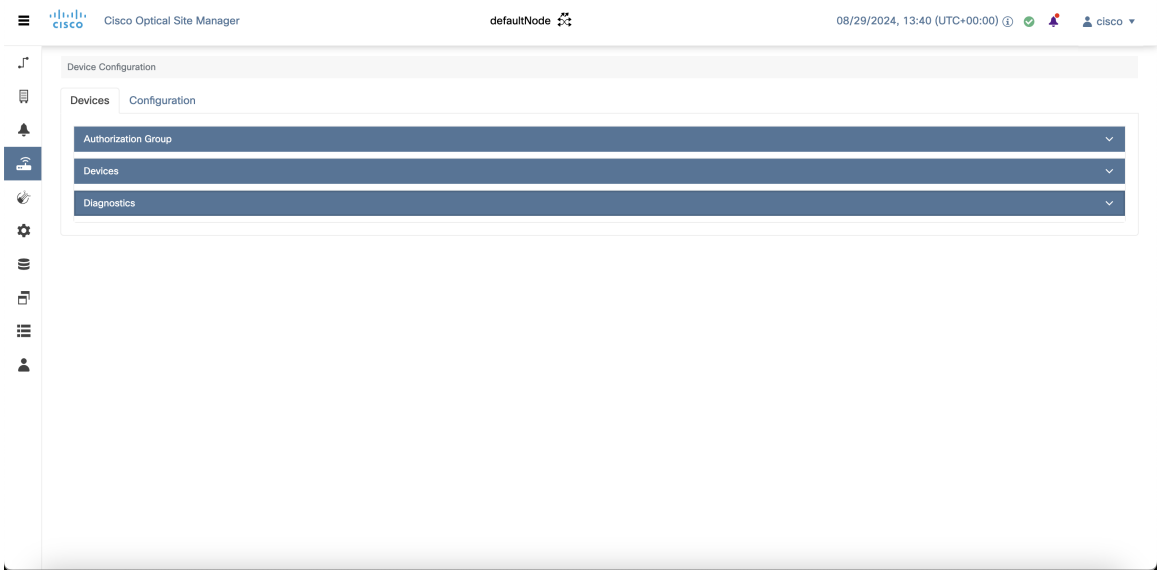


Configure Devices

This chapter describes the tasks related to device configuration in Cisco Optical Site Manager.

Figure 1: Configure Devices



- Create or edit an authorization group, on page 1
- Add a device, on page 3
- Retrieve device diagnostics, on page 11
- SOCKS Proxy, on page 12
- Change the Cooling Profile Control, on page 13
- SVO-LC device onboard in R25.1.1, on page 13

Create or edit an authorization group

create, modify, or remove authorization groups, enabling you to manage user access and permissions efficiently within the network management application.

- Create an authorization group.
- Edit an authorization group.

Authorization groups help you manage user and group attributes used by authentication and authorization processes.

You manage authorization groups from the **Devices** area.

Before you begin

- Log into Cisco Optical Site Manager
- For Cisco Optical Site Manager device management, we strongly recommend to configure the authorization group with credentials for a local IOS XR user account on the managed device. The account must have write-capable NETCONF access, such as a `root-lr` user or equivalent.

  Use IOS XR credentials in this order of preference:

  1. A local IOS XR user account.
  2. If a TACACS+ account is required, configure a local user account with the same username, password, and privileges to ensure seamless management of the device even if TACACS server is not available.
  3. If TACACS+ authentication fails, Cisco Optical Site Manager can manage the device only when the TACACS+ and local user credentials match.

Follow these steps to manage authorization groups.

Procedure

Step 1 Click **Devices** in the left panel.

The **Device Configuration** page appears.

Step 2 In the **Devices** area, click **Authorization Group** to expand it.

The table lists all available authorization groups.

Step 3 Perform these steps, as needed.

To	perform these steps
Create a new authorization group	**a.** Click **Add Auth Group**. The **Add Authorization Group** dialog box appears. **b.** Enter values in the **Auth Group Name**, **Remote User Name**, and **Remote Password** fields. **c.** Click **Add**. The new authorization group is added to the table.
Edit an authorization group	**a.** Click **Edit**. The fields in the table are now editable. **b.** Update the **Remote User Name** and **Remote Password** fields, as needed. **c.** Click **Apply**.

To	perform these steps
	The authorization group is updated in the table.

The authorization group table reflects your changes.

Add a device

Onboard a NCS 1000 or NCS 2000 device so it can be tracked, monitored, and managed within Cisco Optical Site Manager.

Note Wait for the current device to complete synchronization before you add the next device to Cisco Optical Site Manager.

Figure 2: Add a Device

Follow these steps to add an NCS 1000 or NCS 2000 device to Cisco Optical Site Manager.

Before you begin

- Log into Cisco Optical Site Manager
- Use an authorization group with an IOS XR administrative account that has write-capable NETCONF access, such as a `root-lr` user or equivalent, for device onboarding. Cisco Optical Site Manager requires these privileges because it performs configuration changes on the XR device after onboarding.
- Before onboarding an NCS 1001 device, verify that the device has a COSM-supported ECDSA crypto key. Cisco Optical Site Manager uses SSH/SFTP/SCP for device operations such as database backup, SOR file download, device diagnostics, and device software download or activation.

  On the IOS XR device, run:

```
RP/0/RP0/CPU0:ios# show crypto key mypubkey ecdsa

Key label: the_default
Type     : ECDSA General Curve Nistp256
Degree   : 256
Created  : <timestamp>
Data     :
 <key-data>
```

  The output must include one of these supported key types:

```
Type     : ECDSA General Curve Nistp256
Type     : ECDSA General Curve Nistp384
Type     : ECDSA General Curve Nistp521
```

  If no supported ECDSA key is displayed, configure one of the following on the IOS XR device:

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# crypto key generate ecdsa nistp256
RP/0/RP0/CPU0:ios(config)# commit
```

  You can configure one of these keys on the IOS XR device:

```
crypto key generate ecdsa nistp256
crypto key generate ecdsa nistp384
crypto key generate ecdsa nistp521
```

Note In Cisco Optical Site Manager R25.1.1 and R26.1.1, ED25519 keys are not supported for these COSM device operations. For NCS 1001 devices, ED25519 is the default key type, but a supported ECDSA key is required.

- For Cisco Optical Site Manager device management, we strongly recommend to configure the authorization group with credentials for a local IOS XR user account on the managed device. The account must have write-capable NETCONF access, such as a `root-lr` user or equivalent.

  Use IOS XR credentials in this order of preference:

  1. A local IOS XR user account.
  2. If a TACACS+ account is required, configure a local user account with the same username, password, and privileges to ensure seamless management of the device even if TACACS server is not available.

3. If TACACS+ authentication fails, Cisco Optical Site Manager can manage the device only when the TACACS+ and local user credentials match.

Procedure

Step 1 Click **Devices** in the left panel.
The *Device Configuration* page appears.

Step 2 In the **Devices** tab, click the **Devices** section to expand it.

A table appears that lists all the devices that are configured.

Step 3 Click the **Add Device** icon.
The **Add Device** dialog box appears.

Step 4 Select the **Device Type** from the drop-down list.

Select	to
ncs1000	add a NCS 1000 device.
ncs2000	add a NCS 2000 device.
unmanaged-network-element	add a device that is not actively managed by NCS 1000 or NCS 2000.

Step 5 Enter the **Netconf Port**.

Note This field is displayed only if *ncs1000* is selected in the **Device Type** drop-down list.

Step 6 Enter the **Device Name** and **IP Address**.

Use this table to identify the recommended IP address for onboarding NCS 1000 host devices.

Table 1: Recommended IP address for onboarding NCS 1000 host devices

Deployment mode	NCS 1000 device onboarding IP address
HA	Use the IP address of the interface configured as **cosm redundancy interface-name** to onboard each host device.
Standalone	Use the IP address of the interface configured as the **cosm mgmt-interface-name**.

Step 7 Enter the **UID**.

Note This field is displayed only if *ncs1000* or *ncs2000* is selected in the **Device Type** drop-down list.

Step 8 Select an authorization group from the **Auth Group** drop-down list.

Step 9 Click **Add**.

The device is added to Cisco Optical Site Manager and displayed in the **Devices** section.

In an NCS 1000 HA deployment, the Name column displays an A icon for the active node and an S icon for the standby node.

What to do next

Warning Do not perform any cross-connection-related changes through the IOS XR CLI once the device is managed by Cisco Optical Site Manager.

Add Unmanaged Devices

Use this task to add an unmanaged device in Cisco Optical Site Manager.

- Allows you to add and configure passive devices on the network.
- Supports devices that are not actively managed by NCS 1000 or NCS 2000.

Unmanaged devices are devices that are not actively managed by NCS 1000 or NCS 2000. Examples include switches, LAN controllers, and passive optical devices.

The **Add Device** dialog box includes the **unmanaged-network-element** option, which enables adding unmanaged devices.

Table 2: Feature History

Feature Name	Release Information	Description
Add Unmanaged Devices	Cisco IOS XR Release 24.3.1	The **Add Device** dialog box includes the **unmanaged-network-element** option, allowing the addition of unmanaged devices. This enhancement allows you to add and configure passive devices on the network.

- After adding the unmanaged device, add it to a rack unit as a passive unit.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to add an unmanaged device.

Procedure

Step 1 Click **Devices** in the left panel.

The *Device Configuration* page appears.

Step 2 In the **Devices** tab, click the **Devices** section to expand it.

The table lists all configured devices.

Step 3 Click the **Add Device** icon.

The **Add Device** dialog box appears.

Step 4 In the **Add Device** dialog box, perform these steps:

a) Select **unmanaged-network-element** from the **Device Type** drop-down list.

b) Click **Add**.

The device is added to Cisco Optical Site Manager and displayed in the **Devices** section.

Step 5 In the rack view, perform these steps to add a passive unit:

a) Right-click an empty rack unit and select **Add a Passive Unit**.

The **Add Passive Unit in Ru Position** dialog box appears.

b) Select the unmanaged device from the **Select Device** drop-down list.

c) Select the passive type, slot, and passive UID from the respective drop-down lists.

d) Click **Provision**.

A confirmation message appears.

Step 6 Click **OK**.

Step 7 After adding the unmanaged or passive device to the rack, perform these device management actions, as needed.

To	Perform these steps
Delete a device	**a.** Right-click the unmanaged or passive device in the rack. **b.** Select **Delete**.
Move a device to a different rack unit	**a.** Right-click the unmanaged or passive device in the rack and select **Cut**. **b.** Right-click an empty rack unit and select **Paste**.
View device properties	**a.** Right-click the unmanaged or passive device in the rack and select **Properties**.

The unmanaged device is added to Cisco Optical Site Manager and displayed in the **Devices** section.

What to do next

After adding or modifying the passive unit, verify that it is displayed correctly in the rack view and in the device list.

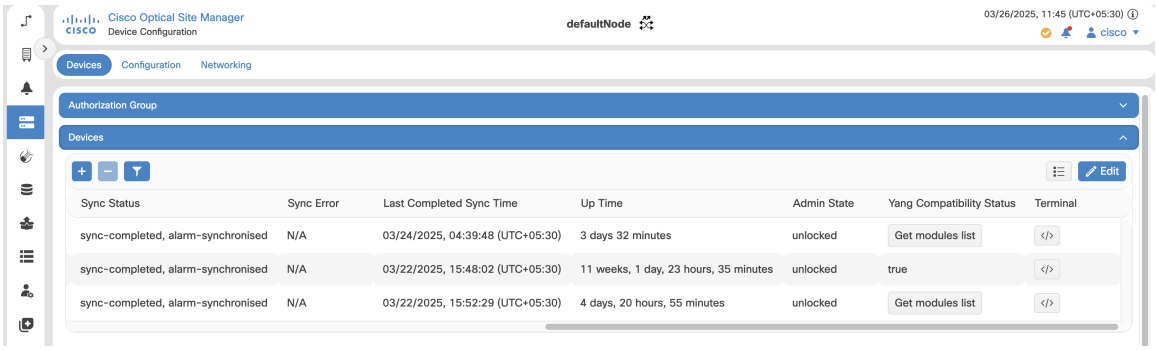
Manage a device using IOS XR CLI

Table 3: Feature History

Feature Name	Release Information	Description
Direct CLI Access for Managed Devices	Cisco IOS XR Release 25.1.1	You can now directly access the Cisco IOS XR CLI for managed devices from the **Devices** section.

Cisco Optical Site Manager provides direct access to the Cisco IOS XR CLI for managed devices through the **Devices** section.

Figure 3: Manage a Device Using IOS XR CLI



Follow these steps to access and manage the device using the IOS XR CLI interface.

Before you begin

Log into Cisco Optical Site Manager

Procedure

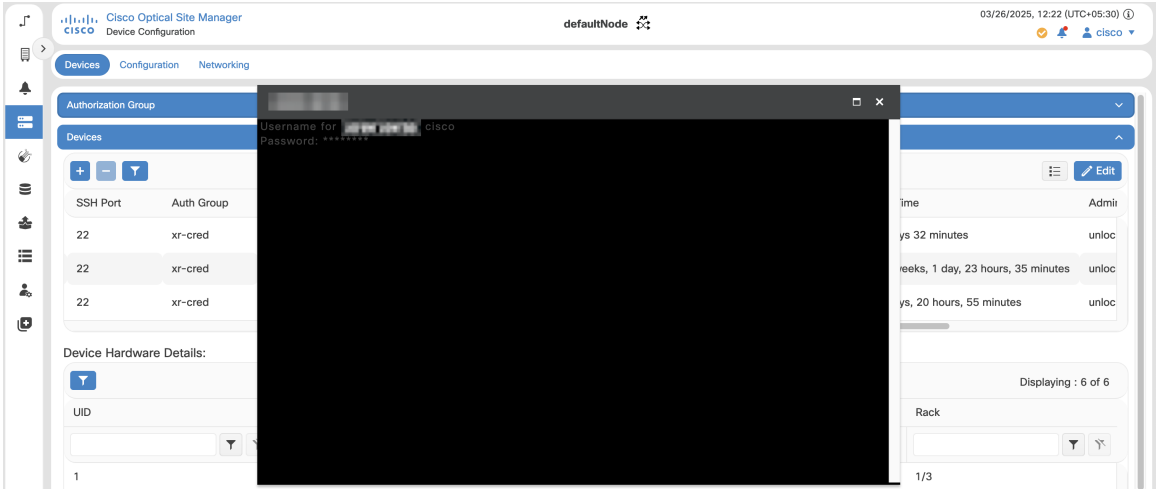
Step 1 Click **Devices** in the left panel.
The *Device Configuration* page appears.

Step 2 In the **Devices** tab, click the **Devices** section to expand it.

A table appears that lists all the devices that are configured.

Step 3 Click the terminal icon next to the device under the **Terminal** column.

The terminal window is displayed, and the system prompts you to enter the username.



Step 4 Type the username and press **Enter**.
The system prompts you to enter the password.

Step 5 Type the password and press **Enter**.

Move a device or view device properties

Manage devices by moving them between rack units or viewing their properties in Cisco Optical Site Manager.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to move or view properties of a device.

Procedure

Step 1 Click **Devices** in the left panel.

Step 2 In the **Devices** tab, click the **Devices** section.

Step 3 Perform these device management actions as needed.

To	Perform these steps
Move a device to a different rack unit	**a.** Right-click the device in the rack and select **Cut**. **b.** Right-click an empty rack unit and select **Paste**.
View device properties	Right-click the device in the rack and select **Properties**.

Delete devices and authorization groups

Maintain network efficiency and security by regularly deleting obsolete devices and authorization groups from the application.

Follow these steps to delete devices, SNMP groups, and authorization groups:

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to delete a device or authorizarion group.

Procedure

Step 1 Click **Devices** in the left panel.

Step 2 Perform these steps as needed.

To	Perform these steps
Delete a device	**a.** Click the **Devices** section. **b.** Select the check box corresponding to the devices you want to delete. **c.** Click **Delete Device(s)**. **d.** Confirm the action when prompted.
Delete an authorization group	**a.** Click the **Username and Password** section. **b.** Select the check box corresponding to the authorization groups you want to delete. **c.** Click the - button to delete the authorization group. **d.** Confirm the action.

A confirmation message appears.

Step 3 Click **Yes**.

The selected device or autoriazrion group is removed from the system.

Retrieve device diagnostics

Retrieve, download, and review diagnostics on the Diagnostics page.

Follow these steps to retrieve and download the device diagnostics:

Before you begin

Log into Cisco Optical Site Manager

Procedure

Step 1 Click **Devices** in the left panel.

Step 2 In the **Devices** tab, click the **Diagnostics** section to expand it.

The configured devices are listed in a table.

Step 3 Select the **Node Diagnostics** check box next to the device for which you want to retrieve the diagnostics.

Step 4 Click **Retrieve**.

A confirmation message appears.

Step 5 Click **Yes** to proceed.

A **Request Accepted** message appears.

Step 6 Click **OK**.

A message appears when the diagnostic action is completed.

Step 7 Select the check box next to the device for which you want to download the diagnostics and click **Download**.

The system downloads a zip file containing the logs.

The downloaded ZIP file contains diagnostic logs, which can be reviewed for troubleshooting, performance monitoring, or compliance purposes.

SOCKS Proxy

Socket Secure (SOCKS) is a standard proxy protocol for IP-based applications developed by IETF. SOCKS Proxy feature allows the Cisco Optical Site Manager node to access remote NCS 2000 nodes using SOCKS Proxy server. You can set the SOCKS proxy server as an External Network Element (ENE) or a Gateway Network Element (GNE).

Benefits

- SOCKS Proxy is used when the Cisco Optical Site Manager node cannot connect directly to the remote NCS 2000 node through DCN.
- OSPF need not be enabled to propagate the routes as routing to the remote node is done by the SOCKS Proxy server.
- SOCKS Proxy allows the Cisco Optical Site Manager node to connect to remote nodes behind the firewall of a GNE.

Limitations

- A SOCKS Proxy server must be used only to connect to small remote nodes (OLA nodes).
- A SOCKS Proxy server must serve only up to five NCS 2000 nodes.

Change the Cooling Profile Control

Use this task to change the cooling profile control of the NCS 2006 node from automatic to manual or the other way round.

Before you begin

Log into Cisco Optical Site Manager

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

Step 2 Click the **Configuration** > **Device Settings** tabs.

Step 3 Choose the control from the **Cooling Profile Control** drop-down list.

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.

SVO-LC device onboard in R25.1.1

Each Cisco Optical Site Manager instance created in the SVO-LC supports on boarding both NCS 2000 and NCS 1000 devices. Communication with these devices is through the bridge interface (***br-devices***) as output interface.

SVO-LC utilizes a SOCKS server to facilitate communication with NCS 2000 devices. For NCS 1000 devices, communication is handled through a local bridge integrated into the SVO-LC, which serves as a gateway with the IP address 192.168.254.65/26. This address should be configured as the Gateway IP when adding a new route to access the NCS 1000 device.

Configure additional route for NCS 1000 device

Use this task to establish communication with the NCS 1000 device.

Before you begin

- Log into Cisco Optical Site Manager
- Select the NCS 1000 device to be connected.

Procedure

Step 1 Click **Devices** in the left panel.
The *Device Configuration* page appears.

Step 2 Click the **Networking** tab.

Step 3 Click the **Add Devices Gateway** icon under **Devices Gateway**.
The **Add Devices Gateway** dialog box appears.

Step 4 Enter the **Subnet** and **Gateway** IP address, and click **Apply**.

The default Gateway IP address is 192.168.254.65

The SVO-LC establishes connection with the NCS 1000 device.

Figure 4: Add Devices Gateway

