



Manage Devices

This section contains the following topics:

- [Device 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 Network Devices](#), on page 14
- [Manage Tags](#), on page 26

Device Management Overview

The Device Management 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 **devices** you manage using Crosswork Optimization Engine. See [Manage Network Devices](#), on page 14.

You can also use Device Management to review the **jobs** executed on your devices. See [View Device Job History](#), on page 25.

About Adding Devices

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

1. Automatically onboard devices and populate the inventory. High-level steps are documented in [Workflow: Auto-Onboard Devices](#).
2. Manually onboard devices using a CSV file or the UI. High-level steps are documented in [Workflow: Manually Import Devices](#)

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:

- **ISIS-System ID**, **OSPF Router ID**, and **TE router ID** will be filled in the device's routing information.
- The **Connectivity IP** is assigned the same value as the **TE router ID**.
- 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 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 by importing a CSV file (see [Import Devices, on page 16](#)). In this case, use the **unmanaged** option for auto-onboarding to prevent repeated unsuccessful collection attempts from 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.
- The **managed** option works only if a single **Credential Profile** will work for accessing all the devices.
- 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. See [Import Devices, on page 16](#) and [Export Devices, on page 24](#).

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 **Device Management > Devices** >  and populate it with all the devices you will need (see [Import Devices, on page 16](#)). 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 17](#)). 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 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 SNMPv2 and SNMPv3 (NoAuth/NoPriv) traps are supported.

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.

```
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
!
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 vldefault
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 830
```

In the following example, we are creating an authgroup called `cisco` with remote name and password of `cisco`. Next, we are setting all the devices with a name that starts with `Router` to a device type of `netconf` using `ned-id` `cisco-iosxr-nc-6.6`. Finally, we are setting all of the devices with a name starting with `Router` to be assigned to authgroup `cisco`. Edit the setting to match your environment. For example:

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```









The following steps unlock the devices and retrieve the ssh keys from all of the devices. NSO then synchronizes itself with the device by uploading the devices current configuration and stores the present configuration. It is important to perform these steps to ensure that the device, NSO, and Crosswork Network Automation applications are starting from a common configuration. 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...
Reachability State 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. This state can also occur if the device is not connected to Cisco Crosswork Data Gateway.
Operational State 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 REACHABLE and discoverable. Any other Reachability 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

Some timezone settings are known to result in Clock Drift errors when no clock drift actually exists. To work around this issue set your devices to use UTC time.

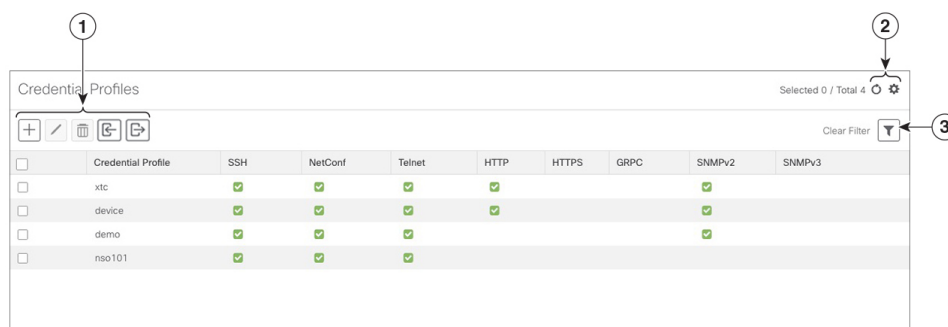
Manage Credential Profiles

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


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

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

Figure 1: Credentials Profile window



Item	Description
1	<p>Click to add a credential profile. See Create Credential Profiles, on page 8.</p> <p>Click to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 12.</p> <p>Click to delete the selected credential profile. See Delete Credential Profiles, on page 12.</p> <p>Click to import new credential profiles from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Credential Profiles, on page 9.</p> <p>Click to export credential profiles to a CSV file. See Export Credential Profiles, on page 13.</p>
2	<p>Click to refresh the Credential Profiles window.</p> <p>Click to choose the columns to make visible in the Credential Profiles window (see Set, Sort and Filter Table Data).</p>

Item	Description
3	Click  to set filter criteria on one or more columns in the Credential Profiles window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Create Credential Profiles

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

If you have many credential profiles to add, you may find it more efficient to put the information in a CSV file and import the file. See [Import Credential Profiles, on page 9](#).

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 9](#)).

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 **Device Management > Credential Profiles**.

Step 2 Click .

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

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

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

Step 5 Complete the credentials fields described in the following table. The required and optional fields displayed 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 User Name , Password , and Confirm Password . The Enable Password is optional.

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

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

Step 7 Click **Save**.


Import Credential Profiles

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

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

If you are re-importing a credential profile CSV file that you previously exported and modified, remember that all the passwords and community strings in the exported credential profile CSV file are replaced with asterisks. You cannot re-import an exported credential profile CSV file with blank passwords. To maintain security, Cisco recommends that you use asterisks in place of real passwords and community strings in the CSV file. After the import, follow the steps in [Edit Credential Profiles, on page 12](#) to replace the asterisks with actual passwords and community strings.

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

Step 2 Click  to open the **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 will 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: srpce .	Required
Connectivity Type	Valid values are: SSH, SNMPv2, NETCONF, TELNET, HTTP, HTTPS, GRPC or SNMPv3	<ul style="list-style-type: none"> • Devices—SNMP and SSH (to avoid operational errors due to clock synchronization checks) are required. • SR-PCE—Since SR-PCE is considered a provider and a device, SSH, and HTTP are required. • NSO—NETCONF is required.

Field	Entries	Required or Optional
User Name	For example: SRPCEUser	Required if Connectivity Type is SSH , NETCONF , TELNET , HTTP , HTTPS , SNMPv3 or GRPC .
Password	The password for the preceding User Name .	Required if Connectivity Type is SSH , NETCONF , TELNET , HTTP , HTTPS or GRPC
Enable Password	Use an Enable password. Valid values are: ENABLE , DISABLE , or leave blank (unselected)	
Enable Password Value	Specify the Enable password to use.	Required only if Enable Password is set to Enable .
SNMPV2 Read Community	For example: readprivate	Required if Connectivity Type is SNMPv2
SNMPV2 Write Community	For example: writeprivate	
SNMPV3 User Name	For example: DemoUser	Required if Connectivity Type is SNMPv3
SNMPV3 Security Level	Valid values are noAuthNoPriv , AuthNoPriv or AuthPriv	Required if Connectivity Type is SNMPv3
SNMPV3 Auth Type	Valid values are HMAC_MD5 or HMAC_SHA	Required if Connectivity Type is SNMPv3 and Snpv3 Security Level is AuthNoPriv or AuthPriv
SNMPV3 Auth Password	The password for this authorization type.	Required if Connectivity Type is SNMPv3 and Snpv3 Security Level is AuthNoPriv or AuthPriv
SNMPV3 Priv Type	Valid values are CFB_AES_128 or CBC_DES_56 The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	Required if Connectivity Type is SNMPv3 and Snpv3 Security Level is AuthPriv
SNMPV3 Priv Password	The password for this privilege type.	Required if Connectivity Type is SNMPv3 and Snpv3 Security Level is AuthPriv

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

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

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

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

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


Edit Credential Profiles

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



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 **Device Management > Credentials**.
- Step 2** From the left-hand side of the **Credential Profiles** window, select the profile you want to update, and click . The **Edit Profile** window of the selected credential is displayed.
- Step 3** Make the necessary changes and then click **Save**.

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 **Device Management > Credential Profiles**) and the **Providers** window (choose **Admin > Providers**).
- Step 3** Reassign the devices or providers to a different credential profile (for help with this task, see [Change the Credential Profile for a Device or Provider, on page 13](#) or [Change the Credential Profile for Multiple Devices, on page 14](#), and [Edit Providers](#)).
- Step 4** After all devices and providers have had their credential profiles reassigned: From the main menu, choose **Device Management > Credential Profiles**.
- Step 5** In the **Credential Profiles** window, choose the profile that you want to delete and then click .

Export Credential Profiles

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

The exported credential profiles CSV file does not contain real passwords or community strings. All the characters in the passwords and community strings entries in the credential profiles are replaced with asterisks in the exported CSV file. If you plan on modifying your exported CSV file and then re-importing it, Cisco recommends that you use asterisks in place of real passwords and community strings. After the import, follow the steps in [Edit Credential Profiles, on page 12](#) to replace the asterisks with actual passwords and community strings.

-
- Step 1** From the main menu, choose **Device Management > Credential Profiles**.
 - Step 2** (Optional) In the **Credential Profiles** window, filter the credential profile list as needed.
 - Step 3** Check the check boxes for the profiles you want to export. Check the check box at the top of the column to select all the profiles for export.
 - Step 4** Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately
-

Change the Credential Profile for a Device or Provider


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 **Device Management > Devices**. The **Network Devices** tab is displayed by default.
 - Step 2** (Optional) 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 network devices, you may find it more efficient to make the change by editing a devices CSV file. The basic method is:

1. Export a CSV file containing the devices whose credential profiles you want to change (see [Export Devices, on page 24](#)).
2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist). Save the edited file.

You will need to make sure that the credential profile to which you are changing already exists. If you have not yet created that credential profile, the CSV import will fail. The credential profile you associate with these devices must also have the authorization credentials for every protocol that was configured for these devices during onboarding. If any credential for a specific protocol configured on the devices is missing from or incorrect in the credential profile, then the CSV import will succeed, but reachability checks will fail for these devices.

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

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

- Click  to include all devices.
- Filter the device list by entering text in the **Search** field or by filtering specific columns. Then click  to include only the filtered list of devices.
- Check the boxes next to the device records you want to change. Then click  to include only the devices that have been checked.

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

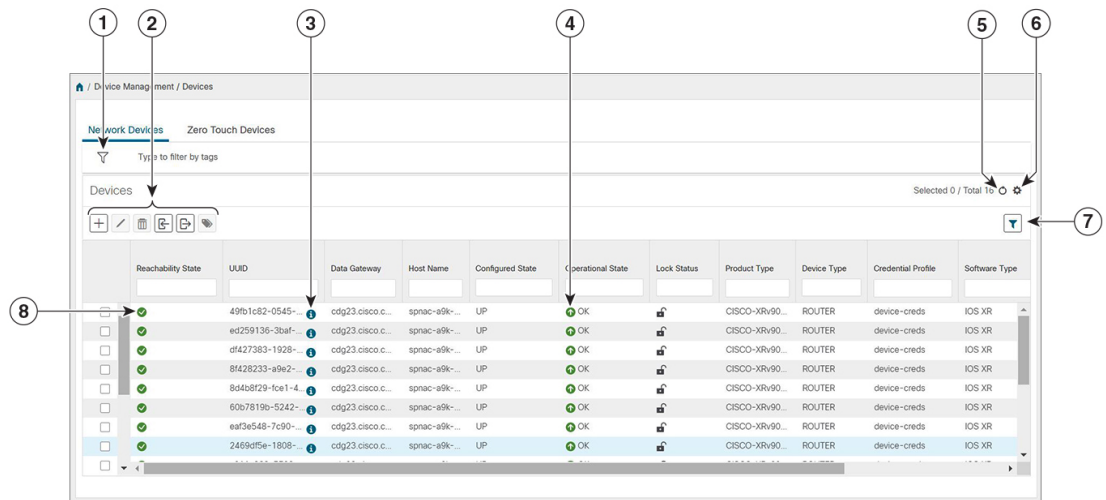
Step 4 Click .

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



Manage Network Devices

The Device Management application's **Network Devices** window (shown below) gives you a consolidated list of all your devices and their status. To view the **Network Devices** window, select **Device Management > Devices**. The **Network Devices** tab is displayed by default.

Figure 2: Devices Window



Item	Description
1	The Filter by tags 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 Filter Devices by Tags, on page 23 .
2	Click to add a new device to the device inventory. See About Adding Devices, on page 1 .
	Click to edit the information for the currently selected devices. See Edit Devices, on page 23 .
	Click to delete the currently selected devices. See Delete Devices, on page 24 .
	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 Import Devices, on page 16 .
	Click to export information for selected devices to a CSV file. See Export Devices, on page 24 .
	Click to modify tags applied to the selected devices. See Apply or Remove Device Tags, on page 29 .
3	Click to open the Device Details pop-up window, where you can view important information for the selected device. See Get Device Details, on page 21 .
4	Icons in the Operational State column show whether a device is operational or not. See Reachability and Operational State, on page 5
5	Click to refresh the Devices list.

Item	Description
6	Click  to select which columns to display in the Devices list (see Set, Sort and Filter Table Data).
7	Click  to set filter criteria on one or more columns in the Devices list.
	Click the Clear Filter link to clear any filter criteria you may have set.
8	Icons in the Reachability State column show whether a device is reachable or not. See Reachability and Operational State, on page 5 .

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, and 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 24](#)).



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 **Device Management > Devices**. The **Network Devices** tab is displayed by default.

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.

Note Confirm that the TE router ID value for each device is populated. This value is used to uniquely identify the device in the topology which is learned from SR-PCE. Without a valid TE router ID for each device, the topology will not be displayed.

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** in the **Connectivity Type** field and you enter **22 ; 161 ; 830** 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

For a list of the fields and the mandatory values you must enter, see the "Add New Device" field table in [Add Devices Through the UI, on page 17](#).

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**.

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 Network Devices, on page 14](#)).

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 **Device 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 UI. 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 **Device Management > Devices**. The **Network Devices** tab is displayed by default.

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
* Configured State	The management state of the device. Options are <ul style="list-style-type: none"> • UNMANAGED—Cisco Crosswork Optimization Engine is not monitoring the device. • DOWN—The device is being managed and is down. • UP—The device is being managed and is up.
* Reachability Check	Determines whether Cisco Crosswork Optimization Engine performs reachability checks on the device. Options are: <ul style="list-style-type: none"> • ENABLE (In CSV: REACH_CHECK_ENABLE)—Checks for reachability and then updates the Reachability State in the UI automatically. • DISABLE (In CSV: REACH_CHECK_DISABLE)—The device reachability check is disabled. <p>Cisco recommends that you always set this to ENABLE. This field is optional if Configured State is marked as UNMANAGED.</p>
* Credential Profile	The name of the credential profile to be used to access the device for data collection and configuration changes. For example: nso23 or srpce123 . This field is optional if Configured State is marked as UNMANAGED .
Host Name	The hostname of the device. Cisco Crosswork Optimization Engine discovers it and updates it.
Inventory ID	Inventory ID value for the device. The value can contain a maximum of 128 alphanumeric characters, and can include dots (.), underscores ("_"), colons (":"), or hyphens ("-"). No other special characters are allowed.
UUID	Universally unique identifier (UUID) for the device.
Serial Number	Serial number for the device.
MAC Address	MAC address of the device.
* Capability	The capabilities that allow collection of device data and that are configured on the device. You must select at least SNMP as this is a required capability. The device will not be onboarded if SNMP is not configured. Other options are YANG_MDT , TL1 , YANG_CLI , and YANG-EPNM . The capabilities you select will depend on the device software type and version.
Tags	The available tags to assign to the device for identification and grouping purposes. 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 or its administrator's email ID. For more information, see Manage Tags .
Connectivity Details	

Field	Description
Protocol	<p>The connectivity protocols used by the device. Choices are: SSH, SNMP, NETCONF, TELNET, HTTP, and HTTPS.</p> <p>To add more connectivity protocols for this device, click + at the end of the first row in the Connectivity Details panel. To delete a protocol you have entered, click × shown next to that row in the panel.</p> <p>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 SSH and SNMP. If you do not configure SNMP, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for NETCONF. TELNET connectivity is optional.</p>
* IP Address / Subnet Mask	<p>Enter the device's IP address (IPv4 or IPv6) and subnet mask.</p> <p>Note Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues.</p>
* Port	<p>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 Protocol you chose. The standard port assignments for each protocol are:</p> <ul style="list-style-type: none"> • SSH: 22 • SNMP: 161 • NETCONF: 830 • TELNET: 23 • HTTP: 80 • HTTPS: 443
Timeout	<p>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.</p>
Routing Info	
ISIS System ID	<p>The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.</p>
OSPF Router ID	<p>The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.</p>
*TE Router ID	<p>The device's OSPF Router ID or ISIS Router ID depending on the IGP used in the network topology.</p>
Streaming Telemetry Config	
Telemetry Interface Source VRF	<p>Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.</p>

Field	Description
Location	
All location fields are optional, with the exception of Longitude and Latitude , which are required for the geographical view of your network topology.	
Longitude, Latitude	Longitude and latitude values are required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude and latitude in Decimal Degrees (DD) format.
Altitude	The altitude, in feet or meters, at which the device is located. For example, 123 .
Providers and Access	
Local Config:Provider and Device Key	Mandatory only when mapping an NSO provider. The Device Key will automatically populate. For CSV entry, use ROBOT_PROVIDER_LOCAL_CONFIG and enter the Provider name.
Compute Config: Provider	(Optional) Provider name used for topology computation. Choose a provider from the list. For CSV entry, use ROBOT_PROVIDER_COMPUTE and enter the Provider name.

Example

Figure 3: Add New Device Window

The screenshot shows a 'Add New Device' window with the following sections and fields:

- General:** Configured State (dropdown), Reachability Check (dropdown), Credential Profile (dropdown), Host Name (text), Inventory ID (text), Software Type (text), Software Version (text), UUID (text), Serial Number (text), Mac Address (text), Capability (dropdown), Tags (dropdown), Product Type (text).
- Connectivity Details:** Protocol (dropdown), IP Address / Subnet Mask (text), Port (text), Timeout (text), + Add Another (button), trash icon.
- Routing Info:** IS-IS System ID (text), OSPF Router ID (text), TE Router ID (text).
- Streaming Telemetry config:** Vrf (text), Source Interface (dropdown, currently 'Loopback'), text field.
- Location:** Building (text), Street (text), City (text), State (text), Country (text), Region (text), Zip (text), Latitude (text), Longitude (text), Altitude (text).
- Providers and Access:** Local Config (dropdown), Provider (dropdown), Device Key (text), Compute Config (dropdown), Provider (dropdown).

Buttons at the bottom: Save, Cancel.

Get Device Details


Whenever you select **Device Management > Devices** and display the list of devices under the **Network Devices** tab, 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 4: Details for DeviceName Window

Details for 1bce17d4-5219-4057-800a-57142080000a ×

▼ Connectivity Details

Protocol	IP Address/Port	Timeout
<input checked="" type="checkbox"/> SSH	10.10.10.10:22	60
<input checked="" type="checkbox"/> TELNET	10.10.10.10:23	60
<input checked="" type="checkbox"/> SNMP	10.10.10.10:161	60
<input checked="" type="checkbox"/> NETCONF	10.10.10.10:830	60

▼ Identifiers

Key Type
Inventory ID
Host Name spnac-a9k-s105
UUID 1bce17d4-5219-4057-800a-57142080000a
Node IP 10.10.10.10
Serial # 256E-00000000
Mac Address 0050-0000-0000

▼ Hardware/Software

Product Type CISCO-XRv9000
Product Family Cisco XRv9K
Product Series Cisco XRV9000 Series Virtual Routers
Manufacturer Cisco Systems Inc.
Software Type IOS XR
Software Version 6.6.3
Capability YANG_MDT;SNMP;YANG_CLI

▼ Routing Info

ISIS System ID
OSPF Router ID
TE Router ID 10.10.10.10

▼ Streaming Telemetry config

Telemetry Interface default
Source VRF

▼ Location

Civic Address
Latitude 41.900000
Longitude 12.400000
Altitude

▼ Providers and Access

Local Config

Device Key cw-00000000
Provider Name nso7
Credential Profile nso-creds

Compute Config

Provider Name
Credential Profile

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 29](#). For help with creating and deleting tags, see [Manage Tags, on page 26](#).


To filter devices by tags:

-
- Step 1** Display the **Devices** window by choosing **Device 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 24](#)).

-
- Step 1** From the main menu, choose **Device Management > Devices**.
- Step 2** (Optional) 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](#).
- Note** In addition to the existing fields, you can also view the **Data Gateway** configured for the selected device. This field is read-only.
- 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 an 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 Cisco 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 24](#)).
- Step 2** From the main menu, choose **Device 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 **Device Management > Devices**. The **Network Devices** tab is displayed by default.
- Step 2** (Optional) 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
















Device 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 **Device Management > Job History**. The **Inventory Jobs** window displays a log of all device-related jobs, like the one shown below.

Figure 5: 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 	654094-660-489e-051f-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 **Admin > Tags** from the main window.

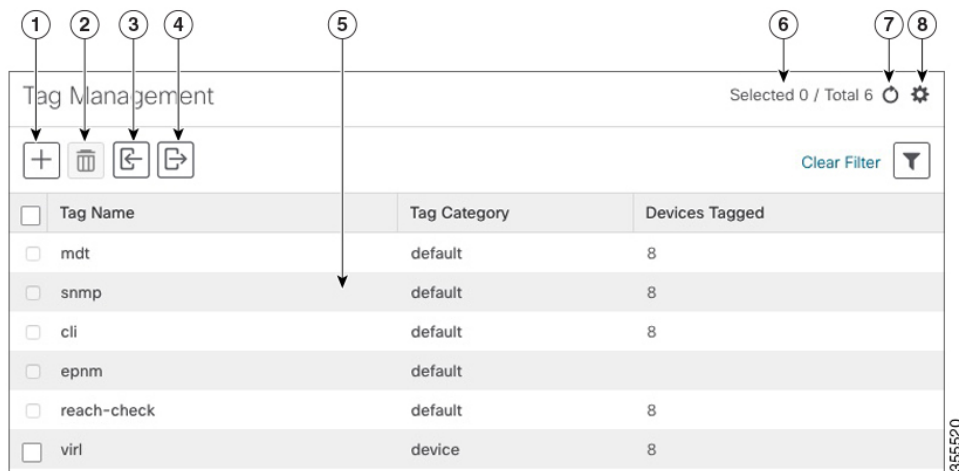


Note Cisco Crosswork Optimization Engine automatically creates a default set of tags and assigns them to every device it manages:






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

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

Figure 6: Tag Management Window



Item	Description
1	Click to create new device tags. See Create Tags .
2	Click to delete currently selected device tags. See Delete Tags .

Item	Description
3	Click  to import the device tags defined in a CSV file into Cisco Crosswork Network Automation. See Import Tags, on page 28 . 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 Export Tags, on page 30 .
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 Tag Management window.
8	Click  to choose the columns to make visible in the Tag Management window (see Set, Sort and Filter Table Data).
	Click  to set filter criteria on one or more columns in the Tag Management window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Create Tags

You can create as many tags and tag categories as you want. If you will have many tags, it might be quicker to list them in a CSV file and import the file, instead of creating each tag individually. See [Import Tags, on page 28](#).



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

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

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

Step 3 In the **Category** area:

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

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

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

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

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

What to do next

Add tags to devices. See [Apply or Remove Device Tags, on page 29](#).

Import Tags

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

When you import the CSV file, any tags not already in the database will be added. Tags with the same name as an imported tag will be overwritten. For this reason, it is a good idea to export a backup copy of all your current tags before import (see [Export Tags, on page 30](#)).

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

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

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

- a) Click the **Download sample 'Tags template (*.csv)' file** link and save the CSV file template to a local storage resource.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each tag. Use a comma to delimit each field within a row. Use a semicolon to separate multiple entries in the same field.

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

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

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

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

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

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

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

What to do next

Add tags to devices. See [Apply or Remove Device Tags, on page 29](#).



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 27](#)).

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

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


-
- Step 1** From the main menu, choose **Device Management > Devices**. The **Network Devices** tab is displayed, showing the list of devices.
 - Step 2** (Optional) If the list is long, click  to set one or more filters and narrow the list to only those devices you want to tag.
 - Step 3** Check the check box next to the device(s) you want to tag. If you select multiple devices, any changes you make will be applied to all the devices you selected.
 - Step 4** From the toolbar, click . The **Modify Tags** window opens, showing the tags currently applied to the device(s) you selected.
 - Step 5** Click in the **Type to autocomplete item** field to display the list of existing tags, or begin typing the name of the tag you want.
 - Step 6** Click on individual tags in the list to add them to the list of tags applied to the device(s). To delete an applied tag, click the X icon shown next to that tag.
-

Delete Tags

To delete device tags, do the following:




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

-
- Step 1** Export a backup CSV file containing the tags you plan to delete (see [Export Tags, on page 30](#)).
 - Step 2** From the main menu, choose **Admin > Tags**. The **Tag Management** window is displayed.
 - Step 3** Check the check box next to the tags you want to delete.
 - Step 4** From the toolbar, click .
 - Step 5** The confirmation dialog box will list the number of devices currently using the tag(s) you are about to delete. Click **Delete** to confirm deletion.
-

Export Tags

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

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