands	Demands not imported
Mon16:00-Mon17:00	110407_0423_UTC.pln	97	43534.32	6702	21

Traffic level	Snapshot	Matching interfaces	Total demand traffic	Total demands	Demands not imported
Tue16:00-Tue17:00	110407_0423_UTC.pln	97	47583.23	6702	21
Wed16:00-Wed17:00	110407_0423_UTC.pln	95	50771.49	6701	22
Thu16:00-Thu17:00	110407_0423_UTC.pln	97	56831.91	6702	21
Fri16:00-Fri17:00	110407_0423_UTC.pln	93	48732.18	6700	23
Fri120:00-Fri21:00	110407_0423_UTC.pln	97	53692.39	6702	21



CHAPTER 4

Manage Licenses

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that

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

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.

Benefits of Smart Licensing

Key benefits of Smart Licensing include:

- Easy activation: Establishes a pool of software licenses that can be used across the entire organization, eliminating the need for Product Activation Keys (PAKs).
- Unified management: Provides a complete view into all of your Cisco products and services in a user-friendly portal, helping you always know what you have and use.
- License flexibility: Allows you to easily use and move licenses as needed since the software is not node-locked to your hardware.

Configuring Smart Licensing

Summary

A Cisco Smart Account provides a repository for Smart enabled products. It 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 CSSM, you can create and manage multiple virtual accounts within your Smart Account to manage licenses. For details on Cisco Licensing, go to cisco.com/go/licensingguide.

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

Workflow

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

1. Set up a Smart Account on Cisco Software Central (software.cisco.com).
   - Go to Smart Account Request.
   - Follow the instructions on the website.
2. (Optional) Configure transport settings. For details, see Configure the transport mode between Cisco Crosswork Planning and CSSM, on page 106.
3. Register Cisco Crosswork Planning with CSSM. For details, see Register Cisco Crosswork Planning via token, on page 107 or Register Cisco Crosswork Planning via offline reservation, on page 110.

Configure the transport mode between Cisco Crosswork Planning and CSSM

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

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

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

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

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

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

Before you begin

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

Procedure

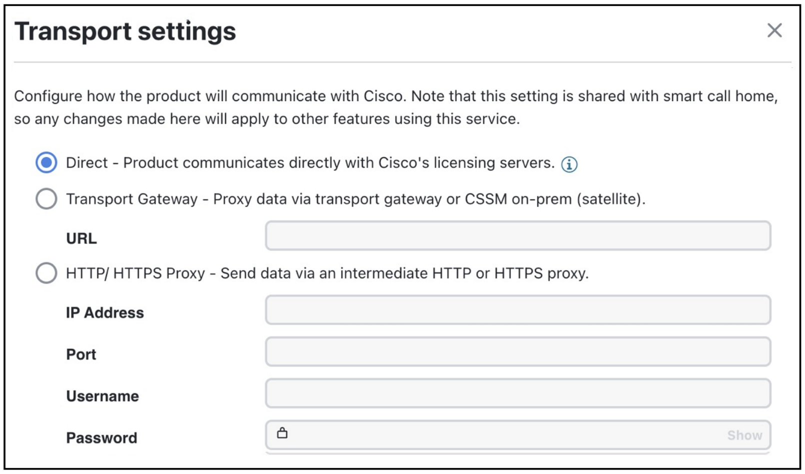
Step 1 From the main menu, choose **Licensing**.

The Smart License page opens.

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

The Transport settings page appears.

Figure 21: Transport settings page



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 appropriate transport mode. Enter values in all the required fields.

Step 4 Click **Save**.

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

Register Cisco Crosswork Planning via token

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

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

Before you begin

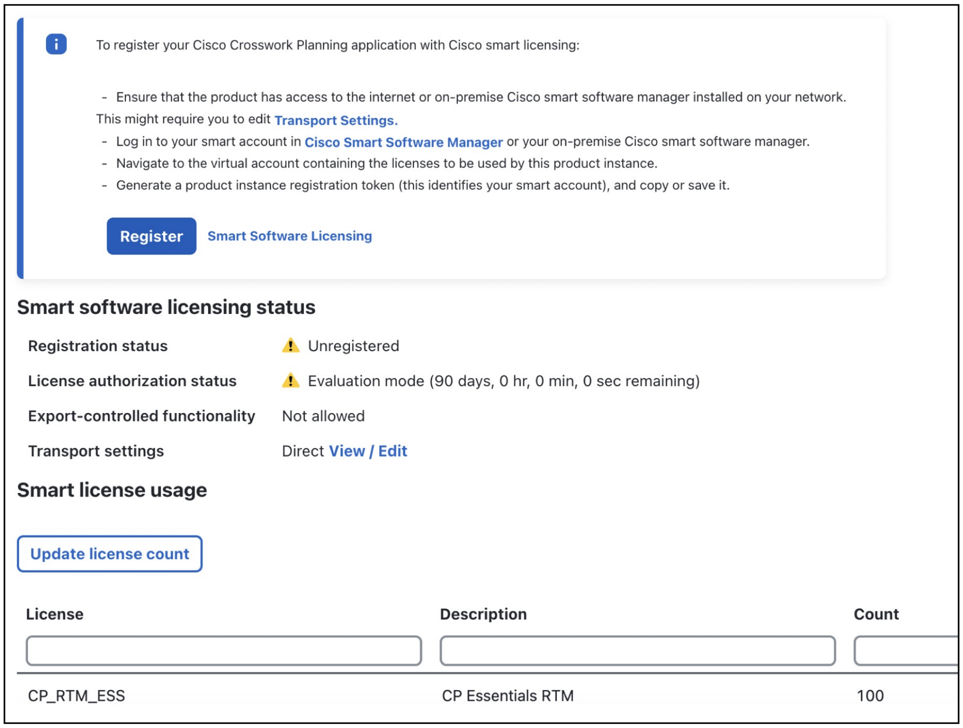
- Confirm that you have a Smart Account. If not, go to Smart Account Request and follow the instructions to create one.
- Ensure you have a valid product instance registration token. For guidance on generating the token, see the support resources in Cisco Software Central.

Procedure

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

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

Figure 22: 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

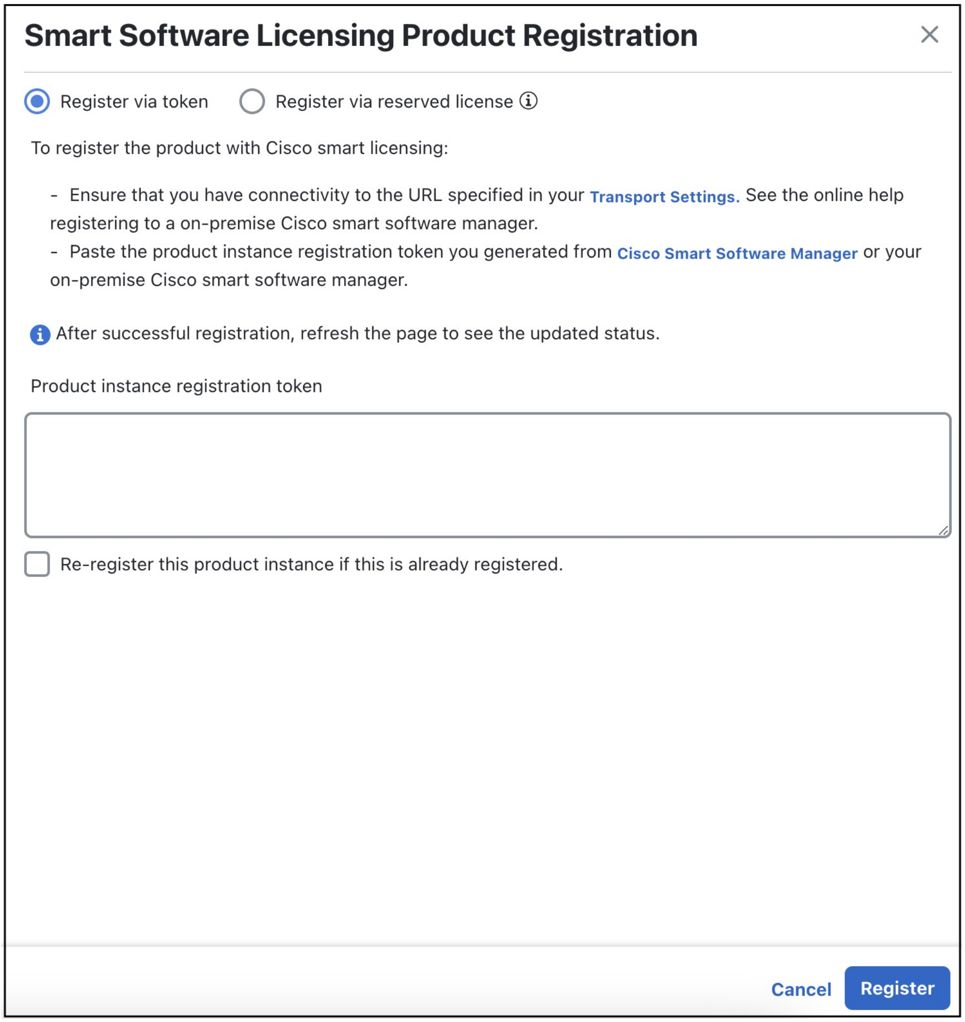
Smart license usage

License	Description	Count
CP_RTM_ESS	CP Essentials RTM	100

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

The Smart Software Licensing Product Registration page opens.

Figure 23: Smart software licensing product registration page



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. Ensure the token ID is accurate and within its validity period.

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

Step 5 Click **Register**.

Note

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

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

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

Manually perform licensing actions

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

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

Before you begin

Ensure the Cisco Crosswork Planning application is in Registered mode.

Procedure

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

The Smart License page appears.

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

Step 3 Select one of these options as required.

a) **Renew Authorization**: manually renews authorization if automatic renewal fails after 30 days.

b) **Renew Registration**: manually renews registration if automatic renewal fails after six months.

c) **Re-register**: re-registers the application, for example, if registration token has expired.

d) **De-register**: de-registers the application, for example, when you need to change the transport settings.

Note

After you de-register the application, it enters the **Evaluation** mode if evaluation period is available. Otherwise, it enters the **Evaluation Expired** mode. For more information, see License authorization statuses, on page 115.

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

Register Cisco Crosswork Planning via offline reservation

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

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

Before you begin

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

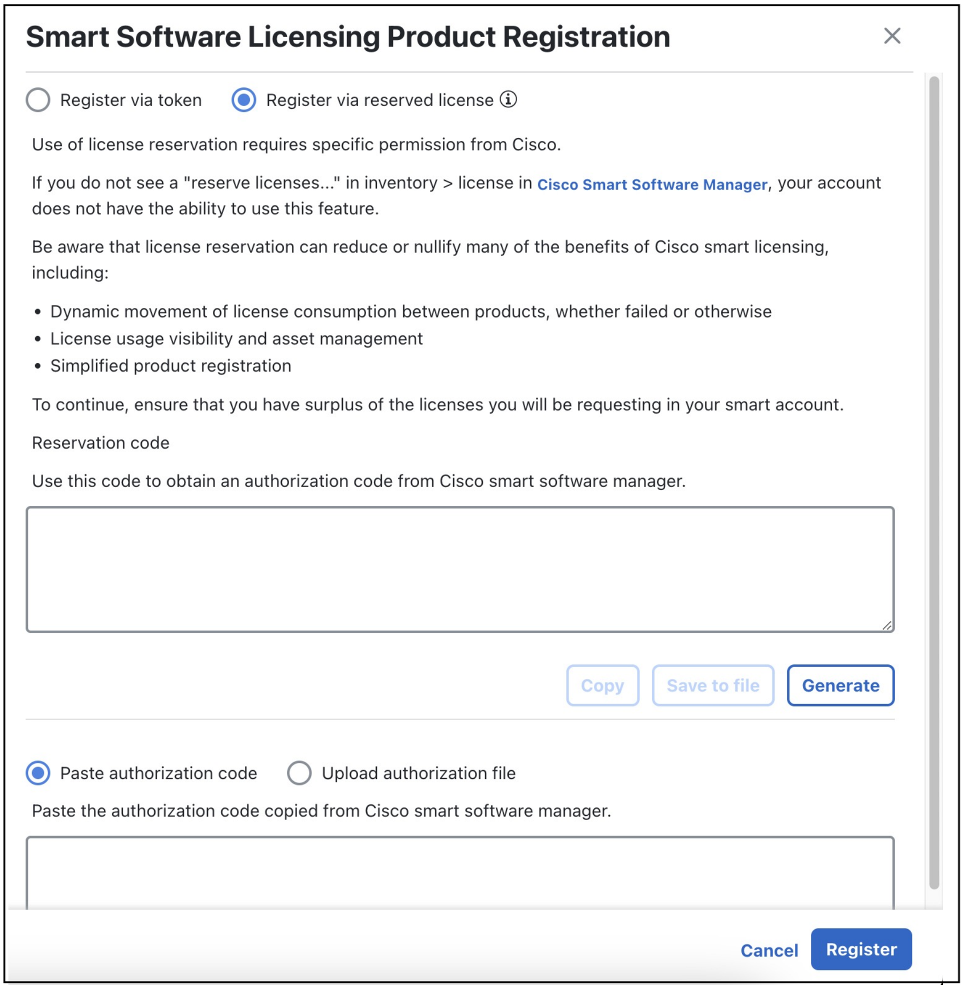
Procedure

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

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

The Smart Software Licensing Product Registration page opens.

Figure 24: Smart software licensing product registration page



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

Step 4 Generate a Reservation Request Code.

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

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

Step 5 Generate the Authorization Code in CSSM.

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

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

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

Step 8 Click **Register**.

It may take a few minutes to process the registration.

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

Update offline reservation

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

Procedure

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

Step 2 Generate the Authorization Code in CSSM.

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

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

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

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

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

Step 6 Enter the Confirmation Code in CSSM.

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

d) Click **OK**.

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

Disable offline reservation

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

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

Procedure

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

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

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

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

Step 4 Enter the Reservation Request Code in CSSM.

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

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

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

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

Update license counts

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

Before you begin

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

Procedure

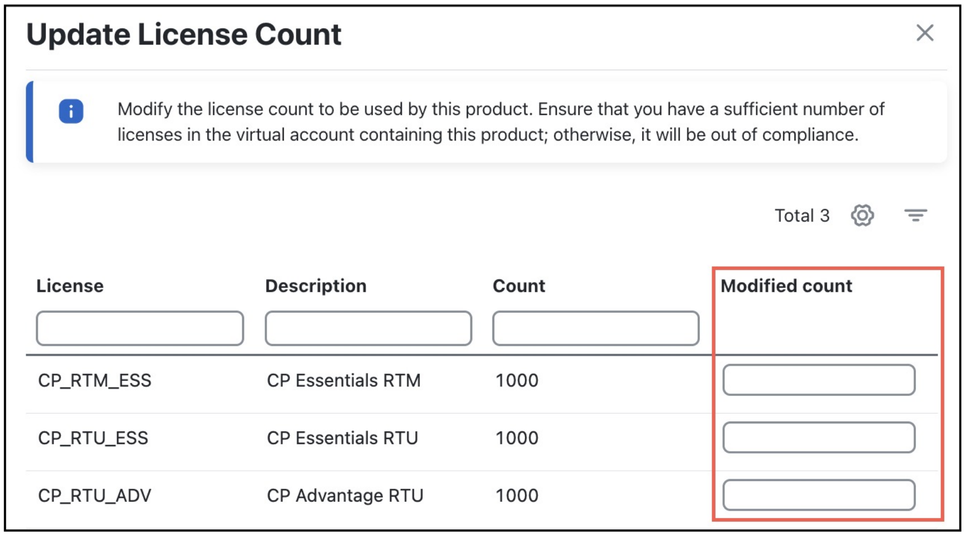
Step 1 From the main menu, choose **Licensing**.

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

The Update License Count page appears.

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

Figure 25: Update license count page



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.

Total 3

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

Step 4 Click **Save**.

The system updates and applies the number of licenses.

License authorization statuses

Based on the system registration status, the application displays several distinct license authorization statuses. This topic describes each possible combination of registration status and license authorization status and explains what each means for application usage.

Table 15: License authorization statuses

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

CHAPTER 5

Manage Administrative Tasks

Certificates

A certificate is an electronic document that

- identifies an individual, a server, a company, or an entity
- associates the entity with a unique key, and
- is digitally signed by an issuer (Certificate Authority or self-signed) to enable secure communication.

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.

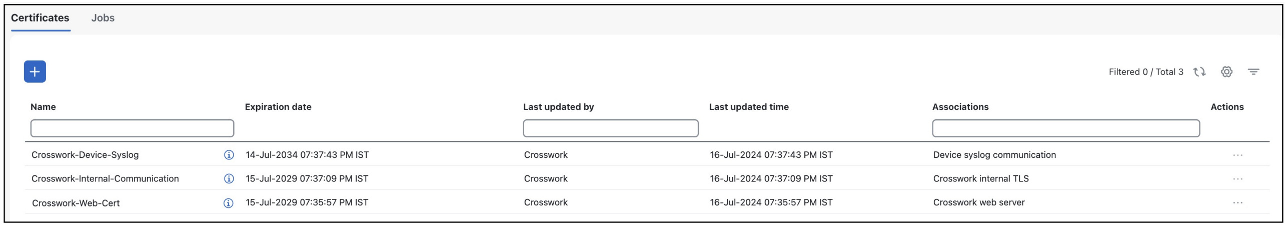
In a TLS exchange, a hierarchy of certificates is used to verify the validity of the certificate's issuer. This hierarchy is called a trust-chain and consists of three types of entities: a root CA certificate (self-signed), possibly multiple levels of intermediate CA certificates, and a server (or client) 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. The root certificate's private key signs and issues the next certificate in the chain. Subsequently, the private key for each certificate in the trust chain signs and issues the following certificate, continuing until the end-entity certificate is signed. The end-entity certificate is the last certificate in the chain. It is used as a client or server certificate.

How are certificates used in Cisco Crosswork Planning

Cisco Crosswork Planning uses the TLS protocol for secure communication between devices and components. TLS uses X.509 certificates to securely authenticate devices and encrypt data to ensure its integrity from source to destination. Cisco Crosswork Planning uses both generated certificates and certificates uploaded by clients. Uploaded certificates can be purchased from Certificate Authorities (CA) or be self-signed. For example, the system's VM-hosted web server and the client browser-based user interface communicate with each other using the system-generated X.509 certificates exchanged over TLS.

The Certificate Management page (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates. Figure 26: Certificate management page, on page 118 displays the default certificates provided by Cisco Crosswork Planning.

Figure 26: Certificate management page



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

Certificates in Cisco Crosswork Planning are classified into various roles with different properties depending on their use case as shown in this 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 that allow you to upload or download trust chains only
- Roles that allow you to upload or download both the trust chain and an intermediate certificate and key

Add a new certificate

This topic describes how to add a new certificate for the **Secure LDAP communication** role.

In this process, you upload the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork, you can add the LDAP server (see Configure LDAP servers, on page 137) 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

- Ensure that the certificate file is in Privacy Enhanced Mail (PEM) format and easily accessible.
- Uploaded Trust chain files 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..
- Ensure the intermediate keys are either in the PKCS1 or PKCS8 format.
- Ensure that the *tyk* service is in a healthy state.

- For information on certificate types and usage, see Certificate types and usage, on page 118.

Procedure

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

Step 2 In the **Certificate name** field, enter a unique name for the certificate.

Step 3 From the **Certificate role** drop-down list, select **Secure LDAP communication**..

Note
Even though UI displays several other options, only **Secure LDAP communication** is applicable for Cisco Crosswork Planning.

Step 4 Click **Browse** and navigate to the certificate trustchain.

Step 5 Click **Save**.

After you upload the certificate, the Crosswork Cert manager accepts, validates, and generates the server certificate. Upon successful validation, an alarm ("Crosswork Web Server Restart") indicates that the certificate will 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 https://<crosswork_ip>:30603 in the URL.

Edit a certificate

This topic describes how to edit a certificate in Cisco Crosswork Planning.

You can edit a certificate to

- add or remove connection destinations
- upload certificates, or
- replace expired or misconfigured certificates.

You can edit only the user-provided certificates and web certificates. You cannot modify the other system certificates provided by Cisco Crosswork, and they will not be available for selection.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- Restart the Crosswork server during this process. The restart will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

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

The Certificate Management page opens.

Step 2 To update a certificate:

a) In the **Actions** column, click ··· on the certificate you want to modify, and select **Update certificate**.

b) Enter the appropriate values in the fields based on the certificate you wish to update. Click the ⓘ icon next to the field for more information.

c) Click **Save** to save the changes.

Step 3 To enable the client certificate authentication of a web certificate:

a) In the **Actions** column, click ··· on the Crosswork web certificate you want to modify, and select **Configure client certificate authentication**.

The **Configure Client Authentication** page opens.

b) Check the **Enable** check box.

The **Certificate schema** and **OCSP** settings appear.

The **OCSP** settings are enabled by default, but you can disable it if required. If enabled, you can check the certificate revocation status using the Online Certificate Status Protocol (OCSP).

c) Select the **Certificate schema** value.

- **Automatic**: Searches for the user principal name (UPN) in the alternate subject name area. If a UPN is not found, the system will use the common name value. This is the default selection.
- **Manual**: Searches for the username in the subject area based on the user identity source and the specified regular expression.

d) (Optional) Select the **OCSP** value:

- Automatic: Extracts the responder URL from the certificate and uses it to perform OCSP validation.
- Manual: You must provide the OCSP responder URL.

e) Click **Save** to save the changes.

Step 4 To update certificate and configure client authentication in a single step:

a) In the **Actions** column, click ··· on the Crosswork web certificate you want to modify, and select **Update certificate & configure client certificate authentication**.

The Update Certificate and Configure Client Authentication page opens.

Note
Choosing the combined option to update the certificate and configure client authentication minimizes downtime during the Crosswork server restart, as it occurs only once instead of twice if these actions are performed separately.

b) Provide the required data according to the instructions in step 2 and step 3.

c) Click **Save** to save the changes.

The selected certificate is updated or reconfigured as specified.

Download a certificate

This topic describes how to download a certificate to your local system.

Procedure

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

The Certificate Management page opens.

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

Step 3 To download the root certificate or the intermediate certificate separately, click ⤓ next to the certificate.

Step 4 To download all the certificates at once, click **Export all**.

The selected certificate is downloaded to your local system.

Update a web certificate using Certificate Signing Request (CSR)

Starting with version 7.0.1, Cisco Crosswork Planning enables updating web certificates via a Certificate Signing Request (CSR) to enhance trust and security. This approach allows you to obtain a certificate signed by an Enterprise or Commercial CA without exposing the private key outside of Cisco Crosswork Planning.

Before you begin

- Updating the certificate may disrupt the existing trust chain of certificates used for client authentication if enabled.
- As part of this process, you need to restart the Crosswork server, which can take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

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

Step 2 Click ··· on the web certificate (Crosswork-Web-Cert) and select **Update certificate**.

Step 3 Create a CSR to submit to the CA.

a) Select **Create a certificate signing request (CSR)** and click **Update certificate**.
b) Click **Create CSR**.

c) Enter relevant values in the fields. Click ⓘ next to the field for more information.

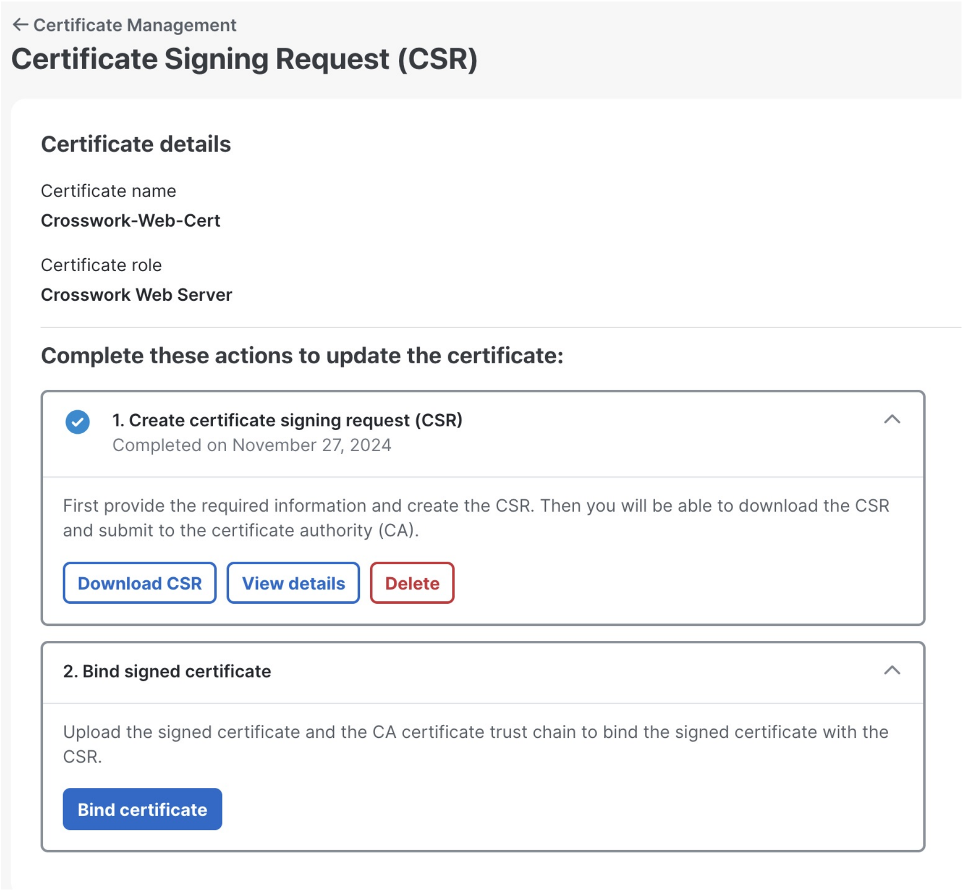
These are the mandatory fields.

- Common name (CN): By default, this is the Fully Qualified Domain Name (FQDN) of the server, but it can be any unique name that identifies the server. The length should not exceed 64 characters.
- IP address: This is the Crosswork VIP address utilized in this deployment. Additional IP addresses should only be added if necessary for certificate validation.
- Key Type: The options are RSA and ECDSA. By default, RSA is selected.
- Key Size (in bits): The options are 2048, 3072, and 4096. By default, 2048 is selected.
- Key Digest: The options are SHA-256, SHA-384, SHA-224, and SHA-512. By default, SHA-256 is selected.

d) Click **Create CSR** to complete the action.

Step 4 After generating the CSR, click **Download** to download it. Then, use the CSR to get a signed certificate from your CA.

Figure 27: Certificate Signing Request (CSR) page



← Certificate Management

Certificate Signing Request (CSR)

Certificate details

Certificate name
Crosswork-Web-Cert

Certificate role
Crosswork Web Server

Complete these actions to update the certificate:

1. Create certificate signing request (CSR)
Completed on November 27, 2024

First provide the required information and create the CSR. Then you will be able to download the CSR and submit to the certificate authority (CA).

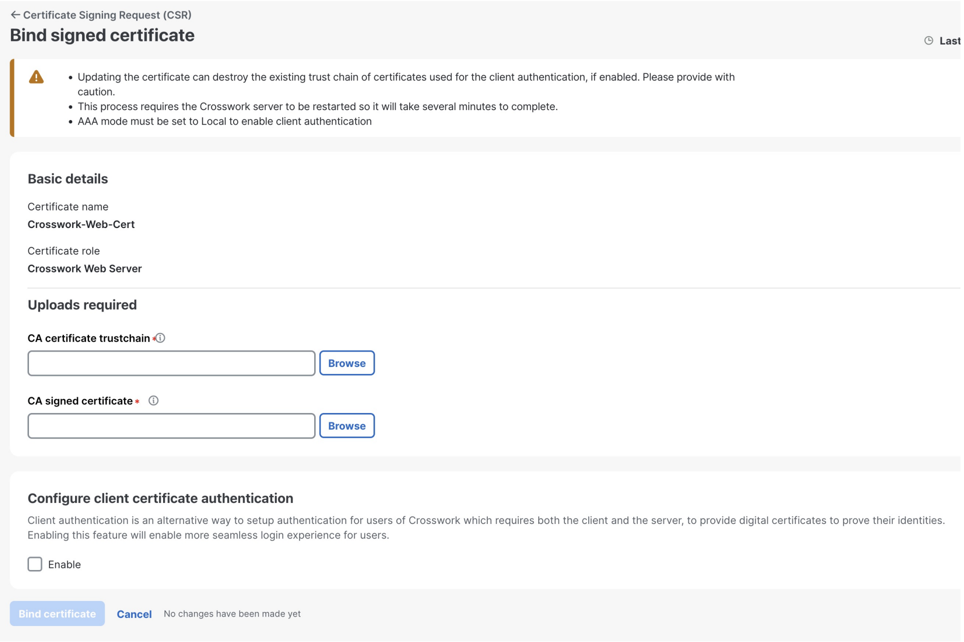
2. Bind signed certificate

Upload the signed certificate and the CA certificate trust chain to bind the signed certificate with the CSR.

Step 5 Upload the CA-signed certificate and the CA certificate trust chain to bind the certificate.

a) In the Certificate Signing Request (CSR) page, click **Bind certificate**.

Figure 28: Bind signed certificate



← Certificate Signing Request (CSR)

Bind signed certificate

- Updating the certificate can destroy the existing trust chain of certificates used for the client authentication, if enabled. Please provide with caution.
- This process requires the Crosswork server to be restarted so it will take several minutes to complete.
- AAA mode must be set to Local to enable client authentication

Basic details

Certificate name
Crosswork-Web-Cert

Certificate role
Crosswork Web Server

Uploads required

CA certificate trustchain *

CA signed certificate *

Configure client certificate authentication

Client authentication is an alternative way to setup authentication for users of Crosswork which requires both the client and the server, to provide digital certificates to prove their identities. Enabling this feature will enable more seamless login experience for users.

□ Enable

No changes have been made yet

b) Upload the relevant data in the fields provided. Click ⓘ next to the field for more information.

- CA certificate trust chain: This is the certificate trust chain for the web server certificate obtained from the CA.
- CA signed certificate: This is the final signed certificate for the web server obtained from the CA.

c) (Optional) Check the **Enable** check box to configure client certificate authentication.

d) Click **Bind certificate** to complete the operation.

After the bind action is completed, the web certificate is updated. Tyk will then restart with the new web certificate.

The Cisco Crosswork Planning's web certificate is updated with the CA-signed certificate and trust chain after server restart.

Manage users

As a best practice, administrators should create separate accounts for all users. During the creation of a user account, you assign a user role to determine which functionality the user can access. If you are using user roles other than "admin", create the user roles before you add your users (see Create a user role, on page 127).

Before you begin

Prepare a list of people who will use Cisco Crosswork Planning. Decide on their usernames and preliminary passwords.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Users** tab. From this page, you can add a new user, edit the settings for an existing user, or 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) Select the check box next to the user name and click ✎.
b) After making changes, click **Save**.

Step 4 To delete a user:

a) Select the check box next to the user name and click 🗑.
b) In the confirmation dialog box, click **Delete**.

Step 5 To view the audit log for a user:

a) Click ··· under the **Actions** column, and select **Audit log**.

The **Audit Log** page appears for the selected user name. For more information, see View the audit log, on page 160.

User accounts are created, updated, or deleted as required.

Administrative users created during installation

During installation, Cisco Crosswork Planning creates two special administrative user IDs:

- 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.
- The **Cisco Crosswork administrator**, with the username **`admin`** and the default password **`admin`**. Product administrators use this ID to log in to the UI, configure the UI, and perform special operations, such as creating new user IDs.

You must change the default password for both administrative user IDs the first time you use them.

User roles, functional categories, and permissions

In Cisco Crosswork Planning, each user account is assigned a user role. This user role controls what the user can do when using the platform and its applications. A user role defines access by combining named functional categories and permissions assigned to each category.

User roles

The **Roles** page 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 a user with that role has access to the APIs needed to perform specific Cisco Crosswork functions controlled by that API, and
- 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, you must select both the category and its underlying API on the **Roles** page for that role. If a functional category is not selected for a user role, users assigned to that role will not have access to that functional area.

Functional categories

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 and provide access to others by selecting them. For example, to create an “Operator” role with permission to change their own password, but not to view or change the settings for your installation’s integration with remote AAA servers, or to create new users and roles, select the “AAA” category name. Then, uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” check boxes.

Permissions

For each role with a selected category, you can define permissions to each underlying functional API on the **Roles** page.

There are three permission types available per API.

- Read: lets the user view and interact with the objects controlled by that API, but not change or delete them.
- Write: lets the user view and change the objects controlled by that API, but not delete them.
- Delete: lets the user role delete privileges over the objects controlled by that API. Note that the delete permission does not override basic limitations set by the Cisco Crosswork platform and its applications.

Rules for permissions

Although you can mix permissions as you wish, note these rules for permissions.

- 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 you want the user to have all permissions on that API and selects all three permissions automatically.
- If you uncheck all the permissions, including “Read”, Cisco Crosswork assumes that you want to deny access to the API, and unselect it for you.

Recommendations

Cisco recommends these best practices when creating custom user roles.

- Restrict "Delete" permissions to admin users who have explicit administrative responsibility for maintaining and managing the Cisco Crosswork deployment as a whole.
- Roles for developers working with all Cisco Crosswork APIs need the same permissions as admin users.
- Assign at least "Read" and "Write" permissions to roles for users who are actively engaged in managing the network using Cisco Crosswork.
- Assign read-only access to roles for users who only need to see the data to support their work as system architects or planners.

This table describes some sample custom user roles you should consider creating.

Table 16: 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 must include permissions for Read, Write, and Delete. Read-write roles need to include both Read and Write permissions.

Create a user role

This topic describes how to create new user roles.

The local "admin" role enables access to all functionality. The system creates this role during installation and you cannot change or delete it. However, you can assign its privileges to new local users. Local users with administrator privileges can create new users as needed (see Manage users, on page 124). New users created this way can perform only the tasks associated with their assigned user role.

Only local users can create or update user roles. External users authenticated by TACACS, RADIUS, or LDAP cannot modify user roles.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles**.

The Roles page has a **Roles** pane on the left side and a corresponding **Global API permissions** tab on the right side. This tab shows the grouping of user permissions for the selected role.

Step 2 In the **Roles** pane, click + to display a new role entry.

Step 3 Enter a unique name for the new role.

Step 4 To define the user role's privilege settings, click the **Global API permissions** tab and follow these steps:

a) Select the check box for every API that users with this role can access.

The APIs are grouped logically based on their corresponding application.

b) For each API, define whether the role has **Read**, **Write**, or **Delete** permission by checking the appropriate check boxes. You can also select an entire API group, such as AAA. All the APIs under the group will be selected with **Read**,**Write**, and **Delete** permissions preselected.

Step 5 Click **Save** to create the new role.

The new user role is now available in the Roles list and can be assigned to user IDs.

What to do next

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (see Edit a user role, on page 129).

Clone a user role

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. You can

- clone an existing role multiple times
- let the cloned user role inherit all the privileges of the original user role
- assign a name that indicates the role you want a group of users to perform, and
- edit user IDs of the group of users to assign their new role (see Manage users, on page 124). Later, edit the roles themselves to give users specific privileges (see Edit a user role, on page 129).

Note Some API permissions are predefined in the system admin role and remain unchanged in the cloned role. For example, the system admin role includes the default **Read** and **Write** permissions for the **Alarms & Events** API. These permissions are not configurable for either the original or cloned admin roles.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles**.

Step 2 Click an existing role.

Step 3 Click ⧉ to create a new duplicate entry in the **Roles** pane 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) Select 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 boxes. You can also select an entire API group, such as AAA. All APIs under the group will be selected with **Read**, **Write**, and **Delete** permissions preselected.

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

The newly cloned role is now available in the Roles pane.

Edit a user role

This topic describes how to change the permissions associated with a user role.

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

Before you begin

Confirm you have administrator privileges.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles**.

Step 2 Select an existing role from the left side. The **Global API Permissions** page on the right side displays the permission settings for the selected role.

Step 3 Define the role's settings:

a) Select the check box for every API that users with this role can access.

b) For each API, define whether the role has **Read**, **Write**, or **Delete** permission by checking the appropriate check boxes. You can also select an entire API group, such as AAA. All the APIs under the group will be selected with **Read**, **Write**, and **Delete** permissions preselected.

Step 4 Click **Save** to save the changes.

The selected user role is updated with the new permissions.

Delete a user role

This topic describes how to delete a user role that is no longer needed.

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. To delete a role that is currently assigned to any users, you must first reassign those users to a different user role.

Before you begin

Confirm you have administrator privileges.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles**.

Step 2 Select the user role you want to delete.

Step 3 Click 🗑.

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

The selected user role is deleted and is no longer available for assignment.

Global API permissions

This table describes the various global API permissions in Cisco Crosswork Planning.

Table 17: Global API permission categories

Category	Global API permissions	Description
AAA	Password Change	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	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	Provides permission to manage users, roles, sessions, and password policies. Supported operations include • creating a new user or role • updating a user or role • deleting a user or role • updating task details for a user or role • managing sessions (idle-timeout, max session) • updating password policy • retrieving password tooltip help text • retrieving 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.
	Know my role - Read only	Enables the logged in users to view their permissions or get new permissions. Write and Delete permissions are not applicable for these APIs.
	User Preferences	Allows you to manage the dashlets in the homepage. The Read permission allows you to view dashboards, the Write permission allows you to edit dashboards, and the Delete permission allows you to delete dashboards.
Administrative Operations	Diagnostic Information	

Category	Global API permissions	Description
Alarms and Events	Alarms and Events	Allows you to manage system alarms. **Note** The alarms and events associated with the Cisco Crosswork Planning applications are not supported.
Crosswork Planning		
Platform	Platform APIs	The Read permission allows you to fetch the server status, 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 or 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, and • 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.
	Views	Manages views in Cisco Crosswork Planning Design. The Read permission allows you to see views, the Write permission allows you to create or update views, and the Delete permission will enable delete capabilities.

Manage active sessions

This topic describes how to monitor and end sessions of the currently logged-in users.

As an administrator, you can

- monitor and manage active sessions in the Cisco Crosswork Planning UI
- terminate a user session, and
- view the 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 cannot view the Active sessions page.

Before you begin

Confirm you have administrator privileges.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Active sessions** tab.

The Active sessions tab displays all currently active sessions 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 log in again 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:

a) In the **Actions** column, click ··· and select **Terminate**.
b) Click **Terminate** in the confirmation dialog box.

Attention

- We recommend 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 this message:

```
"Your session has ended. Log into the system again to continue."
```

Step 3 To view the audit log for a user, in the **Actions** column, click ··· and select **Audit log**.

The Audit Log page appears for the selected user. For more information on Audit Logs, see View the audit log, on page 160.

Setting up user authentication through external servers

Summary

In addition to supporting local users, Cisco Crosswork Planning supports external authentication through integration with the TACACS+, LDAP, and RADIUS servers.

The key components involved in the process are:

- TACACS+, LDAP, and RADIUS servers: External servers that provide user authentication.
- User roles: Access privileges assigned to users authenticated via TACACS+, LDAP, or RADIUS.
- Single Sign-on (SSO): An authentication method that allows logging in with a single ID and password to multiple related but independent software systems.

Workflow

These are the stages of setting up user authentication through external servers.

1. Configure the TACACS+, LDAP, and RADIUS servers.
2. Create the roles that are referenced by the TACACS+, LDAP, and RADIUS users.
3. Configure AAA settings.
4. Enable SSO for authentication of TACACS+, LDAP, and RADIUS users. For more information, see Enable SSO authentication, on page 145.

Caution: Authentication changes interrupt all new logins

Any operations performed according to the instructions in subsequent sections on external authentication servers affect all new logins to the Crosswork UI. To minimize session interruption, perform and submit all your external server authentication changes in a single session.

Note: Permissions for the AAA server page

- The AAA server page operates in bulk update mode, updating all the servers are updated in a single request. Grant write permission for "Remote Authentication Servers Integration API" only to users authorized to delete servers.
- A user with only Read and Write permissions (without "Delete" permission) can still delete the AAA server details from Cisco Crosswork because delete operations are part of "Write" permissions. For more information, see Create a user role, on page 127.
- While adding, editing, or deleting AAA servers, wait a few minutes between changes. Making frequent AAA changes without adequate intervals may cause external login failures.

Configure TACACS+ servers

This topic describes how to add, update, or remove TACACS+ authentication servers to control user and device authentication in Cisco Crosswork Planning.

Cisco Crosswork Planning supports authentication of users via TACACS+ servers. You can integrate Crosswork with a standalone server (such as Open TACACS+) or with an application like Cisco ISE (Identity Services Engine). Integrating with TACACS+ servers helps centralize and control access to network resources.

Before you begin

In the TACACS+ server (standalone or Cisco ISE), configure relevant parameters such as user role, device access group attribute, shared secret format, shared secret value before adding the server to Cisco Crosswork

Planning. For more information on Cisco ISE procedures, see the latest Cisco Identity Services Engine Administrator Guide.

Procedure

Step 1 From the main menu, choose **Administration AAA Servers TACACS+** .

Step 2 To add a TACACS+ server:

a) Click ➕.
b) Enter the required TACACS+ server details. For a description of the fields, see TACACS+ server configuration options, on page 135.
c) Click **Add**.
d) Click **Save**.
   A warning message prompts you to restart the server to update the changes. Click **Save changes** to confirm.

Step 3 To edit a TACACS+ server:

a) Select the TACACS+ server and click ✎.
b) After making the desired changes, click **Update**.

Step 4 To delete a TACACS+ server:

a) Select the TACACS+ server and click 🗑.

   The Delete *server-IP-address* dialog box opens.

b) Click **Delete** to confirm.

The TACACS+ server settings are saved and authentication via TACACS+ is enabled.

TACACS+ server configuration options

This section describes TACACS+ server configuration fields.

Table 18: Field descriptions

Field	Description
Authentication order	Specify a unique priority value to set precedence in the authentication request. The order can be any number from 10 to 99. Numbers 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 names are supported.
Port	The default TACACS+ port number is 49.
Shared secret format	Shared secret for the active TACACS+ server. Select ASCII or Hexadecimal.

Field	Description
Shared secret and Confirm shared secret	Enter the plain text shared secret for the active TACACS+ server. The format of the text you enter must match the selected format (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, ensure the **Shared Secret** parameter you enter on this page matches the shared secret value configured on the TACACS+ server.
Service	Enter the value of the service 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, follow these steps. **1.** Close the browser. **2.** Log in as a local admin user and create the missing user roles in the TACACS+ server. **3.** Log back in to Cisco Crosswork Planning using the TACACS+ user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the (ISE/Standalone) TACACS+ server attributes. These values can be one or more comma-separated entries. In the TACACS+ context, the Device Access Group attribute is typically a custom or authorization attribute that the TACACS+ server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.
Retransmit timeout	Enter the timeout value. The maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for TACACS+: • PAP: Password Authentication Protocol, a protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol, which requires both the client and server to know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than PAP.

Configure LDAP servers

This topic describes how to configure the LDAP server settings in Cisco Crosswork Planning to enable user authentication via LDAP servers.

LDAP servers, including OpenLDAP, Active Directory, and secure LDAP, are used to authenticate users for network management. Cisco Crosswork Planning can use these servers to centralize directory management and enforce access policies. Secure LDAP requires a certificate to enable encrypted communication.

Before you begin

- Configure relevant parameters, such as Bind DN, Policy baseDN, Policy ID, and so on in the LDAP server.
- For secure LDAP, you must add a "Secure LDAP Communication "certificate before adding the LDAP server. For more details on adding certificates, see Add a new certificate, on page 119.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **Servers** > **LDAP**.

Step 2 To add an LDAP server:

a) Click +.
b) Enter the required LDAP server details. For a description of the fields, see LDAP server configuration options, on page 137.
c) Click **Add**.
d) Click **Save**.
A warning message prompts you to restart the server to update the changes. Click **Save changes** to confirm.

Step 3 To edit an LDAP server:

a) Select the LDAP server and click ✎.
b) After making the desired changes, click **Update**.

Step 4 To delete an LDAP server:

a) Select the LDAP server and click 🗑.
b) Click **Delete** to confirm.

The LDAP server settings are saved and authentication via LDAP is enabled.

LDAP server configuration options

This section describes LDAP server configuration fields.

Table 19: Field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number from 10 to 99. Values below 10 are reserved for system use. By default, 10 is selected.
Name	Enter the name of the LDAP handler.
IP address/Host name	Enter the LDAP server IP address or host name.
Secure connection	Enable this 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** You must add the secure LDAP certificate in the Certificate Management screen before configuring the secure LDAP server. This field is disabled by default.
Port	The default LDAP port number is 389. If Secure Connection SSL is enabled, the default LDAP port number is 636.
Bind DN	Enter the database login access details. Bind DN allows users to log in to the LDAP server.
Bind credential and Confirm bind credential	Enter the 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	This filter is used for searching users.
DN format	Enter the format used to identify the user in base DN.
Principal attribute ID	This value represents the UID attribute in the LDAP server user profile under which a particular username is organized.
Policy baseDN	This value represents the role mapping for user roles within your directory.
Policy map attribute	This identifies the user under the policy base DN. This value maps to the `userFilter` parameter in your LDAP server attributes.

Field	Description
Policy ID	Specify the user role you created in the LDAP server. The **Policy ID** is a unique key that the LDAP server uses to identify and retrieve the user role assigned to an authenticated user. This value must match the user role configured on the LDAP server. In Cisco Crosswork Planning, this field corresponds to the *policy_id*. **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.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the LDAP server attributes. These values can be one or more comma-separated entries. In the LDAP context, the Device Access Group attribute is typically a custom or authorization attribute that the LDAP server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.
Connection timeout	Enter the timeout value. The maximum timeout is 30 seconds.

Example

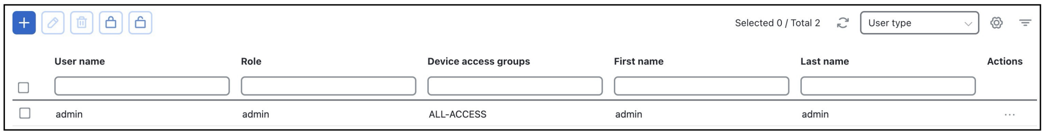
This example shows the parameters that are entered for secure LDAP configuration in Cisco Crosswork Planning. The relevant parameters are configured in the LDAP server.

These are some of the key points:

User settings in the Cisco Crosswork Planning UI

In this example, the existing default user role **admin** is used. You can find this setting on the **Administration** > **Users and Roles** > **Users** page.

- The user name, user role, first name, and last name are set to `admin`.
- The device access group is configured in the LDAP server as `description='ALL-ACCESS'`.



	User name	Role	Device access groups	First name	Last name	Actions
□						
□	admin	admin	ALL-ACCESS	admin	admin	···

LDAP server details

This section describes the user's LDAP server configuration details.

1. System base DN: ou=system
2. The admin user ‘admin’ has these attributes:
    a. DN: uid=admin,ou=system
    b. password: secret
3. Users group with DN: ou=users,ou=system
4. The admin user John belongs to the ‘users’ group and has these attributes:
    a. DN: uid=john,ou=users,ou=system
    b. password: john
    c. mail: John@test.com
    d. display name: John
    e. description: ALL-ACCESS

Important The description must be equal to the **Device access groups** value for the 'admin' user in Cisco Crosswork Planning (see User settings in the Cisco Crosswork Planning UI, on page 139).

5. The group ‘CpAdmins’ has these attributes:
    a. DN: cn=CpAdmins,ou=groups,ou=system
    b. uniqueMember=uid=john,ou=users,ou=system

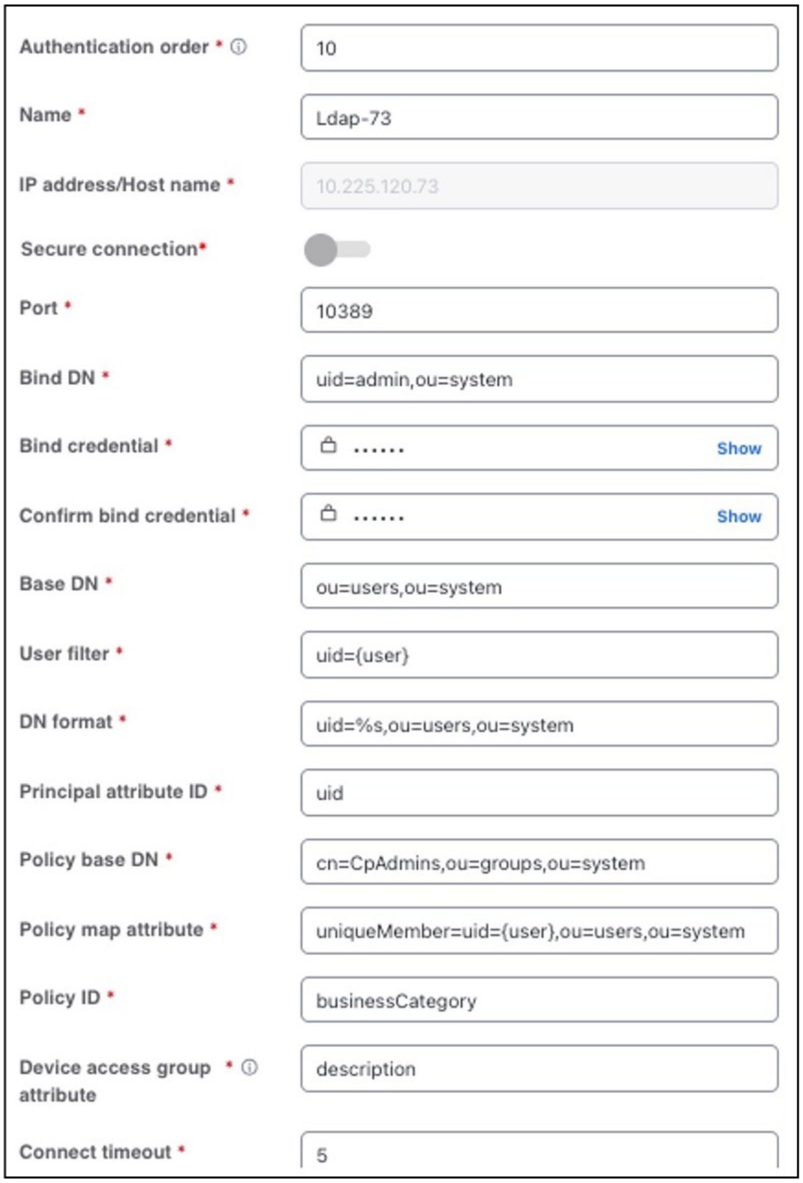
        This indicates the user’s group membership. This value must match with admin user’s DN (see Section 4(a)).
    c. businessCategory: admin

        This indicates the role that needs to be assigned to all users belonging to this group. This value must match with the **Role** value for the admin user in Cisco Crosswork Planning (see User settings in the Cisco Crosswork Planning UI, on page 139).

Corresponding LDAP configuration in the UI

This section describes the corresponding LDAP configuration in the Cisco Crosswork Planning UI.

Figure 29: LDAP configuration in the Cisco Crosswork Planning UI



Authentication order * ⓘ	10
Name *	Ldap-73
IP address/Host name *	10.225.120.73
Secure connection*	
Port *	10389
Bind DN *	uid=admin,ou=system
Bind credential *	•••••• Show
Confirm bind credential *	•••••• Show
Base DN *	ou=users,ou=system
User filter *	uid={user}
DN format *	uid=%s,ou=users,ou=system
Principal attribute ID *	uid
Policy base DN *	cn=CpAdmins,ou=groups,ou=system
Policy map attribute *	uniqueMember=uid={user},ou=users,ou=system
Policy ID *	businessCategory
Device access group attribute * ⓘ	description
Connect timeout *	5

Parameter	Value
Authentication order	10 (default)
Name	Ldap-73 Custom name for the LDAP configuration of a server.
IP Address/Host name	10.225.120.73 LDAP server IP address.

Parameter	Value
Port	10389 LDAP server port.
Bind DN	uid=admin,ou=system Admin user DN, as described in Section 2(a).
Bind credential	secret Admin user password, as described in Section 2(b).
Confirm bind credential	secret Admin user password, as described in Section 2(b).
Base DN	ou=users,ou=system The user's group DN for *authentication* from where the users must be searched, as described in Section 3.
User filter	uid={user} User search filter attribute 'uid', as described in Section 4.
DN format	uid=%s,ou=users,ou=system User's DN format, as described in Section 4.
Principal attribute ID	uid As described in Section 4.
Policy base DN	cn=CpAdmins,ou=groups,ou=system The group that has the role mapping attribute (admin) and under which the users will have group membership, as described in Section 5(a).
Policy map attribute	uniqueMember=uid={user},ou=users,ou=system The user's group membership attribute under the 'CpAdmins' user group (Policy base DN), as described in Section 5(b).
Policy ID	businessCategory The user role attribute (admin) under the 'CpAdmins' group (Policy base DN), as described in Section 5(c). This value must match with the CpAdmins group's attribute having 'admin' value.
Device access group attribute	description The device group attribute under the user DN, as described in Section 4(e). This value must match with the user DN attribute having value 'ALL-ACCESS'.

Configure RADIUS servers

This topic describes how to configure the RADIUS server settings in Cisco Crosswork Planning to enable user authentication via RADIUS servers.

Crosswork supports the use of RADIUS 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

In the RADIUS server (standalone or Cisco ISE), configure relevant parameters, such as user role, device access group attribute, shared secret format, shared secret value in the RADIUS server before adding the server to Cisco Crosswork Planning. For more information on Cisco ISE procedures, see the latest Cisco Identity Services Engine Administrator Guide.

Procedure

Step 1 From the main menu, choose **Administration AAA Servers RADIUS** .

Step 2 To add a RADIUS server:

a) Click +.
b) Enter the required RADIUS server details. For a description of the fields, see RADIUS server configuration options, on page 143.
c) Click **Add**.
d) Click **Save**.
A warning message prompts you to restart the server to update the changes. Click **Save changes** to confirm.

Step 3 To edit a RADIUS server:

a) Select the RADIUS server and click ✎.
b) After making the desired changes, click **Update**.

Step 4 To delete a RADIUS server:

a) Select the RADIUS server and click 🗑.

The Delete *server-IP-address* dialog box opens.

b) Click **Delete** to confirm.

The RADIUS server settings are saved and authentication via RADIUS is enabled.

RADIUS server configuration options

This section describes RADIUS server configuration fields.

Table 20: Field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number from 10 to 99. Numbers below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the RADIUS server (if IP address is selected).
DNS name	Enter the DNS name (if DNS name is selected). Only IPv4 DNS names are supported.
Port	The default RADIUS port number is 1645.
Shared secret format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.
Shared secret and Confirm shared secret	Enter the plain text shared secret for the active RADIUS server. The format of the text you enter must match the selected format (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, ensure the **Shared Secret** you enter on this page matches the shared secret value configured on the RADIUS server.
Service	Enter the value of the service you are attempting to gain access to. For example, "raccess".
Policy ID	Enter the user role that you created in the RADIUS server. **Note** If you try to log in 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, follow these steps. **1.** Close the browser. **2.** Log in as a local admin user and create the missing user roles in the RADIUS server. **3.** Log back in to Cisco Crosswork Planning using the RADIUS user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the RADIUS server attributes. These values can be one or more comma-separated entries. In the RADIUS context, the Device Access Group attribute is typically a custom or authorization attribute that the RADIUS server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.

Field	Description
Retransmit timeout	Enter the timeout value. The maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for RADIUS: • PAP: Password Authentication Protocol, a protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol, which requires both the client and server to know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than PAP.

Single Sign-on (SSO)

Single Sign-on (SSO) is an authentication method that

- enables you to log in with a single ID and password to any of several related, yet independent, software systems.
- allows you to log in once and access the services without reentering authentication factors.
- allows Cisco Crosswork to act 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.

Enable SSO authentication

This topic describes how to enable SSO in Cisco Crosswork Planning so you can access the integrated service provider applications using a single set of credentials, streamlining authentication and simplifying navigation between service providers.

Single sign-on (SSO) is an authentication method that lets users log in once and access multiple independent systems without reentering credentials. Cisco Crosswork Planning acts as an Identity Provider (IdP) and supports SSO integration for service provider applications. You can enable SSO for users authenticated via TACACS+, LDAP, and RADIUS. When SSO is configured, users benefit from seamless access and improved security management.

⚠ **Attention**

- When Cisco Crosswork Planning's CAS pod is restarting or not running, the login page is not available.
- The SSO URL from the Identity Provider (IdP) is *https://<IP>:30603/crosswork/sso/idp/profile/SAML2/Redirect/SSO*, where <IP> represents the Cisco Crosswork Planning's IP address or hostname.

Before you begin

- Check the **Enable source IP for auditing** check box on the **Administration** > **AAA** > **Settings** page.
- Ensure you have the latest service provider metadata to integrate with Cisco Crosswork Planning SSO.
- Confirm that network connectivity exists between Cisco Crosswork Planning (IdP) and each service provider application.
- Verify the CAS pod is running and stable.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **SSO**.

The Identity Provider page opens. On this page, you can add service providers, edit their settings, or delete them.

Step 2 To add a new service provider:

a) Click ⊞.
b) On the Service Provider page, enter the values in these fields:

- Name: Enter the name of the service provider entity.

  Note
  If you provide a URL, the **Service name** entry in the Identity Provider page becomes a hyperlink.

- Evaluation order: Enter a unique number indicating 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.

c) Click **Add** to finish adding the service provider.

Step 3 Click **Save all changes**. When prompted, confirm by clicking **Save changes**.

After you save the settings and log in to the integrated service provider application for the first time, the application redirects 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 4 To edit a service provider:

a) Select the service provider and click ✎.
b) Update the Evaluation order or Metadata as required.
c) Click **Update** to apply the changes.

Step 5 To delete a service provider:

a) Select the check box next to the service provider and click 🗑.
b) Click **Delete** to confirm.

Single sign-on is enabled for selected service provider applications. Users can authenticate once via Cisco Crosswork Planning and seamlessly access associated applications without reentering authentication factors.

What to do next

- If Cisco Crosswork Planning is reinstalled or migrated, update the Identity Provider (IdP) metadata in all service provider applications to avoid authentication errors due to metadata mismatch.
- For first-time users, ensure password change is completed before attempting to log in with a different username. To reset an incomplete session, an administrator must terminate it.

Warning: SSO configuration and login requirements

- When Crosswork is re-installed or migrated, update the latest IDP metadata from Crosswork to the service provider applications. Otherwise, authentication will fail due to mismatched metadata information.
- Users logging in for the first time must change their password before switching to a different username. The only workaround is for the administrator to terminate the session.
- The Cisco Crosswork Planning login page is not rendered when the Central Authentication Service (CAS) pod is restarting or not running.

Configure AAA settings

This topic describes how to control user authentication, authorization, and accounting on the system by configuring AAA settings to enforce security policies and manage user sessions.

Users with relevant AAA permissions can configure the AAA settings. Configure these settings when you need to establish or update how users are authenticated, what resources they can access, and how their activities are tracked. Proper AAA settings help safeguard network resources and ensure compliance with organizational access policies.

Before you begin

- Ensure you have the relevant AAA permissions to configure the AAA settings.
- Review your organization's authentication and password policy requirements.
- Gather information about external authentication servers (if applicable).
- Gather information about external authentication servers (if applicable).

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 Under **Browser session timeout**, select the relevant value for the **Log out inactive users after** field. Any user who remains idle beyond the specified limit will be automatically logged out.

This timeout is enforced by the system and applies even if the user closes the browser tab without explicitly logging out. If no activity (token usage) is detected after the tab is closed, the session expires after the configured timeout. For example, with a 10-minute timeout, if a user closes the browser tab after five minutes of activity, the user must log in again if they return after 10 minutes.

Note

- The default timeout value is 30 minutes.
- Changes to the timeout value take effect immediately, including for active sessions.
- Session termination can take upto a minute more than the configured timeout due to backend scheduling.
- This setting applies only to browser-based UI sessions. API-based sessions continue to follow the existing 8-hour validity behavior.

Step 4 Under **Parallel session**, enter relevant values for the **Number of parallel sessions** and **Number of parallel sessions per user** fields.

Note

- The system supports between 5 and 400 parallel sessions for concurrent users. If the number of parallel sessions is exceeded, an error is displayed during login to Cisco Crosswork Planning.
- Cisco Crosswork Planning supports 50 simultaneous NBI sessions up to 400 sessions..

Step 5 Under **Source IP**, enable auditing of user source IP addresses.

a) 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.

b) Log out, wait a few minutes, then log back in. This pause ensures the change is applied and the actual client IP address is accurately captured.

During this transition, audit logs may temporarily display the Cisco Crosswork Planning node IP instead of the client IP. The correct client IP will appear in new audit log entries created after you log in again. Previous log entries will continue to show the node IP. Once enabled and you have logged in again, the **Source IP** column will appear on both 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

- 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.
- Any changes to the password policy are enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

System and application health monitoring

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 its applications are considered

- **Healthy** if all services are up and running.
- **Degraded** if one or more services are down.
- **Down** if all services are down.

The **Crosswork summary** and **Crosswork health** pages provide various views to monitor system and application health. These pages also supply tools and information that, with support and guidance from the Cisco Customer Experience team, help you identify, diagnose, and fix issues with the Cisco Crosswork, Platform Infrastructure, and installed applications. While both pages can give you access to the same type of information, the purpose of each summary and view is different.

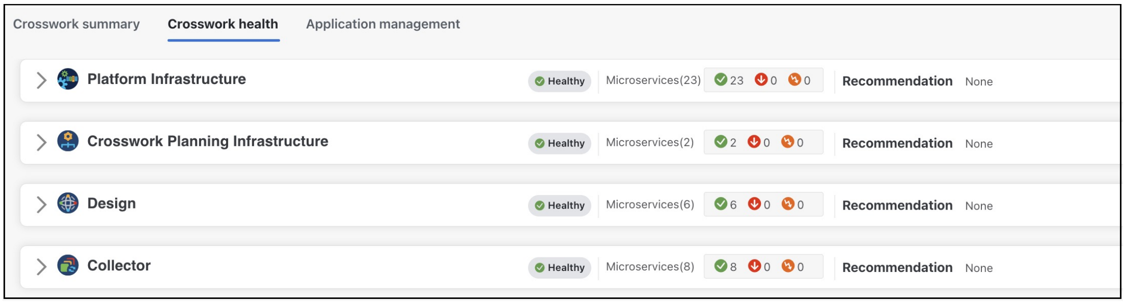
Check platform infrastructure and application health

This topic describes how to view health summaries for Cisco Crosswork Platform Infrastructure and installed applications, including microservice and alarm details.

Procedure

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

Figure 30: Crosswork health tab



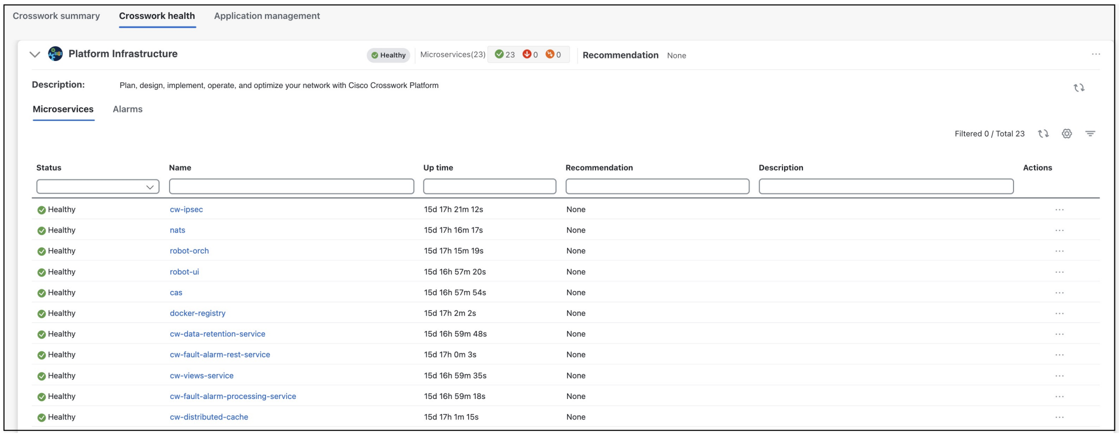
Crosswork summary | Crosswork health | Application management

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

Step 2 Expand an application row to view microservice and alarm information.

Step 3 Click the **Microservices** tab to view the list of microservices.

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		···

- To view associated microservices, click the microservice name.
- To restart or obtain Showtech data and logs per microservice, click ··· .

Note
You must collect the Showtech logs separately for each application.

Step 4 Click the **Alarms** tab to view the alarm details.

From this tab, you can

- filter the list of active alarms
- click the alarm description to view detailed information about the alarm
- change the status of the alarms (Acknowledge, Unacknowledge, Clear)
- add notes to alarms
- view list of events in the product, or
- view the correlated alarm for each event.

Check system health example

In this example, we explain which pages to navigate through and which areas to check to ensure a healthy Crosswork system.

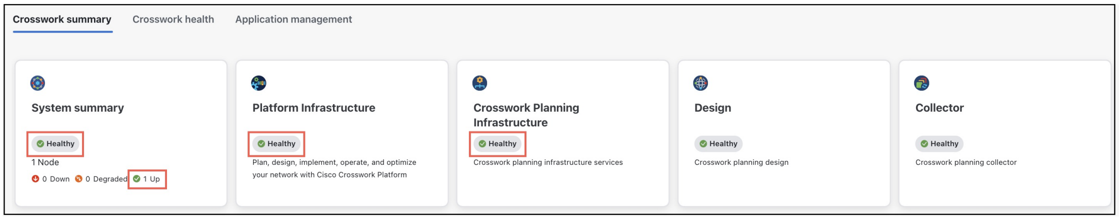
Procedure

Step 1 Check the 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 tab



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

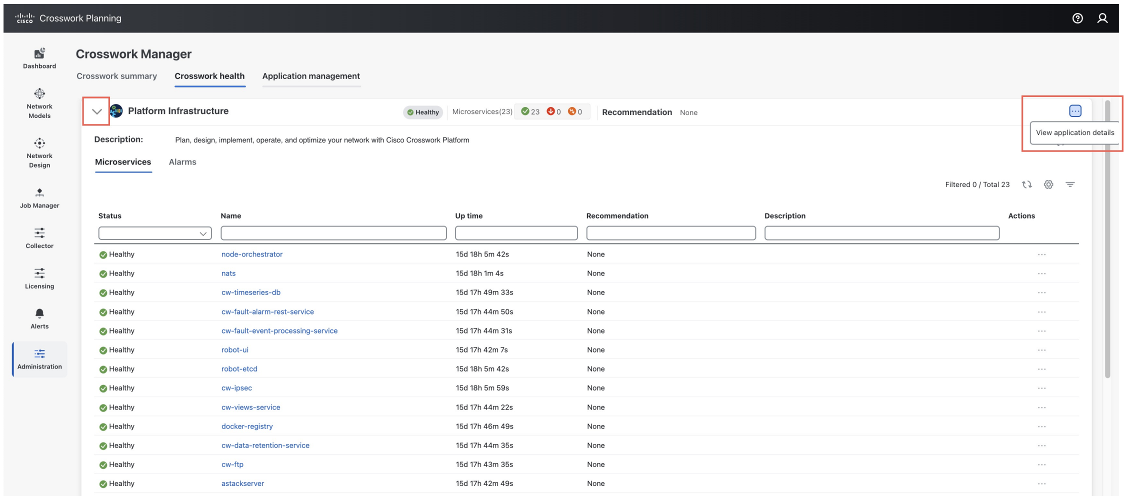
Collector
Healthy
Crosswork planning collector

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 tab



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

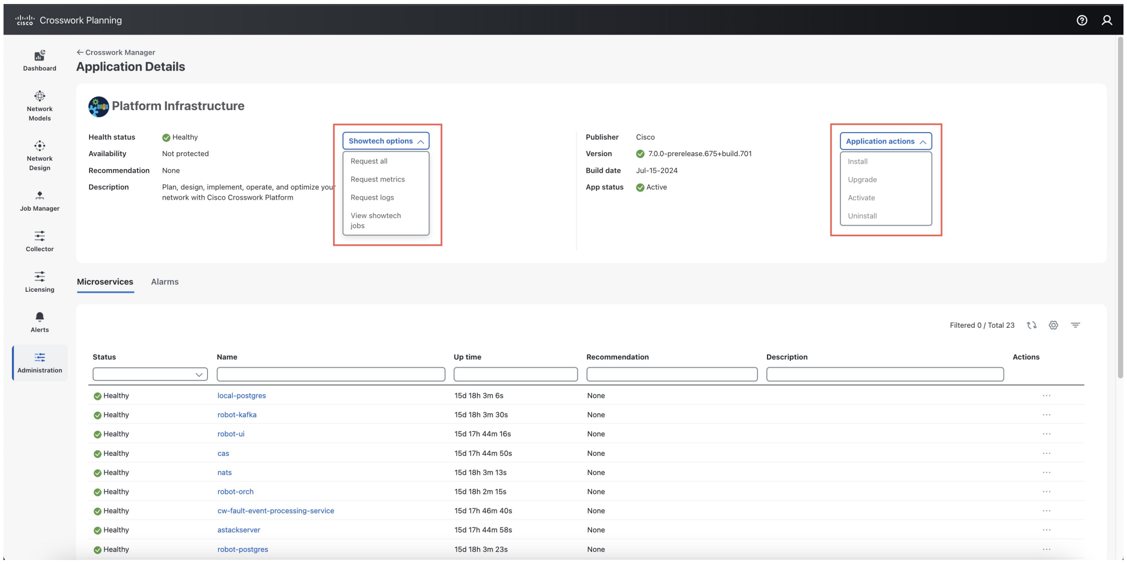
Filtered 0 / Total 23

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		···

The Application Details page opens.

c) From the **Showtech options** drop-down list, you can check microservice details, restart microservices, and collect showtech information. You can also perform installation-related tasks from the **Application actions** drop-down list.

Figure 34: Application Details page



Application Details

Platform Infrastructure

Health status	Healthy
Availability	Not protected
Recommendation	None
Description	Plan, design, implement, operate, and optimize your 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

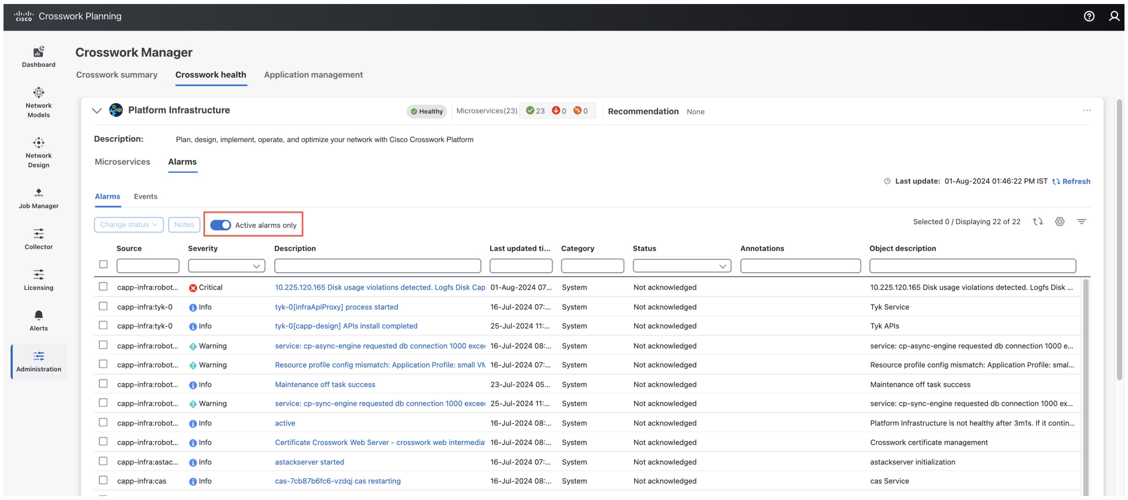
Status	Name	Up time	Recommendation	Description	Actions
Healthy	local-postgres	15d 18h 3m 6s	None		...
Healthy	robot-kafka	15d 18h 3m 30s	None		...
Healthy	robot-ui	15d 17h 44m 16s	None		...
Healthy	cas	15d 17h 44m 50s	None		...
Healthy	nats	15d 18h 3m 13s	None		...
Healthy	robot-orch	15d 18h 2m 15s	None		...
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.

b) Filter the list further by viewing only active alarms.

Figure 35: Alarms tab



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

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

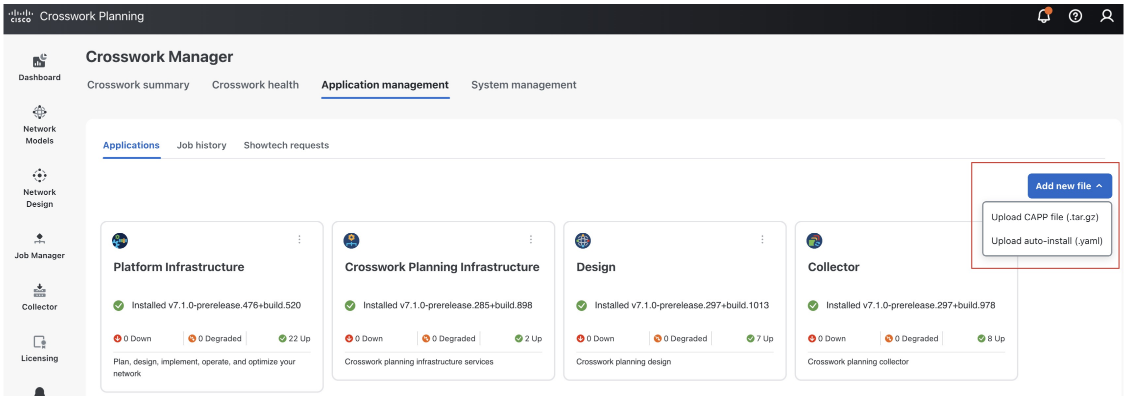
c) Click the **Events** tab to view all Crosswork Platform Infrastructure events and their correlated alarms.

Step 4 View which Crosswork applications are installed.

a) From the main menu, choose **Administration** > **Crosswork Manager** > **Application management** tab and click **Applications**.

This page displays all applications that have been installed.

Figure 36: Application management page



Platform Infrastructure
Installed v7.1.0-prerelease.476+build.520
0 Down | 0 Degraded | 22 Up
Plan, design, implement, operate, and optimize your network

Crosswork Planning Infrastructure
Installed v7.1.0-prerelease.285+build.898
0 Down | 0 Degraded | 2 Up
Crosswork planning infrastructure services

Design
Installed v7.1.0-prerelease.297+build.1013
0 Down | 0 Degraded | 7 Up
Crosswork planning design

Collector
Installed v7.1.0-prerelease.297+build.978
0 Down | 0 Degraded | 8 Up
Crosswork planning collector

b) To install more applications by uploading another application bundle or an auto-install file, click **Add new file**.

Step 5 View the status of jobs.

a) Click the **Job History** tab.

This page provides information about job statuses and the sequence of events executed as part of the job process.

Backup and restore

Cisco Crosswork Planning's backup and restore features are system functions that

- provide options to migrate or recover data in case of system failure or upgrade
- preserve your installed applications and settings, and
- help prevent data loss.

Backup and restore options

Cisco Crosswork Planning offers multiple menu options to back up and restore your data.

Table 21: Backup and restore options

Menu option	Description	Reference link
Actions > **Data backup**	This option preserves the Cisco Crosswork Planning configuration data. You can use the backup file with the data disaster restore (Restore Cisco Crosswork Planning after a disaster, on page 157) to recover from a serious outage.	• Back up data, on page 154 • Restore data, on page 156
Actions > **Data disaster restore**	This option restores the Cisco Crosswork Planning configuration data after a natural or human-caused disaster has required you to rebuild a Cisco Crosswork Planning server.	Restore Cisco Crosswork Planning after a disaster, on page 157

Menu option	Description	Reference link
Actions > **Data migration**	This option migrates data from an older version of Cisco Crosswork Planning to a newer version.	Migrate data using backup and restore, on page 158

Requirements for backup and restore

These items define the mandatory conditions and limitations that must be met for successful backup and restore operations in Cisco Crosswork Planning:

- Configure a destination SCP server to store backup files during your first login. Complete this one-time setup before taking backups or starting restore operations.
- Use the same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- Only one backup or restore operation can run at a time.
- Ensure both Cisco Crosswork Planning and the SCP server are in the same IP environment (for example, both using IPv4).
- By default, backups are not allowed if the system is not considered healthy, but this can be overridden for troubleshooting purposes.

Best practices for backup and restore

These items outline suggested actions that help ensure smoother, safer, and more efficient backup and restore processes for Cisco Crosswork Planning:

- Perform backup or restore operations during a scheduled maintenance window. You should not access the system during these operations. Backups will take the system offline for about 10 minutes, while restore operations can be lengthy and pause other applications, affecting data collection jobs.
- Use the dashboard to monitor the progress of backup or restore processes. Avoid using the system during these processes to prevent errors or incorrect content.
- Operators are responsible for periodically deleting older backups from the target server to ensure adequate storage for new backups, as Cisco Crosswork Planning does not manage them. Deleted backups may still appear in the job list.
- Operators making frequent changes should back up more often, possibly daily. Others might back up weekly or before major system upgrades.
- If using collector agents, manually restart them, as they may remain in a stopped state after the backup and restore operation.

Back up data

This topic describes how to perform a data backup operation from the Cisco Crosswork Planning UI.

Use this task to safeguard your application data in the event of failure or during planned upgrades.

The backup process depends on having SCP access to a server with sufficient amount of storage space. The storage required for each backup depends on the applications installed on the Cisco Crosswork Planning server and the scale requirements. The time taken for the backup process depends on the type of backup and the applications installed on the Cisco Crosswork Planning server.

Attention Building a target machine for the backup is outside the scope of this document. The operator must have the server ready, know the credentials for the server, and have a backup directory with sufficient space.

Before you begin

- Ensure you have a secure SCP server in place, with adequate space for backups. Building the target machine is out of scope for this document.
- Obtain the host name (or IP address) and the port number of the secure SCP server. Verify that the server has sufficient storage available.
- Note the file path on the SCP server, to use as the destination for your backup files.
- Ensure you have user credentials for an account with read and write permissions to the remote path on the destination SCP server.
- Note the build version of the installed applications. Before performing the data restore, you must install the exact versions of those applications. Any mismatch in application build versions can result in data loss or failure of the data restore job.
- Review the requirements and best practices in Requirements for backup and restore, on page 154 and Best practices for backup and restore, on page 154.

Procedure

Step 1 From the main menu, choose **Administration** > **Backup and Restore**.

Step 2 Configure the SCP backup server destination.

a) Click **Destination**.
b) In the Edit Destination dialog box, enter the hostname, port, destination path, and credentials for the SCP server.
c) Click **Save** to confirm the configuration.

Step 3 Create a backup job.

a) Click **Actions** > **Data backup**.
b) In the Data Backup dialog box, provide a relevant name in the **Job Name** field.
c) If the VM or any application is not healthy and you still want to create the backup, check the **Force** check box.

Note
You must use the **Force** option only after consultation with the Cisco Customer Experience team.

d) Complete the remaining fields as needed.

To specify a different remote server upload destination, edit the pre-filled **Host name**, **Port**, **Username**, **Password**, and **Server path/Location** to specify a different destination.

e) (Optional) Click **Verify backup readiness** to verify that Cisco Crosswork Planning has enough free resources to complete the backup.

If the check is successful, Cisco Crosswork Planning displays a warning about the time-consuming nature of the operation. Click **OK** to continue.

If the verification fails, contact the Cisco Customer Experience team for assistance.

f) Click **Start Backup** to start the backup operation.

Cisco Crosswork Planning creates the corresponding backup job set and adds it to the Backup and Restore Job Sets table. The Job Details panel reports the status of each backup step as it is completed.

Note
If you do not see your backup job in the list, refresh the Backup and Restore Job Sets table.

Step 4 Navigate to the destination SCP server directory and confirm that the backup file was created. You will need this backup file during later stages of the upgrade process.

The system configuration backup is created and available on the specified SCP server.

Restore data

This topic describes how to perform a data restore operation from the Cisco Crosswork Planning UI.

The time taken for the restore process depends on the type of backup and the applications installed on the Cisco Crosswork Planning server.

Before you begin

- Ensure you have a backup file available for restore.
- Install the exact build versions of the applications that were present when the backup was created. Any mismatch can result in data loss and failure of the data restore job.

Procedure

Step 1 From the main menu, choose **Administration** > **Backup and Restore**.

Step 2 Select the backup file for restore.

a) In the Backup and Restore Job Sets table, select the data backup file to be used for the restore. The Job Details panel displays information about the selected backup file.
b) With the backup file selected, click **Data Restore** to start the restore operation.

Step 3 Monitor the restore progress. 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.

The system initiates the restore operation from the selected backup file. The restore job appears in the job list with status detail.

Recommendation: Post-restore actions

Editing collections

After restoring the backup, navigate to the **Collector** > **Collections** page and perform the Edit collection operation on each listed collection. Save the collections without making any changes. This ensures that the configuration data is properly updated.

Restarting agents

The restore process only copies the database and file system data. Once the restore process completes, all agents will be in a stopped state, and you must restart them manually from the Cisco Crosswork Planning UI.

- Restart the NetFlow and SR-PCE agents using the **Start** option for the respective agent in the **Setup Agent** page (**Collector** > **Agents**). For more information, see Edit agent settings, on page 22.
- 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 83.

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

This topic describes how to restore operations after a natural or human-caused disaster has destroyed a Cisco Crosswork Planning server.

Before you begin

- Deploy a new server first, following the instructions in *Cisco Crosswork Planning 7.2 Installation Guide*.
- 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.

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** page with the remote server details prefilled.

Step 3 In **Backup file name**, 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.

The system restores server data and configuration from the specified backup file. Once complete, Cisco Crosswork Planning resumes operation with recovered settings and data.

Note

- If the disaster recovery fails, contact the Cisco Customer Experience team.
- Smart Licensing registration for Cisco Crosswork Planning applications is not restored during a disaster restore operation. You must register the applications again.

Migrate data using backup and restore

You must use data migration backup and restore when upgrading your Cisco Crosswork Planning installation to a new software version, or moving your existing data to a new installation.

Before you begin

- Configure a destination SCP server to store the data migration files. You only need to do this once.
- Ensure that both the Cisco Crosswork Planning and SCP server are in the same IP environment. For example, if Cisco Crosswork Planning is communicating over IPv6, the backup server must also use IPv6.
- Create a data migration backup only when upgrading your Cisco Crosswork Planning installation. Perform the backup only during a scheduled upgrade window.
- Do not attempt to access Cisco Crosswork Planning while the data migration backup or restore operations are running.
- Ensure that you have
    - the hostname or IP address and the port number of a secure destination SCP server
    - a file path on the SCP server to use as the destination for your data migration backup files, and
    - user credentials with file read and write permissions for the remote path on the destination SCP server

Procedure

Step 1 Configure an SCP backup server.

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the Add Destination page.
c) Make the relevant entries in the fields provided.
d) Click **Save** to confirm the backup server details.

Step 2 Create a backup.

a) Log in as an administrator to the Cisco Crosswork Planning installation whose data you want to migrate to another installation.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data backup** to display the Data Backup page with the destination server details prefilled.
d) In **Job Name**, provide a relevant name for the backup.
e) To create the backup even if there are microservice issues, check the **Force** check box.
f) Fill in any additional required fields.

   To specify a different remote server upload destination, edit the prefilled **Host name**, **Port**, **Username**, **Password**, and **Server path/Location** fields to specify a different destination.

g) Click **Backup** to start the backup operation.

   Cisco Crosswork Planning creates the corresponding backup job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel displays the status as each backup step completes.

h) To view the progress of a backup job, enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then, click on the job set you want.

   The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If a job fails, hover over the icon next to the **Status** column to view the error details.

i) If the backup fails during upload to the remote server, in the **Job Details** panel, click **Upload backup** under the Status icon to retry the upload.

   If the upload fails due to problems with the remote server, click **Destination** to specify a different remote server path before clicking **Upload backup**.

Step 3 Migrate the backup to the new installation.

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

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

Data is migrated from the source installation to the new software version or installation. The migration status appears in the job progress dashboard.

What to do next

Validate that the migrated data is present and ensure all services are functioning on the new installation.

View system and network alarms

This topic describes how to view current system and network alarms, including their details and status.

Procedure

Step 1 To view all current alarms, go to **Alerts** > **Alarms and Events**.

Step 2 To view application-specific alarms:

a) From the main menu, choose the **Administration** > **Crosswork Manager** > **Crosswork Health** tab.
b) Expand an application and click the **Alarms** tab.

Step 3 To view alarm details, click the alarm description.

Step 4 To change the status of the alarm, follow these steps:

a) Select the alarm.
b) Select the required status from the **Change status** drop-down list. Available options are **Acknowledge**, **Unacknowledge**, or **Clear**.

Step 5 To add notes to an alarm, follow these steps:

a) Select the alarm.
b) Click **Notes** and enter your comments.

View the audit log

This topic describes how to use the **Audit Log** page to view the AAA events.

The Audit Log page tracks these events:

- Create, update, and delete users
- Create, update, and delete roles
- User login activities: login, logout, login failure due to maximum active session limit, and account locked due to maximum login failures.
- Source IP: The IP address of the machine from where the action was performed. This column appears only if you check the **Enable source IP for auditing** check box and then log in to Cisco Crosswork Planning. You can find this check box in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.
- Password modification by user

Procedure

Step 1 From the main menu, choose **Administration** > **Audit Log**.

The Audit Log page opens.

Step 2 Click ≡ to filter the results based on your query.

Step 3 (Optional) Click ⤓ to export the log in CSV format.

When exporting, you can use the default file name or enter a unique name.

The filtered or exported audit log is available for review.

Set the pre-login disclaimer message

This topic describes how to enable the pre-login disclaimer message and customize the message as needed.

Many organizations require that their systems display a disclaimer message in a banner before users log in. The banner reminds authorized users of their obligations when using the system, or provides warnings to unauthorized users.

Procedure

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

Step 2 Under **Notifications**, click **Pre-login disclaimer**.

The Pre-login disclaimer page opens.

Step 3 Follow these steps to enable the disclaimer and customize the banner:

a) Check the **Enable** check box.
b) Customize the banner by editing the **Title**, **Icon**, and **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 may:

- Click **Preview** to see how your changes look when displayed before the 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) Click **Save** to apply the changes and enable the custom disclaimer to all users.

Step 4 To turn off the disclaimer display, return to the **Pre-login disclaimer** page and uncheck the **Enable** check box.

Enable maintenance mode

This topic describes how to place the system in maintenance mode.

Maintenance mode provides a means for shutting down the Cisco Crosswork Planning system temporarily. Cisco Crosswork Planning synchronizes all application data before 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.

Before you begin

Caution

- Make a backup of your Cisco Crosswork Planning system before enabling maintenance mode.
- Notify other users about your intention to put the system in maintenance mode. Give them a deadline to log out. Once you initiate the maintenance mode operation, it cannot be canceled.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.

Step 2 Drag the **Turn on/off maintenance** slider to the right to set it to the On position.
You will receive a warning message that the system is about to enter maintenance mode.

Step 3 Click **Continue** to confirm your choice.

Note
If you are rebooting the system, wait for 5 minutes after the system has entered maintenance mode. This allows the Cisco Crosswork database to synchronize before you proceed.

The system synchronizes data, shuts down temporarily, and enters maintenance mode.

What to do next

To return the system to normal operation after maintenance, drag the **Turn on/off maintenance** slider to the left to set it to the Off position.

- 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, toggle the maintenance mode on and off to allow the applications to function normally.

Update the network access configuration

This topic describes how to update the global network access settings to meet your requirements.

The **Network access configuration** section specifies the parameters used for network access through SNMP, Login, and the SAM interface. You can update these parameters to meet your specific requirements. For example, you can update the SNMP timeout value according to your needs.

Before you begin

Caution Before you edit, 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** > **Network access configuration**.

Step 2 Click **Edit** at the bottom of the page. An alert appears, notifying you that modifying the configuration to disable the required service will result in collection failure. If you intend to change only the timeout or other parameters, click **Confirm**.

The page becomes editable.

Step 3 Edit the file to meet your requirements.

Step 4 After making your changes, save them.

Step 5 (Optional) Click 📤 to download the file to your local machine.

The updated network access configuration is applied globally.

Update collector capability settings

You can view each collector's data source, as well as the tables and columns into which they populate the data, on the **Collector capability** page. This topic describes how to update these configurations according to your requirements.

Before you begin

Caution Before you update, 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** > **Collector capability**.

Step 2 Click **Edit** at the bottom of the page.

The page becomes editable.

Step 3 Edit the collector table and column configurations as needed.

The details use the *Collector.table.table-name=ALL/Column list* format, where ALL indicates that the collector populates all columns in that table. If the collector populates only a subset of columns, then it is specified as a list of column names separated by commas.

Step 4 After making your changes, save them.

Step 5 (Optional) To download the collector capability configurations to your local machine, click ⇪.

Step 6 (Optional) To reset the configurations to their default values, click **Reset default config** at the upper right.

The system applies your updated collector capability configuration globally across all collections, jobs, and plan files.

Configure the aging settings

This topic describes how to configure the retention period for inactive network elements before they are permanently removed from the network.

By default, when a circuit, port, node, or link disappears from the network, it is permanently removed and must be rediscovered. You can configure how long Cisco Crosswork Planning retains these elements before permanent removal.

Before you begin

⚠ **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 Enable aging by selecting **Enable**.

Step 3 Enter the retention duration in the relevant fields.

- **L3 port**: Specify how long an inactive L3 port must be kept in the network.
- **L3 node**: Specify how long an inactive L3 node must be kept in the network.
- **L3 circuit**: Specify how long an inactive L3 circuit must be kept in the network.

Note
The L3 node value must be greater than or equal to the L3 port value, which in turn must be greater than or equal to the L3 circuit value.

Step 4 After making your changes, save them.

Cisco Crosswork Planning uses these settings to determine how long to retain inactive network elements before permanent removal.

Set the retention period for archived plan files

This topic describes how to configure the retention period for archived plan files before they are deleted.

The archived plan files are periodically deleted in Cisco Crosswork Planning to conserve storage space. By default, the files are retained for 30 days.

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 days are deleted.

Step 3 Save the changes.

The system will automatically delete archived plan files older than the retention period you specify.

Note To disable purging of archived plan files, uncheck the **Enable** check box. Be aware that if you disable it, storage space will eventually run out.

Add static routes

Static routes are used to reach the devices in a different subset. Use this procedure to add static routes in Cisco Crosswork Planning.

Note After static routes are applied, their corresponding entries will appear when you run the **ip rule list** command at the Crosswork shell prompt.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Device connectivity management** > **Routes**.

Step 2 Click **+ Add**. The Add Route IP page appears.

Step 3 Enter a 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** on the confirmation page.