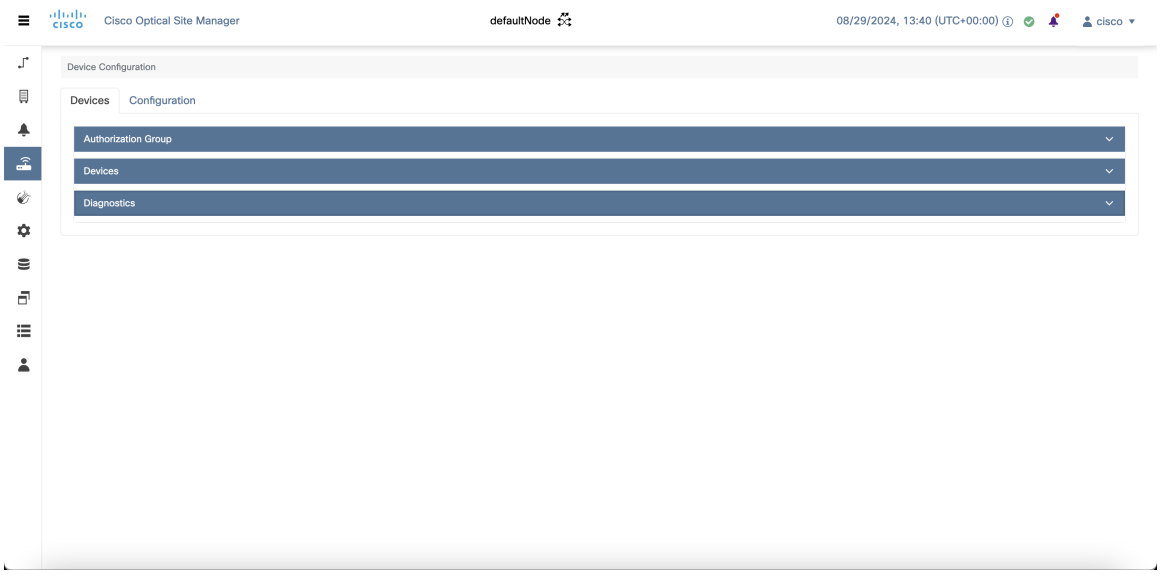


Configure Devices

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 2
- Retrieve device diagnostics, on page 7

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

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**. The authorization group is updated in the table.

The authorization group table reflects your changes.

Add a device

Cisco Optical Site Manager automatically detects and onboards directly connected peer devices on the network. Onboard a NCS 1000 or NCS 2000 device so it can be tracked, monitored, and managed within 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.

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.

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.

To	Perform these steps
	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.