Onboard and Manage Devices

This section contains the following topics:

Add Devices to the Inventory

There are different ways to add devices to Crosswork. Each has its own set of prerequisites, which you must fulfill if the device addition is to succeed. Ensure that your devices are configured properly for communication and telemetry. See guidelines and example configurations in Telemetry Prerequisites for New Devices, on page 3 and Sample Configuration for Cisco NSO Devices, on page 4.

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

1. **Importing devices using the Crosswork APIs:** : This is the fastest and most efficient of all the 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 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 About Adding Providers.

    • Create corresponding credential profiles for all of the devices and providers listed in the CSV file. See Create Credential Profiles.

    • Create tags for use in grouping the new devices. See Create Tags.

    • Download the CSV template file from Crosswork and populate it with all the devices you will need.

3. **Adding them via the UI**: This method is the least error-prone of the three methods, as all data is validated during entry. It is 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. For more information, see Add Devices Through the UI, on page 4.

4. **Auto-onboarding from a Cisco SR-PCE provider**: This method is highly automated and relatively simple. 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. For more information, see the provider properties in Add Cisco SR-PCE Providers.

5. **Auto-onboarding using Zero Touch Provisioning**: This method is automated, but requires that you create device entries first and modify your installation's DHCP server. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After provisioning and onboarding devices using this method, you will need to edit each device to add information that is not automatically supplied. For more information, see Zero Touch Provisioning.

Note   Cisco Crosswork only supports single-stack deployment modes. The devices can be onboarded with either an IPv4 address or an IPv6 address, not both.

If a device onboarded in Cisco Crosswork is on the same subnet as a Cisco Crosswork Data Gateway interface, then it must be on the Cisco Crosswork Data Gateway's southbound network. This is because Cisco Crosswork Data Gateway implements RPF checks and the source address of devices cannot be on the management or northbound networks if multitple NICs (2 or 3 NIC) are deployed.

Note   IOS XR devices (version 7.3.2 or 7.4.1) used for Crosswork Network Controller 3.0 requires NETCONF NED to be configured on Cisco NSO. By default, the NSO policy onboards devices to NSO with CLI NED. You can change to NETCONF NED using the following methods:

- **Before device onboarding:** Change the policy using the API request. For more information, see https://developer.cisco.com/docs/crosswork/#!cat-fp-deployment-manager-api.

- **After device onboarding:**

  1. Change device-type on NSO via cli command (For example, `set devices device <device-name> device-type NETCONF ned-id cisco-iosxr-nc-7.3`).

  2. Perform a device Sync-from operation (For example, `request devices device <device-name> sync-from`).

     Note   Service provisioning may malfunction if the sync operation is not performed (for example, provisioning may display a successful status even when the configuration is not pushed to the device).

Telemetry Prerequisites for New Devices

Before onboarding new devices, you must ensure that the devices are configured to collect and transmit telemetry data successfully with Cisco Crosswork. The following sections provide sample configurations for several telemetry options, including SNMP, NETCONF, SSH and Telnet. Use them as a guide to configuring the devices you plan to manage.

Note   Only SNMPv2 and SNMPv3 (NoAuth/NoPriv) traps are supported.

Pre-Onboarding Device Configuration

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

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
 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>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

SNMPv3 Pre-Onboarding Device Configuration

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

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

Sample Configuration for Cisco NSO Devices

If you plan to use Cisco Network Services Orchestrator (Cisco NSO) as a provider to configure devices managed by Cisco Crosswork, be sure that the Cisco NSO device configurations observe the guidelines in the following example.

This example shows a Cisco NSO configuration that uses the hostname as the device ID. If you are using a CSV file to import devices, use **ROBOT_PROVDEVKEY_HOST_NAME** as the enum value for the provider_node_key field. The example hostname **RouterFremont** used here must match the hostname for the device in the CSV file.

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 830
```

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

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

The following CLI commands unlock and retrieve the SSH keys from all of the devices. Cisco NSO synchronizes itself with the devices by uploading each device's current configuration and then storing the present configuration. It is important to use these commands to ensure that the devices, Cisco NSO, and your Cisco Crosswork applications are starting from a common configuration:

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

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 only when adding a few devices.

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

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 completed.

Step 5 (Optional) Repeat these steps to add more devices.

Table 1: Add New Device Window (*=Required)

Field	Description
* Administration State	The management state of the device. Options are • **UNMANAGED**—Crosswork 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 Crosswork 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 host name of the device.
Inventory ID	Inventory ID value for the device. The value can contain a maximum of 128 alphanumeric characters, and can include dots (.), underscores ("_"), colons (":"), or hyphens ("-"). No other special characters are allowed. Choose the device Host Name or an easily identifiable name for Inventory ID as this will be used to sync the device to Crosswork with the Inventory ID used as the device name.
Software Type	Software type of the device.
Software Version	Software version of the device.
UUID	Universally unique identifier (UUID) for the device.
Serial Number	Serial number for the device.
MAC Address	MAC address of the device.
* Capability	The capabilities that allow collection of device data and that are configured on the device. You must select at least **SNMP** as this is a required capability. The device will not be onboarded if **SNMP** is not configured. Other options are **YANG_MDT**, **YANG_CLI**, **TL1**, and **GNMI**. The capabilities you select will depend on the device software type and version. **Note** For devices with MDT capability, do not select YANG_MDT at this stage.
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.

Field	Description
Product Type	Product type of the device.
Syslog Format	The format in which syslog events received from the device should be parsed by the Syslog Collector. The options are: • **UNKNOWN** - Choose this option if you are uncertain or if you do not want any parsing to be done by the Syslog Collector. The Syslog Collection Job output will contain syslog events as received from device. • **RFC5424** - Choose this option to parse syslog events received from the device in RFC5424 format. • **RFC3164** - Choose this option to parse syslog events received from the device in RFC5424 format. Refer to Section: Syslog Collection Job Output for more details.
Connectivity Details	
Protocol	The connectivity protocols used by the device. Choices are: **SNMP**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **GNMI**, **TL1**, and **GRPC**. **Note** Toggle the **Secure Connection** slider to secure the GNMI protocol that you have selected. 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. **Note** Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues. **Note** If you have multiple protocols with same IP address and subnet mask, you can instruct Crosswork to autofill the details in the other fields.

Field	Description
* 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 GNMI and GNMI_SECURE: The port values range between 57344 to 57999. Ensure that the port number you enter here matches with the port number configured on the device.
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.
Encoding Type	This field is only applicable for **GNMI** and **GNMI_SECURE** protocols. The options are `PROTO` and `JSON IETF`. Based on device capability, only one encoding format is supported at a time in a device.
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.
*TE Router ID	The traffic engineering router ID for the respective IGP. **Note** For visualizing L3 links in topology, devices should be onboarded to Cisco Crosswork with the **TE Router ID** field populated.
IPv6 Router ID	IPv6 router ID for the device. This field is a configurable parameter, and cannot be auto-discovered by Crosswork.
Streaming Telemetry Config	
Vrf	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
Source Interface	The range of loopback in the device type. This field is optional. **Note** This field can be edited only when the device is in DOWN or UNMANAGED state.

Field	Description
Opt Out MDT Config	Enabling this checkbox skips Crosswork from pushing telemetry configuration to the device via NSO. The default setting state is Disabled (which allows Crosswork to push telemetry configuration to the device via NSO). The device must be in ADMIN DOWN state to toggle this setting. Any out of band configuration setup needs to be cleared before moving the setting from Enabled to Disabled.
Location	
All location fields are optional, with the exception of **Longitude** and **Latitude**, which are required for the geographical view of your network topology.	
Longitude, **Latitude**	Longitude and latitude values are required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude and latitude in Decimal Degrees (DD) format.
Altitude	The altitude, in feet or meters, at which the device is located. For example, `123`.
Providers and Access	
To add more providers for this device, click <kbd>+</kbd> at the end of the first row in the **Providers and Access** panel. To delete a provider you have entered, click <kbd>×</kbd> shown next to that row in the panel.	
Provider Family	Provider type used for topology computation. Choose a provider from the list.
Provider Name	Provider name used for topology computation. Choose a provider from the list. **Note** For Cisco NSO LSA deployment, the user can select the resource-facing service (RFS) node to which they want to assign the device.
Credential	The Credential profile used for the provider. This field is read-only and is auto-populated based on the provider you select.

Add Devices By Import From CSV File

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

Importing devices from a CSV file adds any devices not already in the database, and overwrites the data in any device record with an Inventory Key Type field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import). For this reason, it is a good idea to export a backup copy of all your current devices before an import

Note
- While importing large number of devices via a CSV file, value for the **TE Router ID** field should be populated.

- Importing large number of devices with incorrect CSV values using a Firefox browser may render the window unusable. If this happens, login to Cisco Crosswork in a new tab or window, and onboard devices with correct CSV values.

Step 1 From the main menu, choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

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

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

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

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

> **Note**
> - Confirm that the TE router ID value for each device is populated. This value is used to uniquely identify the device in the topology which is learned from SR-PCE. Without a valid TE router ID for each device, the topology will not be displayed.
>
> - After importing a device or onboarding a device, the TE Router ID should not be changed. If it is necessary to change the TE Router ID of a device after it has been imported then then do the following:
>
>   1. The device should be removed from Crosswork.
>
>   2. All SR-PCE Providers should be removed.
>
>   3. Onboard the device again with the new TE Router ID.
>
>   4. Add the SR-PCE providers again.

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

- SSH: port 22

- SNMP: port 161

- NETCONF: port 830

For a list of the fields and the mandatory values you must enter, see the "Add New Device" field table in Add Devices Through the UI, on page 4.

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**.

> **Note** While importing devices or providers via UI using a CSV file, user should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries for each device or provider.

Step 6 Resolve any errors and confirm device reachability.

It is normal for devices to show as unreachable or not operational when they are first imported. However, if they are still displayed as unreachable or not operational after 30 minutes, there may be an issue that needs to be investigated. To investigate, select **Device Management** > **Job History** and click on any error icon 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 server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

Step 7 Once you have successfully onboarded the devices, you must map them to a Cisco Crosswork Data Gateway instance.

Export Device Information to a CSV File

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.

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

Step 2 (Optional) Filter the device list as needed.

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

Step 4 Click the ⇥. 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

Manage Network Devices

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

Figure 1: Network Devices Window
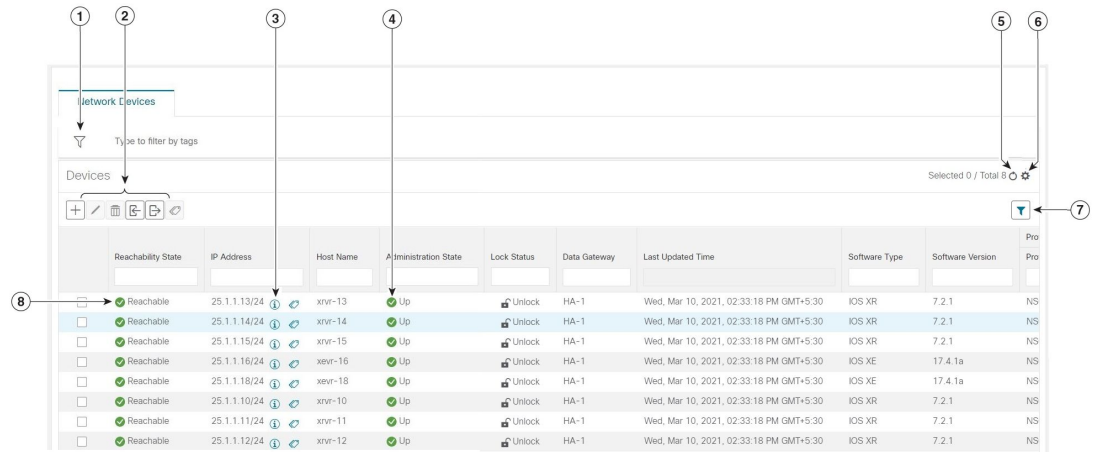
Item	Description
1	The **Filter by tags** field lets you filter the devices by the tags applied to them. Type the name of the tag that has been applied to the device that you are trying to find.
2	Click the ⊞ to add a new device to the device inventory.
	Click the ✎ to edit the information for the currently selected devices. .
	Click the 🗑 to delete the currently selected devices.
	Click the ⬅ 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.
	Click the ➡ to export information for selected devices to a CSV file.
	Click the 🏷 to modify tags applied to the selected devices. See .
3	Click the ⓘ to open the **Device Details** pop-up window, where you can view important information for the selected device.
4	Icons in the **Administration State** column show whether a device is operational or not.
5	Click the ↻ to refresh the Devices list.
6	Click the ⚙ to select which columns to display in the Devices list.
7	Click ▼ to set filter criteria on one or more columns in the Devices list.
	Click the **Clear Filter** link to clear any filter criteria you may have set.
8	Icons in the **Reachability State** column show whether a device is reachable or not.

Device State

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

Table 2: Device 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 cannot determine if the device is reachable, degraded, or unreachable . This state can also occur if the device is not connected to Cisco Crosswork Data Gateway.
Operational State icons show whether a device is operational or not.	
	The device is operational and under management, and all individual protocols are "OK" (also known as "up").
	The device is not operational ("down"). The same icon is used when the device has been set "administratively down" by an operator.
	The device's operational or configuration state is unknown.
	The device's operational or configuration state is degraded.

This Icon...	Indicates...
⊗①	The device's operational or configuration state is in an error condition. It is either not up, or unreachable, or both, due to errors encountered while attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of recent errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available in the Network Topology application).
💬	The device's operational state is currently being checked.
⊗	The device is being deleted.
⊖	The device is unmanaged.
NSO State icons show whether a device is synced with Cisco NSO or not.	
Note In the initial sync between Cisco Crosswork and NSO after onboarding a device, the NSO state column in the device will be blank. This occurs because Cisco Crosswork has not determined if the device needs to sync with NSO based on the policy, and cannot select the default state in the initial sync.	
�	The device is in sync with Cisco NSO.
⚠	The device is out of sync with Cisco NSO.

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

Filter Network 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.

To filter devices by tags:

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

Step 2   In the **Type to filter by tags** bar at the top of the user interface, type all or part of the name of a tag.

The **Type to filter by Tags** bar has a type-ahead feature: As you start typing, the field shows a drop-down list of tags that match all the characters you have typed so far. To force the drop-down list to display all available tags, type **✱**.

Step 3   Choose the name of the tag you want to add to the filter. The filter appears in the **Type to filter by tags** filter bar. The table or map shows only the devices with that tag.

Step 4   If you want to filter on more than one tag:

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.

Get More Information About a Device

Whenever you select **Device Management** > **Network Devices** and display the list of devices under the **Network Devices** tab, you can click the ⓘ 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 2: Details for DeviceName Window

Details for 1bce17d4-5219-

✕

∨ Connectivity Details

Protocol	IP Address/Port	Timeout
☑ SSH	10.	60
☑ TELNET	10.	60
☑ SNMP	10.	60
☑ NETCONF	10.	60

∨ Identifiers

Key Type
Inventory ID
Host Name spnac-a9k-s105
UUID 1bce17d4-5219-
Node IP 10.
Serial # 256E
Mac Address 0050

∨ Hardware/Software

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

∨ Routing Info

ISIS System ID
OSPF Router ID
TE Router ID 10

∨ Streaming Telemetry config

Telemetry Interface default
Source VRF

∨ Location

Civic Address
Latitude 41.9
Longitude 12.4
Altitude

∨ Providers and Access

Local Config

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

Compute Config

Provider Name
Credential Profile

Expand the **Connectivity Details** area at the top of the pop-up window (if it is not already expanded). This area shows the reachability status for all transport types.

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

View Device Job History

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

Step 1   From the main menu, choose **Device Management** > **Inventory Jobs**. The **Inventory Jobs** window opens displaying a log of all device-related jobs, like the one shown below.

Figure 3: Inventory Jobs window

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. Click the column heading again to toggle between ascending and descending sort order.

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

Note   The status may be displayed as **Successful** even when the device is not reachable. You can verify that the status of the jobs that is displayed is correct by also looking into the status of the device (**Device Management** > **Network Devices**).

Use Device Groups to Filter Your Topology View

To help you identify, find, and group devices for a variety of purposes, you can create device groups. Device Groups allow you to visualize and zoom in on data specific to that device group. It reduces the clutter on your screen and allows you to focus on data that is most important to you. For example, as shown in the following figure, we see that the East Coast device group has been selected and is zoomed in on the Topology map. Also note that only the devices belonging to the East Coast device group are listed in the Devices table.

Figure 4: Device Group Selection on Topology Map
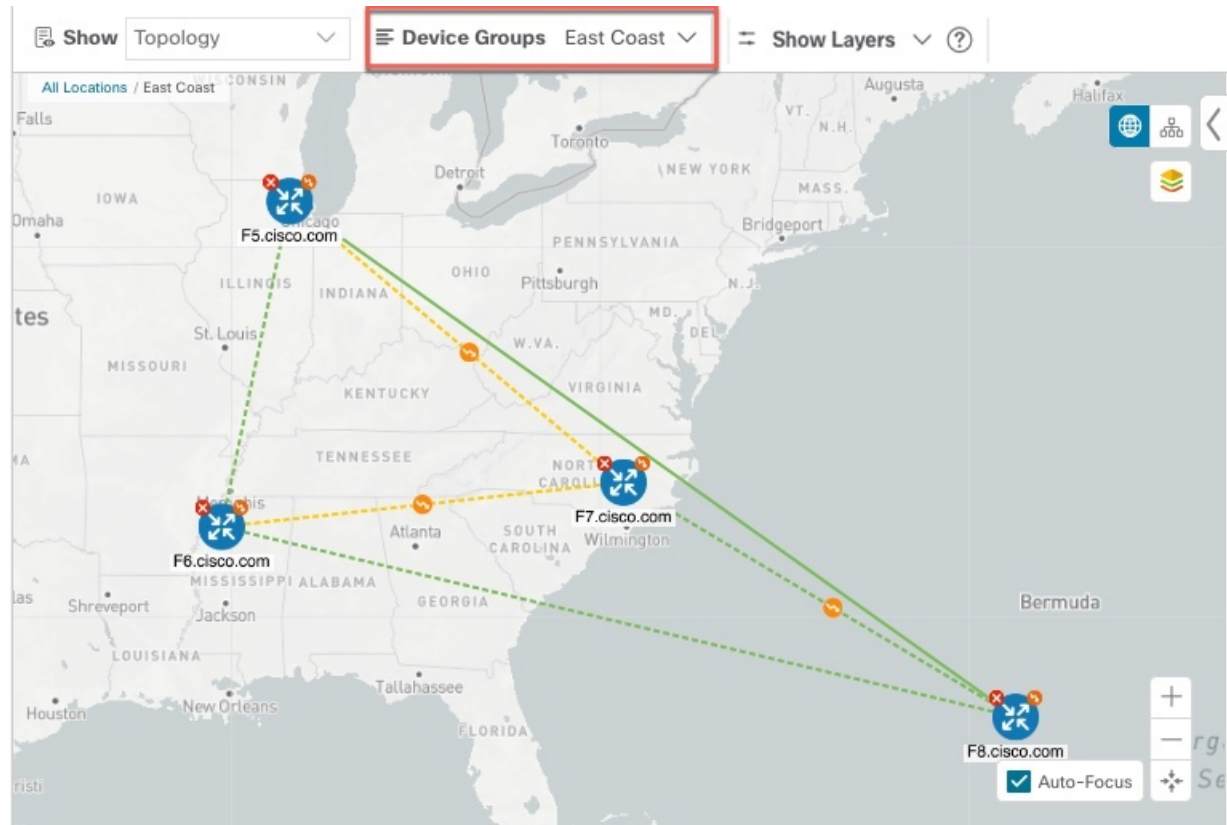
The **Device Groups** window (**Device Management** > **Groups**) allows you to create and manage device groups. By default, all devices initially appear in the **Unassigned Devices** group.

Figure 5: Device Groups
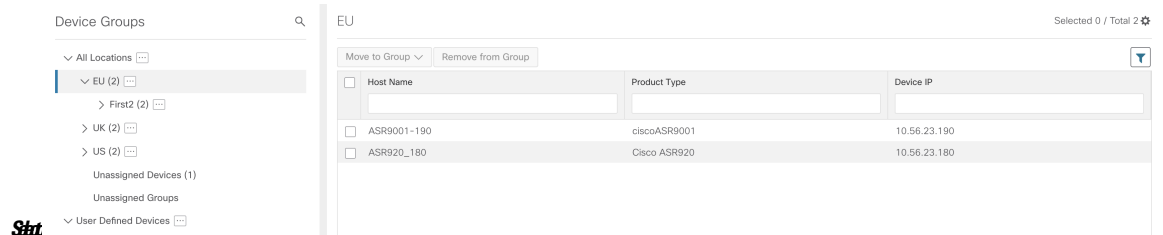

Create and Modify Device Groups

Device groups and assignment of devices to the groups can be done either manually (as described in this section) or automatically (as described in the next section).

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

Step 2   To add a new sub-group, click ⋯ next to **All Locations**.
A new sub-group gets added under **All Locations**.

Step 3   To add a device to a group, from the right-pane, under **Unassigned Devices**, select a device and then from the **Move to Group** drop-down, select the appropriate group.

Step 4   To edit, delete, or add a sub-group under an existing group, from the Device Groups tree, click [...] next to a group.
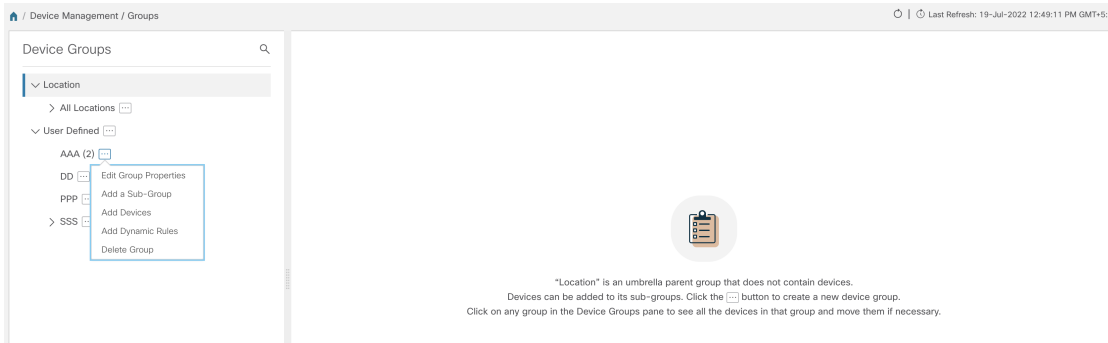
Step 5   Choose to add, delete, or edit (rename or move) a group. If you delete a group, all devices that belong to that group are moved to the Unassigned Devices group. Also, deleting a group deletes all the sub-groups under it.

> **Note**   Devices can belong to only one device group.

Step 6   Click **Save**.

Enable Dynamic Device Grouping

You can create a rule to dynamically create device groups and automatically add unassigned devices to these groups using a Regular Expression (regex) on the device hostname. Any newly added or discovered devices that match the rule will be placed in the appropriate group.

> **Note**   Dynamic rules do not apply to devices that already belong to groups. You must move them to Unassigned Devices if you want them to be considered by the rule.

Before you begin

While you can follow examples given in the Dynamic Groups dialog, it is helpful to be familiar with Regular Expressions.

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

Step 2   Click [...] next to **All Locations > Manage Dynamic Grouping Rule**.

Step 3   Click **Show more details and examples** to help you fill out the required Host Name and Group Name fields.

Step 4   If there are any existing devices in the Unassigned Devices group, click **Test Rule** to view a sampling of what type of group names will be created.

Step 5   Turn the **Enable Rule** toggle ON to enable the rule. After the rule is enabled, the system checks for unassigned devices every minute and will assign them to the appropriate group based on the rule.

Step 6   Click **Save**.

Step 7   Groups that are created this way initially appear under Unassigned Groups (created when a rule is enabled for the first time). Move newly created groups to the desired group hierarchy.

Step 8   To move newly created Unassigned groups to the correct group, do the following:

     a)   Click ⬚ next to All Locations and click **Add a Sub-Group**.
     b)   Enter the New Group details and click **Create**.
     c)   Click on the unassigned devices from the left pane.
     d)   From the right pane, select the devices you want to move and click **Move to Group** to move to an appropriate group.

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.

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

Step 2   (Optional) Filter the list of devices by filtering specific columns.

Step 3   Check the check box of the device you want to change, then click the ✎.

Step 4   Edit the values configured for the device, as needed.

     Note   In addition to the existing fields, you can also view the **Data Gateway** configured for the selected device. This field is read-only.

Step 5   Click **Save**. The Save button remains dimmed until all required fields are completed.

Step 6   Resolve any errors and confirm device reachability.

Delete Devices

Complete the following procedure to delete devices.

Before you begin

- If you set the autoonboard **managed** or **unmanaged** options for an SR-PCE provider, set autoonboard for one or more SR-PCEs to **off**.

- Confirm that the device is disconnected and powered off before deleting the device.

- If devices are mapped to Cisco NSO with MDT capability, and telemetry configuration is pushed, then those configurations will be removed from the device.

- If autoonboard isn't set to **off**, and it's still functional and connected to the network, the device will be rediscovered as unmanaged when it's deleted.

Step 1   Export a backup CSV file containing the devices that you plan to delete.

Step 2   From the main menu, choose **Device Management** > **Network 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 the ▥.

Step 6   In the confirmation dialog box, click **Delete**.