

# Get Started with Cisco Crosswork Network Controller 1.0 (Post-Installation)

---

This is a post-installation document intended to cover the steps required to get up and running with Cisco Crosswork Network Controller and start using the user interface (UI) to execute the supported use cases.

This document is intended for experienced network administrators and assumes familiarity with:

- Networking technologies and protocols (BGP-LS, IGP (OSPF and IS-IS), PCEP, model-driven telemetry, and so on)
- Segment Routing Path Computation Element (SR-PCE) functionality
- Cisco Network Services Orchestrator (Cisco NSO) functionality
- Segment routing (SR-TE) and SR policy provisioning
- Layer 2 and layer 3 VPN topology and provisioning concepts

For an overview of the steps that need to be taken to get started with Cisco Crosswork Network Controller and links to the relevant sections, see [Getting Started Overview, on page 4](#).

This document contains the following sections:

- [Introduction to the Cisco Crosswork Network Controller and its Components, on page 2](#)
- [Getting Started Overview, on page 4](#)
- [Log In and Log Out, on page 4](#)
- [Create Credential Profiles, on page 5](#)
- [Configure Providers, on page 9](#)
- [Manage Cisco Crosswork Data Gateway Servers, on page 13](#)
- [Manage Users, on page 21](#)
- [Create Tags, on page 23](#)
- [Add Devices to the Inventory, on page 24](#)
- [Set Up Your Maps, on page 34](#)
- [Set Up Bandwidth on Demand and Bandwidth Optimization, on page 36](#)
- [Additional Useful Information, on page 42](#)

# Introduction to the Cisco Crosswork Network Controller and its Components

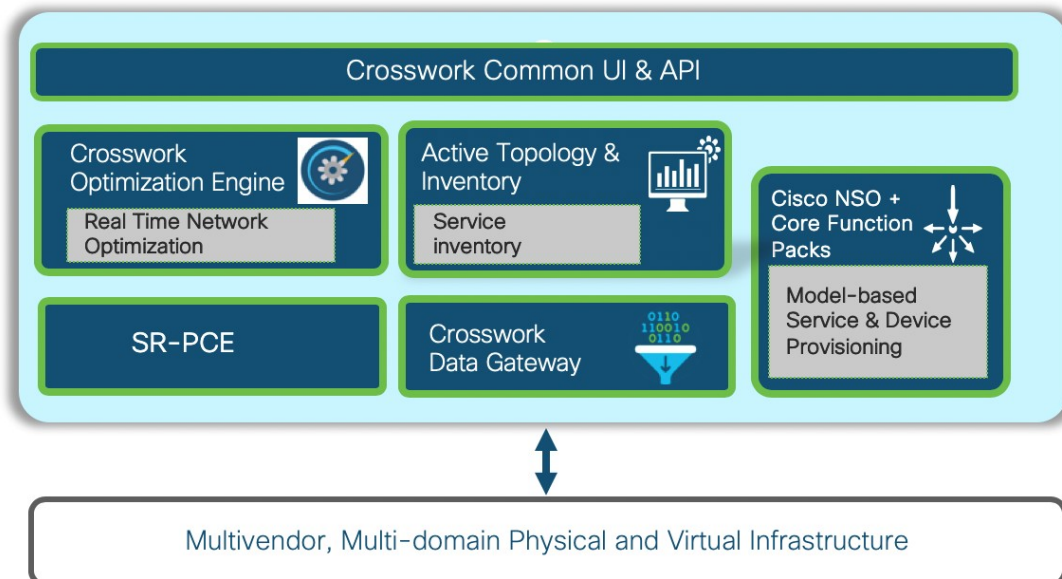
Cisco Crosswork Network Controller is an integrated solution combining Network Services Orchestrator (NSO), Segment Routing Path Computation Element (SR-PCE), and Crosswork applications with a common UI and API. The solution enables you to proactively manage your end-to-end networks and provides intent-based and closed-loop automation solutions to ensure faster innovation, good user experience, and operational excellence.

With this integrated solution, you can:

- Visualize network and service inventory.
- Provision segment routing (SR) traffic engineering policies for services with explicit SLAs by specifying optimization objectives (latency/IGP/TE metric minimization) and constraints (affinities, disjoint paths, bandwidth).
- Provision L2VPN and L3VPN services with associated SLAs.
- Collect realtime performance information and optimize the network to maintain the SLAs. Tactically optimize the network during times of congestion.
- Benefit from realtime bandwidth on demand and bandwidth optimization services.
- Use the APIs to extend the solution based on your specific needs.

The solution is made up of the following components:

**Figure 1: Solution Components**



## Cisco Network Services Orchestrator (NSO)

Cisco Network Services Orchestrator (NSO) is a proven multivendor, cross-domain automation platform that links business intent to an organization's underlying physical and virtual infrastructure. Cisco NSO has been shaped by nearly a decade of helping tier-1 service provider customers to automate everything from simple device turn-up, to cross-domain automation, to sophisticated full lifecycle service management on a multivendor network.

Cisco Crosswork Network Controller uses Cisco NSO as a provider for device management and configuration maintenance services. For provisioning segment routing policies and VPN services and for telemetry configuration, the following function packs must be installed on the Cisco NSO instance:

- Segment Routing Traffic Engineering (SR-TE) Core Function Pack enables provisioning of segment routing policies with SLA, for example, bandwidth and latency.
- Services Sample Function Pack enables Layer 2 and Layer 3 VPN service provisioning on routers, leveraging SR policies set up using the SR-TE Core Function Pack. The sample function pack can be extended and customized for customer-specific requirements.
- Telemetry Function Pack enables telemetry configuration on the routers.

## Segment Routing Path Computation Element (SR-PCE)

Cisco Crosswork Network Controller uses the combination of telemetry and Cisco Segment Routing Path Computation Element (SR-PCE) to analyze and compute optimal SR policy paths. Cisco SR-PCE runs on the Cisco IOS XR operating system. SR-PCE provides stateful PCE functionality that helps control and move SR policies to optimize the network. PCE describes a set of procedures by which a Path Computation Client (PCC) can report and delegate control of head-end tunnels sourced from the PCC to a PCE peer. The PCC and PCE establish a Path Computation Element Communication Protocol (PCEP) connection that SR-PCE uses to push updates to the network.

## Cisco Crosswork Data Gateway

Networks maintain a large amount of data that spans thousands of devices. Cisco Crosswork Network Controller uses a data collection service along with Cisco Crosswork Data Gateway (Crosswork CDG) to collect and manage this data. Crosswork Data Gateway collects physical (e.g., ENTITY-MIB, IF-MIB) and logical (e.g., LAG, VRF) objects from network devices and publishes collected data for the northbound analytics applications. Data from network devices is collected using multiple protocols including CLI, SNMP, and Model Driven Telemetry.

## Cisco Crosswork Optimization Engine

Cisco Crosswork Optimization Engine provides real-time network optimization allowing operators to effectively maximize network capacity utilization, as well as increase service velocity. Leveraging real-time protocols such as BGP-LS and Path Computation Element Communication Protocol (PCEP), SR-PCE and Crosswork Optimization Engine enable closed-loop tracking of the network state, reacting quickly to changes in network conditions to support a self-healing network.

## Cisco Crosswork Active Topology

Cisco Crosswork Active Topology enables visualization of topology and services on logical and geographical maps.

## Crosswork Common UI and API

Crosswork Common UI provides an integrated user interface for device onboarding/management, service provisioning using NSO, SR policy visualization using Cisco Crosswork Optimization Engine, and service inventory and topology visualization using Cisco Crosswork Active Topology. The Crosswork API provides a RESTCONF interface to facilitate integration with higher level controllers/orchestrators.

# Getting Started Overview

To get up and running with Cisco Crosswork Network Controller after you have installed the product, complete the tasks in the following table:

**Table 1: Tasks to Complete to Get Started with Cisco Crosswork Network Controller**

Task	Refer to...
Log into the GUI.	<a href="#">Log In and Log Out, on page 4</a>
Create credential profiles	<a href="#">Create Credential Profiles, on page 5</a>
Add Cisco SR-PCE and Cisco NSO providers.	<a href="#">Configure Providers, on page 9</a>
Manage Cisco Crosswork Data Gateway servers.	<a href="#">Manage Cisco Crosswork Data Gateway Servers, on page 13</a>
Add users and user roles.	<a href="#">Manage Users, on page 21</a>
Create device tags.	<a href="#">Create Tags, on page 23</a>
Add devices to the inventory so that they can be managed. Devices can be added in bulk by importing a CSV file or by auto-onboarding them. Devices can also be added individually through the UI.	<a href="#">Add Devices to the Inventory, on page 24</a>
Set display preferences for your maps.	<a href="#">Set Up Your Maps, on page 34</a>
Enable and configure bandwidth on demand and/or bandwidth optimization functionality.	<a href="#">Set Up Bandwidth on Demand and Bandwidth Optimization, on page 36</a>


## Log In and Log Out

To log into the web UI, enter the following in your web browser's address bar:

```
https://<hypervisor_server_IP_address>:30603/
```

In the displayed login window, enter the username and password configured during installation and click **Log In**.

Upon first-time access, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork Network Controller server. After you do this, the browser accepts the server as a trusted site in all future login attempts.

To log out, click  in the top right of the main window and choose **Log out**.

## Create Credential Profiles

Credential profiles are collections of credentials for SNMP, Telnet/SSH, HTTP, and other network protocols. Using credential profiles lets you automate device configuration changes and monitoring, and communicate with providers.



**Note** SSH and SNMP credentials are mandatory for onboarding devices and synchronizing with the NSO provider.

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.
- 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, you can edit the credential profile to replace the asterisks with actual passwords and community strings.

### Procedure

- 
- Step 1** From the main menu, choose **Device Management > Credential Profiles**.
- Step 2** Click .
- Step 3** In the **Profile Name** field, enter a descriptive profile name. The name can contain a maximum of 128 alphanumeric characters, plus 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 <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> . The <b>Enable Password</b> is optional.
SNMPv2	Enter the required SNMPv2 <b>Read Community</b> string. The <b>Write Community</b> string is optional.
NETCONF	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
TELNET	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> . The <b>Enable Password</b> is optional.
HTTP	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
HTTPS	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
GRPC	Enter the required <b>User Name</b> , <b>Password</b> , and <b>Confirm Password</b> .
SNMPv3	<p>Choose the required <b>Security Level</b> and enter the <b>User Name</b>.</p> <p>If you chose the NO_AUTH_NO_PRIV <b>Security Level</b> of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional.</p> <p>If you chose the AUTH_NO_PRIV <b>Security Level</b>, you must choose an <b>Auth Type</b> and enter an <b>Auth Password</b>.</p> <p>If you chose the AUTH_PRIV <b>Security Level</b>, you must choose an <b>Auth Type</b> and <b>Priv Type</b>, and enter an <b>Auth Password</b> and <b>Priv Password</b>.</p> <p>Only the following SNMPv3 Privacy Types are supported</p> <ul style="list-style-type: none"> <li>• CFB_AES_128</li> <li>• CBC_DES_56</li> </ul> <p>The following Privacy Types are not supported:</p> <ul style="list-style-type: none"> <li>• AES192</li> <li>• AES256</li> <li>• 3DES</li> </ul>

**Step 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 Network Controller.



**Note** SSH and SNMP credentials are mandatory for onboarding devices and synchronizing with the NSO provider.

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, you can edit the credential profile to replace the asterisks with actual passwords and community strings.

## Procedure

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

**Step 2** Click  to open the **Import Credentials** dialog box.

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

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

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

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

Also note:

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

Field	Entries	Required or Optional
<b>Credential Profile</b>	The name of the credential profile. For example: <b>srpce</b> .	Required

Field	Entries	Required or Optional
<b>Connectivity Type</b>	Valid values are: <b>SSH</b> , <b>SNMPv2</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , <b>HTTPS</b> , <b>GRPC</b> or <b>SNMPv3</b>	<ul style="list-style-type: none"> <li>• Devices—SNMP and SSH (to avoid operational errors due to clock synchronization checks) are required.</li> <li>• SR-PCE—Since SR-PCE is considered a provider and a device, SSH, and HTTP are required.</li> </ul>
<b>User Name</b>	For example: <b>SRPCEUser</b>	Required if <b>Connectivity Type</b> is <b>SSH</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , <b>HTTPS</b> , <b>SNMPv3</b> or <b>GRPC</b> .
<b>Password</b>	The password for the preceding <b>User Name</b> .	Required if <b>Connectivity Type</b> is <b>SSH</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , <b>HTTPS</b> or <b>GRPC</b>
<b>Enable Password</b>	Use an Enable password. Valid values are: <b>ENABLE</b> , <b>DISABLE</b> , or leave blank (unselected)	
<b>Enable Password Value</b>	Specify the Enable password to use.	Required only if <b>Enable Password</b> is set to <b>Enable</b> . Required if <b>Connectivity Type</b> is <b>SSH</b> or <b>TELNET</b> and <b>Enable Password</b> is set to <b>ENABLE</b> . Otherwise leave blank.
<b>SnmPV2 Read Community</b>	For example: <b>readprivate</b>	Required if <b>Connectivity Type</b> is <b>SNMPv2</b>
<b>SnmPV2 Write Community</b>	For example: <b>writeprivate</b>	Required if <b>Connectivity Type</b> is <b>SNMPv2</b>
<b>SnmPV3 User Name</b>	For example: <b>DemoUser</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b>
<b>SnmPV3 Security Level</b>	Valid values are <b>noAuthNoPriv</b> , <b>AuthNoPriv</b> or <b>AuthPriv</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b>
<b>SnmPV3 Auth Type</b>	Valid values are <b>HMAC_MD5</b> or <b>HMAC_SHA</b>	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmPV3 Security Level</b> is <b>AuthNoPriv</b> or <b>AuthPriv</b>
<b>SnmPV3 Auth Password</b>	The password for this authorization type.	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmPV3 Security Level</b> is <b>AuthNoPriv</b> or <b>AuthPriv</b>



Field	Entries	Required or Optional
<b>SnmpV3 Priv Type</b>	Valid values are <b>CFB_AES_128</b> or <b>CBC_DES_56</b>  The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmpV3 Security Level</b> is <b>AuthPriv</b>
<b>SnmpV3 Priv Password</b>	The password for this privilege type.	Required if <b>Connectivity Type</b> is <b>SNMPv3</b> and <b>SnmpV3 Security Level</b> is <b>AuthPriv</b>

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

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

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

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

## Configure Providers

Cisco Crosswork Network Controller uses Cisco SR-PCE and Cisco NSO providers for various functions, including inventory collection, route segmentation, configuration maintenance, route calculation, and service provisioning. Providers must be added to Cisco Crosswork Network Controller so that their connectivity details are saved and made available to the various components for interaction purposes.

Follow the instructions in these sections to add the required providers:

- [Add Cisco NSO Providers, on page 9](#)
- [Add Cisco SR-PCE Providers, on page 11](#)

## Add Cisco NSO Providers

The Cisco Network Services Orchestrator (Cisco NSO) provider supplies the following functionality within Cisco Crosswork Network Controller:

- Provisioning of segment routing (SR) policies. The Cisco NSO core function pack provides SR policy provisioning capability in Cisco Crosswork Network Controller.
- Provisioning of Layer 2 and Layer 3 services running over SR-TE (ODN or preferred path). Cisco NSO provides sample function packs for provisioning of these services, allowing the services to be instantiated "as-is" or extended to meet specific needs using the APIs.
- Device management and configuration maintenance services.



**Note** The NSO sample function packs provide example implementations as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. The intention is for customers to work with a Cisco Customer Experience representative to adapt these sample function packs to their specific networks and requirements. Although these implementations can be used "as is" to provision flat Layer 2 and Layer 3 VPN services using the GUI or API, they are not guaranteed to be complete and fully tested, and they are not products supported by Cisco.

This release of Cisco Crosswork Network Controller supports only one instance of Cisco NSO as a provider. Follow the steps below to add (through the UI) a Cisco NSO provider for Cisco Crosswork Network Controller. Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Cisco Crosswork Network Controller.

### 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.



**Note** You can find the Cisco NSO and NED versions using the `version` and `package-version` commands, as shown in the below examples:

```
nso@nso-virtual-machine:~$ ncs --version
5.2.03

admin@ncs> show packages package package-version
NAME                                PACKAGE VERSION
-----
cisco-iosxr-cli-7.13                7.13.9
```

- Know the Cisco NSO server IP address.

### Procedure

**Step 1** From the main menu, choose **Admin > 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 Network Controller.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO**.

- **Device Key:** The device key is generally used as the default method of identifying devices if no attribute is set on the device itself. Since it is mandatory to configure the Inventory ID for devices added to Cisco Crosswork Network Controller, Inventory ID will always be used to identify the devices and this default will not be required.
  - Under Connection Type(s), **Protocol:** Enable both **NETCONF** and **HTTPS** protocols.
    - Note** HTTPS should be configured with port 8888 to correspond with what is configured on the NSO VM in etc/ncs/ncs.conf.
  - **IP Address/Subnet Mask:** Enter the IPv4 IP address 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 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, click the **+Add Another** link to add another supported model.
  - **Version:** Enter the default software version of the device.
- 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** Under Provider Properties, enter a **Provider Key** of **forward** and a **Property Value** of **true**.

**Step 5** 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 Network Controller. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices.

Follow the steps below to add (through the UI) up to two instances of Cisco SR-PCE as providers for Cisco Crosswork Network Controller.

### 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 **unmanaged** when added. For more information, see [Auto-Onboard Devices, on page 30](#).

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

## Procedure

**Step 1** From the main menu, choose **Admin > 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 Network Controller.
- **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
<b>auto-onboard</b>	<b>off</b>
<b>auto-onboard</b>	<b>unmanaged</b>

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.



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

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

## Manage Cisco Crosswork Data Gateway Servers

Networks maintain a large amount of data that spans thousands of devices. Cisco Crosswork Network Controller uses a data collection service along with Cisco Crosswork Data Gateway to collect and manage this data. Cisco Crosswork Data Gateway collects physical (e.g., ENTITY-MIB, IF-MIB) and logical (e.g., LAG, VRF) objects from network devices and publishes collected data for the northbound analytics applications.

Cisco Crosswork Data Gateway is initially deployed with just a basic virtual machine (VM) called the Base VM (containing only enough software to register itself with its controller, which in this case is Cisco Crosswork Network Controller). Depending on your network's size and configuration, it may be necessary to deploy multiple Cisco Crosswork Data Gateway instances to address the requirements for geo-separated regions and/or massive scale. Cisco recommends the simplest approach of a fixed configuration of devices to a particular instance (such as x to y for CDG1 and (y+1) to z for CDG2).




---

**Note** More complicated approaches for resource optimization and dynamic assignment of tasks are possible and if desired, we recommend working with the Cisco Customer Experience team to design the behavior.

---

After installing the instances of Cisco Crosswork Data Gateway, you must generate an enrollment package and then enroll each instance with Cisco Crosswork Network Controller. See the following sections:

- [Access Cisco Crosswork Data Gateway Through vCenter, on page 13](#)
- [Generate An Enrollment Package, on page 14](#)
- [Export Enrollment Package, on page 15](#)
- [Enroll Cisco Crosswork Data Gateway, on page 16](#)
- [Cisco Crosswork Data Gateway Authentication and Bootstrap, on page 18](#)
- [Troubleshoot the Cisco Crosswork Data Gateway Installation and Enrollment, on page 19](#)

## Access Cisco Crosswork Data Gateway Through vCenter

Follow these steps to log in via vCenter:

### Procedure

---

- Step 1** Locate the VM in vCenter and then right click and select **Open Console**.  
The Cisco Crosswork Data Gateway flash screen comes up.
- Step 2** Enter username (`dg-admin` or `dg-oper` as per the role assigned to you) and the corresponding password (the one that you created during installation process) and press **Enter**.
-

## Generate An Enrollment Package

Every Cisco Crosswork Data Gateway instance must be identified by means of an immutable identifier. This requires generation of a Cisco Crosswork Data Gateway enrollment package. The enrollment package can be generated during installation by supplying OVF parameters or by using the **Export Enrollment Package** option from the interactive menu in the console.

The enrollment package is a JSON document created from the information obtained through the OVF template populated by the user during installation. It includes the all necessary information about Cisco Crosswork Data Gateway required for registering, such as Certificate, UUID of the Cisco Crosswork Data Gateway instance, and metadata like Cisco Crosswork Data Gateway instance name, creation time, version info, and so on.

If you opted not to export the enrollment package during install, then you must export it before you can enroll the Cisco Crosswork Data Gateway instance with Cisco Crosswork Network Controller. The steps to do so are described in [Export Enrollment Package, on page 15](#).




---

**Note** The enrollment package is unique to each Cisco Crosswork Data Gateway instance.

---

A sample enrollment package JSON file is shown below:

```
{
  "name": "dg116.cisco.com",
  "description": "CDG Base VM for Automation",
  "profile": {
    "cpu": 8,
    "memory": 31,
    "nics": 3
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "00:50:56:9e:09:7a",
      "ipv4Address": "<ip_address>/24"
    },
    {
      "name": "eth1",
      "mac": "00:50:56:9e:67:c3",
      "ipv4Address": "<ip_address>/16"
    },
    {
      "name": "eth2",
      "mac": "00:50:56:9e:83:83",
      "ipv4Address": "<ip_address>/16"
    }
  ],
  "certChain": [
    ],
  "version": "1.1.0 (branch dg110dev - build number 152)",
  "duuid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}
```

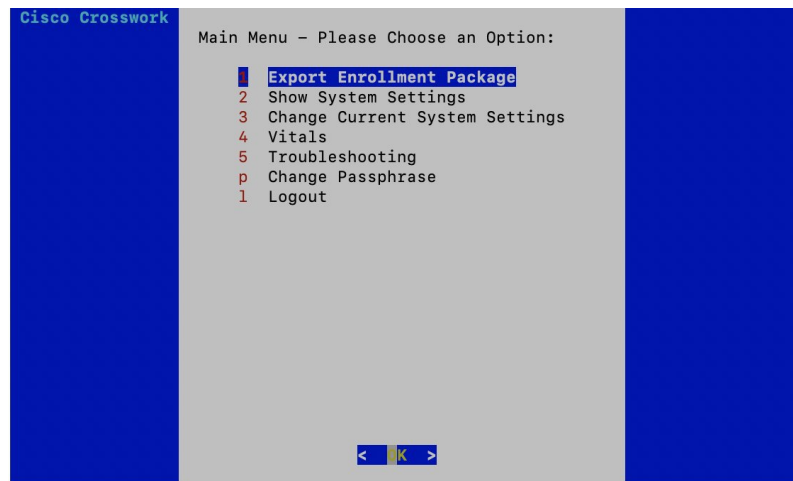
## Export Enrollment Package

To enroll the Cisco Crosswork Data Gateway with Cisco Crosswork Network Controller, you must have a copy of the enrollment package on your local computer.

Follow these steps:

### Procedure

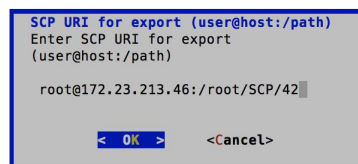
- Step 1** Log into the Cisco Crosswork Data Gateway Base VM.
- Step 2** From the Main Menu, select **1 Export Enrollment Package** and click **OK**.



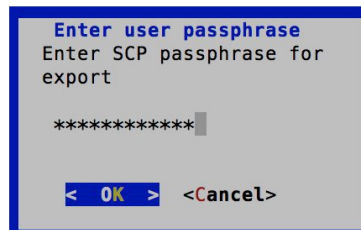
- Step 3** Enter the SCP URI for exporting the enrollment package and click **OK**.

**Note** The host must run an SCP server. Ideally, you should export the enrollment package to the local computer you will use to access the Crosswork server. If no alternative SCP server is available, then Crosswork server can be used. An example URI is given below:

```
cw-admin@<Crosswork_VM_Management_IP_Address>:/home/cw-admin
```



- Step 4** Enter the SCP passphrase (the SCP user password) and click **OK**.



The enrollment package is exported.

- Step 5** If you could not copy the enrollment package directly to your local computer, manually copy the enrollment package from the SCP server to your local computer.
- Step 6** Proceed with importing the Controller Signing Certificate file.

## Enroll Cisco Crosswork Data Gateway

### Procedure

- Step 1** Log into Cisco Crosswork Network Controller.
- Step 2** From the Main Menu, select **Admin > Data Gateway Management**.  
The **Data Gateway Management** page opens.
- Step 3** Click the **Add** button.  
The **Enroll New Data Gateway** dialog opens.
- Step 4** Click **Browse** and navigate to the folder to which you copied the enrollment package and select it.
- Step 5** Select the **Data gateway admin state** in which you want to bring up the Cisco Crosswork Data Gateway:
- **Up** (recommended): Select this state if you want to bring up the Cisco Crosswork Data Gateway in active mode. Up state moves the operational state of the Cisco Crosswork Data Gateway to Up with no intermediate step.



- **Maintenance:** Select this state if you want to bring up the Cisco Crosswork Data Gateway in maintenance state. Maintenance state moves the operational state of the Cisco Crosswork Data Gateway to Up but it is flagged as being in Maintenance mode while you perform any additional testing and setup.

The **Enroll New Data Gateway** dialog displays a summary of the selected enrollment package:

- Name of the Cisco Crosswork Data Gateway instance
- Description of the Cisco Crosswork Data Gateway instance
- Labels associated with the Cisco Crosswork Data Gateway instance

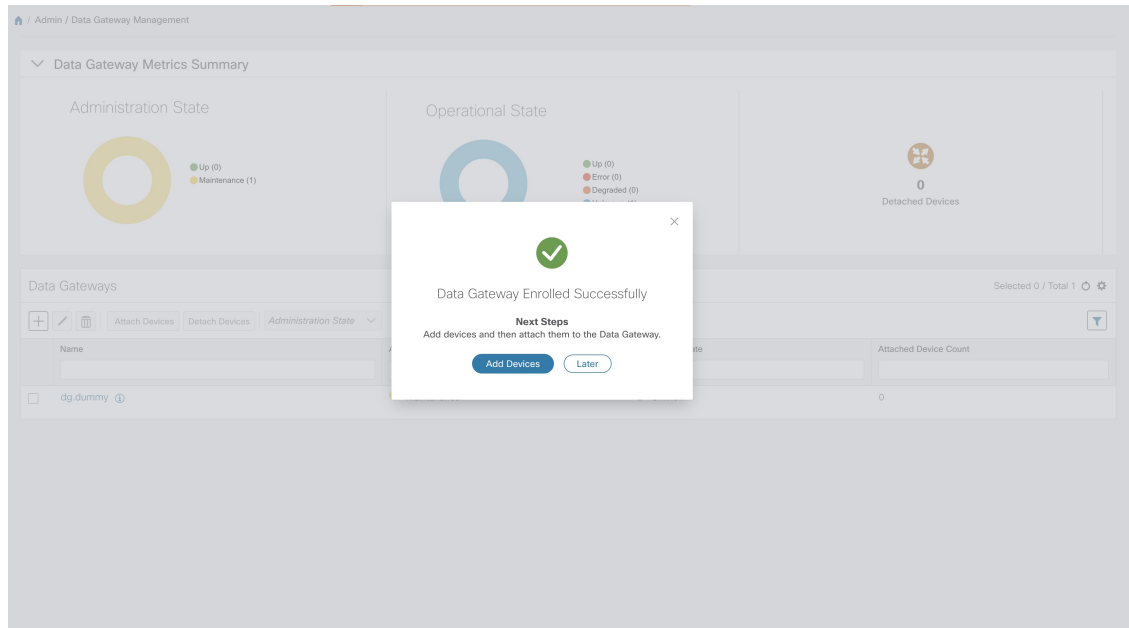
It also displays additional details:

- Number of CPUs
- Memory
- Number of NICs
- Interface name
- Interface MAC address
- Interface IPv4Address
- certChain
- Version
- DUUID

**Step 6** Click **Enroll**.


Once you click **Enroll**, a dialog pops up asking if you want to attach devices now or later. It is recommended to choose **Later** as devices must only be attached once the operational state of the Cisco Crosswork Data Gateway instance is **Up**.

See [Attach a Device to a Cisco Crosswork Data Gateway Instance, on page 30](#).



### What to do next

The Operational Status of a Cisco Crosswork Data Gateway instance is shown as "**Degraded**" until it establishes a connection with Cisco Crosswork Network Controller and downloads collector binary files. While it depends on the bandwidth between the Cisco Crosswork Data Gateway instance and Cisco Crosswork Network

Controller, this operation typically takes less than 5 minutes. Click the  icon in the **Data Gateways** pane to refresh the pane to reflect the latest operational status of the Cisco Crosswork Data Gateway instance and wait for it to become **Up**. If the Cisco Crosswork Data Gateway instance fails to enroll, contact Cisco CX for assistance.

## Cisco Crosswork Data Gateway Authentication and Bootstrap

During the enrollment process, the enrollment package is uploaded to the controller application, i.e., Cisco Crosswork Network Controller, which then instantiates a new Cisco Crosswork Data Gateway instance in its database and waits for a "first-sign-of-life" from the Cisco Crosswork Data Gateway.

### Session Establishment

Once the connectivity is established, the Cisco Crosswork Data Gateway instance confirms the identity of the controller and offers its own proof of identity via signed certificates during this initial connection.

### Download of Configuration Files

Once the session is established, Cisco Crosswork Data Gateway downloads the following configuration files:

**Table 2: Configuration Files**

<b>boot-config</b>	A json response created by Crosswork that contains a list of services (docker containers) and functional images should be downloaded on that particular Cisco Crosswork Data Gateway instance.
<b>docker-compose</b>	A YAML file that contains instructions and order to start up the right set of services and functional images.

**Download of Functional Images**

A functional image represents a collection profile for a protocol, i.e., CLI, SNMP, or MDT. Cisco Crosswork Data Gateway downloads the following functional images:

**Table 3: Functional Images**

<b>CLI Collection</b>	To connect to a device using SSH/Telnet, collect <b>show</b> commands output, and send it to the designated output destination.
<b>SNMP Collection</b>	To connect to a device using SNMP protocol, collect SNMP responses, receive SNMP traps, and send them to a designated output destination.
<b>MDT Collection</b>	To connect to a device and collect model-driven telemetry or event-driven telemetry events, and send them to a designated output destination.

After the downloads, Cisco Crosswork Data Gateway boots the containers.

Cisco Crosswork Data Gateway is now ready to collect data.

## Troubleshoot the Cisco Crosswork Data Gateway Installation and Enrollment

The following table lists common problems that might be experienced while installing or enrolling Cisco Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

**Table 4: Troubleshooting the Installation/Enrollment**

<b>Issue</b>	<b>Action</b>
<b>1. Cannot enroll Cisco Crosswork Data Gateway with Crosswork</b>	

Issue	Action
<p>Cisco Crosswork Data Gateway cannot be enrolled with Cisco Crosswork Network Controller due to an NTP issue, i.e., there is a clock-drift between the two.</p> <p>The clock-drift might be with either Cisco Crosswork Data Gateway or Cisco Crosswork Network Controller.</p> <p>Also, on the NTP servers for Cisco Crosswork Network Controller and Cisco Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured.</p> <p>Sync the clock time on the host and retry.</p>	<ol style="list-style-type: none"> <li>Log into the Cisco Crosswork Data Gateway VM.</li> <li>From the main menu, go to <b>5 Troubleshooting &gt; Run show-tech</b>. Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>. In the show-tech logs (in file <code>session.log</code> at location <code>/opt/dg/data/controller-gateway</code>), if you see the error <code>UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid</code>, then there is a clock-drift between Cisco Crosswork Data Gateway and Cisco Crosswork Network Controller.</li> <li>From the main menu, go to <b>3 Change Current System Settings &gt; 1 Configure NTP</b>. Configure NTP to sync with the clock time on the Cisco Crosswork Network Controller server and try re-enrolling Cisco Crosswork Data Gateway. It is also possible that the Cisco Crosswork Network Controller's NTP server might be down or its address might be incorrect.</li> </ol>
<p><b>2. Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals"</b></p>	
<p>Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.</p>	<ol style="list-style-type: none"> <li>Log into the Cisco Crosswork Data Gateway VM.</li> <li>From the main menu, select <b>5 Troubleshooting &gt; Run show-tech</b>. Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>. In the show-tech logs (in file <code>gateway.log</code> at location <code>/opt/dg/log/controller-gateway/gateway.log</code>), if you see certificate errors, then re-upload the Controller Signing Certificate, as explained in the steps below: <ol style="list-style-type: none"> <li>From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certification</b>.</li> <li>From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> </li> </ol>
<p><b>3. Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established"</b></p>	

Issue	Action
Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established" due to certificate errors.	<ol style="list-style-type: none"> <li>1. Re-upload the certificate file as explained in the troubleshooting scenario <b>2.</b> above.</li> <li>2. Reboot the Cisco Crosswork Data Gateway VM following the steps below:               <ol style="list-style-type: none"> <li>a. From the main menu, select <b>5 Troubleshooting</b> and click <b>OK</b>.</li> <li>b. From the Troubleshooting menu, select <b>7 Reboot VM</b> and click <b>OK</b>.</li> <li>c. Once the reboot is complete, check if the Cisco Crosswork Data Gateway's operational status is <b>Up</b>.</li> </ol> </li> </ol>

## Manage Users

During installation, an administrator user is created. This user has access privileges for all Cisco Crosswork Network Controller functionality.

As a best practice, administrators should create separate accounts for all users. Prepare a list of the people who will use Cisco Crosswork Network Controller. Decide on their user names and preliminary passwords, and create user profiles for them. See [Add Users, on page 21](#). During the creation of a user account, you assign a user role to determine the functionality to which the user will have access. If you will be using user roles other than "admin", create the user roles before you add your users. See [Create User Roles, on page 22](#).

From the main menu, select **Admin > Users** to display the **Users** window. Using this window, you can add a new user, edit the settings for an existing user, delete a user from the network, and create user roles.



**Note** Only a local admin user can add, update, and delete other local user accounts. A TACACS+ user, regardless of role assigned, will not be able to manage local users.

## Add Users

Follow the steps below to create a new user ID.

The user ID's user name must be unique. You cannot create a new user ID with the same user name as an existing user ID.

The special administrative user names **admin** (for administering Cisco Crosswork Network Controller) and **cw-admin** (for administering the virtual machine hosting the product) are created during installation and are reserved for those purposes.

### Procedure

**Step 1** From the main menu, choose **Admin > Users**.  
The **Users** window opens.

If it is not already displayed, click the **Users** tab.

**Step 2** Click  to open the **Add New User** dialog box.

**Step 3** Enter the following information for the user you are adding:

- **User Name:** Enter a unique name for the user ID. User names cannot contain spaces or special characters.
- **First Name** and **Last Name:** Enter the first and last name of the person assigned to this user ID.
- From the **Role** drop-down at the bottom of the dialog box, choose the role that you want to assign to the user. See [Create User Roles](#) for more information.
- **Password** and **Confirm Password:** Enter the default password for this user ID. The user will be required to change the default password the first time they attempt to log on using it.

**Note** The user password must be string of minimum 8 characters without spaces and should include letters, numbers, upper-case and lower-case characters, and one of the allowed special characters ("@!\$%\*?&").

**Step 4** Click **Save**.

---

## Create User Roles

Local users with administrator privileges can create new users as needed (see [Add Users, on page 21](#)).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

The local **admin** role enables access to all functionality. It is created during installation and cannot be changed or deleted. However, its privileges can be assigned to new local users. Only local users can create or update user roles; TACACS users cannot.

Follow the steps below to create a new user role.

### Procedure

---

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

The **Users** window opens.

If it is not already displayed, click the **Roles** tab. The **Roles** window has a **Roles** table on the left side and a corresponding **admin** table on the right side which shows the grouping of user permissions for the selected role.

**Step 2** On the **Roles** table, click  to display a new role entry in the table.

**Step 3** Enter a unique name for the new role.

**Step 4** Define the user role's privilege settings:

- a) Check the check box for every API that users with this role can access. The APIs are grouped logically based their corresponding application.

- b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.

**Step 5** Click **Save** to create the new role.

---

## Create Tags

Tags are simple text strings that you can attach to objects to help group them. Cisco Crosswork Network Controller comes with a short list of ready-made tags used to group network devices. You can create your own tags and use them to identify, find, and group devices for a variety of purposes. For example, in addition to type and geo-location, you may want to identify and group devices by their location in your network topology (spine vs. leaf), or the function they serve in your network (Provider vs. Provider Edge).

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 24.



**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.

---

### Procedure

---

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

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

**Step 3** In the **Category** area:

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

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

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

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

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

---


## 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 Network Controller. 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.

### Procedure

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

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

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

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

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

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

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

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

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

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

## Add Devices to the Inventory

In order for your network devices to be managed, monitored and visualized, they must be added to the Cisco Crosswork Network Controller inventory. Methods for adding devices to the inventory include:

- Importing a CSV file that is populated with information for multiple devices. See [Import Devices, on page 26](#).
- Adding devices manually via the UI. See [Add Devices Through the UI, on page 27](#).



- Auto-onboarding devices. See [Auto-Onboard Devices, on page 30](#).

Before adding devices to the inventory, you need to do the following:

1. Ensure that your devices are configured properly for communication and telemetry. See guidelines and example configurations in [Prerequisites for Onboarding Devices, on page 25](#).
2. Create a device credential profile. See [Create Credential Profiles, on page 5](#).
3. Add NSO and SR-PCE providers. See [Configure Providers, on page 9](#).
4. (Optional) Create tags for device identification and grouping. See [Create Tags, on page 23](#).

After you have added your devices to the inventory, you must register them with a Cisco Data Gateway instance for management. See [Attach a Device to a Cisco Crosswork Data Gateway Instance, on page 30](#).

After they have been registered with Cisco Data Gateway, the devices are automatically pushed to Cisco NSO. See [Auto-Sync of Managed Devices With Cisco NSO, on page 32](#).

If you want to enable MDT functionality on devices, you can do so after they have been added to the inventory. See [Enable MDT Functionality on Devices, on page 33](#).

## 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 Network Controller. 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 Network Controller.




---

**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 6.5.3/6.6.3 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>
```

## Import Devices

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

### Procedure

**Step 1** From the main menu, choose **Device 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.

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

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter **SSH ; SNMP ; NETCONF ; 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 27](#).

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.

It is normal for devices to show as unreachable or not operational when they are first imported. However, if after 30 minutes they are still displayed as unreachable or not operational, there is an issue that needs to be investigated. To investigate, select **Device Management > Job History** and click on any  you see in the **Status** column. Common issues include failure to ensure the associated credential profile contains the correct credentials. You can test this by opening a terminal window on the Cisco Crosswork Network Controller 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.

### Procedure


- Step 1** From the main menu, choose **Devices Management > 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 complete.)
- Step 5** (Optional) Repeat to add more devices.

Table 5: Add New Device Window (\*=Required)

Field	Description
* <b>Configured State</b>	<p>The management state of the device. Options are</p> <ul style="list-style-type: none"> <li>• <b>UNMANAGED</b>—Cisco Crosswork Network Controller is not monitoring the device.</li> <li>• <b>DOWN</b>—The device is being managed and is down.</li> <li>• <b>UP</b>—The device is being managed and is up.</li> </ul>
* <b>Reachability Check</b>	<p>Determines whether Cisco Crosswork Network Controller performs reachability checks on the device. Options are:</p> <ul style="list-style-type: none"> <li>• <b>ENABLE</b> (In CSV: <b>REACH_CHECK_ENABLE</b>)—Checks for reachability and then updates the Reachability State in the UI automatically.</li> <li>• <b>DISABLE</b> (In CSV: <b>REACH_CHECK_DISABLE</b>)—The device reachability check is disabled.</li> </ul> <p>Cisco recommends that you always set this to <b>ENABLE</b>. This field is optional if <b>Configured State</b> is marked as <b>UNMANAGED</b>.</p>
* <b>Credential Profile</b>	<p>The name of the credential profile to be used to access the device for data collection and configuration changes. For example: <b>nso23</b> or <b>srpce123</b>.</p> <p>This field is optional if <b>Configured State</b> is marked as <b>UNMANAGED</b>.</p>
<b>Host Name</b>	The host name of the device.
<b>Inventory ID</b>	Inventory ID value for the device. Inventory ID is mandatory. Choose the device Host Name or an easily identifiable name for Inventory ID as this will be used to sync the device to Cisco NSO with the Inventory ID used as the device name in Cisco NSO.
<b>Software Type</b>	Software type of the device.
<b>Software Version</b>	Software version of the device.
<b>UUID</b>	Universally unique identifier (UUID) for the device.
<b>Serial Number</b>	Serial number for the device.
<b>MAC Address</b>	MAC address of the device.
* <b>Capability</b>	<p>The capabilities that allow collection of device data and that are configured on the device. You must select at least <b>SNMP</b> as this is a required capability. The device will not be onboarded if <b>SNMP</b> is not configured. Other options are <b>TL1</b>, <b>YANG_CLI</b>, and <b>YANG-EPNM</b>. The capabilities you select will depend on the device software type and version.</p> <p><b>Note</b> For devices with MDT capability, do not select <b>YANG_MDT</b> at this stage. Follow the procedure in <a href="#">Enable MDT Functionality on Devices, on page 33</a>.</p>
<b>Tags</b>	<p>The available tags to assign to the device for identification and grouping purposes.</p> <p>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.</p>

Field	Description
<b>Connectivity Details</b>	
<b>Protocol</b>	<p>The connectivity protocols used by the device. Choices are: <b>SSH</b>, <b>SNMP</b>, <b>NETCONF</b>, <b>TELNET</b>, <b>HTTP</b>, and <b>HTTPS</b>.</p> <p>You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol. You must enter details for at least <b>SSH</b> and <b>SNMP</b>. If you do not configure <b>SNMP</b>, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for <b>NETCONF</b>. <b>TELNET</b> connectivity is optional.</p>
<b>* IP Address / Subnet Mask</b>	Enter the device's IP address (IPv4 or IPv6) and subnet mask.
<b>* Port</b>	<p>The port used for this connectivity protocol. Each protocol is mapped to a port, so be sure to enter the port number that corresponds to the <b>Protocol</b> you chose. The standard port assignments for each protocol are:</p> <ul style="list-style-type: none"> <li>• SSH: 22</li> <li>• SNMP: 161</li> <li>• NETCONF: 830</li> <li>• TELNET: 23</li> <li>• HTTP: 80</li> <li>• HTTPS: 443</li> </ul>
<b>Timeout</b>	The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.
<b>Routing Info</b>	
<b>ISIS System ID</b>	The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.
<b>OSPF Router ID</b>	The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.
<b>*TE Router ID</b>	The MPLS traffic engineering router ID for the respective IGP.
<b>Streaming Telemetry Config</b>	
<b>Telemetry Interface Source VRF</b>	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
<b>Location</b>	
All location fields are optional, with the exception of <b>Longitude</b> and <b>Latitude</b> , which are required for the geographical view of your network topology.	

Field	Description
<b>Longitude, Latitude</b>	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.
<b>Altitude</b>	The altitude, in feet or meters, at which the device is located. For example, <b>123</b> .
<b>Providers and Access</b>	
<b>Local Config: Device Key and Provider</b>	The Device Key will automatically populate and the Credential Profile appears.
<b>Compute Config: Provider</b>	(Optional) Provider name used for topology computation. Choose a provider from the list. For CSV entry, use <code>ROBOT_PROVIDER_COMPUTE</code> and enter the Provider name.

## Auto-Onboard Devices

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

To configure auto-onboarding, you must add an SR-PCE provider with the following auto-onboard option:

- **Unmanaged:** All discovered devices will be registered in the inventory database, with their configured state set to **unmanaged**. SNMP polling will be disabled for these devices, and no management IP information will be included. IGP topology will be shown on the topology map (logical view), but the information available is restricted to the information SR-PCE provides. Therefore, interface names are not shown, and in the case of OSPF, device Hostnames are also not shown. IP addresses are shown and can be used to identify devices and interfaces.




---

**Note** To get these devices into the **managed** state later, you will need to download them as a CSV file, 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. You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).

---

## Attach a Device to a Cisco Crosswork Data Gateway Instance




---

**Note** A device can only be attached to one Cisco Crosswork Data Gateway instance.

---

Follow the steps below to attach a device to a Cisco Crosswork Data Gateway instance.

### Before you begin

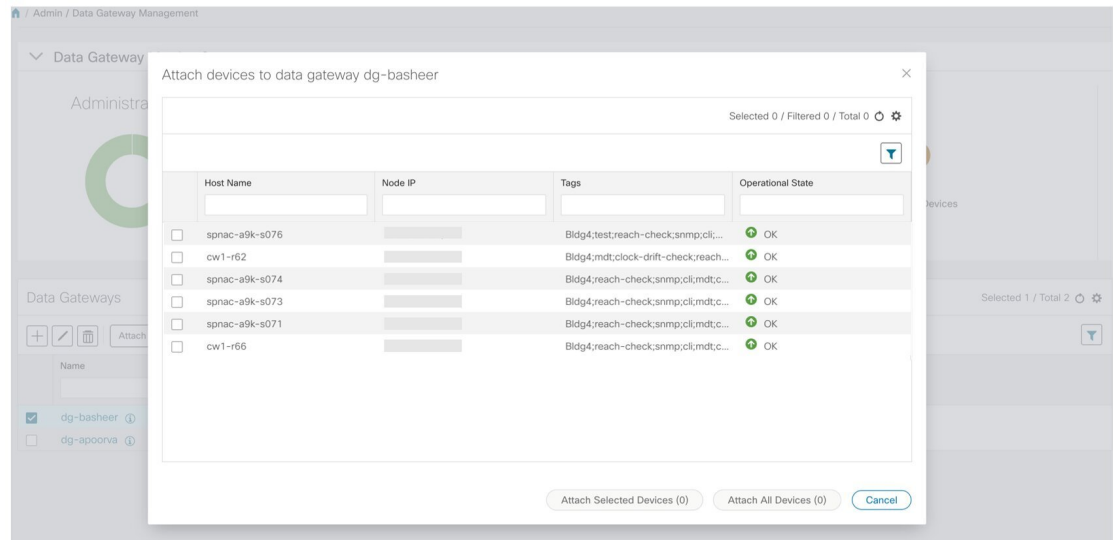
1. For optimal performance, it is recommended that device attaching to Cisco Crosswork Data Gateway instance should be done in batches of no more than 300 devices.

You can add more than 300 devices. However, doing so may cause a performance impact.

2. Ensure that both the administration state and operational state of the Cisco Crosswork Data Gateway instance to which you want to attach devices is "Up". Only then proceed with attaching devices.

### Procedure


- Step 1** From the main menu, choose **Admin > Data Gateway Management**. The **Data Gateway Management** view opens.
- Step 2** From the **Data Gateways** window, select the Cisco Crosswork Data Gateway instance to which you want to attach devices.
- Step 3** Click **Attach Devices**. The **Attach Devices** window opens. It lists all the devices available for attaching.



- Step 4** To attach all the devices, click **Attach All Devices**. Otherwise, select the devices you want to attach and click **Attach Selected Devices**.

### What to do next

To verify if the devices were attached to the VM, check the **Attached Device Count** under the **Data Gateways** pane. The count would have increased.

Click on the  icon next to the attached device count to see the list of all devices attached to the selected instance, as shown in the following figure.

Host Name	Node IP	Tags	Operational State
cw1-r68		Bldg4;reach-check;snmp;cli;mdt;c...	OK
cw1-r61		Bldg4;reach-check;snmp;cli	CHECKING
spnac-a9k-s072		Bldg4;reach-check;snmp;cli;mdt;c...	OK
cw1-r65		Bldg4;test;Denver;reach-check;sn...	OK
cw1-r64		Bldg4;reach-check;snmp;cli;mdt;c...	OK
cw1-r67		Bldg4;reach-check;snmp;cli;mdt;c...	OK
cw1-r69		Bldg4;reach-check;snmp;cli;mdt;c...	OK
spnac-a9k-s076		Bldg4;test;reach-check;snmp;cli;...	OK
cw1-r62		Bldg4;mdt;clock-drift-check;reach...	OK
spnac-a9k-s074		Bldg4;reach-check;snmp;cli;mdt;c...	OK
spnac-a9k-s073		Bldg4;reach-check;snmp;cli;mdt;c...	OK
spnac-a9k-s071		Bldg4;reach-check;snmp;cli;mdt;c...	OK
cw1-r66		Bldg4;reach-check;snmp;cli;mdt;c...	OK
spnac-a9k-s075		Bldg4;reach-check;snmp;cli;mdt;c...	OK
cw1-r63		Bldg4;reach-check;snmp;cli;mdt;c...	OK



**Note** After attaching the devices to a Cisco Crosswork Data Gateway instance, the devices will be automatically synced with Cisco NSO. After you verify that the devices are in Cisco NSO, you must run the following commands from Cisco NSO:

- **fetch-ssh-keys**
- **sync-from**

## Auto-Sync of Managed Devices With Cisco NSO

New devices that are added to Cisco Crosswork Network Controller are reflected automatically in Cisco NSO. Additionally, whenever device, credential, or provider data is changed, a sync operation will take place and the changes will reflect in Cisco NSO.



**Note** The device sync is one-directional - from Cisco Crosswork Network Controller to Cisco NSO. Devices cannot be imported or synced from Cisco NSO to Cisco Crosswork Network Controller.

For auto-sync to work, you need to do the following in NSO (ncs.conf file):

- • In the SSL section, enable HTTPS and specify port 8888.
- • For an IPv6 NSO deployment, include the following in the SSL section:

```
<extra-listen>
  <ip>:::/ip>
  <port>8888</port>
</extra-listen>
```

In Cisco Crosswork Network Controller, ensure that:



- Netconf connectivity is configured for NSO as a provider and that the NSO provider is "Reachable". Go to **Admin > Providers**.
- Devices have a specified Software Type. Go to **Device Management > Devices**.
- Devices are associated with credential profiles that contain an SSH entry. Go to **Device Management > Credential Profiles**.



**Note** After the devices have been synced with Cisco NSO, you must run the following commands from Cisco NSO:

- `fetch-ssh-keys`
- `sync-from`

## Enable MDT Functionality on Devices


Cisco Crosswork Network Controller supports data collection from network devices using Model-driven Telemetry (MDT) to consume telemetry streams directly from devices.

MDT must be enabled after the devices have been onboarded and attached to a Cisco Crosswork Data Gateway instance. Follow these steps to enable MDT on managed devices:

### Before you begin

- Make sure that a Cisco NSO provider has been configured and is reachable. See [Add Cisco NSO Providers, on page 9](#).

### Procedure

- 
- Step 1** Add devices to the inventory:
- If devices are being discovered from SR-PCE, make sure the auto-onboard property for the SR-PCE provider is set to **unmanaged**. See [Add Cisco SR-PCE Providers, on page 11](#)
  - If you are adding devices using the UI or by importing a CSV file, make sure that the management state of the device is up (ADMIN\_UP) and that YANG\_MDT capability is *not* selected. Also make sure that SSH connectivity information is configured and that the device software version is specified. See [Add Devices Through the UI, on page 27](#) and [Import Devices, on page 26](#).
- Step 2** When the devices have been added to the inventory, attach them to a Cisco Crosswork Data Gateway instance. See [Attach a Device to a Cisco Crosswork Data Gateway Instance, on page 30](#).
- At this stage, the devices will be automatically synced with Cisco NSO. See [Auto-Sync of Managed Devices With Cisco NSO, on page 32](#).
- Step 3** Check that the devices have been pushed to Cisco NSO.
- Step 4** In Cisco NSO, run the `sync-from` and `fetch-host-keys` commands for all the devices.
- Step 5** Export all the devices that will have MDT capability to a .csv file:
- In the Cisco Crosswork Network Controller UI, go to **Device Management > Devices**.
  - Select the devices you want to export and click .

c) Save the .csv file.

**Step 6** In the .csv file, update the capabilities to include YANG\_MDT and save the file.

**Step 7** Import the updated .csv file into Cisco Crosswork Network Controller. See [Import Devices, on page 26](#).

On successful import of the .csv file, the MDT configuration will be pushed to all the devices.

## Set Up Your Maps

The network topology can be displayed on a logical map or a geographical map, where the devices and links are shown in their geographic context. The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. The geographical map shows single devices, device clusters, links, and tunnels, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude).

To set up your maps and adjust them for your needs, see the following sections:

- [Choose a Provider for the Geographical Map Display, on page 34](#)
- [Use Internal Maps for Geo Map Display, on page 35](#)
- [Set Display Preferences for Devices and Links, on page 35](#)
- [Define Color Thresholds for Link Bandwidth Utilization, on page 36](#)

### Choose a Provider for the Geographical Map Display

The source of the displayed world map can be:

- The default map provider (Mapbox)
- A map provider of your choice
- Locally installed map resources

The system is set up by default to get the geo map tiles from a specific Mapbox URL through a direct Internet connection. If required, you can use a different (custom) map tiles provider by providing a specific URL. Both of these options require an Internet connection. If you do not have an Internet connection, you can install the map resources locally and specify that you want the system to use the local map resources, which means that you are effectively working offline. See [Use Internal Maps for Geo Map Display, on page 35](#) for more information.

To choose a geo map provider:

#### Procedure

**Step 1** From the main menu, choose **Admin > Visualization Settings** and click the **Map** tab.

- a) To specify a different external map provider, select the **Connect to external map provider** radio button, select **Custom**, and provide the URL the system should access for the geo map tiles.
- b) To use internal map files, select the **Work offline with internal maps** radio button and click **Manage**.

**Step 2** Click **Save**.

## Use Internal Maps for Geo Map Display

If you do not have an Internet connection and therefore the system cannot access an external map provider to retrieve geo map tiles, you can install and use internal map files to represent the areas of the world you require for your network. These map files must be downloaded from Cisco.com and then installed and activated. The name of the map file indicates the area of the world it contains, for example,

**Crosswork\_Patch\_3.1.1-geoserver-africa-1.0.0\_signed.tar.gz**. If you will be managing a network in a specific part of the world, download and install only the relevant map files. You do not need to install all available map files.




**Note** If you choose to work offline with internal maps and you do not install map files, your geo map will display as a generic world map without details of cities, streets, and so on.

To use internal maps for your geo map:

### Before you begin


Download the required map files from Cisco.com and place them on an accessible server.

### Procedure

- Step 1** From the main menu, choose **Admin > Visualization Settings** and click the **Map** tab.
- Step 2** Select the **Work offline with internal maps** radio button and click **Manage**.
- Step 3** In the Manage Internal Maps dialog, Click  to install a new map file.
- Step 4** In the Install New Map dialog, provide details of the server to which you downloaded the map file so that the system can access the file. Note that this server must support SCP protocol for file transfer.
- Step 5** Click **Install Map**.  
The system uploads the map from the specified server. When the process is complete, the new map appears under **Installed Maps** in the Manage Internal Maps dialog.
- Step 6** Install additional maps, as required.
- Step 7** Click **Update All Maps** to save all changes to installed maps. This update process might take some time.

## Set Display Preferences for Devices and Links

You can determine how devices and links will be shown on the topology map, based on your needs and preferences.

To set map display preferences, click  in the top right section of the topology map.

- For devices, you can choose whether to show the device state and how the devices should be labeled. By default, the device state is shown on the map and the host name is used to label devices.

- For links, you can choose whether to show aggregated links and how links should be colored so that you can easily see their state and utilization status. By default, aggregated links will be differentiated from single links on the map and links will be colored based on link utilization thresholds. Administrators can change the utilization thresholds and their corresponding colors. See [Define Color Thresholds for Link Bandwidth Utilization, on page 36](#).

## Define Color Thresholds for Link Bandwidth Utilization

Cisco Crosswork Network Controller comes with a default set of bandwidth utilization thresholds (percentage ranges) and corresponding color indicators. You can customize these to meet your needs, taking into account the following notes and limitations:

- You can enter values in the "To" ranges. Each row begins automatically from the end of the previous row's range.
- The thresholds must be sequential, meaning that each row's range must follow on from the previous row's range. For example, if the range in the first row is 0-25%, the second row's range must end with a value greater than 25.
- You cannot use the same color for multiple thresholds. For example, you cannot choose **Green** for both the first and second rows.

Administrator privileges are required to change these settings.

### Procedure

- 
- Step 1** From the main menu, choose **Admin > Visualization Settings**.
- Step 2** Click the **Bandwidth Utilization** tab.
- Step 3** In the **Polling Interval** field, enter a whole number from 5 to 60 (minutes) to specify how often links will be polled for bandwidth utilization. By default, link bandwidth is polled every 5 minutes.
- Step 4** In the **Link Coloring Thresholds** area, define the criteria for coloring the links. Each row defines a color and the bandwidth percentage range that the color will represent. The default thresholds are:
- Green—0–25% usage
  - Yellow—25–50% usage
  - Orange—50–75% usage
  - Red—75–100% usage
- Step 5** Click **Save**.
- 

## Set Up Bandwidth on Demand and Bandwidth Optimization

During installation of Cisco Crosswork Network Controller, the following function packs are installed:

- **Bandwidth on Demand (BoD):** This function pack provides a bandwidth-aware Path Computation Element (PCE) to derive SR policy paths with requested bandwidth when available. Computed paths are deployed to the network through SR-PCE. BWoD continuously monitors link utilization to ensure no

congestion occurs along the path. If conditions change in the network which causes link utilization to exceed the congestion threshold set by the user, BWoD automatically reoptimizes the policy path. See [Bandwidth on Demand, on page 37](#) and [Configure Bandwidth on Demand, on page 38](#).

- **Bandwidth Optimization (BWOpt):** This function pack provides automated SR policy based tactical traffic engineering capability to detect and mitigate congestion in your network. It achieves this through a real-time view of the network topology overlaid with a demand matrix built through telemetry-based Segment Routing Traffic Matrix (SRTM). BWOpt uses the threshold interface utilization requested by the user and compares it to the actual utilization in the network. When interface congestion is detected by BWOpt, it attempts to shift traffic away from hot spots through the use of tactical traffic engineered SR policies which are deployed to the network via SR-PCE. As network conditions (topology and/or traffic) change over time, BWOpt will continue to monitor interface utilization and manage any tactical SR policies deployed, including changing their paths and/or removing them from the network when deemed no longer necessary. See [Bandwidth Optimization, on page 39](#) and [Configure Bandwidth Optimization, on page 40](#).

## Bandwidth on Demand

The Bandwidth on Demand (BWoD) function pack provides a bandwidth-aware Path Computation Element (PCE) to derive SR policy paths with requested bandwidth when available. Computed paths are deployed to the network through SR-PCE. BWoD continuously monitors link utilization to ensure no congestion occurs along the path. If conditions change in the network which causes link utilization to exceed the congestion threshold set by the user, BWoD automatically reoptimizes the policy path.

BWoD utilizes a near real-time model of the network along with a demand matrix derived from telemetry-based Segment Routing Traffic Matrix (SRTM) reporting to ensure BWoD policies meet their bandwidth constraints. Users may fine tune the behavior of BWoD, affecting the path it computes, through the selection of application options including network utilization threshold (definition of congestion) and path optimization objectives. The BWoD function pack works as a bandwidth-aware PCE for SR policies created through the Cisco Crosswork Network Controller UI, and for SR policies created through CLI configuration on a headend with delegation to SR-PCE. In the latter case, SR-PCE will subdelegate the SR policy with bandwidth constraint to BWoD for path computation and relay the computed path returned by BWoD to the headend for instantiation.

### Operation Modes

There are two modes of operation for BWoD based on the "Priority" option setting for the application. In non-Priority mode, BWoD takes into account all traffic in the network when computing a path for a SR policy with bandwidth constraint. In this case, BW SR policies compete with all other traffic for resources and may be provided a path that is longer to avoid congestion on links along the shortest path.



**Note** In non-Priority mode, BWoD *should not* be enabled at the same time as the Bandwidth Optimization function pack to ensure they do not conflict.

The Priority mode allows BWoD to ignore all other traffic in the network that is not flowing through a BWoD SR policy and give its policies priority treatment when computing paths. This means that BWoD policies are only contending for resources with other BWoD policies and will likely take the shortest path unless there are links that include a significant amount of other BWoD traffic.



**Note** To mitigate any congestion that may occur by ignoring other traffic, the Bandwidth Optimization function pack *should* be used in conjunction with BWoD in the Priority mode to shift other traffic away from any hotspots caused by the BWoD traffic.

The other traffic may then be sent over alternate (possibly longer) paths to mitigate congestion in this case, while BWoD maintains its policies along the shortest paths.

## Configure Bandwidth on Demand

Do the following to enable and configure Bandwidth on Demand.

### Procedure

**Step 1** From the main menu, choose **Optimization Engine > Function Packs > Bandwidth on Demand**.

**Figure 2: Bandwidth on Demand Configuration Window**

**Step 2** From the **Enable** tile, toggle the slider to **True**.

Notice that each time a tile is updated it turns blue.

**Step 3** Select one of the following **Primary Objectives**:

- **Maximize Available Bandwidth**—Computes an SR policy path maximizing the overall available bandwidth in the network. This setting generally attempts to maximize usable network capacity at the expense of potentially longer paths.
- **Metric Minimization**—Computes an SR policy path minimizing the metric selected. This setting generally results in the shortest available paths for a metric type.

**Step 4** In the **Link Utilization** tile, enter the congestion constraint (in percentage). When the Bandwidth on Demand application searches a path for the policies being delegated, it will avoid any paths that may exceed the congestion utilization threshold.

**Step 5** In the **Reoptimization Interval** tile, enter the duration (in seconds) after which the paths will be reoptimized if conditions in the network change. This is a count down timer where the BWoD policy will wait to reoptimize until this duration has expired.

**Step 6** In the **Metric Reoptimization Interval** tile, enter the duration (in seconds) after which the paths can be reoptimized for metric optimization. If the bandwidth constraint is still being met, but a shorter IGP or TE

path is available, BWoD will not run reoptimization until the timer has expired. This value is meant to dampen frequent path changes and reoptimizations in the network.

- Step 7** From the **Priority Mode** tile, toggle the slider to **True** if you have also enabled Bandwidth Optimization.
- Step 8** Click the **Advanced** tab for more advanced configuration (see the following table for field descriptions).
- Step 9** Click **Commit Changes** to save the configuration.

**Table 6: Advanced Bandwidth on Demand Fields**

Field	Description
<b>Private New SR Policies</b>	If <b>True</b> , all policies that are created using Bandwidth on Demand are private.
<b>SR Policy Traffic</b>	Determines the type of bandwidth optimization that is performed with each policy. <ul style="list-style-type: none"> <li>• <b>Simulated</b>—Uses the current simulated traffic on the BWoD provisioned SR policies for optimization calculations.</li> <li>• <b>Measured</b>—Uses the current measured traffic of BWoD provisioned SR policies for optimization calculations.</li> <li>• <b>Max Simulated Requested</b>—Uses the maximum value between the current simulated traffic on BWoD provisioned SR policies or the amount of bandwidth requested for optimization calculations.</li> <li>• <b>Max Measured Requested</b>—Uses the maximum value between the current measured traffic on BWoD provisioned SR policies or the amount of bandwidth requested for optimization calculations.</li> </ul>
<b>Deployment Timeout</b>	The time (in seconds) to wait for a PCE dispatcher response.
<b>Update Throttle</b>	When enabled, this option throttles updates from Cisco Crosswork Network Controller and instructs BWoD to only accept 1 update per <i>x</i> seconds. Set it to <b>0</b> to disable the throttle.
<b>Debug Optimizer</b>	
<b>Debug Opt Max Plan Files</b>	The maximum number of debug plan files you would like to save.
<b>Debug Opt</b>	If <b>True</b> , debug log files will be saved.

## Bandwidth Optimization

The Bandwidth Optimization (BWOpt) function pack provides automated SR policy based tactical traffic engineering capability to detect and mitigate congestion in your network. It achieves this through a real-time view of the network topology overlaid with a demand matrix built through telemetry-based Segment Routing Traffic Matrix (SRTM). BWOpt uses the threshold interface utilization requested by the user and compares it to the actual utilization in the network. When interface congestion is detected by BWOpt, it attempts to shift traffic away from hot spots through the use of tactical traffic engineered SR policies which are deployed to the network via SR-PCE. As network conditions (topology and/or traffic) change over time, BWOpt will continue to monitor interface utilization and manage any tactical SR policies deployed, including changing their paths and/or removing them from the network when deemed no longer necessary.

## Configure Bandwidth Optimization

After Bandwidth Optimization is enabled, Cisco Crosswork Network Controller monitors all interfaces in the network for congestion based on the configured utilization threshold. When the utilization threshold is exceeded, it automatically deploys tactical polices and moves traffic away from the congested links. When congestion is alleviated, Bandwidth Optimization automatically removes the tactical SR policy.

Do the following to enable and configure Bandwidth Optimization.

### Procedure

**Step 1** From the main menu, choose **Optimization Engine > Function Packs > Bandwidth Optimization**.

**Figure 3: Bandwidth Optimization Configuration Window**

The screenshot shows the 'Bandwidth Optimization Configuration' window. On the left, there is a navigation menu with 'Configuration' selected. The main area is titled 'Configuration' and has two tabs: 'Basic' and 'Advanced'. The 'Basic' tab is active and contains several configuration tiles:

- Enable:** A toggle switch currently set to 'False'.
- Optimization Objective:** A dropdown menu set to 'Minimize the IGP metric'.
- Color:** A text input field containing '1000'.
- Utilization Threshold:** A text input field containing '100'.
- Utilization Hold Margin:** A text input field containing '5'.
- Maximum Global Reoptimization Interval:** A text input field containing '0'.
- Delete Tactical SR Policies when Disabled:** A toggle switch currently set to 'False'.
- Profile ID:** A text input field containing '0'.
- Max Number of Parallel Tactical Policies:** A text input field containing '1'.

**Step 2** From the **Enable** tile, toggle the slider to **True**.

Notice that each time a tile is updated it turns blue.

**Step 3** Select one of the following **Optimization Objectives**:

- **Maximize Available Bandwidth**—Leads to preferred paths that result in higher available bandwidth values on interfaces.
- **Minimize the IGP/TE/Delay**—Leads to preferred paths that result in lower total IGP/TE or Delay metrics.

**Step 4** In the **Color** tile, enter a color value to be assigned to Bandwidth Optimization SR policies.

**Step 5** In the **Utilization Threshold** tile, enter a percentage that represents the interface utilization threshold for congestion. Traffic utilization on any interface exceeding this threshold will trigger Bandwidth Optimization to attempt to mitigate. To set thresholds for individual links, see [Set Bandwidth Threshold for Links, on page 42](#).

**Step 6** In the **Utilization Hold Margin** tile, enter a percentage that represents the utilization below the threshold required of all interfaces to consider removing existing tactical SR policies. For example, if the Utilization Threshold is 90% and the Utilization Hold Margin is 5%, then tactical SR policies deployed by Bandwidth Optimization will only be removed from the network if all interface utilization is under 85% (90 - 5) without the tactical policy in the network. This serves as a dampening mechanism to prevent small oscillations in interface utilization from resulting in repeated deployment and deletion of tactical SR policies. The Utilization Hold Margin must be between 0 and the Utilization Threshold.




- Step 7** In the **Maximum Global Reoptimization Interval** tile, enter the maximum time interval (in minutes) to reoptimize the existing tactical SR policies globally. During a global reoptimization, existing tactical policies may be rerouted or removed to produce a globally more optimal solution. Set to 0 to disable.
- Step 8** From the **Delete Tactical SR Policies when Disabled** tile, toggle the slider to **True** if you want all deployed tactical SR policies deleted when Bandwidth Optimization is disabled.
- Step 9** In the **Profile ID** tile, enter the profile ID that will be assigned to tactical SR policies that are created. Enter **0** if you do not wish to assign a profile ID.
- Step 10** In the **Max Number of Parallel Tactical Policies** tile, enter the number of parallel tactical policies that Bandwidth Optimization can create between the same source and destination to obtain the utilization threshold. This is helpful when faced with large demands that cannot be moved in its entirety. Having the ability to create parallel tactical policies increases the chance for Bandwidth Optimization to mitigate congestion.
- Step 11** Click the **Advanced** tab for more advanced configuration (see the following table for field descriptions).
- Step 12** Click **Commit Changes** to save the configuration. Cisco Crosswork Network Controller begins to monitor network congestion based on the threshold that was configured.
- Note**
- You can easily turn Bandwidth Optimization on or off by toggling the **Enable** slider to **True** or **False**.
  - Click  to view events relating to instantiation and removal of tactical SR policies created by Bandwidth Optimization.

Table 7: Advanced Bandwidth on Demand Fields



Field	Description
<b>Fix Tactical SR Policy Duration</b>	The minimum time (in seconds) between the creation of a new tactical SR policy and when it can be removed or modified. This serves as a dampening factor to control the rate of change to deployed tactical SR policies.
<b>Removal Suspension Interval</b>	The time (in seconds) between any tactical SR policy change and when any tactical SR policy can be removed or modified. This allows SRTM to converge after a tactical SR policy creation, allowing traffic on the policy to be reported accurately.
<b>Deployment Timeout</b>	The maximum time (in seconds) to wait until deployment of tactical SR policies is confirmed.  The value assigned should be larger for larger networks to account for the increased processing time needed by SR-PCE to deploy an SR policy. Tactical SR policies not confirmed before this timeout are declared failed and Bandwidth Optimization will disable itself for troubleshooting.
Congestion Check Suspension Interval	The minimum duration in seconds after any tactical SR policy addition or deletion to suspend congestion detection or mitigation to allow model convergence.
<b>Debug Optimizer</b>	
<b>Debug Opt Max Plan Files</b>	The maximum number of optimizer debug files written to disk.
<b>Debug Opt</b>	If <b>True</b> , optimizer debug files will be saved to disk in the <code>/tmp</code> directory of the Bandwidth Optimization container.

## Set Bandwidth Threshold for Links

Networks have many different links (10G, 40G, 100G) that require different thresholds to be set. The Bandwidth Optimization Link Management feature allows a threshold value to be set per interface instead of just one value for the entire network.

### Procedure

---

- Step 1** From the main menu, choose **Optimization Engine > Function Packs > Bandwidth Optimization**.
- Step 2** Click . The Import Configuration File dialog box appears.
- Step 3** Click the **Download sample configuration file** link.
- Step 4** Open and edit the file with the node, interface, and threshold information that you want to set.
- Step 5** Save the file with your changes and go back to the Import Configuration File dialog box.
- Step 6** Click **Browse** and navigate to the CSV file you just edited.
- Step 7** Click **Import**. Bandwidth Optimization checks the CSV node entries for validity. If valid, all the entries appear in the Link Management table.
- Step 8** You can do the following from this table:
- To delete all entries, click **Delete All**.
  - To export the entries as a CSV file, click .
- 

## Additional Useful Information

Although not strictly related to getting up and running, the following topics provide additional information that might be useful when working with Cisco Crosswork Network Controller.

- [Change the IP Address of the Cisco NSO Provider, on page 42](#)
- [Update Device Information, on page 43](#)
- [Delete Devices, on page 44](#)

## Change the IP Address of the Cisco NSO Provider


To change the IP address of the Cisco NSO provider:

### Before you begin

This task must be done during a maintenance window.

## Procedure

---

- Step 1** Set all devices to ADMIN\_DOWN state and remove YANG\_MDT capability from devices, where relevant. This can be done in bulk by exporting the devices to a .csv file, making the change for all the devices in the .csv file, and then importing the file back into Cisco Crosswork Network Controller.
- In the Cisco Crosswork Network Controller UI, go to **Device Management > Devices**.
  - Select the devices you want to export and click .
  - Save the .csv file.
  - Set all devices to ADMIN\_DOWN state.
  - Remove YANG\_MDT capability from the relevant devices.
  - Save the .csv file.
- Step 2** Import the updated .csv file. See [Import Devices, on page 26](#).
- Step 3** Edit the provider:
- In the Cisco Crosswork Network Controller UI, go to **Admin > Providers**.
  - Make the required updates to the IP address under **Connectivity Type(s)**.
  - Click **Save**.
- Within a few minutes, all the devices should be synced to the updated Cisco NSO provider.
- Step 4** Check that the devices have been pushed to Cisco NSO.
- Step 5** In Cisco NSO, run the **sync-from** and **fetch-host-keys** commands for all the devices.
- Step 6** Replace YANG\_MDT capability on the relevant devices and set all the devices to ADMIN\_UP state by exporting the devices to a .csv file, updating the file, and then importing it back into Cisco Crosswork Network Controller, as described above.
- Step 7** Check that the MDT configuration has been added to the devices.
- 

## Update Device Information

Device information can be updated for individual devices or for multiple devices at the same time (using the export and import functions).

### Before you begin


You must change the device state to ADMIN\_DOWN before updating any of the following device parameters:


- Connectivity information
- Capability
- Telemetry information

## Procedure

---

- Step 1** Before updating devices, it is always good practice to export a backup of the devices.
- Go to **Device Management > Devices**.

- b) Select the devices you want to export and click .
- c) Save the .csv file.

- Step 2** Make sure that the state of the devices you want to update is ADMIN\_DOWN.
- Step 3** From the main menu, choose **Device Management > Devices**.
- Step 4** Select the device(s) you want to update, then click .
- Step 5** Edit the device parameters, as required. For a description of the fields you can update, see [Add Devices Through the UI, on page 27](#).
- Step 6** Click **Save**.
- Step 7** Confirm device reachability.

## Delete Devices

Complete the following procedure to delete devices.

### Before you begin


- If the auto-onboard **managed** or **unmanaged** options are set for the SR-PCE provider, you should set auto-onboard for the SR-PCE(s) to **off**.
- Confirm that the device is not connected to the network or that it is powered off before deleting the device.
- If a device has services associated with it, you must remove the service associations in Cisco NSO before deleting the device in Cisco Crosswork Network Controller. If the service removal is not fully successful, zombie links might remain in Cisco NSO. In this case, the device would be deleted successfully in Cisco Crosswork Network Controller but you need to remove the zombie links and delete the device from Cisco NSO.




### Note

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

### Procedure

- Step 1** Export a backup CSV file containing the devices you plan to delete.
- Step 2** From the main menu, choose **Device Management > Devices**.
- Step 3** (Optional) In the **Devices** window, filter the list of devices by entering text in the **Search** field or filtering specific columns.
- Step 4** Check the check boxes for the devices you want to delete.
- Step 5** Click  to change each device's state to ADMIN DOWN or UNMANAGED.

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

**Step 6** Click .

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

---

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.