

# Configuration Guide for Cisco Optical Site Manager, IOS XR Release 24.3.x

**First Published:** 2024-09-04

**Last Modified:** 2026-09-30

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2024 Cisco Systems, Inc. All rights reserved.



# CONTENTS


CHAPTER 1 **Cisco Optical Site Manager** 1

Cisco Optical Site Manager 1

Log into Cisco Optical Site Manager 1

CHAPTER 2 **Node Functional View** 3

Understanding Node Functional View 4

NFV icons 6

View node details 8

View degree details for a OLS node 8

Optical Channel Monitoring 9

View Optical Channel Monitoring data 11

OCM spectrum graph 11

OCM utilization table 12

Optical Time Domain Reflectometer 13

OTDR icons 14

Run a manual OTDR scan in expert, multi-region, or auto-sector mode 15

Enable Automatic OTDR Scan 16

View side details 17

View side details for an OLS node 18

View card details 19

View port details 20

View patch cord details 21

View circuit details 21

Connection verification 22

Verify connections 23

Customize NFV layout 24

View active circuit list 25

CHAPTER 3 Cisco Optical Site Manager Topology 27

Topology 27

Add a rack 27

Add a chassis 28

Open the card view 29

Identify a passive device associated with a USB 30

View voltage, temperature and current information 30

View power monitoring parameters 31

CHAPTER 4 Monitor Faults 33

Fault Monitoring 33

View rack, chassis, or card alarms 34

View all alarms and conditions 35

View rack, chassis, or card transient conditions 36

View alarms history 36

Alarm profiles 37

Create and load alarm profiles 38

Associate alarm profiles 39

CHAPTER 5 Configure Devices 41

Create or edit an authorization group 41

Add a device 43

Add Unmanaged Devices 47

Move a device or view device properties 49

Delete devices and authorization groups 49

Retrieve device diagnostics 50

CHAPTER 6 Provision Line Cards 53

Supported NCS 1000 line cards 54

Open the card view 54

NCS 1000 line card modes 55

Configuring card modes 57

Select a card mode 57
Select trunk and client data rate 59
Add Internal Patch Cords 60
Add trunk details 62
Verify configuration details 63
Edit card mode for NCS 1000 cards 64
Reset a line card 65
Provision trail trace monitoring 66
Provision ODU interfaces 67
Provision OTU interfaces 69
Provision Ethernet interfaces 71
Provision optical channels 73
Change Trunk Port Parameters 75
Provision optical threshold settings 76
Configure G.709 thresholds 78
Provision FEC thresholds 79
Configure RMON thresholds 80
Configure loopback interfaces 81
Configure optical safety 82
Enable attention LED 84
PSM card protection mechanism 85
Enable the revertive protection switching 86
Configure the non-revertive protection switching 87
Perform a manual switch 87

CHAPTER 7 **Configure the Node** 89
Import a Cisco Optical Network Planner configuration file 90
Optical Degrees 91
Manage Optical Degrees 91
Internal patch cords 93
Create internal patch cords 93
Automatic Power Control 96
APC at the Shelf Controller Layer 96
APC at the Amplifier Card Level 98

Forcing Power Correction 99
Enable APC 99
Disable APC 99
Span Loss Measurement 100
View or modify span loss parameters 100
Configure amplifier parameters 102
Provision interface parameters 104
Provision Raman Amplifier Parameters 106
Manage Raman Interface Parameters 108
Optical cross-connect circuits 110
View Optical Cross-Connect Circuits 111
Troubleshooting incorrect OXC path endpoints 113
Update OXC endpoints by importing a configuration XML file 113
Edit OXC endpoints from the COSM CLI 115

CHAPTER 8 **Cisco Optical Site Manager Settings** 119
Configure time zone and measurement units 119
Download device diagnostics 120
View Audit Logs 121
Smart licensing for Cisco Optical Site Manager 122
Configure smart licensing workflow 124
Smart transport mode 125
Smart licensing CSLU mode 125
Create a Token 126
Configure DNS to Access Cisco Optical Site Manager 127
Configure transport mode 128
Establish trust 129
Smart licensing offline mode 130
Configure offline transport mode in Cisco Optical Site Manager 131
Download trust request file from Cisco Optical Site Manager 131
Upload trust request file to CSSM 132
Download acknowledgment from CSSM 133
Import acknowledgment file into Cisco Optical Site Manager 133

CHAPTER 9 **Backup and Restore Database** 135

Database Backup and Restore 137

Backup and download database 137

Restore Database 138

Upload Database 139

CHAPTER 10 **Upgrade Software** 141

Cisco Optical Site Manager software packages 141

Workflow for Software Upgrade 142

Download GISO image 143

Download Software Package on Device 144

Activate NCS 1000 device software 145

Delete software package 146

CHAPTER 11 **View Inventory** 147

View inventory of all racks or chassis 147

View inventory of a rack or chassis 148

CHAPTER 12 **User access and authentication** 149

User configuration settings 150

Create users 150

Change user password 151

Configure user profile settings 152

Delete users 153

Single sign-on (SSO) 153

Configure and enable SSO with SAMLv2 154

Create an SSO with CAS 155

Enable an SSO with CAS 156

Manage External Authentication 156

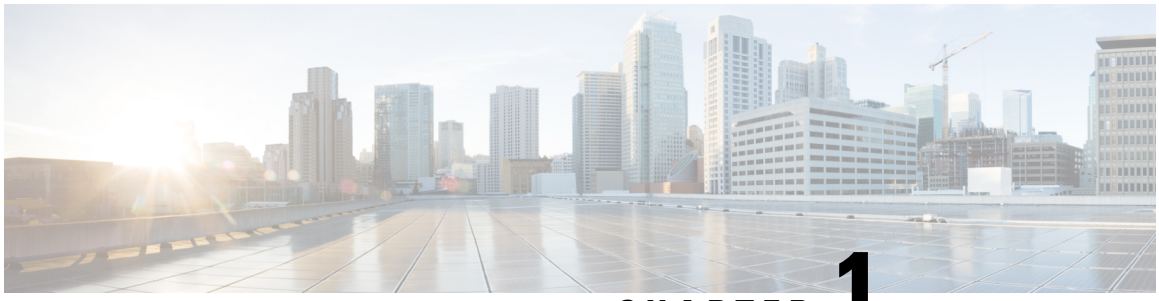
Manage External Authentication 156

Configure static IPv4 route 158

Configure loopback interface as source 158

Limitations for RADIUS or TACACS Authentication 160

User role mapping for TACACS+ and RADIUS authentication 160
RADIUS Authentication 160
Create RADIUS Server Entry 161
Enable RADIUS Authentication 161
Modify RADIUS Server Parameters 162
Disable the RADIUS Authentication 163
Delete the RADIUS Server from Cisco Optical Site Manager 163
TACACS+ Authentication 164
Create TACACS+ Server Entry on Cisco Optical Site Manager 164
Enable TACACS+ Authentication 165
Modify TACACS+ Server Parameters 166
Disable the TACACS+ Authentication 166
Delete the TACACS+ Server from Cisco Optical Site Manager 167
x509 certificates 167
Generate and upload x509 certificates 168
Active login user details 169
View active login sessions 169
View the user login history 170
Session timeout 171
Configure Netconf and webUI session timeout 171



CHAPTER 1

# Cisco Optical Site Manager


- Cisco Optical Site Manager, on page 1


# Cisco Optical Site Manager

Cisco Optical Site Manager provides centralized management and visibility for all optical devices within a site, enabling efficient automation and site-level operations for software-defined optical networks.

Cisco Optical Site Manager offers these key features that facilitate site-level aggregation and management of optical devices:

- **Site Aggregation for Optical Sites:** Aggregates NCS 1010, NCS 1014, NCS 1004, and NCS 1001 devices, giving a unified view of optical site topology and supporting abstraction for OLS, OT, and combined OLS+OT sites.
- **Site-Level Management:** Collects and manages comprehensive site information, including inventory, topology, performance monitoring, and correlated alarms, for streamlined site operations.

Cisco Optical Site Manager delivers enhanced operational control and monitoring capabilities:

- **Web-Based User Interface:** Provides a user-friendly Web UI for managing NCS 1000 devices, visualizing chassis, cards, and passive components, and monitoring active and acknowledged alarms.
- **High Availability:** Can be configured for high availability across two devices within the same network, ensuring continued manageability if one hosting device fails (feature planned for release 24.1).
- **Performance Monitoring:** Enables tracking of current and historical performance metrics for cards and chassis, with options to verify connections and perform loopbacks.

## Log into Cisco Optical Site Manager

Access the Cisco Optical Site Manager web interface to manage and monitor optical site topology, device inventory, performance, and alarms.

**Before you begin**

Perform the Standalone Cisco Optical Site Manager Configuration.

Follow these steps to log into Cisco Optical Site Manager web interface:

### Procedure

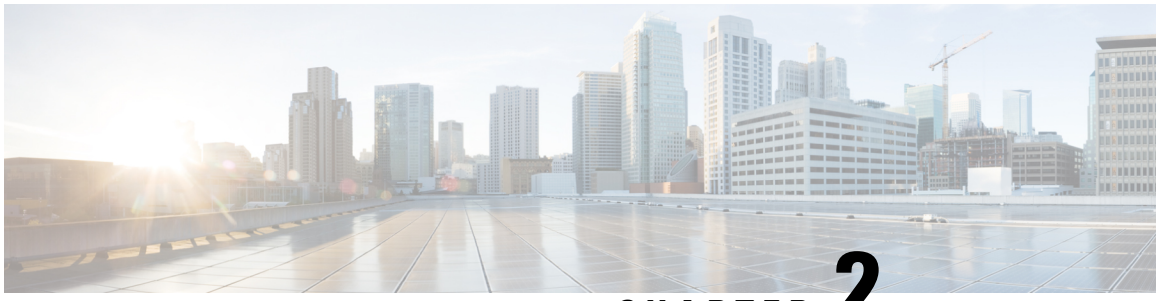
**Step 1** Enter the IP address of the Cisco Optical Site Manager instance in the browser URL field.
The Cisco Optical Site Manager login page appears.

**Step 2** Enter the username and password.

**Note**
Use the credentials configured during the Standalone Cisco Optical Site Manager Configuration) to log into a Cisco Optical Site Manager.

**Step 3** Click **Login**.

The **Topology** page appears.



CHAPTER 2

# Node Functional View

This chapter describes the Node Functional View (NFV) used in Cisco Optical Site Manager and its related tasks.

***Table 1: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Detailed View in NFV for Transponder and Muxponder Card on Third-party OLS Networks | Cisco IOS XR Release 24.2.1 | The Node Functional View (NFV) has been enhanced to provide a detailed view of transponder and muxponder cards on NCS1014 deployed within networks utilizing third-party Optical Line Systems (OLS).<br><br>This detailed view provides a graphical representation of the connections between the trunk and client ports on the transponder and muxponder cards, thereby simplifying the visualization of the network's connection layout. |
| Detailed View in NFV for Transponder and Muxponder Cards on OLS Networks | Cisco IOS XR Release 24.1.1 | You can now access a detailed graphical representation of the connections between the trunk and client ports of the transponder and muxponder cards on Optical Line System (OLS) NCS 1010 networks. This is available in the Map View of Node Functional View (NFV).<br><br>This view is based on the card mode configured on the cards. When you access the detailed view, the right-panel of the Node Functional View displays the card mode details and a list of ports and their settings. |

• Understanding Node Functional View, on page 4
• NFV icons, on page 6
• View node details, on page 8
• View degree details for a OLS node, on page 8
• Optical Channel Monitoring, on page 9
• Optical Time Domain Reflectometer, on page 13
• View side details, on page 17
• View side details for an OLS node, on page 18
• View card details, on page 19
• View port details, on page 20
• View patch cord details, on page 21
• View circuit details, on page 21
• Connection verification, on page 22
• Customize NFV layout, on page 24
• View active circuit list, on page 25

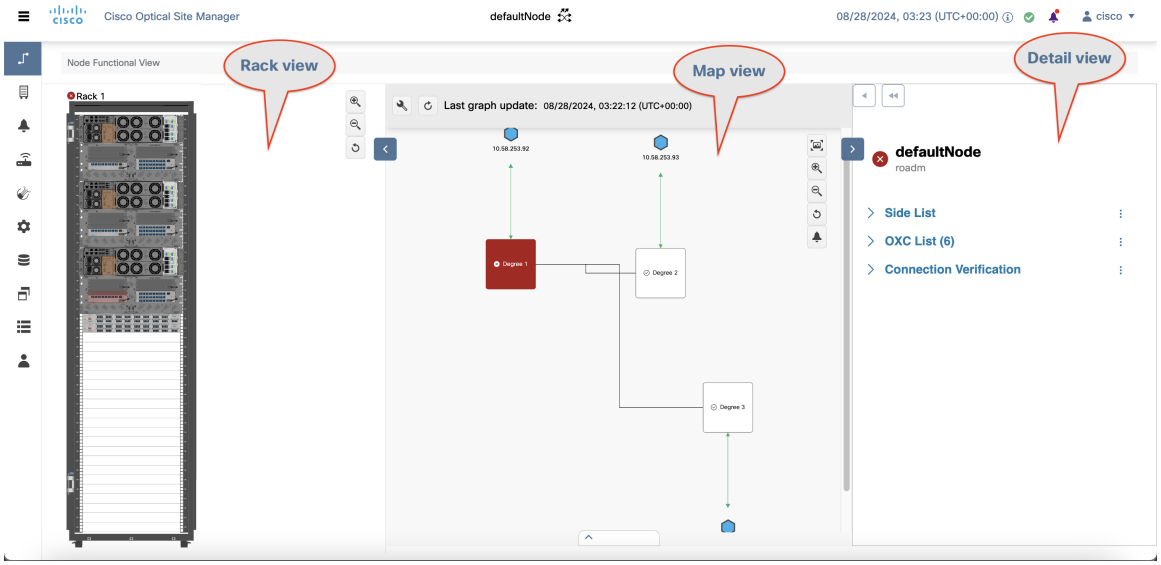
# Understanding Node Functional View

A Node Functional View (NFV) is a visual representation that provides details of a network rack, including the node and its associated components.

Using NFV, you can:

- includes components such as cards and chassis.
- switch between different views.
- explore detailed maps of physical connections.
- interact between the Map and Rack views, allowing you to highlight and zoom in on specific components and their connections, such as optical cross-connections and port details.

*Figure 1: Node Functional View*




## Node Functional View panels

This table describes the NFV panels.

*Table 2: Overview of NFV panels*

| UI element | Description | Use when you need to... | How to access |
|---|---|---|---|
| Rack view | Displays a visual representation of a rack, including the node and its cards. | • Add chassis or passive units.<br>• Open, delete, or view details of chassis and cards. | Click the **Collapse Shoulder** button to expand or collapse this view. |
| Map view | Displays a visual map of the components of the node connected by patch cords according to physical connections. | • Toggle between node, side, card, circuit, port, and patch cord views.<br>• Zoom or highlight a node or card in the rack view<br>• See trunk-client port connections and internal patch cords (IPC) based on card mode. | This view is always visible. |

| UI element | Description | Use when you need to... | How to access |
|---|---|---|---|
| Detail view | Displays all relevant information about nodes, sides, cards, circuits, ports, or patch cords. | • Check optical degrees and their status<br>• View and manage optical cross connections (OXC)<br>• Run connection verification between components<br>• View card mode configuration and details<br>• List available ports and inspect individual port settings | Click the **Collapse Shoulder** button to expand or collapse this view. |

# NFV icons

This section provides an overview of the icons used across various panels in the Node Functional View.

### NFV common icons

This table describes the action icons used in the NFV.

***Table 3: NFV common icons***

| Icon | Description |
|---|---|
|  | Resets the zoomed view to normal view. |
|  | Refreshes the map view with current information. |
|  | Expands or collapses the rack or Detailed view. |

| Icon | Description |
|---|---|
|  | Displays or hides the alarms icon in the map and detailed view.<br>1. Click this button.<br>2. Select or deselect the alarm icons in the drop-down list to display or hide the alarms icon in the map and detailed view. |
|  | Sets the user preferences.<br>For more details, see Customize NFV layout, on page 24. |
|  | Zooms in the rack or map view. |
|  | Zooms out the rack or map view. |
|  | Navigates to the default view in the map view. |
|  | Navigates to the previous page in the map View. |
|  | Expands or collapses the bottom panel that contains the Alarms, OCM, or OTDR tabs. |
|  | Magnifies the selected area of the map view, providing a closer and more detailed view of that specific section. |

### Map view icon colors

Map view icon colors change according to the corresponding alarm severity levels.

***Table 4: Map view icon severity***

| Color | Alarms Severity |
|---|---|
| Red | Critical |
| Orange | Major |
| Yellow | Minor |
| Blue | Default color |

# View node details

The details of a node can be viewed from the right-panel, including the list of nodes, active circuits, and physical connections.

Follow these steps to view the details of a node in the NFV.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

The Node Functional View page appears.

**Note**
The NVF page might take longer to load the first time you open it.

**Step 2** Click **Collapse Shoulder** to expand the right-panel.

The following table describes the details of the sections on the right-panel.

***Table 5: Node details***

| Section | Description |
|---|---|
| Side List | Displays a list of the nodes along with its details, such as span loss value, the IP address of the device it is connected to, and its degree. |
| OXC List | Displays a list of active circuits passing through a particular card.<br>For more details, see View active circuit list, on page 25. |
| Connection Verification | Displays a list of the connections between the line cards and all passive modules.<br>For more details, see Connection verification, on page 22. |

# View degree details for a OLS node

Follow these steps to view the details of the degree for a OLS node in NFV.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

The **Node Functional View** page appears.

**Step 2** Perform any of these to view the details of a degree:

- Right-click a side in the map view and choose **View Details**.
- Click > next to the degree name in the right panel.

**Step 3** (Optional) Click the vertical ellipsis icon and choose from any of the following options to sort the list of ports or OXC:

- **A-Z**
- **Z-A**
- **High Severity**
- **Low Severity**.

You can view these details in the right panel:

- Overall alarm status as a colored label and an icon
- (Optional) Span loss
- (Optional) ORL of OTDR
- (Optional) Fiber End of OTDR
- (Optional) OSC power
- (Optional) IP address of the node of its optional neighbor. To open the Cisco Optical Site Manager web UI of the neighbor node in a new browser tab, click the IP address of the neighbor node.
- Degree of its optional neighbor
- **Card List** tab - Displays the list of all the cards present in both sides. The shelf number and slot number are displayed with the card name. The trunk port number is also displayed for TXP cards.
- **Circuit List** tab - Displays the list of all the circuits present in the side.

# Optical Channel Monitoring

Optical Channel Monitoring (OCM) is a technology used to monitor the performance and health of optical signals (wavelengths) running through fiber networks. It enables operators to gain real-time visibility into the optical spectrum without disrupting traffic.

OCM improves network visibility, enables proactive maintenance, and provides signal assurance. These enhancements reduce downtime and operational complexity in large optical transport networks.

### Key features of OCM

The Optical Channel Monitoring capabilities in the NCS 1010 provide the following essential functions for managing and troubleshooting optical networks:

- **Real-Time Spectrum Monitoring:** OCM scans the optical C-band and visualizes the power levels of individual optical channels. This feature helps detect signal degradation, identify channel presence or absence, and recognize spectral interference.
- **Integration with NCS 1010 ROADM:** The OCM integrated with the ROADM helps validate wavelength routing, power levels, and OSNR (Optical Signal to Noise Ratio).
- **Graphical Spectrum View:** Cisco Optical Site Manager provides a visual representation of the spectrum with channel peaks, helping easily spot anomalies.

### OCM tab icons and elements

The table describes the action icons available in the OCM tab.

| UI Element/Icon | Description |
|---|---|
| Direction | When graph view is enabled:<br>• **RX:** Select to view the optical spectrum in the RX direction.<br>• **TX:** Select to view the optical spectrum in the TX direction.<br>When table view is enabled:<br>• **C-band:** Select to view the optical spectrum for the C band.<br>• **L-band:**Select to view the optical spectrum for the L band. |
|  | Click this button to change to the table or graph view. |
|  | Expected channel missing or underpowered (useful for fault detection). |
|  | Reload the graph or table. |

# View Optical Channel Monitoring data

Optical Channel Monitoring (OCM) on Cisco NCS 1010 enables continuous monitoring of optical signal parameters for each individual wavelength on a fiber.

View power levels (in dBm) of individual wavelengths traveling through a fiber using OCM on Cisco NCS 1010.

Follow these steps to view the OCM for the receive (Rx) and transmit (Tx) directions.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

**Step 2** Right-click an optical degree in the map view and select **Open**.

**Step 3** Expand the panel at the bottom of the page.

**Step 4** Click the **OCM** tab.

**Step 5** Select **RX** or **TX** to view the OCM data for the receive or transmit direction in the spectrum graph.

For more details about the spectrum graph, see OCM spectrum graph, on page 11.

**Step 6** Click the **Spectrum Occupancy Chart** button to view the spectrum occupancy table.

For more details about the spectrum occupancy table, see OCM utilization table, on page 12.

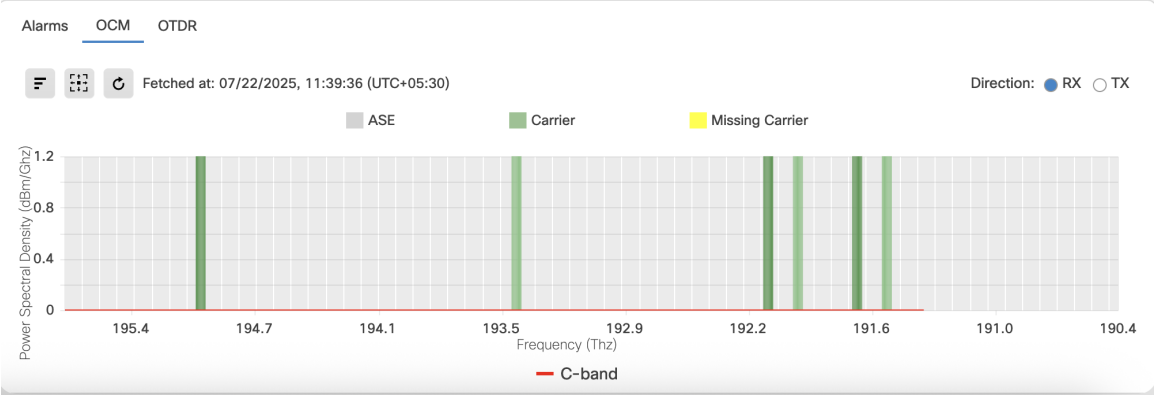
You can view the transmission or reception power levels for the optical degree you selected in the OCM data and spectrum occupancy graph and table.

# OCM spectrum graph

The OCM spectrum graph displays the power spectral density (dBm per GHz) across the optical C-band in the RX or TX directions. This highlights the presence and consistency of carriers.

- **X-Axis (Frequency in THz):** Represents optical frequencies that cover the C-band.
- **Y-Axis (Power Spectral Density):** Displays signal power in dBm per GHz, indicating the strength of received signals at each frequency.

*Figure 2: OCM spectrum graph*




### OCM spectrum graph color elements

The color coding in the OCM spectrum graph identifies the type of signal at each frequency:

| Color | Elements | Description |
|---|---|---|
| Green | Carrier | Valid optical channel present at that frequency. |
| Grey | ASE | Amplified spontaneous emission that represents optical noise level. |
| Yellow | Missing Carrier | Expected channel missing or underpowered (useful for fault detection). |

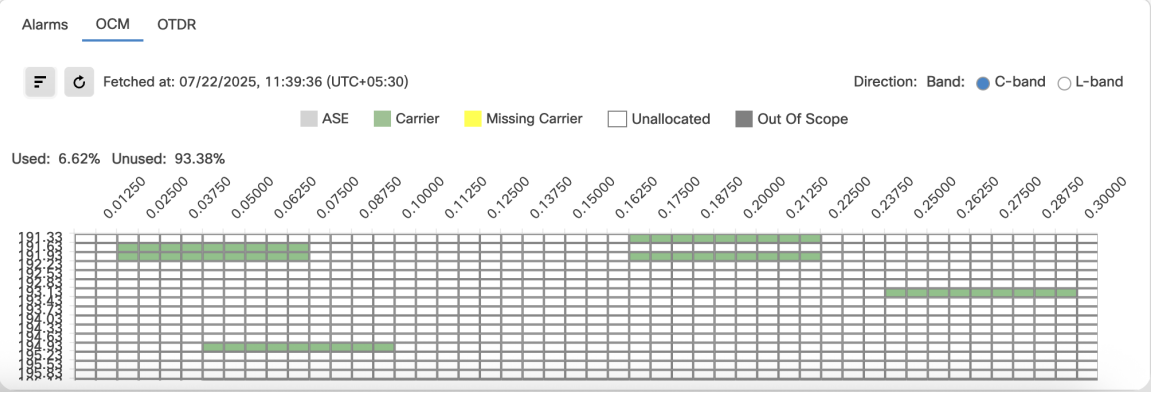
# OCM utilization table

The OCM utilization table presents a frequency-slot grid showing how much of the optical spectrum is currently in use, with each cell representing a discrete frequency-time slot. This table helps network operators quickly assess spectrum occupancy and identify free or underutilized slots for provisioning.

Read and interpret the layout of the OCM table as described in these points:

- **Columns:** The columns in the table represent discrete frequency slot positions, indexed using normalized values (e.g., 0.01250, 0.02500), and aligned with the C-band spectrum.
- **Rows:** Each row shows a specific optical frequency in THz, arranged from higher to lower values.

*Figure 3: OCM utilization table*




### OCM utilization table color elements

The color coding in the OCM table shows different spectral components:

*Table 6: OCM utilization table color coding*

| Color | Element | Description |
|---|---|---|
| Green | Carrier | A green cell shows an active optical signal in that frequency slot and indicates live data traffic or a provisioned channel. |
| Light Gray | ASE | Light gray cells represent amplified spontaneous emission, which is optical noise. |
| Yellow | Missing Carrier | A yellow cell means the expected channel is not detected. This result can indicate signal loss, misalignment, or a transponder issue. |
| Dark Gray | Out of Scope | A dark gray cell shows a frequency region outside the monitoring scope of your current configuration. |

# Optical Time Domain Reflectometer

An Optical Time Domain Reflectometer (OTDR) is a built-in fiber diagnostic tool that

- sends light pulses through the optical fiber,
- measures the reflected signals to detect faults, measure span loss,
- and locates events such as fiber cuts or high reflections.

### OTDR benefits

Cisco Optical Site Manager allows you to access the OTDR functionality of the underlying device in a unified manner, regardless of potential device differences.

The OTDR feature offers several advantages for fiber management:

- Assess fiber quality during system installation before activating traffic.
- Measure real-time loss and back reflection for the fiber pair connected to the TX and RX ports.
- Monitor the fiber during live system operation.
- Inspect the fiber following cable cut and repair events
- Detect fiber degradation due to aging and environmental factors by automatically monitoring span loss and ORL thresholds.

# OTDR icons

The OTDR tab displays the optical trace for the selected degree and direction, helping you analyze signal quality, detect faults, and verify fiber link health.

### OTDR icon descriptions

The table provides an overview of the icons available on the OTDR tab, along with a description of each operation they perform.

***Table 7: OTDR icon descriptions***

| Icon | Description |
|---|---|
| — | To zoom into a specific area, press **Shift** and drag to create a rectangle around the area you want to zoom into. |
| — | Scroll down to zoom out of the graph. |
|  | Resets the graph to its original zoom and position. |
|  | Download the graph as an image. |
|  | Download SOR file that contains the fiber trace details such as the distance, reflectance, loss, and fiber attenuation measurements. |
|  | Save the current OTDR scan results as a baseline. |
|   | Clear the reflections or losses alarms. |

| Icon | Description |
|---|---|
|  | Enable or disable automatic OTDR scan after a fiber cut or Raman Turn Up. |
|  | Indicates the status of the last successful scan. |

# Run a manual OTDR scan in expert, multi-region, or auto-sector mode

Manually run an OTDR scan in expert, multi-region, or auto-sector mode during fiber installation or troubleshooting to verify link quality and locate faults.

*Table 8: Feature History*

### Before you begin

- Log into Cisco Optical Site Manager, on page 1

Follow these steps to manually run an OTDR scan.

### Procedure

**Step 1** Open the **OTDR** tab for an optical degree.

a) Click **Node Functional View** in the left panel.
b) Right-click an optical degree in the map view and click **Open**.
c) Expand the panel at the bottom of the page.
d) Click the **OTDR** tab.

**Step 2** Scroll to the bottom of the panel and click the **gear** icon.

**Step 3** In the **Scan Options** dialog box, select the scan options.

a) From the **Direction** drop down menu, select **rx** or **tx** to run the OTDR scan in the RX or TX directions, respectively.
b) From the **Fiber Scan Mode** drop down menu, select a fiber scan mode.

*Table 9: OTDR fiber scan modes*

| Use | To |
|---|---|
| **auto-sector** | Automatically select the optimal values for OTDR. |

**Step 4** Click **Start Scan** button to start OTDR scan.

The `OTDR-SCAN-IN-PROGRESS-RX` alarm is raised and displayed on the **Alarms** tab of the **Fault Monitoring** menu.

The scan results are displayed in the graph.

### What to do next

1. (Optional) Click **Stop Scan** icon to terminate the OTDR scan.

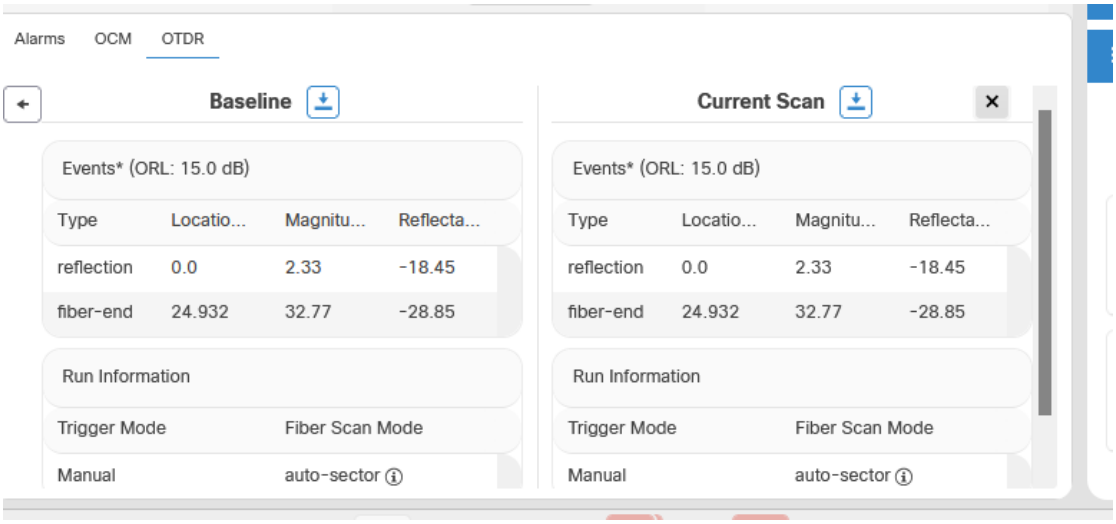
   An informational message appears indicating that the OTDR scan has been terminated.

2. (Optional) In the right-side panel, click **OTDR Data**. This action displays a comprehensive list of OTDR events, including reflections and losses.

   To view detailed analysis data, click the **Enhanced View** radio-button.

3. After the scan is completed, click the i icon to view the scan details and download the SOR files.

***Figure 4: OTDR detailed view***




# Enable Automatic OTDR Scan

Use this task to enable or disable automatic Optical Time Domain Reflectometer (OTDR) scans for supported optical cards.

- Automatically trigger OTDR scans after specific network events.
- Configure delay timers and threshold values for automatic scan execution.

In automatic mode, the system triggers an OTDR scan after events such as span faults, fiber restoration, device power cycles, line card reloads, or Raman turn-up completion (where supported).

Automatic OTDR scan options vary depending on the NCS 1000 or NCS 2000 card types.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to enable or disable automatic OTDR scans.

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

**Step 2** Right-click an optical degree in the map view and click **Open**.

**Step 3** Expand the panel at the bottom of the page.

**Step 4** Click the **OTDR** tab.

**Step 5** Click the ellipsis icon and choose **OTDR Settings**.

The **OTDR Configurations** dialog box appears.

**Step 6** Click the **Global** tab.

a) Select the required check boxes in the **Automatic OTDR Scans Settings** section.

*Table 10: Automatic OTDR Scan Options*

| If you want to enable automatic OTDR scan... | Then select... |
|---|---|
| After a system startup, fiber cut, or repair (supported on both NCS 1000 and NCS 2000 cards) | **System Start-up, Fiber Cut & Repair**<br>Supported for both NCS 1000 and NCS 2000 card types. |

**Step 7** Click **Apply**.

The system enables automatic OTDR scans based on the selected conditions and configured parameters.

# View side details

Use this task to view the details of the side in NFV.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

The Node Functional View page appears.

**Step 2** Right-click a side in the map view and choose **View Details** to view the details of the selected side along with the right shoulder.

**Step 3** View the following information that is displayed in the right shoulder. Optional means that the information is displayed when available.

- Name of the side

- Overall alarm status as a colored label and an icon
- (Optional) Span loss
- (Optional) ORL of OTDR
- (Optional) Fiber End of OTDR
- (Optional) OSC power
- (Optional) IP address of the node of its optional neighbor. To open the Cisco Optical Site Manager web UI of the neighbor node in a new browser tab, click the IP address of the neighbor node.
- Degree of its optional neighbor
- **Card List** tab - Displays the list of all the cards present in the side. The shelf number and slot number are displayed with the card name. The trunk port number is also displayed for TXP cards.

  To sort the list of cards, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.
- **Circuit List** tab - Displays the list of all the circuits present in the side.

  To sort the list of circuits, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

# View side details for an OLS node

Use this task to view the details of the side for a node in NFV.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

The Node Functional View page appears.

**Step 2** Right-click a side in the map view and choose **View Details** to view the details of the selected side along with the right shoulder.

Or

Click the arrow near the side name that is displayed inside the right shoulder.

**Step 3** View Side 1 and Side 2 merged information that is displayed in the right shoulder. Optional means that the information is displayed when available.

- Overall alarm status as a colored label and an icon
- (Optional) Span loss

- (Optional) ORL of OTDR
- (Optional) Fiber End of OTDR
- (Optional) OSC power
- (Optional) IP address of the node of its optional neighbor. To open the Cisco Optical Site Manager web UI of the neighbor node in a new browser tab, click the IP address of the neighbor node.
- Degree of its optional neighbor
- **Card List** tab - Displays the list of all the cards present in both sides. The shelf number and slot number are displayed with the card name. The trunk port number is also displayed for TXP cards.

  To sort the list of cards, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.
- **Circuit List** tab - Displays the list of all the circuits present in the side.

  To sort the list of circuits, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

# View card details

View card details, such as card name, location, port list, and optical cross-connections.

Follow these steps to view the details of the card in NFV.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

**Step 2** Right-click a card in the map view and choose **View Details**.

**Step 3** (Optional) Click the vertical ellipsis icon and choose from any of the following options to sort the list of ports or OXC:

- **A-Z**
- **Z-A**
- **High Severity**
- **Low Severity**.

You can view these card information in the right panel:

| Section | Description |
|---|---|
| Name | Displays the name of the device. |
| Location | Displays the shelf, rack, or slot of the device. |
| Port list | Displays all the ports on the device. |
| OXC List | Displays the list of all the optical cross-connections. |

# View port details

Follow these steps to view the details of the port on a card.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

The Node Functional View page appears.

**Step 2** Right-click a card in the map view and choose **Open**.

**Step 3** Click the port on the device in the map view.

**Step 4** (Optional) Click the vertical ellipsis icon and choose from any of the following options to sort the list of OXC:

- **A-Z**
- **Z-A**
- **High Severity**
- **Low Severity**.

You can view these port information in the right panel:

| Section/Field | Description |
|---|---|
| Name | Displays the name of the port. |
| Location | Displays the shelf, rack, or slot of the card. |
| Powers | Displays the list of all the links with their aggregate power.<br>The aggregate power displays the current power in case of a single port. The aggregate power displays a list of all the different power levels in case of an MPO port or logical group. |

| Section/Field | Description |
|---|---|
| OXC List | Displays the list of all the optical cross-connections. |

# View patch cord details

View patch cord details, such as patch cord name, ports that the patch cord connects, and optical cross-connections.

Follow these steps to view the details of a patch cord.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

**Step 2** Right-click a degree and select **Open**.

**Step 3** Click the patch cord connecting two devices in the map view.
You can view these patch cord information in the right panel:

***Table 11: Patch cord details***

| Section/Field | Description |
|---|---|
| Name | Displays the name of the patch cord. |
| Connections | Displays the ports that the patch cord connects with their cards and the aggregate power. |
| Connection Verification | Displays a list of the connections between the line cards and all passive modules. For more details, see Connection verification, on page 22. |

# View circuit details

View the logical connections established between optical ports or channels within a device.

Follow these steps to view the details of the optical cross connections (OXC) in NFV.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

**Procedure**

**Step 1** Click **Node Functional View** in the left panel.

**Step 2** Click **Collapse Shoulder** to open the right panel.

**Step 3** Click > against the circuit to view the details.

You can view these circuit information in the right panel:

***Table 12: Patch cord details***

| Section/Field | Description |
|---|---|
| **Circuit Info** | Displays these details about the circuit:<br>• **Admin State**<br>• **Service State**<br>• **Frequency**<br>• **Wavelength** |
| **Path** | Displays these details:<br>• **Internal link:** List of ports that are internally connected within the device.<br>• **PIn:** Optical input power level received.<br>• **POut:** Optical output power level. |

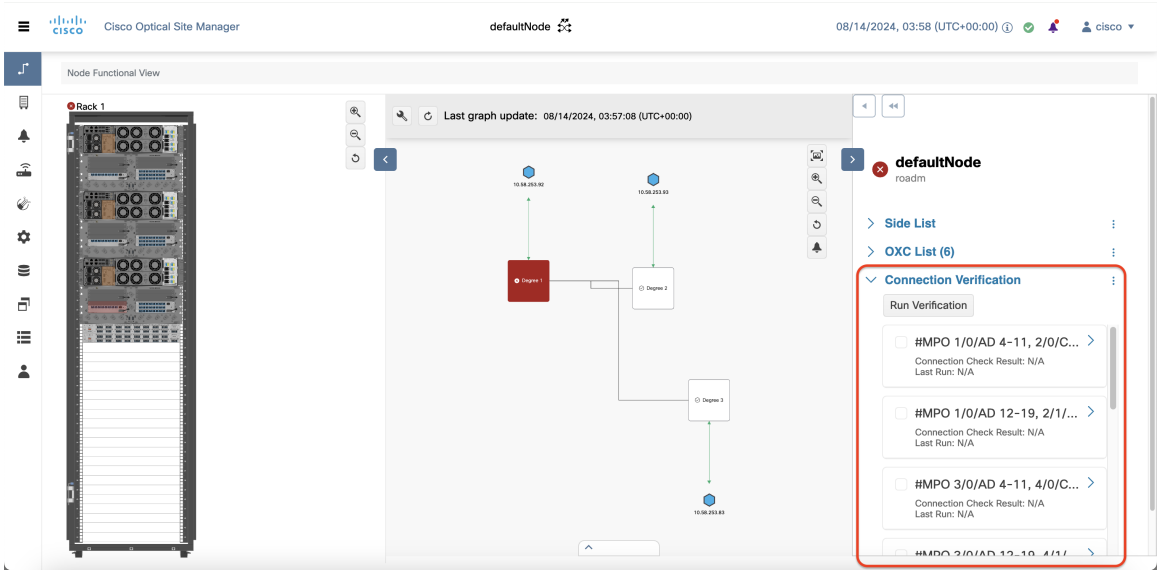
# Connection verification

Cisco Optical Site Manager offers a connection verification process that checks the cabling between the OLT-C line card and passive modules in an NCS 1010 device, helping prevent miscabling during node installation.

The connection verification process generates a specific probe signal from the Connection Verification Tunable Laser (CV-TL) located at COM-RX-2. This probe signal is then detected on the following components:

- The same OLT-C line card.
- Passive modules (Mux/Demux panel or breakout panel) connected to the OLT-C line card.
- A different OLT-C line card or passive module belonging to the same near-end (NE) node.
- An optical interface (router ports or transponders) connected to the line card.

*Figure 5: Connection Verification*




### Connection verification status

This table describes the various connection verification status that are displayed in the **Connection Check Result** field of the right panel.

| Status | Description |
|---|---|
| Connected | Cable or patchcord is connected. |
| Disconnected | Cable or patchcord is disconnected. |
| Connection-Not-Verified | Cable or patchcord is not tested for connection verification. |

# Verify connections

Verify physical connectivity between line cards and passive modules on an NCS 1010 device, ensuring correct cabling and preventing installation errors.

Follow these steps to verify connections.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

**Step 2** Click the **Expand shoulder** icon to expand the right panel.

**Step 3** Scroll to the **Connection Verification** section and click to expand it.
A list of available connections is displayed.

**Step 4** Select the check boxes corresponding to the connections you want to verify.

**Step 5** Click **Run Verification**.
Connection verification is initiated for the selected connections and an information message is displayed.

**Step 6** Click **OK**.

The **Connection Check Result** field displays the status of the connection verification.

# Customize NFV layout

Customize the layout, spacing, and visualization behavior of components in the NFV. These settings are stored in the local storage of the browser and are retained for that browser.

Use this task to customize the NFV layout.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Settings** from the left panel.

**Step 2** Click the **Preferences** tab.

**Step 3** Perform these steps in the **General** section:

| If you want to ... | then |
|---|---|
| Change date format | Select a format from the **Date format** drop-down list. |
| Change the channel | Select **Frequency** or **Wavelength** from the **Configuration channel** drop-down list. |
| Change the measurement unit of length | Select a unit from the **Length measurement unit** drop-down list. |

**Step 4** Select options from the drop-downs in the **Right Shoulder** section to set the default order of lists in the NFV right panel.

**Step 5** Perform these steps in the **Left Shoulder** section:

| If you want to ... | then |
|---|---|
| Set the default opacity factor in rack | Type a value in the **Rack opacity factor** field.<br>Valid range: 0 to 1 in increments of 0.1 |

| If you want to ... | then |
|---|---|
| Set the default left panel width | Type a value in pixels (px) in the **Left shoulder width** field.<br>Valid range: 400 px to 600 px |
| Display only visible cards in the rack | Select the **Show only visible cards on the rack** check box. |

**Step 6** Perform these steps in the **NFV** section:

| If you want to ... | then |
|---|---|
| Set default space between items relative to the center point. | Type a value in the **Degrees space from the center** field. |
| Set the default vertical (or horizontal) distance between stacked layers. | Type a value in the **Layers spacing** field. |
| Set default space between adjacent columns in the layout | Type a value in the **Column spacing** field. |
| Set a default zoom level | Type a value in the **Zoom scaling factor** field. |

**Step 7** Click **Apply**.

**Step 8** Refresh the browser to apply the configured settings.

# View active circuit list

Use this task to view the total number of circuits passing through a degree and a selected card.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Node Functional View** in the left panel.

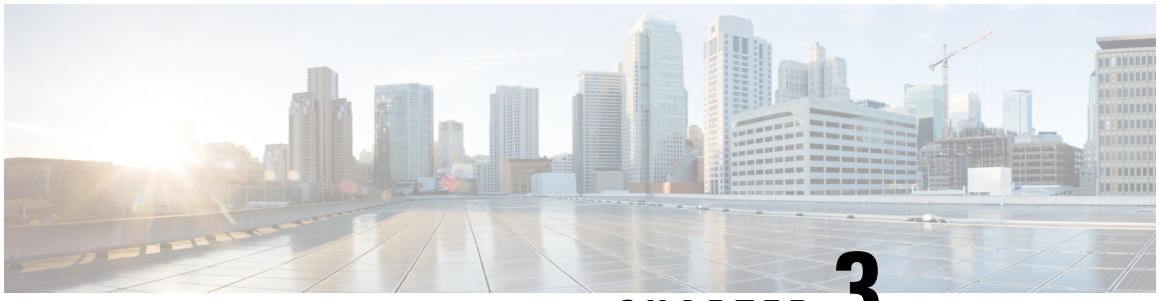
The Node Functional View page appears.

**Step 2** Right-click a **Degree** and click **Open**.

The **OXC List** in the right panel displays the the total number of connections passing through the degree.

**Step 3** Right-click a card and click **Open**.

The **Connections** list in the right panel displays the the total number of connections passing through the degree.



CHAPTER 3

# Cisco Optical Site Manager Topology

This chapter describes the different Cisco Optical Site Manager views. In this chapter, you will also learn to add new racks.


- Topology, on page 27
- Add a rack, on page 27
- Add a chassis, on page 28
- Open the card view, on page 29
- Identify a passive device associated with a USB, on page 30
- View voltage, temperature and current information, on page 30
- View power monitoring parameters, on page 31


# Topology

The **Topology** page provides a visual and tabular representation that allows users to manage optical site configurations effectively. The page offers two distinct views for managing site configurations:

- Rack View
- Table View

### Rack View

Provides a graphical representation of a rack, including nodes and cards. Users can hover over a device or node to display its name in a tooltip, aiding in quick identification.

### Table View

Displays a detailed list of chassis with information such as node UIDs, rack numbers, chassis types, and descriptions. This view also allows users to add new racks, simplifying updates and management.

# Add a rack

Use this task to add a rack in Cisco Optical Site Manager. This creates a logical container for devices managed by Cisco Optical Site Manager and enables structured placement and visualization of chassis and other components.

A rack serves as a container for devices that are managed within Cisco Optical Site Manager.

After creating a rack, you can add chassis and other supported devices to it. Racks are displayed in both rack and table views.

- Racks are displayed in both rack and table views.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1

Follow these steps to add a rack in Cisco Optical Site Manager.

**Procedure**

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

The Cisco Optical Site Manager Topology page appears.

**Step 2** Click **Add Rack**.

The **Add Rack** dialog box appears.

**Step 3** Enter a rack ID in the **Rack ID** field.

You can enter any numeric value from 1 through 32767.

**Step 4** Click **Apply**.

The rack is created and displayed in the rack and table views.

The rack is available for adding chassis and managing devices in Cisco Optical Site Manager.

**What to do next**

After creating the rack, add one or more chassis to begin device management.

# Add a chassis

Use this task to add a chassis to Cisco Optical Site Manager so that the device can be tracked, monitored, and managed.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to add a chassis to Cisco Optical Site Manager.

**Procedure**

**Step 1** In the NFV view, right-click a rack and select **Add Chassis**.

The **Add Chassis** dialog box appears.

**Step 2** Select a device from the **Device** drop-down list.

**Step 3** Select the appropriate **Chassis Type**.

**Step 4** Select the **Chassis ID** and enter the **Chassis UID**.

**Step 5** Enter a chassis name in the **Display Name** field.

**Step 6** Click **Provision**.

**Step 7** After adding the chassis, perform these chassis management actions, as needed.

| To | perform these steps |
|---|---|
| Delete a chassis | **a.** Right-click the chassis in the rack.<br>**b.** Select **Delete**. |
| Move a chassis to a different slot | **a.** Right-click the chassis in the rack and select **Cut**.<br>**b.** Right-click an empty slot and select **Paste**. |
| View chassis properties | **a.** Right-click the chassis in the rack and select **Properties**. |

The chassis is added to Cisco Optical Site Manager and displayed in the selected rack.

### What to do next

After adding or modifying a chassis, verify that the device status is synchronized and operational.

# Open the card view

Follow these steps to open the card in a card view.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

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

The rack and **Topology** view appear.

**Step 2** To open the card view, perform any of these steps:

- Right-click the outer edge of the chassis or line card from the rack view and select **Open**.
- Double-click the line card in the rack view.

The card view appears.

# Identify a passive device associated with a USB

Identify a specific passive device associated with a USB port using the LED blink function.

Follow these steps to identify a passive device associated with a USB:

### Before you begin

- Log into Cisco Optical Site Manager, on page 1

### Procedure

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

**Step 2** Click the rack name in the rack view.

**Step 3** Click the **Provisioning** tab.

**Step 4** Click **Passives** to expand the section.

The table displays a list of passive devices.

**Step 5** Select the check box corresponding to a device and click **Edit**.
After selecting a device, the **USB Port** field becomes editable.

**Step 6** Select the USB port from the drop-down list.

**Step 7** Click **Apply**.

**Step 8** Perform one of these steps:

| To | Click |
|---|---|
| start blinking the LED of the passive device | **LED Blink** |
| know the LED status of the associated device | **LED Status** |
| stop the LED blinking | **LED Blink** |

# View voltage, temperature and current information

View the voltage, temperature, and current information of a device using the Cisco Optical Site Manager.

Cisco Optical Site Manager facilitates the monitoring of device voltage, temperature, and current to ensure stable operation, prevent overheating, and maintain safe and efficient device performance.

Follow these steps to view the voltage, temperature, and current information:

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

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

The **Topology** page appears.

**Step 2** Click the rack name from the Rack view.

**Step 3** Right-click the outer edge of the chassis from the Rack view and select **Open** to open the Chassis view.

Alternatively, you can also double-click the chassis to open the Chassis view.

The Chassis view appears.

**Step 4** Click the **Provisioning** tab.

**Step 5** Click the **Voltage/Temperature/Current** section to expand it.

**Step 6** Expand the **Voltage**, **Temperature**, and **Current** sections to view the voltage , temperature, and current information of the chassis.

You can now view the voltage, temperature, and current information.

# View power monitoring parameters

You can view different power metrics of a chassis, such as total power consumption and maximum power, using Cisco Optical Site Manager.

Follow these steps to view the power monitoring parameters of a chassis:

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

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

The **Topology** page appears.

**Step 2** Click the rack name from the rack view.

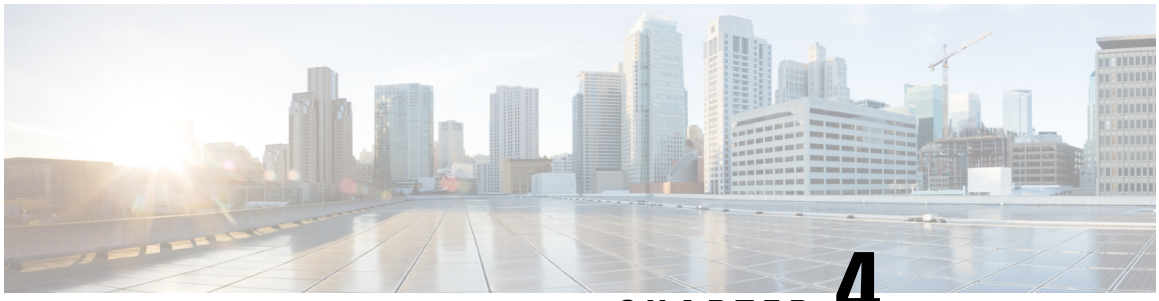
**Step 3** To open the chassis view, perform any of these steps:

- Right-click the outer edge of the chassis from the rack view and select **Open**.
- Double-click the chassis.

**Step 4** Click the **Provisioning** tab.

**Step 5** Click the **Power Monitor** section to expand it.

The chassis total power consumption and maximum power display.



CHAPTER 4

# Monitor Faults

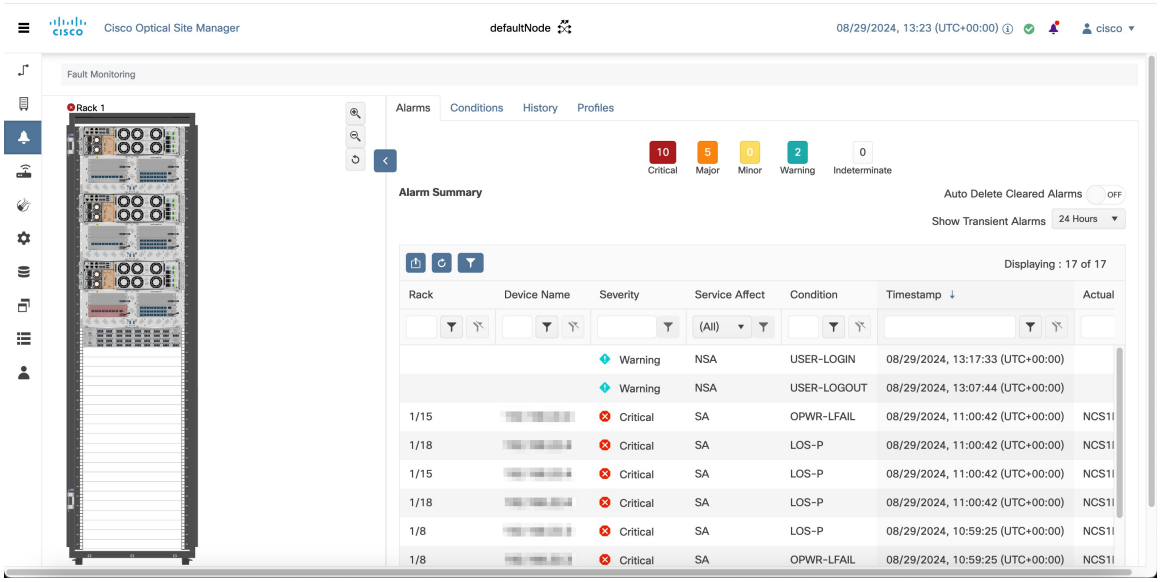
This chapter describes the tasks to view alarms and create alarm profiles.


- Fault Monitoring, on page 33
- View rack, chassis, or card alarms, on page 34
- View all alarms and conditions, on page 35
- View rack, chassis, or card transient conditions, on page 36
- View alarms history, on page 36
- Alarm profiles, on page 37


## Fault Monitoring

The Fault Monitoring panel displays a summary of all encountered alarms and conditions. It displays the number of Critical (CR), Major (MJ), Minor (MN), Warnings (W), and Non-applicable (NA) alarms. It displays the alarms, transient conditions, and historical alarms that are related to chassis, passive devices, pluggables, line cards, amplifier cards, and control cards. You can also create custom alarm profiles and apply them on the node using this pane.

***Figure 6: Fault Monitoring***



**Note** The Cisco Optical Site Manager UI begins capturing XR alarms only after the Cisco Optical Site Manager package is activated. As a result, any alarms generated on the device before this activation are not synchronized with the Cisco Optical Site Manager UI. This leads to a discrepancy where the IOS-XR CLI may show a more complete set of alarms compared to what is available in the Cisco Optical Site Manager UI.

# View rack, chassis, or card alarms

You can view the alarms raised on a rack, chassis, or card from the Alarms tab.

Follow these steps to view the alarms raised on a rack, chassis, or card.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Topology** in the left panel.
The **Topology** page appears.

**Step 2** Perform one of the following steps to view alarms for a rack, chassis or card:

- Click the rack name from the Rack view to view alarms for a rack.
- Right-click the chassis screws from the Rack view and select **Open** to view alarms for a chassis.
- Right-click the card from the Rack view and select **Open** to view alarms for a card.

The **Alarms** tab displays alarms with various severities, each indicated by a different color:

- Critical
- Major
- Minor
- Warning
- Intermediate

**Step 3** (Optional) Select a sepcific time slot from the **Show Transient Alarms** drop-down list to view alarms for a specific time slot.

**Step 4** (Optional) Click the **Auto Delete Cleared Alarms** toggle button to automatically delete the cleared alarms.

**Step 5** (Optional) Click the **Excel Export** button to export and download the alarms to an Excel sheet.

You can view, filter, manage, and export alarms by severity for specific racks, chassis, or cards.

# View all alarms and conditions

Use this task to display, filter, and export alarms and transient conditions in Cisco Optical Site Manager (COSM). This task helps you identify system issues and confirm component health across the managed site.

- Inspect active alarms and transient conditions for system components.
- Export alarms for reporting or archival purposes.
- Enable or disable automatic deletion of cleared alarms as required.



**Note** Cisco Optical Site Manager relies on the default IOS XR syslog format for alarm, event, and notification processing. To ensure proper network monitoring and management, RFC 5424 syslog formatting must not be enabled on devices managed by Cisco Optical Site Manager.

The alarms view aggregates notifications from racks, chassis, cards, and ports. Use it to monitor severity, age, and history of alarmed conditions across the site.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1

Follow these steps to view all alarms and transient conditions:

## Procedure

**Step 1** Click **Fault Monitoring** in the left panel.

Alternatively, click the bell icon in the top-right corner to open the alarms view.

**Step 2** Click the **Alarms** tab to view all active alarms.

Alarms are shown with severities such as Critical, Major, Minor, Warning, and Intermediate. Each severity is indicated by a distinct color.

**Step 3** Click the **Conditions** tab to view transient conditions.

**Step 4** Click the **History** tab to review historical alarm events and cleared alarms.

**Step 5** (Optional) Toggle **Auto Delete Cleared Alarms** to automatically remove cleared alarms from the list.

When enabled, cleared alarms are removed automatically according to the UI setting; when disabled, cleared alarms remain visible in the History view for manual review.

**Step 6** (Optional) Click **Excel Export** to export the currently displayed alarms to an Excel file.

Use the exported sheet for reporting or offline analysis.

The Alarms tab lists active alarms with details such as severity, timestamp, source component, and a brief description. The Conditions tab lists transient conditions and the History tab shows historical alarm events and cleared alarms.

Use exported alarm data for diagnostics, reporting, or to correlate events with device-side logs.

# View rack, chassis, or card transient conditions

View transient conditions on network components such as racks, chassis, and cards. You can download these conditions to an Excel report for further analysis.

Follow these steps to view transient conditions that include standing or transient notifications on the network, node, or card.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Topology** in the left panel.
The Topology page appears.

**Step 2** Perform one of the following steps to view the transient conditions:

| If you want to view the ... | then |
|---|---|
| transient conditions for a rack | click the rack name. |
| transient conditions for a chassis | right-click the chassis screws and select **Open**. |
| transient conditions for a card | right-click the card and select **Open**. |

**Step 3** Click the **Conditions** tab.

**Step 4** Select a time slot from the **Show Transient Alarms In** drop-down list to view transient conditions for a specific time slot.

**Step 5** (Optional) Click the **Excel Export** button to export the transient conditions to an Excel sheet.

# View alarms history

View the alarms history to track and analyze past network issues for effective troubleshooting and trend identification.

Follow these steps to display the alarms history raised on a rack, chassis, or card.

**Procedure**

**Step 1** Click **COSM Topology** in the left panel.
The COSM Topology page appears.

**Step 2** Perform one of the following steps to view the alarms history:

| If you want to ... | then |
|---|---|
| view alarms history for a rack | click the rack name from the rack view. |
| view alarms history for a chassis | right-click the chassis screws from the rack view and select **Open**. |
| view alarms history for a card | right-click the card from the Rack view and select **Open**. |

**Step 3** Click the **History** tab.

The alarms are displayed with various severities, each indicated by a different color:

- Critical
- Major
- Minor
- Warning
- Intermediate

**Step 4** (Optional) Click the **Excel Export** button to export the alarms hisyory to an Excel sheet.

# Alarm profiles

An alarm profile enables you to customize alarm severities by creating unique profiles for individual components such as ports, cards, chassis, passive units, optical cross-connects, and optical interfaces.

Cisco Optical Site Manager includes two predefined alarm profiles:

- Default profile
- All suppressed alarms profile

### Default profile

The *Default* profile serves as the baseline for alarm severities and provides a standardized configuration for all alarms:

- The default alarm profile is preprovisioned on the node and contains all alarms.

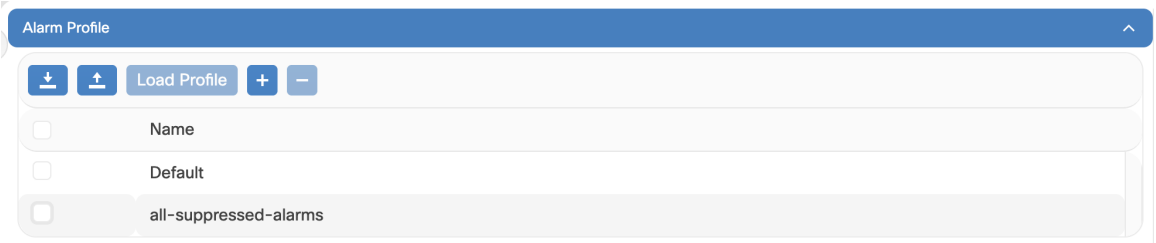
- It sets alarm severities according to standard Telcordia GR-474-CORE guidelines, which cannot be changed.
- Default severities are applied to all alarms and conditions until a new custom profile is created and applied.
- Example of inheritance: A card with an inherited alarm profile adopts the severities applied at the node level.
- Different profiles can be applied at various levels (e.g., node, card, port). You could use the Default profile on a node, cards, and ports, but apply a custom profile to downgrade alarms on a specific card.

### All suppressed alarms Profile

The *all-suppressed-alarms* profile focuses on alarms that are intentionally excluded from monitoring and management:

- The profile includes all alarms that are suppressed.
- It is helpful for troubleshooting by excluding non-critical alerts.
- When applied, the profile ensures that suppressed alarms do not affect the monitoring process.

***Figure 7: Alarm Profiles***




### Customizing alarm profiles

Alarm profiles offer flexibility by allowing users to apply different profiles at various levels of the network hierarchy, enabling tailored alarm management.

- **Default Behavior:** Default severities remain active for all alarms and conditions until a new profile is created and applied.
- **Flexible Application:** Alarm profiles can be applied at different levels of the network hierarchy, providing flexibility in alarm management. For example, the default profile can be used for the node, cards, and ports, while a custom profile may be applied to downgrade alarms on a specific card.
- **Severity Modification:** When modifying an alarm profile, all Critical (CR) or Major (MJ) severity settings—whether default or user-defined—are demoted to Minor (MN) in Non-Service-Affecting (NSA) settings, and vice versa, as per Telcordia GR-474 standards.

# Create and load alarm profiles

Using alarm profiles helps streamline fault monitoring and reduce alarm noise, making it easier to focus on critical issues in the network.

Follow these steps to create and load alarm profiles a node.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Fault Monitoring** in the left panel.

**Step 2** Click the **Profiles** tab.

**Step 3** Click **Alarm Profile** to expand the section.
The default profile **all-suppressed alarms** is displayed along with the list of alarms.

**Step 4** Click the + button to create an alarm profile.

The **Alarm Profile** dialog box appears.

**Step 5** Enter the name of the custom alarm profile in the **Name** field.

**Step 6** (Optional) Choose the resources such as card, ecu, and fan-tray from the **Resources** drop-down list.

You can select multiple resouces from the list.

**Step 7** Click **Apply**.

The alarm profile is created and displayed in the list along with the default alarm profile.

**Step 8** Select the check-box corresponding to the alarm profile and click **Load Profile** to load the alarm profile on the node.

The alarms that belong to the selected alarm profile appear in the **Alarms for Profile** sub-section.

# Associate alarm profiles

Log into Cisco Optical Site Manager, on page 1

Associate custom alarm profiles with the resources, such as ports, cards, chassis, passive units, optical cross-connects, and optical interfaces, to customize alarm severities.

Follow these steps to associate alarm profiles with resources: ports, cards, chassis, passive units, optical cross-connects, and optical interfaces.

### Procedure

**Step 1** Click **Fault Monitoring** in the left panel.

**Step 2** In the **Profiles** tab, click **Profile Association** to expand the section.

**Step 3** Follow these steps to create a profile association:

a) Click the + button.
The **Profile Association** dialog box appears.

b) Type the name of the profile association in the **Association** field.

c) Select the alarm profile from the **Profile** drop-down list and click **Apply**.
The association name and profile are displayed in the table.

**Step 4** Click the + button to expand the association name.

**Step 5** Follow these steps to create a resource type:

a) Click the + button above the *Resource Type* column to create a resource type.

The **Resource** dialog box appears.

b) Select a resource from the **Resource Type** drop-down list:

The **Resource Type** drop-down list contains all the resources to which the alarm profile can be associated. Multiple resources can be associated with the same alarm profile.

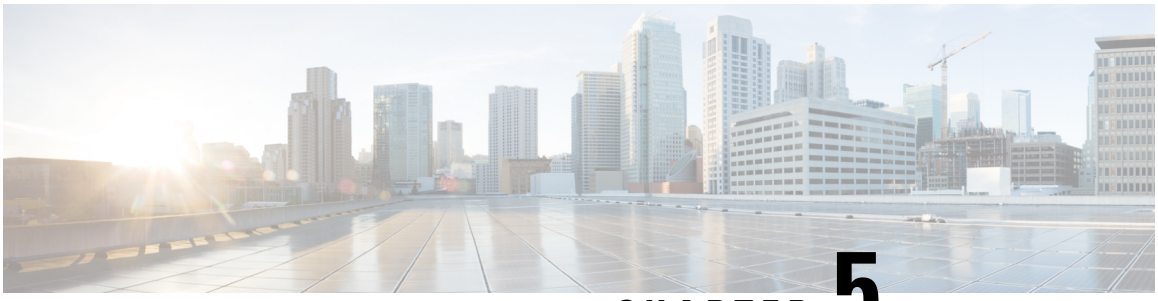
c) Select any of these options from the **Inherited** drop-down list.

- **true** - To indicate if the association should be applied to all the children of this resource.
- **false** - To indicate if the association should not be applied.

d) Select the desired values from the other drop-down lists and click **Apply**.

---

When the alarm profile is associated with the resources, all the outstanding and new alarms matching these resources are immediately set with the new alarm severities.

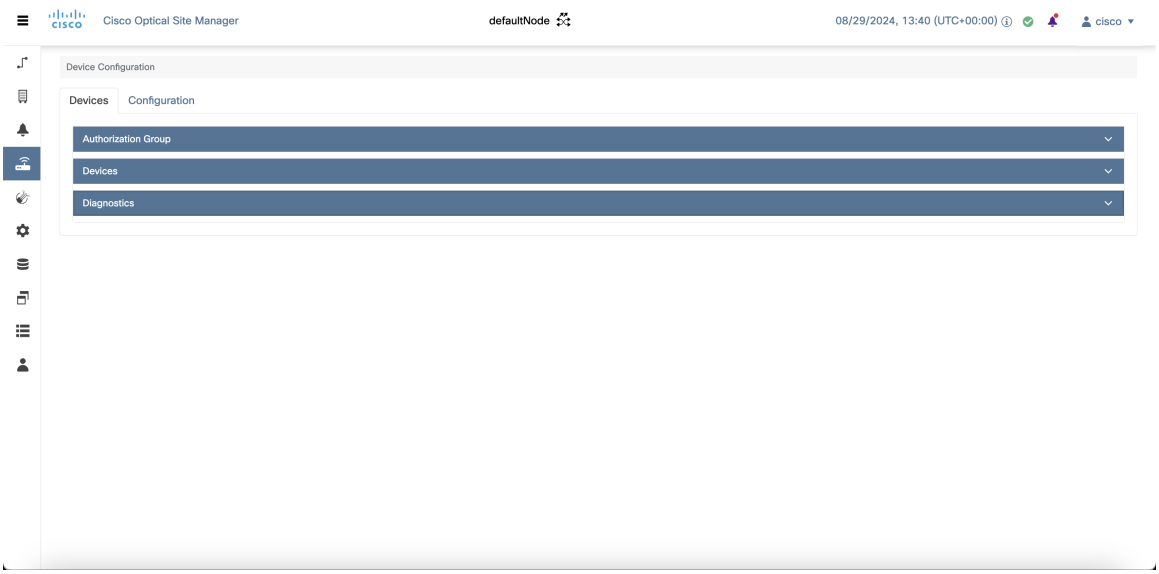


CHAPTER 5

# Configure Devices

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

***Figure 8: Configure Devices***





- Create or edit an authorization group, on page 41
- Add a device, on page 43
- Retrieve device diagnostics, on page 50


# 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, on page 1
- 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**.<br>The **Add Authorization Group** dialog box appears.<br>**b.** Enter values in the **Auth Group Name**, **Remote User Name**, and **Remote Password** fields.<br>**c.** Click **Add**.<br>The new authorization group is added to the table. |
| Edit an authorization group | **a.** Click **Edit**.<br>The fields in the table are now editable.<br>**b.** Update the **Remote User Name** and **Remote Password** fields, as needed.<br>**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 9: 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, on page 1
- 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 13: 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 14: 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.<br>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, on page 1

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.<br>**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**.<br>**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.

# 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, on page 1

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**.<br>**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, on page 1

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.<br>**b.** Select the check box corresponding to the devices you want to delete. |

| To | Perform these steps |
|---|---|
| | **c.** Click **Delete Device(s)**.<br>**d.** Confirm the action when prompted. |
| Delete an authorization group | **a.** Click the **Username and Password** section.<br>**b.** Select the check box corresponding to the authorization groups you want to delete.<br>**c.** Click the - button to delete the authorization group.<br>**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, on page 1

### 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**.

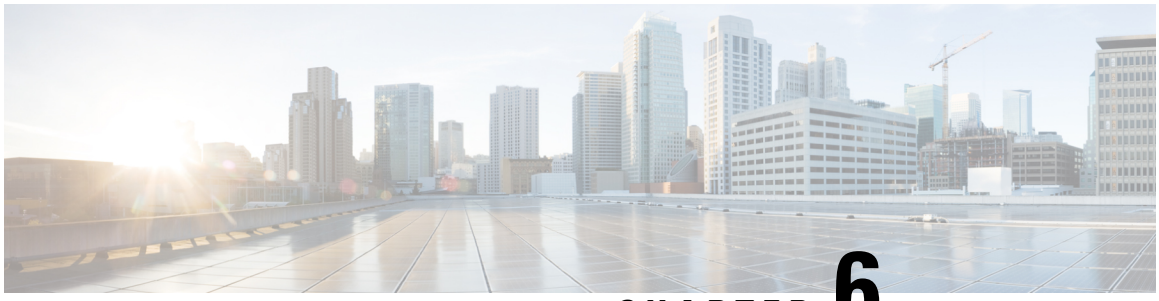
A message appears when the diagnostic action is completed.

**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.

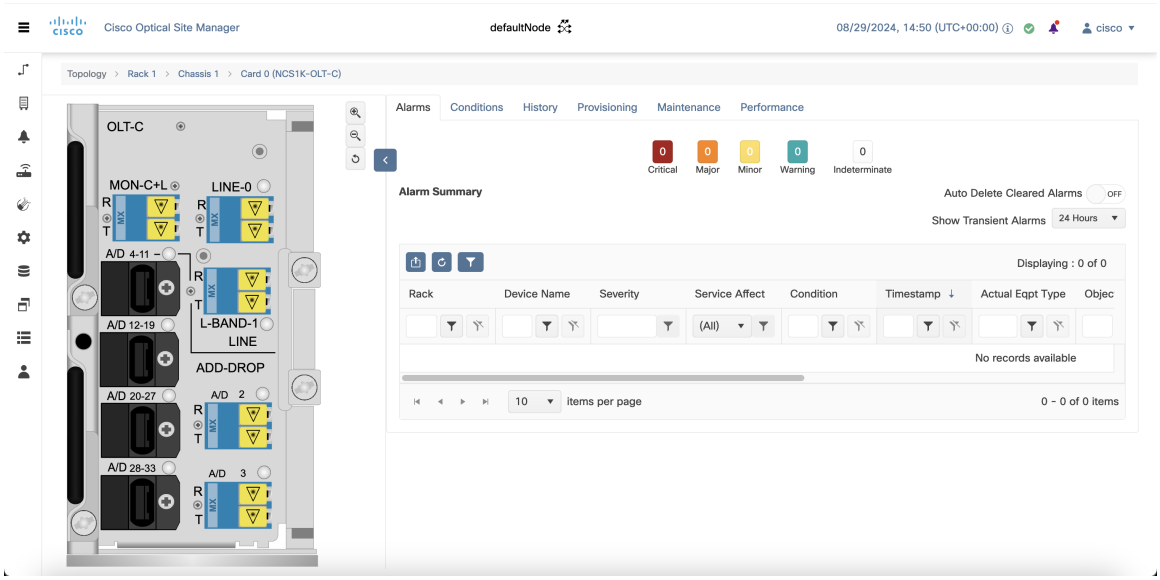


CHAPTER 6

# Provision Line Cards

This chapter describes the tasks related to provisioning the Cisco NCS 1000 line cards in Cisco Optical Site Manager.

***Figure 10: Provision Line Cards***





- Supported NCS 1000 line cards, on page 54
- Open the card view, on page 54
- NCS 1000 line card modes, on page 55
- Reset a line card, on page 65
- Provision trail trace monitoring, on page 66
- Provision ODU interfaces, on page 67
- Provision OTU interfaces , on page 69
- Provision Ethernet interfaces, on page 71
- Provision optical channels, on page 73
- Change Trunk Port Parameters, on page 75
- Provision optical threshold settings, on page 76
- Configure G.709 thresholds , on page 78
- Provision FEC thresholds, on page 79

- Configure RMON thresholds, on page 80
- Configure loopback interfaces, on page 81
- Configure optical safety, on page 82
- Enable attention LED, on page 84
- PSM card protection mechanism, on page 85

# Supported NCS 1000 line cards

Cisco Optical Site Manager supports configuration and management of line cards for these NCS 1000 devices.

- Cisco NCS 1014
- Cisco NCS 1010
- Cisco NCS 1004
- Cisco NCS 1001

For detailed information about the supported cards, refer to these topics:

- Cisco NCS 1014
- Cisco NCS 1010
- Cisco NCS 1004
- Cisco NCS 1001

# Open the card view

Access detailed information and manage specific line cards within a rack or chassis.

Opening a card in Cisco Optical Site Manager allows you to:

- View detailed information about the card, including its status, type, alarms, and ports.
- Access various tabs for managing the card such as Alarms, Conditions, History, Circuits, Provisioning, Maintenance, Performance, and Inventory.
- Perform card-specific maintenance and provisioning tasks, including configuring ports, circuits, thresholds, and optical parameters.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to open a card:

**Procedure**

**Step 1** Click **Topology**.

The **Topology View** page appears.

**Step 2** Right-click the card from the rack view and select **Open Card**.

Alternatively, you can double-click the card to open the card view.

The card opens and displays its details in the right panel.

The right panel displays these tabs, which provide access to various management functions.

| Tab | Description |
|---|---|
| **Alarms** | Lists current alarms (Critical, Major, Minor) for the card or node and updates them in real time. |
| **Conditions** | Displays a list of standing conditions on the card or node. |
| **History** | Provides a history of alarms including date, type, severity, and object. |
| **Provisioning** | Provides configuration options for the card or node, depending on the card type (for example, line thresholds or optics). |
| **Maintenance** | Performs maintenance tasks specific to the card or node. |

# NCS 1000 line card modes

Use this information to identify supported Cisco NCS 1000 line card modes and related Cisco Optical Site Manager configuration requirements.

These tables summarize the card mode feature additions for NCS 1000 and related cards across recent releases.

***Table 15: Features introduced in R25.3.1***

| Feature Name | Release Information | Description |
|---|---|---|

*Table 16: Features introduced in R25.1.1*

*Table 17: Features introduced in R24.3.1*

| Feature Name | Release Information | Description |
|---|---|---|
| Additional Card Mode and Trunk Rates for the NCS1K4-OTN-XP Card | Cisco IOS XR Release 24.3.1 | The **Select Card Mode** page of the **Card Configuration Wizard** is updated to include the **1.2T Splitted** configuration on the **Trunk 0** port.<br>You can also use the wizard to configure these trunk rates in the muxponder mode:<br>• 100-GE client traffic for 600-G and 1000-G<br>• 500-G and 900-G |
| Support for NCS 1004 Card and Card Modes | Cisco IOS XR Release 24.3.1 | The **Card Configuration Wizard** now supports configuring these card modes for NCS1K4-OTN-XP cards:<br>• 10G-GREY-MXP<br>• 40x10G-4x100G-MXP<br>You can also use the wizard to configure card mode for the NCS1K4-2-QDD-C-K9 card. |

*Table 18: Features introduced in R24.1.1*

| Feature Name | Release Information | Description |
|---|---|---|
| Card Configuration Wizard Enhancements | Cisco IOS XR Release 24.1.1 | The **Card Configuration Wizard** is updated to select the **MXP-1K** muxponder mode supported by the new NCS1K14-2.4T-X-K9 card. |

You can use the add card mode feature in Cisco Optical Site Manager to configure NCS 1000 line cards. The configuration performed through the Card Configuration Wizard in Cisco Optical Site Manager allows you to:

- Select the card mode for NCS 1000 line cards
- Set trunk and client data rates tailored to your network requirements.
- Add internal patch cords by specifying ports and chassis details to establish virtual links.
- Configure trunk details including administrative state, frequency, baud rate, bits per symbol, and rate.
- Verify all configuration details in a recap window before applying the settings to ensure accuracy.

# Configuring card modes

You can configure NCS 1000 line cards in various operational modes, such as Muxponder and Slice configurations. These modes determine how the line card processes data and manages traffic, enabling efficient client-to-trunk mapping.

### Summary

The process is performed using the **Card Configuration Wizard** within Cisco Optical Site Manager. Card Configuration Wizard guides you through selecting the card mode, setting trunk and client data rates, adding internal patch cords, configuring trunk details, and verifying the configuration.

### Workflow

Perform these tasks to add a card mode using the **Card Configuration Wizard** in Cisco Optical Site Manager:

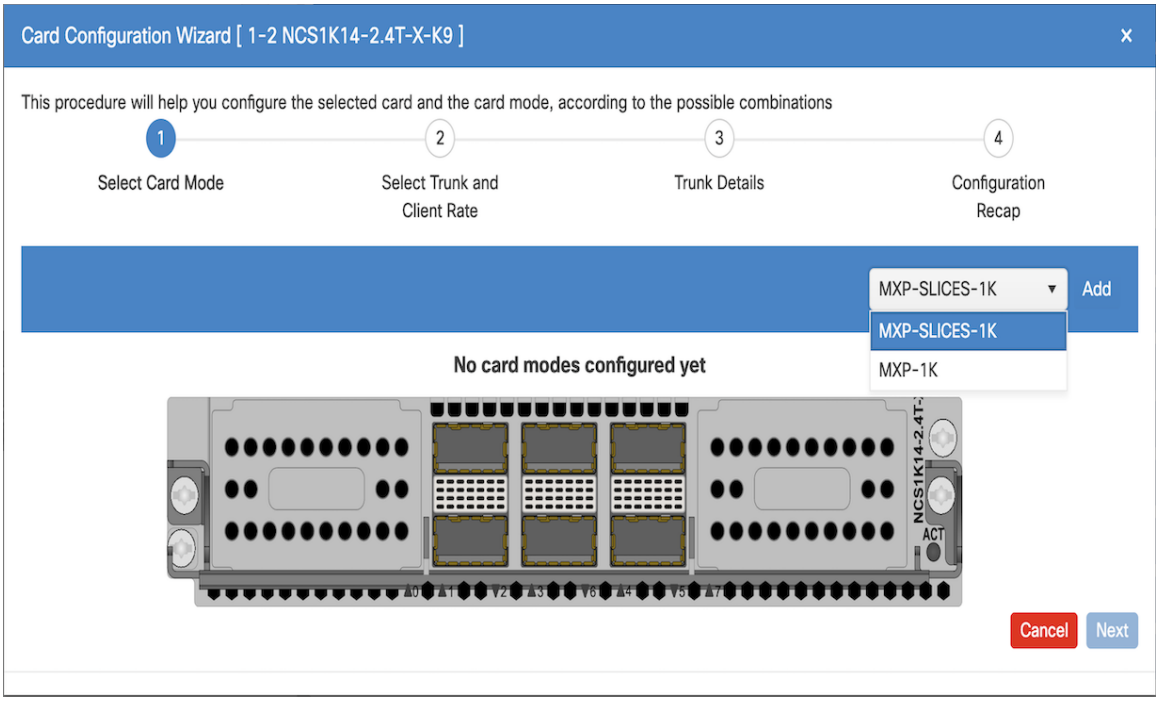
1. Select a card mode, on page 57
2. Select trunk and client data rate, on page 59
3. Add Internal Patch Cords, on page 60

   The Internal PC page is available only when the optical type is configured as ROADM.
4. Add trunk details, on page 62
5. Verify configuration details, on page 63

## Select a card mode

The **Select Card Mode** in the Cisco Optical Site Manager **Card Configuration Wizard** allows you to choose from various card modes available for a line card.

*Figure 11: Select card mode*




**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to enter into the **Card Configuration Wizard** and select a card mode.

## Procedure

**Step 1** Open the **Card Configuration Wizard** in any of these ways.

| From rack or card view | From the tabbed view |
|---|---|
| **a.** Right-click a line card.<br>**b.** Click **Card Mode**.<br>**c.** Select **Install**. | **a.** Click the **Provisioning** tab.<br>**b.** Click the **Card Modes** section to expand it.<br>**c.** Click the **Add Card mode** button. |

**Step 2** Select the card mode from the drop-down list and click **Add**.

*Table 19: Supported card modes*

| For details on card modes for | refer to |
|---|---|
| NCS 1014 | Configuring the Card Mode on NCS 1014 Line Cards |
| NCS 1004 | Configuring the Card Mode on NCS 1004 Line Cards |

**Note**
When configuring the MXP-4x100G-TXP-400G or 10G-Grey-MXP operation modes on an OTN-XP card using Cisco Optical Site Manager without defining associated slice, trunk, or client configurations, the mode is effectively applied to both Cisco Optical Site Manager and Cisco IOS XR. However, if you later remove this mode from Cisco Optical Site Manager, it is deleted from the Cisco Optical Site Manager interface but remains in the Cisco IOS XR configuration, causing a synchronization mismatch between Cisco Optical Site Manager and the device.

When these operation modes are configured with their required slice, trunk, and client settings, the deletion process correctly removes the configuration from both Cisco Optical Site Manager and Cisco IOS XR. To maintain configuration integrity and prevent orphaned settings on your device, always include the necessary slice, trunk, and client configurations when setting these operation modes in Cisco Optical Site Manager.

**Step 3** Click **Next**.

The card mode is added

### What to do next

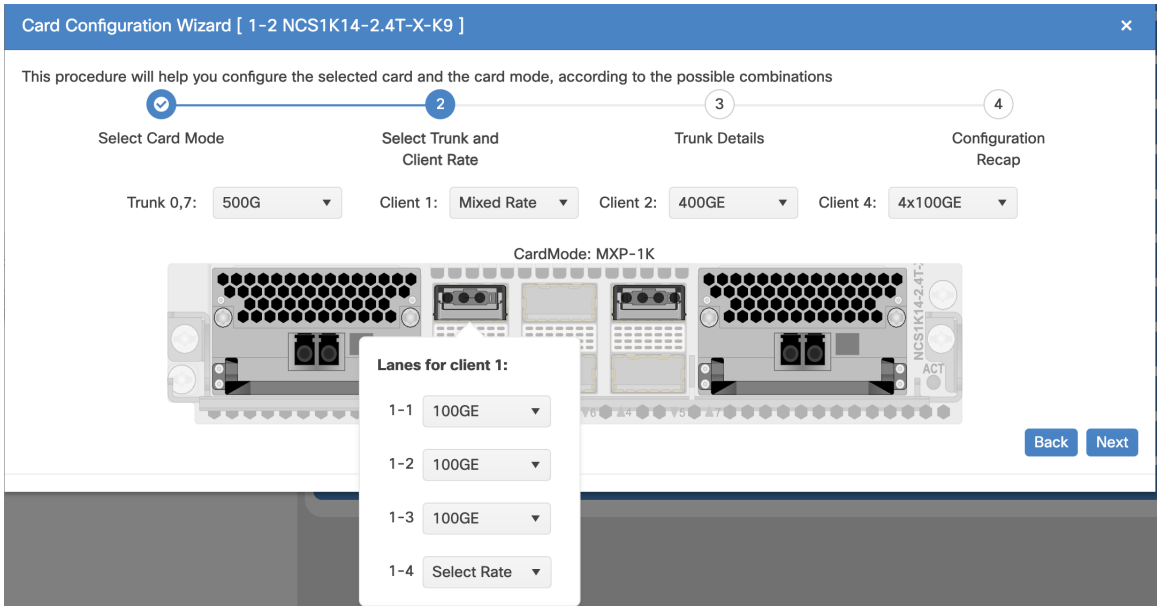
Select the Trunk and Client Data Rates.

## Select trunk and client data rate

Use this task to select the trunk and client data rates for a card mode configured on an NCS 1000 line card. This step defines how the line card processes data and manages traffic efficiently.

This configuration helps you map client traffic to trunk ports and supports various card modes, including Muxponder and Slice configurations.

***Figure 12: Select Trunk and Client Data Rate***




### Before you begin

Select a card mode, on page 57

Follow these steps to select the trunk and client port data rates in the **Card Configuration Wizard**.

### Procedure

**Step 1** Select the trunk data rate from the **Trunk** drop-down list.
The **Client** drop-down lists are displayed.

**Step 2** Select the client data rates using one of these ways:

***Table 20: Client data rate options***

| For mixed client data rate for client ports | For same client data rate for all client ports |
|---|---|
| From the **Client** drop-down lists, select the same data rate for each client port. | **a.** From the **Client** drop-down lists, select **Mixed Rate**.<br>**Mixed rate configuration** information message is displayed.<br>**b.** Close the message box.<br>**c.** Right-click the lane in the line card image and select the data rate from the available drop-down lists. |

**Step 3** Click **Next**.

The system configures the trunk and client data rates for the selected card mode and maps client traffic as specified.

### What to do next

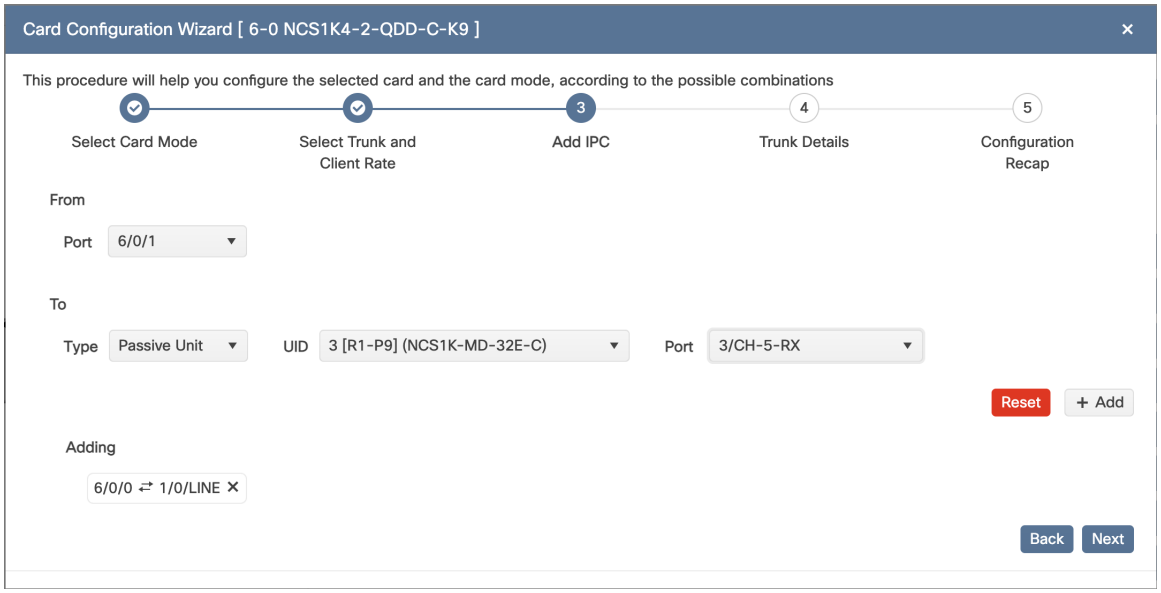
| If optical type is | then |
|---|---|
| *txp* | Add trunk details, on page 62 |
| *roadm* | Add Internal Patch Cords, on page 60 |

## Add Internal Patch Cords

You add Internal Patch Cords to establish internal connections that optimize data flow to enable efficient client-to-trunk mapping. IPC links trunk and client ports across line cards. They are necessary when the optical type is set to ROADM.

This task involves creating IPC that are virtual links between network termination points, such as OSC ports, transponder or muxponder trunk ports, line ports, and passive device ports within the node.

*Figure 13: Add IPC*




**Before you begin**

Select trunk and client data rate, on page 59

Follow these steps to add IPC in the **Card Configuration Wizard**.

**Note** **Add IPC** page is only available if optical type is configured as *roadm*.

## Procedure

**Step 1** Select the port from the **Port** drop-down list in the **From** section.

**Step 2** In the **To** section, perform these steps:

Use this table to choose the correct option based on your need:

*Table 21: IPC drop-down lists displayed based on device type*

| To create an IPC for a | Select an option from these drop-down lists |
|---|---|
| • Chassis<br>• Passive Chassis | • UID<br>• Slot<br>• Port |
| Passive Unit | • UID<br>• Port |

**Step 3** Click the **Add** button.

**Step 4** (Optional) Remove the internal patch cord using one of these methods:

- To remove a single internal patch cord, click the cross (x) icon next to the internal patch cord under the **Adding** section.
- To remove all added internal patch cords, click the **Reset** button.

**Step 5** Click **Next**.

The IPC are added and displayed.

### What to do next

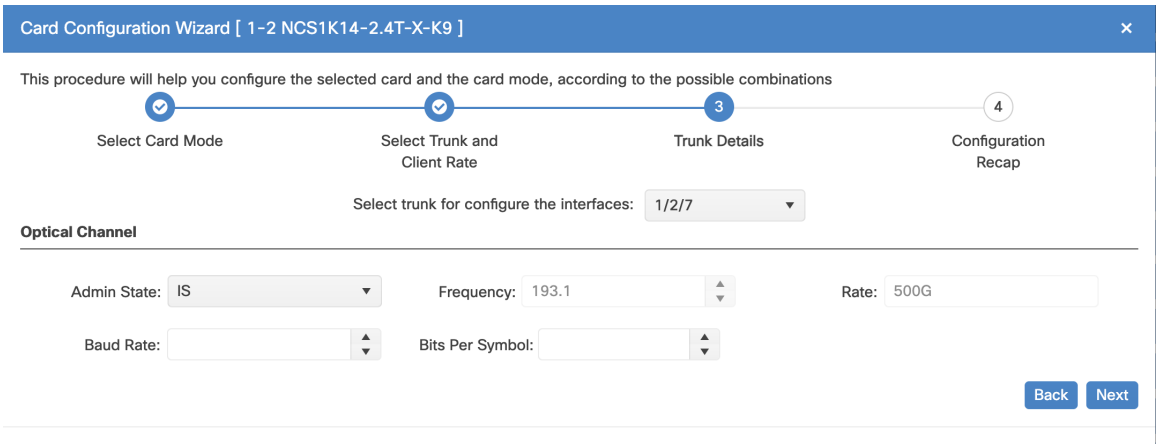
Add the Trunk Details to configure the interfaces.

## Add trunk details

Add trunk details to specify trunk interface parameters. These parameters help establish trunk connections, enabling efficient data transport and client-to-trunk mapping.

You can configure trunk port details using the **Card Configuration Wizard** for line cards by selecting parameters such as admin state, frequency, application code, baud rate, bits per symbol, and rate.

***Figure 14: Add Trunk Details***




### Before you begin

| If optical type is configured as | then ensure |
|---|---|
| *roadm* | Add Internal Patch Cords, on page 60 |
| *txp* | Select trunk and client data rate, on page 59 |

Follow these steps to add the trunk details in the **Card Configuration Wizard** to configure the interfaces.

### Procedure

**Step 1** Select the trunk port from the **Select trunk for configure the interfaces** drop-down list.

**Step 2** Select these parameters from their corresponding drop-down lists in the **Optical Channel** section:

- **Admin State**
- **Frequency**
- **Baud Rate**

  **Note**
  Cisco Optical Site Manager displays the Baud Rate value with seven digits after the decimal point.

- **Bits Per Symbol**
- **Rate**

**Step 3** Click **Next**.

The trunk details are configured.

### What to do next

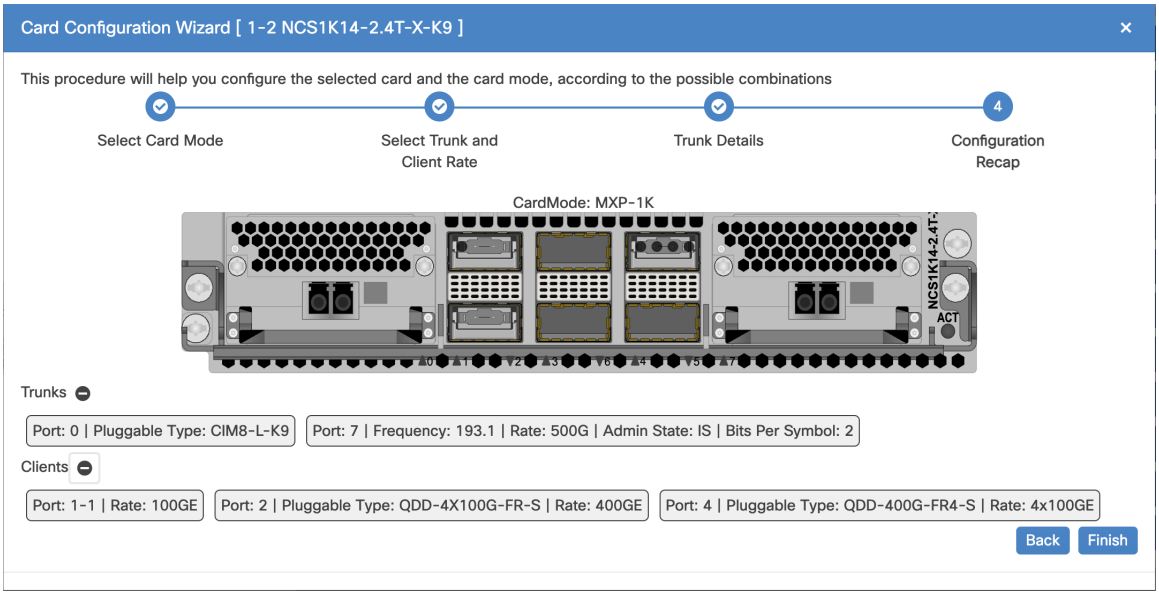
Verify configuration details, on page 63

## Verify configuration details

After you add a card mode, verify configuration details to ensure that all selected settings, such as trunk and client configurations, are correct and consistent before adding the card mode.

In the **Card Configuration Wizard**, verify the configuration in the **Configuration Recap** window for the **Trunk** and **Client** sections.

*Figure 15: Verify Configuration Details*




**Before you begin**

Add trunk details, on page 62

Follow these steps to verify the card mode configuration details.

**Procedure**

**Step 1** Click to expand the *Trunk* and *Client* sections to verify the configured details.

**Step 2** Click **Finish** to add the card mode.

Verifying the configuration details ensures that the card mode is added with the correct parameters.

# Edit card mode for NCS 1000 cards

Edit the card mode for NCS 1000 line cards to update the line card configuration to reflect the new trunk and client data rates.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to edit the trunk and client port data rates for a card mode configured on a for a NCS 1000 line card.

### Procedure

**Step 1** Open the **Card Configuration Wizard** in any of these ways.

| From rack or card view | From the tabbed view |
|---|---|
| **a.** Right-click a line card.<br>**b.** Click **Card Mode**.<br>**c.** Select **Install**. | **a.** Click the **Provisioning** tab.<br>**b.** Click the **Card Modes** section to expand it.<br>**c.** Click the **Add Card mode** button. |

**Step 2** Select the trunk and client data rates.

For more details about selecting trunk and client data rates, see Select trunk and client data rate, on page 59.

The updated trunk and client details are displayed in the **Card Modes** section of the **Provisioning** tab.

# Reset a line card

Reset a line card to recover from operational issues or to reinitialize the card.

- Choose a soft reset when you need to reboot the line card and reload software without removing power or disrupting traffic on active or standby control cards.
- Choose a hard reset when you need to remove power to clear all memory, equivalent to reseating the card, after placing the card in standby or maintenance mode to avoid traffic disruption.

This task is performed from the NFV view by using the context menu on the line card in the rack.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to reset a line card.

### Procedure

**Step 1** In the NFV view, right-click the line card in the rack.

The context menu for the selected line card appears.

**Step 2** Select **Soft Reset** or **Hard Reset**.

A confirmation message appears.

**Step 3** Click **Yes** to confirm.

The system performs the selected reset operation on the line card.

The line card is reset based on the selected option (soft reset or hard reset).

# Provision trail trace monitoring

Provision trail trace monitoring to configure parameters that monitor the integrity and connectivity of optical transport paths. This is done by setting and verifying trail trace identifiers (TTI) on OTU and ODU interfaces.

Trail trace monitoring can be configured at different levels, such as Section (OTU interfaces) and Path (ODU interfaces). You can configure parameters such as transmit and expected trace strings, detection modes, and alarm propagation settings.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to configure the parameters for trail trace monitoring.

**Procedure**

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **Trail Trace Monitoring** section to expand it.

**Step 3** From the **Level** drop-down list, select any of these options:

| To | Select |
|---|---|
| List all the OTU interfaces | **Section** |
| List all the ODU interfaces | **Path** |

**Step 4** Modify required settings as listed in this table.

***Table 22: Trail Trace Identifier Settings***

| Parameter | Description | Options |
|---|---|---|
| Port | Displays the port number. | This field is not editable. |
| Legacy Tx-TTI | Set the current transmit string of the TTI. This is the string that network transmits at the beginning of a path. It helps the far-end device verify the source and integrity of the connection. | Valid values:<br>0-64 bytes |

| Parameter | Description | Options |
|---|---|---|
| Legacy Expected-TTI | Set the TTI value that the network device expects from the far end of the optical path.<br>The device continuously compares the *Legacy Rx-TTI* with this expected value to verify the integrity and correctness of the connection. | 0-64 bytes |
| Legacy Rx-TTI | Displays the trail trace identifier string that your network device receives from the remote (far-end) device over a monitored path. | This field is not editable. |
| Alarm Propagation | If a discrepancy is detected between the expected and received trace, it raises an alarm. If set to *true*, the alarm is propagated downstream to the other nodes. | Available options:<br>• true<br>• false |
| Detect Mode | Enable this mode to allow the system to automatically detect and display the trail trace identifier (TTI) received from the far end of an optical path.<br>• When this mode is enabled, the device does not compare the *Legacy Rx-TTI* to a pre-configured expected value.<br>• Instead, it simply captures and shows the actual TTI being received from the remote end. | Available options:<br>• Disabled<br>• Enabled<br>• SAPI<br>• DAPI<br>• SAPI-and-DAPI |

**Step 5** Click **Apply**.

After provisioning, the system continuously monitors the trail trace identifiers on the specified interfaces. Any mismatch between the expected and received trace strings triggers alarms.

# Provision ODU interfaces

To ensure proper operation and monitoring of the ODU layer in the optical transport network, configure the ODU settings on optical line cards. Adjust these settings to manage signal quality, set error thresholds, and control client interface behavior.

Set parameters for ODU interfaces, such as Signal Fail Bit Error Rate (SF BER), Signal Degrade Bit Error Rate (SD BER), squelch mode (which controls laser behavior on signal loss), and squelch hold-off time.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1

- Open the card view, on page 54

Follow these steps to modify the ODU settings of a card.

## Procedure

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **ODU Interfaces** section to expand it.

**Step 3** Modify required settings as described in the #unique_64 unique_64_Connect_42_ID9913, on page 68table.

*Table 23: ODU Interface Settings*

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port name. | — |
| Description | Displays the description of the port. | — |
| SF BER | Sets the signal fail (SF) bit error rate (BER). | Only 1E-5 is allowed. |
| SD BER | Sets the signal degrade (SD) bit error rate (BER). | • 1E-5<br>• 1E-6<br>• 1E-7<br>• 1E-8<br>• 1E-9 |
| Squelch Mode | When a LOS is detected on the near-end client input, the far-end client laser is turned off. It is said to be squelched.<br>Alternatively, an AIS can be invoked.<br>The OTU2-XP card supports Squelch Mode parameter when the card mode is set as Regenerator. The valid values are Squelch and AIS. When the card mode is set to Transponder or Mixed, the Squelch Mode cannot be changed and the parameter defaults to the Squelch value. | • Squelch<br>• AIS |
| SquelchHold Off Time | Sets the period in milliseconds that the client interface waits for resolution of issues on the trunk side. The client squelching starts after this period. | • Disable<br>• 50 ms<br>• 100 ms<br>• 250 ms<br>• 500 ms |

| Parameter | Description | Options |
|---|---|---|
| Service State | Displays the service state. | — |
| Rate | Displays the rate. | — |

**Step 4** Click **Apply**.

After you provision the ODU interfaces with the desired signal thresholds and squelch behavior, you can monitor and handle signal degradation or failure more effectively.

# Provision OTU interfaces

Configure OTU (Optical Transport Unit) interfaces on optical line cards to manage forward error correction, synchronization, and interoperability, as well as related settings.

Use this task to adjust OTU parameters such as HD FEC mode, interoperability with non-native equipment, synchronization support, and administrative synchronization status message settings for optimal network performance and compatibility.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to modify the OTU settings of the card.

## Procedure

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **OTU Interfaces** section to expand it.

**Step 3** Modify the required settings described in the #unique_65 unique_65_Connect_42_ID9913, on page 69 table.

***Table 24: OTU Interface Settings***

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port name. | — |
| Description | Displays the description of the port. | — |

| Parameter | Description | Options |
|---|---|---|
| HD FEC | Sets the OTN lines to forward error correction (FEC). | • DISABLE_FEC<br>• EFEC<br>• EFEC_14<br>• EFEC_17<br>• HG_FEC_20<br>• HG_FEC_7<br>• STANDARD_FEC |
| Interop Mode | Enables interoperability between line cards and other vendor interfaces. | • InteropNone<br>• InteropEnable |
| Supports Sync | (Display only) Displays the SupportsSync card parameter. If the value is true, the card functions as a NE timing reference. | • true<br>• false |
| Sync Msg In | Sets the EnableSync card parameter. Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source. | • true<br>• false |

| Parameter | Description | Options |
|---|---|---|
| Admin SSM In | Overrides the synchronization status message (SSM) and the synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, the system uses the STU value. | • G811<br>• STU<br>• G812T<br>• G812L<br>• SETS<br>• DUS<br>• PRS<br>• ST2<br>• ST3E<br>• ST3<br>• SMC<br>• ST4<br>• RES<br>• STU_SDH<br>• DUS_SDH<br>• SSM_FAILED<br>• RES_SDH<br>• TNC |
| Rate | Displays the rate. | — |
| Service State | Displays the service state. | — |

**Step 4** Click **Apply**.

The system saves your changes, and the modified OTU settings are displayed for the selected card.

# Provision Ethernet interfaces

Provision Ethernet interfaces by configuring Ethernet port parameters on a network card or device, ensuring proper operation and network integration.

Set operational parameters such as speed, duplex mode, MTU size, Forward Error Correction (FEC), Auto-Negotiation, and service state.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to provision the parameters for the Ethernet interfaces of a card.

## Procedure

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **Ethernet Interfaces** section to expand it.

**Step 3** Click the **Edit** button.

**Step 4** Modify any of the Ethernet settings as described in the Table 25: Ethernet Settings, on page 72 table.

The available parameters depend on the card mode.

**Step 5** Click **Apply**.

The system saves your changes, and the modified ethernet interface settings are displayed for the selected card.

***Table 25: Ethernet Settings***

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port number | — |
| Description | Description of the port. | — |
| Speed | Sets the expected port speed. | — |
| MTU | Sets the maximum size of the Ethernet frames that are accepted by the port. The port must be in OOS or locked state. | Numeric.<br>• Default value: 1548<br>• Valid range: 64 – 9700 |
| FEC | Sets the FEC mode. When set to On, FEC is enabled. | • NA<br>• Auto (default)<br>• On<br>• Off |
| Duplex | Sets the expected duplex capability of ports. | • Full<br>• Half |
| Mapping | Sets the mapping mode. | • CBR<br>• GFP |

| Parameter | Description | Options |
|---|---|---|
| Auto Negotiation | Enables or disables auto-negotiation on the port. | • Disabled<br>• Enabled |
| Squelch Mode | Sets the squelch mode. | • Disable<br>• Squelch<br>• LF |
| Squelch Hold Off Time | Sets the period in milliseconds that the client interface waits for resolution of issues on the trunk side. The client squelching starts after this period or local fault is sent. | • Disable<br>• 50 ms<br>• 100 ms<br>• 250 ms<br>• 500 ms |
| Service State | Displays the service status of the port. | |

# Provision optical channels

Provision Optical Channels involves configuring parameters for optical channels on network cards within DWDM (Dense Wavelength Division Multiplexing) systems. The process sets attributes, including:

- reach
- forward error correction (FEC) standards
- transmit power
- frequency
- wavelength
- chromatic dispersion thresholds
- administrative states

Use this task to establish and optimize the optical signal path for data transmission across the network. This action enables reliable, high-capacity transport of client signals over the optical infrastructure.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to configure the parameters for the optical channels on the card.

### Procedure

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **Optical Channel** section to expand it.

**Step 3** Click the **Edit** button.

**Step 4** Modify the required parameters in the Table 26: Optical Channel Settings, on page 74 table.

**Step 5** Click **Apply**.

The system saves the changes. The modified optical channel parameters are displayed for the selected card.

***Table 26: Optical Channel Settings***

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port name. | — |
| Description | Type the description of the port. | — |
| Admin State | Sets the port service state unless network conditions prevent the change. | • Unlocked (ETSI)/ IS (ANSI)<br>• Locked, disabled (ETSI)/ OOS, DSBLD (ANSI)<br>• Locked, maintenance (ETSI)/ OOS, MT (ANSI)<br>• Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI) |
| Service State | Displays the service state. | — |
| Reach | Indicates the distance from one node to another node. | • Auto Provision<br>• List of reach values |
| SD FEC | Indicates the standard FEC. | • SD_FEC_15_DE_OFF<br>• SD_FEC_15_DE_ON<br>• SD_FEC_20<br>• SD_FEC_25_DE_OFF<br>• SD_FEC_25_DE_ON<br>• SD_FEC_7 |

| Parameter | Description | Options |
|---|---|---|
| Tx Power (dBm) | Sets the Tx power on the trunk port. | The range is –10.0 to 0.25 dBm. |
| PSM Info | When enabled on a TXP or MXP trunk port that is connected to a PSM card, it allows fast switching on the cards. | • NA<br>• Enable<br>• Disable |
| Frequency (THz) | Sets the frequency in THz | - |
| Wavelength (nm) | Displays the wavelength, which is set based on the **Frequency**. | - |
| Tx Shutdown | (Display only) | • true<br>• false |
| Width (GHz) | (Display only) | - |
| CD (Working Range) High (ps/nm) | Sets the threshold for maximum chromatic dispersion. | - |
| CD (Working Range) Low (ps/nm) | Sets the threshold for minimum chromatic dispersion. | - |
| Target Power | Sets the Rx VOA target power.<br>**Note**<br>You cannot configure this parameter if **Fixed Ratio** is already configured. | • Valid range: -19 dBm to +3 dBm<br>• Default value: -2.0 dBm |
| Fixed Ratio | Sets the Rx VOA fixed ratio.<br>**Note**<br>You cannot configure this parameter if **Target Power** is already configured. | • Valid value: 0.0 dBm |
| Rate | Displays the rate. | — |

# Change Trunk Port Parameters

Adjust trunk port parameters to ensure proper configuration. You can enable or disable the port, set the frequency or wavelength, and optimize data transmission rates for network traffic and operational requirements.

Use this task to modify trunk port settings. Typically, you access these settings through management interfaces and adjust parameters such as administrative state, frequency, baud rate, and bits per symbol.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to configure the trunk port parameters.

**Procedure**

**Step 1** Right-click a trunk port in the Rack, Chassis, or Card view and click **Change Trunk Details**.
The **Change Configuration** dialog box is displayed.

**Step 2** Select the **Admin State** to change the admin status of the trunk port to *Out of Service* or *Automatic in Service*.

**Step 3** Enter or select the frequency in the **Frequency** field.

The wavelength of the trunk port is automatically selected based on the frequency configured.

**Step 4** Enter or select the **Baud Rate** or **Bits Per Symbol**.

For more details about these fields, see Table 26: Optical Channel Settings, on page 74

**Step 5** Click **Apply**.

After changing the trunk port parameters and applying the configuration, the updated settings are saved and reflected in the system's provisioning interface.

# Provision optical threshold settings

Set the limits for optical performance parameters that trigger alarms or threshold crossing alerts (TCAs). This enables proactive monitoring and management of optical signal quality when parameters exceed or fall below defined thresholds.

Provisioning optical threshold settings involves configuring threshold crossing alert values for optical parameters on network cards such as SVO, OSCM, OSC-CSM, or DWDM cards. These thresholds include these parameters:

- received/transmitted optical power
- laser bias
- chromatic dispersion
- OSNR
- polarization mode dispersion

**Note** This feature is not supported for the FX-MXP card mode of the OTN-XP card.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to set the threshold crossing alert values on the card.

### Procedure

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **Optics Thresholds** section to expand it.

**Step 3** Choose the type of threshold that you want to change, *15 Min* or *24 Hour*.

**Step 4** Click **Add Optical Threshold** button.
**New Optical Threshold** dialog box is displayed.

**Step 5** In the **New Optical Threshold** dialog box, add these details:

a) Select the **Interface** from the drop-down list.
b) Select **Granularity** from the drop-down list to set the threshold crossing alert for 15-minute or 24-hour interval.
c) Select **Location** from the drop-down list.
d) Select **Direction** from the drop-down list.
e) Select the performance monitoring type from the **PM Type** from the drop-down.
f) Select the parameter for which you want to set the threshold value from the **PM Type Extension** drop-down list.

For more details about the parameters, see Table 27: Performance Monitoring Parameters, on page 77.

g) Enter the minimum threshold value in the **Low** field and the maximum threshold value in the **High** field.

**Step 6** Click **Apply**.

After configuring and applying the optical threshold settings, the system monitors the optical parameters against these thresholds. Alarms are raised when thresholds are crossed.

***Table 27: Performance Monitoring Parameters***

| Use this parameter | to |
|---|---|
| amplifierTilt | configure the thresholds for ingress or egress amplifier tilt. |
| amplifierGain | configure the thresholds for ingress or egress amplifier gain. |
| opticalPower | configure the thresholds for total Rx or Tx power. |
| opticalPowerOSC | configure the thresholds for total Rx or Tx OSC power. |
| opticalPowerBackReflection | configure thresholds for optical power back reflection. |
| opticalPowerBackReflectionRatio | configure threshold to monitor and limit the amount of optical signal reflected back toward the transmitter. |
| Raman - 1 | configure threshold to monitor and control the performance of the first Raman amplifier, ensuring optimal signal amplification in the optical link. |

# Configure G.709 thresholds

Define limits for key OTN performance parameters that trigger alarms or threshold crossing alerts (TCAs). By establishing these limits, network operators can proactively monitor the health and quality of OTN links, detect degradations or faults early, and maintain network reliability and performance.

Provisioning G.709 thresholds involves setting performance monitoring (PM) threshold values for OTN ports compliant with the ITU-T G.709 standard. These thresholds apply to various PM parameters and can be configured for Near End or Far End monitoring. The monitoring can occur over two time intervals:

- fifteen minutes
- one day

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to provision the G.709 performance monitoring thresholds for the OTN ports.

**Procedure**

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **G.709 Thresholds** section to expand it.

**Step 3** Select the value for the G.709 PM thresholds, and click **Apply**.

For more details about the parameters, refer to the Table 28: G.709 PM Thresholds, on page 78.

After you provision the G.709 thresholds and apply the configuration, the system continuously monitors the OTN ports against these thresholds. If any parameter exceeds its configured limit, the system generates an alert.

***Table 28: G.709 PM Thresholds***

| Parameter | Description |
|---|---|
| ES (Errored Seconds) | The number of errored seconds recorded during the PM time interval. |
| SES (Severely Errored Seconds) | The number of severely errored seconds recorded during the PM time interval. |
| UAS (Unavailable Seconds) | The number of unavailable seconds recorded during the PM time interval. |
| BBE (Background Block Error) | The number of background block errors recorded during the PM time interval. |

| Parameter | Description |
|---|---|
| FC (Failure Counter ) | The number of failure counts recorded during the PM time interval. |

# Provision FEC thresholds

Define limits for Forward Error Correction (FEC) performance parameters that trigger threshold crossing alerts (TCAs) or alarms. FEC uses Reed-Solomon RS (255,239) encoding to correct and detect errors on optical links, improving signal quality and reducing the need for signal regeneration.

Provisioning FEC thresholds involves setting performance monitoring (PM) threshold values for FEC parameters on optical cards such as transponders or muxponders. These thresholds apply to key FEC metrics, such as BIT-EC and UNC-WORDS. The metrics are measured during these specified monitoring intervals:

- fifteen minutes
- one day

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to configure the FEC thresholds for the card.

**Procedure**

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **FEC Thresholds** section to expand it.

**Step 3** Select the value for the FEC PMs and click **Apply**.

You can set the FEC thresholds for fifteen minutes or one day intervals.

**Step 4** Select a performance monitoring type from the options in this table.

| PM type | Description |
|---|---|
| BIT-EC | Sets the value for bit errors corrected. |
| UNC-WORDS | Sets the value for uncorrectable words. |

The system continuously monitors the FEC parameters against these thresholds. When the number of corrected bit errors or uncorrectable words exceeds the configured limits within the selected interval, alerts are generated.

# Configure RMON thresholds

RMON thresholds establish monitoring parameters that alert network operators to abnormal conditions. These parameters help detect and resolve network issues early. As a result, network performance and reliability are maintained at optimal levels.

RMON thresholds define specific limits on network performance variables monitored by devices. These thresholds specify conditions that trigger alarms or events when network statistics exceed or fall below set values, enabling continuous observation of Ethernet ports or interfaces.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to provision the RMON thresholds on the control card.

**Procedure**

**Step 1** Click **Provisioning**, then click **RMON Thresholds**.

**Step 2** Click the + button.

The **Create RMON Threshold** dialog box appears.

**Step 3** Specify the parameters in the **Create RMON Threshold** dialog box.

For more details about the parameters, refer to Table 29: RMON threshold parameters, on page 80.

**Step 4** Click **Apply**.

Once RMON thresholds are configured, the system tracks the selected variables against the defined rising and falling limits during sampling intervals. Alarms activate when values surpass rising thresholds. They clear when values drop below falling thresholds. This process enables the system to trigger events repeatedly when thresholds are crossed.

***Table 29: RMON threshold parameters***

| Parameter | Description |
|---|---|
| Port ID | The identifier for the port that you configure the RMON threshold for. |

| Parameter | Description |
|---|---|
| Variable | The specific MIB variable to be sampled. This variable must be any of these ASN.1 primitive type:<br>• INTEGER\<br>• Counter32<br>• Counter64<br>• Gauge<br>• TimeTicks |
| Alarm Type | Indicates which threshold crossing triggers the alarm:<br>• Rising<br>• Falling<br>• Rising or Falling |
| Sampling Type | The method used to sample the variable:<br>• **Absolute**: the threshold to use the total number of occurrences, regardless of the time period<br>• **Relative**: restricts the threshold to use the number of occurrences within the user-set sample period. |
| Sampling Period | The interval in seconds over which the data is sampled and compared against the thresholds. |
| Rising Threshold | The threshold value that triggers a rising alarm event when the sampled statistic rises to or above it.<br>**Note**<br>For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1,000 collisions every 15 seconds and a problem causes 1,001 collisions in 15 seconds, the excess occurrences trigger an alarm. |
| Falling Threshold | The threshold value that triggers a falling alarm event when the sampled statistic falls to or below it. |

# Configure loopback interfaces

A loopback is a logical interface that enables testing of network ports and circuits. This helps to identify and isolate faults before live traffic is transmitted.

Loopbacks facilitate troubleshooting by confirming the operational status of interfaces, cabling, and device components. This improves network reliability and performance.

**Note** This feature is not supported for the FX-MXP card mode of the OTN-XP card.

Loopbacks test and diagnose network interfaces by routing traffic back to the source. They isolate faults in line cards or optical paths by verifying signal integrity and device programming.

**Caution** This task is traffic-affecting.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54
- Configure loopback only when the card is in maintenance service state. If you need to place trunk ports in a locked maintenance state, see Provision optical channels, on page 73.

Follow these steps to configure loopback on the card.

**Procedure**

**Step 1** Click the **Maintenance** tab.

**Step 2** Click the **Loopback** section to expand it.

**Step 3** From the **Loopback Type** drop-down list, select any of these options for each port required:

- Terminal
- Facility
- Terminal-Drop
- Facility-Drop

**Step 4** Select the admin state from the **Admin State** drop-down list.

**Step 5** Click **Apply**.

The selected port transmits traffic, which is looped back either internally or at the line interface. This setup allows you to verify signal flow and detect errors such as loss of signal or CRC errors. Loopback states are maintained in the maintenance administrative state. You can verify these states using show commands.

# Configure optical safety

Configure optical safety parameters to ensure compliance with laser safety standards. The system can automatically shut down or control laser output power during fault conditions such as fiber breaks or signal loss.

Optical safety provisioning protects optical components and personnel from hazardous laser exposure. This process includes configuring parameters for automatic laser shutdown (ALS) modes, optical safety remote

interlock (OSRI), and recovery pulse settings on various optical cards, such as line cards, amplifier cards, and service channel cards.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to configure the optical safety parameters for cards.

## Procedure

**Step 1** Click the **Maintenance** tab.

**Step 2** Click the **Optical Safety** section to expand it.

**Step 3** Modify required settings as described in the Table 30: Optical safety parameters for cards, on page 83 table.

**Step 4** Click **Apply** to save the changes.

The system monitors optical signals. When needed, it automatically activates safety mechanisms, such as ALS, to shut down laser output.

***Table 30: Optical safety parameters for cards***

| Parameter | Description | Options |
|---|---|---|
| Interface | (Display only) Displays the port name, port type, and direction. | — |
| Supported Safety | (Display only) Displays the supported safety mechanism. | • ALS for line cards and control cards.<br>• ALS-OSRI for amplifier cards. |
| ALS Mode | Automatic laser shutdown mode. ALS mode is disabled for RX ALS interfaces. | From the drop-down list, choose one of the following:<br>• ALS-Disabled—Deactivates ALS.<br>• Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired.<br>• Manual Restart |

| Parameter | Description | Options |
|---|---|---|
| OSRI | Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down.<br>**Note**<br>OSRI configuration is not supported on the transponder and muxponder cards. | From the drop-down list, choose one of the following:<br>• OSRI-OFF<br>• OSRI-ON |
| ALS Status | (Display only) ALS status of the device. | • Working<br>• Shutdown |
| Recovery Pulse Interval (Sec.) | Displays the interval between two optical power pulses. | 60 to 300 seconds. |
| Recovery Pulse Duration (Sec.) | Displays the duration of the optical power pulse that begins when an amplifier restarts. | 2 to 100 seconds |
| Manual Restart | Triggers manual restart for the ALS interface. Manual restart does not occur if Mode is set to Automatic Restart or Disabled. | — |

# Enable attention LED

The Attention LED feature helps field engineers identify specific devices—ports, line cards, chassis, or controller cards, within a network installation. Use it during maintenance or troubleshooting.

***Table 31: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Enable Attention LED on Demand | Cisco IOS XR Release 24.1.1 | You can now turn on the Attention LED by selecting *true* from the **Attention Led for** drop-down list in the **Provisioning** tab. The Attention LED is available for specific ports, chassis, line cards, and controller cards. Once turned on, it will help field engineers quickly identify the relevant device at the installation location for maintenance or troubleshooting. |

The attention LED can be enabled on specific ports, chassis, line cards, or controller cards. This feature helps with troubleshooting and maintenance because it allows field engineers to locate the device in its installed location.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to enable the attention LED:

**Procedure**

**Step 1** Click the **Provisioning** tab.

**Step 2** Click the **Attention Led** section.

**Step 3** Perform any one of these steps to turn on the attention LED:

| To turn on the attention LED of | perform these steps. |
|---|---|
| • a chassis provisioned on the rack or<br>• all the ports on a line card | Select *true* from the **Attention Led for** drop-down list, then click **Apply**. |
| a specific port of a line card | **a.** Click **Edit**.<br>**b.** Select *true* corresponding to the port you want to blink the Attention LED, then click **Apply**. |

**Step 4** Select *false* from the drop down list and click **Apply** to turn off the Attention LED for a chassis or port.

When enabled, the Attention LED flashes on the selected device or port. This makes it easier for field personnel to physically identify the equipment and reduces the time spent locating devices, improving efficiency in troubleshooting and maintenance.

# PSM card protection mechanism

PSM card protection switching is a high-availability mechanism that automatically transfers optical traffic from a primary Protection Switching Module (PSM) card to a redundant standby PSM card in the event of a failure or degradation of the active card.

- It provides automatic failover, ensuring continuous operation and minimizing service interruption.
- It enhances the overall reliability and uptime of the optical transport network.
- It is typically implemented in one-plus-one or one-to-one protection schemes to maintain optical signal integrity.

### Types of Protection Switching

The PSM card supports the following types of protection switching:

- Revertive Protection Switching: Traffic automatically returns to the working path from the protection path once the fiber issue is resolved and the Loss of Signal (LOS) alarm is cleared on the working path.
- Non-Revertive Protection Switching: Once traffic is switched to the protection path due to a signal failure, it remains on the protection path even after the failure on the working path is resolved.

# Enable the revertive protection switching

Protection switching offers a safeguard against optical fiber faults. When a failure is detected, the system automatically switches live traffic from the working path to the protection path. This process ensures uninterrupted data transmission.

Revertive switching is one of the two protection switching modes. In non-revertive mode, traffic remains on the protection path even after the working path is restored. The revertive mode includes a configurable Wait to Restore (WTR) timer that delays the switch back to the working path to ensure stability.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to enable revertive protection switching on the PSM card:

### Procedure

**Step 1** Click the **Maintenance** tab.

**Step 2** Click the **Protection** section to expand it.

**Step 3** Click the **Edit** button.
The fields in the table become editable.

**Step 4** Select **true** from the drop-down list under the **Revertive** column.

**Step 5** Specify the time in seconds under the **Wait to Restore** column.

**Wait to Restore** (WTR) is the time delay (in seconds) applied after a Loss of Signal (LOS) alarm on the working path is cleared. Once the WTR timer expires, traffic is switched back to the working path.

**Step 6** Click **Apply**.
Revertive protection switching is enabled on the card.

Revertive protection switching automatically switches traffic back to the working path after the fault is cleared and the WTR timer expires. This process minimizes service disruption and optimizes network performance.

### What to do next

-

# Configure the non-revertive protection switching

Non-revertive protection switching ensures that, once traffic is switched to the protection path due to a signal failure, it remains there even after the failure on the working path is cleared.

Non-revertive switching contrasts with revertive switching, where traffic automatically returns to the working path after fault resolution. Non-revertive mode is often used to maintain traffic on the protection path until a manual switch is performed or other conditions are met. It is also applicable in MPLS-TE path protection and EVPN configurations to control failover behavior.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to enable or disable non-revertive protection switching on a PSM card interface:

**Procedure**

**Step 1** Click the **Maintenance** tab.

**Step 2** Click the **Protection** section to expand it.

**Step 3** Select the check-box corresponding to the PSM switch and then click **Protection Switch** button. The **New Switch Command** dialog box is displayed.

**Step 4** Complete these steps to enable non-revertive switching in the **New Switch Command** dialog box:

a) Select the interface you want to lockout from the **Target Interface** drop-down list.
b) Select **Lock-Out** from the **Switch Command** drop-down list.
c) Click **Apply**.

**Step 5** Complete these steps to disable non-revertive switching:

a) Select **Release** from the **Switch Command** drop-down list.
b) Click **Apply**.

Traffic remains on the protection path after a failure is cleared. This behavior avoids potential disruptions that can result from switching paths repeatedly. When non-revertive mode is disabled, traffic reverts automatically to the original working path once it is restored.

# Perform a manual switch

A manual switch lets you transfer traffic between the working and protection paths. Typically, this switch is used during scheduled maintenance or when manual intervention is necessary.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 54

Follow these steps to perform a manual switch:

### Procedure

**Step 1** Click the **Maintenance** tab.

**Step 2** Click the **Protection** section to expand it.

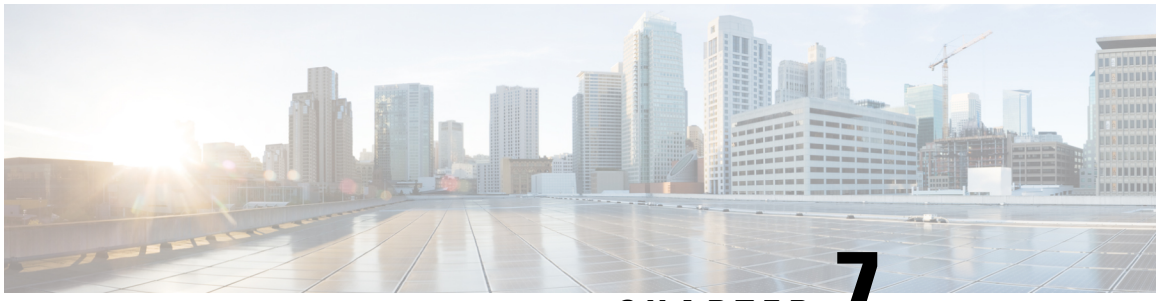
**Step 3** Select the check-box corresponding to the PSM switch and then click **Protection Switch** button.
The **New Switch Command** dialog box is displayed.

**Step 4** Select the interface you want to manually switch to from the **Target Interface** drop-down list.

**Step 5** Select **Manual-Switch** from the **Switch Command** drop-down list.

**Step 6** Click **Apply**.

The system status shows the manual switch state and confirms that the traffic is switched.



CHAPTER 7

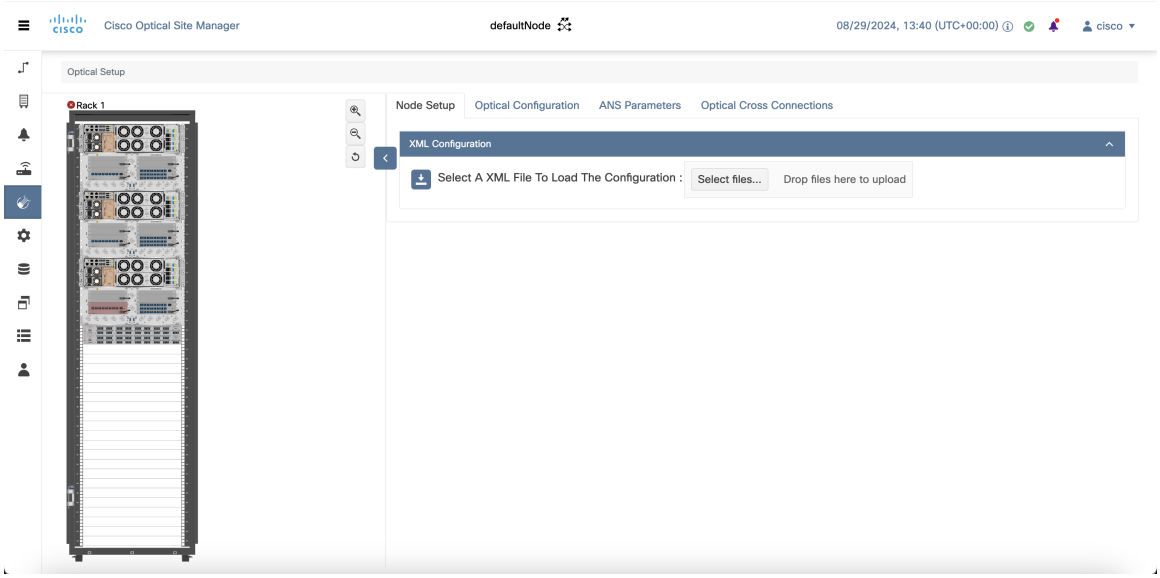
# Configure the Node

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

If Cisco Optical Site Manager is used to manage an XR device, any configuration changes made to the device using XR (CLI or NETCONF) will trigger a resynchronization of the device in Cisco Optical Site Manager. This means that Cisco Optical Site Manager will temporarily be out of sync with the device while it updates itself with the changes. Any alarms during this period will be reported on Cisco Optical Site Manager after the synchronization process is complete.

**Note** Removing any line card from the XR device will cause the configuration of the card to revert to the preconfigure state. This will result in the same behavior described above.

***Figure 16: Configure the Node***




- Import a Cisco Optical Network Planner configuration file, on page 90
- Optical Degrees, on page 91
- Internal patch cords, on page 93
- Automatic Power Control, on page 96

- Span Loss Measurement, on page 100
- Configure amplifier parameters, on page 102
- Provision interface parameters, on page 104
- Provision Raman Amplifier Parameters, on page 106
- Manage Raman Interface Parameters, on page 108
- Optical cross-connect circuits, on page 110


# Import a Cisco Optical Network Planner configuration file

Use this task to import a Cisco Optical Network Planner NETCONF file (.xml) into Cisco Optical Site Manager to configure device parameters automatically.

If you have a NETCONF file (.xml) exported from Cisco Optical Network Planner (Cisco ONP), you can import it to Cisco Optical Site Manager. This file includes:

- Node, shelf, card type, and port information, including wavelength
- Pluggable Port Module (PPM), OTN, and FEC parameters
- Degree, IPC, and link-related information
- Fiber attributes and other network parameters

**Note** While you will typically upload a Cisco ONP-generated file, there are cases where you must upload the 'golden XML' file provided to you.

***Figure 17: Upload Configuration***

### Before you begin

Ensure that:

- The NETCONF file (.xml) contains these parameters available on Cisco Optical Site Manager:
  - device name
  - uid
  - rack id
  - chassis/passive unit id
- Ensure the Cisco Optical Site Manager site name (in the CONP XML file or any other location) does not contain the string *IP*. If this string appears in the site name, network discovery in Cisco Optical Network Controller does not work correctly.
- Cisco Optical Site Manager is newly activated with no devices added to it.
- The Cisco Optical Network Planner configuration file does not include any Optical Cross-Connects.
- Log into Cisco Optical Site Manager, on page 1.

**Procedure**

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Node Setup** tab.

**Step 3** In the **Upload Configuration** section, click **Select a configuration file**.

a) Navigate to the location where the NETCONF file (.xml) is present and select it.
b) Click **Yes**.
c) Click **Upload**.
A confirmation message appears after the upload is complete.

**Step 4** Verify these configuration before adding a device:

a) Click **Optical Setup**.
b) In the **Optical Configuration** and **ANS Parameters** tabs, verify the successful configuration of CONP XML data onto the device.

**Step 5** (Optional) To download the device configuration details in an XML file, follow one of these steps:

- You can download all device configuration details in an XML file by clicking **Download Configuration**.

**Note**
We highly recommend not to directly reuse the downloaded XML file for uploading.

**Step 6** Create an authorization group for the device added through the imported XML. For details, see Create or edit an authorization group, on page 41

**Step 7** Edit the device details:

a) Click **Devices** in the left panel.
b) In the **Devices** tab, click the Devices section to expand it.
c) Select the device and update its **IP Address**, **SSH Port**, **Netconf Port**, and **Auth Group**.
d) Click **Apply**.
e) Wait until **Sync Status** shows *sync-completed*, and *alarm-synchronized*.

**Note**
You can edit the details of multiple devices before clicking Apply. However, it may take a few retries for all devices to achieve the *sync-completed*, and *alarm-synchronized* states.

# Optical Degrees

From a topological point of view, all the units that are equipped in a node belong to a side. A side can be identified by a letter, or by the ports that are physically connected to the spans. A node can be connected to a maximum of 20 different spans. Each side identifies one of the spans to which the node is connected.

## Manage Optical Degrees

Use this task to create, view, modify, or delete optical degrees in the node.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Optical Configuration** tab and then click **Optical Degrees** to expand it.

**Step 3** Perform these steps, as needed.

a) To create an optical degree, perform these steps:

1. Click the + button.

   The **Create Optical Degree** dialog box appears.

2. Select the **Degree**, **Line In**, and **Line Out**, values from their respective drop-down lists.
3. (Optional) Enter a description in the **Description** field.
4. Click **Apply**.

b) To modify any one of the optical degree parameters described below degree, perform the following step as needed:

- To modify the span validation of an optical degree, select a value from the drop-down list in the **Span Validation** column and click **Apply**.
- Go to the related cell in the **Channel Spacing** column, select 50 or 100 from the drop-down list, and click **Apply**
- Go to the related cell in the **Spectrum Occupancy** column, enter a valid value, and click **Apply**.

c) To delete an optical degree, perform these steps:

1. Check the check box corresponding to the optical degree you want to delete.
2. Click the - button to delete the selected optical degree.

   A confirmation message appears.

3. Click **Yes**.

   The optical degree is deleted from the table.

**Step 4** (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

**Note** You can only create a maximum of 20 optical degrees. The optical degree is created and added to the table that displays the following information.

- **Degree**—Specifies the optical span of the side.

- **Description**—Specifies the description as entered while creating the optical degree.
- **Line In**—Specifies line in settings.
- **Line Out**—Specifies line out settings.
- **Connected-to (IP/Degree)**—Specifies the IP address and the optical degree of the remote Cisco Optical Site Manager instance that is connected on the other side of the span.
- **Span Validation**—Specifies whether the span can be used by the GMPLS algorithm for channel routing and validation. Values are True or False.
- **Channel Grid**—Specifies the type of grid. Values are Flexible-Grid or Fixed-Grid.
- **Channel Spacing**—Specifies the minimum frequency spacing between two adjacent channels in the optical grid. Values are 100 or 50 GHz.
- **Spectrum Occupancy**—Specifies a percentage of the spectral density (the ratio of the C-band used by the carrier versus the total bandwidth). The valid range is 50% to 91%.
- **Domain Type**—Specifies the algorithm that is active on the span. By default, LOGO is displayed.

# Internal patch cords

Virtual links can be created between network termination points using Internal Patch Cords (IPC). These termination points include OSC ports, transponder or muxponder trunk ports, line ports, and passive device ports.

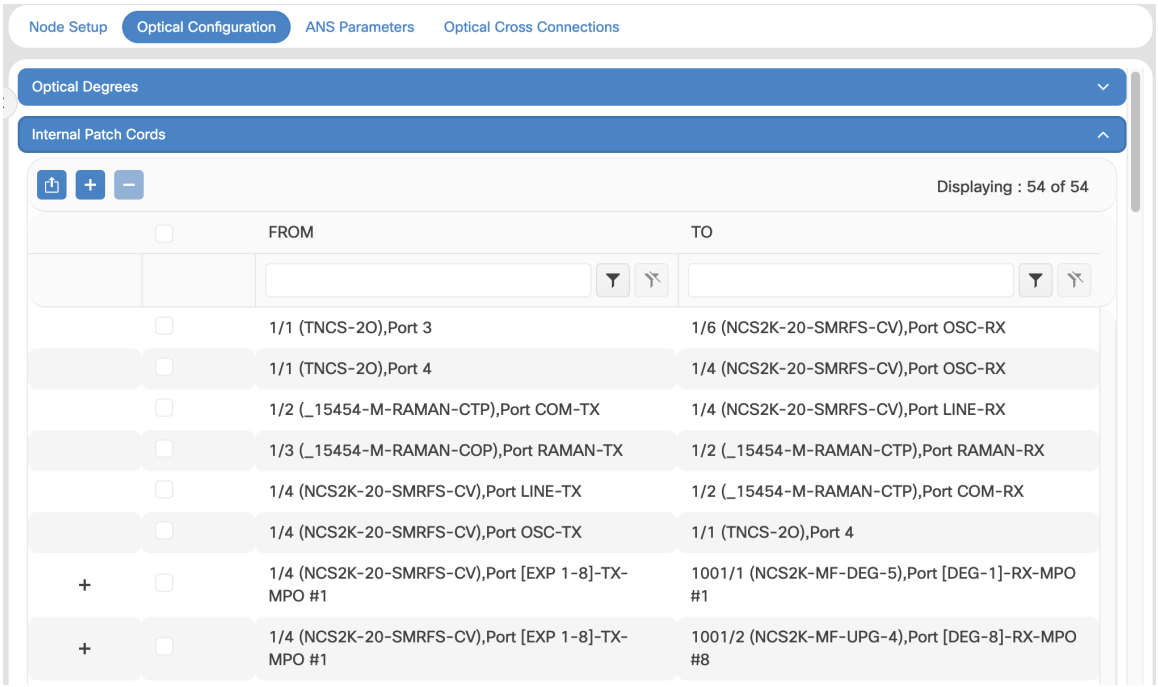
### Additional information

## Create internal patch cords

Use this task to create internal patch cords.

Use this task to create, modify, view, or delete internal patch cords in the node.

*Figure 18: Internal Patch Cords*




**Before you begin**

Log into Cisco Optical Site Manager, on page 1

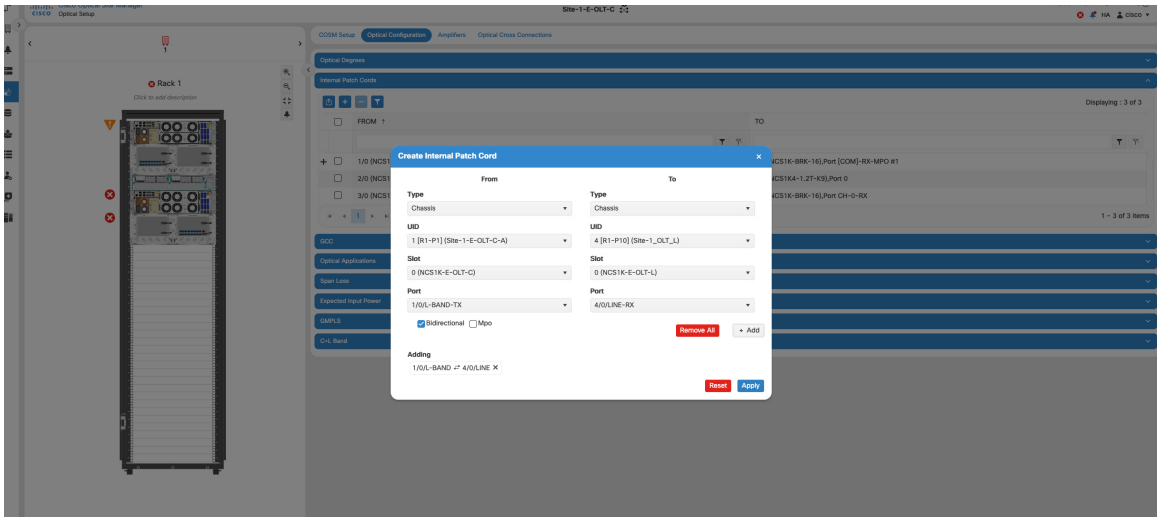
Follow these steps to create internal patch cords.

## Procedure

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Optical Configuration** tab and then click **Internal Patch Cords** to expand it.

**Step 3** Click the + button.
The **Create Internal Patch Cord** dialog box appears. It displays the **From** and **To** columns indicating the two termination points.




**Step 4** Perform the following steps for the **From** and **To** columns:

a) Select the patch cord type from the **Type** drop-down lists in the **From** and **To** columns.

Available options are *Chassis*, *Passive Chassis*, and *Passive Unit*.

The **UID** drop-down is displayed.

b) Select the unique ID of the device from the **UID** drop-down list
The **Port** drop-down is displayed.

c) Select the **Bidirectional** or **MPO** check box for the **From** column.

If you want to make the patch cord bidirectional, select the **Bi-directional** check box.

d) Select the slot from the **Slot** type drop-down list for the **To** column.

If the selected UID in the previous step is a *Passive Unit*, the **Slot** field is not displayed.

e) Click the **Add** button to add the selected Internal Patch Cord options to the **Adding** list.

f) (Optional) Click **Reset** to remove all added internal patch cords from the **Adding** list.

**Step 5** Click **Apply**.
The internal patch cord is created and added to the table that displays the following information:

- **From**-Specifies the location from where the connection originates.
- **To**-Specifies the location where the connection terminates.
- **Type**-Specifies the type of internal patch cord. Possible values are Transport and Add-Drop.

**Step 6** (Optional) Select the check boxes corresponding to the internal patch cords you want to delete and click the - button.

**Step 7** (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

**Note** You can view the internal patch cords and detailed information about cards and ports from the Map and Detailed views.

# Automatic Power Control

The Automatic Power Control (APC) feature performs the following functions:

- Maintains constant per-channel power increases optical network resilience, even when changes to the number of channels occur.
- Compensates for the degradation of optical networks caused by aging effects.
- Simplifies installation and upgrades of DWDM optical networks by automatically calculating amplifier setpoints.

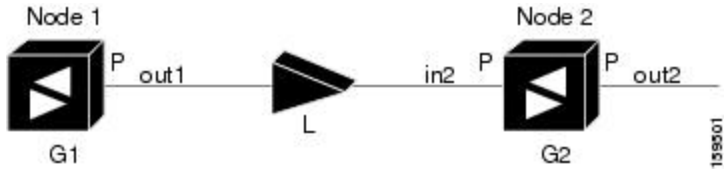
The amplifier software uses a control gain loop to keep channel power constant regardless of the number of channels. It monitors input power changes and adjusts output power proportionately. The shelf controller software emulates the control output power loop to compensate for fiber degradation.

For proper functioning, the control card needs to know the channel distribution via a signaling protocol, and the expected per-channel power which you can set. It compares actual amplifier output power with expected power and adjusts setpoints if needed.

## APC at the Shelf Controller Layer

Amplifiers are managed through software to monitor changes in the input power. Changes in the network characteristics have an impact on the amplifier input power. Changes in the input power are compensated for by only modifying the original calculated gain, because input power changes imply changes in the span loss. As a consequence, the gain to span loss established at the amplifier start-up is no longer satisfied, as shown in the following figure.

***Figure 19: Using Amplifier Gain Adjustment to Compensate for System Degradation***




In the preceding figure, Node 1 and Node 2 are equipped with booster amplifiers and preamplifiers. The input power received at the preamplifier on Node 2 (Pin2) depends on the total power launched by the booster amplifier on Node1, Pout1(n) (where n is the number of channels), and the effect of the span attenuation (L) between the two nodes. Span loss changes due to aging fiber and components or changes in operating conditions. The power into Node 2 is given by the following formula:

Pin2 = LPout1(n)

The phase gain of the preamplifier on Node 2 (GPre-2) is set during provisioning to compensate for the span loss so that the Node 2 preamplifier output power (Pout-Pre-2) is equal to the original transmitted power, as represented in the following formula:

Pout-Pre-2 = L x GPre-2 x Pout1(n)

In cases of system degradation, the power received at Node 2 decreases due to the change of span insertion loss (from L to L'). As a consequence of the preamplifier gain control working mode, the Node 2 preamplifier output power (Pout-Pre-2) also decreases. The goal of APC at the shelf controller layer is simply to detect if an amplifier output change is needed because of changes in the number of channels or to other factors. If

factors other than the "changes in the number of channels" factor occur, APC provisions a new gain at the Node 2 preamplifier (GPre-2') to compensate for the new span loss, as shown in the formula:

GPre-2' = GPre-2 (L/ L') = GPre-2 + [Pout-Pre-2 –Exp(Pout-Pre-2)]

Generalizing on the preceding relationship, APC is able to compensate for system degradation by adjusting working amplifier gain or variable optical attenuation (VOA) and to eliminate the difference between the power value read by the photodiodes and the expected power value. The expected power values are calculated using:

- Provisioned per channel power value
- Channel distribution (the number of express, add, and drop channels in the node)
- ASE estimation

Channel distribution is determined by the sum of the provisioned and failed channels. Information about provisioned wavelengths is sent to APC on the applicable nodes during the circuit creation. Information about failed channels is collected through a signaling protocol that monitors alarms on ports in the applicable nodes and distributes that information to all the other nodes in the network.

ASE calculations purify the noise from the power level that is reported from the photodiode. Each amplifier can compensate for its own noise, but cascaded amplifiers cannot compensate for ASE generated by preceding nodes. The ASE effect increases when the number of channels decreases; therefore, a correction factor must be calculated in each amplifier of the ring to compensate for ASE build-up.

APC is a network-level feature that is distributed among different nodes. An APC domain is a set of nodes that are regulated by the same instance of APC at the network level. An APC domain optically identifies a network portion that can be independently regulated. Every domain is terminated by two node sides residing on a terminal node, ROADM node, hub node, line termination meshed node, or an XC termination meshed node. An optical network can be divided into several different domains, with the following characteristics:

- Every domain is terminated by two node sides. The node sides terminating domains are:
  - Terminal node (any type)
  - ROADM node
  - Hub node
  - Cross-connect (XC) termination mesh node
  - Line termination mesh node
- APC domains are shown in the GUI.

Inside a domain, the APC algorithm designates a primary node that is responsible for starting APC hourly or every time a new circuit is provisioned or removed. Every time the primary node signals APC to start, gain and VOA setpoints are evaluated on all nodes in the network. If corrections are needed in different nodes, they are always performed sequentially following the optical paths starting from the primary node.

APC corrects the power level only if the variation exceeds the hysteresis thresholds of +/– 0.5 dB. Any power level fluctuation within the threshold range is skipped because it is considered negligible. Because APC is designed to follow slow time events, it skips corrections greater than 3 dB. This is the typical total aging margin that is provisioned during the network design phase. After you provision the first channel or the amplifiers are turned up for the first time, APC does not apply the 3-dB rule. In this case, APC corrects all the power differences to turn up the node.

To avoid large power fluctuations, APC adjusts power levels incrementally. The maximum power correction is +/– 0.5 dB. This is applied to each iteration until the optimal power level is reached. For example, a gain deviation of 2 dB is corrected in four steps. Each of the four steps requires a complete APC check on every node in the APC domain. APC can correct up to a maximum of 3 dB on an hourly basis. If degradation occurs over a longer time period, APC compensates for it by using all margins that you provision during installation.

APC can be manually disabled. In addition, APC automatically disables itself when:

- A Hardware Fail (HF) alarm is raised by any card in any of the domain nodes.
- A Mismatch Equipment Alarm (MEA) is raised by any card in any of the domain nodes.
- An Improper Removal (IMPROPRMVL) alarm is raised by any card in any of the domain nodes.
- Gain Degrade (GAIN-HDEG), Power Degrade (OPWR-HDEG), and Power Fail (PWR-FAIL) alarms are raised by the output port of any amplifier card in any of the domain nodes.
- A VOA degrade or fail alarm is raised by any of the cards in any of the domain nodes.
- The signaling protocol detects that one of the APC instances in any of the domain nodes is no longer reachable.

APC raises the following minor, non-service-affecting alarms:

- APC Out of Range—APC cannot assign a new setpoint for a parameter that is allocated to a port because the new setpoint exceeds the parameter range.
- APC Correction Skipped—APC skipped a correction to one parameter allocated to a port because the difference between the expected and current values exceeds the +/– 3-dB security range.

# APC at the Amplifier Card Level

In constant gain mode, the amplifier power out control loop performs the following input and output power calculations, where G represents the gain and t represents time.

- Pout (t) = G * Pin (t) (mW)
- Pout (t) = G + Pin (t) (dB)

In a power-equalized optical system, the input power scales with the number of channels, and the amplifier software adjusts for power fluctuations caused by changes in the incoming signal's channel count.

The amplifier software detects input power changes at two instances, t1 and t2, as traffic fluctuations occur. In the formula, 'm' and 'n' denote distinct channel numbers, and Pin/ch signifies the input power per channel.

- Pin (t1)= nPin/ch
- Pin (t2) = mPin/ch

The output power is quickly adjusted in response to input power changes, maintaining constant power for each channel, even during upgrades or fiber cuts, with a reaction time in milliseconds.

The power and mode for each channel are determined by Automatic Node Setup (ANS) on a per-degree basis during provisioning.

# Forcing Power Correction

A wrong use of maintenance procedures can lead the system to raise the APC Correction Skipped alarm. The APC Correction Skipped alarm strongly limits network management (for example, a new circuit cannot be converted into In-Service (IS) state).

The **Force Power Correction** button in the **APC** section helps the user to restore normal conditions by clearing the APC Correction Skipped alarm. The use of the **Force Power Correction** button must be supervised by Cisco TAC to prevent any traffic loss.

# Enable APC

Use this task to enable APC.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Optical Configuration** tab and then click **APC** to expand it.
A list of degrees is displayed.

**Step 3** Select the check box corresponding to the degree you want to enable APC and click the **Edit** button.

**Step 4** Select **automatic-enabled** from the **Admin Status** drop-down list.

Only degrees with Admin Status as force-disabled can be enabled.

**Step 5** Click **Apply**.

**Step 6** Verify that the **Service Status** field changes to enabled.

# Disable APC

Use this task to disable APC.

**Caution** When APC is disabled, aging compensation is not applied and circuits cannot be activated. Disable APC only to perform specific troubleshooting or node provisioning tasks. When the tasks are completed, enable and run APC. Leaving APC disabled can cause traffic loss.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

**Procedure**

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Optical Configuration** tab and then click **APC** to expand it.
A list of degrees is displayed.

**Step 3** Select the check box corresponding to the degree you want to enable APC and click the **Edit** button.

**Step 4** Select **force-disabled** from the **Admin Status** drop-down list.

Only degrees with Admin Status as automatic-enabled can be disabled.

**Step 5** Click **Apply**.

**Step 6** Verify that the **Service Status** field changes to force-disabled.

# Span Loss Measurement

Span loss measurements (in dB) check the span loss and are useful whenever changes to the network occur.

The span loss operational parameters are:

- **Measured By**—Displays whether the span loss is measured by the channel or Optical Service Channel (OSC). If a channel is not configured, the span loss is measured by the OSC. An EDFA measures the span loss based on circuits.
- **Measured Span Loss**—Displays the measured span loss.
- **Measured Span Loss Accuracy**—Displays the accuracy of the span loss measurement. For example, if the measured span loss is 20 dB and the displayed accuracy value is 2.5, the actual span loss could either be 19 or 21 dB.
- **Measured Time**—Displays the time and date when the last span loss measured value is changed.

If there is a new network with Cisco Optical Site Manager, the operational parameters list of span loss has two rows. The first row displays the OSC-measured span loss details. After the channel is configured, the second row is added, which displays the channel-measured span loss details. After the channel is configured, only the channel-measured span loss details are updated.

## View or modify span loss parameters

Use this task to measure span loss and update the minimum and maximum expected span loss values for an optical span.

Span loss parameters help monitor optical span performance and detect conditions where measured loss exceeds expected thresholds.

If a channel or OSC is not configured, span loss measurement is not reported and the operational parameters list is empty.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to view or modify span loss parameters.

## Procedure

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Optical Configuration** tab, and then click **Span Loss** to expand it.

**Step 3** Click the + icon next to a degree to expand it.

**Step 4** Select a row and click **Measure Span Loss**.

A message appears.

Click **OK**.

**Step 5** Click **Retrieve** to view updated values.

The measured span loss, accuracy, and measurement time are updated.

**Step 6** Enter values for **Min. Exp. Span Loss** or **Max. Exp. Span Loss** in dB.

The valid range is from 0 to 99 dB.

**Step 7** Click **Apply**.

A confirmation message appears.

**Step 8** Click **Yes**.

The span loss range is extended to include the accuracy value.

A *Span Loss Out of Range* condition is raised when the measured span loss exceeds the extended range.

**Step 9** (Optional) Click **Export to Excel** to export the data.

The **Span Loss Measured Data** section displays the following information:

| Field | Description |
|---|---|
| **Degree** | Displays the side for which span loss information is shown. |
| **Measured By** | Indicates whether the measurement was executed using OSC or channels. |
| **Min. Exp. Span Loss (dB)** | Displays the minimum expected span loss value. |
| **Max. Exp. Span Loss (dB)** | Displays the maximum expected span loss value. |
| **Measured Span Loss (dB)** | Displays the measured span loss value. |
| **Measured Accuracy (dB)** | Displays the accuracy of the span loss measurement.<br>For example, if the measured span loss is 20 dB and the accuracy value shown is 2.5, the actual span loss may range approximately from 19 dB to 21 dB. |

| Field | Description |
|---|---|
| **Measured Time** | Displays the date and time of the last span loss measurement. |

# Configure amplifier parameters

Set the optical amplifier settings for cards. This includes selecting the amplifier working mode (such as Channel Power or Fixed Gain), setting gain values, tilt, power setpoints, and other parameters to optimize the amplifier's performance and maintain signal quality across the optical network.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 29

Follow these steps to configure the optical amplifier parameters.

**Procedure**

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Provisioning** tab and then click **Amplifier** to expand it.

**Step 3** Click the **Edit** button to enable editing of the parameters.

**Step 4** Modify any of these settings.

For more details about the parameters, see the Parameters for amplifier cards table.

**Step 5** Click **Apply** to save the changes.

The **Amplifier** section displays the following details:

***Table 32: Parameters for amplifier cards***

| Parameter | Description | Displayed Values |
|---|---|---|
| Port | (Display only) Displays the port number, port type, and direction (TX or RX). | — |
| Total Output Power (dBm) | (Display only) Shows the current power level for each port. | — |
| Output Power Setpoint (dBm) | Shows the output power setpoint. | — |
| Working Mode | Select the working mode. | • Total Power<br>• Optimized<br>• Start and Hold |

| Parameter | Description | Displayed Values |
|---|---|---|
| Role | Role of the amplifier. | • Preamplifier<br>• Booster |
| Actual Gain (dB) | Actual gain setpoint. | — |
| Target Gain (dB) | Target gain setpoint. | — |
| Tilt Setpoint (dB) | Target output tilt requested by the user. | — |
| PSD Optimized (dBm/GHz) | Optimized PSD | — |
| Gain Setpoint (dB) | Target amplifier gain requested by the user. | — |
| Gain Range | Sets the gain range of the amplifier. | • Gain Range 1<br>• Gain Range 2<br>• No Gain Range |
| Power Degrade Threshold (High) (dBm/GHz) | Shows the current value of the optical power degrade high threshold. | — |
| Power Degrade Threshold (Low) (dBm/GHz) | Shows the current value of the optical power degrade low threshold. | — |
| Status | Shows the current status of the amplifier. | — |
| Gain Degrade High (dB) | (Display only) Shows the current value of the gain degrade high threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode.<br>Gain Degrade High refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up. | — |

| Parameter | Description | Displayed Values |
|---|---|---|
| Gain Degrade Low (dB) | (Display only) Shows the current value of the gain degrade low threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode.<br>Gain Degrade Low refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up. | — |
| Max OSC Power Delta | The maximum allowable deviation or change in the optical power level of the OSC before an alarm or warning is triggered. | — |

# Provision interface parameters

Use this task to provision or modify interface parameters. This supports operational requirements for enabling, disabling, or tuning optical interfaces as needed.

- Change administrative state, set optical thresholds, and adjust interface-related parameters for RX or TX ports.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 29

Follow these steps to provision interface parameters:

**Procedure**

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **ANS Parameters** tab and then click **Interface** to expand it.

**Step 3** Modify the required settings in the interface table. This table describes each parameter and its options.

***Table 33: Interface Options***

| Parameter | Description | Options |
|---|---|---|
| Port | Displays the port number, port type, and direction (RX or TX). | All RX and TX ports (Display only) |

| Parameter | Description | Options |
|---|---|---|
| Admin State | Sets the administrative state of the port. | • Unlocked / IS<br>• Locked, disabled / OOS, DSBLD<br>• Locked, maintenance / OOS, MT<br>• Unlocked, automaticInService / IS, AINS |
| Service State | Displays the autonomously generated state that gives the port's overall condition (display only). States appear as: Primary State-Primary State Qualifier, Secondary State. | • IS-NR / Unlocked-enabled<br>• OOS-AU, AINS / Unlocked-disabled, automaticInService<br>• OOS-MA, DSBLD / Locked-enabled, disabled<br>• OOS-MA, MT / Locked-enabled, maintenance |
| Optical Power (dBm) | Displays the optical power for each port (display only). | — |
| OSC Power (dBm) | Displays the service-channel power level for each port (display only). | — |
| Optical PSD Setpoint (dBm/GHz) | Target output Power Spectral Density requested by the user. | -50 to 10 |
| Attenuator Value (dB) | Sets the attenuator value. | — |
| Optical Power Threshold Low (dBm) | Fail low threshold used to detect the LOS alarm on the port. | — |
| OSC Power Threshold Low (dBm) | Displays the OSC power level for each port (display only). | — |
| Current Power Degrade High (dBm) | Shows the current value of the optical power degrade high threshold configured in the card (display only). Power Degrade High refers to the Signal Output Power value and is automatically calculated. | — |

| Parameter | Description | Options |
|---|---|---|
| Current Power Degrade Low (dBm) | Shows the current value of the optical power degrade low threshold configured in the card (display only). Power Degrade Low refers to the Signal Output Power value and is automatically calculated. | — |
| Current Power Failure Low (dBm) | Shows the optical power failure low threshold for the port (display only). | — |

**Step 4** Click **Apply** to save the changes.

**Note**
For passive modules, the **Service State** is displayed as **IS-NR** by default.

The specified ANS interface parameters are provisioned as required.

### What to do next

Verify the state and alarms of the affected ports after making changes. Adjust further as required to ensure stable operation.

# Provision Raman Amplifier Parameters

Use this task to provision the optical Raman amplifier parameters.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 29

### Procedure

**Step 1** Click **Optical Setup** in the left panel.
**Step 2** Click the **ANS Parameters** tab and then click **Raman Amplifier** to expand it.
**Step 3** Modify any of the settings described in the following table.

*Table 34: Raman Amplifier Parameters for Amplifier Cards*

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port number, port type, and direction (TX or RX). | — |
| Status | Displays the Status of the port. | |
| Gain Setpoint (dB) | Target amplifier gain requested by the user. | — |
| Actual Gain (dB) | (Display only) Displays the actual amplifier gain. | — |
| Pumping Scheme | (Display only) Displays the pumping scheme that the card uses. | • Counter-Propagating for the RAMAN-CTP, RMN-CTP-CL, EDRA-1-xx, and EDRA-2-xx cards.<br>• Co-Propagating for the RAMAN-COP card. |
| Calibration Type | Calibration type that the card uses.<br>The RAMAN-COP card supports only manual calibration. The RAMAN-CTP card supports both automatic and manual calibration. The RMN-CTP-CL card supports only automatic calibration. If a node has both RAMAN-CTP and RAMAN-COP cards, the RAMAN-CTP card supports only manual calibration. | • Automatic<br>• Manual<br>• No-Calibration |
| Unsaturated Gain Setpoint (dBm) | Unsaturated target amplifier gain. This field is editable only for the RAMAN-COP card. | 0–50 |

**Step 4** Click **Apply** to save the changes.
The RAMAN port section is displayed.

**Step 5** Expand the RAMAN port to view the pump power details.

*Table 35: RAMAN Pump Power Parameters*

| Parameter | Description |
|---|---|
| Pump ID | (Display only) Identifier of the Raman Pump (2 pumps with RAMAN-CTP and 4 pumps with EDRA). |

| Parameter | Description |
|---|---|
| Pump Power Setpoint (mW) | (Only for RAMAN-CTP and RAMAN-COP cards) Provisioned value of pump power setpoint. This value is effective only for manual calibration of RAMAN-CTP and RAMAN-COP cards and if the calibration is not performed. The value of this parameter must also be provided for automatic calibration of the RAMAN-CTP card even if the value is not effective. |
| Pump Power Target (mW) | (Display only) Target power set by the internal control algorithm. The result of calibration can be both automatic and manual. |
| Pump Power (mW) | (Display only) Actual power value of the individual pump. |

**Step 6** Click **Apply** to save the changes.

# Manage Raman Interface Parameters

Use this task to manage the Raman interface parameters.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 29

### Procedure

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **ANS Parameters** tab and then click **Raman Interface** to expand it.

**Step 3** View the settings described in the following table. Only the Admin State parameter can be modified.

*Table 36: Interface Options*

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port number, port type, and direction (RX or TX) | All the RX and TX ports |

| Parameter | Description | Options |
|---|---|---|
| Admin State | Sets the administrative state of the port. | From the drop-down list, choose one of the following:<br>• Unlocked (ETSI)/ IS (ANSI)<br>• Locked, disabled (ETSI)/OOS, DSBLD (ANSI)<br>• Locked, maintenance (ETSI)/OOS, MT (ANSI)<br>• Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI) |
| Service State | (Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State. | • IS-NR/<br>Unlocked-enabled<br>• OOS-AU,AINS/<br>Unlocked-disabled, automaticInService<br>• OOS-MA,DSBLD/<br>Locked-enabled,disabled<br>• OOS-MA,MT/<br>Locked-enabled,maintenance |
| Optical Power (mW) | (Display only) Displays the optical power for each port. | — |
| Current Optical Power Setpoint (mW) | (Display only) Shows the current value of the optical power setpoint that must be reached. | — |
| Current Power Degrade High (mW) | (Display only) Shows that the current value of the optical power degrade high threshold.<br>Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card. | — |

| Parameter | Description | Options |
|---|---|---|
| Current Power Degrade Low (mW) | (Display only) Shows that the current value of the optical power degrade high threshold configured in the card.<br>Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card. | — |
| Current Power Failure Low (mW) | (Display only) Shows the optical power failure low threshold for the port. | — |

**Step 4** Click **Apply** to save the changes.

# Optical cross-connect circuits

An Optical Cross-Connect (OXC) circuit is a bidirectional optical connection that links two optical nodes over a specified C-band wavelength within a DWDM system.

- Defined and instantiated using data models.
- Operates on C-band wavelengths.
- Provides bidirectional connectivity between optical nodes through DWDM elements.

### OXC Circuit and administrative states

An OXC circuit establishes an optical path through DWDM network elements and provides a wavelength-based bidirectional connection between two interface ports.

The connection is formed through these optical components:

- Wavelength selective switches (WSS)
- Multiplexers and demultiplexers
- Add/drop cards

Typical signal flow for an OXC circuit:

1. Enters the DWDM system from the source interface port.
2. Traverses DWDM network elements (WSS, mux/demux, add/drop).
3. Exits the DWDM system toward the destination interface port.

This table describes the administrative states of an OXC circuit.

*Table 37: OXC Administrative States*

| State | Operational Status | Description |
|---|---|---|
| IS/Unlocked | In Service | The circuit is active and unlocked. |
| IS, AINS/Unlocked | Automatic In Service | The circuit automatically transitions to an in-service state. |
| OOS, DSBLD/Locked | Out of Service | The circuit is disabled and locked. |

**Important** Cisco Optical Site Manager operates with native IOS XR NETCONF (CLI) data models. Configurations performed using OpenConfig (OC) models are incompatible with IOS XR native models. Do not use OpenConfig models to configure devices that are intended to be managed by Cisco Optical Site Manager.

**Note** Administrative state changes affect circuit availability but do not change the physical optical path.

### Optical cross-connections management in Cisco Optical Site Manager

- If a device already has optical cross-connections configured, they are imported into Cisco Optical Site Manager (COSM) the first time the device is synchronized or when a degree is created on the device, whichever occurs later.
- After a device is managed by Cisco Optical Site Manager, you must create, edit, or delete OXCs only through Cisco Optical Network Controller or Cisco Optical Site Manager using NETCONF.
- Do not perform any cross-connection-related changes through the IOS XR CLI once the device is managed by Cisco Optical Site Manager.

# View Optical Cross-Connect Circuits

Use this task to view the configuration and operational details of Optical Cross-Connect (OXC) circuits that are modeled on a node. The task explains how to access OXC information, export OXC data, and synchronize OXC information with the managed device.

- Inspect OXC parameters such as central frequency, allocation width, and path endpoints.
- Export OXC details for reporting or offline review.
- Synchronize OXC data with the associated NCS device to refresh the displayed information.

OXC circuits are created using data models and provide bidirectional wavelength-based connectivity between two optical nodes in a DWDM network. This task describes how to view those OXC records in the Web UI.

The information shown on the **Optical Cross Connections** tab is primarily read-only. Some actions (for example, deletion or device synchronization) depend on your deployment and device capabilities.

- OXC entries represent modeled, bidirectional circuits mapped to C-band wavelengths.

- To refresh OXC data from the device, use the **Sync from device** action (if available for your device model).

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Ensure network connectivity to the associated NCS device if you plan to use the **Sync from device** action.

Follow these steps to view the configuration and operational details of Optical Cross-Connect circuits that are modeled on a node.

## Procedure

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Optical Cross Connections** tab.

**Step 3** Expand the cross-connect entry to view Path 1 and Path 2 details by clicking the + icon.

Click the down arrow on the right of a path to show internal path parameters.

**Step 4** Review the cross-connect summary fields displayed in the table.

The table includes the following fields for each cross-connect:

- **Connection Label**—Name of the cross-connect.
- **Type**—Type of cross-connect (bidirectional).
- **Admin Status**—Administrative state of the circuit.
- **Service Status**—Operational status of the service.
- **Central Frequency (THz)**—Spectral position of the circuit.
- **Allocation Width (GHz)**—Bandwidth occupied by the service (range: 25–300 GHz).
- **Signal Width (GHz)**—Carrier bandwidth.
- **Path 1 End-points**—Source and destination interfaces for Path 1.
- **Path 2 End-points**—Source and destination interfaces for Path 2.

To view per-path internal details, expand Path 1 or Path 2 and review these items:

- **Interface Name**—Interface identifier.
- **Optical Power**—Measured optical power.
- **Power Failure Low**—Threshold for power-failure detection.
- **Optical PSD Setpoint (dBm/GHz)**—Configured optical power spectral density setpoint (independent of circuit width).
- **Current PSD Setpoint**—Current PSD setpoint.
- **Optical Power Setpoint**—Power setpoint scaled to the circuit width.

**Step 5** (Optional) Click the **Export to Excel** button to export the displayed OXC information to an Excel file.

**Step 6** (Optional) Click the **Download OXC as XML** button to download the cross-connect details as an XML file.

**Step 7** (Optional) Click the **Sync from device** button to synchronize the OXC information with the associated device.

**Step 8** (Conditional) To remove a cross-connect, select the check box for the cross-connect and click the - button.

Note: The **Optical Cross Connections** entries are typically read-only in many deployments. Deletion is only possible when your COSM deployment and device model allow direct modification of modeled OXC records. If deletion is not available, use device-side management or a supported provisioning workflow.

The **Optical Cross Connections** tab displays a list of OXC circuits with the fields described above. Expanding an entry reveals per-path details and measured values.

### What to do next

After viewing or exporting OXC information, confirm any required follow-up actions such as device-side configuration or synchronization.

- If you synchronized from the device, verify that the displayed **Service Status** reflects the expected operational state.
- If you exported data, store the export in your documentation system as required.

# Troubleshooting incorrect OXC path endpoints

Identify when OXC discovery can map a circuit to incorrect path endpoints and select the correction method.

OXC discovery can map a circuit to incorrect path endpoints when a cross-connect is already present in IOS XR before the device is onboarded in Cisco Optical Site Manager. These colorless devices do not provide a deterministic 1:1 port mapping between the COM port and the channel ports. As a result, the discovered OXC can be associated with an incorrect channel port. This behavior applies when the OXC is extended to a colorless device such as:

- **NCS1K-BRK-24** or
- **NCS1K14-CCMD-16-C**

After onboarding the device, verify the discovered circuit endpoints against the physical topology. If the discovered endpoints are incorrect, update the endpoints by using one of these tasks:

- Update OXC endpoints by importing a configuration XML file
- Edit OXC endpoints from the COSM CLI

**Note** After correcting the endpoints, do not click the **Sync** button in the **Optical Cross Connections** tab.

## Update OXC endpoints by importing a configuration XML file

Update OXC endpoints when Cisco Optical Site Manager discovers an OXC through a colorless passive device and maps the endpoint to an incorrect passive port.

OXC discovery can map a circuit to an incorrect endpoint when the OXC is connected through a colorless passive device, such as BRK-24 or CCMD. This can occur when the passive device does not provide a 1:1 mapping between the COM port and channel ports.

After device onboarding, verify the discovered OXC endpoints against the physical topology. If the discovered endpoints are incorrect, update the endpoints in a configuration XML file and import the corrected file into Cisco Optical Site Manager.

**Before you begin**

- You are logged in to Cisco Optical Site Manager.
- You have verified the physical topology and identified the correct channel endpoints for the OXC.
- You have the **Connection Label** of the OXC that must be corrected.

Follow these steps to update OXC endpoints by importing a configuration XML file.

## Procedure

**Step 1** Click **Optical Setup** in the left panel, and then click the **Optical Cross Connections** tab.

**Step 2** Identify the OXC with the incorrect endpoint and note the value in the **Connection Label** column.

Use the physical topology to identify the correct channel endpoint that must replace the discovered COM endpoint.

**Step 3** Click the **Node Setup** tab, and then click **Download Node Configuration as XML**.

The current node configuration XML file is downloaded.

**Step 4** Open the downloaded XML file in an XML editor and search for the OXC by using the connection label.

For example, search for a connection label such as **`1001_Ch1`**.

**Step 5** Update the OXC endpoint values to match the correct channel ports for your topology.

| Replace | with |
|---|---|
| *5/2/COM-TX* | *6/CH-1-TX* |
| *5/2/COM-RX* | *6/CH-1-RX* |
| *5/2/COM-TX* | *6/CH-3-TX* |
| *5/2/COM-RX* | *6/CH-3-RX* |

**Example:**

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <nodes xmlns="http://cisco.com/yang/opt-node">
  <node>
    <id>0</id>
    <oxc xmlns="http://cisco.com/yang/optical/xconnect">
      <connection-name>1001_Ch1</connection-name>
      <oxc-type>bidirectional</oxc-type>
      <central-frequency>195.95</central-frequency>
      <allocation-width>150.0</allocation-width>
      <signal-width>150.0</signal-width>
      <path1>
```

```
        <endpoints>
          <src-if>5/3/LINE-RX</src-if>
          <dst-if>6/CH-1-TX</dst-if>
        </endpoints>
      </path1>
      <path2>
        <endpoints>
          <src-if>6/CH-1-RX</src-if>
          <dst-if>5/3/LINE-TX</dst-if>
        </endpoints>
      </path2>
    </oxc>
    <oxc xmlns="http://cisco.com/yang/optical/xconnect">
      <connection-name>1001_Ch3</connection-name>
      <oxc-type>bidirectional</oxc-type>
      <admin-state>In-Service</admin-state>
      <central-frequency>195.65</central-frequency>
      <allocation-width>150.0</allocation-width>
      <signal-width>150.0</signal-width>
      <path1>
        <endpoints>
          <src-if>5/3/LINE-RX</src-if>
          <dst-if>6/CH-3-TX</dst-if>
        </endpoints>
      </path1>
      <path2>
        <endpoints>
          <src-if>6/CH-3-RX</src-if>
          <dst-if>5/3/LINE-TX</dst-if>
        </endpoints>
      </path2>
    </oxc>
  </node>
  </nodes>
</config>
```

**Step 6** In the configuration XML file, keep only the updated OXC entries under the `<nodes>` element.

Remove unrelated OXC entries and other node configuration content before saving the file.

**Step 7** Click **Optical Setup** in the left panel, then click the **Node Setup** tab.

**Step 8** Click **Select Files**, select the corrected configuration XML file, and click **Yes** when the confirmation message appears.

**Step 9** Click **Upload**.

The upload completes with a **Done** status and the **XML file upload completed** message.

**Step 10** Click the **Optical Cross Connections** tab and verify that the corrected OXC endpoints are displayed.

Expand the OXC and review the **Path 1 End-points** and **Path 2 End-points** values.

---

The selected OXC entries use the corrected channel endpoints in Cisco Optical Site Manager.

## Edit OXC endpoints from the COSM CLI

Edit the OXC endpoint configuration directly from the Cisco Optical Site Manager CLI when a discovered OXC is associated with an incorrect passive endpoint.

OXC discovery can map a circuit to an incorrect endpoint when a colorless passive device does not provide a 1:1 mapping between the COM port and channel ports. Before you edit the OXC configuration, verify the discovered endpoints against the physical topology.

**Before you begin**

- You have identified the OXC **Connection Label** and the correct channel endpoints.
- You can lock and unlock the device from Cisco Optical Site Manager.
- You have IOS XR CLI access to the Cisco Optical Site Manager host device. If the Cisco Optical Site Manager host device uses different credentials than Cisco Optical Site Manager, you also have the Cisco Optical Site Manager username.

Follow these steps to edit OXC endpoints from the COSM CLI.

## Procedure

**Step 1** Lock the device in Cisco Optical Site Manager web-UI:

a) Click **Devices** in the left panel.
b) Select the device and click **Edit**
c) Set **Admin state** to **Locked**
d) Click **Apply**.

**Step 2** Log in to the Cisco Optical Site Manager host device using one of these steps.

| If | Then |
|---|---|
| the Cisco Optical Site Manager host device uses the same credentials that you use for Cisco Optical Site Manager. | **a.** Log in to the COSM host device using the same credentials that you use for Cisco Optical Site Manager.<br>**b.** Run the **cosm** command from the IOS XR prompt.<br>`RP/0/RP0/CPU0:ios#cosm`<br>`NODE01:cosm#` |

| If | Then |
|---|---|
| the Cisco Optical Site Manager host device uses different credentials than Cisco Optical Site Manager. | **a.** Use the **bash** command from the IOS XR prompt to reach the Linux prompt.<br>`RP/0/RP0/CPU0:ios#bash`<br>`[node0_RP0_CPU0:~]$`<br>**b.** Access the **COSM** container.<br>`[node0_RP0_CPU0:~]$ docker exec -it COSM bash`<br>`[COSM:/]$`<br>**c.** Log in to the Cisco Optical Site Manager CLI by using the **ncs_cli -C -u** command and the Cisco Optical Site Manager username.<br>`[COSM:/]$ ncs_cli -C -u cisco1`<br>`User cisco1 last logged in 2026-05-13T07:36:57.343064+00:00, to COSM, from 127.0.0.1 using cli-console`<br>`cisco1 connected from 127.0.0.1 using console on COSM`<br>`NODE01:cosm#`<br>If your deployment uses a different Cisco Optical Site Manager username, replace **`cisco1`** with that username. |

**Step 3** Run the **show running-config nodes node** command to retrieve the OXC details from the running configuration with the OXC connection label.

**Example:**

```
NODE01:cosm# show running-config nodes node 0 oxc 1001_Ch1
nodes node 0
 oxc 1001_Ch1
  oxc-type          bidirectional
  central-frequency 195.95
  allocation-width  150.0
  signal-width      150.0
  path1 endpoints src-if 5/3/LINE-RX
  path1 endpoints dst-if 5/2/COM-TX
  path2 endpoints src-if 5/2/COM-RX
  path2 endpoints dst-if 5/3/LINE-TX
 !
!
NODE01:cosm# show running-config nodes node 0 oxc 1001_Ch2
nodes node 0
 oxc 1001_Ch2
  oxc-type          bidirectional
  central-frequency 195.95
  allocation-width  150.0
  signal-width      150.0
  path1 endpoints src-if 5/1/LINE-RX
  path1 endpoints dst-if 6/CH-1-TX
  path2 endpoints src-if 6/CH-1-RX
  path2 endpoints dst-if 5/1/LINE-TX
 !
!
```

To identify the OXC label from the Cisco Optical Site Manager GUI, click **Optical Setup**, click the **Optical Cross Connections** tab, and export the OXC list to Excel.

**Step 4** Enter the configuration terminal and select the OXC that must be corrected.

**Example:**

```
NODE01:cosm# conf
Entering configuration mode terminal
NODE01:cosm(config)# nodes node 0 oxc 1001_Ch1
NODE01:cosm(config-oxc-1001_Ch1)#
```

**Step 5** Update the path endpoints to use the correct MD-32 channel ports and commit the change.

**Example:**

```
NODE01:cosm(config-oxc-1001_Ch1)# path1 endpoints dst-if 6/CH-1-TX
NODE01:cosm(config-oxc-1001_Ch1)# path2 endpoints src-if 6/CH-1-RX
NODE01:cosm(config-oxc-1001_Ch1)# commit
```

Repeat this step for each OXC that has incorrect endpoints.

**Step 6** Verify that the OXC endpoints are updated in the running configuration.

**Example:**

```
NODE01:cosm# show running-config nodes node 0 oxc 1001_Ch1
nodes node 0
 oxc 1001_Ch1
  oxc-type          bidirectional
  central-frequency 195.95
  allocation-width  150.0
  signal-width      150.0
  path1 endpoints src-if 5/3/LINE-RX
  path1 endpoints dst-if 6/CH-1-TX
  path2 endpoints src-if 6/CH-1-RX
  path2 endpoints dst-if 5/3/LINE-TX
 !
!
NODE01:cosm# show running-config nodes node 0 oxc 1001_Ch2
nodes node 0
 oxc 1001_Ch2
  oxc-type          bidirectional
  central-frequency 195.95
  allocation-width  150.0
  signal-width      150.0
  path1 endpoints src-if 5/1/LINE-RX
  path1 endpoints dst-if 6/CH-1-TX
  path2 endpoints src-if 6/CH-1-RX
  path2 endpoints dst-if 5/1/LINE-TX
 !
!
```

**Step 7** Unlock the device in Cisco Optical Site Manager and wait until synchronization is complete.

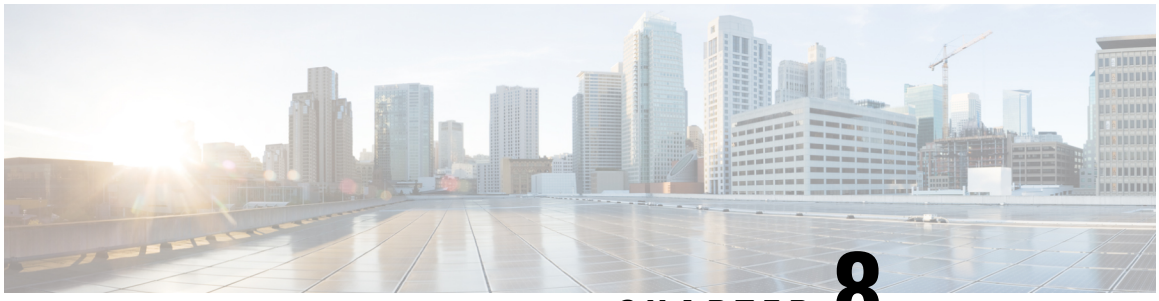
**Step 8** Verify the OXC endpoints again after the device is unlocked.

**Example:**

```
NODE01:cosm# show running-config nodes node 0 oxc 1001_Ch1
NODE01:cosm# show running-config nodes node 0 oxc 1001_Ch2
```

---

The selected OXC entries use the corrected channel endpoints in Cisco Optical Site Manager.



CHAPTER 8

# Cisco Optical Site Manager Settings

This chapter explains how to configure the Cisco Optical Site Manager timezone and node information. It also covers additional settings such as the default order of the right panel list, the opacity and width of the left panel rack, and Smart Licensing configuration tasks.


- Configure time zone and measurement units, on page 119
- Download device diagnostics, on page 120
- View Audit Logs, on page 121
- Smart licensing for Cisco Optical Site Manager, on page 122
- Configure smart licensing workflow, on page 124
- Smart transport mode, on page 125
- Smart licensing CSLU mode, on page 125
- Create a Token, on page 126
- Configure DNS to Access Cisco Optical Site Manager, on page 127
- Configure transport mode, on page 128
- Establish trust, on page 129
- Smart licensing offline mode, on page 130


# Configure time zone and measurement units

Configure the display format, time zone, measurement units, and data channel preferences in the Cisco Optical Site Manager application.

Follow these steps to configure preferences for the Cisco Optical Site Manager application.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Settings**.

**Step 2** Click the **Preferences** tab.

**Step 3** Configure the date format, time zone, channel configuration, and length unit in the **General** section.

**Step 4** Click **Apply**.

A confirmation message appears.

**Step 5** Click **Yes**.

**Step 6** Reload the browser to apply the updated settings.

# Download device diagnostics

Use this task to retrieve and download Cisco Optical Site Manager diagnostic logs for troubleshooting and support. Download a ZIP file that contains the selected COSM and device diagnostic logs.

Cisco Optical Site Manager diagnostics help you collect operational data such as alarms, audit logs, and device diagnostics, which can be shared with Cisco TAC or used for internal troubleshooting.

To avoid timeouts, retrieve only the required log types and devices.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to retrieve and download device diagnostics information.

## Procedure

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

The **Diagnostic** page appears.

**Step 2** Click the **Logs** tab.

**Step 3** To collect and download Cisco Optical Site Manager diagnostic logs, perform these steps:

a) In the **Application** section, select the check boxes for the logs that you want to retrieve.

**Note**
By default, all the check boxes are selected except **NCS Callback Log**.

*Table 38: Log types*

| Fields | Description |
|---|---|
| Alarms | Collects the active alarms. |
| Audit Logs | Collects NSO audit logs. |
| Conditions | Collects the active conditions. |
| Admin Logs | Collects the admin logs. |
| Engineer Logs | Collects all the system software logs. |
| History Logs | Collects the alarms history logs. |
| Inventory Logs | Collects the hardware inventory logs. |

| Fields | Description |
|---|---|
| NCS Callback Log | Collects information about the implementation status and return values of the entire NSO data tree. |
| Device Audit Log | Collects the audit logs for the device. |
| Device Diagnostics | Collects the diagnostic logs for the device. |

b) From the **Devices** section, select the devices for which you want to retrieve the logs.
c) Click **Retrieve**.

A confirmation message appears.

d) Click **Yes**.

Wait until the **Progress Status** indicates that the diagnostic log collection is *completed*.

e) Click **Download Diagnostic** to download the diagnostics report.

**Note**
If the diagnostic log download fails in a browser, retry the download or use an alternate browser.

A ZIP file containing the selected logs is downloaded.

# View Audit Logs

Use this task to retrieve and download Cisco Optical Site Manager audit logs.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Diagnostic** in the left panel.
The **Diagnostic** page appears.

**Step 2** Click the **Audit** tab.

**Step 3** Select the search criteria from the **Filters** section and click **Filter**.

Details of each event including the date, user type, SID and event details are displayed in a table.

# Smart licensing for Cisco Optical Site Manager

*Table 39: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| Cisco Optical Site Manager Smart Licensing | Cisco IOS XR Release 24.3.1 | Cisco Optical Site Manager now supports the smart licensing. It enables you to automate the time-consuming manual licensing tasks and allows you to easily track the status of your license and software usage trends. |

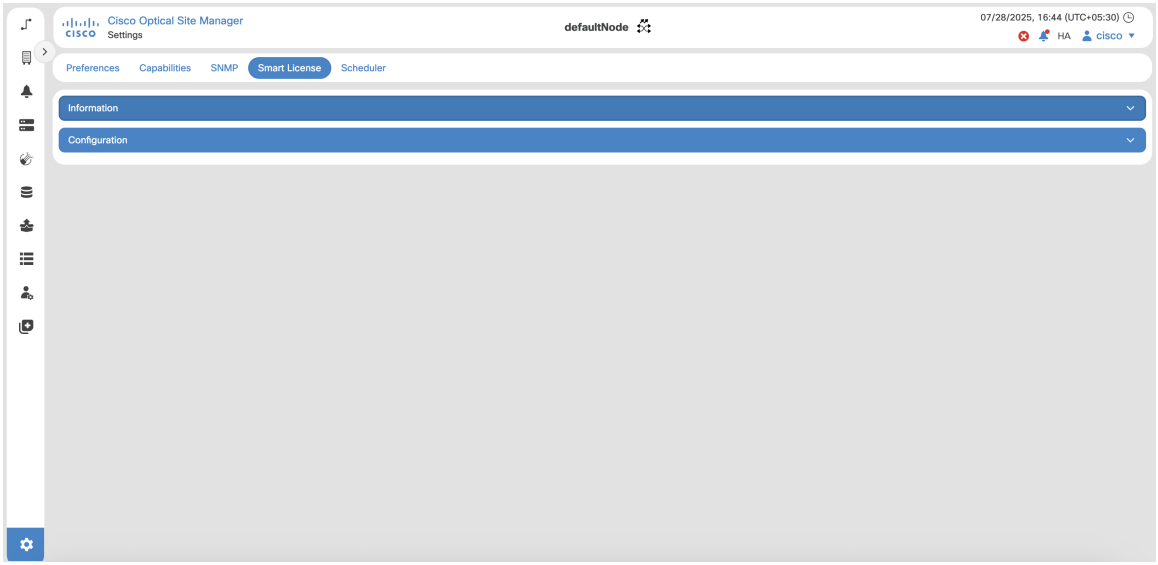
Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

### Smart licensing core functions

Smart Licensing helps you simplify three core functions:

- **Purchasing:** Register installed software without needing Product Activation Keys.
- **Management:** Automatically track license usage across your network without installing license files on each node. Create license pools to match your organizational structure. Use Cisco Smart Software Manager, a centralized portal, to manage all Cisco licenses in one place.
- **Reporting:** Access a unified view of purchased and deployed licenses through the portal. This visibility helps you make informed purchasing decisions based on actual usage.

*Figure 20: Smart Licensing*



These are the key features of Smart Licensing:

- **Direct and proxy registration**: registers Cisco Optical Site Manager application.
- **Centralized management**: manages your license inventory using CSSM, simplifying software asset tracking and management.
- **License portability**: moves or transfers your licenses easily between devices, offering flexibility in deploying software assets within the organization.
- **Simplified activation**: simplifies this process by using a pool of licenses that aren't tied to a specific device as against Traditional licensing.
- **Automatic license renewal**: renews licenses automatically, reducing the administrative burden of tracking license expiration dates and manual renewals.
- **Usage reporting**: generates detailed reports on license usage to understand device software consumption, optimizing your license investments.
- **Compliance assurance**: provides visibility into license entitlements versus actual usage, helping that you stay compliant.
- **Support for hybrid environments**: supports both on-premises and cloud-based environments, allowing for consistent license management across different deployment models.
- **Real-time updates**: receives real-time updates from Cisco, ensuring that you have access to the latest features and compliance information.

### Cisco Smart Account

Cisco Optical Site Manager integrates with Cisco Smart Accounts to simplify license management.

Smart Accounts provide a centralized, organized, and simple-to-use solution for managing Cisco software licenses across an entire organization. They act as a container that holds all Cisco software assets, allowing customers to view, store, manage, and move these assets as needed. Smart Accounts enable full visibility into license entitlements and usage, helping optimize software management. Smart Accounts support license pooling, portability, and provide compliance reporting.

When creating a Smart Account, you must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval process. See http://software.cisco.com to learn about, set up, or manage Smart Accounts.

### Cisco Smart Software Manager

Cisco Smart Software Manager enables you to manage all of your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances). Use the Cisco Smart Software Manager to do the following tasks:

- Create, manage or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove or view product instances.
- Run reports against your virtual accounts.

- Modify your email notification settings.
- View overall account information.

### Virtual accounts

Virtual Accounts are customizable subaccounts within a Smart Account used to organize and optimize Cisco licenses. They can be structured to reflect business units, product types, or geographic locations, allowing better planning and utilization of assets. They are created and maintained by the Smart Account administrator. Smart Licencing allows you to create multiple license pools or virtual accounts within the Smart Software Manager portal. Using the Virtual Accounts option you can aggregate licenses into discrete bundles associated with a cost center so that one section of an organization cannot use the licenses of another section of the organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region.

All new licenses and product instances are placed in the default virtual account in the Smart Software Manager, unless you specify a different one during the order process. Once in the default account, you may choose to transfer them to any other account as desired, provided you have the required access permissions.

Use the Smart Software Manager portal to create license pools or transfer licenses.

# Configure smart licensing workflow

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

For NCS 2000, NCS 1014, NCS 1004, and NCS 1001 the license count is based on the number of line cards available on Cisco Optical Site Manager application. Each line card consumes one license. Controller cards do not consume licenses. NCS2K-SVO-K9 or NCS 2000 SVO line cards do not consume licenses. For NCS 1010, the license count is based on the number of chassis. There are two main deployment options for Smart Licensing:

- Cisco Smart Software Manager (CSSM): Smart Licensing offers you Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website so that you do not have to install the license file on every node. You can create license pools (logical grouping of licenses) to reflect your organization structure.
- On-Premise software: You may want to operate totally offline with On-Premise software that allows you to have only this On-Premise host to do the talking for licensing information exchange with the Cisco Cloud and in turn provide information to the end devices as to their state of compliance.

Follow these tasks to configure smart licensing:

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Order your license from Cisco Commerce Workspace (CCW).

**Step 2** Access CSSM and create the smart account and virtual accounts to organize your licenses.

**Step 3** Perform any of these tasks to configure the smart licensing modes:

| To configure | Follow this workflow |
|---|---|
| Smart transport mode | Smart transport mode workflow, on page 125 |
| CSLU mode | Smart licensing CSLU mode workflow, on page 126 |
| Offline mode | Smart licensing offline mode workflow, on page 131 |

**Note**
The UNTRUSTED-APPLICATION and USAGE-NOT-REPORTED alarms are raised when Smart License is not configured. These alarms are cleared once the trust is properly established with CSSM.

**Step 4** Configure the smart license transport mode and register the device with CSSM.

For more details, see Configure transport mode, on page 128.

**Step 5** Generate your report from the device. Synchronize the report with CSSM either automatically or manually.

Monitor the license usage and compliance status through the CSSM portal.

# Smart transport mode

The Smart Transport mode is a method that enables Cisco devices to send license usage information directly over the internet to the Cisco Smart Software Manager (CSSM). Here are the benefits of this mode:

- Simplifies license usage reporting by enabling direct communication with CSSM.
- Eliminates the need for intermediate servers or manual file exchanges.
- Supports secure, automated license management suitable for connected environments.

### Smart transport mode workflow

The smart transport mode workflow involves:

- Create a Token
- Configure DNS to Access Cisco Optical Site Manager
- Configure transport mode, on page 128
- Establish trust, on page 129

# Smart licensing CSLU mode

The Cisco Smart Licensing Utility (CSLU) mode is a transport mode used in Cisco Smart Licensing to manage licenses on-premises without requiring direct device connectivity to the Cisco Smart Software Manager (CSSM). CSLU provides the following key functions:

- Collects license usage data from Cisco Optical Site Manager and acts as an intermediary between Cisco Optical Site Manager and Cisco Smart Software Manager (CSSM).
- Ideal for environments with restricted or no internet access as Cisco Optical Site Manager communicates with CSLU instead of directly connecting to CSSM.

### Smart licensing CSLU mode workflow

The smart licensing CSLU mode workflow involves:

- Configure transport mode, on page 128
- Establish trust, on page 129

# Create a Token

A token acts as a registration key that securely connects your device to your Cisco Smart Software Manager (CSSM) virtual account, establishing trust and authorization between the device and Cisco's licensing system. This enables the device to be identified and managed within your organization's smart licensing account.

### Procedure

**Step 1** Log in to the Cisco Smart Software Manager.

**Step 2** Click the **Inventory** tab, and select your virtual account from the **Virtual Account** drop-down list.

The **Create Registration Token** dialog box appears.

**Step 3** Click the **General** tab, then select **New Token**.

**Step 4** Enter the token description.

**Step 5** Specify the token's active duration in days.

**Step 6** Select the **Allow export-controlled functionality on the products registered with this token** check box.

**Step 7** Click **Create Token**.
The token ID is created and displayed.

**Step 8** Copy the token ID and register Cisco Optical Site Manager with the same token ID.

**Example:**

An example of the token ID:

```
YzY2ZjYyNjktY2NlOS00NTc4LWIxNTAtMjZkNmNiNzMxMTY1LTE2NjAzNjQ3
%0ANzY4Njl8ZVJSckxKN2pFV2tIeHVoMUkxbGxTazFDVm9kc1B5MGlHQmlFWUUi%0Ac3VNRT0%3D%0A
```

### What to do next

Configure DNS to Access Cisco Optical Site Manager.

# Configure DNS to Access Cisco Optical Site Manager

Configure the DNS for Cisco Optical Site Manager to communicate with Cisco Smart Software Manager (CSSM) and other Cisco licensing services.

**Before you begin**

- If Cisco Optical Site Manager and the DNS or proxy server are in different subnets, configure a static route for server reachability. For configuration instructions, see Configure static routes for proxy server reachability
- Create a Token

Follow these steps to configure the DNS server for Cisco Optical Site Manager from your network.

**Procedure**

**Step 1** Run the **cosm** command to enter into COSM configuration mode.

**Example:**

```
RP/0/RP0/CPU0:ios#cosm
```

**Step 2** Run the **config** command to enter into the configuration mode.

**Example:**

```
RP/0/RP0/CPU0:cosm#config
```

**Step 3** Run the **admin server-information networking dns-configuration dns-server <ipaddress>** command to configure the DNS.

**Example:**

```
RP/0/RP0/CPU0:cosm(config)#admin server-information networking dns-configuration dns-server
 10.0.1.2
```

**Step 4** Run the **Commit** and **Exit** command to commit the changes and exit the configuration mode.

**Example:**

```
commit
exit
```

This example shows how to configure DNS for Cisco Optical Site Manager:

```
RP/0/RP0/CPU0:ios#cosm
RP/0/RP0/CPU0:cosm#config
RP/0/RP0/CPU0:cosm(config)#admin server-information networking dns-configuration dns-server
 10.0.1.2
RP/0/RP0/CPU0:cosm(config)#commit
RP/0/RP0/CPU0:cosm(config)#exit
```

### What to do next

Configure transport mode

# Configure transport mode

Configure the transport mode as Smart Transport, CSLU, or Offline to send usage information directly over the internet, administer licenses and associated product instances from an on-premises environment, or manage devices on premises without connecting to CSSM.

Follow these steps to configure transport mode.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- After you restore Cisco Optical Site Manager to factory defaults, delete its registered unique identifier (UID) from Cisco Smart Software Manager before you establish trust again. A factory reset clears the trust information from Cisco Optical Site Manager but does not delete the registered UID from Cisco Smart Software Manager.

### Procedure

**Step 1** Click **Settings**

**Step 2** Click the **Smart License** tab.

**Step 3** Click the **Configuration** section to expand it.

**Step 4** Select one of these options from the **Transport Mode** drop-down list:

| Select | To configure |
|---|---|
| Smart Transport | smart transport mode that enables devices to send usage information directly over the internet to the CSSM. |
| CSLU/OnPrem | CSLU mode to administer licenses and their associated Product Instances from their premises mode. |
| Offline | offline mode that allows you to manage your devices on premises without connecting to CSSM |

**Note**
Select the transport mode before you establish trust with Cisco Smart Software Manager. To change the transport mode after trust is established, restore Cisco Optical Site Manager to factory defaults and establish trust again. Changing the transport mode without a factory reset retains the trust and unique identifier information and can cause an invalid-signature error when trust is re-established.

**Step 5** Specify the smart transport or CSLU url.

| If *Transport Mode* is | Then |
|---|---|
| Smart Transport | specify *https://smartreceiver.cisco.com/licservice/license* as **Smart Transport URL**. |
| CSLU/OnPrem | Specify *http://<Device IP>:8182/cslu/v1/pi* as **CSLU URL**. |

**Step 6** Specify the **Proxy Setting**.

**Step 7** Perform these steps under the **Reports Settings** section:

a) Specify the number of days between each time a report is generated in the **Reporting Interval (days)** field.

You can enter a value between 1 and 30 days. The default value is 5 days.

b) Select the **Send Hostname** check box to receive the hostname information in the report.

c) Select the **Send Product Version** check box to receive the product version in the report.

**Step 8** Click **Apply** to apply the settings.

**Step 9** Click **Check Connection** to check the connection.

**Note**
If the connection fails and Cisco Optical Site Manager and the DNS or proxy server are on different subnets, verify that the static route is configured correctly.

Verify the connection

| If.. | Then.. |
|---|---|
| The **Check Connection** button turns *Green*. | Connection is successfully established. |
| The **Check Connection** button turns *Yellow* | Connection could not be established. |

### What to do next

Establishing trust to access and view license usage data.

# Establish trust

Establishing trust enables secure and authorized license management between the Cisco Optical Site Manager and Cisco's licensing system.

- Creates a trusted connection by installing a trust code from a registration token, linking Cisco Optical Site Manager to the smart licensing account.
- Authorizes Cisco Optical Site Manager within Cisco's licensing system for management under the organization's smart licensing framework.
- Enables communication of license usage and status to Cisco Smart Software Manager (CSSM) for automatic tracking and compliance.

**Before you begin**

Configure transport mode

Follow these steps to establish trust between the Cisco Optical Site Manager and Cisco's licensing system.

**Procedure**

**Step 1** Click the **Information** section to expand it.

**Step 2** Click the **Establish Trust** button.

The **Establish Trust** dialog box appears.

**Step 3** Paste the token in the **ID Token** field and click **Trust**.

For more details, see Create a Token.

**Step 4** Click the **Sync** button.

**Step 5** Verify that these fields under the **Trust** panel display *Success* indicating that trust is established:

- **Trust Established**
- **Last Attempt Result**

After completing the synchronization, this status information is displayed:

| Panel | Field | Expected value | Description |
|---|---|---|---|
| Trust | **Attempt in Progress** | *True* | Whether an installation is currently running. |
| | **Last Attempt Result** | *Success* | Outcome of the last installation attempt. |
| Reporting | **Last Report Pushed** | *Timestamp* | Time when the last status report was sent. |
| | **Last Ack Received** | *Timestamp* | Time when the last acknowledgment was received. |
| License Usage | **COSM Managed Line Card License** | Number \| Status | Describes the number of licenses and their status. |

# Smart licensing offline mode

Offline mode enables you to:

- Manage your devices locally without requiring a connection to Cisco Smart Software Manager (CSSM).
- Set up and operate devices without internet access or communication with Cisco.

- Maintain device management in highly secure environments with strict security requirements.

### Smart licensing offline mode workflow



**Note** If you perform a usage report before establishing trust, the usage-file.xml generated by Cisco Optical Site Manager automatically includes a trust request. This allows you to establish trust and report usage in a single operation.

# Configure offline transport mode in Cisco Optical Site Manager

Offline transport mode allows you to manage your devices on premises without connecting to CSSM.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to configure offline transport mode.

### Procedure

**Step 1** Click **Settings**, then click the **Smart License** tab.

**Step 2** Click the **Configuration** section to expand it.

**Step 3** Select **Offline** from the **Transport Mode** drop-down list.

**Step 4** Configure the **Reports Settings**:

a) Select the **Send Hostname** check box to receive the hostname information in the report.

b) Select the **Send Product Version** check box to receive the product version in the report.

**Step 5** Click **Apply** to apply the settings.

**Check Connection** is disabled for **Offline** mode.

### What to do next

Download request file from Cisco Optical Site Manager

# Download trust request file from Cisco Optical Site Manager

Initiate the trust establishment between Cisco Optical Site Manager and CSSM in environments without internet connectivity.

Download the trust request file from Cisco Optical Site Manager. This file is then uploaded to CSSM to start the offline trust establishment process.

**Before you begin**

Configure offline transport mode

Follow these steps to download the trust-request file.

### Procedure

**Step 1** Click the **Information** tab to expand it.

**Step 2** Click the **Save** button and choose **Trust Request**.

The trust request file is downloaded.

### What to do next

Upload trust request file to CSSM

# Upload trust request file to CSSM

Upload the trust file to CSSM to validate the Cisco Optical Site Manager and licensing details offline.

**Before you begin**

Download request file from Cisco Optical Site Manager

Follow these steps to upload the trust request file to CSSM.

### Procedure

**Step 1** Click **Reports**, then click **Usage Data Files**.

**Step 2** Click **Upload Usage Data** and select the **Virtual Account**.

**Step 3** Click **Ok**.
The **Upload Usage Data** window is displayed.

**Step 4** Click the **Browse** button and upload the **trust-request** file.

**Step 5** Go to the **Reporting** Status tab and verify that the status shows **No Errors**.

- It may take a few minutes for the status to update.
- If the status shows **Errors**, fix them before continuing.

CSSM processes the uploaded file and generates an acknowledgement.

**Step 6** Click **Download** under **Acknowledgment** tab.

The acknowledgement file is downloaded.

### What to do next

Download Acknowledgement from CSSM

# Download acknowledgment from CSSM

After you upload the trust request file from Cisco Optical Site Manager to CSSM, it processes this file and generates an acknowledgment file. You then download this acknowledgment file from CSSM and import it back into Cisco Optical Site Manager.

**Before you begin**

Upload trust request file to CSSM

Follow these steps to download the acknowledgment from CSSM.

**Procedure**

**Step 1** Go to **Usage Data Files** and click **Upload Usage Data**.
The **Upload Usage Data** window is displayed.

**Step 2** Click **Browse** and select **rum-report-xxx**.

**Step 3** Click **Open**, then click **Upload Data**.
The **Select Virtual Accounts** window is displayed.

**Step 4** Select the appropriate account, then click **ok**.

- It may take a few minutes for the status to update.
- If the status shows **Errors**, fix them before continuing.

**Step 5** Click **Download** to get the acknowledgment file if no errors are reported.

The acknowledgment file is downloaded.

**What to do next**

Import acknowledgment in Cisco Optical Site Manager

# Import acknowledgment file into Cisco Optical Site Manager

After importing the acknowledgment file into Cisco Optical Site Manager, the trust relationship between Cisco Optical Site Manager and CSSM is established, enabling the configuration of offline license mode.

**Before you begin**

Download acknowledgment from CSSM

Follow these steps to the import the acknowledgment file into Cisco Optical Site Manager.

**Procedure**

**Step 1** Click the **Import** button.
The **Import Acknowledgement File** dialog is displayed.

**Step 2** Click **Select files...** and upload the acknowledgment file.

**Step 3** Click **Save**, then select **Usage**.
The **Select report type** dialog is displayed.

**Step 4** Select any of these options from the **Report type** drop-down list.

- **unreported**: to download report for unreported days.
- **all**: to download the report for all days.
- **days**: to download the report for selected number of days.

The report is downloaded.

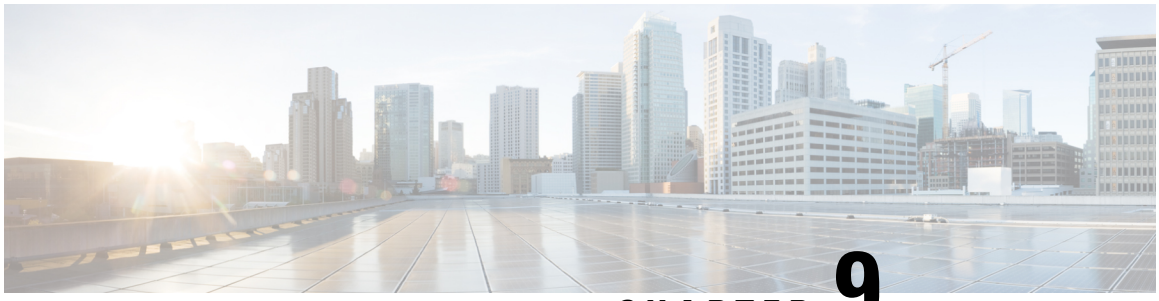
**Step 5** Click the **Refresh** button in the **Information** section to see updated details.

**Step 6** Perform these steps to verify the configuration:

a) Go to the **Trust** tab to verify that the **Trust Established Time** is displayed.
b) Go to the **Reporting** tab to verify that the **ACK Report Time** is displayed.
c) Go to the **License Usage** tab to verify that the license count is displayed.

---

The offline smart licensing mode is configured.



CHAPTER 9

# Backup and Restore Database

This chapter describes the tasks to backup and restore Cisco Optical Site Manager database.

***Table 40: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Backup and Restore Database | Cisco IOS XR Release 24.3.1 | Cisco Optical Site Manager now supports backup and restore for both its own database and the databases of the devices it manages.<br><br>When unexpected failures occur, such as hardware malfunctions or software corruption, your data is securely backed up and easily recoverable. |

*Figure 21: Back Up and Restore Database*

• Database Backup and Restore, on page 137

# Database Backup and Restore

Cisco Optical Site Manager allows the backup of its own database as well as the databases of the devices it manages, ensuring that data can be restored in case of disaster. Backup are executed and stored within the device on which Cisco Optical Site Manager is installed and are accessible through the Cisco Optical Site Manager web user interface.

## Backup and download database

Backing up the Cisco Optical Site Manager database ensures data integrity and availability in case of unexpected failures, such as hardware malfunctions or software corruption. By maintaining regular backup, administrators can quickly restore the system to its last known good state, minimizing downtime and operational disruptions.

Follow these steps to back up and download the database for both Cisco Optical Site Manager and the devices it manages.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

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

**Step 2** Click the **Backup** button.
A confirmation dialog box appears.

**Step 3** (Optional) Enable the **Stop on Error** toggle button to stop the backup process if any of the selected devices for backup are disconnected, unresponsive, or locked.

**Step 4** Click **Yes** to start the backup.

The *Logs Summary* section displays the backedup components, their status, and timestamps.

The DBBACKUP-IN-PROGRESS alarm is triggered and can be viewed in the **Alarms** tab of the **Fault Monitoring** menu.

**Step 5** Click the backup file name under **Back Up Information** to download entire backup as a ZIP file on your local system.

**Note**
If database backup download fails in a browser, the files can still be downloaded by retrying or using an alternate browser.

# Restore Database

When performing a restore operation, you restore Cisco Optical Site Manager and its managed devices database to the state it was in at the backup time. You can choose to restore only the Cisco Optical Site Manager database, only one or multiple managed devices database, or both simultaneously.

**Important** Database restoration is supported only if the device node names remain unchanged after the database is downloaded. If the node names are changed post-download, the restore operation will not succeed.

**Note** Cisco Optical Site Manager database backup does not include customer-sensitive private information, such as private keys and certificates.

- If Cisco Optical Site Manager uses self-signed certificates, the certificates are regenerated automatically after the database is restored.
- If Cisco Optical Site Manager uses customer-provided certificates, these certificates are not reinstalled during a database restore. If the certificates are missing after the restore, you will need to reinstall them. This can be done by deactivating and then activating the system, removing and recreating the container, or performing a fresh reinstallation of the same image. After these steps, reinstall the customer-provided certificates from the local certificate archive.

Use this task to restore the database of either the Cisco Optical Site Manager or the devices it manages.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

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

**Step 2** Click the **Restore current backup** button.
The **Select what do you want to restore** dialog box appears.

**Step 3** Perform any of these tasks to restore the database:

**Note**
When restoring the Cisco Optical Site Manager or full database on the host device, the Cisco Optical Site Manager becomes temporarily unavailable.

| To restore | click the *Restore* button |
|---|---|
| only Cisco Optical Site Manager database, | in the *COSM* section. |
| only the managed devices database, | in the *Devices* section after selecting the one or all check boxes corresponding to the devices for which you want to restore the data. |

| To restore | click the *Restore* button |
|---|---|
| both Cisco Optical Site Manager and the managed devices database, | in the *Full* section. |

A confirmation dialog box appears.

**Step 4** (Optional) Enable the **Stop on Error** toggle button to stop the restore process if a mismatch is detected.

A mismatch can include a difference in the number of devices between backup and restore, or situations where any of the selected devices for restore are disconnected, unresponsive, or locked.

**Step 5** Click **Yes** to start the restore process.

The *Logs Summary* section displays the restored components, their status, and timestamps.

The DBREST-IN-PROGRESS alarm is triggered and can be viewed in the **Alarms** tab of the **Fault Monitoring** menu.

# Upload Database

While multiple backups can be created, only the most recent backup is available for download and restoration. You may need to upload and restore your database in the following situations:

- **Reinstall Cisco Optical Site Manager**: If you need to reinstall Cisco Optical Site Manager, uploading the backup file allows you to restore the data to its state prior to the re-installation.
- **Database Transfer Between Nodes**: Copy the database from one device to another by backing up from the source device and uploading it on the destination device.

Use this task to upload the database from a downloaded backup ZIP file.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

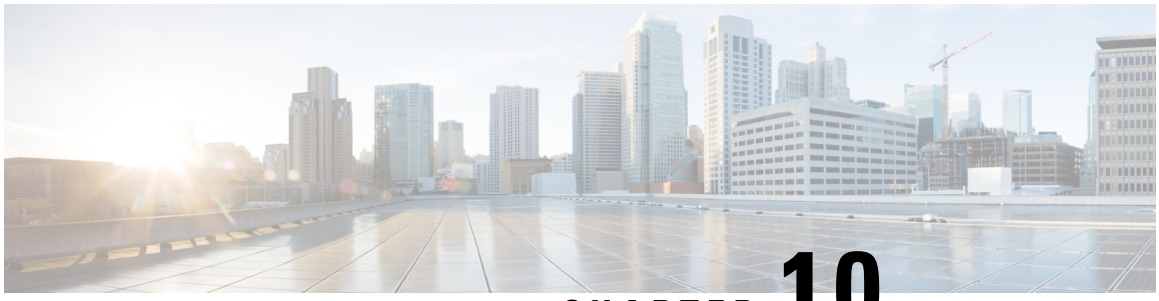
**Step 1** Click **Database** in the left panel.

**Step 2** Click the **Upload Backup** button.
The **Upload DB Backup** dialog box appears.

**Step 3** Click **Select Files** to select a ZIP file.

**Tip**
You can also drag and drop the backup ZIP file in the **Upload DB Backup** dialog box.

**Step 4** Click **Upload** to upload the backup.
The uploaded backup file is displayed under **Back Up Information**.



CHAPTER 10

# Upgrade Software

This chapter describes the software upgrade in Cisco Optical Site Manager and its related tasks.


- Cisco Optical Site Manager software packages, on page 141
- Workflow for Software Upgrade, on page 142
- Download GISO image, on page 143
- Download Software Package on Device, on page 144
- Activate NCS 1000 device software, on page 145
- Delete software package, on page 146


## Cisco Optical Site Manager software packages

***Table 41: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| SSH Upgrade | Cisco IOS XR Release 25.1.1 | The Cisco Optical Site Manager software package now includes integrated SSH libraries. When you upgrade to Release 25.1.1, these libraries are automatically incorporated into the NCS 2000 Cisco Optical Site Manager software package.<br><br>This upgrade provides new packages for these SSH libraries, enhancing security and addressing additional vulnerabilities. |

In Cisco Optical Site Manager, software package distribution is:

- Distributed as a single file containing all necessary components for system upgrades.
- Format of the file depends on the Cisco Optical Site Manager installation type.
- For line card installations, the package is provided as an ISO image file.

# Workflow for Software Upgrade

You can upgrade NCS 1000 device and Cisco Optical Site Manager application software using the Software Manager.

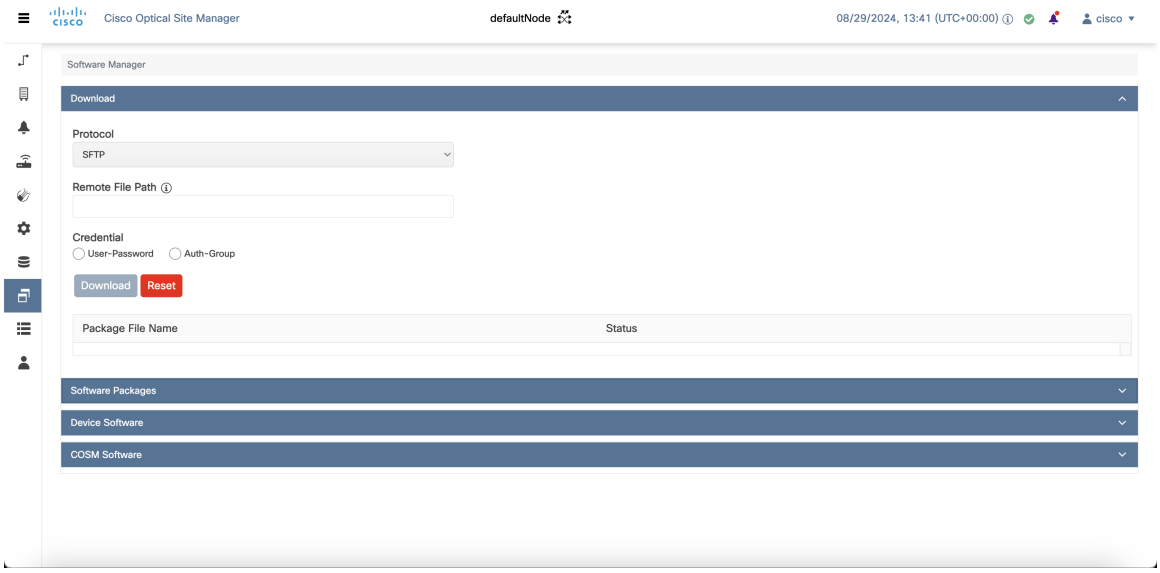
**Important** Downgrading Cisco Optical Site Manager software is not supported and should not be used as a recovery method following an upgrade.

Perform these tasks to upgrade software NCS 1000 device and Cisco Optical Site Manager application software.

1. **Download Software Package** : Download the necessary packages from the Cisco repository to the Cisco Optical Site Manager. For more details, see Download GISO image, on page 143. The downloaded packages appear in the **Software Packages** tab.
2. **Download Software Package to Device**: Download the software package from Cisco Optical Site Manager to the NCS 1000 device. For more details, see Download Software Package on Device, on page 144.
3. **Activate Device Software**: Activate the device software. For more details, see Activate NCS 1000 device software, on page 145.

**Note** If the software reports an internal error during software download or activation without identifying the cause or failure stage, collect diagnostic logs to determine the root cause.

***Figure 22: Software Upgrade***



**Note** When Cisco Optical Site Manager is upgraded from R25.1.1 to R25.4.1, trust must be re-established. See Establish Trust.

# Download GISO image

Before

Download the necessary GISO image from the Cisco repository to the Cisco Optical Site Manager.

**Note** For R25.3.1, when performing a software download on the Cisco NCS 1004 device, use a Golden ISO (GISO) image that excludes the Cisco Optical Site Manager rpm file. Including the Cisco Optical Site Manager rpm file increases the GISO size, which may exceed the available disk space and cause the software upgrade to fail.

Follow these steps to download the GISO image.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Software Manager** from the left panel.

**Step 2** Click the **Download** tab.

**Step 3** Select SFTP from the **Protocol** drop-down list.

**Step 4** Enter the path of the software package file in the **Remote File Path** field.

**Step 5** Choose to enter the credentials either through **User-Password** or **Auth-Group**.

- If you choose **User-Password**, enter the **Username** and **Password** in the given fields.
- If you choose **Auth-Group**, choose the authentication group from the **Auth Group** drop-down list.

**Step 6** Click **Download** to download the software package.

The download status is displayed in the **Status** column.

**Step 7** Click the **Refresh** icon in the **Software Packages** section.
The downloaded software package ID is displayed in the **Software Packages** list in the increasing order of their release.

The software package is downloaded and listed in the **Software Packages** section.

# Download Software Package on Device

Use this task to download the software package from the Cisco Optical Site Manager to NCS 1000 device.

### Before you begin

- Download GISO image, on page 143

### Procedure

**Step 1** Click **Software Manager** from the left panel.

**Step 2** Click the **Device Software** section.
The following describes the fields displayed in the on the **Device Software** section:

*Table 42: Device Software Fields*

| Field | Description |
|---|---|
| Name | Displays the IP address of the device. |
| Component | Displays the platform component name. |
| App Status | Displays the status of the Cisco Optical Site Manager application on the device.<br>• *Active*: Cisco Optical Site Manager is currently active on the device.<br>• *Standby*:<br>Cisco Optical Site Manager is in standby mode on the device. If the *Active* application fails, this application takes over. |
| Working SW Version | Displays the currently active software version on the device. |
| Status | Displays the progress of the download. |

**Step 3** Select the check boxes for one or more devices to download the new software.

**Note**
The **Device Software** tab lists the NCS 1000, cosm-primary, and cosm-secondary devices. Only the NCS 1000 IOS XR software package can be downloaded.

**Step 4** Click **Download**.

The **Select Software Image** dialog box appears.

**Step 5** Select the software package from the **Software Image** drop-down list.

**Step 6** Click **Download**.

The **Status** column displays the download progress.

**Step 7** (Optional) Click the **Terminate Download** button to terminate the software downloading on the selected device.

**Note**
When upgrading the software for the Cisco Optical Site Manager High Availability devices , select and upgrade all devices listed under **Device Software**.

**What to do next**

Activate NCS 1000 device software, on page 145

# Activate NCS 1000 device software

Activate the Cisco Optical Site Manager software immediately after downloading it to ensure proper operation.

To activate software on the Cisco NCS 1004 device, utilize a Golden ISO (GISO) image that does not include the Cisco Optical Site Manager rpm file. Including this file can increase the GISO size, potentially exceeding available disk space and leading to a software upgrade failure.

**Warning**

- Do not activate a base IOS XR GISO on a device that is running Cisco Optical Site Manager, as this action will remove the application.
- Do not activate a target IOS XR GISO that does not include the Cisco Optical Site Manager RPM on a device where Cisco Optical Site Manager is already installed. The target GISO must contain the Cisco Optical Site Manager, RPM; otherwise, the existing Cisco Optical Site Manager, application will be removed.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1

Follow these steps to activate the NCS 1000 device software package.

**Procedure**

**Step 1** Click **Software Manager**.

**Step 2** Click the **Device Software** section.

**Step 3** Select the NCS 1000 device for which you want to activate the software, then click **Activate**.

**Step 4** For the NCS 1000 device, select the ISO to be activated.

**Note**

If the device hosting the Cisco Optical Site Manager application is activated, manageability is temporarily lost while the new device image is loaded and the updated Cisco Optical Site Manager application restarts.

**Caution**
Do not install a base ISO without Cisco Optical Site Manager component on the device that already has Cisco Optical Site Manager. This will remove the Cisco Optical Site Manager application and leave the device in an inconsistent state.

The selected software is activated.

# Delete software package

Log into Cisco Optical Site Manager, on page 1

Follow these steps to delete the software package on the Cisco Optical Site Manager card or application.

**Procedure**

**Step 1** Click **Software Manager** from the left panel.

**Step 2** Click to expand the **Software Packages** section.

A list of package names and their corresponding software versions is displayed.

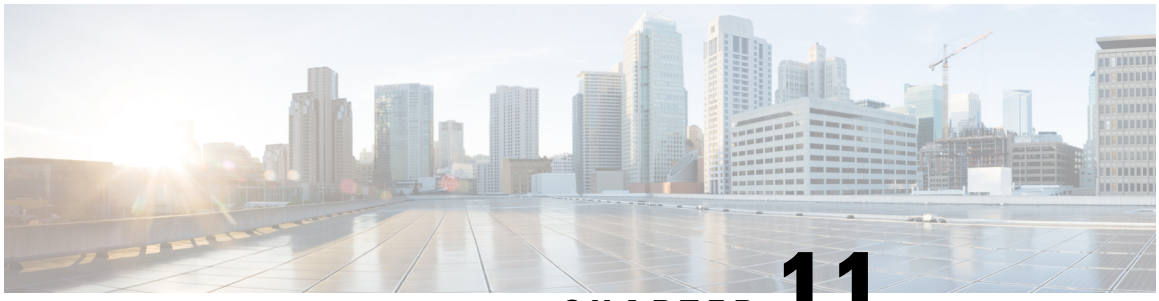
**Step 3** Select the checkbox corresponding to the *SW Package ID* of the Cisco Optical Site Manager package you want to delete.

**Step 4** Click **Delete**.

A confirmation message appears.

**Step 5** Click **Ok**.

The selected software package is deleted.

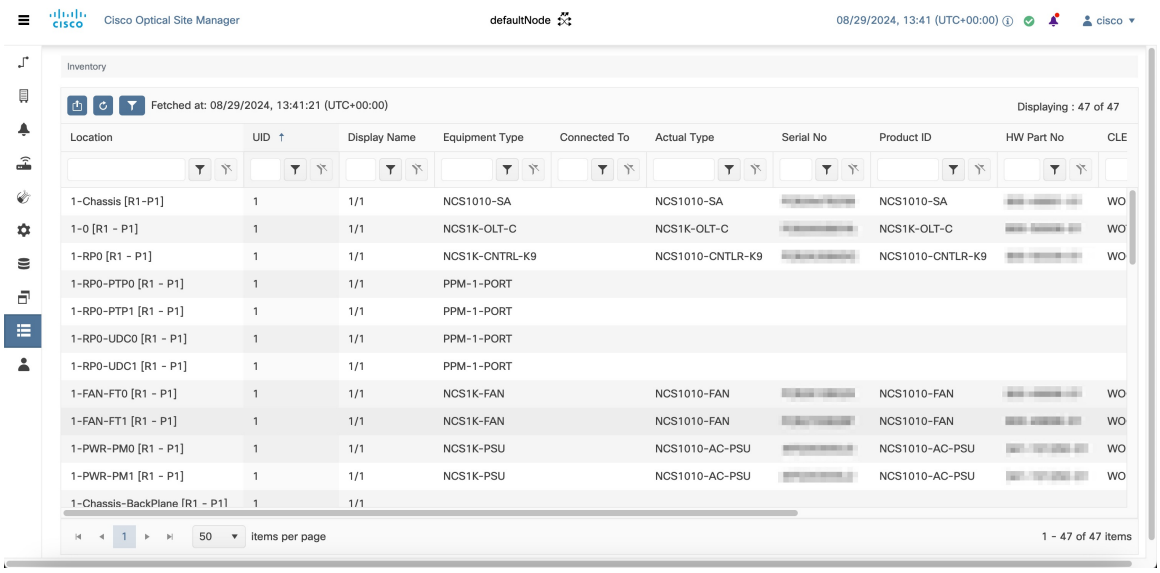


CHAPTER 11

# View Inventory

This chapter describs the tasks to view the inventory details of a single or multiple racks.

***Figure 23: View Inventory***





- View inventory of all racks or chassis, on page 147
- View inventory of a rack or chassis, on page 148


# View inventory of all racks or chassis

You can view inventory details of all racks and chassis, such as location, display name, and equipment type.

By default, the **Inventory** page sorts the inventory table by the **UID** column. To sort the table by location, click the **Location** column header.

Follow these steps to view the inventory of all the racks and chassis:

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Inventory**.

The **Inventory** page appears and displays the inventory details.

**Step 2** Click the **Export to Excel** icon to export and download the inventory information to an Excel file (optional).

# View inventory of a rack or chassis

You can view inventory details, such as location, display name, and equipment type, for a specific rack or chassis.

Follow these steps to view the inventory details of a rack or chassis:

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

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

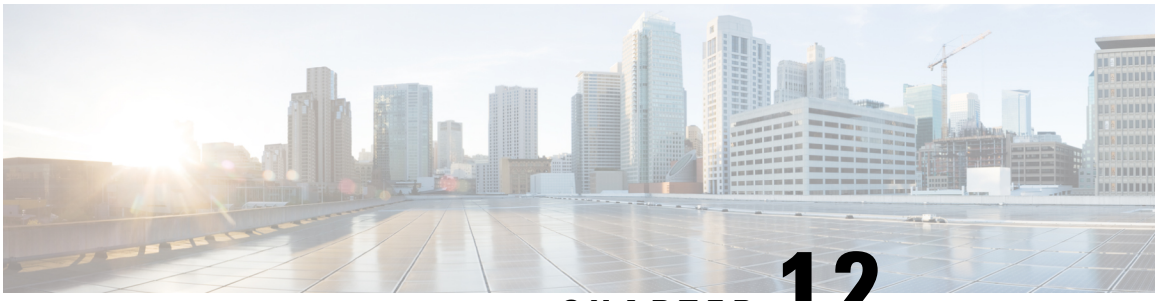
**Step 2** Perform one of these steps:

- Double-click the rack name from the rack view.
- Right-click the chassis from the rack view and select **Open**

**Step 3** Click the **Inventory** tab.

**Step 4** Click the **Export to Excel** icon to export and download the inventory information to an Excel file (optional).

The **Inventory** page appears and displays the inventory details.



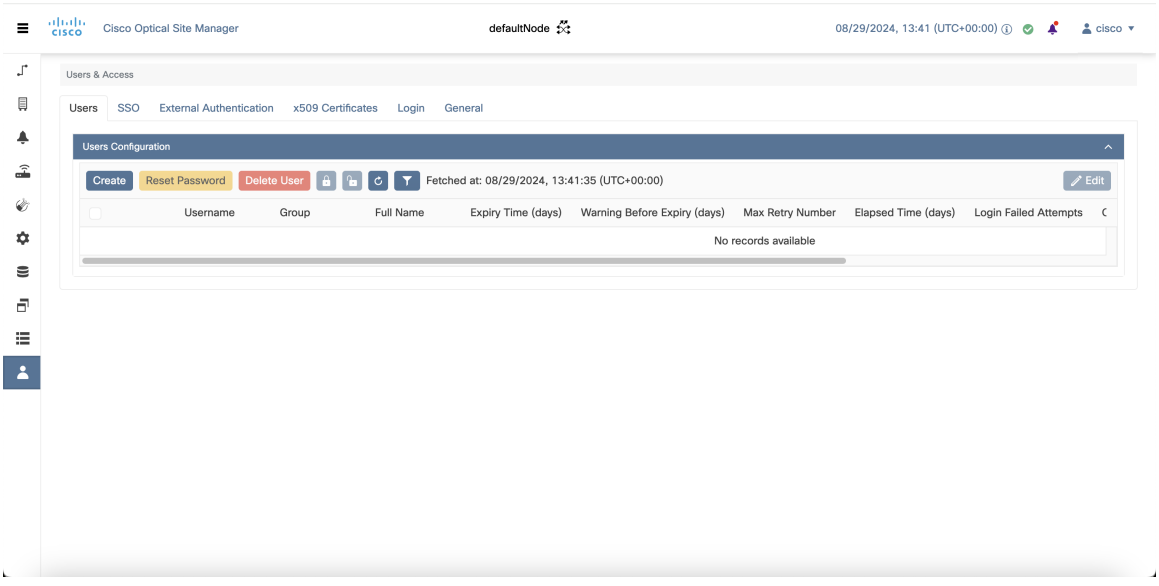
CHAPTER 12

# User access and authentication

This chapter describes these tasks for user access and authentication:

- Local user accounts
- Single sign-on (SSO) authentication
- External authentication
- Web certificates

***Figure 24: Manage User Access and Authentication***





- User configuration settings, on page 150
- Single sign-on (SSO), on page 153
- Manage External Authentication, on page 156
- x509 certificates, on page 167
- Active login user details, on page 169
- Session timeout, on page 171

# User configuration settings

This section explains how to create users, manage existing users, and set user profile passwords.

-

## Create users

Add new user accounts with specific roles and permissions. This enables controlled access to the Cisco Optical Site Manager for managing optical site operations, ensuring that only authorized personnel can perform configuration and monitoring tasks.

Only users with admin privileges can create new users. The process involves specifying user details such as username, password, password expiry, retry limits, and user group (for example, admin, editor, maintenance, snmp, viewer).

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to create new users.

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **Users** tab.

**Step 3** In the **Users Configuration** section, click **Create**.
The **Create User** dialog box is displayed.

**Step 4** Enter the details as described in the Table 43: User details, on page 150 table.

**Step 5** Click **Create**.

A new user is created. The user account is added to the Cisco Optical Site Manager with the configured credentials and permissions.

***Table 43: User details***

| Field | Description / Requirements |
|---|---|
| User Name | Type the user name.<br>User name requirements:<br>• Must be 6–40 characters long.<br>• Can include alphanumeric characters (a-z, A-Z, 0-9) and special characters: @, - (hyphen), . (dot). |

| Field | Description / Requirements |
|---|---|
| Password | Enter the login password.<br>Password requirements:<br>• Must be 8–127 characters long. Must include alphanumeric (a-z, A-Z, 0-9) and special characters (+, #, %).<br>• Must not contain the user name. |
| Retype Password | Re-enter the password for confirmation. |
| Expiry Time (days) | Enter the number of days before the user must change the password.<br>Example:<br>• If set to 20 days, the user must change the password before 20 days are over.<br>• After expiry, the user is moved to the Password group and must update the password before performing any other action. |
| Warning Before Expiry (days) | Enter the number of days in advance to warn the user before the password expires. |
| Max Retry Number | Maximum number of consecutive failed login attempts. After this limit, the account is moved to the Password group. |
| Group | Select the group from the drop-down list.<br>Available options:<br>• admin<br>• editor<br>• maintenance<br>• snmp<br>• viewer |

# Change user password

Change a user password to maintain secure access control within Cisco Optical Site Manager. This task ensures that user credentials are updated and protected according to security policies, preventing unauthorized access.

Only an admin can change the password.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to change password for a user.

**Procedure**

**Step 1** Click **Users & Access** in the left panel.
The **User & Access** page is displayed.

**Step 2** Click the **Users** tab.

**Step 3** Select the check box corresponding to the user you want to change the password in the **Users Configuration** section.

**Step 4** Click **Reset Password**.

The **Reset** *Username* **Password** dialog box appears.

**Step 5** Enter the new password in the **New Password** field.

The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters. The minimum number of characters in the password is eight and the maximum is 127. The password must not contain the user name.

**Step 6** Retype the same password in the **Retype Password** field.

**Step 7** Click **Reset Password**.

**Step 8** Click **OK**.

A confirmation message or status indicates that the password has been successfully changed.

# Configure user profile settings

Use this task to configure user profile settings in Cisco Optical Site Manager that allows you to manage retry limits and expiration policies.

User profile settings determine authentication behavior, password expiration, and access privileges.

You can enable or disable retry limits and expiration timers based on operational requirements.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to configure the user profile settings.

**Procedure**

**Step 1** Click the username in the upper-right corner, then click **User Profile**.

The **User Profile** window appears.

**Step 2** (Optional) Enter a value in the **Full Name** field.

**Step 3** Configure retry and expiration settings.

a) Enter a value in the **Max Retry Number** field.
b) Select **Disable Max Retry Number** to remove retry restrictions.

c) Enter a value in the **Expire Time (Days)** field.
d) Select **Disable Expire Time** to prevent account expiration.
e) Enter a value in the **Warning Before Expire (Days)** field.

**Step 4** Assign the user to a group.
a) Select a value from the **Group** drop-down list.

**Step 5** Click **Apply**.

The updated user profile settings are saved.

---

The user profile settings are updated and displayed in the **User Profile** window.

For more details about the fields, see Table 43: User details, on page 150 table.

# Delete users

Remove user accounts that are no longer needed. This practice maintains security and proper access control. Only authorized users will have access to the system.

Only administrators can delete users.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to delete users.

**Procedure**

---

**Step 1** Click **Users & Access** in the left panel.
**Step 2** Click the **Users** tab.
**Step 3** Select the check-box corresponding to the user you want to delete in the **Users Configuration** section.
**Step 4** Click **Delete User**.

A confirmation message appears.

**Step 5** Click **OK**.

---

The selected user is deleted and the account is removed from Cisco Optical Site Manager.

# Single sign-on (SSO)

Single Sign-On (SSO) is an authentication process. It enables a user to access multiple applications or services using a single set of login credentials, such as a username and password. This means users authenticate once. They then gain seamless access to all authorized applications without needing to log in separately to each one. The benefits of SSO include:

- Eliminates the need to remember multiple passwords.

- Reduces the frequency of login prompts during a session.

# Configure and enable SSO with SAMLv2

Enable Single Sign-On (SSO) for COSM using SAMLv2. Users can authenticate once through an identity provider (IdP) and then access the system without separate logins.

Only an admin can configure SSO SAMLv2 details.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to configure and enable SSO SAMLv2 details.

## Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **SSO SAMLv2** section to expand it.

**Step 3** Select the **Enable SAML** check box to enable the SAMLv2 protocol.

**Step 4** Enter the details as mentioned in the Table 44: SSO fields, on page 154 table.

**Step 5** Click **Apply**.

A trust relationship between Cisco Optical Site Manager and the IdP is established, enabling SSO functionality.

For details about each configuration field, see this table.

***Table 44: SSO fields***

| Field | Description |
|---|---|
| IDP Entity ID | A globally unique identifier for the Identity Provider within an SSO federation.<br>This serves as a distinct name for the IdP, allowing Service Providers to correctly identify and communicate with it. |
| IDP Metadata URL | The web address that points to the Identity Provider's metadata XML document.<br>Instead of manually configuring the service provider with all the IdP's details, the service provider can simply be provided with this URL. |
| Proxy Address | The network IP address of a proxy server sits between users and the applications they want to access, typically in an SSO setup. |
| Proxy Port | Network port number on which a proxy server listens for incoming connections. |

| Field | Description |
|---|---|
| Group Attribute Name | Name of an attribute within a SAML assertion or other SSO token that carries information about the user's group memberships. |
| IDP Metadata | Details that contains all the necessary configuration information about the Identity Provider. |

# Create an SSO with CAS

Cisco Optical Site Manager administrators can configure SSO users with Central Authentication Service (CAS). This allows a user to access multiple applications with only one login credential.

Only administrators can add new SSO users by specifying the username and assigning a user group, either *viewer* or *editor*.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 1
- Ensure that SSO users and other users have unique usernames.

Follow these steps to add an SSO user with CAS.

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **SSO CAS** section to expand it

**Step 3** Click the + button.

The **Create SSO User** dialog box appears.

**Step 4** Enter the username in the **Username** field.

**Step 5** Select a user group from the **Group** drop-down list.

| Group | Description |
|---|---|
| editor | When mapped for SSO, can only view the Cisco Optical Site Manager configurations. |
| viewer | When mapped for SSO, can configure devices. |

**Step 6** Click **Apply**.

A confirmation message appears.

**Step 7** Click **Yes**.

The SSO user is successfully created.

# Enable an SSO with CAS

Cisco Optical Site Manager administrators can configure SSO users with a Central Authentication Service (CAS). This allows a user to access multiple applications with only one login credential.

Only administrators can enable SSO with CAS on Cisco Optical Site Manager.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to enable SSO with CAS:

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **SSO CAS** tab.

**Step 3** Click **SETTINGS** to expand it.

**Step 4** Select the **Enable CAS** check box.

**Step 5** Enter the Cisco Optical Network Controller server IP address in the **IP Address** field.

**Step 6** (Optional) Specify the port number in the **Port** field.

The default port number is 443.

**Step 7** Click **Apply**.

A confirmation message appears.

**Step 8** Click **Yes**.

SSO with CAS on Cisco Optical Site Manager is successfully enabled.

# Manage External Authentication

This chapter describes the tasks related to external authentication in Cisco Optical Site Manager.

# Manage External Authentication

Cisco Optical Site Manager supports RADIUS and TACACS modes of external authentication. Ensure that you enable and use either RADIUS or TACACS authentication method. You can add a maximum of up to ten servers for each of RADIUS or TACACS on Cisco Optical Site Manager.

There should be at least one RADIUS or TACACS authentication server that is configured for authentication to be enabled. In order to delete the last RADIUS or TACACS server, you must disable the external authentication first, and then delete the RADIUS or TACACS server.

When your login to Cisco Optical Site Manager with the external authentication enabled, Cisco Optical Site Manager first tries with the configured list of servers. If external authentication servers are not reachable, then

Cisco Optical Site Manager uses local authentication provided the local authentication is enabled on Cisco Optical Site Manager.

To manage Cisco Optical Site Manager, the following users are created:

- Local users (local authentication)—Specifies users who are created to manage Cisco Optical Site Manager instances.
- External users (external authentication)—Specifies users who are created on the external authentication servers.

For more information related to users, see External Authentication Users for SVO.

**Note** A proper privilege level must be set on the external authentication server associated to the user. See the Privilege level and user group mapping table.

If a privilege level is not set for a user in the external authentication server, the user is allowed to log in only as **Viewer**. In this case, **LOGIN-MISSING-GROUP** alarm is raised.

The following table lists some external authentication scenarios that describe some possible authentication errors, causes, and actions.

***Table 45: External and Local Authentication Scenarios***

| External and Local Authentication Combination | Possible Authentication Scenario | Possible Cause | Action to be Taken |
|---|---|---|---|
| • External Authentication enabled and Local Authentication disabled | Server denies authentication | External username or password is incorrect | Enter the correct username and password to log in to the system. |
| | Server not reachable | IP address, shared secret or port number is not configured correctly although username or password could be correct | You are locked out of the system. Ensure that you have configured correct IP address, shared secret, and port number. |
| | User authenticated with lowest privilege (Viewer) despite the intended one | Privilege level is not set or incorrectly set on the external authentication server | Set the proper privilege level associated to the user on the external authentication server |

| External and Local Authentication Combination | Possible Authentication Scenario | Possible Cause | Action to be Taken |
|---|---|---|---|
| • External authentication enabled and Local authentication enabled | Server denies authentication (although local authentication is enabled) | External username or password is incorrect | Enter the correct username and password to log in to the system.<br>Local authentication only works when the RADIUS or TACACS external servers are not reacheable. |
| | Server not reachable (Local authentication is enabled) | IP address, shared secret, port number is not configured correctly although username or password could be correct | Use local authentication credentials to log in to Cisco Optical Site Manager. |
| | User authenticated with lowest privilege (Viewer) despite the intended one | Privilege level is not set or incorrectly set on the external authentication server | Set the proper privilege level associated to the user on the external authentication server |

# Configure static IPv4 route

Configure a static IPv4 route on the router to the TACACS server which serves as the gateway for the Cisco Secure ISE server.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

### Procedure

Run the **router static address-family ipv4** command to configure a static IPv4 route.

**Example:**

```
RP/0/RP0/CPU0:R1#config
Wed Jul 12 19:12:58.900 UTC
RP/0/RP0/CPU0:R1(config)#router static address-family ipv4 unicast 10.xx.xx.0/22 10.xx.xx.1
RP/0/RP0/CPU0:R1(config)#exit
```

# Configure loopback interface as source

If the Cisco Optical Site Manager management interface is configured as a loopback interface, Cisco Optical Site Manager uses it as the default source. If your network has filtering rules that restrict access to certain

servers like RADIUS or TACACS+, you can configure a specific interface IP address to be used as the source address for this traffic.

Follow these steps to configure a specific interface IP as source:

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Run the **linux networking** command to enter into the linux configuration mode.

**Example:**

```
RP/0/RP0/CPU0:WHIT-OLT-1(config)#linux networking
```

**Step 2** Run the **vrf default** command to apply the configuration to the *default* Virtual Routing and Forwarding (VRF) table.

**Example:**

```
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-net)#vrf default
```

**Step 3** Run the **address-family ipv4** to apply the configuration for the IPv4 address family.

**Example:**

```
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-vrf)#address-family ipv4
```

**Step 4** Run the source-hint default-route interface <interface-name> command to configure the specified interface as the source interface for that traffic.

**Example:**

```
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-af)#source-hint default-route interface
MgmtEth0/RP0/CPU0/0
```

### Example

This example shows how to configure a specific interface as source:

```
RP/0/RP0/CPU0:WHIT-OLT-1#conf t
RP/0/RP0/CPU0:WHIT-OLT-1(config)#linux networking
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-net)#vrf default
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-vrf)#address-family ipv4
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-af)#source-hint default-route interface
MgmtEth0/RP0/CPU0/0
```

# Limitations for RADIUS or TACACS Authentication

External user list is maintained with username and its respective group (admin, editor, viewer, or maintenance). The user list is populated whenever a new username is successfully authenticated. This user list is limited to 500 users. The **Clear External Users List** button available under the **External Authentication** tab is activated when 450 users limit is reached. Whenever you click the **Clear External Users List** button, the external users are cleared. In the user list, if the user limit is reached (500 users), then the new external user ($501^{th}$ external user) cannot login to Cisco Optical Site Manager.

If you are logged in as external user and cleared the list, ensure that you must relogin on all the logged-in sessions. If you do not relogin, the system might not respond properly and information might not appear properly.

# User role mapping for TACACS+ and RADIUS authentication

User role mapping for TACACS+ and RADIUS authentication assigns specific user roles after the authentication and authorization succeeded flows. These roles determine the level of access and permissions granted to the user on the network device or management system for their session.

- User roles are assigned based on attributes returned by the authentication server.
- These roles determine the access level and permissions a user has on network devices or management systems.

Cisco Optical Site Manager interprets these privilege level values received from authorization responses and assigns the corresponding internal role:

***Table 46: Privilege level and user group mapping***

| Privilege Level | User Group |
|---|---|
| 0 | viewer |
| 1 | editor |
| 2 | maintenance |
| 3 | admin |
| 7 | maintenance |
| 15 | admin |

**Note** Viewer and maintenance users can view all paths except `/admin` and `/auth`, and can edit only their own profile information. Editor user can view and edit all paths except `/admin` and `/auth`. Admin user has full access to view and edit everything.

# RADIUS Authentication

Use the following tasks to manage RADIUS authentication on Cisco Optical Site Manager.

**Note** Only an admin can manage RADIUS authentication on Cisco Optical Site Manager.

## Create RADIUS Server Entry

Use this task to create RADIUS server entry on Cisco Optical Site Manager. Only an admin can add RADIUS server.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Ensure that you have added Cisco Optical Site Manager instances with RADIUS IP addresses in the Cisco Identity Services Engine (ISE).
- Configure or assign the privilege level settings based on RADIUS user or group in the Cisco Secure ISE server. This will allow RADIUS users to log in to and access COSM.

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **RADIUS Configuration** section, perform the following steps:

a) Click the + button.

The **Create RADIUS Server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the RADIUS server.
- **Host**—IPv4 address of the RADIUS server.
- **Authentication Port**—1812 is default for RADIUS. The range is from 0 to 65535. RADIUS server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the RADIUS server.
- **Confirm Secret**—Confirm the above shared secret for the RADIUS server.

c) Click **Apply**.

The RADIUS server is added to the RADIUS server list on Cisco Optical Site Manager.

## Enable RADIUS Authentication

Use this task to enable RADIUS authentication. Only an admin can enable RADIUS authentication. You can add upto ten RADIUS servers on Cisco Optical Site Manager.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Create RADIUS Server Entry, on page 161

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **RADIUS Configuration** area, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Check the **Enable RADIUS Authentication** check box to enable RADIUS server on Cisco Optical Site Manager.

c) Check the **Enable node as final authentication when no RADIUS server is reachable** check box to enable the RADIUS server as a final authentication option.

**Note**
It is recommended to configure the system to use local authentication if all remote RADIUS or TACACS+ servers become unreachable. Ensure that valid local user accounts with appropriate credentials are created in advance, as local authentication requires these accounts. User accounts created through remote authentication methods cannot be used for local authentication.

d) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the RADIUS server before retrying to contact the server.

e) In the **Attempts** field, enter the number of attempts to contact the first RADIUS server in the authentication list. If there is no response after the allotted number of attempts, then Cisco Optical Site Manager tries to contact the the next RADIUS server in the list.

**Step 4** Click **Apply**.

## Modify RADIUS Server Parameters

Use this task to modify RADIUS authentication settings. Only an admin can modify RADIUS server settings.

### Before you begin

Log into Cisco Optical Site Manager, on page 1 and Create RADIUS Server Entry, on page 161

### Procedure

**Step 1** Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **RADIUS Configuration** area, select the RADIUS server to edit from the list of available RADIUS servers and perform the following tasks:

a) Click the **Edit** button.

b) Edit the following fields:

- **Host**
- **Authentication Port**
- **Shared Secret**

c) Click **Apply**.

## Disable the RADIUS Authentication

Use this task to disable RADIUS authentication.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the RADIUS Configuration area, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Uncheck the **Enable RADIUS Authentication** check box to disable RADIUS authentication on Cisco Optical Site Manager.

c) Uncheck the **Enable node as final authentication when no RADIUS server is reachable** check box to disable the RADIUS server as a final authentication option.

**Note**
When external authentication is disabled, then local authentication is disabled by default.

**Step 4** Click **Apply**.

## Delete the RADIUS Server from Cisco Optical Site Manager

Use this task to delete the RADIUS server entry from Cisco Optical Site Manager.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **RADIUS Configuration** area, select the RADIUS server to delete and click the **-** button.

# TACACS+ Authentication

Use the following tasks to manage TACACS+ authentication.

**Note** Only users with admin privileges can manage TACACS+ authentication on Cisco Optical Site Manager.

## Create TACACS+ Server Entry on Cisco Optical Site Manager

Use this task to create TACACS+ server entry on Cisco Optical Site Manager. Only an admin can add TACACS+ server. You can add upto ten TACACS+ servers.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Ensure that you have added Cisco Optical Site Manager instances with TACACS+ IP addresses in the Cisco Identity Services Engine (ISE).
- Configure or assign the privilege level settings based on TACACS+ user or group in the Cisco Secure ISE server. This will allow TACACS+ users to log in to and access COSM.

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **TACACS+ Configuration** section, perform the following steps:

a) Click the **+** button.

The **Create TACACS+ server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the TACACS+ server.
- **Host**—IP address of the TACACS+ server.
- **Authentication Port**—49 is default for TACACS+. TACACS+ server must be running on the port that is configured.

- **Shared Secret**—Shared secret configured on the TACACS+ server.
- **Confirm Secret**—Confirm the above shared secret for the TACACS+ server.

c) Click **Apply**.

The TACACS+ server is added to the TACACS+ server list on Cisco Optical Site Manager.

## Enable TACACS+ Authentication

Use this task to enable TACACS+ authentication.

### Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Create TACACS+ Server Entry on Cisco Optical Site Manager, on page 164

### Procedure

**Step 1** Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **TACACS+ Configuration** section, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Check the **Enable TACACS+ Authentication** check box to enable TACACS+ server on Cisco Optical Site Manager.

c) Check the **Enable node as final authentication when no TACACS+ server is reachable** check box to enable the TACACS+ server as a final authentication option.

**Note**
It is recommended to configure the system to use local authentication if all remote RADIUS or TACACS+ servers become unreachable. Ensure that valid local user accounts with appropriate credentials are created in advance, as local authentication requires these accounts. User accounts created through remote authentication methods cannot be used for local authentication.

d) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the TACACS+ server before retrying to contact the server.

e) In the **Attempts** field, enter the number of attempts to contact the first TACACS+ server in the authentication list. If there is no response after the allotted number of attempts, then Cisco Optical Site Manager tries to contact the the next RADIUS server in the list.

**Step 4** Click **Apply**.

# Modify TACACS+ Server Parameters

Use this task to modify TACACS+ authentication settings. Only an admin can modify TACACS+ server settings.

### Before you begin

Log into Cisco Optical Site Manager, on page 1 and Create TACACS+ Server Entry on Cisco Optical Site Manager, on page 164

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **TACACS+ Configuration** area, select the TACACS+ server to edit from the list of available TACACS+ servers and perform the following tasks:

a) Click the **Edit** button.

b) Edit the following fields:

- **Host**
- **Authentication Port**
- **Shared Secret**

c) Click **Apply**.

# Disable the TACACS+ Authentication

Use this task to disable TACACS+ authentication.

### Before you begin

Log into Cisco Optical Site Manager, on page 1

### Procedure

**Step 1** Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

**Step 2** Click the **External Authentication** tab.

**Step 3** In the **TACACS+ Configuration** area, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Uncheck the **Enable TACACS+ Authentication** check box to disable TACACS+ authentication on Cisco Optical Site Manager.

c) Uncheck the **Enable node as final authentication when no TACACS+ server is reachable** check box to disable the TACACS+ server as a final authentication option.

**Note**
When external authentication is disabled, then local authentication is disabled by default.

**Step 4** Click **Apply**.

## Delete the TACACS+ Server from Cisco Optical Site Manager

Use this task to delete the TACACS+ server entry from Cisco Optical Site Manager.

**Before you begin**

Disable the TACACS+ Authentication, on page 166

**Procedure**

**Step 1** Click **Users & Access** in the left panel.
**Step 2** Click the **External Authentication** tab.
**Step 3** In the **TACACS+ Configuration** area, select the TACACS+ server to delete and click the **-** .

# x509 certificates

x509 certificates are used to establish a secure communication channel between a client and a server. In Cisco Optical Site Manager, you can automatically generate a self-signed x509 certificate or upload a CA-authorized certificate in digital or PFX format. This certificate:

- builds trust between the client and server,
- protects sensitive information from unauthorized parties
- and provides the ability to detect any tampering or modification of data during transmission.

*Table 47: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Improved x509 Certificate Handling | Cisco IOS XR Release 24.1.1 | You can now upload an x509 certificate in the Personal Information Exchange (PFX) format, which improves the security of the connection between the Cisco Optical Site Manager and its server. PFX files can be password-protected, offering an extra layer of protection against potential attackers.<br>The options to automatically generate and upload certificates are available in the new **x509 Certificates** tab under the **Users & Access** menu. |

# Generate and upload x509 certificates

Establish secure communication channels between clients and servers to ensure encrypted and trusted communications. This ensures data confidentiality, integrity, and authentication. It protects sensitive information from unauthorized access and tampering during transmission.

Use this task to upload certificates in digital (.cert) or PFX (.pfx) file formats. You can generate certificates internally as self-signed, or upload them in several formats such as:

- Certificate and key (CERT + KEY)
- Personal Information Exchange (PFX) and password (PFX + PASSWORD)
- PEM

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to automatically generate and apply a x509 certificate.

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **x509 Certificates** tab.

**Step 3** Click the **Certificates Configuration** section to expand it.

**Step 4** Perform any one of the following steps to auto-generate or upload certificate files:

| To auto generate and apply | To upload a digital certificate | To upload a PFX certificate |
|---|---|---|
| Click **Auto Generate and Apply Certificate** to automatically generate and apply a self signed certificate. | **a.** Select *CERT + KEY* from the **Certificate Type** drop-down list.<br>**b.** Select the *.cert* or *.crt* file from the **Certificate File** field and click **Upload**.<br>**c.** Select the *.key* file in the **Key File** field and click **Upload**. | **a.** Select *PFX + PASSWORD* from the **Certificate Type** drop-down list.<br>**b.** Select the *.pfx* file from the **Certificate File** field and click **Upload**.<br>**c.** Type the password in the **Password** field if the input private key file is password protected. |

**Step 5** Click **Apply**.

The uploaded ceritifcate is validated, which enables secure, encrypted communication.

# Active login user details

Cisco Optical Site Manager displays details of users who are currently logged in and displays their session information. Monitoring user activity and managing sessions are made more effective with this information. These user session details are displayed:

- username
- login time
- interface name
- IP address

## View active login sessions

Administrators can use Cisco Optical Site Manager to view active login sessions, monitor current user activity, and enhance security management.

You can view the users currently logged in and their details, such as username, login time, interface name, and IP address.

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to view the list of currently logged in users:

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

**Step 2** Click the **Login** tab.

**Step 3** Click **Active Login Sessions** to view the currently logged in users and their details.

The system displays the username, login time, interface name, and IP address for each user currently logged in.

# View the user login history

Administrators can access the past login activities of a user. This access facilitates auditing user activities, enables tracking of security events, and helps identify unauthorized or suspicious login attempts.

You can view user login history and details such as:

- Login ID
- username
- Last login and logout date
- Interface name
- IP address

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to view the user login history:

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

**Step 2** Click the **Login** tab.

**Step 3** Click **Last Successful Logins** to view user login history and associated details.

The system displays the user login history for each user.

# Session timeout

This section describes the tasks to configure session timeouts for these session types:

- WebUI sessions
- Netconf protocol

## Configure Netconf and webUI session timeout

Configure the timeout settings for user sessions in Cisco Optical Site Manager to ensure that inactive sessions are automatically signed out after a specified period. This enhances security and resource management.

You can configure timeout values to control how long a user session can remain inactive or active before being terminated.

You can configure timeout values for two types of sessions:

- Netconf: Configure timeout for the NETCONF (Network Configuration Protocol) protocol. This includes an idle timeout (in minutes).
- WebUI: Configure timeout for a user's session in a web-based user (WebUI) interface. This includes both an idle timeout (in minutes) and an absolute timeout (in hours).

**Before you begin**

Log into Cisco Optical Site Manager, on page 1

Follow these steps to configure timeout for WebUI and Netconf sessions:

**Procedure**

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **Sessions Control** tab.

**Step 3** Select the time and hours from the respective drop-down lists as described in this table:

| Drop-down | Description |
|---|---|
| Webui Idle Timeout | Defines the maximum period of inactivity allowed for a user's session in a WebUI before that session is automatically terminated.<br>Valid values: 1 to 30 minutes in increments of 1 minute |
| Webui Absolute Timeout | Defines the maximum total duration a user's session in a WebUI user interface can remain active, irrespective of user activity.<br>Valid values: 1 to 16 hours in increments of 1 hour |

| Drop-down | Description |
|---|---|
| Netconf Timeout | Defines a configurable time limit for operations performed over the NETCONF protocol.<br>Valid values: 1 to 30 minutes in increments of 1 minute |

**Step 4** Click **Apply**.

The settings are saved and users are automatically signed out of their Nodal Craft or Netconf sessions based on the configured idle or absolute timeout values.