



# Manage Inventory

---

This section contains the following topics:

- [Inventory Management Overview](#), on page 1
- [About Adding Devices](#), on page 1
- [Prerequisites for Onboarding Devices](#), on page 3
- [Sample Configuration for Devices in Cisco NSO](#), on page 4
- [Reachability and Operational State](#), on page 5
- [Manage Credential Profiles](#), on page 7
- [Manage Providers](#), on page 14
- [Manage Devices](#), on page 27
- [Manage Tags](#), on page 40

## Inventory Management Overview

The application lets you create, edit, and delete:

- The **credential profiles** that control Crosswork Optimization Engine's access to devices and providers. See [Manage Credential Profiles](#), on page 7.
- The **providers** who supply special services, such as device configuration, data storage, or alert processing, to Crosswork Optimization Engine. See [Manage Providers](#), on page 14.
- The **devices** you manage using Crosswork Optimization Engine. See [Manage Devices](#), on page 27.
- The **tags** you use to sort and group devices. See [Manage Tags](#), on page 40.

You can also use to review the **jobs** executed on your devices. See [View Device Job History](#), on page 39.

## About Adding Devices

There are two ways to add devices to Cisco Crosswork Optimization Engine:

1. Automatically onboard devices and populate the inventory.
2. Manually onboard devices using a CSV file or the UI.

## Auto-Onboard Devices

Auto-onboarding simplifies and expedites the device onboarding process. It automatically discovers and imports preformatted device data from a Cisco SR-PCE provider and enables you to quickly view the IGP topology (including devices, links and IP addresses) in the Cisco Crosswork Optimization Engine topology map.

To configure auto-onboarding, you add an SR-PCE provider with one of the following auto-onboard options: **managed** or **unmanaged**.

The auto-onboard **managed** option requires a single default credential profile (having SNMP access, at minimum) that will work for all devices.

The devices are auto-onboarded with the following attributes::

- The OSPF Router ID or TE Router ID is assigned as the **Node IP** of the device. **Node IP** is configured as the Device Key Type.
- For devices running IS-IS, a **Hostname** is assigned. It is not available for OSPF.
- The **Connectivity IP** is assigned the same value as the **Node IP**.
- The default credential profile is set as the **Credential Profile** for each device.



### Note

If a common credential profile cannot be used for all devices, or a different **Connectivity IP** is required, use the auto-onboard **unmanaged** option or Cisco Crosswork Optimization Engine will keep trying to connect to the devices and fail.

The auto-onboard **unmanaged** option should be used if you prefer devices not to be assigned a **Credential Profile** or **Connectivity IP**. SNMP or any other device collection is not performed. However, IGP topology is still seen on the topology map (logical view), but the information available is restricted to the information SR-PCE provides. Therefore, interface names are not shown, and in the case of OSPF, device Hostnames are also not shown. IP addresses are shown and can be used to identify devices and interfaces.

### Auto-Onboard Notes and Limitations:


Consider the following information when choosing between **unmanaged** and **managed** options:

- The OSPF or TE router ID is used as the Connectivity IP of the device. This is the IP address Cisco Crosswork Optimization Engine will use to perform SNMP or CLI collection from the device. If the devices need to be reached over a separate management network, the Connectivity IP of all devices will need to be updated using the CSV **Update Existing** option (see [Import Devices, on page 28](#)). In this case, use the **unmanaged** option for auto-onboarding to prevent repeated unsuccessful collection attempts from the devices.
- The **managed** option works only if a single **Credential Profile** will work for accessing all the devices.
- With the **unmanaged** option, since SNMP collection from the devices cannot be performed, interface names and possibly hostnames will not be available until the devices in inventory are updated with the correct **Connectivity IP** and **Credential Profile** and their state is updated to Managed.
- Several device attributes cannot be discovered and need to be manually supplied. After the inventory is populated, you can download the device inventory CSV file, edit the file to add additional information (such as geographical location), and import it back into Cisco Crosswork Optimization Engine using the CSV **Update Existing** option. See [Import Devices, on page 28](#) and [Export Devices, on page 38](#).

To quickly get up and running with Cisco Crosswork Optimization Engine, follow the high-level steps documented in [Workflow: Auto-Onboard Devices](#).

### Manually Add Devices

You can manually onboard devices from a CSV file or add them using the UI. After adding credential profiles, configure providers and tags to group new devices (optional) you do one of the following:

- Download the CSV template file from **Inventory Management > Devices** >  and populate it with all the devices you will need (see [Import Devices, on page 28](#)). This method can be time consuming, as you must create and enter all of the data yourself beforehand (including not only devices, but also the providers, credential profiles and tags), and then ensure all of these items are properly associated with the devices.

To quickly get up and running with Cisco Crosswork Optimization Engine by importing devices, follow the high-level steps documented in [Workflow: Manually Import Devices](#).

- Add devices using the UI (see [Add Devices Through the UI, on page 30](#)). It is the most time-consuming since all data is validated during entry.

## Prerequisites for Onboarding Devices

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




---

**Note** Only users configured with privilege level 15 can use the NETCONF APIs. Privilege level 15 can be used to configure the "enable" password option in XE devices. In such cases, NETCONF must not be included as one of the protocols to verify reachability and operational state for the onboarded devices.

---

### Pre-Onboarding SNMP v2 Device Configuration

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and Telnet rate limits. The NETCONF setting is only needed if the device is MDT-capable (XR 612 or higher).

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
line default
  exec-timeout 0 0
  width 107
  length 37
  absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
  server <NTPServerIPAddress>
```

```

!
service cli history size 5000
service cli interactive disable
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
grpc
  port 57400
!
netconf agent tty
!
netconf-yang agent
  ssh
!

```

### Pre-Onboarding SNMPv3 Device Configuration

If you want to enable SNMPv3 data collection, repeat the SNMPv2 configuration commands in the previous section, and add the following commands:

```

snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>

```

## Sample Configuration for Devices in Cisco NSO

If you plan to use Cisco NSO as a provider to configure devices managed by Cisco Crosswork Optimization Engine, be sure that the Cisco NSO device configurations observe the following guidelines.

The following example shows a Cisco NSO setup that uses the hostname as the device ID. If you are using a CSV file to import devices, use **ROBOT\_PROVDEVKEY\_HOST\_NAME** as the enum value for the `provider_node_key` field. The example hostname **RouterFremont** used here must match the hostname for the device in the CSV file.

```

configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 22

```

The authgroup username and password in the CSV file must match the username and password in the credential profile associated with the Cisco NSO provider. For example:

```

set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type cli ned-id cisco-ios-xr
set devices device Router* authgroup cisco

```

The device itself must be synchronized with Cisco NSO before you import that device. For example:

```









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





```

# Reachability and Operational State

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

**Table 1: Reachability and Operational State Icons**

This Icon...	Indicates...
<b>Reachability State</b> icons show whether a device or a provider is reachable or not	
	Reachable: The device or provider can be reached by all configured protocols configured for it.
	Reachability Degraded: The device or provider can be reached by at least one protocol, but is not reachable by one or more of the other protocols configured for it.
	Unreachable: The device or provider cannot be reached by any protocol configured for it.
	Reachability Unknown: Cisco Crosswork Optimization Engine cannot determine if the device is reachable, degraded, or unreachable.
<b>Operational State</b> icons show whether a device is operational or not.	
	The device is operational and under management, and all individual protocols are "OK" (also known as "up").
	The device is not operational ("down"). The same icon is used when the device has been set "administratively down" by an operator.
	The device's operational or configuration state is unknown.
	The device's operational or configuration state is degraded.

This Icon...	Indicates...
	The device's operational or configuration state is in an error condition. It is either not up, or unreachable, or both, due to errors encountered while attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of recent errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available in the Network Topology application.)
	The device's operational state is currently being checked
	The device is being deleted.
	The device is unmanaged.

The Reachability State of a device is computed as follows:

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

The Operational State of a device is computed as follows:

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


**Note**

Confirm that devices have Telnet/SSH enabled. If it is not enabled, the Clock Drift throws an error and the operational state will always show a clock synchronization error.

# 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.

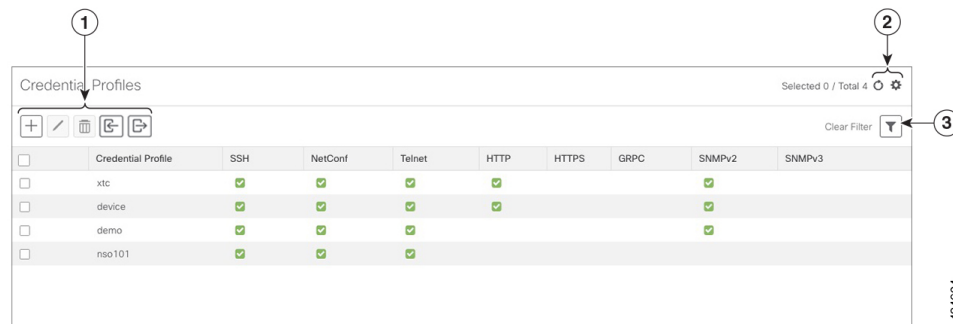
Using credential profiles lets you automate device configuration changes and monitoring, and communicate with providers. When you add or import devices, or create providers, you specify the credential profile(s) those devices and providers use.






**Note** Credentials just validates authentication since the corresponding protocol configured on the devices does the work. Devices should be present in the **Devices** window and be reachable.

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 **Inventory Management > Credentials** from the main menu.

**Figure 1: Credentials Profile window**



Item	Description
1	Click  to add a credential profile. See <a href="#">Create Credential Profiles, on page 8</a> .
	Click  to edit the settings for the selected credential profile. See <a href="#">Edit Credential Profiles, on page 12</a> .
	Click  to delete the selected credential profile. See <a href="#">Delete Credential Profiles, on page 12</a> .
	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 <a href="#">Import Credential Profiles, on page 10</a> .
	Click  to export credential profiles to a CSV file. See <a href="#">Export Credential Profiles, on page 13</a> .

Item	Description
2	Click  to refresh the <b>Credential Profiles</b> window.
	Click  to choose the columns to make visible in the <b>Credential Profiles</b> window (see <a href="#">Set, Sort and Filter Table Data</a> ).
3	Click  to set filter criteria on one or more columns in the <b>Credential Profiles</b> window.
	Click the <b>Clear Filter</b> 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 10](#)


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

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

- All the characters in each password or community string entry in every credential profile exported to a CSV file are replaced with asterisks ([Export Credential Profiles, on page 13](#)).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see [Import Credential Profiles, on page 10](#)).


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

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

**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 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** Click the  next to **Add Protocol Credentials**.

**Step 5** Select a protocol from the **Connectivity Type** dropdown.



**Step 6** Complete the credentials fields described in the following table. The required and optional fields displayed will vary with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
SSH	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> . The <b>Enable Password</b> is optional.
SNMPv2	Enter the required SNMPv2 <b>Read Community</b> string. The <b>Write Community</b> string is optional.
NETCONF	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
TELNET	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> . The <b>Enable Password</b> is optional.
HTTP	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
HTTPS	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
GRPC	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
SNMPv3	<p>Choose the required <b>Security Level</b> and enter the <b>User Name</b>.</p> <p>If you chose the NO_AUTH_NO_PRIV <b>Security Level</b> of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional.</p> <p>If you chose the AUTH_NO_PRIV <b>Security Level</b>, you must choose an <b>Auth Type</b> and enter an <b>Auth Password</b>.</p> <p>If you chose the AUTH_PRIV <b>Security Level</b>, you must choose an <b>Auth Type</b> and <b>Priv Type</b>, and enter an <b>Auth Password</b> and <b>Priv Password</b>.</p> <p>Only the following SNMPv3 Privacy Types are supported</p> <ul style="list-style-type: none"> <li>• CFB_AES_128</li> <li>• CBC_DES_56</li> </ul> <p>The following Privacy Types are not supported:</p> <ul style="list-style-type: none"> <li>• AES192</li> <li>• AES256</li> <li>• 3DES</li> </ul>

**Step 7** Repeat steps 4 through 7, as needed, for all other protocols and corresponding credentials you want to add to this credential profile.

**Step 8** Click **Save**.

## Import Credential Profiles

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

Importing credential profiles from a CSV file adds any profiles not already in the database. You cannot import a device credential 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 12](#) to replace the asterisks with actual passwords and community strings.

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

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

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

- a) Click the **Download sample 'Credential template (\*.csv)' file** link and save the CSV file template to your local disk.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each credential profile.

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

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

Also note:

- Be sure to enter SNMP community string information exactly as currently entered on your devices. Failure to do so may result in loss of device connectivity.
- 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: <b>srpce</b> .	Required

Field	Entries	Required or Optional
<b>Connectivity Type</b>	Valid values are: <b>SSH</b> , <b>SNMPv2</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , <b>HTTPS</b> , <b>GRPC</b> or <b>SNMPv3</b>	<ul style="list-style-type: none"> <li>• Devices—SNMP and SSH (to avoid operational errors due to clock synchronization checks) are required.</li> <li>• SR-PCE—Since SR-PCE is considered a provider and a device, SSH, and HTTP are required.</li> </ul>
<b>User Name</b>	For example: <b>SRPCEUser</b>	Required if <b>Connectivity Type</b> is <b>SSH</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , <b>HTTPS</b> , <b>SNMPv3</b> or <b>GRPC</b> .
<b>Password</b>	The password for the preceding <b>User Name</b> .	Required if <b>Connectivity Type</b> is <b>SSH</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , <b>HTTPS</b> or <b>GRPC</b>
<b>Enable Password</b>	Use the Enable password. Valid Values are: <b>ENABLE</b> , <b>DISABLE</b> , or leave blank (unselected)	
<b>Enable Password Value</b>	The Enable password to use.	Required only if <b>Enable Password</b> is set to <b>Enable</b> .
<b>SntpV2 Read Community</b>	For example: <b>readprivate</b>	Required if <b>Connectivity Type</b> is <b>SNMPv2</b>
<b>SntpV2 Write Community</b>	For example: <b>writeprivate</b>	
<b>SntpV3 User Name</b>	For example: <b>DemoUser</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b>
<b>SntpV3 Security Level</b>	Valid values are <b>noAuthNoPriv</b> , <b>AuthNoPriv</b> or <b>AuthPriv</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b>
<b>SntpV3 Auth Type</b>	Valid values are <b>HMAC_MD5</b> or <b>HMAC_SHA</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SntpV3 Security Level</b> is <b>AuthNoPriv</b> or <b>AuthPriv</b>
<b>SntpV3 Auth Password</b>	The password for this authorization type.	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SntpV3 Security Level</b> is <b>AuthNoPriv</b> or <b>AuthPriv</b>
<b>SntpV3 Priv Type</b>	Valid values are <b>CFB_AES_128</b> or <b>CBC_DES_56</b>  The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SntpV3 Security Level</b> is <b>AuthPriv</b>
<b>SntpV3 Priv Password</b>	The password for this privilege type.	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SntpV3 Security Level</b> is <b>AuthPriv</b>

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 **Devices** window.

## Edit Credential Profiles

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



**Warning** Changing the settings in a credential profile without first changing the settings on the device associated with the profile may result in a loss of connectivity.

Before editing any credential profile, it is always good practice to export a CSV backup of the profiles you want to change (see [Export Credential Profiles, on page 13](#)).

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

**Step 2** From the left-hand side of the **Credential Profiles** window, click the profile you want to update.

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

## 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 13](#)).

**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 **Inventory Management > Credentials**) and the **Providers** window (choose **Inventory Management > Providers**).

**Step 3** Reassign the devices or providers to a different credential profile (for help with this task, see [Change a Device's Credential Profile, on page 13](#) or [Change the Credential Profile for Multiple Devices, on page 14](#), and [Edit Providers, on page 25](#)).

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

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

---

## Export Credential Profiles

Exporting credential profiles stores all the profiles you selected in a CSV file. This is a quick way to make backup copies of your credential profiles. You can also edit the CSV file as needed, and re-import it to add new credential profile data. You cannot overwrite existing credential profiles by importing a CSV file.


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

---

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

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

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

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

---

## Change a Device's Credential Profile

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

### Before you begin

You need a credential profile to complete this task. To create a credential profile, see [Create Credential Profiles, on page 8](#).




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

---

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

**Step 2** (Optional) In the **Devices** window, filter the device list by entering text in the **Search** field or filtering specific columns.

**Step 3** Check the check box of the device you want to change, and click .

**Step 4** Choose a different credential profile from the **Credential Profile** drop-down list.

**Step 5** Click **Save**.

---

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

## Change the Credential Profile for Multiple Devices

If you want to change the credential profile for a large number of 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 Devices, on page 38](#)).
2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist). Save the edited file.
3. Import the edited devices CSV file using the **Update Existing** option. You will overwrite the credential profile data for each device (see [Import Devices, on page 28](#)).

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 **Inventory Management > Devices**.

**Step 2** In the **Devices** window, 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** In the **Devices** window, click .

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

---

## Manage Providers

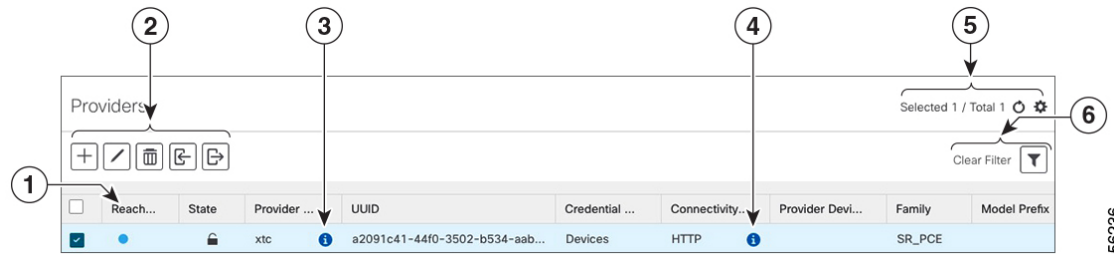
Cisco Crosswork Optimization Engine communicates with SR-PCE and NSO providers. Cisco Crosswork Optimization Engine stores the provider connectivity details and makes that information available to applications.



**Note** Other providers are available on the UI. However, they are not used by Cisco Crosswork Optimization Engine. They are used by other Cisco Network Automation applications.




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

**Figure 2: Providers window**



356236

Item	Description
1	The icon shown next to the provider in this column indicates the provider's <b>Reachability</b> . For more on the icons and how reachability is determined, see <a href="#">Reachability and Operational State, on page 5</a> .
2	Click  to add a provider. See <a href="#">Add Cisco SR-PCE Providers, on page 16</a> . Click  to edit the settings for the selected provider. See <a href="#">Edit Providers, on page 25</a> . Click  to delete the selected provider. See <a href="#">Delete Providers, on page 25</a> . 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 <a href="#">Import Providers, on page 22</a> . Click  to export a provider to a CSV file. See <a href="#">Export Providers, on page 26</a> .
3	Click  next to the provider in the <b>Provider Name</b> column to open the <b>Properties for</b> pop-up window, showing the details of any startup session key/value pairs for the provider.
4	Click  next to the provider in the <b>Connectivity Type</b> column to open the <b>Connectivity Details</b> pop-up window, showing the protocol, IP and other connection information for the provider.

Item	Description
5	Click  to refresh the <b>Providers</b> window.
	Click  to choose the columns to make visible in the Providers window (see <a href="#">Set, Sort and Filter Table Data</a> ).
6	Click  to set filter criteria on one or more columns in the <b>Providers</b> window.
	Click the <b>Clear Filter</b> link to clear any filter criteria you may have set.

## Add Cisco SR-PCE Providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers supply device discovery, management, configuration-maintenance and route-calculation services to Cisco Crosswork Optimization Engine. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices.

Follow the steps below to use the user interface to add up to two instances of Cisco SR-PCE as providers for Cisco Crosswork Optimization Engine.

### Before you begin

You will need to:

- Create a credential profile for the Cisco SR-PCE provider (see [Create Credential Profiles, on page 8](#)). 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.
- 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 **managed** or **unmanaged** when added. For more information, see [Auto-Onboard Property Descriptions, on page 18](#).
- 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.
- If you want to ensure high availability by setting up two Cisco SR-PCE providers and then using them both with Cisco Crosswork Optimization Engine, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but having matching configurations (see [Multiple Cisco SR-PCEs, on page 19](#)).

---

**Step 1** From the main menu, choose **Inventory Management > Providers**.



**Step 2** Click .

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

a) Required fields:

- **Provider Name:** Name of the SR-PCE provider that will be used in Cisco Crosswork Optimization Engine.
- **Credential Profile:** Select the previously created Cisco SR-PCE credential profile.
- **Family:** Select **SR\_PCE**. All other options should be ignored.
- **Protocol:** Select **HTTP**. All other options should be ignored.
- **IPv4 Address:** Enter the IPv4 address of the server.
- **Provider Properties:** Enter one of the following key/value pairs in the first set of fields (see [About Adding Devices, on page 1](#) and [Auto-Onboard Property Descriptions, on page 18](#)):

Property Key	Value
auto-onboard	off
auto-onboard	unmanaged
auto-onboard	managed

If you enter the **auto-onboard/managed** pair:

1. Click the  next to the first set of fields to add a new set.
2. In the new **Property Key** field, enter **device-profile**.
3. In the new **Property Value** field, enter the name of a credential profile that contains SNMP credentials for all the new devices.

b) Optional values:

- **IPv6 Address:** Leave blank. Reserved for future use.
- **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 shows a green Reachability status without any errors. You can also view the Events window to see if the provider has been configured correctly.



**Note** It is not recommended to modify auto-onboard options (**managed/unmanaged/off**) once set. If you need to modify them, do the following:

1. Delete the provider and wait until deletion confirmation is displayed in the Events page.
2. Re-add the provider with the updated auto-onboard option.
3. Confirm the provider has been added with the correct auto-onboard option in the Events page.

#### What to do next

- If you entered the **auto-onboard/off** pair, navigate to **Inventory Management > Devices** to add a device list (see [Import Devices, on page 28](#)).
- If you opted to automatically onboard devices, navigate to **Inventory Management > 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.

## Auto-Onboard Property Descriptions

The following table describes auto-onboard property provider fields.

Field	Description
<b>off</b>	If this option is enabled, you add or import devices manually (typically using a .csv file). When devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in Crosswork Optimization Engine Inventory Management database.
<b>unmanaged</b>	If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Optimization Engine Inventory Management database, with their configured state set to <b>unmanaged</b> . SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the <b>managed</b> state later, you will need to download them as a CSV file (see <a href="#">Export Devices, on page 38</a> ), and modify the CSV file to add the SNMP and management IP address information. You can then update the auto-onboarded devices with this information by importing the modified CSV file (see <a href="#">Import Devices, on page 28</a> ). You can also assign credential profile by adding them to the device CSV file before import (the credential profiles must already exist).
<b>managed</b>	If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Optimization Engine Inventory Management database, with their configured state set to <b>managed</b> . SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (Router ID). You will also need to add a second <b>Provider Properties</b> key/value pair, with the key <b>device-profile</b> and the value being the name of a credential profile for the new devices.



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

## 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 24](#)). 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** window 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, delete the SR-PCE and add it back (when connectivity returns) using the UI.

If you are running into provider reachability problems, you can troubleshoot 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.
- ```
curl --raw -vN "http://<hostname or ip-address>:8080/topology/subscribe/txt"
curl --raw -vN "http://<username>:<password>@"
```
- 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-PCEs

You can set up two Cisco SR-PCEs to ensure high availability (HA). The two 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. The network topology will continue to be updated correctly and you can view SR-PCE connectivity events in the Events table. To troubleshoot SR-PCE connectivity issues, see [Cisco SR-PCE Reachability Issues, on page 19](#).

### Configure HA

The following configurations must be done to enable HA when two Cisco SR-PCE providers are added in Cisco Crosswork Optimization Engine. There must be a direct link between both SR-PCE's to enable HA. The PCE IP address of the other SR-PCE should be reachable through this sync link.

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 rest 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>

Issue the following command on the PCC:

```
# segment-routing traffic-eng pcc redundancy pcc-centric
```

### SR-PCE Delegation

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

- SR-PCE initiated—An SR policy that is configured directly on an SR-PCE device. The source SR-PCE is delegated.
- PCC initiated—An SR policy 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
```

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




---

**Note** This is the only type of SR policy that Cisco Crosswork Optimization Engine can modify or delete (see [Create and Manage SR Policies](#)).

---

### 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 Optimization Engine, the following occur:
  - SR-PCE delegation assignments remain, but the SR-PCE that has been disconnected will not appear in Cisco Crosswork Optimization Engine.
  - You are not able to modify Cisco Crosswork Optimization Engine SR-PCE initiated SR policies if the disconnected SR-PCE is the delegated PCE.
- After an SR-PCE reloads, do the following:
  1. Execute the following command:

```
# process restart pce_server
```
  2. Remove the PCE sibling configuration in both SR-PCEs and then add the sibling configuration again.
- In some cases, when an SR 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.

## Add Cisco NSO Providers

Cisco Network Services Orchestrator (Cisco NSO) providers supply device management and configuration-maintenance services to Cisco Crosswork Optimization Engine.

Follow the steps below to add through the UI one or more instances of (Cisco NSO) as providers for Cisco Crosswork Optimization Engine. You can also add providers using CSV files (see [Import Providers, on page 22](#)).

### Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see [Create Credential Profiles, on page 8](#)).  
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.
- Know the Cisco NSO server IP address and hostname.
- Confirm Cisco NSO device configurations (see [Sample Configuration for Devices in Cisco NSO, on page 4](#)).


---

**Step 1** From the main menu, choose **Inventory Management > Providers**.

**Step 2** Click .

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

- a) Required fields:

- **Provider Name:** The name for the provider that will be used in Cisco Crosswork Optimization Engine.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO** only.
- **Protocol:** Select **NETCONF** only.
- **Device Key:** Select the method that Cisco NSO uses to identify devices uniquely. This will serve as the way maps the device to Cisco NSO. Choose **NODE\_IP** and other options you wish.
- **IPv4 Address:** Enter the IPv4 address of the Cisco NSO server. If you are using the DNS hostname as the provider name, the IP address is resolved automatically.
- **Port:** Enter the Cisco NSO. The default is **2022**.
- **Model:** Select the model (**Cisco-IOS-XR**, **Cisco-NX-OS**, or **Cisco-IOS-XE**) from the drop-down list and enter its associated NED driver version for each type of device that will be used in the topology. If you have more than one select  to add another supported model.

For more information on fields, see [Import Providers, on page 22](#).

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.
- **IPv6 Address:** Leave blank. Reserved for future use.

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

## Import Providers

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

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 26](#)).

**Step 1** From the main menu, choose **Inventory Management > Providers**.

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

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

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

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate entries with semicolons, the order in which you enter values is important. For example, if you enter **SSH ; SNMP ; NETCONF ; TELNET** in the **connectivity\_type** field and

you enter **22 ; 161 ; 830 ; 23** in the **connectivity\_port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830
- Telnet: port 23

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Required or Optional                                                                                      |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Provider Name</b>           | Enter the name for the provider that will be used in Crosswork Optimization Engine. For example: <b>MySRPCE</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Required                                                                                                  |
| <b>Connectivity Type</b>       | Enter the name of the protocol that Crosswork Optimization Engine will use to connect to the provider. For example:<br><b>ROBOT_MSVC_TRANS_HTTP</b> = HTTP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Required                                                                                                  |
| <b>Connectivity IPv4</b>       | Enter the IPv4 address of the provider.<br><br>If you are using the DNS hostname as the <b>provider_name</b> , the IP address is resolved automatically                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Required                                                                                                  |
| <b>Connectivity IPv6</b>       | Leave blank. Reserved for future use                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Optional                                                                                                  |
| <b>Connectivity Port</b>       | Enter the port number to use to connect to the provider's server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Required                                                                                                  |
| <b>Connectivity Timeout</b>    | Enter the amount of time (in seconds) to wait before the connection to the provider times out. The default is 30 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Optional                                                                                                  |
| <b>Credential Profile Name</b> | Enter the name of the credential profile that Crosswork Optimization Engine will use to connect to the provider. This profile must already exist in the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Required                                                                                                  |
| <b>Provider Device Key</b>     | Enter the enum value corresponding to the key that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way Crosswork Optimization Engine maps the device to the Cisco NSO provider. Valid values are: <ul style="list-style-type: none"> <li>• <b>ROBOT_PROVDEVKEY_HOST_NAME</b>—If you are using the device hostname as the device ID within NSO, this value must match the hostname that is specified for the device in the inventory.</li> <li>• <b>ROBOT_PROVDEVKEY_NODE_IP</b>—Use this enum value if the NSO device identifier is the IP address for the Node IP value in the CSV file.</li> <li>• <b>ROBOT_PROVDEVKEY_INVENTORY_ID</b>—Use this enum value if the inventory ID is the device identifier for NSO.</li> </ul> | This entry is only required if you are creating or updating a Cisco NSO provider. Otherwise, leave blank. |
| <b>Family</b>                  | Enter <b>ROBOT_PROVIDER_SR_PCE</b> or <b>ROBOT_PROVIDER_SR_NSQ</b> . Do not choose other options as they are reserved for use by other Cisco Network Automation applications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Required                                                                                                  |

| Field                | Description                                                                                                                                                                                                                                                                                                       | Required or Optional                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Model Prefix</b>  | If you are adding a Cisco NSO provider: Select the model prefix that matches the NED CLI used by the NSO server. Valid entries are: <b>Cisco-IOS-XR</b> , <b>Cisco-NX-OS</b> , <b>Cisco-IOS-XE</b> .<br><br>For telemetry, only Cisco-IOS-XR is supported.                                                        | Required for Cisco NSO providers only                                                                        |
| <b>Model Version</b> | If you adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the server.                                                                                                                                                                                                                    | Required for Cisco NSO providers only                                                                        |
| <b>Properties</b>    | Enter the Cisco SR-PCE appropriate auto-onboard entries:<br><del>auto-onboard: &lt;auto-onboard-property&gt; device-profile: &lt;SR-PCE-credential-profile-name&gt;</del><br>For example:<br><b>auto-onboard:managed;device-profile:cisco</b><br><br>See <a href="#">Add Cisco SR-PCE Providers, on page 16</a> . | This entry is only required if you are creating or updating a Cisco SR-PCE provider. Otherwise, leave blank. |

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 **Inventory Management > Providers**.

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

**Figure 3: Providers Window**




| Rea...                   | Provide... | UUID                       | Credential... | Connect... | Provider D... | Family         | Model Prefix | Model Version |
|--------------------------|------------|----------------------------|---------------|------------|---------------|----------------|--------------|---------------|
| <input type="checkbox"/> | xtc-CE2    | 5841cb3d-92b6-312c-8b7...  | XTC1-CE2      | HTTP       |               | SR_PCE         |              |               |
| <input type="checkbox"/> | xtc-CE4    | 313b3a98-36e8-3ec1-90b...  | XTC1-CE2      | HTTP       |               | SR_PCE         |              |               |
| <input type="checkbox"/> | NSO179     | de20c619-55e8-3f70-84f1... | NSO-Cred      | NETCONF    | NODE_IP       | NSO            | Cisco-IOS-XR | 6.6.2         |
| <input type="checkbox"/> | Syslog     | 6e9a49a1-1054-3758-85c...  | syslog        | SSH        |               | SYSLOG_STOR... |              |               |



**Step 2** The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols. For a description of each icon and its meaning, see [Reachability and Operational State, on page 5](#).

Cisco Crosswork Optimization Engine checks provider reachability immediately after a provider is added or modified. Other than these events, Cisco 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) 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 19](#).

---

## Edit Providers

When editing provider settings, be aware that a provider can be mapped to many devices.



### 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 16](#) 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 26](#)).

---

**Step 1** From the main menu, choose **Inventory Management > Providers**.

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

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

**Step 4** Resolve any errors and confirm provider reachability.

---

## Delete Providers

Follow the steps below to delete a provider.




**Note** If an SR-PCE provider's auto-onboard **managed** or **unmanaged** options are set, you must do one of the following:

- Reconfigure and remove the devices from the network before deleting the device from Cisco Crosswork Optimization Engine. This avoids Cisco Crosswork Optimization Engine from rediscovering and adding the device back to Cisco Crosswork Optimization Engine.
- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork Optimization Engine. However, doing so will not allow Cisco Crosswork Optimization Engine to detect or auto-onboard any new devices in the network.

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 26](#)).

**Step 2** Delete the provider as follows:

- From the main menu, choose **Inventory Management > Providers**.
- In the **Providers** window, choose the provider(s) that you want to delete and click .
- 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 **Inventory Management > Providers**.

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

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

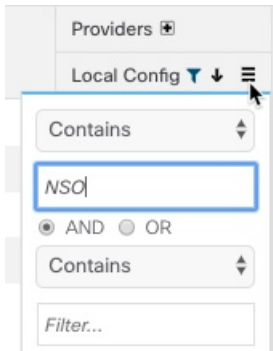
**Step 4** Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately.

## View Devices Assigned to a Provider

To see a list of devices that are assigned to a particular Cisco NSO provider:

- Step 1** From the main menu, choose **Inventory Management > Devices**.
- Step 2** In the **Devices** window, scroll across the table until you find the **Providers** column.
- Step 3** Under the Local Config field, set the filter criteria by selecting the logical operator from the drop down list in the first field, and then enter the Provider name in the second field.

**Figure 4: Filter Providers Column**

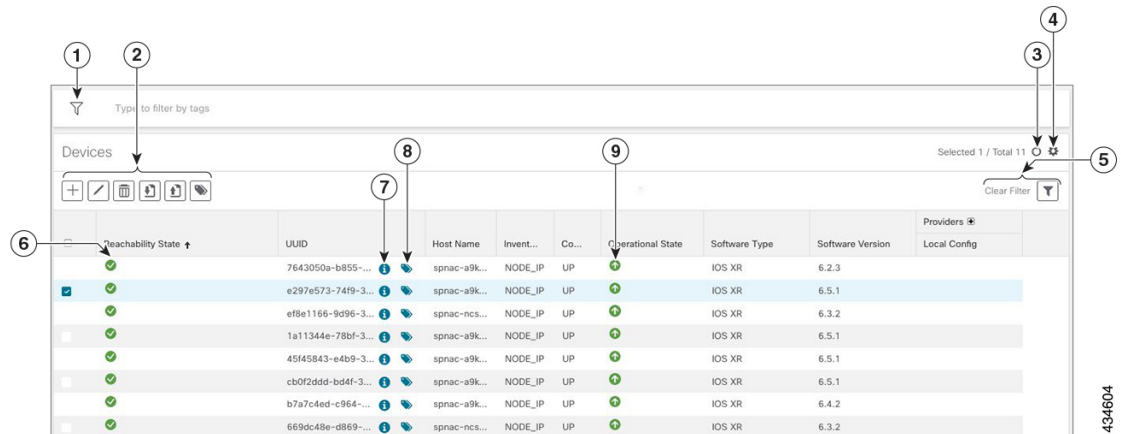


The table displays only the devices with the Provider criteria you entered.












## Manage Devices

The Inventory Management application's **Devices** window (shown below) gives you a consolidated list of all your devices and their status. To view the **Devices** window, select **Inventory Management > Devices**.

**Figure 5: Devices Window**



| Item | Description                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | The <b>Filter by tags</b> field lets you filter the devices by the tags applied to them. Type the name of the tag that has been applied to the device that you are trying to find. See <a href="#">Filter Devices by Tags, on page 37</a> . |

| Item | Description                                                                                                                                                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2    | Click  to add a new device to the device inventory. See <a href="#">About Adding Devices, on page 1</a> .                                                                                                                                                                                   |
|      | Click  to edit the information for the currently selected devices. See <a href="#">Edit Devices, on page 37</a> .                                                                                                                                                                           |
|      | Click  to delete the currently selected devices. See <a href="#">Delete Devices, on page 38</a> .                                                                                                                                                                                           |
|      | Click  to import new devices and update existing devices, using a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See <a href="#">Import Devices, on page 28</a> . |
|      | Click  to export information for selected devices to a CSV file. See <a href="#">Export Devices, on page 38</a> .                                                                                                                                                                           |
|      | Click  to modify tags applied to the selected devices. See <a href="#">Apply or Remove Device Tags, on page 42</a> .                                                                                                                                                                        |
| 3    | Click  to refresh the Devices list.                                                                                                                                                                                                                                                         |
| 4    | Click  to select which columns to display in the Devices list (see <a href="#">Set, Sort and Filter Table Data</a> ).                                                                                                                                                                       |
| 5    | Click  to set filter criteria on one or more columns in the Devices list.                                                                                                                                                                                                                 |
|      | Click the <b>Clear Filter</b> link to clear any filter criteria you may have set.                                                                                                                                                                                                                                                                                            |
| 6    | Icons in the <b>Reachability State</b> column show whether a device is reachable or not. See <a href="#">Reachability and Operational State, on page 5</a> .                                                                                                                                                                                                                 |
| 7    | Click  to open the <b>Device Details</b> pop-up window, where you can view important information for the selected device. See <a href="#">Get Device Details, on page 35</a> .                                                                                                            |
| 8    | Click  to see all the tags that have been applied to the device. See <a href="#">Manage Tags, on page 40</a> .                                                                                                                                                                            |
| 9    | Icons in the <b>Operational State</b> column show whether a device is operational or not. See <a href="#">Reachability and Operational State, on page 5</a>                                                                                                                                                                                                                  |

## Import Devices

Complete the steps below to create a CSV file that specifies multiple devices and then import it into Cisco Crosswork Optimization Engine.


Importing devices from a CSV file adds any devices not already in the database. The **Update Existing** option overwrites the data in any device record with an Inventory Key Type and device key field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import).

For this reason, it is a good idea to export a backup copy of all your current devices before an import (see [Export Devices, on page 38](#)).



**Note** If you plan on using a CSV file to import devices managed by Cisco Network Services Orchestrator (Cisco NSO), you must prepare the CSV following the guidelines given in [Sample Configuration for Devices in Cisco NSO, on page 4](#).

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

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

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

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

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter **SSH ; SNMP ; NETCONF ; 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

For a list of the fields and the values you can enter, see the "Add New Device" field table in [Add Devices Through the UI, on page 30](#).

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** to add new devices or **Update Existing** to add or change data to devices already in the system.

**Step 6** Resolve any errors and confirm device reachability.

The device information you imported should be displayed in the **Devices** window within a few minutes (see [Manage Devices, on page 27](#)).

It is normal for devices to show as unreachable or not operational when they are first imported. However, if after 30 minutes they are still displayed as unreachable or not operational, there is an issue that needs to be investigated. To

investigate, select **Inventory Management > Job History** and click on any   you see in the **Status** column. Common issues include failure to ensure the associated credential profile contains the correct credentials. You can test this by


opening a terminal window on the Cisco Crosswork Optimization Engine server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

## Add Devices Through the UI

Follow the steps below to add devices one by one, using the GUI. Under normal circumstances, you will want to use this method when adding one or a few devices only .



### Before you begin

Be sure you have completed the planning steps and setup requirements discussed in [Get Started](#), and that the devices themselves have been pre-configured as explained in [Prerequisites for Onboarding Devices](#), on page 3.

- Step 1** From the main menu, choose **Inventory Management > Devices**. The **Devices** window opens.
- Step 2** Click .
- Step 3** Enter values for the new device, as listed in the table below.
- Step 4** Click **Save**. (The Save button is disabled until all mandatory fields are complete.)
- Step 5** (Optional) Repeat to add more devices.

**Table 2: Add New Device Window (\*=Required)**

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * <b>Configured State</b> | The management state of the device. Options are <ul style="list-style-type: none"> <li>• <b>UNMANAGED</b>—Cisco Crosswork Optimization Engine is not monitoring the device.</li> <li>• <b>DOWN</b>—The device is being managed and is down.</li> <li>• <b>UP</b>—The device is being managed and is up.</li> </ul>                                                                                                                                  |
| <b>Reachability Check</b> | Determines whether Cisco Crosswork Optimization Engine performs reachability checks on the device. Options are: <ul style="list-style-type: none"> <li>• <b>ENABLE/REACH_CHECK_ENABLE</b>—Checks for reachability and then updates the Reachability State in the UI automatically.</li> <li>• <b>DISABLE/REACH_CHECK_DISABLE</b>—The device reachability check is disabled.</li> </ul> Cisco recommends that you always set this to <b>ENABLE</b> . |
| <b>Credential Profile</b> | The name of the credential profile assigned to the device and used to access it for data collection and configuration changes. For example: <b>nso23</b> or <b>srpce123</b> .                                                                                                                                                                                                                                                                       |

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * <b>Inventory Key Type</b>         | The type of identification key for the device. You must choose one of the available types. In all cases other than <b>UUID</b> , you must enter the corresponding key field with a unique ID value. For example: If you choose <b>HOST_NAME</b> as the * <b>Inventory Key Type</b> , you must fill in the <b>Host Name</b> field with the unique host name of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| * <b>Host Name</b>                  | The hostname of the device. Required only if * <b>Inventory Key Type</b> is <b>HOST_NAME</b> . Otherwise, Cisco Crosswork Optimization Engine discovers it and updates it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Inventory ID</b>                 | Inventory ID value for the device. Required only if * <b>Inventory Key Type</b> is <b>INVENTORY_ID</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>UUID</b>                         | Universally unique identifier (UUID) for the device. If you choose <b>UUID</b> as the * <b>Inventory Key Type</b> , leave this field blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Serial Number</b>                | Serial number for the device. Required only if * <b>Inventory Key Type</b> is <b>SERIAL_NUMBER</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Node IP</b>                      | Node IP value for the device. Required only if * <b>Inventory Key Type</b> is <b>NODE_IP</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>MAC Address</b>                  | MAC address for the device. Required only if * <b>Inventory Key Type</b> is <b>MAC</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| * <b>Capability</b>                 | The capabilities that allow collection of device data and that are configured on the device. You must select at least <b>SNMP</b> , as this is a required capability. The device will not be onboarded if <b>SNMP</b> is not configured. Other options are <b>YANG_MDT</b> , <b>TL1</b> , <b>YANG_CLI</b> , and <b>YANG-EPNM</b> . The capabilities you select will depend on the device software type and version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Tags</b>                         | The available tags to assign to the device.<br><br>Use device tags to group devices for monitoring, and to provide additional information that might be of interest to other users, such as the device's physical location and its administrator's email ID. For more information, see <a href="#">Manage Tags</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Connectivity Details</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Protocol</b>                     | The connectivity protocols used by the device. Choices are: <b>SSH</b> , <b>SNMP</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , and <b>HTTPS</b> .<br><br>To add more connectivity protocols for this device, click  at the end of the first row in the <b>Connectivity Details</b> panel. To delete a protocol you have entered, click  shown next to that row in the panel.<br><br>You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol. You must enter details for at least <b>SSH</b> and <b>SNMP</b> . If you do not configure <b>SNMP</b> , the device will not be on-boarded. If you want to manage the device (or you are managing XR devices), you must enter details for <b>NETCONF</b> . <b>TELNET</b> connectivity is optional. |
| * <b>IPv4 Address / Subnet Mask</b> | Enter the device's IPv4 address and CIDR subnet mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>IPv6 Address / Subnet Mask</b>   | Enter the device's IPv6 address and subnet mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Field                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>* Port</b>                                                                                                                                                               | The port used for this connectivity protocol. Each protocol is mapped to a port, so be sure to enter the port number that corresponds to the <b>Protocol</b> you chose. The standard port assignments for each protocol are: <ul style="list-style-type: none"> <li>• SSH: 22</li> <li>• SNMP: 161</li> <li>• NETCONF: 830</li> <li>• TELNET: 23</li> <li>• HTTP: 80</li> <li>• HTTPS: 443</li> </ul> |
| <b>Timeout</b>                                                                                                                                                              | The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.                                                                                          |
| <b>Routing Info</b>                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>ISIS System ID</b>                                                                                                                                                       | The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.                                                                                                                                                                                                                                                                             |
| <b>OSPF Router ID</b>                                                                                                                                                       | The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.                                                                                                                                                                                                                                                                               |
| <b>Streaming Telemetry Config</b>                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Telemetry Interface Source VRF</b>                                                                                                                                       | Name of the VRF in whose context Model Driven Telemetry (MDT) traffic is routed.                                                                                                                                                                                                                                                                                                                      |
| <b>Location</b>                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                       |
| All location fields are optional, with the exception of <b>Longitude</b> and <b>Latitude</b> , which are required for a correct geographical view of your network topology. |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Longitude, Latitude</b>                                                                                                                                                  | Entries in these fields are recommended. Without <b>Longitude</b> and <b>Latitude</b> values, the topology map's geographical view shows all devices and links bunched together at the same spot. With these values, the map can present the correct geographical location of each device and its links to other nodes.                                                                               |
| <b>Altitude</b>                                                                                                                                                             | The altitude, in feet or meters, at which the device is located. For example, <b>123</b> .                                                                                                                                                                                                                                                                                                            |
| <b>Providers and Access</b>                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Local Config: Device Key and Provider</b>                                                                                                                                | This field is mandatory only when mapping an NSO provider. The Device Key will automatically populate and the Credential Profile appears.<br>For CSV entry, use ROBOT_PROVIDER_LOCAL_CONFIG and enter the Provider name.                                                                                                                                                                              |
| <b>Compute Config: Device Key and Provider</b>                                                                                                                              | (Optional) Provider name used for topology computation. Choose a provider from the list.<br>For CSV entry, use ROBOT_PROVIDER_COMPUTE and enter the Provider name.                                                                                                                                                                                                                                    |



## Example

*Figure 6: Add Device Window*

Add New Device



\*Configured State UNMANAGED  
 Reachability Check  
 Credential Profile NSO-Cred  
 \*Inventory Key Type NODE\_IP  
 Host Name  
 Inventory ID  
 UUID  
 Serial Number  
 \*Node IP 172. /  
 Mac Address  
 Capability Select capability  
 Tags Select Tags

Connectivity Details

| Protocol | IPv4 Address / Subnet Mask | IPv6 Address / Subnet Mask | Port | Timeout |
|----------|----------------------------|----------------------------|------|---------|
| NETCONF  | 172. /24                   | /                          | 23   | 60      |

Routing Info

IS-IS System ID ?  
 OSPF Router ID ?

Streaming Telemetry config

Telemetry Interface Source VRF ?

Location

Building ABC\_Building  
 Street Cisco123 St  
 City San Jose  
 State CA - California  
 Country United States  
 Region California  
 Zip 95128  
 Latitude  
 Longitude  
 Altitude

Providers and Access

Local Config ?


Provider NSO179  
 Device Key 172.  
 Credential Profile NSO-Cred

Compute Config ?

Provider xtc-CE2  
 Credential Profile XTC1-CE2

Save Cancel

## Get Device Details

Whenever you select **Inventory Management > Devices** and display the list of devices, you can click  next to any listed device to get more information about that device. Clicking this icon opens the **Details for DeviceName** pop-up window, as shown in the following example:

*Figure 7: Details for DeviceName Window*

Expand the **Connectivity Details** area at the top of the pop-up window (if it is not already expanded). This area shows the reachability status for all transport types (for help with the icons shown in this area, see [Device and Link Icons](#)).

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

## Filter Devices by Tags

By creating a tag and assigning it to a particular device, you can easily provide additional information that might be of interest to other users, such as the device's physical location and its administrator's email ID. You can also use tags to find and group devices with the same or similar tags in any window that lists devices.

For help with tagging your devices, see [Apply or Remove Device Tags, on page 42](#). For help with creating and deleting tags, see [Manage Tags, on page 40](#).

To filter devices by tags:

- 
- Step 1** Display the **Devices** window by choosing **Inventory Management > Devices**.
- Step 2** In the **Type to filter by tags** bar at the top of the user interface, type all or part of the name of a tag.
- The **Type to filter by Tags** bar has a type-ahead feature: As you start typing, the field shows a drop-down list of tags that match all the characters you have typed so far. To force the drop-down list to display all available tags, type **\***.
- Step 3** Choose the name of the tag you want to add to the filter. The filter appears in the **Type to filter by tags** filter bar. The table or map shows only the devices with that tag.
- Step 4** If you want to filter on more than one tag:
- Repeat Steps 2 and 3 for each additional tag you want to set as part of the filter.
  - When you have selected all the tags you want, click **Apply Filters**. The table or map shows only the devices with tags that match **all** the tags in your filter.
- Step 5** To clear all tag filters, click the **Clear Filters** link. To remove a tag from a filter containing multiple tags, click the **X** icon next to that tag's name in the filter.
- 

## Edit Devices

Complete the following procedure to update a device's information.

Before editing any device, it is always good practice to export a CSV backup of the devices you want to change (see [Export Devices, on page 38](#)).

- 
- Step 1** From the main menu, choose **Inventory Management > Devices**.
- Step 2** (Optional) In the **Devices** window, filter the list of devices by filtering specific columns.
- Step 3** Check the check box of the device you want to change, then click
- Step 4** Edit the values configured for the device, as needed.
- For a description of the fields you can update, see [Add Devices Through the UI](#).
- Step 5** Click **Save**. (The Save button remains dimmed until all required fields are filled in.)

**Step 6** Resolve any errors and confirm device reachability.

---

## Delete Devices

Complete the following procedure to delete devices.

### Before you begin

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



### Note


- If devices are mapped to NSO with MDT capability, and telemetry configuration is pushed, then those configurations will be removed from the device.
  - If auto-onboard is not set to **off**, and it is still functional and connected to the network, the device will be rediscovered as unmanaged as soon as it is deleted.
- 

**Step 1** Export a backup CSV file containing the devices you plan to delete (see [Export Devices, on page 38](#)).

**Step 2** From the main menu, choose **Inventory Management > Devices**.

**Step 3** (Optional) In the **Devices** window, filter the list of devices by entering text in the **Search** field or filtering specific columns.

**Step 4** Check the check boxes for the devices you want to delete.

**Step 5** Click  to change each device's state to ADMIN DOWN or UNMANAGED.

If you want to delete devices in bulk, Cisco recommends that you change the device state in this manner in batches of 50 devices, then complete deletion of these devices before deleting another batch.

**Step 6** Click .

**Step 7** In the confirmation dialog box, click **Delete**.

---


## Export Devices

When you export the device list, all device information is exported to a CSV file. Exporting the device list is a handy way to keep a record of all devices in the system at one time. You can also edit the CSV file as needed, and re-import it to overwrite existing device data.

---

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

**Step 2** (Optional) In the **Devices** window, filter the device list as needed.



- Step 3** Check the check boxes for the devices you want to export. Check the check box at the top of the column to select all the devices for export.
- Step 4** Click . Your browser will prompt you to select a path and the file name to use when saving the CSV file, or to open it immediately


## View Device Job History




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

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

**Figure 8: Job History Window With Error Details Popup**

Inventory Jobs Total 48  


Clear Filter 

| Start Time               | End Time                 | Status                                                                                       | Transaction ID                 | Description                   | User Name |
|--------------------------|--------------------------|----------------------------------------------------------------------------------------------|--------------------------------|-------------------------------|-----------|
| Thu Jul 11 2019 00:29:45 | Thu Jul 11 2019 00:29:45 | ✔ Completed                                                                                  | 2df5abfb-a773-44cf-90eb-bb3... | Update 1 Provider(s)          | admin     |
| Thu Jul 11 2019 00:29:37 | Thu Jul 11 2019 00:29:37 | ✔ Completed                                                                                  | a48fc525-294f-401c-931f-6ec... | Insert 1 Credential(s)        | admin     |
| Thu Jul 11 2019 00:29:06 | Thu Jul 11 2019 00:29:06 | ✔ Completed                                                                                  | b2ff90c2-ada7-449b-9e1c-34b... | Insert 1 Provider(s)          | admin     |
| Wed Jul 10 2019 23:54:27 | Wed Jul 10 2019 23:54:27 | ✘ Failed  | f9bbc535-109e-4621-a1c5-c6...  | Delete 7 Tag(s)               | admin     |
| Wed Jul 10 2019 23:51:51 | Wed Jul 10 2019 23:51:51 | ✔ Completed                                                                                  | b6362a8a-7ff9-4d9d-9c6d-d1...  | Insert 1 Tag(s)               | admin     |
| Wed Jul 10 2019 23:30:25 | Wed Jul 10 2019 23:30:25 | ✔ Completed                                                                                  | b34cb396-9077-4561-a294-e...   | Update 8 Node(s) Via CS...    | admin     |
| Wed Jul 10 2019 23:28:32 | Wed Jul 10 2019 23:28:32 | ✔ Completed                                                                                  | 2823a33e-8ce1-499d-89f1-9c...  | Update 1 Node(s)              | admin     |
| Wed Jul 10 2019 23:28:32 | Wed Jul 10 2019 23:28:32 | ✔ Completed                                                                                  | 662ffc8c-4992-4778-a7ba-22b... | Unassign Tags                 | admin     |
| Wed Jul 10 2019 23:28:26 | Wed Jul 10 2019 23:28:26 | ✔ Completed                                                                                  | 180a0b48-cacc-48e2-913c-5a...  | Update 1 Node(s)              | admin     |
| Wed Jul 10 2019 23:22:45 | Wed Jul 10 2019 23:22:45 | ✘ Failed  | 455409d4-f69d-4a9e-951f-4d...  | Insert 2 Provider(s) Via C... | admin     |
| Wed Jul 10 2019 23:14:18 | Wed Jul 10 2019 23:14:18 | ✘ Failed  |                                |                               |           |
| Wed Jul 10 2019 23:14:10 | Wed Jul 10 2019 23:14:10 | ✔ Completed                                                                                  |                                |                               |           |

**Error Details**

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

The jobs display in descending order of creation time. The most recent job is shown first. To sort the data in the table, click a column heading. You can toggle between ascending and descending sort order (for more help, see [Set, Sort and Filter Table Data](#)).

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

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

# Manage 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 **Inventory Management > Tags** from the main window.

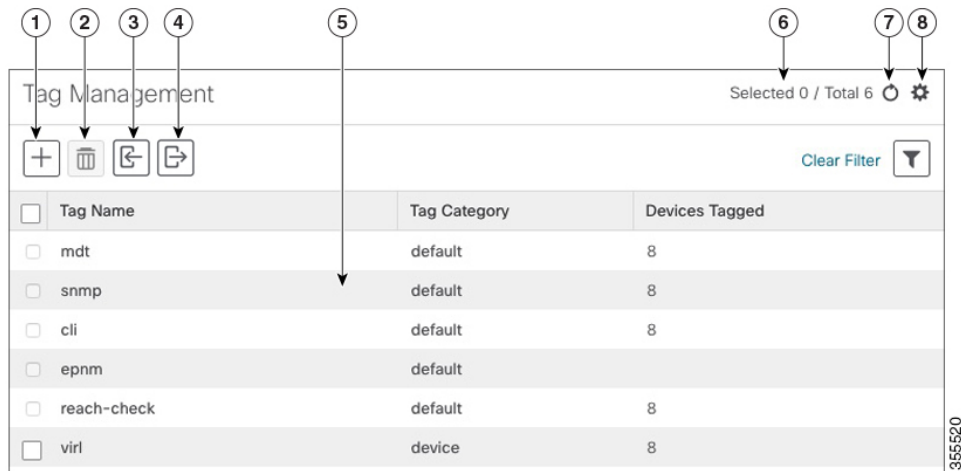


**Note** Cisco Crosswork Optimization Engine automatically creates a default set of tags and assigns them to every device it manages:

- cli
- mdt
- reach-check
- snmp
- clock-drift-check






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

**Figure 9: Tag Management Window**



| Item | Description                                                                        |
|------|------------------------------------------------------------------------------------|
| 1    | Click  to create new device tags. See <a href="#">Create Tags</a> .                |
| 2    | Click  to delete currently selected device tags. See <a href="#">Delete Tags</a> . |



| Item | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | Click  to import the device tags defined in a CSV file into Cisco Crosswork Network Automation. See <a href="#">Import Tags, on page 42</a> . You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. |
| 4    | Click  to export a CSV file that lists the tags that are currently configured and their attributes. You can update this file and import it back into Cisco Crosswork Optimization Engine to quickly add or edit multiple tags. See <a href="#">Export Tags, on page 43</a> .                                 |
| 5    | Displays the tags currently available in Cisco Crosswork Optimization Engine and their attributes.                                                                                                                                                                                                                                                                                            |
| 6    | Indicates the number of tags that are currently selected in the table.                                                                                                                                                                                                                                                                                                                        |
| 7    | Click  to refresh the <b>Tag Management</b> window.                                                                                                                                                                                                                                                          |
| 8    | Click  to choose the columns to make visible in the <b>Tag Management</b> window (see <a href="#">Set, Sort and Filter Table Data</a> ).                                                                                                                                                                     |
|      | Click  to set filter criteria on one or more columns in the <b>Tag Management</b> window.                                                                                                                                                                                                                    |
|      | Click the <b>Clear Filter</b> link to clear any filter criteria you may have set.                                                                                                                                                                                                                                                                                                             |

## Create Tags

You can create as many tags and tag categories as you want.

**Step 1** From the main menu, choose **Inventory Management > 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 Tag names, click **Save**.

**What to do next**

Add tags to devices. See [Apply or Remove Device Tags, on page 42](#).


## Import Tags

Complete the steps below to create a CSV file that specifies tags and then import it into Cisco Crosswork Optimization Engine. This is the easiest way to create a lot of new tags and tag categories quickly.

You can create as many tags and tag categories as you want. Tag and tag category names are case-insensitive and can contain up to 128 alphanumeric characters. They cannot contain special characters, symbols, or spaces.

Importing adds any tags not already in the database, and overwrites the data in any tags with the same name as an imported tag. 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 43](#)).

**Step 1** From the main menu, choose **Inventory Management > Tag Management**.

**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 '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: <b>San Francisco</b> . | Required             |
| Tag Category | Enter the tag category. For example: <b>City</b> .             | Required             |

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

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

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

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

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

**What to do next**

Add tags to devices. See [Apply or Remove Device Tags, on page 42](#).



## Apply or Remove Device Tags

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

In order to apply a tag to a device or group of devices, the tag must already exist (see [Create Tags, on page 41](#)).

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 **Inventory Management > Devices**. The **Devices** window opens, 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 43](#)).
  - Step 2** From the main menu, choose **Inventory Management > Tag Management**.
  - 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 **Inventory Management > 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.
-