Prepare Infrastructure for Device Management

This section contains the following topics:

Manage Credential Profiles

Credential profiles are collections of credentials for SNMP, Telnet, SSH, HTTP, and other network protocols. You can have multiple protocols and credentials in a single credential profile.

Using credential profiles lets you automate device configuration changes and monitoring, and communicate with providers. When you add or import devices, or create providers, you specify the credential profile.

From the **Credential Profiles** window, you can create a new credential profile, update the settings configured for an existing profile, or delete a profile. To open this window, choose **Device Management** > **Credential Profiles** from the main menu.

Figure 1: Credentials Profile window

Item	Description
1	Click ➕ to add a credential profile. See Create Credential Profiles, on page 2.
	Click ✏ to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 6.
	Click 🗑 to delete the selected credential profile. See Delete Credential Profiles, on page 7.
	Click ⬇ to import new credential profiles from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Credential Profiles, on page 4.
	Click ⬆ to export credential profiles to a CSV file. See Export Credential Profiles, on page 6.
2	Click ↻ to refresh the **Credential Profiles** window.
	Click ⚙ to choose the columns to make visible in the **Credential Profiles** window.
3	Click ≡ to set filter criteria on one or more columns in the **Credential Profiles** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

Create Credential Profiles

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

If you have many credential profiles to add, you may find it more efficient to put the information in a CSV file and import the file. See Import Credential Profiles, on page 4.

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

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

- All the characters in each password or community string entry in every credential profile exported to a CSV file are replaced with asterisks (Export Credential Profiles, on page 6).

- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see Import Credential Profiles, on page 4).

To maintain network security, Cisco recommends that you use asterisks in place of real passwords, and community strings in any CSV file you plan to import. After the import, follow the steps in Edit Credential Profiles, on page 6 to replace the asterisks with actual passwords and community strings.

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

Step 2 Click ＋.

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

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

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

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

Connectivity Type	Fields
SSH	Enter the required **User Name**, **Password**, and **Confirm Password**. The **Enable Password** is optional.
SNMPv2	Enter the required SNMPv2 **Read Community** string. The **Write Community** string is optional.
NETCONF	Enter the required **User Name**, **Password**, and **Confirm Password**.
TELNET **Note** There may be some security limitations when using this protocol.	Enter the required **User Name**, **Password**, and **Confirm Password**. The **Enable Password** is optional.
HTTP	Enter the required **User Name**, **Password**, and **Confirm Password**.
HTTPS	Enter the required **User Name**, **Password**, and **Confirm Password**.
GRPC	Enter the required **User Name**, **Password**, and **Confirm Password**.
gNMI	Enter the required **User Name**, **Password**, and **Confirm Password**.
TL1	Enter the required **User Name**, **Password**, and **Confirm Password**.

Connectivity Type	Fields

SNMPv3	Choose the required **Security Level** and enter the **User Name**.
	
	If you chose the NO_AUTH_NO_PRIV **Security Level** of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional.
	
	If you chose the AUTH_NO_PRIV **Security Level**, you must choose an **Auth Type** and enter an **Auth Password**.
	
	If you chose the AUTH_PRIV **Security Level**, you must choose an **Auth Type** and **Priv Type**, and enter an **Auth Password** and **Priv Password**.
	
	The following SNMPv3 Privacy Types are supported:
	
	   • CFB_AES_128
	
	   • CBC_DES_56
	
	   • AES-192
	
	   • AES-256
	
	   • 3-DES

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

Step 7   Click **Save**.

Import Credential Profiles

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

Importing credential profiles from a CSV file adds any profiles not already in the database. You cannot import a credential profile that already exists.

If you are re-importing a credential profile CSV file that you previously exported and modified, remember that all the passwords and community strings in the exported credential profile CSV file are replaced with asterisks. You cannot re-import an exported credential profile CSV file with blank passwords. To maintain security, Cisco recommends that you use asterisks in place of real passwords and community strings in the CSV file. After the import, follow the steps in Edit Credential Profiles, on page 6 to replace the asterisks with actual passwords and community strings.

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

Step 2   Click ⬆ to open the dialog box.

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

     a)   Click the **Download sample 'Credential template (*.csv)' file** link and save the CSV file template to your local disk.

     b)   Open the template using your preferred tool. Begin adding rows to the file, one row for each credential profile.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter `SSH;NETCONF;TELNET` in the **Connectivity Type** field and you enter `UserTom;UserDick;UserHarry;` in the **User Name** field, the order of entry determines the mapping between the two fields:

- SSH: UserTom
- NETCONF: UserDick
- TELNET: UserHarry

Also note:

- Be sure to enter SNMP community string information exactly as currently entered on your devices.
- Password and community string information associated with a user ID are stored in plain text in the CSV file you prepare. Be aware of the security implications of this, and apply appropriate safeguards.

Field	Entries	Required or Optional
Credential Profile	The name of the credential profile. For example: .	Required
Connectivity Type	Valid values are: `SSH`, `SNMPv2`, `NETCONF`, `TELNET`, `HTTP`, `HTTPS`, `GRPC` or `SNMPv3`	
User Name	For example:	Required if **Connectivity Type** is `SSH`, `NETCONF`, `TELNET`, `HTTP`, `HTTPS`, `SNMPv3` or `GRPC.`
Password	The password for the preceding **User Name**.	Required if **Connectivity Type** is `SSH`, `NETCONF`, `TELNET`, `HTTP`, `HTTPS` or `GRPC`
Enable Password	Use an Enable password. Valid values are: `ENABLE`, `DISABLE`	
Enable Password Value	Specify the Enable password to use.	
SNMPV2 Read Community	For example: `readprivate`	Required if **Connectivity Type** is `SNMPv2`
SNMPV2 Write Community	For example: `writeprivate`	
SNMPV3 User Name	For example: `DemoUser`	Required if **Connectivity Type** is `SNMPv3`
SNMPV3 Security Level	Valid values are `noAuthNoPriv`, `AuthNoPriv` or `AuthPriv`	Required if **Connectivity Type** is `SNMPv3`
SNMPV3 Auth Type	Valid values are `HMAC_MD5` or `HMAC_SHA`	Required if **Connectivity Type** is `SNMPv3` and **SnmpV3 Security Level** is `AuthNoPriv` or `AuthPriv`

Field	Entries	Required or Optional
SNMPV3 Auth Password	The password for this authorization type.	Required if **Connectivity Type** is `SNMPv3` and **SnmpV3 Security Level** is `AuthNoPriv` or `AuthPriv`
SNMPV3 Priv Type	Valid values are `CFB_AES_128` or `CBC_DES_56` The following SNMPv3 privacy types are not supported: AES-192, AES-256, 3-DES	Required if **Connectivity Type** is `SNMPv3` and **SnmpV3 Security Level** is `AuthPriv`
SNMPV3 Priv Password	The password for this privilege type.	Required if **Connectivity Type** is `SNMPv3` and **SnmpV3 Security Level** is `AuthPriv`

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

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

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

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

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

Edit Credential Profiles

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

Before editing any credential profile, it is always good practice to export a CSV backup of the profiles you want to change (see).

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

Step 2 From the left-hand side of the **Credential Profiles** window, select the profile you want to update, and click ✎.
The **Edit Profile** window of the selected credential is displayed.

Step 3 Make the necessary changes and then click **Save**.

Export Credential Profiles

Exporting credential profiles stores all the profiles you selected in a CSV file. This is a quick way to make backup copies of your credential profiles. You can also edit the CSV file as needed, and re-import it to add new or modify credential profile data.

The exported credential profiles CSV file does not contain real passwords or community strings. All the characters in the passwords and community strings entries in the credential profiles are replaced with asterisks in the exported CSV file. If you plan on modifying your exported CSV file and then re-importing it, Cisco recommends that you use asterisks in place of real passwords and community strings. After the import, follow

the steps in Edit Credential Profiles, on page 6 to replace the asterisks with actual passwords and community strings.

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

Step 2 (Optional) In the **Credential Profiles** window, filter the credential profile list as needed.

Step 3 Check the check boxes for the profiles you want to export. Check the check box at the top of the column to select all the profiles for export.

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

Delete Credential Profiles

Follow the steps below to delete a credential profile.

✎

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

Step 1 Export a backup CSV file containing the credential profile you plan to delete (see Export Credential Profiles, on page 6).

Step 2 Check whether any devices or providers are using the credential profile you plan to delete. You can do this by filtering on the **Credential Profile** column, which is available on both the **Devices** window (choose **Device Management** > **Credential Profiles**) and the Providers window (choose **Administration** > **Manage Provider Access**).

Step 3 Reassign the devices or providers to a different credential profile (for help with this task, see Change the Credential Profile for Multiple Devices, on page 7 and Edit Providers, on page 36).

Step 4 After all devices and providers have had their credential profiles reassigned: From the main menu, choose **Device Management** > **Credential Profiles**.

Step 5 In the **Credential Profiles** window, choose the profile that you want to delete and then click 🗑.

Change the Credential Profile for Multiple Devices

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

1. Export a CSV file containing the devices whose credential profiles you want to change (see Export Device Information to a CSV File).

2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist). Save the edited file.

You will need to make sure that the credential profile to which you are changing already exists. If you have not yet created that credential profile, the CSV import will fail. The credential profile you associate with these devices must also have the authorization credentials for every protocol that was configured for these devices

during onboarding. If any credential for a specific protocol configured on the devices is missing from or incorrect in the credential profile, then the CSV import will succeed, but reachability checks will fail for these devices.

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

Step 2   Choose the devices whose credential profiles you want to change. Your options are:

- Click ⬆ to include all devices.

- Filter the device list by entering text in the **Search** field or by filtering specific columns. Then click ⬆ to include only the filtered list of devices.

- Check the boxes next to the device records you want to change. Then click ⬆ to include only the devices that have been checked.

Step 3   Edit and save the new CSV file using the tool of your choice. Be sure to enter the correct credential profile name in the **Credential Profile** field for each device.

Step 4   Click ⬇.

Step 5   In the **Import** dialog box, click **Browse**, choose the new CSV file, and click **Import**.

Manage Providers

Cisco Crosswork applications communicate with external providers. Cisco Crosswork stores the provider connectivity details and makes that information available to applications. For more information, see Before You Begin.

From the **Providers** window, you can add a new provider, update the settings configured for an existing provider, and delete a particular provider. To open this window, choose **Administration** > **Manage Provider Access**.

Note   Wait until the application responds between performing a succession of updates. For example, wait for some time between adding, deleting, or readding providers. Topology services may not receive these changes if you perform these actions too quickly. However, if you find that topology is out of sync, restart the topology service.

Figure 2: Providers Window

Item	Description
1	The icon shown next to the provider in this column indicates the provider's **Reachability**. See Device State.
2	Click ➕ to add a provider. See About Adding Providers, on page 11.
	Click ✎ to edit the settings for the selected provider. See Edit Providers, on page 36.
	Click 🗑 to delete the selected provider. See Delete Providers, on page 36.
	Click ⬇ to import new providers or update existing providers from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Providers, on page 34.
	Click ⬆ to export a provider to a CSV file. See Export Providers, on page 37.
3	Click ⓘ next to the provider in the **Provider Name** column to open the **Properties for** pop-up window, showing the details of any startup session key/value pairs for the provider.
4	Click ⓘ next to the provider in the **Connectivity Type** column to open the **Connectivity Details** pop-up window, showing the protocol, IP, and other connection information for the provider.
5	Click ↻ to refresh the **Providers** window.
	Click ⚙ to choose the columns to make visible in the Providers window (see).
6	Click ☰ to set filter criteria on one or more columns in the **Providers** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

About Provider Families

Cisco Crosswork supports different types, or families, of providers. Each provider family supplies its own mix of special services, and each comes with unique requirements and options.

The currently supported provider families are shown in the following table.

Table 1: Supported Provider Families

Provider Family	Description
NSO	Instances of Cisco Network Services Orchestrator (Cisco NSO), used to configure network devices. See Add Cisco NSO Providers, on page 13.

Provider Family	Description
SR-PCE	Instances of Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) containing the configuration information needed to allow Cisco Crosswork applications to communicate with and retrieve segment routing information for the network. See Add Cisco SR-PCE Providers, on page 18.
WAE	Instances of Cisco WAN Automation Engine (Cisco WAE) provide "what if" analysis used to evaluate network changes. See Add Cisco WAE Providers, on page 29 .
Syslog Storage	Instances of storage servers (remote or on the Cisco Crosswork application VM itself) where you want store syslogs and other data retrieved from devices by KPIs and Playbooks. See Add Syslog Storage Providers, on page 30.
Alert	Instances of providers (such as Cisco Crosswork Situation Manager) to which alerts collected during KPI monitoring are to be forwarded. See Add an Alert Provider, on page 31
Proxy	Instances of proxy providers. See Add Proxy Providers, on page 32

Provider Dependency

This section explains the provider configurations required for each Cisco Crosswork application and for Cisco Crosswork Network Controller.

Cisco Crosswork Network Controller is an integrated solution that combines Cisco Crosswork Active Topology and Cisco Crosswork Optimization Engine. You can also optionally integrate Crosswork Network Controller with Crosswork Change Automation, Crosswork Health Insights, and Crosswork Zero Touch Provisioning.

Table 2: Provider Dependency matrix

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider	Cisco WAE Provider	Syslog Storage Provider	Alert Provider
Crosswork Network Controller	Mandatory Required protocol is HTTPS Provider property key **forward** must be set as *true*.	Mandatory Required protocol is HTTP.	Optional	Optional	Optional
Crosswork Optimization Engine	Optional	Mandatory Required protocol is HTTP.	Optional	Optional	Optional

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider	Cisco WAE Provider	Syslog Storage Provider	Alert Provider
Crosswork Change Automation Crosswork Health Insights	Mandatory Required protocol is HTTPS. Provider property key **forward** must be set as *true*.	Optional	Optional	Optional	Optional
Crosswork Zero Touch Provisioning	Optional	Optional	Optional	Optional	Optional

About Adding Providers

Cisco Crosswork depends on a variety of providers to perform various functions. For example, Cisco Network Services Orchestrator provides segment routing policies and device information. Features that depend on new providers may be added in the future, and you may need to communicate with more than one instance of a single provider. To access each provider's services, the provider must be added to the Cisco Crosswork application's system configuration.

There are two ways to add providers:

1. **Adding providers via the UI**: This method is explained in Add Providers Through the UI, on page 11. Although this method is the most time-consuming, it is more often used because most deployments will not need a lot of provider instances.

2. **Importing providers from a providers CSV file**: This method is explained in Import Providers, on page 34. Importing a CSV file is useful when you have a lot of provider instances to add or update at one time.

Note that both methods require that you:

- Create a corresponding credential profile, beforehand, so that the Cisco Crosswork applications can access the provider. For help, see Create Credential Profiles, on page 2.

- Know the protocol, IP address, port number, and other information needed to connect with the provider.

- Know any special properties the provider may require during the session startup.

Add Providers Through the UI

Use this procedure to add a new external provider. You can then map the provider to devices.

Step 1   From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2   Click ➕.

Step 3   Enter values for the provider as listed in the following table.

Step 4   When you have complete entries in all of the required fields, click **Save** to add the new provider.

Step 5   (Optional) Repeat to add more providers.

Table 3: Add Provider Fields (=required)*

Field	Description
* **Provider Name**	The name for the provider that will be used to refer to it in the Cisco Crosswork application. For example: `Linux_Server`. The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.
* **Credential Profile**	Select the name of the credential profile that is used by the Cisco Crosswork application to connect to the provider.
* **Family**	Select the provider family. Choices are: **NSO**, **WAE**, **SR-PCE**, **ALERT** and **SYSLOG_STORAGE**.
Connection Type(s)	
* **Protocol**	Select the principal protocol that the Cisco Crosswork application will use to connect to the provider. Options include: **HTTP**, **HTTPS**, **SSH**, **SNMP**, **NETCONF**, **TELNET**, and more. To add more connectivity protocols for this provider, click ⊕ at the end of the first row. To delete a protocol you have entered, click ⊗ shown next to that row. You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol.
* **Server Details**	Select and provide one of the options: • IP Address (IPv4 or IPv6) and subnet mask of the provider's server. • FQDN (Domain name and Host name)
* **Port**	Enter the port number to use to connect to the provider's server. This is the port corresponding to the protocol being configured. For example, if the protocol used to communicate with the provider server is SSH, the port number is usually 22.
Timeout	Enter the amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.
Model Prefix Info	

Field	Description

* **Model**	Required only if you are adding a Cisco NSO provider: Select the model prefix that matches the NED CLI used by Cisco NSO. Valid values are:
	
	 `Cisco-IOS-XR`
	
	 `Cisco-NX-OS`
	
	 `Cisco-IOS-XE`
	
	 For telemetry, only `Cisco-IOS-XR` is supported.
	
	 To add more model prefix information for this Cisco NSO provider, click the ⊕ at the end of any row in the **Model Prefix Info** section. To delete a model prefix you have entered, click the ⊗ shown next to that row.

* **Version**	Required only if you are adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the NSO server.
Provider Properties	
Property Key	Enter the name of the key for the special provider property you want to configure. Provider properties control how the Cisco Crosswork application interacts with the provider. Not all providers need them, and the number and type of properties vary with the provider family. These properties are documented in topics about adding specific providers elsewhere in this Guide. Please note, however, that the Cisco Crosswork application does not validate provider properties. Make sure the properties you enter are valid for the provider. **Note** In a two network interface configuration, the Cisco Crosswork applications default to communicating with providers using the Management Network Interface (`eth0`). You can change this behavior by adding **Property Key** and **Property Value** as `outgoing-interface` and `eth1` respectively. This is most often necessary when creating the SR-PCE provider, as its management interface may reside on the data network instead of the management network.
Property Value	Enter the value to assign to the property key. To add more special properties for this provider, click ⊕ at the end of any key/value pair in the **Provider Properties** section. To delete a key/value pair you have entered, click ⊗ shown next to that pair.

Add Cisco NSO Providers

This topic explains the steps to add a Cisco NSO provider through the Crosswork UI.

The Cisco Network Services Orchestrator (Cisco NSO) provider functions as the provider for Cisco Crosswork to configure the devices according to their expected functions, including optionally configuring MDT sensor paths for data collection. Cisco NSO provides the important functions of device management, configuration and maintenance services.

Cisco Crosswork also supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.

Note The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used "as is" in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.

See View Installed NSO Function Packs, on page 17 to monitor the state of the installed NSO function packs.

Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Crosswork (see Import Providers, on page 34).

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see Create Credential Profiles, on page 2).

- Know the name you want to assign to the Cisco NSO provider.

- Know the Cisco NSO NED device models and driver versions used in your topology. You can find the Cisco NSO version using the `version` command.

- Know the Cisco NSO server IP address or FQDN (Domain name and host name). When NSO is configured with HA, the IP address would be management VIP address.

- Confirm Cisco NSO device configurations. For more information, see Sample Configuration for Cisco NSO Devices.

- The NSO cross launch feature is not available for user roles with read-only permissions.

For NSO LSA deployment:

- If you plan to add a NSO LSA provider, you must first enable LSA settings. See Enable Layered Service Architecture (LSA), on page 16 for details.

- If you forgot to enable the LSA setting or misconfigures the provider property values, please perform the recovery steps mentioned in NSO LSA Setup Recovery, on page 17.

- The RFS node IP addresses used on the CFS must match with the IP addresses on the Crosswork UI. A mismatch will generate the error "*LSA cluster is missing RFS providers*".

- In case of the CFS node, only the **forward** property key is used.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click ➕.

Step 3   Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name**: Enter a name for the provider.

- **Credential Profile**: Select the previously created Cisco NSO credential profile.

- **Family**: Select **NSO**.

- **Protocol**: Select **HTTPS**. For more information, see Provider Dependency, on page 10.

- **Server Details**: Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) of the server.

- **Port**: For HTTPS, enter the port that corresponds with what is configured on the NSO VM in etc/ncs/ncs.conf to access NSO using HTTPS. NSO uses **8888** as default port.

- **Model**: Select the model (Cisco-IOS-XR, Cisco-NX-OS, or Cisco-IOS-XE). Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.

- **Version**: Enter the NED software version installed for the device model in NSO.

Important   When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

c) **Provider Properties**: Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
forward	**true** This property is necessary when using the Cisco Crosswork Network Controller solution to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway.
nso_crosslaunch_url **Note** This property is used only for NSO standalone provider.	Enter the URL for cross-launching NSO in the format: **https://<NSO IP address/FQDN>: port number** To enable cross-launch of the NSO application from the Crosswork UI. Requires a valid protocol (**HTTP** or **HTTPS**), and the provider must be reachable. The cross launch icon (⬀) is displayed in the **Provider Name** column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.

input_url_prefix
 	
Note   This property is used only for NSO LSA provider.
	Enter the RFS ID in the format: **/rfc-x**, where **x** refers to the number of the RFS node.
	
	`Example (for RFS node 1):`
	`input_url_prefix: /rfc-1`

Step 4   When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

Step 5   In the Providers window, select the NSO provider you created and click **Actions** > **Edit Policy Details**.

The **Edit Policy Details** window for the selected NSO provider is displayed.

Step 6   Edit the configuration fields to match the requirements of your environment. Click **Save** to save your changes.

Enable Layered Service Architecture (LSA)

This procedure is applicable only when you have opted for Cisco NSO LSA deployment to add arbitrarily many device nodes for improved memory and provisioning throughput.

Step 1   From the main menu, select **Administration** > **Settings** > **System Settings** > **Layered Service Architecture**.

Figure 3: Enabling Layered Service Architecture Window
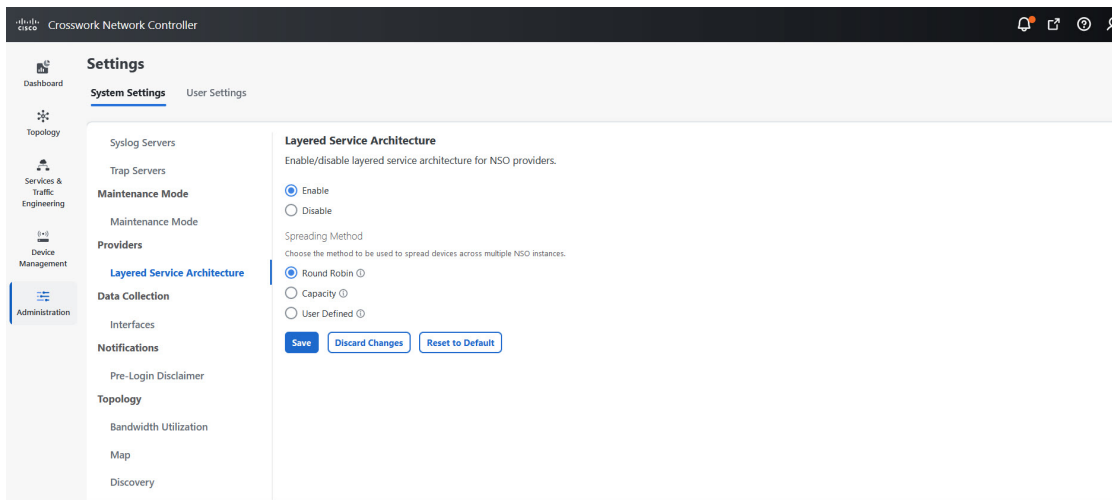
Step 2   Select **Enable**.

Step 3   Select the method to spread the devices across multiple NSO instances:

- **Round Robin** - Even distribution of devices to RFS nodes in a cyclical manner (for example, Device 1 to RFS1, Device 2 to RFS2, and so on).

- **Capacity** - The number of devices are assigned to each RFS instance based on its total capacity.

- **User Defined** - Devices are assigned to the NSO providers specified for the device in the device settings. For more information, see Add Devices through the UI.

Step 4   Click **Save**.

Note   Once you have saved the settings, you cannot disable it without removing all the NSO providers.

NSO LSA Setup Recovery

This topic explains the steps for NSO LSA setup recovery in case of any misconfigurations.

Step 1 Remove the NSO providers and associated devices on Device Management window.

Step 2 Clean up the associated services on the Cisco NSO application.

Step 3 Enable the LSA settings and add the NSO LSA provider with correct property values.

Step 4 Add the NSO providers and devices again to Crosswork, and map them to the Crosswork Data Gateway.

Step 5 Perform the sync operation on the NSO nodes (RFS and CFS) again to sync the devices correctly.

This will recover the functionality as expected.

View Installed NSO Function Packs

Cisco Crosswork allows you to monitor the status of the installed NSO Function Packs.

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

Step 2 On the **Crosswork Manager** window, select the **NSO Deployment Manager** tab.

The **Installed NSO Function Packs**, **NSO Function Pack Bundles**, and **Job History** tabs are displayed.

Note You can also navigate here from the NSO provider entries in the **Providers** window (click **Actions** > **View Function Packs**).

The **Installed NSO Function Packs** tab displays a list of NSO function pack bundles deployed on the configured NSO server.

Figure 4: Installed NSO Function Packs
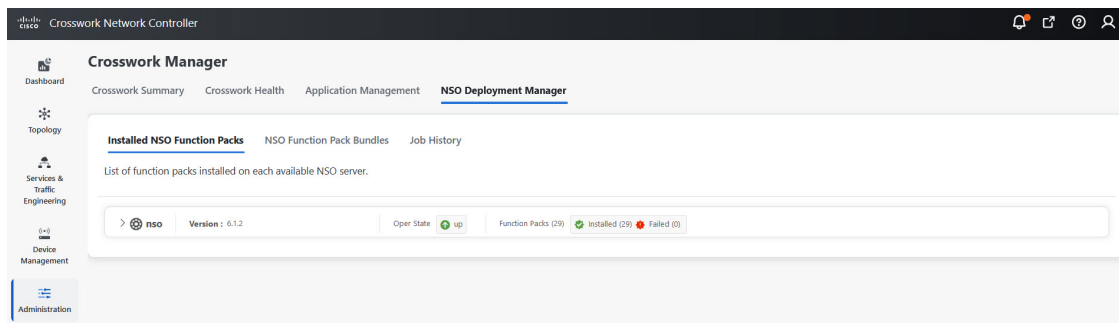
Step 3 Expand the bundles to view the number of function packs within each bundle, the function pack name, operational state as **Up** or **Down**, description, and version.

Add Cisco SR-PCE Providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers supply device discovery, management, configuration-maintenance and route-calculation services to the Cisco Crosswork applications. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices. You have the option to configure a second SR-PCE as a backup. Both SR-PCE devices must be connected to the same network as does not support managing more than one domain.

✎

Note   To enable Cisco Crosswork application access to an SR-PCE as an SDN controller on the management domain, SR-PCE needs to be added as a provider.

Follow the steps below to add (through the UI) one or more instances of Cisco SR-PCE as providers.

Before you begin

You will need to:

- Configure a device to act as the SR-PCE. See SR configuration documentation for your specific device platform to enable SR (for IS-IS or OSPF protocols) and configure an SR-PCE (for example: *Segment Routing Configuration Guide for Cisco NCS 540 Series Routers*).

- Create a credential profile for the Cisco SR-PCE provider (see Create Credential Profiles, on page 2). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the Cisco SR-PCE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.

- Know the name you want to assign to the Cisco SR-PCE provider. This is usually the DNS hostname of the Cisco SR-PCE server.

- Know the Cisco SR-PCE server IP address.

- Know the interface you want to use to communicate between Cisco SR-PCE and the Cisco Crosswork application server.

- Determine whether you want to auto-onboard the devices that Cisco SR-PCE discovers and, if so, whether you want the new devices to have their management status set to **off**, **managed** or **unmanaged** when added.

- If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:

  - Assign an existing credential profile for communication with the new managed devices.

  - The credential profile must be configured with an SNMP protocol.

- For high availability, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations .

Step 1   From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2   Click ⊞ .

Step 3   Enter the following values for the SR-PCE provider fields:

a) Required fields:

- **Provider Name**: Name of the SR-PCE provider.

- **Credential Profile**: Select the previously created Cisco SR-PCE credential profile.

- **Family**: Select **SR_PCE**. All other options should be ignored.

- **Protocol**: Select **HTTP**.

- **Server Details**: Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) and subnet mask of the server.

- **Port**: Enter **8080** for the port number.

- **Provider Properties**: Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
auto-onboard	**off**
	Note Use this option if you plan to manually (via UI or CSV import) enter all of your network devices.
	When devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in Cisco Crosswork Inventory Management database.
auto-onboard	**unmanaged**
	If this option is enabled, all devices that Cisco Crosswork discovers will be registered in the Cisco Crosswork Inventory Management database, with their configured state set to **unmanaged**. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the **managed** state later, you will need to either edit them via the UI or export them to a CSV make modifications and then import the updated CSV. You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).
auto-onboard	**managed**
	If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Inventory Management database, with their configured state set to **managed**. SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (TE Router ID for IPv4, or IPv6 Router ID for IPv6 deployment). The devices will be added with the credential profile associated with the device-profile key in the SR-PCE provider configuration.

Property Key	Value
device-profile	The name of a credential profile that contains SNMP credentials for all the new devices. **Note** This field is necessary only if **auto-onboard** is set to **managed**. If the **auto-onboard** is set to **managed** and there is no valid **device-profile** set, the device will be onboarded as **unmanaged** instead.
outgoing-interface	**eth1** **Note** You have to set this only if you want to enable Cisco Crosswork application access to SR-PCE via the data network interface when using the two NIC configuration.
topology	**off** or **on**. This is an optional property. If not specified, the default value is **on**. If value is specified as **off**, it means that L3 topology is not accessible for the SR-PCE provider.
pce	**off** or **on**. This is an optional property. If not specified, the default value is **on**. If value is specified as **off**, it means that LSPs and policies are not accessible for the SR-PCE provider.

Note Topology can be visualized even with **auto-onboard** as **off** and no **device-profile**.

Figure 5: Provider Property Key and Value Example

Note If **managed** or **unmanaged** options are set and you want to delete a device later, you must do one of the following:.

- Reconfigure and remove the devices from the network before deleting the device from Cisco Crosswork. This avoids Cisco Crosswork from rediscovering and adding the device back.

- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork. However, doing so will not allow Cisco Crosswork to detect or auto-onboard any new devices in the network.

b) Optional values:

• **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the SR-PCE server. The default is 30 seconds.

Step 4   When you have completed entries in all of the required fields, click **Save** to add the SR-PCE provider.

Step 5   Confirm that the SR-PCE provider shows a green Reachability status without any errors. You can also view the Events window (**Administration** > **Events**) to see if the provider has been configured correctly.

Step 6   Repeat this process for each SR-PCE provider.

Note   It is not recommended to modify auto-onboard options once set. If you need to modify them, do the following:

1.   Delete the provider and wait until deletion confirmation is displayed in the Events window.

2.   Re-add the provider with the updated auto-onboard option.

3.   Confirm the provider has been added with the correct auto-onboard option in the Events window.

What to do next

• If you entered the `auto-onboard`/`off` pair, navigate to **Device Management** > **Network Devices** to add a devices.

• If you opted to automatically onboard devices, navigate to **Device Management** > **Network Devices** to view the device list. To add more node information such as geographical location details, export the device list (.csv), update it, and import it back. If geographical location data is missing, you will only be able to see device topology using the logical map.

Cisco SR-PCE Reachability Issues

You can find reachability issues raised in the Events table and reachability status in the **Providers** window (see Get Provider Details, on page 34). If the SR-PCE goes down, all links in the topology will display with the last known state since the SR-PCE cannot send any notification updates. When the SR-PCE becomes reachable again, a message will show in the **Events** table (⬛) that SR-PCE is reconnected and the topology will be updated accordingly. If you find that the SR-PCE goes down for an extended amount of time, it is not syncing, updates are not happening, then delete the SR-PCE and add it back (when connectivity returns) using the UI:

1.   Execute the following command:

```
# process restart pce_server
```

2.   From the UI, navigate to **Administration** > **Manage Provider Access** and delete the SR-PCE provider and then add it back again.

You can also troubleshoot reachability as follows:

Step 1   Check device credentials.

Step 2   Ping the provider host.

Step 3   Attempt a connection using the protocols specified in the connectivity settings for the provider. For an SR-PCE provider, it is typically HTTP and port 8080.

Step 4   Check your firewall setting and network configuration.

Step 5   Check the Cisco SR-PCE host or intervening devices for Access Control List settings that might limit who can connect.

Multiple Cisco SR-PCE HA Pairs

You can set up to eight Cisco SR-PCE HA pairs (total of 16 SR-PCEs) to ensure high availability (HA). Each HA pair of Cisco SR-PCE providers must have matching configurations, supporting the same network topology. In HA, if the primary SR-PCE becomes unreachable, Cisco Crosswork Optimization Engine uses the secondary SR-PCE to discover the network topology. If this pair fails, then the next HA pair takes over and so forth. The network topology will continue to be updated correctly and you can view SR-PCE connectivity events in the Events table ( ).

Multiple HA Pairs

In the case of multiple SR-PCE HA pairs, each SR-PCE pair sees the same topology but manages and only knows about tunnels created from its Path Computation Clients (PCCs). The following figure is a sample of a three SR-PCE HA pair topology. Note the following:

- HA Pair 1—PCE iosxrv-1 and iosxrv-2 provisions and discovers *only* tunnels whose headends are iosxrv-7 and iosxrv-8. Note that iosxrv-9 and iosxrv-10 are not PCC routers.

- HA Pair 2—PCE iosxrv-3 and iosxrv-4 provisions and discovers *only* tunnels whose headends are iosxrv-11, iosxrv-12, iosxrv-17, and iosxrv-18. Note that iosxrv-13, iosxrv-14, iosxrv-15, and iosxrv-16 are not PCC routers.

- HA Pair 3—PCE iosxrv-5 and iosxrv-6 provisions and discovers *only* about tunnels whose headends are iosxrv-21, and iosxrv-22. Note that iosxrv-19, and iosxrv-20 are not PCC routers.

Figure 6: Sample 3 HA Pair Topology
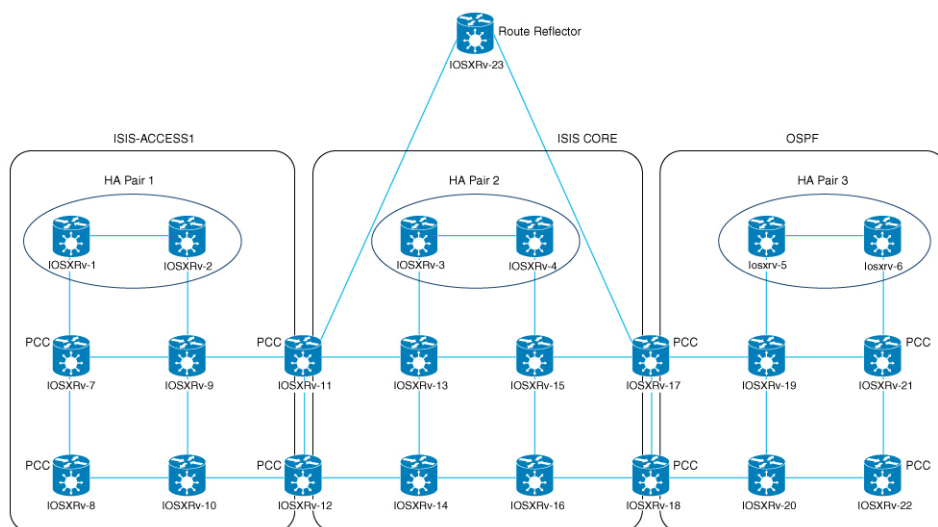
Note   If any of the SR-PCEs are included in a *subset* of the main network topology, then that SR-PCE provider must be added with the Property Key as **topology** and the Property Value as **off**. When this value is set, then this SR-PCE will not be used to learn the topology.

Configure HA

The following configurations must be done to enable each pair of HA Cisco SR-PCE providers to be added in Cisco Crosswork Optimization Engine.

Note   There must be resilient IPv4 connectivity between both SR-PCEs to enable HA. The PCE IP address of the other SR-PCE should be reachable by the peer at all times.

Issue the following commands on *each* of the Cisco SR-PCE devices:

Enable the interface:

```
# interface <interface><slot>/<port>
ipv4 address <sync-link-interface-ip-address> <subnet-mask>
no shut
```

Enable HA:

```
# pce api sibling ipv4 <other-node-pce-address>
```

Establish a sync link between the two SR-PCEs:

```
# router static
address-family ipv4 unicast
<other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

(Optional) `# pce segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>`

It should be entered for each PCC and not for other PCE nodes.

Issue the following command on the PCC:

For SR Policies: `# segment-routing traffic-eng pcc redundancy pcc-centric`

For RSVP-TE Tunnels: `# mpls traffic-eng pce stateful-client redundancy pcc-centric`

Confirm Sibling SR-PCE Configuration

From the SR-PCE, enter the `show tcp brief` command to verify synchronization between SR-PCEs in HA are intact:

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

Confirm that following information is correct:

Local Address	Foreign Address	State
<local-SR-PCE-router-id>:8080	*<remote-SR-PCE-router-id>*:*<any-port-id>*	ESTAB
<local-SR-PCE-router-id>:*<any-port-id>*	*<remote-SR-PCE-router-id>*:8080	ESTAB

For example:

```
RP/0/0/CPU0:iosxrv-1#sh tcp brief | i 192.168.0.2:
Mon Jun 22 18:43:09.044 UTC
0x153af340 0x60000000 0 0 192.168.0.1:47230 192.168.0.2:8080 ESTAB
0x153aaa6c 0x60000000 0 0 192.168.0.1:8080 192.168.0.2:16765 ESTAB
```

In this example, 192.168.0.2 is the remote SR-PCE IP.

SR-PCE Delegation

Depending on where an SR-TE policy is created, the following SR-PCE delegation occurs:

- SR-PCE initiated—Policies configured on a PCE. SR-TE policies are delegated back to the source SR-PCE.

Note
- The policy can be PCE initiated even if it is created using the UI, but in that case it is not configured explicitly on SR-PCE.

- RSVP-TE tunnels cannot be configured directly on a PCE.

- PCC initiated—An SR-TE policy or RSVP-TE tunnel that is configured directly on a device. The SR-PCE configured with the lowest precedence is the delegated SR-PCE. If precedence is not set, then SR-PCE with the lowest PCE IP address is the delegated SR-PCE. The following configuration example, shows that **10.0.0.1** is assigned a precedence value of 10 and will be the delegated SR-PCE.

```
segment-routing
  traffic-eng
    pcc
      source-address ipv4 10.0.0.2
      pce address ipv4 10.0.0.1
        precedence 10
       !
      pce address ipv4 10.0.0.8
        precedence 20
       !
       report-all
       redundancy pcc-centric
```

For RSVP-TE Tunnel:

```
mpls traffic-eng
interface GigabitEthernet0/0/0/0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
!
pce
  peer source ipv4 192.168.0.02
  peer ipv4 192.168.0.9
    precedence 10
  !
  peer ipv4 192.168.0.10
    precedence 20
  !
  stateful-client
   instantiation
   report
```

```
     redundancy pcc-centric
     autoroute-announce
    !
  !
 auto-tunnel pcc
   tunnel-id min 1000 max 5000
```

- Cisco Crosswork SR-PCE initiated—An SR-TE policy that is configured using Cisco Crosswork. SR-PCE delegation is random per policy.

> **Note** Only SR-TE policies or RSVP-TE tunnels created by Cisco Crosswork Optimization Engine can be modified or deleted by Cisco Crosswork Optimization Engine.

HA Notes and Limitations

- It is assumed that all PCCs are PCEP connected to both SR-PCEs.

- When an SR-PCE is disconnected only from Cisco Crosswork, the following occurs:

  - SR-PCE delegation assignments remain, but the SR-PCE that has been disconnected will not appear in Cisco Crosswork.

  - You are not able to modify Cisco Crosswork SR-PCE initiated SR-TE policies if the disconnected SR-PCE is the delegated PCE.

- In some cases, when an SR-TE policy that was created via the UI is automatically deleted (intentional and expected) from Cisco Crosswork Optimization Engine, a warning message does not appear. For example, if the source PCC is reloaded, the UI created SR policy disappears and the user is not informed.

- In an extreme case where one SR-PCE fails on all links (to PCCs/topology devices) except the up-link to Cisco Crosswork Optimization Engine, then topology information will not be accurate in Cisco Crosswork Optimization Engine. When this happens, fix the connectivity issue or delete both SR-PCEs from the Provider page and re-add the one that is reachable.

SR-PCE Configuration Examples

The following configurations are *examples* to guide you in a multiple SR-PCE setup for HA. Please modify accordingly.

Sample redundant SR-PCE configuration (on PCE with Cisco IOS-XR 7.x.x)

```
pce
 address ipv4 192.168.0.7
 state-sync ipv4 192.168.0.6
 api
  sibling ipv4 192.168.0.6
```

Sample redundant SR-PCE Configuration (PCC)

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 192.0.2.1
   pce address ipv4 192.0.2.6
```

```
 precedence 200
 !
 pce address ipv4 192.0.2.7
 precedence 100
 !
 report-all
 redundancy pcc-centric
```

Sample redundant SR-PCE Configuration (on PCC) for RSVP-TE

Note   `Loopback0` represents the TE router ID.

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mpls traffic-eng
 pce
  peer source ipv4 209.165.255.1
  peer ipv4 209.165.0.6
   precedence 200
  !
  peer ipv4 209.165.0.7
   precedence 100
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
 !
 auto-tunnel pcc
  tunnel-id min 1000 max 1999
 !
!
```

Sample SR-TM Configuation

```
telemetry model-driven
 destination-group crosswork
  address-family ipv4 198.18.1.219 port 9010
   encoding self-describing-gpb
   protocol tcp
  !
 !
 sensor-group SRTM
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes

  !
 subscription OE
  sensor-group-id SRTM sample-interval 60000
  destination-id crosswork
  source-interface Loopback0
!
traffic-collector
 interface GigabitEthernet0/0/0/3
 !
 statistics
  history-size 10
```

> ✎
>
> **Note** The destination address uses the southbound data interface (eth1) address of the Cisco Crosswork Data Gateway VM.

It is required to push sensor path on telemetry configuration via NSO to get prefix and tunnel counters. It is assumed that the Traffic Collector has been configured with all the traffic ingress interface. This configuration is needed for demands in the Bandwidth on Demand and Bandwidth Optimization function packs to work.

Telemetry Sensor Path

```
sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
```

Telemetry configuration pushed by Cisco Crosswork Optimization Engine to all the headend routers via NSO

```
telemetry model-driven
  destination-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
    vrf default
    address-family ipv4 172. 19.68.206 port 31500
      encoding self-describing-gpb
      protocol top
    !
  !
destination-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  vrf default
  address-family ipv4 172. 19.68.206 port 31500
    encoding self-describing-gpb
    protocol top
  !
!
sensor-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
sensor-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
!
subscription CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-group-id CW_43dc8a5ea99529715899b4f5218408a785e40fce sample-interval 300000
  destination-id CW_43dc8a5ea99529715899b4f5218408a785e40fce
!
subscription CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-group-id CW_4b3c69a200668b%a8dc155caff295645c684a8f8 sample-interval 300000
  destination-id CW_463c69a200668b0a8dc155caff295645c684a8f8
  !
!
```

Traffic Collector configurations (all Ingress traffic interface to be added below in the Traffic Collector)

```
RP/0/RSP0/CPU0:PE1-ASR9k#sh running-config traffic-collector
Fri May 22 01:14:35.845 PDT
traffic-collector
  interface GigabitEthernet0/0/0/0
  !
  statistics
    history-size 1
    collection-interval 1
    history-timeout 1
```

```
        history-minute-timeout
   !
!
```

Add BGP neighbor next-hop-self for all the prefix (to show TM rate counters)

```
bgp router-id 5.5.5.5
address-family ipv4 unicast
  network 5.5.5.5/32
  redistribute static
!
address-family link-state link-state
!
neighbor 1.1.1.1
  remote-as 65000
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
!
```

Traffic collector tunnel and prefix counters

```
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters prefix
Fri May 22 01:13:51.458 PDT
Prefix            Label         Base rate        TM rate         State
                                (Bytes/sec)      (Bytes/sec)
----------------  ------------  ---------------  --------------  -----------------
1.1.1.1/32        650001        3                0               Active
2.2.2.2/32        650002        3                0               Active
3.3.3.3/32        650003        6                0               Active
4.4.4.4/32        650004        1                0               Active
6.6.6.6/32        650200        6326338          6326234         Active
7.7.7.7/32        650007        62763285         62764006        Active
8.8.8.8/32        650008        31129168         31130488        Active
9.9.9.9/32        650009        1                0               Active
10.10.10.10/32    650010        1                0               Active
RP/0/RSP0/CPU0:PE1-ASR9k#stt
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters tunnel
Fri May 22 01:13:52.169 PDT
RP/0/RSP0/CPU0:PE1-ASR9k#]
```

Path Computation Client (PCC) Support

PCCs can support delegation and reporting of both RSVP-TE tunnels and SR policies to SR-PCE. In order for both to be supported on the same PCC, two separate PCEP connections must be established with the SR-PCEs. Each PCEP connection must have a distinct source IP address (Loopback) on the PCC.

The following is a Cisco IOS-XR configuration example of PCEP connections for RSVP-TE, where 192.168.0.2 is the PCEP session source IP for RSVP-TE tunnels delegated and reported to SR-PCE. It is a loopback address on the router. Two SR-PCEs are configured for PCEP sessions, where the first will be preferred for delegation of RSVP-TE tunnels due to precedence. Auto-tunnel PCC is configured with a range of tunnel IDs that will be used for assignment to PCE-initiated RSVP-TE tunnels like those created in Cisco Crosswork Optimization Engine.

```
mpls traffic-eng
interface GigabitEthernet0/0/0/2
admin-weight 1
!
interface GigabitEthernet0/0/0/3
admin-weight 1
  pce
```

```
        peer source ipv4 192.168.0.2
        peer ipv4 192.168.0.1
          precedence 10
          !
        peer ipv4 192.168.0.8
          precedence 11
          !
        stateful-client
          instantiation
          report
          !
      !
      auto-tunnel pcc
        tunnel-id min 10 max 1000
        !
  !
  ipv4 unnumbered mpls traffic-eng Loopback0

  rsvp
  interface GigabitEthernet0/0/0/2
  bandwidth 1000000
  !
  interface GigabitEthernet0/0/0/3
  bandwidth 1000000
  !
  !
```

Add Cisco WAE Providers

Cisco WAN Automation Engine (Cisco WAE) providers supply traffic and topology analysis to the Cisco Crosswork applications. The foundation software is Cisco WAE Planning, which provides a cross-sectional view of traffic, topology, and equipment state. It takes advantage of a predictive model that performs "what if" analysis of failure impacts.

Follow the steps below to use the UI to add one or more instances of Cisco WAE as providers. You can also add providers using CSV files (see Import Providers, on page 34).

Before you begin

You will need to:

- Create a credential profile for the Cisco WAE provider (see Create Credential Profiles, on page 2). This should be a basic HTTP/HTTPS text-authentication credential (currently, MD5 authentication is not supported). If the Cisco WAE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP/HTTPS protocol.

- Know the name you want to assign to the provider. This is usually the DNS hostname of the Cisco WAE server.

- Know the Cisco WAE server IP address and port. The connection protocol will be HTTP or HTTPS.

Step 1	From the main menu, choose **Administration** > **Manage Provider Access**.
Step 2	Click ➕.
Step 3	Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the Cisco WAE provider.

- **Credential Profile**: Select the previously created credential profile.

- **Family**: Select **WAE**.

- **Protocol**: Select **HTTP** or **HTTPS** respectively as per the credential profile you are using.

- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.

- **Port**: Enter the port number (usually, **8080** for HTTP, and **8843** for HTTPS).

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

Step 4   When you have completed entries in all of the required fields, click **Save** to add the provider.

Add Syslog Storage Providers

Storage providers supply storage for data collected during Playbook execution.

Follow the steps below to use the UI to add one or more storage providers. You can also add providers using CSV files (see).

Before you begin

You will need to:

- Create a credential profile for the storage provider (see). This should be an SSH credential.

- Know the name you want to assign to the storage provider. This is usually the DNS hostname of the server.

- Know the storage provider's server IPv4 address and port. The connection protocol will be SSH.

- Know the destination directory on the storage provider's server. You will need to specify this using the **Provider Properties** fields.

Step 1   From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2   Click ➕.

Step 3   Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the storage provider.

- **Credential Profile**: Select the previously created storage credential profile.

- **Family**: Select **SYSLOG_STORAGE**.

- **Protocol**: Select **SSH** to be protocol that Cisco Crosswork application will use to connect to the provider.

- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.

- **Port**: Enter the port number (usually, **22** for SSH.

- **Provider Properties**: Enter the following key/value pair in these fields:

Property Key	Property Value
DestinationDirectory	The absolute path where the collected data will be stored on the server. For example: **/root/cw-syslogs**

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the storage server.

Step 4   When you have completed entries in all of the required fields, click **Save** to add the syslog storage provider.

Add an Alert Provider

An Alert provider is a destination to which you want to forward alerts collected during KPI monitoring (such as Cisco Crosswork Situation Manager). An alert provider must be capable of receiving and processing incoming alert packages.

Follow the steps below to use the UI to add an alert provider. You can also add the alert provider by importing a CSV file (see Import Providers, on page 34).

Currently, only one alert provider is supported.

Before you begin

You will need to:

- Create a credential profile for the alert provider (see Create Credential Profiles, on page 2). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the provider does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.

- Know the name you want to assign to the alert provider. This is usually the DNS hostname of the server.

- Know the alert server IPv4 address and port. The connection protocol will be HTTP.

- Know the URL of the alert server endpoint. You will need to specify this using the **Property Value** field.

Step 1   From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2   Click ➕.

Step 3   Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the alert provider.

- **Credential Profile**: Select the previously created alert provider credential profile.

- **Family**: Select **ALERT**.

- **Protocol**: **HTTP** is pre-selected.

- **IP Address/ Subnet Mask**: Enter the IP Address (IPv4 or IPv6) and subnet mask of the alert server.

- **Port**: Enter the port number (usually, 80 for HTTP).

- **Provider Properties**: The **alertEndpointUrl** property key name is pre-entered. In the Property Value field, enter the alert server endpoint only. For example, if the complete path to the endpoint is **http://aws.amazon.com:80/myendpoint/bar1/**, you would enter **/myendpoint/bar1/** only.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the alert server.

Step 4   When you have completed entries in all of the required fields, click **Save** to add the alert provider.

Add Proxy Providers

This section explains how to add a proxy provider in Crosswork. Crosswork supports the addition of the following proxy providers:

- Cisco NSO

- Cisco Optical Network Controller (ONC) version 1.0

The NSO APIs can be directly accessed if NSO is configured with an externally accessible IP address. However, if NSO is deployed in the same private network as the Crosswork network, then it will be reachable only through the Crosswork interface. Proxy providers enables you to use Crosswork interface to perform service provisioning with NSO.

Before you begin

You will need to:

- Create a credential profile for the Proxy provider (see Create Credential Profiles, on page 2). This should be a basic HTTP or HTTPS text-authentication credential.

- Know the name of the Resource Facing Service (RFS) node added to the Customer Facing Service (CFS) node in your LSA cluster.

- Know the name you want to assign to the provider. This is usually the DNS hostname of the Proxy server.

- Know the Proxy server IP address and port. The connection protocol will be HTTP or HTTPS.

- Ensure that the Cisco NSO providers are added. For more information, see Add Cisco NSO Providers, on page 13.

• In case of NSO proxy provider, please create a credential profile with **HTTP/HTTPS** with **Basic Authentication**.

• In case of ONC 1.0 proxy provider, please create a credential profile with **HTTPS** with **Basic Authentication**.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click ![+] .

Step 3 Enter the following values for the provider fields:

• **Provider Name**: Name of the Proxy provider.

• **Credential Profile**: Select the previously created credential profile.

> **Note**   In case of ONC provider, please select the credential profile configured with ONC TAPI APIs. This is not the ONC UI credentials.

• **Family**: Select **PROXY**.

• **Protocol**: Select **HTTP** or **HTTPS**.

• **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the NSO cluster or the ONC 1.0 cluster VIP.

• **Port**: Enter the port number (usually, **30603** for HTTPS).

• **Timeout**: (Optional) The amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

Step 4 Under Provider Properties, enter the following properties:

Table 4: Provider Properties for NSO proxy provider

Property Key	Property Value
`forward`	`true`
`input_url_prefix` **Note** This property is required only in case of RFS nodes.	`/<rfs-node-name>` *<rfs-node-name>* refers to the name of the RFS node added to the CFS node in the LSA cluster.

Table 5: Provider Properties for ONC 1.0 proxy provider

Property Key	Property Value
`forward`	`true`
`input_url_prefix`	`/onc-tapi`
`output_url_prefix`	`/crosswork/onc-tapi`

Step 5   When you have completed entries in all of the required fields, click **Save** to add the provider.

Import Providers

Complete the steps below to create a CSV file that specifies providers and then import it into the Cisco Crosswork application.

Importing providers from a CSV file adds any providers not already in the database, and updates any providers with the same name as an imported provider. For this reason, it is a good idea to export a backup copy of all your current providers before an import (see Export Providers, on page 37).

Step 1   From the main menu, choose **Administration** > **Manage Provider Access**.

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

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

   a)   Click the **Download sample 'Provider template (*.csv)' file** link and save the CSV file template to a local storage resource.

   b)   Open the template using your preferred tool. Begin adding rows to the file, one row for each provider.

   Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate entries with semicolons, the order in which you enter values is important. For example, if you enter `SSH;SNMP;NETCONF;TELNET` in the **connectivity_type** field and you enter `22;161;830;23` in the **connectivity_port** field, the order of entry determines the mapping between the two fields:

   - SSH: port 22

   - SNMP: port 161

   - NETCONF: port 830

   - Telnet: port 23

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

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

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

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

The provider information you imported should now be displayed in the **Providers** window.

Step 6   Resolve any errors reported during the import and check provider details to confirm connection.

Get Provider Details

Use the **Providers** window to get details about your providers and to check on their reachability.

Step 1   From the main menu, choose **Administration** > **Manage Provider Access**.

For each provider configured in the Cisco Crosswork application, the **Providers** window lists information such as the provider's name, universally unique identifier (UUID), associated credential profile and more, as shown in the figure below.

Figure 7: Providers Window

Step 2   The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols. For more information, see Device State.

Cisco Crosswork application checks provider reachability immediately after a provider is added or modified. Other than these events, Crosswork Change Automation and Health Insights checks reachability every 5 minutes and Crosswork Optimization Engine checks SR-PCE reachability about every 10 seconds.

Step 3   Get additional details for any provider, as follows:

a) In the **Provider Name** column, click the ⓘ to view provider-specific key/value properties.

b) In the **Connectivity Type** column, click the ⓘ to view detailed connectivity information for the provider, such as provider-specific protocol, IP format, IP address, port, and timeout information.

c) In the **Model Prefix** column, click the ⓘ to view the supported NED version(s) for a Cisco Network Services Orchestrator (Cisco NSO) provider's configured NED model prefix(es).

d) When you are finished, click ✕ to close the details window.

If you are running into Cisco SR-PCE reachability problems, see Cisco SR-PCE Reachability Issues, on page 21. Check that HTTP and port 8080 is set.

For general provider reachability problems, you can troubleshoot as follows:

a. Ping the provider host.

b. Attempt a connection using the protocols specified in the connectivity settings for the provider. .

The following CLI command can be used to perform this check:

```
curl -v -H "X-Subscribe: stream" "http://<ip-address>:8080/
bwod/subscribe/json?keepalive-30&priority=5"
```

c. Check your firewall setting and network configuration.

d. Check the provider host or intervening devices for Access Control List settings that might limit who can connect.

Edit Providers

When editing provider settings, be aware that a provider can be mapped to many devices, even thousands of devices in a large network.

Note
- Before making any changes to a provider configuration you should be certain that you understand the full impact of the change. If you are unsure about the potential risk of making a change, contact Cisco services for guidance.

- See Add Cisco SR-PCE Providers, on page 18 before modifying an SR-PCE provider. There are additional steps that must be done when editing an SR-PCE provider.

.

Before editing any provider, it is always good practice to export a CSV backup of the providers you want to change (see Export Providers, on page 37).

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 In the **Providers** window, choose the provider you want to update and click ✎.

Step 3 Make the necessary changes and then click **Save**.

Step 4 Resolve any errors and confirm provider reachability.

Delete Providers

Follow the steps below to delete a provider.

You are alerted when you try to delete a provider that is associated with one or more devices or credential profiles.

Step 1 Export a backup CSV file containing the provider you plan to delete (see Export Providers, on page 37).

Step 2 (Optional) Check whether any devices are mapped to the provider and change the provider before deletion.

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

b) In the **Network Devices** window, enter the obsolete provider name in the **Search** field.

c) Check the check box for the device that is mapped to the obsolete provider, and click ✎.

d) Choose a different provider from the **Provider** drop-down list.

e) Click **Save**.

Step 3 Delete the provider as follows:

a) From the main menu, choose **Administration** > **Manage Provider Access**.

b) In the **Providers** window, choose the provider(s) that you want to delete and click 🗑.

c) In the confirmation dialog box, click **Delete**.

Export Providers

You can quickly export provider data to a CSV file. This is a handy way to keep backup copies of your provider information.

Note You cannot edit a CSV file and then re-import it to update existing providers.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 (Optional) In the **Providers** window, filter the provider list as needed.

Step 3 Check the check boxes for the providers you want to export. Check the check box at the top of the column to select all the providers for export.

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

Manage Tags

Use the **Tag Management** window to manage the tags available for assignment to the devices in your network. Tags can provide information such as the device's physical location and its administrator's email ID, and are used to group devices.

To open this window, choose **Administration** > **Tags**.
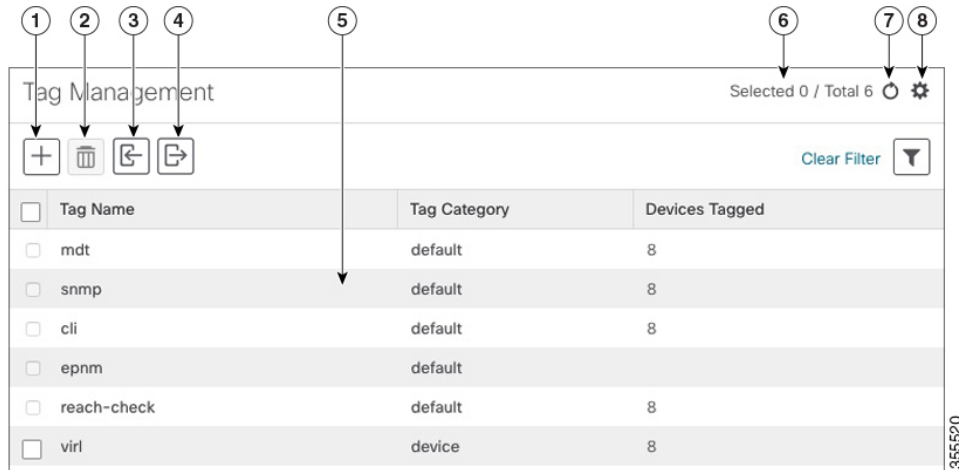
Note Cisco Crosswork applications automatically create a default set of tags and assign them to every device they manage:

- cli

- mdt

- reach-check

- snmp

- clock-drift-check

You cannot select, edit, delete, or manually associate these default tags with any device.

Figure 8: Tag Management Window

Item	Description
1	Click ➕ to create new device tags. See Create Tags, on page 39.
2	Click 🗑 to delete currently selected device tags. See Delete Tags, on page 41.
3	Click ⬇ to import the device tags defined in a CSV file into the Cisco Crosswork application. See Import Tags, on page 39. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file.
4	Click ⬆ to export a CSV file that lists the tags that are currently configured and their attributes. You can update this file and import it back into the Cisco Crosswork application to quickly add or edit multiple tags. See Export Tags, on page 41.
5	Displays the tags and their attributes currently available in the Cisco Crosswork application.
6	Indicates the number of tags that are currently selected in the table.
7	Click ⟳ to refresh the **Tag Management** window.
8	Click ⚙ to choose the columns to make visible in the **Tag Management** window.
	Click ≡ to set filter criteria on one or more columns in the **Tag Management** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

Create Tags

You can create as many tags and tag categories as you want. If you will have many tags, it might be quicker to list them in a CSV file and import the file, instead of creating each tag individually. See Import Tags, on page 39.

✎

Note
- Tag and tag category names are case-insensitive and can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.

- The maximum number of tags that you can create is 100.

Step 1 From the main menu, choose **Administration** > **Tags**. The **Tag Management** window opens.

Step 2 Click ➕. The **Create New Tags** pane opens.

Step 3 In the **Category** area:

- To associate your new tags with an existing category: Choose the category from the drop-down list.

- To associate your new tags with a new category: Click the **New Category** link, enter the new category's name in the text field, and click **Save**.

All the new tags you create after this step will be assigned to the category you selected or created.

Step 4 In the **Tags** area: Start entering the names of the new tags that you want to create. Press **Return** after you type each tag.

To keep from entering duplicate tags, click the **Show Tags** link. The **Create New Tags** window will list only the tags that already exist in your currently selected category.

Step 5 When you are finished entering new tags, click **Save**.

What to do next

Add tags to devices. See Apply or Remove Device Tags, on page 40.

Import Tags

Complete the steps below to create a CSV file that lists the tags you want to apply to your devices, and then import it into the Cisco Crosswork applications. This is the easiest way to create a lot of new tags and tag categories quickly.

When you import the CSV file, any tags not already in the database will be added. Tags with the same name as an imported tag will be overwritten. For this reason, it is a good idea to export a backup copy of all your current tags before import (see Export Tags, on page 41).

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

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

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

a) Click the **Download sample 'Tags template (*.csv)' file** link and save the CSV file template to a local storage resource.

b) Open the template using your preferred tool. Begin adding rows to the file, one row for each tag. Use a comma to delimit each field within a row. Use a semicolon to separate multiple entries in the same field.

Field	Description	Required or Optional
Tag Name	Enter the name of the tag. For example: `SanFrancisco` or `Spine/Leaf`.	Required
Tag Category	Enter the tag category. For example: `City` or `Network Role`.	Required

Note   **Tag Name** and **Tag Category** fields are case-insensitive and can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.

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

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

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

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

The tags and tag categories that you imported should now be displayed in the **Tag Management** window.

What to do next

Add tags to devices. See .

Apply or Remove Device Tags

Tags and their categories are your main tool for grouping devices. Once you have tagged a set of devices with the same tag, they are considered part of a group, and you can manage them more easily.

In order to apply a tag to a device or group of devices, the tag must already exist (see).

For efficiency, Cisco Crosswork automatically updates inventory data, including topology, for all the devices in a tagged group, as a single set of inventory collection jobs. But please note that tag-group membership is static for other functions.

You can apply a maximum of 15 tags to any one device.

To apply tags to a device or set of devices, do the following:

Step 1   From the main menu, choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed, showing the list of devices.

Step 2   (Optional) If the list is long, click ☰ to set one or more filters and narrow the list to only those devices you want to tag.

Step 3   Check the check box next to the device(s) you want to tag. If you select multiple devices, any changes you make will be applied to all the devices you selected.

Step 4   From the toolbar, click ⬛. The **Modify Tags** window opens, showing the tags currently applied to the device(s) you selected.

Step 5   Click in the **Type to autocomplete item** field to display the list of existing tags, or begin typing the name of the tag you want.

Step 6   Click on individual tags in the list to add them to the list of tags applied to the device(s). To delete an applied tag, click the X icon shown next to that tag.

Delete Tags

To delete device tags, do the following:

✎

Note   If the tag is mapped to any devices, then the tag cannot be deleted.

Step 1   Export a backup CSV file containing the tags you plan to delete (see Export Tags, on page 41).

Step 2   From the main menu, choose **Administration** > **Tags**. The **Tag Management** window is displayed.

Step 3   Check the check box next to the tags you want to delete.

Step 4   From the toolbar, click ⬛.

Step 5   The confirmation dialog box will list the number of devices currently using the tag(s) you are about to delete. Click **Delete** to confirm deletion.

Export Tags

You can quickly export tags and tag categories to a CSV file. This will allow you to keep backup copies of your tags. You can also edit the CSV file as needed, and re-import it to overwrite existing tags. Note that you will need to re-associate devices and tags in some cases.

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

Step 2   (Optional) In the **Tag Management** window, filter the tag list as needed.

Step 3   Check the check boxes for the tags you want to export. Check the check box at the top of the column to select all the tags for export.

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