Manage Inventory

This section contains the following topics:

Inventory Management Overview

The Inventory Management application lets you create, edit, and delete:

- The **credential profiles** that control Cisco Crosswork Change Automation and Health Insights's access to devices and providers. See Manage Credential Profiles, on page 3.
- The **providers** who supply special services, such as device configuration, data storage, or alert processing, to Cisco Crosswork Change Automation and Health Insights. See Manage Providers, on page 11.
- The **devices** you manage using Cisco Crosswork Change Automation and Health Insights. See Manage Devices, on page 27.
- The **tags** you use to sort and group devices. See Manage Tags, on page 41.

You can also use Inventory Management to review the **jobs** executed on your devices. See View Device Job History, on page 41.

Reachability and Operational State

Cisco Crosswork Change Automation and Health Insights 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 reachable by any protocol configured for it.
	Reachability Unknown: Cisco Crosswork Change Automation and Health Insights 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.
	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 Visualization application.)
	The device's operational state is currently being checked
	The device is being deleted.

This Icon...	Indicates...
	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 <=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

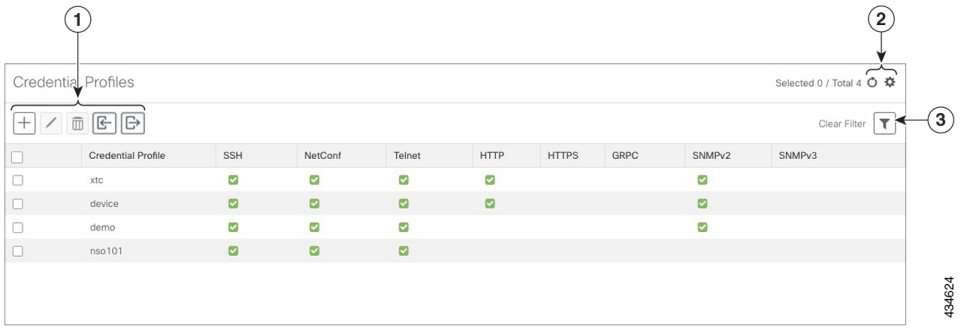
Credential profiles are collections of credentials for SNMP, Telnet/SSH, HTTP, and other network protocols. You can have multiple protocols and credentials in a single credential profile.

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** > **Credential Profiles** from the main menu.

Figure 1: Credentials Profile window



Item	Description
1	Click to add a credential profile. See Create Credential Profiles, on page 5.
	Click to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 8.
	Click to delete the selected credential profile. See Delete Credential Profiles, on page 9.
	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 6.
	Click to export credential profiles to a CSV file. See Export Credential Profiles, on page 9.
2	Click to refresh the **Credential Profiles** window.
	Click to choose the columns to make visible in the **Credential Profiles** window (see Set, Sort and Filter Table Data).
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 6.

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 9).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see Import Credential Profiles, on page 6).

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 8 to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Inventory 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 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.
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	Enter the required **User Name**, **Password**, and **Confirm Password**. The **Enable Password** is optional.
HTTP	Enter the required **User Name**, **Password**, and **Confirm Password**.

Connectivity Type	Fields
HTTPS	Enter the required **User Name**, **Password**, and **Confirm Password**.
GRPC	Enter the required **User Name**, **Password**, and **Confirm Password**.
SNMPv3	Choose the required **Security Level** and enter the **User Name**. If you chose the NO_AUTH_NO_PRIV **Security Level** of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional. If you chose the AUTH_NO_PRIV **Security Level**, you must choose an **Auth Type** and enter an **Auth Password**. If you chose the AUTH_PRIV **Security Level**, you must choose an **Auth Type** and **Priv Type**, and enter an **Auth Password** and **Priv Password**. Only the following SNMPv3 Privacy Types are supported • CFB_AES_128 • CBC_DES_56 The following Privacy Types are not supported: • 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 Change Automation and Health Insights.

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 8 to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Inventory 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 may result in loss of device connectivity, and inability to collect certain KPI data or execute configured Playbooks on devices associated with the credential profile.
- 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: **`nso`**.	Required
Connectivity Type	Valid values are: **`SSH`**, **`SNMPv2`**, **`NETCONF`**, **`TELNET`**, **`HTTP`**, **`HTTPS`**, **`GRPC`** or **`SNMPv3`**	Required
User Name	For example: **`NSOUser`**	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`**	Required if **Connectivity Type** is **`SSH`** or **`TELNET`**. Otherwise leave blank.
Enable Password Value	Specify the Enable password to use.	Required if **Connectivity Type** is **`SSH`** or **`TELNET`** and **Enable Password** is set to **`ENABLE`**. Otherwise leave blank.
SnmpV2 Read Community	For example: **`readprivate`**	Required if **Connectivity Type** is **`SNMPv2`**
SnmpV2 Write Community	For example: **`writeprivate`**	Required if **Connectivity Type** is **`SNMPv2`**

Field	Entries	Required or Optional
SnmpV3 User Name	For example: **DemoUser**	Required if **Connectivity Type** is **SNMPv3**
SnmpV3 Security Level	Valid values are **noAuthNoPriv**, **AuthNoPriv** or **AuthPriv**	Required if **Connectivity Type** is **SNMPv3**
SnmpV3 Auth Type	Valid values are **HMAC_MD5** or **HMAC_SHA**	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthNoPriv** or **AuthPriv**
SnmpV3 Auth Password	The password for this authorization type.	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthNoPriv** or **AuthPriv**
SnmpV3 Priv Type	Valid values are **CFB_AES_128** or **CBC_DES_56** The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthPriv**
SnmpV3 Priv Password	The password for this privilege type.	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthPriv**

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

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

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

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

The credential profiles you imported should now be displayed in the **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, inability to collect certain KPI data, or an inability to execute configured playbooks on devices associated with the modified profile. For example: If the SNMP community string on the device no longer matches what is in the credential profile, SNMP-based KPIs will not function.

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 9).

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

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 9).

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** > **Credential Profiles**) 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 10 or Change the Credential Profile for Multiple Devices, on page 10, and Edit Providers, on page 26).

Step 4 After all devices and providers have had their credential profiles reassigned: From the main menu, choose **Inventory 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 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 8 to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Inventory 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 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 5.

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 40).
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 32).

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 .

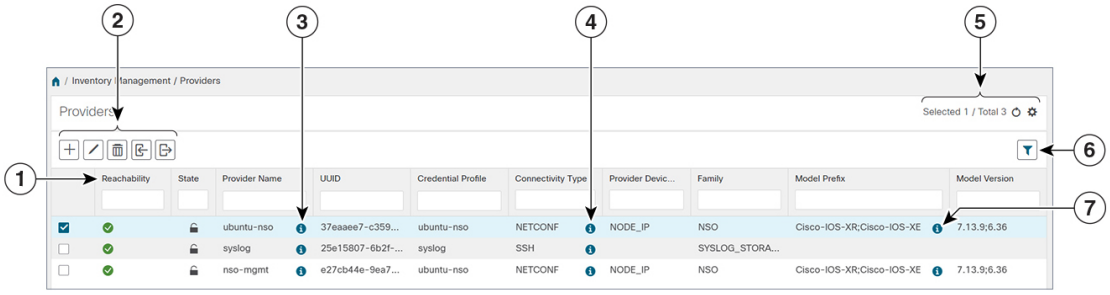
Step 5 In the **Import** dialog box, click **Browse**, choose the new CSV file, and click **Import**.

Manage Providers

Cisco Crosswork Change Automation and Health Insights communicates with external providers. You decide which providers you will use and then configure them. Cisco Crosswork Change Automation and Health Insights stores the provider connectivity details and makes that information available to 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



Item	Description
1	The icon shown next to the provider in this column indicates the provider's **Reachability**. For more on the icons and how reachability is determined, see Reachability and Operational State, on page 1.

Item	Description
2	Click to add a provider. See About Adding Providers, on page 13.
	Click to edit the settings for the selected provider. See Edit Providers, on page 26.
	Click to delete the selected provider. See Delete Providers, on page 26.
	Click to import new providers or update existing providers from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Providers, on page 16.
	Click to export a provider to a CSV file. See Export Providers, on page 27.
3	Click next to the provider in the **Provider Name** column to open the **Properties for** pop-up window, showing the details of any startup session key/value pairs for the provider.
4	Click next to the provider in the **Connectivity Type** column to open the **Connectivity Details** pop-up window, showing the protocol, IP and other connection information for the provider.
5	Click to refresh the **Providers** window.
	Click to choose the columns to make visible in the Providers window (see Set, Sort and Filter Table Data).
6	Click to set filter criteria on one or more columns in the **Providers** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.
7	Click next to the provider in the **Model Prefix** column to open the **Supported Models** pop-up window, showing a list of the model prefix names and versions in use (for Cisco NSO providers only).

About Provider Families

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

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

Table 2: Supported Provider Families

Provider Family	Description
NSO	Instances of Cisco Network Services Orchestrator (Cisco NSO), used to configure network devices. See Add Cisco NSO Providers, on page 18.
WAE	Instances of Cisco WAN Automation Engine (Cisco WAE) provide "what if" analysis used to evaluate network changes as part of Cisco Crosswork Change Automation and Health Insights Playbooks. See Add Cisco WAE Providers, on page 22.
SR-PCE	Instances of Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) containing the configuration information needed to allow Cisco Crosswork Change Automation and Health Insights to communicate with and retrieve segment routing information for the network. See Add Cisco SR-PCE Providers, on page 19.
Syslog Storage	Instances of storage servers (remote or on the Cisco Crosswork Change Automation and Health Insights VM itself) where you want store syslogs and other data retrieved from devices by KPIs and Playbooks. See Add Syslog Storage Providers, on page 23.
Alert	Instances of providers (such as Cisco Crosswork Situation Manager) to which alerts collected during KPI monitoring are to be forwarded. See Add an Alert Provider, on page 24

About Adding Providers

Cisco Crosswork Change Automation and Health Insights depends on a variety of providers to perform various functions. For example, Cisco Network Services Orchestrator provides device and routing information. Features that depend on new providers may be added in the future, and you may need to communicate with more than one instance of a single provider. Also, not every Cisco Crosswork Change Automation and Health Insights deployment will use the same mix of providers. In any case, to access each provider's services, the provider must be added to the Cisco Crosswork Change Automation and Health Insights system configuration.

There are two ways to add providers:

1. **Adding providers via the UI**: This method is explained in Add Providers Through the UI, on page 14. Although this method is the most time-consuming, it is more often used because most deployments will not need a lot of separate providers or provider instances.
2. **Importing providers from a providers CSV file**: This method is explained in Import Providers, on page 16. Importing a CSV file is useful when you have a lot of separate providers or provider instances to add or update at one time.

Note that both methods require that you:

- Create a corresponding credential profile, beforehand, so that Cisco Crosswork Change Automation and Health Insights can access the provider. For help, see Create Credential Profiles, on page 5.
- Know the protocol, IP address, port number, and other information needed to connect with the provider.

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

For help on adding the most common providers using the UI, see the following topics.

Add Providers Through the UI

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

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

Step 2 Click +.

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

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

Step 5 (Optional) Repeat to add more providers.

Table 3: Add Provider Fields (=required)*

Field	Description
* **Provider Name**	The name for the provider that will be used to refer to it in Cisco Crosswork Change Automation and Health Insights. For example: **`MyWAE`**. The name can contain a maximum of 128 alphanumeric characters, plus underscores ("_") or hyphens ("-"). No other special characters are allowed.
* **Credential Profile**	Select the name of the credential profile that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider.
* **Family**	Select the provider family. Choices are: **`NSO`**, **`WAE`**, **`SR-PCE`**, **`ALERT`** and **`SYSLOG_STORAGE`**.
* **Device Key**	Select the method that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way Cisco Crosswork Change Automation and Health Insights maps the device in its own inventory to the device as it is stored in the Cisco NSO provider. Choices are: • **`NODE_IP`**—Use this value if the device identifier Cisco NSO uses is the IP address. • **`INVENTORY_ID`**—Use this value if the device identifier Cisco NSO uses is the inventory ID. • **`HOST_NAME`**—If Cisco NSO uses the device hostname as the device identifier, this value must match the hostname that is specified for the device in the inventory. Note that the **Device Key** is only required for the Cisco NSO provider. It is not needed for other providers.
Connection Type(s)	

Field	Description
*** Protocol**	Select the principal protocol that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. Options include: **`HTTP`**, **`HTTPS`**, **`SSH`**, **`SNMP`**, **`NETCONF`**, **`TELNET`**, and more. To add more connectivity protocols for this provider, click  at the end of the first row. To delete a protocol you have entered, click  shown next to that row. You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol.
*** IP Address/ Subnet Mask**	Enter the IP address (IPv4 or IPv6) and subnet mask of the provider's server.
*** Port**	Enter the port number to use to connect to the provider's server. This is the port corresponding to the protocol being configured. For example, if the protocol used to communicate with the provider server is SSH, the port number is usually 22.
Timeout	Enter the amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.
Model Prefix Info	
*** Model**	Required only if you are adding a Cisco NSO provider: Select the model prefix that matches the NED CLI used by Cisco NSO. Valid values are: **`Cisco-IOS-XR`** **`Cisco-NX-OS`** **`Cisco-IOS-XE`** For telemetry, only **`Cisco-IOS-XR`** is supported. To add more model prefix information for this Cisco NSO provider, click the  at the end of any row in the **Model Prefix Info** section. To delete a model prefix you have entered, click the  shown next to that row.
*** Version**	Required only if you are adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the NSO server.
Provider Properties	
Property Key	Enter the name of the key for the special provider property you want to configure. Provider properties control how Cisco Crosswork Change Automation and Health Insights interacts with the provider. Not all providers need them, and the number and type of properties vary with the provider family. These properties are documented in topics about adding specific providers elsewhere in this Guide. Please note, however, that Cisco Crosswork Change Automation and Health Insights does not validate provider properties. Make sure the properties you enter are valid for the provider.

Field	Description
Property Value	Enter the value to assign to the property key. To add more special properties for this provider, click  at the end of any key/value pair in the **Provider Properties** section. To delete a key/value pair you have entered, click  shown next to that pair.

Import Providers

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

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 27).

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:

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

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

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

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

Field	Description	Required or Optional
Provider Name	Enter the name for the provider that will be used in Cisco Crosswork Change Automation and Health Insights. For example: **`MyWAE`**.	Required

Field	Description	Required or Optional
Connectivity Type	Enter the name of the protocol that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. Valid values are: **ROBOT_MSVC_TRANS_TCP**, **ROBOT_MSVC_TRANS_UDP**, **ROBOT_MSVC_TRANS_HTTP**, **ROBOT_MSVC_TRANS_HTTPS**, **ROBOT_MSVC_TRANS_GRPC**, **ROBOT_MSVC_TRANS_SSH**, **ROBOT_MSVC_TRANS_NETCONF**, **ROBOT_MSVC_TRANS_TELNET**, **ROBOT_MSVC_TRANS_SNMP**, **ROBOT_MSVC_TRANS_TL1**, **ROBOT_MSVC_TRANS_TL1_SECURE**, **ROBOT_MSVC_TRANS_ICMP**, **ROBOT_MSVC_TRANS_KAFKA**, **ROBOT_MSVC_TRANS_NATS**.	Required
Connectivity IP	Enter the IP address (IPv4 or IPv6) of the provider.	Required
Connectivity Port	Enter the port number to use to connect to the provider's server.	Required
Connectivity Timeout	Enter the amount of time (in seconds) to wait before the connection to the provider times out. The default is 30 seconds.	Required
Credential Profile	Enter the name of the credential profile that Cisco Crosswork Change Automation and Health Insights will use to connect to the provider. This profile must already exist in the system.	Required
Provider Device Key	Enter the enum value corresponding to the key that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way Cisco Crosswork Change Automation and Health Insights maps the device to the Cisco NSO provider. Valid values are: • **ROBOT_PROVDEVKEY_HOST_NAME**—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. • **ROBOT_PROVDEVKEY_NODE_IP**—Use this enum value if the NSO device identifier is the IP address for the Node IP value in the CSV file. • **ROBOT_PROVDEVKEY_INVENTORY_ID**—Use this enum value if the inventory ID is the device identifier for NSO. This entry is only required if you are creating or updating a Cisco NSO provider.	Required
Family	Enter the provider family. Valid entries are: **WAE**, **SYSLOG_STORAGE**, **ALERT**, **SR_PCE**, and **NSO**.	Required
Model Prefix	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: **Cisco-IOS-XR**, **Cisco-NX-OS**, **Cisco-IOS-XE**. For telemetry, only Cisco-IOS-XR is supported.	Required for Cisco NSO providers only

Field	Description	Required or Optional
Model Version	If you adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the Required for Cisco NSO only server (should be 6.0.4).	Required for Cisco NSO providers only
Properties	Enter the name of the key for the special provider property you want to configure. See the documentation on adding individual providers for property key/value requirements. Cisco Crosswork Change Automation and Health Insights does not validate provider property key names or values. Make sure the properties you enter are valid for the provider.	Required for some providers, otherwise optional

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.

Add Cisco NSO Providers

Cisco Network Services Orchestrator (Cisco NSO) providers supply device management and configuration maintenance services to Cisco Crosswork Change Automation and Health Insights.

Follow the steps below to add (through the UI) one or more instances of Cisco NSO as providers for Cisco Crosswork Change Automation and Health Insights. You can also add providers using CSV files (see Import Providers, on page 16).

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see Create Credential Profiles, on page 5).

  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 31).

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**: Enter a name for the provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **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 Cisco Crosswork Change Automation and Health Insights maps the device to Cisco NSO. Choices are: **`NONE`**, **`NODE_IP`**, **`INVENTORY_ID`**, or **`HOST_NAME`**.
- **IP Address/Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the Cisco NSO server.
- **Port**: Enter the port to use to connect to the Cisco NSO server. 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. Add a model for each type of device that will be used in the topology. If you have more than one, select to add another supported model.
- **Version**: Enter the Cisco NSO NED driver version used on the NSO server.

For more information on fields, see Import Providers, on page 16.

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.

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

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 Change Automation and Health Insights. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices that are part of the topology using XR Topology Controller (XTC).

Follow the steps below to add (through the UI) one or more instances of Cisco SR-PCE as providers for Cisco Crosswork Change Automation and Health Insights.

Before you begin

You will need to:

- Create a credential profile for the Cisco SR-PCE provider (see Create Credential Profiles, on page 5). 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. Your options, set using the **Provider Properties** fields, are as follows:
  - **`auto-onboard`** is **`off`**: If you set these **Provider Properties** values, you will add or import devices manually. When Cisco SR-PCE discovers devices, the device data is recorded in the Cisco SR-PCE database, but is not registered in the Cisco Crosswork Change Automation and Health Insights Inventory Management database.
  - **`auto-onboard`** is **`unmanaged`**: If you set these **Provider Properties** values, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Change Automation and Health Insights Inventory Management database, with their configured state set to **`unmanaged`**. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the **`managed`** state later, you will need to download them as a CSV file (see Export Devices, on page 40), 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 Import Devices, on page 32). You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).
  - **`auto-onboard`** is **`managed`**: If you set these **Provider Properties** values, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Change Automation and Health Insights Inventory Management database, with their configured state set to **`managed`**. Their connectivity IP addresses will be set to their router IDs, and SNMP polling will be enabled. For successful SNMP polling, you will have to correct the connectivity IP address. You can do this by editing the device, or use the device CSV import feature to correct it. You will also need to add a second **Provider Properties** key/value pair, with the key **`device-profile`** and the value being the name of an SNMP credential profile for the new devices.
  - **`outgoing-interface`**: Cisco SR-PCE reachability can be established over management network by providing **`outgoing-interface`** and **`eth1`** as the property key/value pair. If this property is set, a static route is installed on the Cisco Crosswork Change Automation and Health Insights pointing to the **`eth1`** interface gateway. You can do this by editing the device or using the device CSV import feature to correct it.
- If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:
  - Assign an existing credential profile for communication with the new managed devices.
  - The credential profile must be configured with an SNMP protocol.
- For high availability, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations .

Step 1 From the main menu, choose **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 Change Automation and Health Insights.
- **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.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Provider Properties**: Enter one of the following key/value pairs in the first set of fields:

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 value:

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

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

Step 5 Confirm that the SR-PCE provider shows a green Reachability status without any errors. You can also view the Events window 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.

Add Cisco WAE Providers

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

Follow the steps below to use the UI to add one or more instances of Cisco WAE as providers. You can also add providers using CSV files (see About Adding Providers, on page 13).

Before you begin

You will need to:

- Create a credential profile for the Cisco WAE provider (see Create Credential Profiles, on page 5). This should be a basic HTTP/HTTPS text-authentication credential (currently, MD5 authentication is not supported). If the Cisco WAE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP/HTTPS protocol.
- Know the name you want to assign to the provider. This is usually the DNS hostname of the Cisco WAE server.
- Know the Cisco WAE server IP address and port. The connection protocol will be HTTP or HTTPS.

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

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the Cisco WAE provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile**: Select the previously created credential profile.
- **Family**: Select **`WAE`**.
- **Protocol**: Select **`HTTP`** or **`HTTPS`** respectively as per the credential profile you are using.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port**: Enter the port number (usually, **`8080`** for HTTP, and **`8083`** for HTTPS).

b) Optional values:

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

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

Add Syslog Storage Providers

Storage providers supply storage for data collected during KPI monitoring, Playbook execution, and other operations (such as syslog storage).

Follow the steps below to use the UI to add one or more storage providers for Cisco Crosswork Change Automation and Health Insights. You can also add providers using CSV files (see About Adding Providers, on page 13).

Before you begin

You will need to:

- Create a credential profile for the storage provider (see Create Credential Profiles, on page 5). This should be an SSH or HTTPS credential, depending on the protocol you plan to use (SSH is recommended).
- Know the name you want to assign to the storage provider. This is usually the DNS hostname of the server.
- Know the storage provider's server IPv4 address and port. The connection protocol will be SSH or HTTPS.
- Know the destination directory on the storage provider's server. You will need to specify this using the **Provider Properties** fields.

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

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the storage provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile**: Select the previously created storage credential profile.
- **Family**: Select **`SYSLOG_STORAGE`**.
- **Protocol**: Select **`SSH`** or **`HTTPS`**.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port**: Enter the port number (usually, **`22`** for SSH or **`443`** for HTTPS).
- **Provider Properties**: Enter the following key/value pair in these fields:

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

b) Optional values:

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

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

Add an Alert Provider

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

Follow the steps below to use the UI to add an alert provider for Cisco Crosswork Change Automation and Health Insights. You can also add the alert provider by importing a CSV file (see About Adding Providers, on page 13).

Currently, only one alert provider is supported.

Before you begin

You will need to:

- Create a credential profile for the alert provider (see Create Credential Profiles, on page 5). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the provider does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the alert provider. This is usually the DNS hostname of the server.
- Know the alert server IPv4 address and port. The connection protocol will be HTTP.
- Know the URL of the alert server endpoint. You will need to specify this using the **Property Value** field.

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

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the provider that will be used in Cisco Crosswork Change Automation and Health Insights.
- **Credential Profile**: Select the previously created alert provider credential profile.
- **Family**: Select **`ALERT`**.
- **Protocol**: **`HTTP`** is pre-selected.
- **IP Address/ Subnet Mask**: Enter the IP Address (IPv4 or IPv6) and subnet mask of the alert server.
- **Port**: Enter the port number (usually, 80 for HTTP).
- **Provider Properties**: The **`alertEndpointUrl`** property key name is pre-entered. In the Property Value field, enter the alert server endpoint only. For example, if the complete path to the endpoint is **`http://aws.amazon.com:80/myendpoint/bar1/`**, you would enter **`/myendpoint/bar1/`** only.

b) Optional values:

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

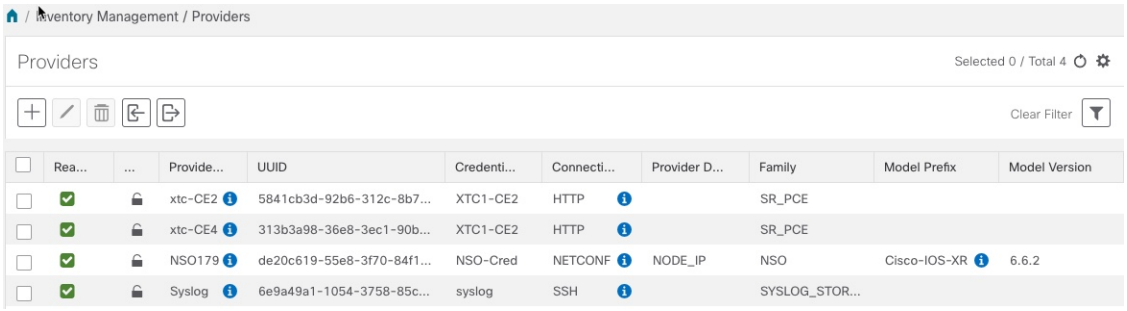
Step 4 When you have completed entries in all of the required fields, click **Save** to add the alert provider.

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 Change Automation and Health Insights, 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



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 1.

Cisco Crosswork Change Automation and Health Insights checks provider reachability immediately after a provider is added or modified. Other than these events, Cisco Crosswork Change Automation and Health Insights checks reachability every 5 minutes.

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

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

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

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

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

If you are running into provider reachability problems, you can troubleshoot as follows:

a. Ping the provider host.

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

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

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

c. Check your firewall setting and network configuration.

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

Edit Providers

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

Note

- Before making any changes to a provider configuration you should be certain that you understand the full impact of the change. If you are unsure about the potential risk of making a change, contact Cisco services for guidance.
- See Add Cisco SR-PCE Providers, on page 19 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 27).

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 Change Automation and Health Insights. This avoids Cisco Crosswork Change Automation and Health Insights from rediscovering and adding the device back.
- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork Change Automation and Health Insights. However, doing so will not allow Cisco Crosswork Change Automation and Health Insights 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 27).

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

a) From the main menu, choose **Inventory Management** > **Devices**.
b) In the **Devices** window, enter the obsolete provider name in the **Search** field.
c) Check the check box for the device that is mapped to the obsolete provider, and click .
d) Choose a different provider from the **Provider** drop-down list.
e) Click **Save**.

Step 3 Delete the provider as follows:

a) From the main menu, choose **Inventory Management** > **Providers**.
b) In the **Providers** window, choose the provider(s) that you want to delete and click .
c) In the confirmation dialog box, click **Delete**.

Export Providers

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

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

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

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

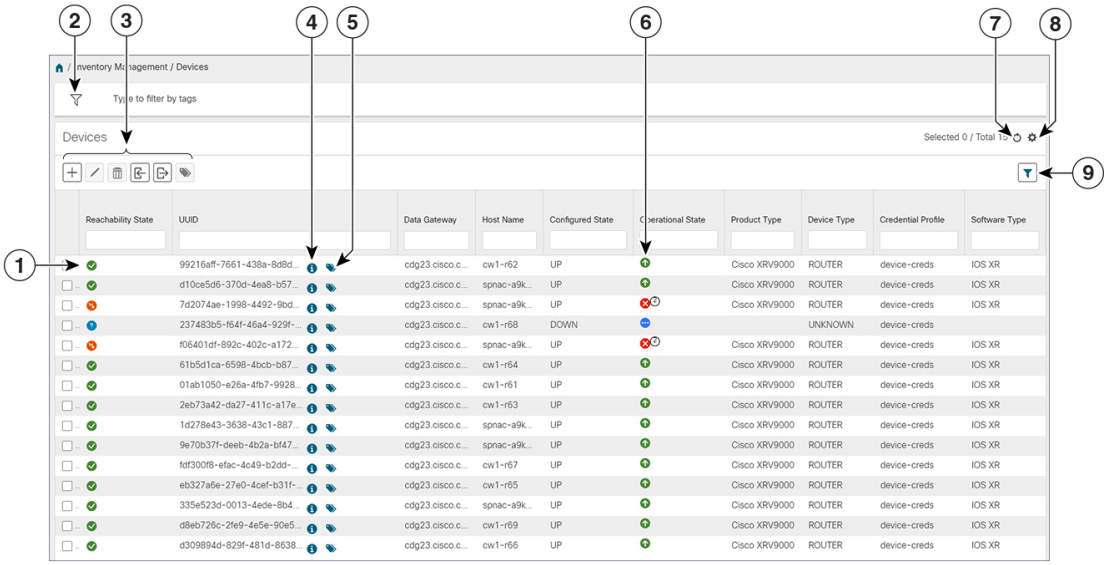
Step 3 Check the check boxes for the providers you want to export. Check the check box at the top of the column to select all the providers for export.

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.

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 4: Devices Window



Item	Description
1	Icons in the **Reachability State** column show whether a device is reachable or not. See Reachability and Operational State, on page 1.
2	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 38.
3	Click to add a new device to the device inventory. See About Adding Devices to Inventory, on page 29.
	Click to edit the information for the currently selected devices. See Edit Devices, on page 39.
	Click to delete the currently selected devices. See Delete Devices, on page 39.
	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 32.
	Click to export information for selected devices to a CSV file. See Export Devices, on page 40.
	Click to modify tags applied to the selected devices. See Apply or Remove Device Tags, on page 44.
4	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 37.

Item	Description
5	Click  to see all the tags that have been applied to the device. See Manage Tags, on page 41.
6	Icons in the **Operational State** column show whether a device is operational or not. See Reachability and Operational State, on page 1
7	Click  to refresh the Devices list.
8	Click  to select which columns to display in the Devices list (see Set, Sort and Filter Table Data).
9	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.

About Adding Devices to Inventory

There are four ways to add devices to Cisco Crosswork Change Automation and Health Insights. Each has its own set of prerequisites, which you must fulfill if the device addition is to succeed.

In order of preference for most users, the methods and their prerequisites are:

1. **Importing devices using the Cisco Crosswork Change Automation and Health Insights APIs:** : This is the fastest and most efficient of the three methods, but requires programming skills and API knowledge. For more, see the inventory management APIs on Cisco Devnet.
2. **Importing devices from a Devices CSV file**: This method is explained in Import Devices, on page 32. This method is time-consuming and error-prone, as you must create and format 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 after the CSV import. To succeed with this method, you must first:
   - Create the provider(s) that will be associated with the devices (see Manage Providers, on page 11)
   - Create corresponding credential profiles for all of the devices and providers listed in the CSV file (see Create Credential Profiles, on page 5)
   - Create tags for use in grouping the new devices (see Manage Tags, on page 41)
   - Download the CSV template file from Cisco Crosswork Change Automation and Health Insights and populate it with all the devices you will need.
3. **Adding them via the UI**: This method is explained in Add Devices Through the UI, on page 33. It is the least error-prone of the three methods, as all data is validated during entry, but also the most time-consuming, being suitable only for adding a few devices at a time. Note that the providers, credential profiles and tags you want to apply to them must exist beforehand.
4. **Auto-onboarding from a Cisco SR-PCE provider**: This method is explained in Add Cisco SR-PCE Providers, on page 19. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After onboarding devices from this source, you will need to edit each device to add device information that is not automatically discovered.

5. **Onboard the devices on Cisco Crosswork Data Gateway**: This method is explained in Attach a Device to a Cisco Crosswork Data Gateway Instance.

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 Change Automation and Health Insights. 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 Change Automation and Health Insights.

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 should not be included as one of the protocols to verify reachability and operational state for the onboarded devices.

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 (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>
```

Pre-Onboarding SNMPv2 and SNMPv3 Trap Configuration

If you want the device to send SNMP traps to Cisco Crosswork Change Automation and Health Insights, use the following commands to perform a pre-onboarding device configuration and test for the trap version you want.

For SNMP v2 traps:

```
snmp-server trap link ietf

snmp-server host <CrossworkVMDataPortIPAddress> traps version 2c cisco123 udp-port 30162

snmp-server community cisco123

snmp-server traps snmp linkup

snmp-server traps snmp linkdown
```

For SNMP v3 traps:

```
snmp-server trap link ietf

snmp-server host <CrossworkVMDataPortIPAddress> traps version 3 cisco123 udp-port 30162

snmp-server community cisco123

snmp-server traps snmp linkup

snmp-server traps snmp linkdown
```

Please note that, for traps to be received, the node_ip field for the device as listed in the Cisco Crosswork Change Automation and Health Insights inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork Change Automation and Health Insights will reject the traps. Also, the device needs to be in ADMIN_UP state for traps to be received.

Sample Configuration for Devices in Cisco NSO

If you plan to use Cisco NSO as a provider to configure devices managed by Cisco Crosswork Change Automation and Health Insights, 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
```

Import Devices

Complete the steps below to create a CSV file that specifies multiple devices and then import it into Cisco Crosswork Change Automation and Health Insights.

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 31.

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 mandatory values you must enter, see the "Add New Device" field table in Add Devices Through the UI, on page 33.

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 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 Change Automation and Health Insights 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. For the bulk of your devices, add them either by synchronization with a provider (see Add Cisco SR-PCE Providers, on page 19), or by importation from a CSV file (see Import Devices, on page 32).

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 30.

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 4: Add New Device Window (=Required)*

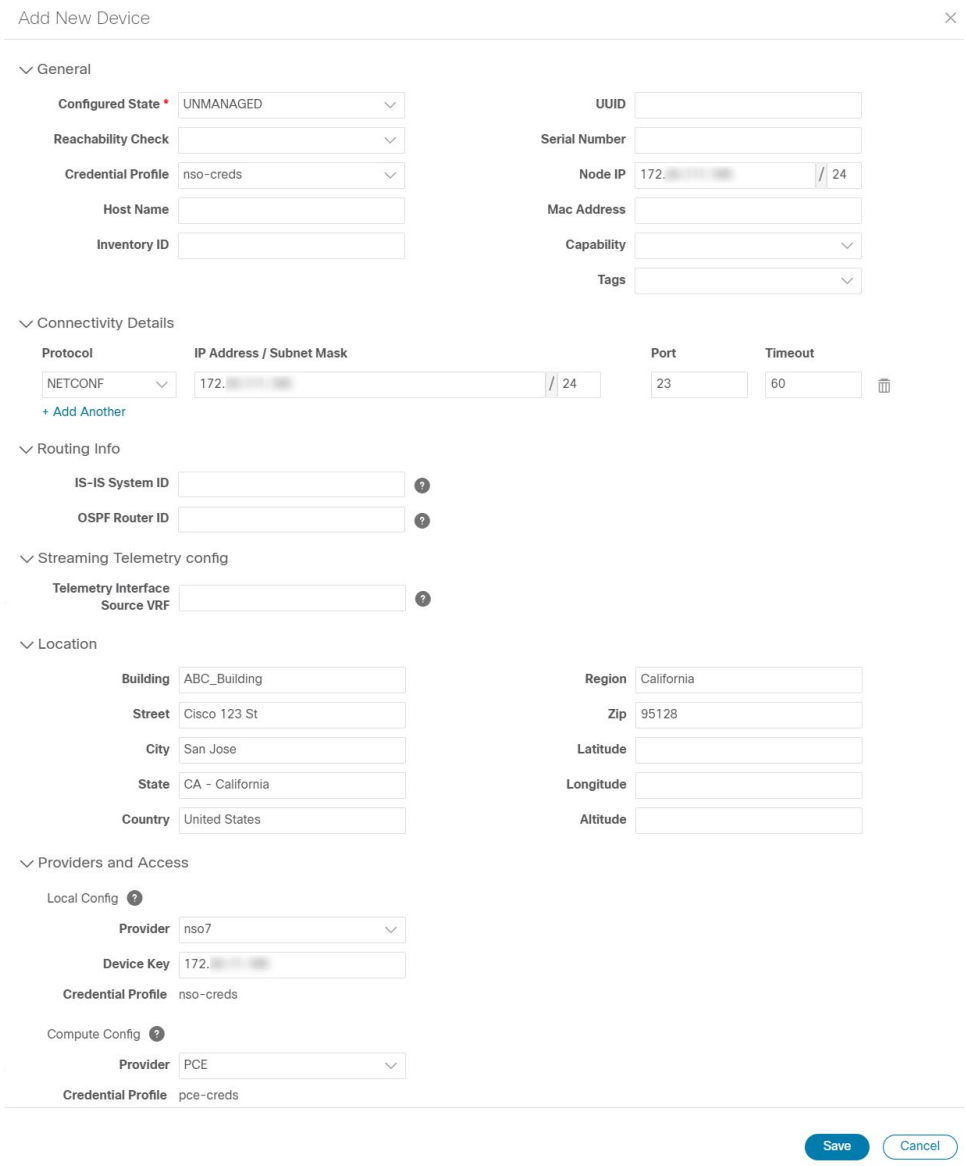
Field	Description
*** Configured State**	The management state of the device. Options are • **UNMANAGED**—Cisco Crosswork Change Automation and Health Insights is not monitoring the device. • **DOWN**—The device is being managed and is down. • **UP**—The device is being managed and is up.
*** Reachability Check**	Determines whether Cisco Crosswork Change Automation and Health Insights performs reachability checks on the device. Options are: • **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. Cisco recommends that you always set this to **ENABLE**. This field is optional if **Configured State** is marked as **UNMANAGED**.
*** 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 Change Automation and Health Insights discovers it and updates it.
Inventory ID	Inventory ID value for the device.
UUID	Universally unique identifier (UUID) for the device.
Serial Number	Serial number for the device.
Node IP	IP address of 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	The connectivity protocols used by the device. Choices are: **SSH**, **SNMPv2**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **GRPC**, and **SNMPv3**. 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. 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.
*** IP Address / Subnet Mask**	Enter the device's IP address (IPv4 or IPv6) and subnet mask.
*** Port**	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: • SSH: 22 • SNMP: 161 • NETCONF: 830 • TELNET: 23 • HTTP: 80 • HTTPS: 443
Timeout	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.
Routing Info	
ISIS System ID	The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.
OSPF Router ID	The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.
Streaming Telemetry Config	
Telemetry Interface Source VRF	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
Location All location fields are optional, with the exception of **Longitude** and **Latitude**, which are required for the geographical view of your network topology.	

Field	Description
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: **Device Key** and **Provider**	Provider type used to configure devices. Choose a provider from the list. If a Cisco NSO provider is chosen, the Device Key will automatically populate and the Credential Profile appears. For CSV entry, use ROBOT_PROVIDER_LOCAL_CONFIG and enter the Provider name.
Compute Config: **Provider**	Provider type used for topology computation. Choose a provider from the list. For CSV entry, use ROBOT_PROVIDER_COMPUTE and enter the Provider name.

Example

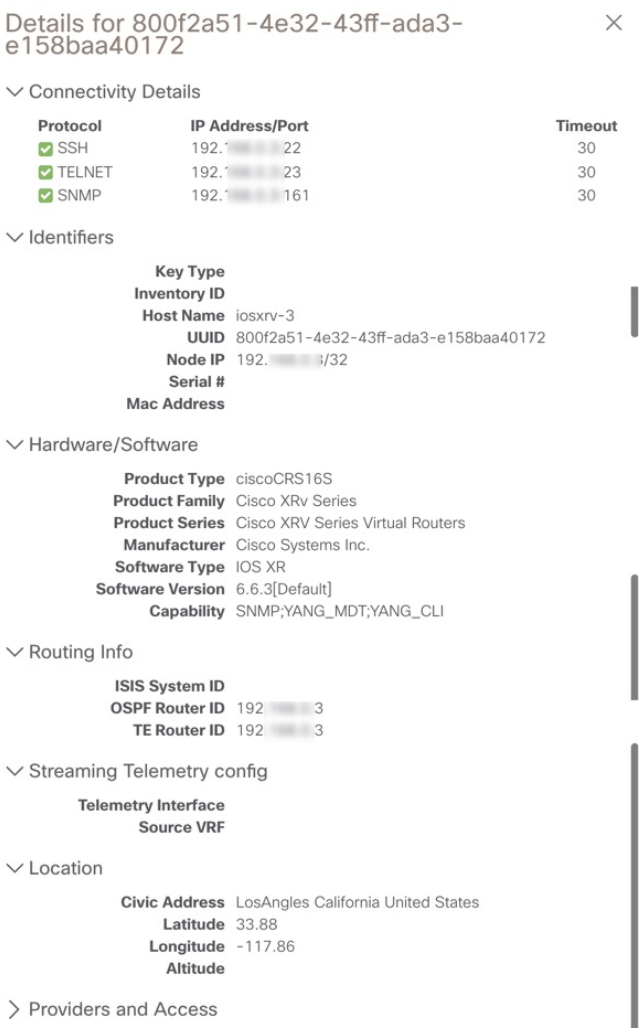
Figure 5: Add New Device Window



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 6: 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 ✕ 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 44. For help with creating and deleting tags, see Manage Tags, on page 41.

To filter devices by tags:

Step 1 Display the **Devices** window or the **Network Topology** map:

a) Display the **Devices** window by choosing **Inventory Management** > **Devices**.

b) Display the topology map by choosing **Network Visualization** > **View Topology**.

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:

a) Repeat Steps 2 and 3 for each additional tag you want to set as part of the filter.

b) 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 40).

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.

Note In addition to the exising 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.

Step 1 Export a backup CSV file containing the devices you plan to delete (see Export Devices, on page 40).

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 edit the devices, as follows:

a) Change each device's state to 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.

b) Delete any KPIs currently running on the devices.

c) Abort any Playbooks running on or scheduled to run on the devices.

Step 6 Click .

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

Step 8 After deleting a device from the user interface, delete any telemetry configuration objects on the router that match the regex pattern *.*CW_*.** . For example: You would find and delete router config objects like the three shown below:

```
 !
 destination-group CW_df5068767b68f9f0d9649cb32aca0cde917e5694
   address-family ipv4 172.16.2.31 port 31500
    encoding self-describing-gpb
    protocol tcp
   !
!
  sensor-group CW_df5068767b68f9f0d9649cb32aca0cde917e5694
   sensor-path Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/summary
  !
 subscription CW_df5068767b68f9f0d9649cb32aca0cde917e5694
   sensor-group-id CW_df5068767b68f9f0d9649cb32aca0cde917e5694 sample-interval 120000
   destination-id CW_df5068767b68f9f0d9649cb32aca0cde917e5694
  !
 !
```

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.

Note The exported device CSV file will contain only the name of the credential profile for each device, not the credentials themselves.

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.

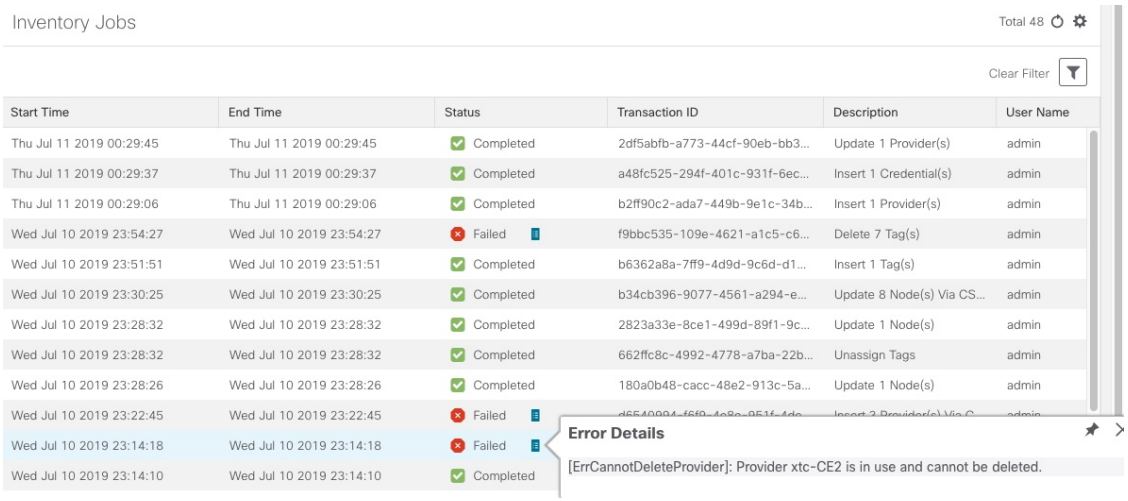
Step 4 Click . Your browser will prompt you to select a path and the file name to use when saving the CSV file, or to open it immediately

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 7: Job History Window With Error Details Popup



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

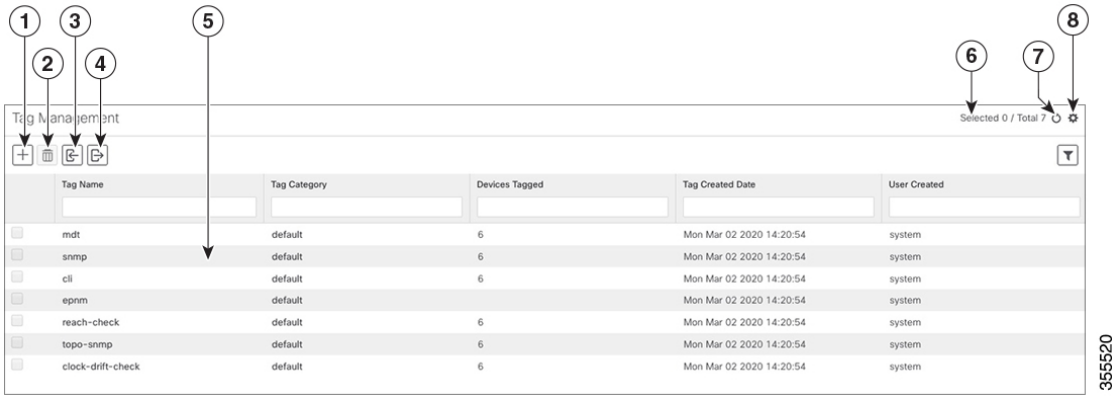
Use the **Tag Management** window to manage the tags available for assignment to the devices in your network. Tags can provide information such as the device's physical location and its administrator's email ID, and are used to group devices.

To open this window, choose **Inventory Management** > **Tags** from the Cisco Crosswork Change Automation and Health Insights main window.

Note Cisco Crosswork Change Automation and Health Insights 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.



Item	Description
1	Click to create new device tags. See Create Tags.
2	Click to delete currently selected device tags. See Delete Tags.
3	Click to import the device tags defined in a CSV file into Cisco Crosswork Change Automation and Health Insights. See Import Tags, on page 44. 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 Change Automation and Health Insights to quickly add or edit multiple tags. See Export Tags, on page 45.
5	Displays the tags currently available in Cisco Crosswork Change Automation and Health Insights and their attributes.

Item	Description
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 44.

Note Tag and tag category names are case-insensitive and can contain up to 128 alphanumeric characters, and can use full stops ("."), underscores ("_"), and hyphens ("-"). They cannot contain other special characters, symbols, or spaces.

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 tags, click **Save**.

What to do next

Add tags to devices. See Apply or Remove Device Tags, on page 44.

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 Change Automation and Health Insights. 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 45).

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

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 44.

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 43).

For efficiency, Cisco Crosswork Change Automation and Health Insights automatically updates inventory data, including topology, for all the devices in a tagged group, as a single set of inventory collection jobs. But please note that tag-group membership is static for other functions. For example, if you add or remove a device

from a tagged group after applying a KPI, the KPI will monitor only the original group members. If you change group membership and want the KPI to monitor all the members of the group, re-apply the KPI to the changed group.

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

Use caution when deleting existing tags. They are used to group devices and deleting them can affect which KPIs are being monitored and the Playbooks run on them.

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 45).

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.