

Configuration Guide for Cisco Optical Site Manager, IOS XR Release 25.x.x

First Published: 2025-03-30

Last Modified: 2026-10-05

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

© 2026 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 9

View degree details for a OLS node 10

Optical Channel Monitoring 11

View Optical Channel Monitoring data 12

OCM spectrum graph 13

OCM utilization table 14

Optical Time Domain Reflectometer 15

OTDR icons 15

Run a manual OTDR scan in expert, multi-region, or auto-sector mode 16

Enable Automatic OTDR Scan 18

View side details 19

View side details for an OLS node 20

View card details 21

View port details 22

View patch cord details 23

View circuit details 23

Connection verification 24

Verify connections 25

Customize NFV layout 26

View active circuit list 27

CHAPTER 3 **Cisco Optical Site Manager Topology 29**

Topology 29

Add a rack 30

Add a chassis 30

Open the card view 31

Identify a passive device associated with a USB 32

View CPU and memory usage 33

View voltage, temperature and current details 35

View power monitoring parameters 36

CHAPTER 4 **Monitor Faults 37**

Fault Monitoring 37

View rack, chassis, or card alarms 38

View all alarms and conditions 39

View correlated alarms 40

View rack, chassis, or card transient conditions 41

View alarms history 42

Alarm profiles 42

Create and load alarm profiles 44

Associate alarm profiles 44

User tags 45

Create user tags 46

CHAPTER 5 **Configure Devices 47**

Create or edit an authorization group 47

Add a device 49

Add Unmanaged Devices 53

Manage a device using IOS XR CLI 55

Move a device or view device properties 56

Delete devices and authorization groups 57

Retrieve device diagnostics 57

SOCKS Proxy 58

Change the Cooling Profile Control 59
SVO-LC device onboard in R25.1.1 59
Configure additional route for NCS 1000 device 59

CHAPTER 6 **Provision Line Cards** 63
Supported NCS 1000 line cards 64
Configure the administrative state of Pluggable Port Modules and line cards 65
Open the card view 65
Provision an NCS 1000 or NCS 2000 card 66
NCS 1000 line card modes 67
Configuring card modes 72
Select a card mode 73
Select trunk and client data rate 74
Add Internal Patch Cords 76
Add trunk details 77
Verify configuration details 79
Edit card mode for NCS 1000 cards 79
Configuring card modes for NCS 2000 line cards 80
Select a card mode for an NCS 2000 line card 81
Add secondary modules 83
Add pluggable modules to ports 85
Verify card configuration details 85
Configure card mode on a NCS 2000 control card 86
Supported operating modes and port mapping details for NCS 2000 cards 87
Reset a line card 90
Provision SONET or SDH trace monitoring 91
Provision trail trace monitoring 92
Provision ODU interfaces 94
Provision OTU interfaces 95
Provision Ethernet interfaces 97
Provision SONET or SDH Interfaces 99
Provision optical channels 102
Change Trunk Port Parameters 105
Provision optical threshold settings 105

Configure G.709 thresholds 107
Provision FEC thresholds 108
Configure RMON thresholds 109
Configure loopback interfaces 110
Configure optical safety 111
Configure thresholds for SONET or SDH 113
Enable attention LED 114
PSM card protection mechanism 116
Enable the revertive protection switching 116
Configure the non-revertive protection switching 117
Perform a manual switch 118
View performance monitoring parameters 118
SVO Card 119
Installing the SVO Card 120
View UDC details 124
View Insertion Loss Parameters 125
Manage the Protection Group 125
Provisioning Optical Amplifier Cards 127
RAMAN-CTP and RAMAN-COP Cards 127
RAMAN-CTP and RAMAN-COP Cards Power Monitoring 128
Clear the Raman Laser Shutdown Condition 129
Collect Failure Logs 129
Perform Automatic Calibration 130
Perform Manual Calibration 133
Provision FPD Upgrade 135
Retrieve MAC Addresses through LLDP 135
Limitations of LLDP Support on the 1.2T-MXP Card 136
Provision FPD Upgrade for the Ports 136
Provision FPD Upgrade for MR-MXP Card 137
Enable Proactive Protection 138
Provision ODU Circuit 140
Functional Module Group 141
Configure Card Mode using Functional Module Group 142
Provision ZR Plus Interfaces 144

Provision ZR Plus Interfaces 145
Provision ZR Plus Trail Trace Monitoring 146
Provision ZR Plus Trail Trace Monitoring 146
Provision Pluggable Ports 147
View Circuit Protection Parameters 148
NCS 2000 Cards 150
10x10G-LC Card 151
Operating Modes for 10x10G-LC Card 151
200G-CK-C Card 152
Key Features of 200G-CK-C and 10x10G-LC Cards 153
Operating Mode for 200G-CK-C Card 155
400G-XP Card 155
Key Features 156
Interoperability 158
Regeneration Mode for 400G-XP-LC 161
1.2T-MXP Card 162
Key Features of 1.2T-MXP 162
Limitations of 1.2T-MXP Card 163
Operating Modes and Slice Definition in the 1.2T-MXP Card 163

CHAPTER 7 **Configure the Node** 167
Import a Cisco Optical Network Planner configuration file 168
Optical Degrees 170
Manage Optical Degrees 170
Internal patch cords 171
Create internal patch cords 172
Automatic Power Control 174
APC at the Shelf Controller Layer 174
APC at the Amplifier Card Level 176
Forcing Power Correction 177
Enable APC 177
Disable APC 178
Span Loss Measurement 178
View or modify span loss parameters 179

Configure amplifier parameters 180
Provision interface parameters 183
Provision Raman Amplifier Parameters 185
Manage Raman Interface Parameters 187
Optical cross-connect circuits 189
View Optical Cross-Connect Circuits 190
Troubleshooting incorrect OXC path endpoints 192
Update OXC endpoints by importing a configuration XML file 192
Edit OXC endpoints from the COSM CLI 194
Submarine Line Terminating Equipment mode 198
Enable or disable submarine mode 198
GMPLS UNI 200
How to Create a GMPLS UNI Tunnel 201
Create static Link Management Protocol link for GMPLS 202
Select the LMP type 202
Select the optical parameters for LMP 203
Select the End Points for LMP 204
Verify the LMP configurations 205
Create LMP regeneration pair 205
FEC modes and Trunk modes supported for Alien IDs 206
DCN Extension 208
Manage DCN Extension 209
Remote Node Management Using GCC 210
Manage Remote Node Using GCC 210
Provision a Node in GCC Using Light Web UI for Remote Node 211
Add a device 212

CHAPTER 8 **Backup and Restore Database** 217
Database Backup and Restore 219
Backup and download database 219
Restore Database 220
Upload Database 221

CHAPTER 9 **Upgrade Software** 223

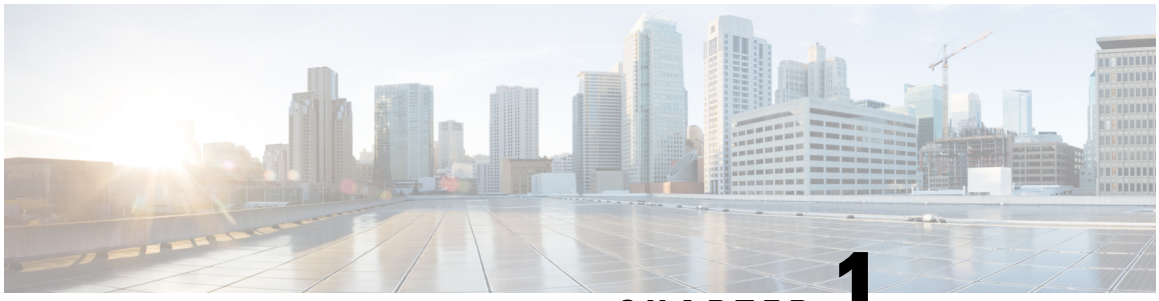
Cisco Optical Site Manager software packages 223
Workflow for Software Upgrade 224
Download GISO image 225
Download Software Package on Device 226
Activate NCS 1000 and NCS 2000 device software 227
Activate Cisco Optical Site Manager and Admin Plane Image for the SVO-LC 228
Delete software package 229

CHAPTER 10 View Inventory 231
View inventory of all racks or chassis 231
View inventory of a rack or chassis 232

CHAPTER 11 User access and authentication 233
User configuration settings 234
Create users 234
Change user password 235
Configure user profile settings 236
Delete users 237
Single sign-on (SSO) 237
Configure and enable SSO with SAMLv2 238
Create an SSO with CAS 239
Enable an SSO with CAS 240
Manage External Authentication 240
Manage External Authentication 240
Configure static IPv4 route 242
Configure loopback interface as source 242
Limitations for RADIUS or TACACS Authentication 244
User role mapping for TACACS+ and RADIUS authentication 244
RADIUS Authentication 244
Create RADIUS Server Entry 245
Enable RADIUS Authentication 245
Modify RADIUS Server Parameters 246
Disable the RADIUS Authentication 247
Delete the RADIUS Server from Cisco Optical Site Manager 247

TACACS+ Authentication 248
Create TACACS+ Server Entry on Cisco Optical Site Manager 248
Enable TACACS+ Authentication 249
Modify TACACS+ Server Parameters 250
Disable the TACACS+ Authentication 250
Delete the TACACS+ Server from Cisco Optical Site Manager 251
x509 certificates 251
Generate and upload x509 certificates 252
Active login user details 253
View active login sessions 253
View the user login history 254
Session timeout 255
Configure Netconf and webUI session timeout 255

CHAPTER 12 **Cisco Optical Site Manager Settings** 257
Configure time zone and measurement units 257
Download device diagnostics 258
Configure NTP servers for node time synchronization 259
View Audit Logs 260
Smart licensing for Cisco Optical Site Manager 261
Configure smart licensing workflow 263
Smart transport mode 264
Smart licensing CSLU mode 265
Create a Token 265
Configure DNS to Access Cisco Optical Site Manager 266
Configure transport mode 267
Establish trust 269
Smart licensing offline mode 270
Configure offline transport mode in Cisco Optical Site Manager 270
Download trust request file from Cisco Optical Site Manager 271
Upload trust request file to CSSM 271
Download acknowledgment from CSSM 272
Import acknowledgment file into Cisco Optical Site Manager 273



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

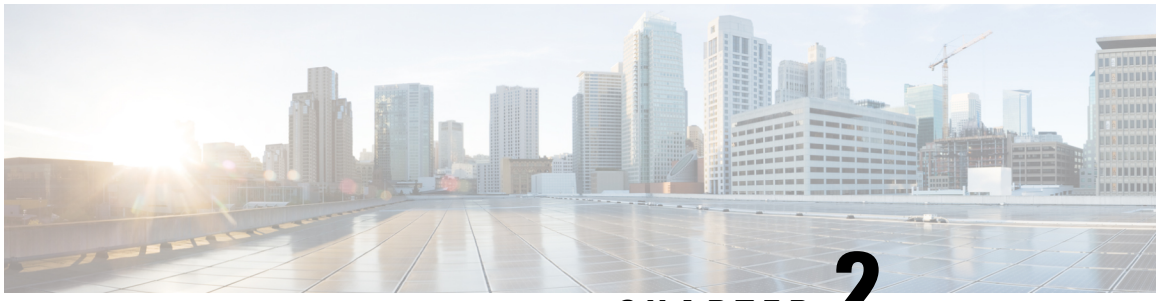
Step 1 Enter the IP address of the Cisco Optical Site Manager instance in the browser URL field.
The Cisco Optical Site Manager login page appears.

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
NFV Map View Enhancements	Cisco IOS XR Release 25.3.1	The NFV map view now features a clearer and more organized site optical diagram with updated icons, improved data flow representation, and streamlined functional block layout. Omnidirectional blocks are grouped for efficient navigation, and the OXC view is always expanded horizontally for consistent data flow visualization.
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). 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.

Feature Name	Release Information	Description
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). 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 9
- View degree details for a OLS node, on page 10
- Optical Channel Monitoring, on page 11
- Optical Time Domain Reflectometer, on page 15
- View side details, on page 19
- View side details for an OLS node, on page 20
- View card details, on page 21
- View port details, on page 22
- View patch cord details, on page 23
- View circuit details, on page 23
- Connection verification, on page 24
- Customize NFV layout, on page 26
- View active circuit list, on page 27

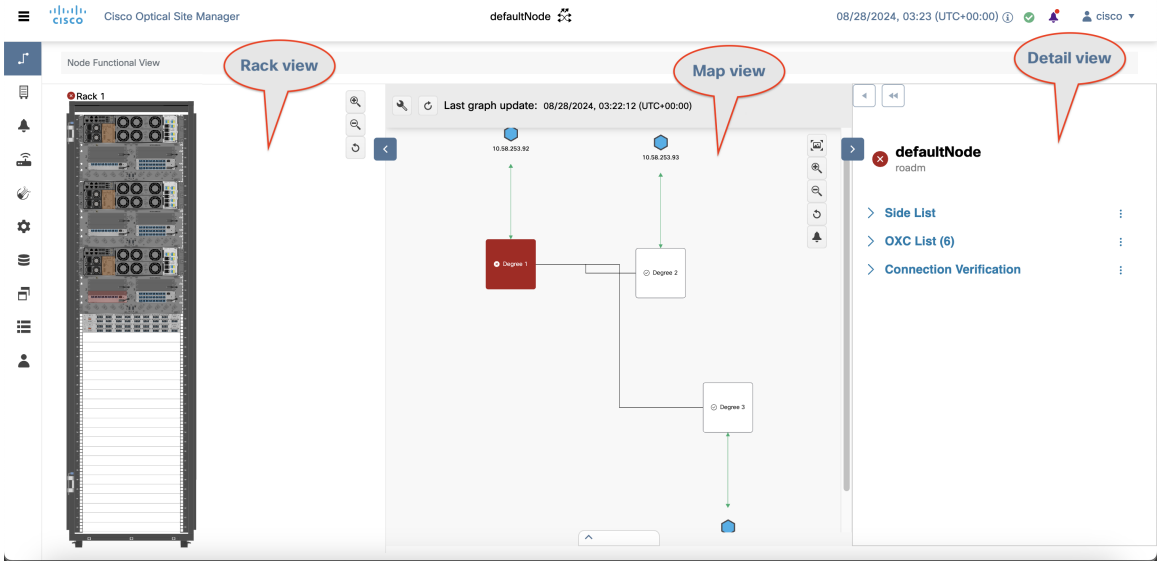
Understanding Node Functional View

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. • 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. • Zoom or highlight a node or card in the rack view • 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 • View and manage optical cross connections (OXC) • Run connection verification between components • View card mode configuration and details • 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.

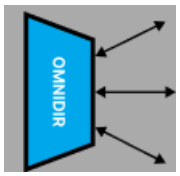
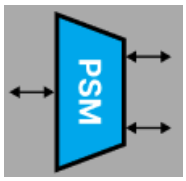
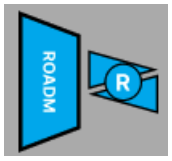
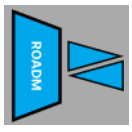
Icon	Description
	Displays or hides the alarms icon in the map and detailed view. 1. Click this button. 2. Select or deselect the alarm icons in the drop-down list to display or hide the alarms icon in the map and detailed view.
	Sets the user preferences. For more details, see Customize NFV layout, on page 26.
	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 icons

This table describes the icons available on the Map view.

Table 4: Map view icons

Icon	Description
	Remote site

Icon	Description
	PP mesh
	TXP/MXP
	amplifier
	Amplifier with Raman
	Omnidir
	PSM
	Roadm Raman amplifier
	Roadm amplifier

Map view icon colors

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

Table 5: 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 6: 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.

Section	Description
OXC List	Displays a list of active circuits passing through a particular card. For more details, see View active circuit list, on page 27.
Connection Verification	Displays a list of the connections between the line cards and all passive modules. For more details, see Connection verification, on page 24.

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: • **RX:** Select to view the optical spectrum in the RX direction. • **TX:** Select to view the optical spectrum in the TX direction. When table view is enabled: • **C-band:** Select to view the optical spectrum for the C band. • **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 13.

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 14.

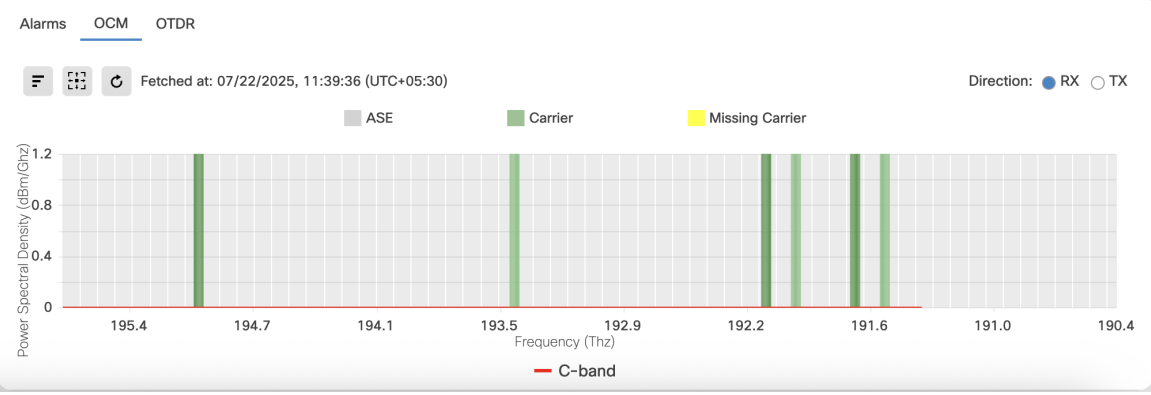
You can view the transmission or reception power levels for the optical degree you selected in the OCM data and spectrum occupancy graph and table.

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).

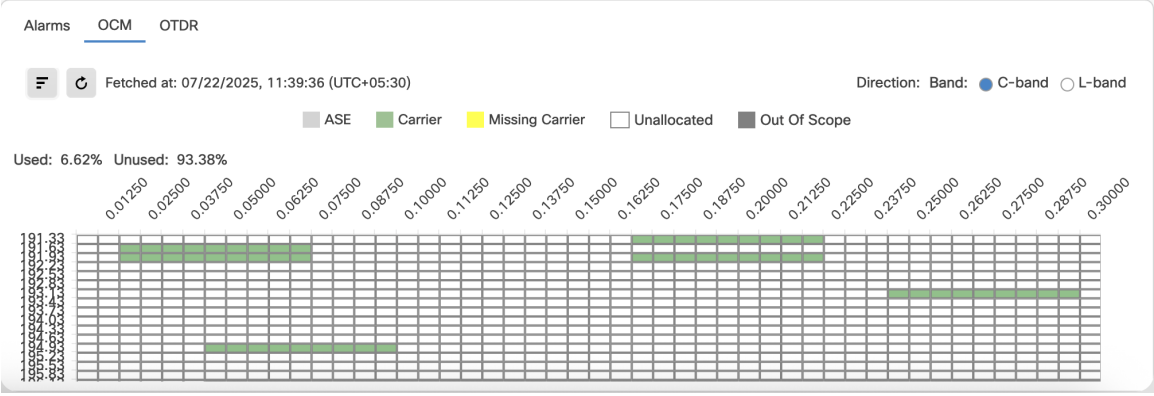
OCM utilization table

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 7: 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.

Note When performing an OTDR scan on Cisco optical nodes, it is expected system behavior for the OTDR trace to display a long tail of noise extending beyond the fiber end or the configured scan range; this does not indicate a malfunction. In **Auto mode**, the system detects the actual fiber end, though a noise tail may still appear beyond this point. In and Expert modes, the scan range is determined exclusively by the configured "capture start" and "capture end" points (in km), rather than the span length configuration; consequently, a noise tail may appear beyond the configured capture end point.

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 8: 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.
	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 9: 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 10: 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.

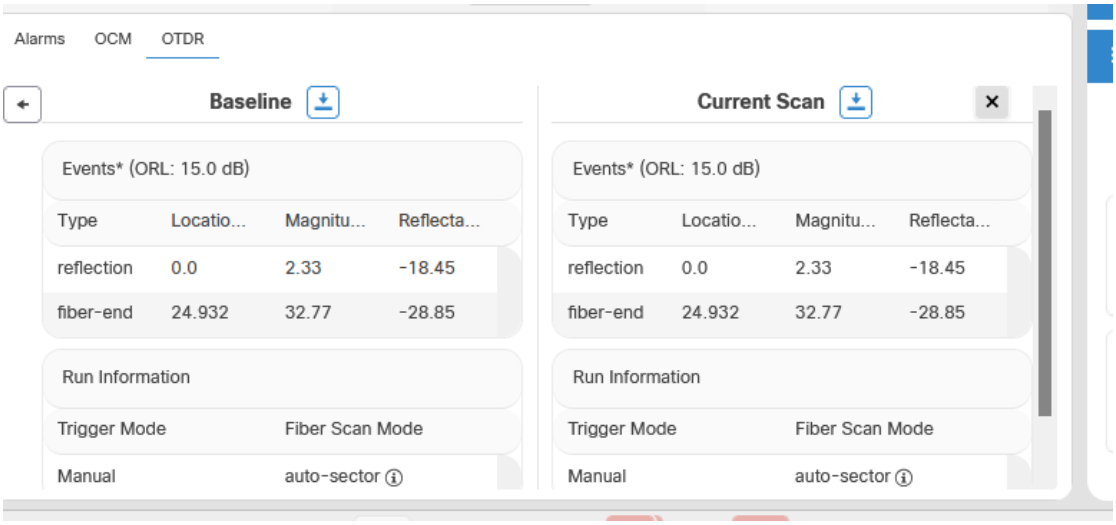
   An informational message appears indicating that the OTDR scan has been terminated.

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 11: 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** 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.

Note In Cisco Optical Site Manager, the IP address of a neighbor node may persist after the node is deleted or deactivated. This persistence can cause a wrong discovery of neighbour before any new node insertion or when updating existing neighbor IP addresses. It is recommended to remove the configuration and system description from the device where COSM is deactivated using the **no lldp system-description** IOS XR command.

- 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. 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 12: 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 24.

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 13: Patch cord details

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

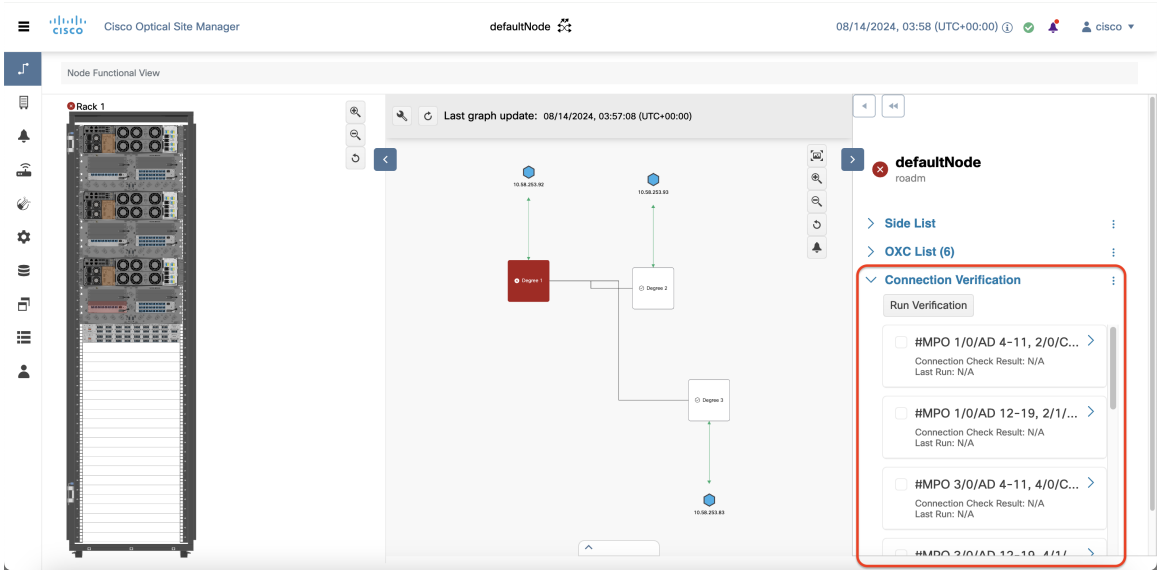
Connection verification

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. 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. 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.

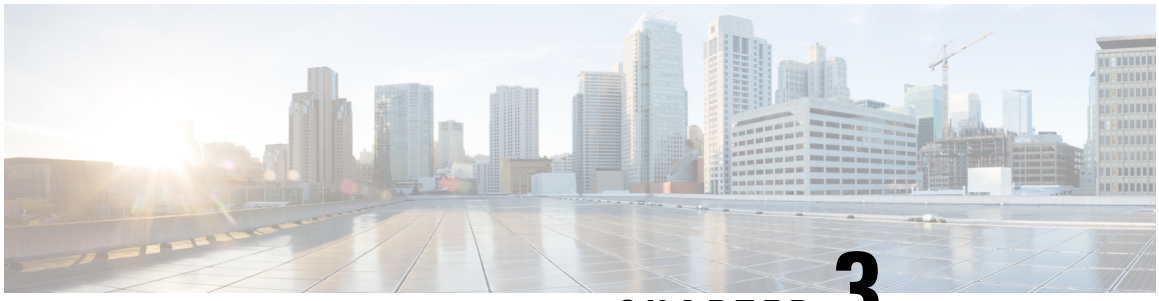
The Node Functional View page appears.

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 29
- Add a rack, on page 30
- Add a chassis, on page 30
- Open the card view, on page 31
- Identify a passive device associated with a USB, on page 32
- View CPU and memory usage, on page 33
- View voltage, temperature and current details, on page 35
- View power monitoring parameters, on page 36

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. **b.** Select **Delete**.
Move a chassis to a different slot	**a.** Right-click the chassis in the rack and select **Cut**. **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**

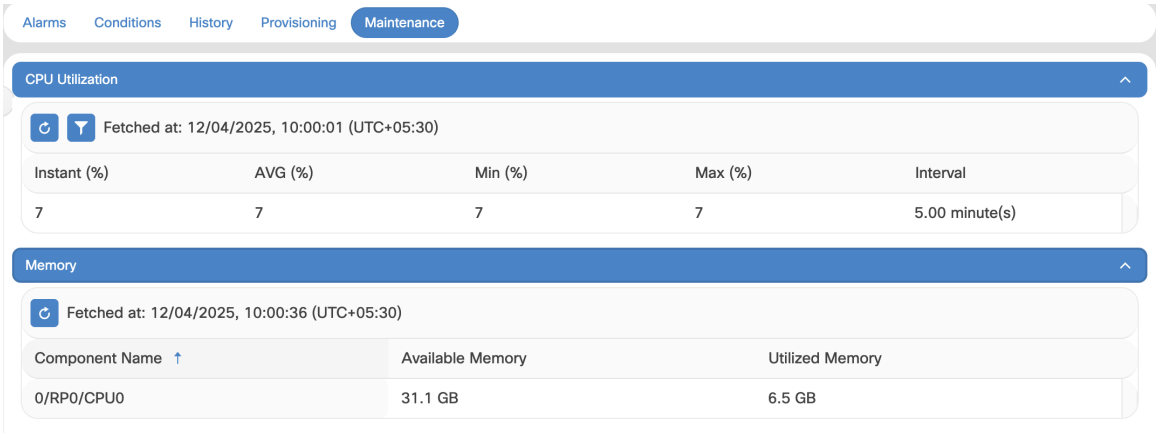
View CPU and memory usage

Monitor real-time CPU utilization and memory consumption on the device. This monitoring capability helps in quickly assessing the device's performance and identifying any resource bottlenecks or issues.

Table 14: Feature History

Feature Name	Release Information	Description
Real-Time CPU and Memory Monitoring	Cisco IOS XR release 25.4.1	You can now monitor real-time CPU usage and memory data in the **CPU Utilization** and **Memory** sections of the **Maintenance** tab. This helps you to quickly assess the device performance and take action as needed.

Figure 6: CPU and Memory Usage



Before you begin

Log into Cisco Optical Site Manager, on page 1

Follow these steps to view the CPU usage and memory information:

Procedure

Step 1 Click **Topology**.

Step 2 Click the rack name from the rack view.

Step 3 To open the chassis or line 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** to open the chassis view.
- Double-click the chassis or line card to open the chassis or line card view.

Step 4 Navigate to the **Maintenance** tab for your selected chassis or line card, then select **CPU Utilization** and **Memory** to view usage details.

For more details about the filed descriotions, see the Table 15: CPU Utilization and Memory field descriptions, on page 34 table.

You can now view real-time CPU and memory usage statistics for the selected device.

This table describes the fields displayed in the **CPU Utilization** and **Memory** sections:

Table 15: CPU Utilization and Memory field descriptions

Field	Description
CPU Utilization	
Instant	Shows the current CPU utilization at the moment the data was fetched.
AVG	Displays the average CPU utilization calculated over the **Interval** .
Min	Indicates the lowest CPU usage recorded during the **Interval** .
Max	Indicates the highest CPU usage recorded during the **Interval** .
Memory	
Component Name	Displays the specific device for which the memory details are shown.
Available Memory	Shows the total memory currently free and available for use by that device.
Utilized memory	Indicates the amount of memory currently in use by the device.
Interval	Specifies the time window (in minutes) used to collect and compute the CPU utilization statistics.

View voltage, temperature and current details

Table 16: Feature History

Feature Name	Release Information	Description
Environmental Monitoring in the Maintenance Tab	Cisco IOS XR release 25.1.1	The **Maintenance** tab now features an **Environmental Monitoring** section, providing real-time voltage, current, and temperature data for line cards and chassis. This addition simplifies device monitoring and management.

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.

Step 2 Click the rack name from the rack view.

Step 3 To open the chassis or line 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** to open the chassis view.
- Double-click the chassis or line card to open the chassis or line card view.

Step 4 Click the **Maintenance** tab.

Step 5 Click the **Environmental Monitoring** section to expand it.

Step 6 From the **Type** drop-down list, select any of these options to view the related information:

- Voltage
- Temperature
- Current
- Fan (Only available for Chassis)

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.

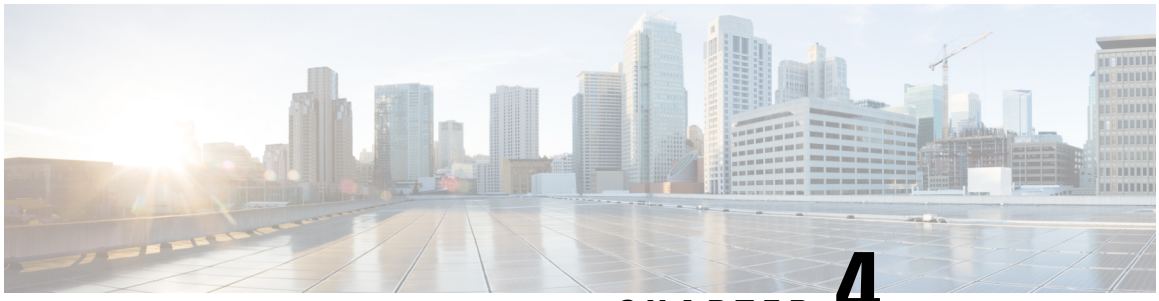
Step 2 Click the rack name from the rack view.

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 **Maintenance** tab.

Step 5 Click the **Power Monitoring** section to expand it.
The chassis total power consumption and maximum power display.



CHAPTER 4

Monitor Faults

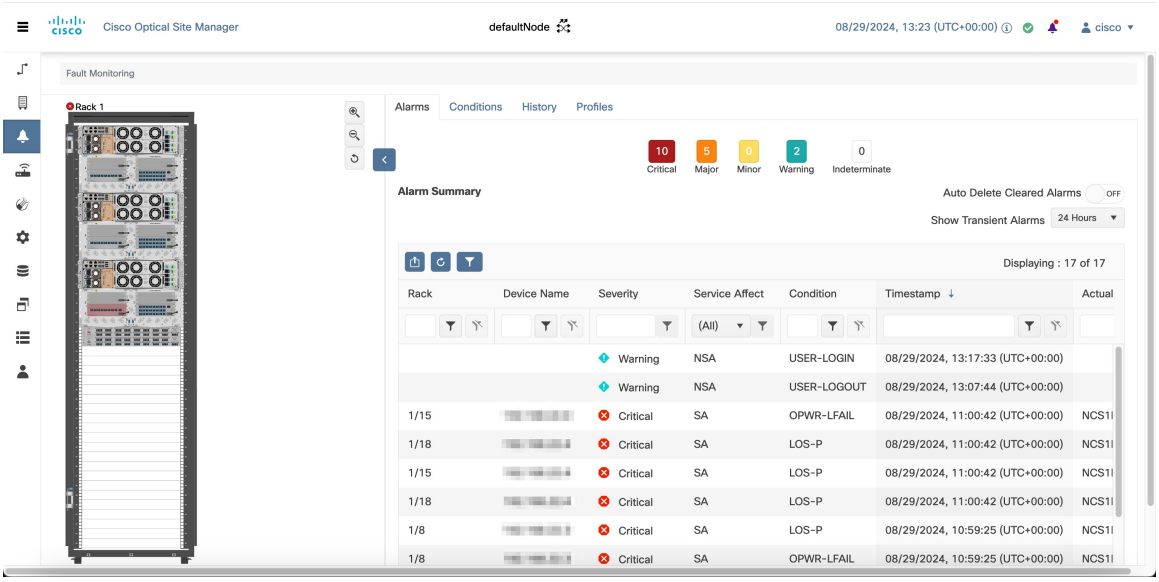
This chapter describes the tasks to view alarms and create alarm profiles.

- Fault Monitoring, on page 37
- View rack, chassis, or card alarms, on page 38
- View all alarms and conditions, on page 39
- View correlated alarms, on page 40
- View rack, chassis, or card transient conditions, on page 41
- View alarms history, on page 42
- Alarm profiles, on page 42
- User tags, on page 45

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 7: 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.

Note The Cisco Optical Site Manager Web UI does not display OTS-OCH alarms raised on the NCS1K-MD-32E-CE device in an MOLS 2.0 setup of NCS 1014, even when no cross-connect configuration is present. Verify device-side alarms in such deployments.

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 correlated alarms

Table 17: Feature History

Feature Name	Release Information	Description
Correlated Alarms	Cisco IOS XR Release 25.1.1	You can now view correlated alarms for a device in the **Alarms** tab, streamlining system performance management by highlighting primary alarms and suppressing secondary ones.

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

Before you begin

Log into Cisco Optical Site Manager, on page 1

Procedure

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

Alternatively, you can also click the bell icon on the top-right corner.

Step 2 Click the **Alarms** tab.
Alarms are displayed with several severities, such as Critical, Major, Minor, Warning, and Intermediate. The alarm severities are indicated by different colors.

Step 3 Click the **Expand Correlated Alarms** icon under the **Severity** column next to the device name to view the correlated alarms.
The RCA table displays a list of the correlated alarms for the device.

Step 4 Click **Back to Alarms Overview** button to go back to alarms list.

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:

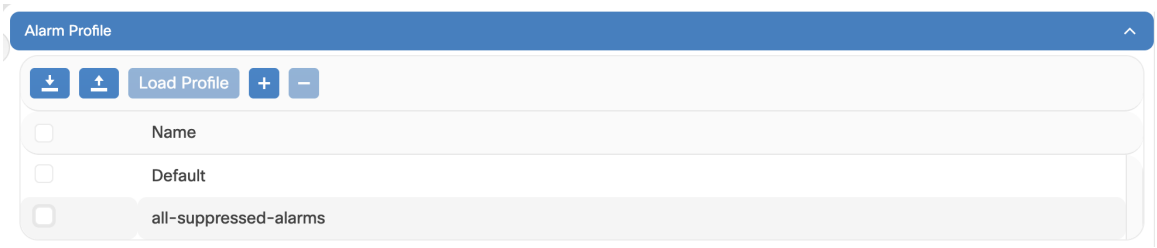
- The default alarm profile is preprovisioned on the node and contains all alarms.
- It sets alarm severities according to standard Telcordia GR-474-CORE guidelines, which cannot be changed.
- Default severities are applied to all alarms and conditions until a new custom profile is created and applied.
- 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 8: 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.

User tags

Table 18: Feature History

Feature Name	Release Information	Description
User Tags	Cisco IOS XR Release 25.1.1	You can now add user tags to a chassis, module, PPM, interfaces, or OXC from the **User Tag** tab on the **Fault Monitoring** page. The added tags appear in the **User Tag** column of the alarms list. User tags streamline the identification and management of geographic locations and equipment across network sites where alarms are triggered.

User tags are identifiers that simplify the management of a chassis and its components within a network hierarchy, ensuring efficient location and equipment tracking.

Key features of user tags

User tags provide several functionalities to enhance alarm management and location tracking:

- **Alarm identification:** User tags assist in identifying a chassis, module, PPM, interface, or OXC when alarms are raised.
- **Tree structure representation:** The **User Tag** tab displays chassis and their components in a tree structure. You can expand or collapse items by clicking the chassis or component name, or the "+" or "-" icon.
- **CLLI application:** User tags apply CLLI (Common Language Location Identifier), a standardized 11-character code that uniquely identifies geographic locations and equipment for network sites, network support sites, and customer locations.

User tag inheritance

To ensure consistent tagging within a network hierarchy, user tags follow specific inheritance rules:

- User tags propagate from parent to child components of a chassis by default.
- A user tag assigned to a child component overrides the inherited tag from its parent.

Create user tags

Add user tags to devices, such as chassis, modules, PPMs, interfaces, or OXCs, to streamline identification and management of equipment across network sites with active alarms.

Use this task to create user tags to quickly identify the affected device.

Before you begin

Log into Cisco Optical Site Manager, on page 1

Procedure

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

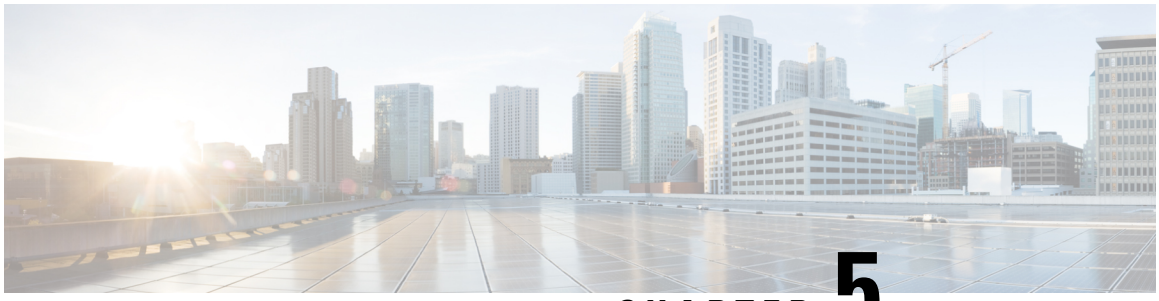
Step 2 Click the **User Tag** tab.

Step 3 Click the **Edit** button.
You can now edit the tag fields corresponding to the devices in the list.

Step 4 Type the tag name corresponding to the site, rack, chassis, or device, and press **Enter**.

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

View the tag name in the **User Tag** column under the **Alarms** tab to easily identify the affected device.

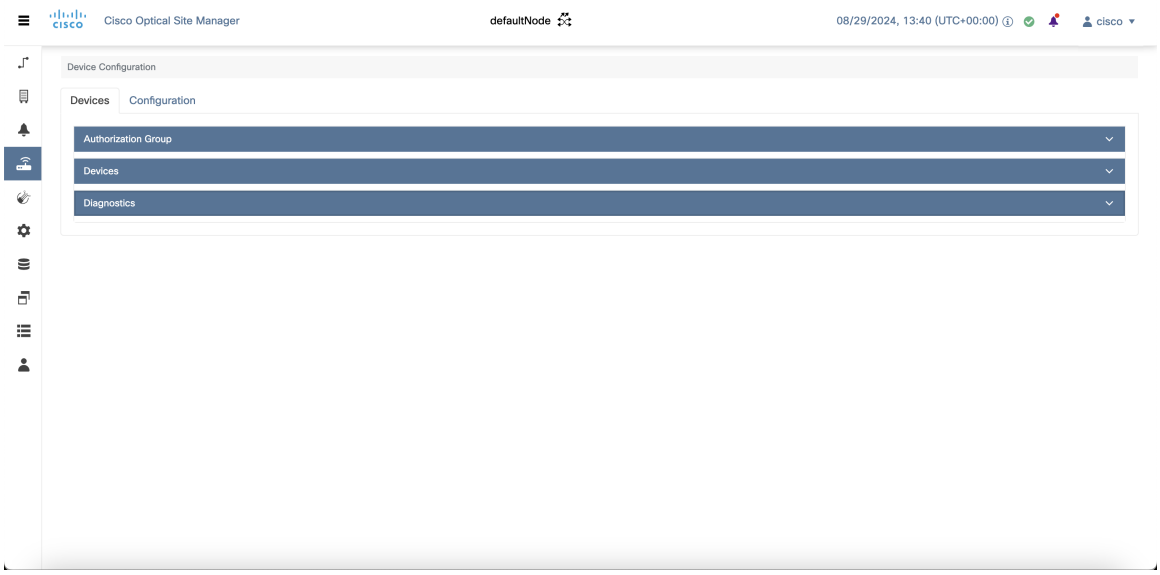


CHAPTER 5

Configure Devices

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

Figure 9: Configure Devices



- Create or edit an authorization group, on page 47
- Add a device, on page 49
- Retrieve device diagnostics, on page 57
- SOCKS Proxy, on page 58
- Change the Cooling Profile Control, on page 59
- SVO-LC device onboard in R25.1.1, on page 59

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

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

The authorization group table reflects your changes.

Add a device

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

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

Figure 10: 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 19: 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 20: Feature History

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

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

Before you begin

Log into Cisco Optical Site Manager, 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. **b.** Select **Delete**.
Move a device to a different rack unit	**a.** Right-click the unmanaged or passive device in the rack and select **Cut**. **b.** Right-click an empty rack unit and select **Paste**.
View device properties	**a.** Right-click the unmanaged or passive device in the rack and select **Properties**.

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

What to do next

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

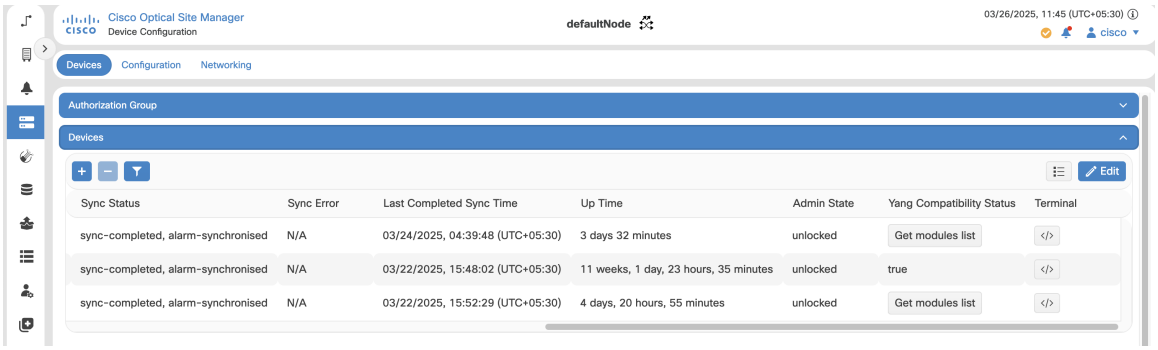
Manage a device using IOS XR CLI

Table 21: Feature History

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

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

Figure 11: Manage a Device Using IOS XR CLI



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

Before you begin

Log into Cisco Optical Site Manager, on page 1

Procedure

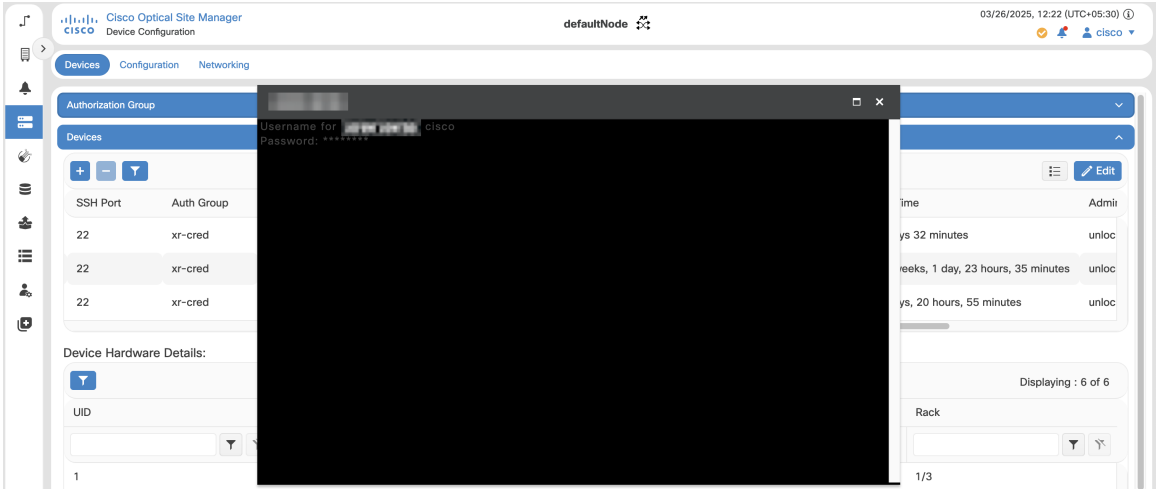
Step 1 Click **Devices** in the left panel.
The *Device Configuration* page appears.

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

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

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

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



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

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

Move a device or view device properties

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

Before you begin

Log into Cisco Optical Site Manager, 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**. **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. **b.** Select the check box corresponding to the devices you want to delete. **c.** Click **Delete Device(s)**. **d.** Confirm the action when prompted.
Delete an authorization group	**a.** Click the **Username and Password** section. **b.** Select the check box corresponding to the authorization groups you want to delete. **c.** Click the - button to delete the authorization group. **d.** Confirm the action.

A confirmation message appears.

Step 3 Click **Yes**.

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

Retrieve device diagnostics

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

Follow these steps to retrieve and download the device diagnostics:

Before you begin

Log into Cisco Optical Site Manager, 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.

SOCKS Proxy

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

Benefits

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

Limitations

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

Change the Cooling Profile Control

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

Before you begin

Log into Cisco Optical Site Manager, on page 1

Procedure

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

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

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

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.

SVO-LC device onboard in R25.1.1

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

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

Configure additional route for NCS 1000 device

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

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Select the NCS 1000 device to be connected.

Procedure

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

Step 2 Click the **Networking** tab.

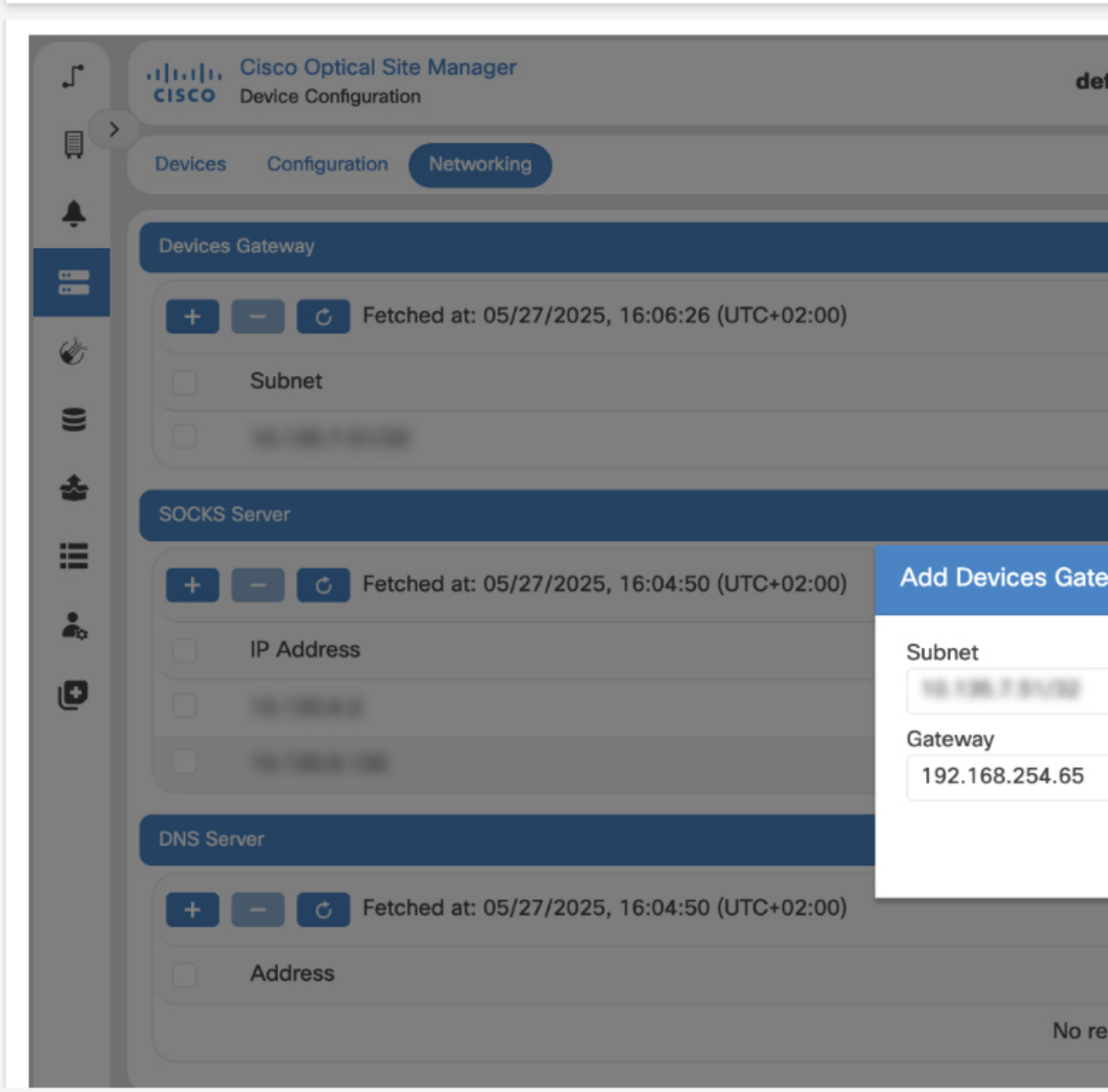
Step 3 Click the **Add Devices Gateway** icon under **Devices Gateway**.
The **Add Devices Gateway** dialog box appears.

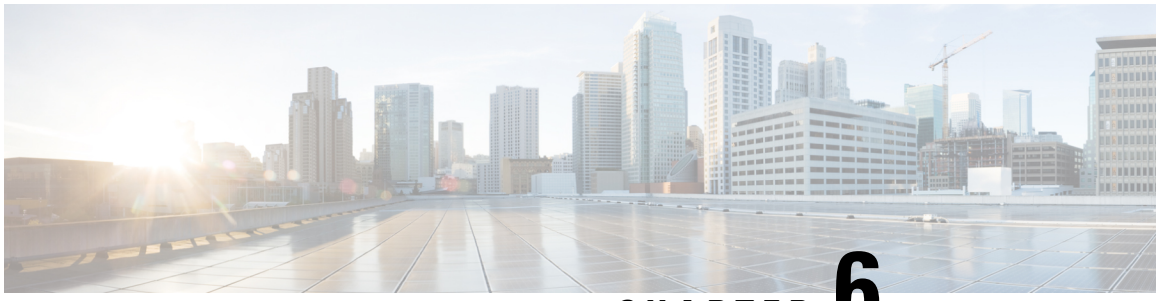
Step 4 Enter the **Subnet** and **Gateway** IP address, and click **Apply**.

The default Gateway IP address is 192.168.254.65

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

Figure 12: Add Devices Gateway



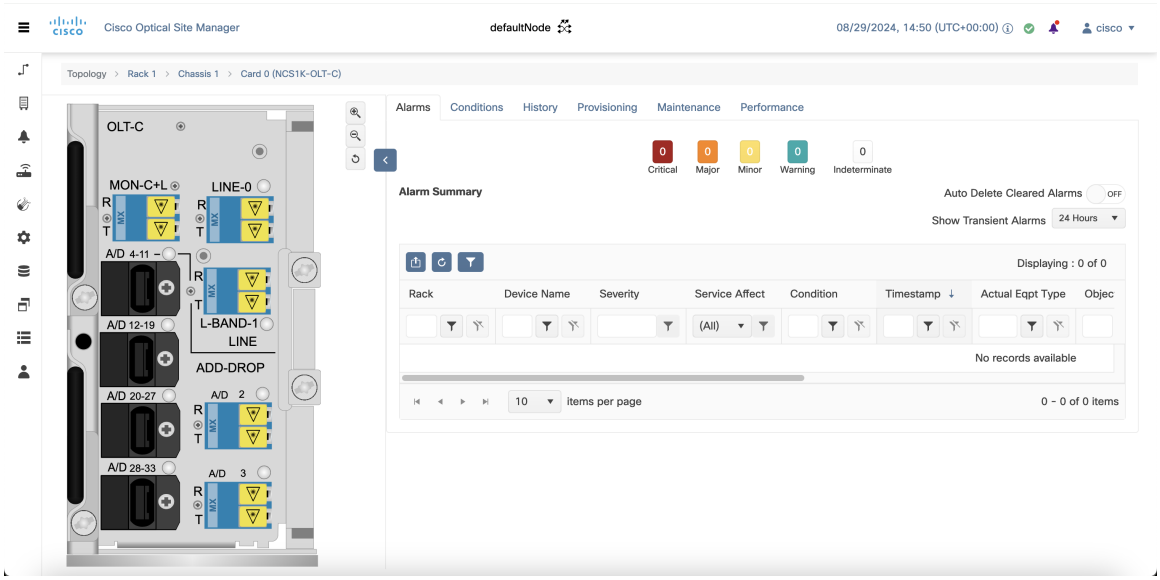


CHAPTER 6

Provision Line Cards

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

Figure 13: Provision Line Cards



- Supported NCS 1000 line cards, on page 64
- Configure the administrative state of Pluggable Port Modules and line cards, on page 65
- Open the card view, on page 65
- Provision an NCS 1000 or NCS 2000 card, on page 66
- NCS 1000 line card modes, on page 67
- Configuring card modes for NCS 2000 line cards, on page 80
- Reset a line card, on page 90
- Provision SONET or SDH trace monitoring, on page 91
- Provision trail trace monitoring, on page 92
- Provision ODU interfaces, on page 94
- Provision OTU interfaces , on page 95
- Provision Ethernet interfaces, on page 97
- Provision SONET or SDH Interfaces, on page 99

- Provision optical channels, on page 102
- Change Trunk Port Parameters, on page 105
- Provision optical threshold settings, on page 105
- Configure G.709 thresholds , on page 107
- Provision FEC thresholds, on page 108
- Configure RMON thresholds, on page 109
- Configure loopback interfaces, on page 110
- Configure optical safety, on page 111
- Configure thresholds for SONET or SDH, on page 113
- Enable attention LED, on page 114
- PSM card protection mechanism, on page 116
- View performance monitoring parameters, on page 118
- SVO Card, on page 119
- View UDC details, on page 124
- View Insertion Loss Parameters, on page 125
- Manage the Protection Group, on page 125
- Provisioning Optical Amplifier Cards, on page 127
- Retrieve MAC Addresses through LLDP, on page 135
- Provision FPD Upgrade for the Ports, on page 136
- Provision FPD Upgrade for MR-MXP Card, on page 137
- Enable Proactive Protection, on page 138
- Provision ODU Circuit, on page 140
- Functional Module Group, on page 141
- Provision ZR Plus Interfaces, on page 144
- Provision ZR Plus Interfaces, on page 145
- Provision ZR Plus Trail Trace Monitoring, on page 146
- Provision ZR Plus Trail Trace Monitoring, on page 146
- Provision Pluggable Ports, on page 147
- View Circuit Protection Parameters, on page 148
- NCS 2000 Cards, on page 150

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

Configure the administrative state of Pluggable Port Modules and line cards

Use this task to configure the administrative state of ports on Pluggable Port Modules (PPM) and line cards.

Pluggable port modules extend the port capacity of line cards in Cisco Optical Site Manager.

You can provision ports on PPM or line cards by setting their administrative state, which determines whether the ports are operational or shut down.

- Administrative state changes take effect immediately after the configuration is applied.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Follow these steps to provision PPM ports or a line card in Cisco Optical Site Manager.

Procedure

Step 1 Click the **Provisioning** tab.

Step 2 Click the **Pluggable Port Modules** section to expand it.

Step 3 Click **Edit**.

The fields in the table become editable.

Step 4 Select an administrative state from the **Admin State** column and click **Apply**.

Alternatively, you can also right-click a PPM or a line card in the rack from the **Topology** page, and choose **Change Admi State** to change the administrative state.

The ports on the pluggable port module or line card become operational or non-operational based on the selected administrative state.

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.

Provision an NCS 1000 or NCS 2000 card

Add a card from the chassis view by using the provisioning option that matches the card configuration.

- Add a card without configuring a card mode.
- Add an NCS 2000 line card and configure the card mode by using the Card Configuration Wizard.

Use **Module Provision** to add an NCS 1000 or NCS 2000 card without assigning a card mode.

Use **Advanced Provision** to add an NCS 2000 line card with a specific operating mode or sub operating mode. The Card Configuration Wizard shows the supported card-mode options based on the primary module that you select.

Before you begin

- Log in to Cisco Optical Site Manager. For more information, see Log in to Cisco Optical Site Manager.
- Open the chassis or card view for the device.

Follow these steps to provision an NCS 1000 or NCS 2000 card.

Procedure

Step 1 Right-click the empty slot where you want to add the card.

Step 2 Choose how to provision the card.

Table 22: Card provisioning options

If...	Then...
You want to add a card without configuring a card mode	**a.** Select **Module Provision**. **b.** Select the required card from the **Select Module** drop-down list. **c.** Click **Provision**.
You want to add an NCS 2000 line card and configure a card mode	**a.** Select **Advanced Provision**. **b.** On the **Add Primary Module** page, select a card from the **Primary Module** drop-down list, and click **Next**. **c.** Complete the card-mode workflow. For details, see Configuring card modes for NCS 2000 line cards, on page 80.

Cisco Optical Site Manager adds the card to the selected chassis slot. If you used **Advanced Provision**, the card uses the card-mode configuration that you completed in the Card Configuration Wizard.

What to do next

Verify that the card appears in the chassis view with the expected inventory and operational state.

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 23: Features introduced in R25.4.1

Feature Name	Release Information	Description

Support for NCS1K14-EDFA2 card in Cisco Optical Site Manager	Cisco IOS XR Release 25.4.1	Cisco Optical Site Manager now supports the NCS1K14-EDFA2 card. To use the EDFA2 card, set the optical type to ROADM. The EDFA2 card supports these pluggables and passive modules: • ONS-SC-PTP-1510: Optical Supervisory Channel (OSC) pluggable • ONS-QSFP-OTDR: Optical Time-Domain Reflectometer (OTDR) pluggable • DP01QSDD-ZT5-A1: Coherent probe pluggable • NCS1K-MD-32O-CE: 32-channel Odd Mux/Demux Patch Panel, C-band Enhanced • NCS1K-MD-32E-CE: 32-channel Even Mux/Demux Patch Panel, C-band Enhanced This integration enables comprehensive Operations, Administration, and Maintenance (OAM) capabilities for the card within Cisco Optical Site Manager. The Cisco Optical Site Manager supports only these capabilities: • Inventory • Alarms and alarm history • Provisioning (Amplifier, ZRPlus Interfaces, Interface, Ethernet Interfaces, and Optical Channel) • Performance monitoring and TCA (Threshold crossing alerts) • Maintenance (Live Data, Environmental Monitoring, and Power Monitoring) • Optical Degrees, Internal patchcord (IPCs), Network Function Virtualization (NFV)
Additional Trunk Rates for the NCS1K14-2.4T-X-K9 Card	Cisco IOS XR Release 25.4.1	The **Select Card Mode** page of the **Card Configuration Wizard** has been updated to configure these trunk rates in the muxponder mode for 2x100-GE client traffic: • 400G • 500G • 600G

Table 24: Features introduced in R25.4.1

Feature Name	Release Information	Description

Support for NCS1K14-EDFA2 card in Cisco Optical Site Manager	Cisco IOS XR Release 25.4.1	Cisco Optical Site Manager now supports the NCS1K14-EDFA2 card. To use the EDFA2 card, set the optical type to ROADM. The EDFA2 card supports these pluggables and passive modules: • ONS-SC-PTP-1510: Optical Supervisory Channel (OSC) pluggable • ONS-QSFP-OTDR: Optical Time-Domain Reflectometer (OTDR) pluggable • DP01QSDD-ZT5-A1: Coherent probe pluggable • NCS1K-MD-32O-CE: 32-channel Odd Mux/Demux Patch Panel, C-band Enhanced • NCS1K-MD-32E-CE: 32-channel Even Mux/Demux Patch Panel, C-band Enhanced This integration enables comprehensive Operations, Administration, and Maintenance (OAM) capabilities for the card within Cisco Optical Site Manager. The Cisco Optical Site Manager supports only these capabilities: • Inventory • Alarms and alarm history • Provisioning (Amplifier, ZRPlus Interfaces, Interface, Ethernet Interfaces, and Optical Channel) • Performance monitoring and TCA (Threshold crossing alerts) • Maintenance (Live Data, Environmental Monitoring, and Power Monitoring) • Optical Degrees, Internal patchcord (IPCs), Network Function Virtualization (NFV)
Additional Trunk Rates for the NCS1K14-2.4T-X-K9 Card	Cisco IOS XR Release 25.4.1	The **Select Card Mode** page of the **Card Configuration Wizard** has been updated to configure these trunk rates in the muxponder mode for 2x100-GE client traffic: • 400G • 500G • 600G

Table 25: Features introduced in R25.3.1

Feature Name	Release Information	Description

Additional Card Modes for OTN-XP Card	Cisco IOS XR Release 25.3.1	The **Card Configuration Wizard** now supports configuring these card modes for NCS1K4-OTN-XP card: • 400G-TXP-DD • 4x100GE-MXP-DD • OTU-CN-REGEN

Table 26: Features introduced in R25.1.1

Feature Name	Release Information	Description
Additional Trunk Rates for the NCS1K14-2.4T-X-K9 Card	Cisco IOS XR Release 25.1.1	The **Select Card Mode** page of the **Card Configuration Wizard** has been updated to configure these trunk rates in the muxponder mode for 2x100-GE client traffic: • 800G • 900G • 1000G • 1100G
Additional Card Modes for OTN-XP Card	Cisco IOS XR Release 25.1.1	The **Card Configuration Wizard** now supports configuring these card modes for NCS1K4-OTN-XP card: • FC-MXP • MXP-4x100G-TXP-400G with 400GE and 100GE/OTU4 client rates Additionally, you can configure the OC192 and STM64 client datarates for the MXP-40X10G-4X100G card mode in the 40x10G HM configuration.
Support for 1.2T Cards	Cisco IOS XR Release 25.1.1	The **Card Configuration Wizard** now supports configuration of card mode for these cards: • NCS1K4-1.2T-K9 • NCS1K4-1.2TLCW-K9

Feature Name	Release Information	Description

Support for NCS 2000 Cards	Cisco NCS 2000 Release 25.1.1	The **Card Configuration Wizard** now supports these cards and their operating modes:
		• 10x10G-LC
		  • TXP-10G
		  • RGN-10G
		• 10x10G + 200G-CK-C
		  • MXP-10x10G
		• 200G-CK-C
		  • TXP-100G
		  • RGN-100G
		• 400G-XP-LC
		  • MXP
		  • RGN-100G
		  • RGN-200G
		• NCS2K-1.2T-MXP
		  • TXPMXP

Table 27: 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. You can also use the wizard to configure these trunk rates in the muxponder mode: • 100-GE client traffic for 600-G and 1000-G • 500-G and 900-G

Feature Name	Release Information	Description
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: • 10G-GREY-MXP • 40x10G-4x100G-MXP You can also use the wizard to configure card mode for the NCS1K4-2-QDD-C-K9 card.

Table 28: 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:

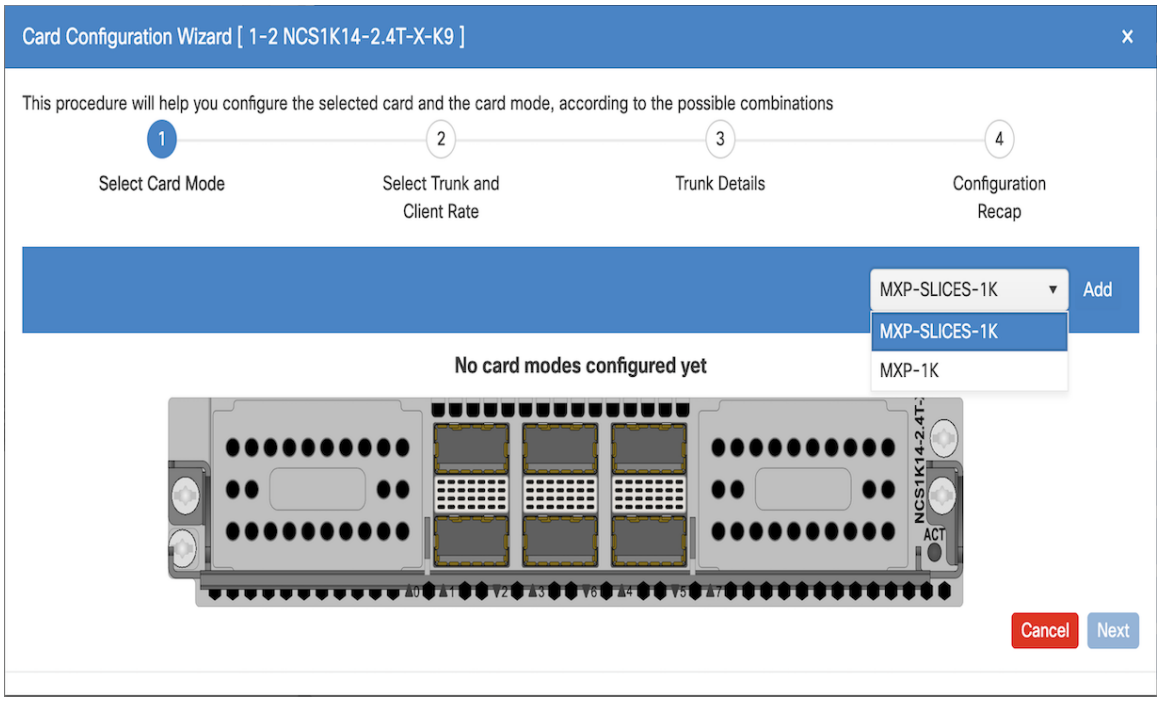
1. Select a card mode, on page 73
2. Select trunk and client data rate, on page 74
3. Add Internal Patch Cords, on page 76

   The Internal PC page is available only when the optical type is configured as ROADM.
4. Add trunk details, on page 77
5. Verify configuration details, on page 79

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 14: 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. **b.** Click **Card Mode**. **c.** Select **Install**.	**a.** Click the **Provisioning** tab. **b.** Click the **Card Modes** section to expand it. **c.** Click the **Add Card mode** button.

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

Table 29: 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

Step 3 Click **Next**.

The card mode is added

What to do next

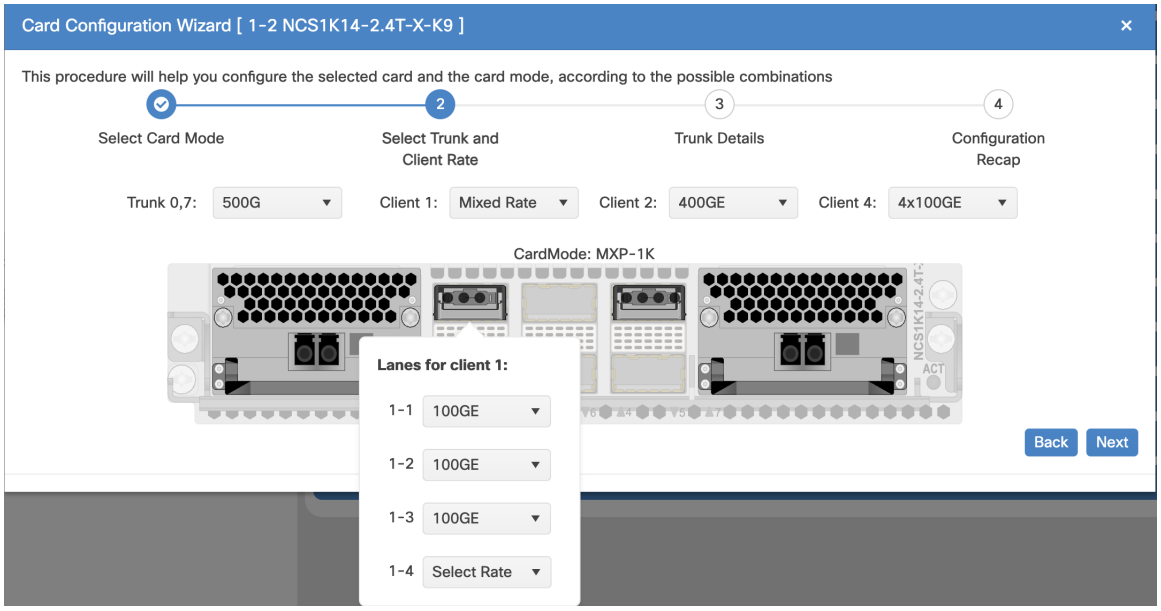
Select the Trunk and Client Data Rates.

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 15: Select Trunk and Client Data Rate



Before you begin

Select a card mode, on page 73

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 30: 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**. **Mixed rate configuration** information message is displayed. **b.** Close the message box. **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

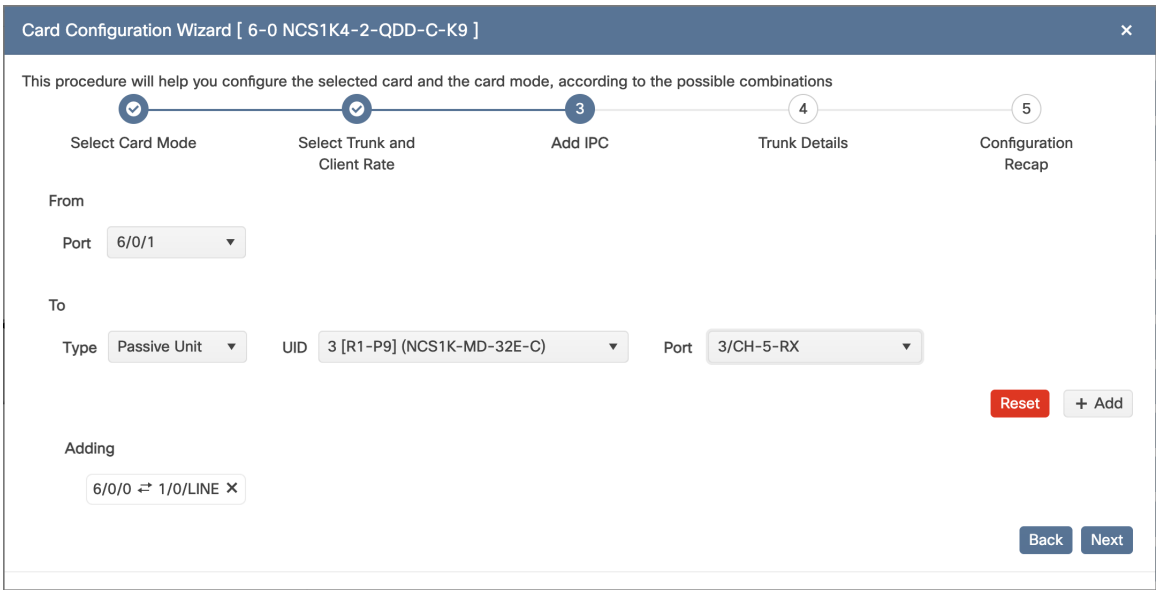
If optical type is	then
txp	Add trunk details, on page 77
roadm	Add Internal Patch Cords, on page 76

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 16: Add IPC



Before you begin

Select trunk and client data rate, on page 74

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 31: IPC drop-down lists displayed based on device type

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

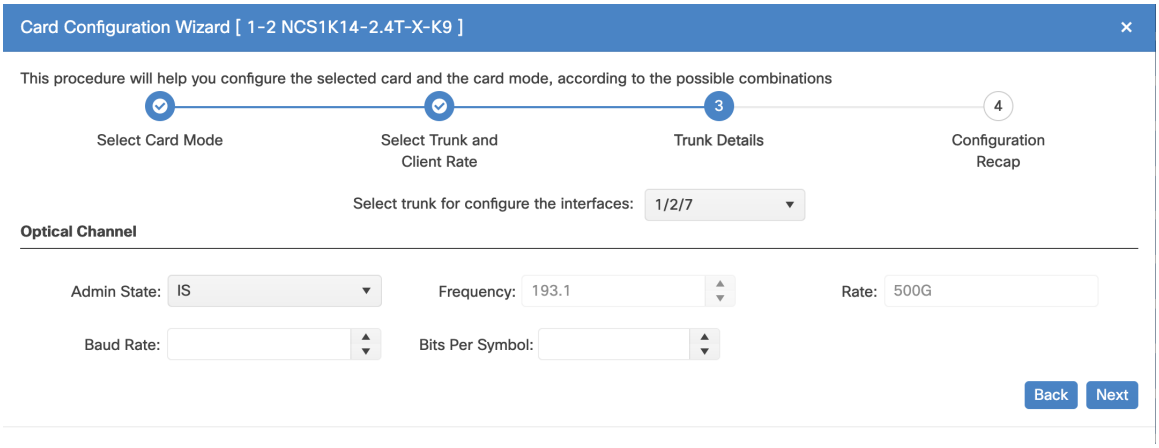
Add the Trunk Details to configure the interfaces.

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 17: Add Trunk Details



Before you begin

If optical type is configured as	then ensure
roadm	Add Internal Patch Cords, on page 76
txp	Select trunk and client data rate, on page 74

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

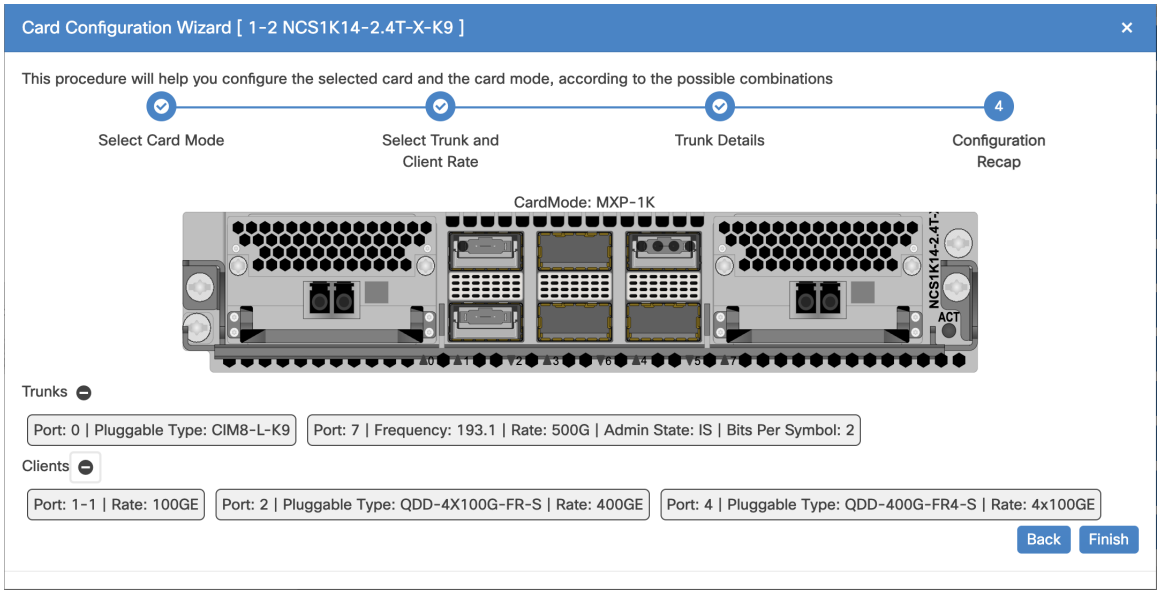
Verify configuration details, on page 79

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 18: Verify Configuration Details



Before you begin

Add trunk details, on page 77

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. **b.** Click **Card Mode**. **c.** Select **Install**.	**a.** Click the **Provisioning** tab. **b.** Click the **Card Modes** section to expand it. **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 74.

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

Configuring card modes for NCS 2000 line cards

You can configure NCS 2000 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

Configuring card modes for NCS 2000 line cards enables optimized data processing and traffic management by selecting the operational mode and setting relevant parameters.

- **NCS 2000 line card**: Provides multiple operational modes such as Muxponder and Slice to manage client-to-trunk mapping.
- **Card Configuration Wizard**: A tool within Cisco Optical Site Manager that guides the user through the configuration steps.
- **Cisco Optical Site Manager**: The management interface where the configuration workflow is executed.

For details about the supported card modes for Cisco NCS 2000 cards, including peer-card requirements and client-to-trunk port mappings, see Supported operating modes and port mapping details for NCS 2000 cards, on page 87.

Note When configuring the **MXP-4x100G-TXP-400G** or **10G-Grey-MXP** operation modes on an OTN-XP card via Cisco Optical Site Manager (COSM), consider these synchronization behaviors:

- **Partial configuration (Mode only)**: If you apply the operation mode without defining the associated slice, trunk, or client configurations, the mode will be applied to both COSM and IOS-XR. However, if you later delete this mode from COSM, it will be removed from the COSM interface but will remain in the IOS-XR configuration, resulting in a synchronization discrepancy.
- **Full configuration (Mode + Slice/Trunk/Client)**: If you configure the operation mode alongside its required slice, trunk, and client settings, the deletion process will correctly propagate, removing the configuration from both COSM and 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.

Workflow

The process involves these stages:

1. Select the required card mode for the NCS 2000 line card. For details, see Select a card mode for an NCS 2000 line card, on page 81.
2. Add secondary modules for the selected card mode. For details, see Add secondary modules, on page 83.
3. Add pluggable modules to the required ports. For details, see Add pluggable modules to ports, on page 85.
4. Verify configuration details and complete the wizard. For details, see Verify card configuration details, on page 85.

Result

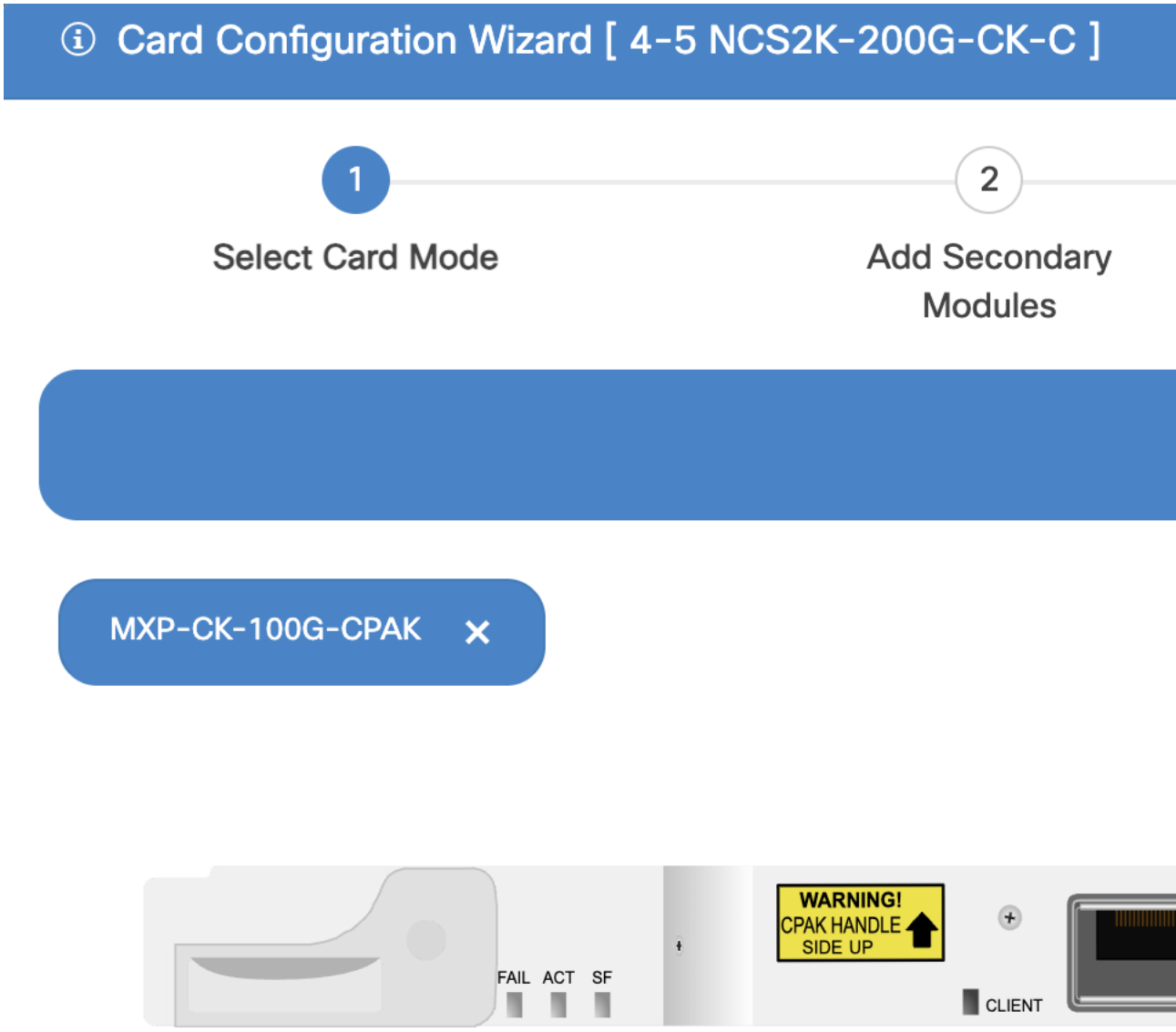
The line card is configured in the selected operational mode.

Select a card mode for an NCS 2000 line card

Set the operational behavior for an NCS 2000 line card. Choose the card mode that matches your deployment requirement.

The **Card Configuration Wizard** in Cisco Optical Site Manager provides an interface for selecting card modes. The selected card mode determines which functions and capabilities are enabled for the line card.

Figure 19: Select card mode



Before you begin

Log into Cisco Optical Site Manager, on page 1

Follow these steps to open the **Card Configuration Wizard** and select a card mode for an NCS 2000 line card.

Procedure

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

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

Step 2 From the drop-down list, select the card mode, and then click **Add**.

Step 3 Click **Next**.

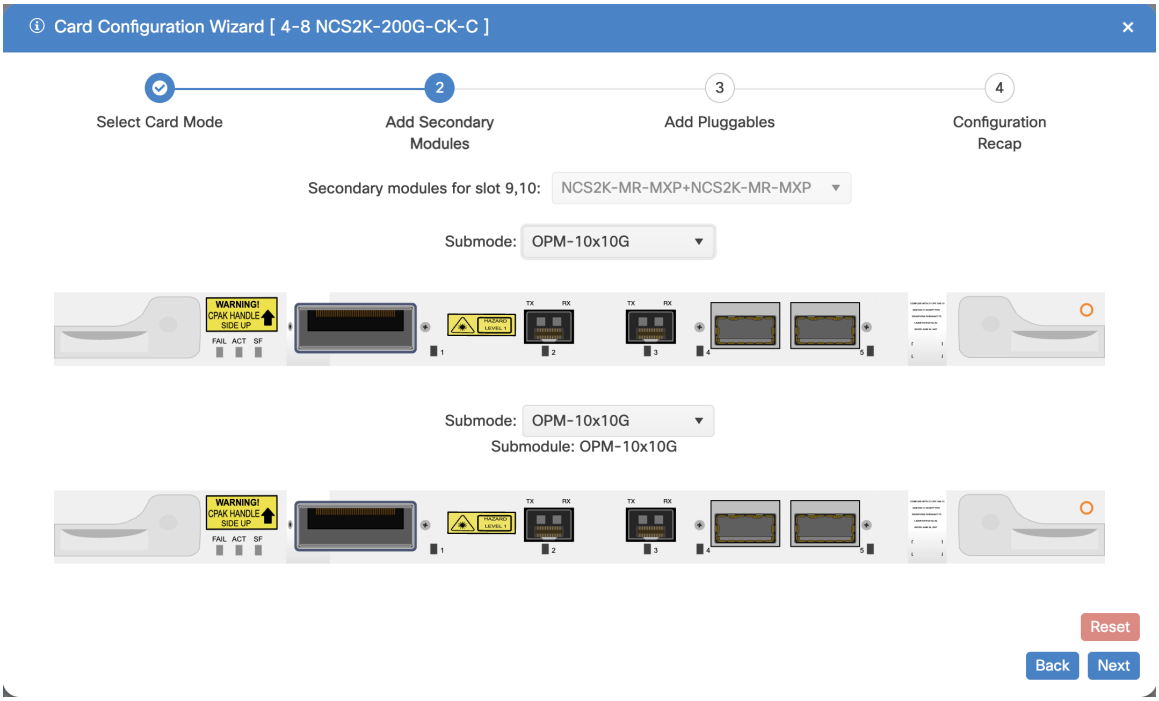
What to do next

Add secondary modules, on page 83

Add secondary modules

Use this task to add a secondary module in the **Card Configuration Wizard** for the selected card mode. A secondary module is an add-on hardware module for the NCS 2000 line card that expands interface capacity based on the selected card mode.

Figure 20: Add secondary modules



Before you begin

Select a card mode for an NCS 2000 line card, on page 81

Follow these steps to add a secondary module for an NCS 2000 line card:

Procedure

Step 1 From the **Secondary modules for slot** drop-down list, select the required secondary module.

This drop-down list is only enabled if the supported secondary modules are available for the card.

Step 2 Select a submode for all slots from the **Submode** drop-down list.

This drop-down list is enabled only when the supported sub modes are available for the card.

Step 3 Click **Next**.

The selected secondary module is added.

What to do next

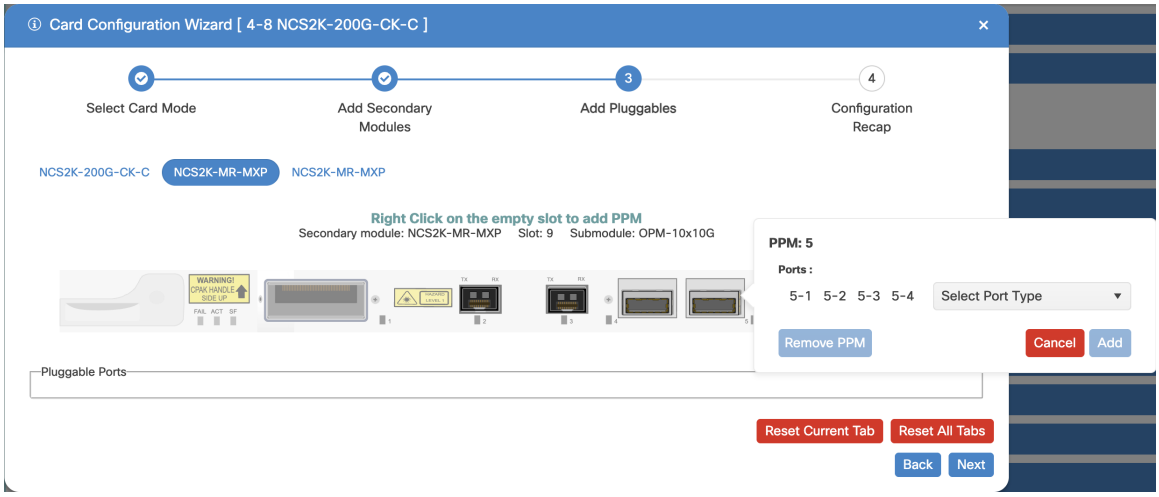
Add pluggable modules to ports, on page 85

Add pluggable modules to ports

Add pluggable modules to the required ports to expand or update the card capabilities.

Use the Card Configuration Wizard to assign or remove pluggable modules (PPMs) on specific ports during the card setup or modification process.

Figure 21: Add pluggable modules



Before you begin

Add secondary modules, on page 83

Procedure

Step 1 Right-click a port and select the PPM from the **Select Port Type** drop-down list.

Step 2 Click **Add** to assign the PPM to the selected port.

Step 3 If you need to remove a module, click **Remove PPM**.

Step 4 Repeat steps 1 through 3 for each port you want to configure.

Step 5 Click **Next**.

The selected pluggable modules are added to the ports.

What to do next

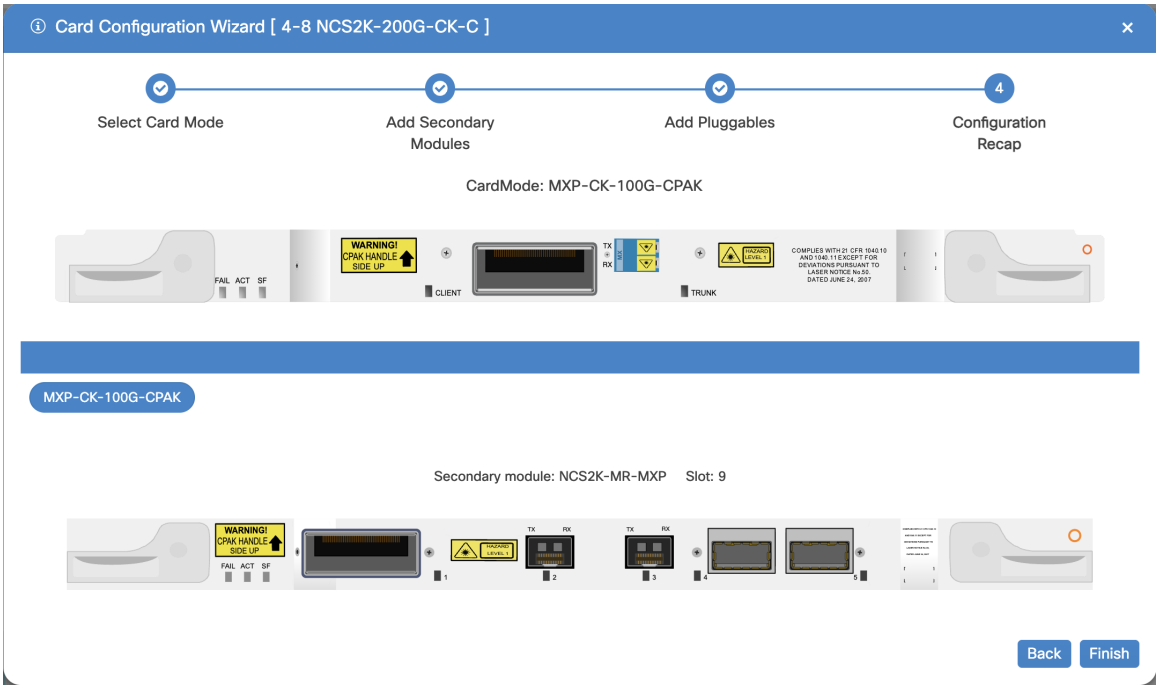
Verify card configuration details, on page 85

Verify card configuration details

Ensure that the card configuration, including card mode, secondary modules, and port module assignments, is correct before completing the wizard.

In the **Card Configuration Wizard**, verify the configuration in the **Configuration Recap** window.

Figure 22: Verify configuration details



Before you begin

Add pluggable modules to ports, on page 85

Follow these steps to verify card configuration details and complete the Card Configuration Wizard:

Procedure

Step 1 Verify the card mode displayed in the **Configuration Recap** window.

Step 2 Verify secondary modules and slot details.

Step 3 To verify the PPM and pluggable port assignments, expand the **Pluggable Port Modules** and **Pluggable Ports**.

Step 4 Click **Finish**.

The system saves the card configuration with the verified settings.

Configure card mode on a NCS 2000 control card

Add a card mode to an NCS 2000 controller card in Cisco Optical Site Manager to enable switching between supported control card modes.

Control cards support multiple card modes that determine how the card processes payloads.

You can configure the operating mode based on the type of control card installed in the shelf.

- TNC is the default operating mode.

- TNCO mode is required when a TNCS-O card is installed.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Follow these steps to provision an operating mode on a control card.

Procedure

Step 1 Click the **Provisioning**, then click **Card Modes** tabs.

Step 2 Select **TNC-MODE** or **TNCO-MODE**, then click **Apply**.

The control card can operate in either TNC or TNCO mode.

- TNC mode is the default operating mode.
- TNCO mode is required when a TNCS-O card is installed.

The operating mode is provisioned on the control card.

Supported operating modes and port mapping details for NCS 2000 cards

Use this reference to identify supported operating modes, valid peer-card combinations, and port mapping details for Cisco NCS 2000 cards before configuring card modes in Cisco Optical Site Manager.

Supported card modes for NCS 2000 cards

This table lists the operating modes that are supported on the NCS 2000 cards.

Table 32: Supported Card modes for NCS 2000 cards

Card	Operating mode	Peer cards	Client-trunk ports
MR-MXP	TXP-100G	200G-CK-LC card or 100GS-CK-C card	Not applicable
	MXP-100G	200G-CK-LC card or 100GS-CK-C card	Not applicable
	100G-B2B-CPAK	MR-MXP	CPAK
	100G-B2B-SFP-QSFP	MR-MXP	2xSFP+2xQSFP
	MXP-2X40G-2X10G	200G-CK-LC	Not applicable

Card	Operating mode	Peer cards	Client-trunk ports	
100G-CK-C	TXP-100G	Not applicable	Not applicable	
	RGN-100G	100G-CK-C, 100G-LC-C	Not applicable	
	MXP-2x40G	Not applicable	Not applicable	
100G-LC-C	TXP-100G	Not applicable	Not applicable	
	RGN-100G	100G-LC-C, 100G-CK-C	Not applicable	
	100GS-CK-C	TXP-100G	Not applicable	Not applicable
RGN-100G		200G-CK-LC or 100GS-CK-C	Not applicable	
MXP-CK-100G-SFP-QSFP		MR-MXP	2xSFP+2xQSFP	
MXP-CK-100G-CPAK		MR-MXP	CPAK	
MXP-200G		MR-MXP. Skip card is MR-MXP.	Not applicable	
MXP-10x10G-100G		10x10G-LC + MR-MXP. Skip card is MR-MXP.	Not applicable	
10x10G-LC	MXP-10x10G	100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C	Not applicable	
	RGN-10G	Not applicable	1-2, 3-4, 5-6, 7-8, 9-10	
	TXP-10G	Not applicable	1-2, 3-4, 5-6, 7-8, 9-10	
	Low Latency	Not applicable	1-2, 3-4, 5-6, 7-8, 9-10	
	Fanout-10X10G	Not applicable	Not applicable	
	TXPP-10G	Not applicable	3-4-6, 7-8-10	
	MXP-10x10G	100G-LC-C 400G-XP-LC	Client ports: 1 to 10 Trunk port:	

Card	Operating mode	Peer cards	Client-trunk ports
200G-CK-LC	TXP-100G	Not applicable	Not applicable
	RGN-100G	200G-CK-C or 100GS-CK-C	Not applicable
	MXP-200G	MR-MXP. Skip card is MR-MXP. OPM-10x10G or OPM-2x40G-2x10G sub OpMode is required.	Not applicable
	MXP-CK-100G-CPAK	MR-MXP	CPAK
	MXP-CK-100GSFP-QSFP	MR-MXP	2xSFP+2xQSFP
	MXP-10x10G-100G	10x10G-LC + MR-MXP	Not applicable
CFP-LC	CFP-TXP	One or two 100G-LC-C, 100G-CK-C	Not applicable
	CFP-MXP	Only one 100G-LC-C, 100G-CK-C	Not applicable
	REGEN-200G	Not applicable	No slices
	REGEN-100G	Not applicable	No slices
	MXP-2x150G	Not applicable	Three slices
	MXP	Not applicable	Four slices

Port pair configuration for 10x10G-LC cards

Use the operating mode data to validate card behavior and port mapping before deployment.

Table 33: Port pair configuration for 10x10G-LC cards

Configuration Aspect	Description
Supported Modes	The 10x10G-LC card supports a maximum of five TXP-10G modes, two TXPP-10G modes, five RGN-10G modes, five Low Latency modes, or a combination of five TXP-10G, RGN-10G, and Low Latency modes.
TXPP-10G Client Ports	For TXPP-10G mode, client ports can be port 3, port 7, or both.
TXPP-10G Trunk Ports (Client Port 3)	When port 3 is selected as the client port, ports 4 and 6 can be selected as trunk ports.
TXPP-10G Trunk Ports (Client Port 7)	When port 7 is selected as the client port, ports 8 and 10 can be selected as trunk ports.

NCS 2000 card mode details

This table describes the card mode for the for the 400G-XP-LC, 400G-XP, and 10x10G-LC cards.

Table 34: Card mode details for 400G-XP-LC, 400G-XP, and 10x10G-LC cards

Card	Operating mode or aspect	Description
400G-XP-LC and 400G-XP	REGEN-200G	Both trunk ports use the same 200G rate. The trunk configuration from CFP2-11 is copied to CFP2-12.
400G-XP-LC and 400G-XP	REGEN-100G	Both trunk ports use the same 100G rate. The trunk configuration from CFP2-11 is copied to CFP2-12.
400G-XP-LC and 400G-XP	MXP-2x150G	Both trunk ports are configured for 150G.
400G-XP-LC and 400G-XP	OTNXC	Supported operating mode for these card types.
400G-XP-LC and 400G-XP	MXP	Supported operating mode for these card types.
10x10G-LC	Supported modes	The card supports up to five TXP-10G modes, two TXPP-10G modes, five RGN-10G modes, five Low Latency modes, or a supported combination of TXP-10G, RGN-10G, and Low Latency modes.
10x10G-LC	TXPP-10G client ports	Client ports can be port 3, port 7, or both ports.
10x10G-LC	TXPP-10G trunk ports with client port 3	When port 3 is the client port, trunk ports 4 and 6 are available.
10x10G-LC	TXPP-10G trunk ports with client port 7	When port 7 is the client port, trunk ports 8 and 10 are available.

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 SONET or SDH trace monitoring

Configure trace monitoring parameters for OC192 (SONET) and STM64 (SDH) payloads. This ensures proper monitoring of the trace strings transmitted and received on the optical network, helping detect discrepancies and maintain network integrity.

SONET and SDH trace monitoring is supported on OTN XP cards.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Follow these steps to provision the trace monitoring parameters that are supported for both the OC192 and STM64 payloads.

Procedure

Step 1 Click the **Provisioning** tab.

Step 2 Perform one of the following steps:

Table 35: Provision trace monitoring for SONET/SDH

To...	Click...
provision trace monitoring parameters for SONET	**SONET Trace Monitoring**
provision trace monitoring parameters for SDH	**SDH Trace Monitoring**

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

Step 4 Modify required settings as described in this table.

Table 36: SONET and SDH Trace Monitoring Parameters

Parameter	Description	Options
Port	Displays the port number.	—
Tx-String	Sets a new transmit string.	0–15 bytes
Expected-String	Sets a new expected string.	0–15 bytes
Rx-String	(Display only) Displays the current received string.	
Detect-Mode	Sets the mode for detecting the discrepancy between the expected and received trace.	• True • False
Trace-Format	Sets the format in which the received string is displayed.	• 1BYTE • 16BYTE • 64BYTE

Step 5 Click **Apply**.

After provisioning the SONET or SDH trace monitoring parameters, the system actively monitors the trace strings on the optical network.

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 65

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 37: 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: 0-64 bytes
Legacy Expected-TTI	Set the TTI value that the network device expects from the far end of the optical path. 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: • true • 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. • When this mode is enabled, the device does not compare the *Legacy Rx-TTI* to a pre-configured expected value. • Instead, it simply captures and shows the actual TTI being received from the remote end.	Available options: • Disabled • Enabled • SAPI • DAPI • 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 65

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_86 unique_86_Connect_42_ID9913, on page 94table.

Table 38: 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 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Parameter	Description	Options
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. Alternatively, an AIS can be invoked. 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 • 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 • 50 ms • 100 ms • 250 ms • 500 ms
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 65

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_87 unique_87_Connect_42_ID9913, on page 96 table.

Table 39: OTU Interface Settings

Parameter	Description	Options
Port	(Display only) Displays the port name.	—
Description	Displays the description of the port.	—
HD FEC	Sets the OTN lines to forward error correction (FEC).	• DISABLE_FEC • EFEC • EFEC_14 • EFEC_17 • HG_FEC_20 • HG_FEC_7 • STANDARD_FEC
Interop Mode	Enables interoperability between line cards and other vendor interfaces.	• InteropNone • InteropEnable
Supports Sync	(Display only) Displays the SupportsSync card parameter. If the value is true, the card functions as a NE timing reference.	• true • 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 • 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 • STU • G812T • G812L • SETS • DUS • PRS • ST2 • ST3E • ST3 • SMC • ST4 • RES • STU_SDH • DUS_SDH • SSM_FAILED • RES_SDH • 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 65

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 40: Ethernet Settings, on page 98 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 40: 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. • Default value: 1548 • Valid range: 64 – 9700
FEC	Sets the FEC mode. When set to On, FEC is enabled.	• NA • Auto (default) • On • Off
Duplex	Sets the expected duplex capability of ports.	• Full • Half
Mapping	Sets the mapping mode.	• CBR • GFP

Parameter	Description	Options
Auto Negotiation	Enables or disables auto-negotiation on the port.	• Disabled • Enabled
Squelch Mode	Sets the squelch mode.	• Disable • Squelch • 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 • 50 ms • 100 ms • 250 ms • 500 ms
Service State	Displays the service status of the port.	

Provision SONET or SDH Interfaces

Provisioning SONET or SDH interfaces involves configuring parameters for synchronous optical network (SONET) or synchronous digital hierarchy (SDH) interfaces on optical line cards. This action enables the transport of SONET or SDH signals over the network and supports payloads such as OC192 for SONET and STM64 for SDH.

Set the operational parameters that control signal quality monitoring, synchronization, and interface behavior. This ensures that the interfaces process and transport SONET/SDH signals correctly, maintain synchronization, handle signal failures, and support trace monitoring and threshold settings for performance management.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Follow these steps to provision the parameters for the SONET or SDH interfaces of a card.

Procedure

Step 1 Click the **Provisioning** tab.

Step 2 Perform one of these steps:

- Click the **SONET Trace Monitoring** section to provision interface parameters for SONET.
- Click the **SDH Trace Monitoring** section to provision interface parameters for SDH.

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

Step 4 Modify required settings as described in the Table 41: SONET or SDH Interface Parameters, on page 100 table.

Step 5 Click **Apply**.

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

Table 41: SONET or SDH Interface Parameters

Field	Description	Valid Values
Port	Displays the port number.	—
Description	Displays the port description. **Note** This parameter is not supproted for the OC192 and STM64 card modes.	—
Type	Displays the current payload for the port. OC192 is displayed for SONET systems and STM64 is displayed for SDH systems.	• OC192 • STM64
SF BER	Sets the signal fail (SF) bit error rate (BER).	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade (SD) bit error rate (BER).	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 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. Alternatively, an AIS can be invoked. **Note** This parameter is not supported for the OC192 and STM64 card modes.	• Squelch • AIS

Field	Description	Valid Values
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. **Note** This parameter is not supported for the OC192 and STM64 card modes.	• Disable • 50 ms • 100 ms • 250 ms • 500 ms
ProvidesSync	(Display only) Displays the ProvidesSync card parameter. **Note** This parameter is not supported for the OC192 and STM64 card modes.	• true • false
Send DoNotUse	When checked, sends a “Do Not Use for Synchronization (DUS)” message on the S1 byte. **Note** This parameter is not supported for the OC192 and STM64 card modes.	• true • false
Sync SyncMsgIn	Sets the ProvidesSync card parameter. Enables synchronization status messages, which allow the node to choose the best timing source. **Note** This parameter is not supported for the OC192 and STM64 card modes.	• true • false
Admin SSM	Overrides the synchronization status message (SSM) and the synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, it defaults to STU. **Note** This parameter is not supported for the OC192 and STM64 card modes.	• DUS • PRS • RES • SMC • ST2 • ST3 • ST3E • ST4 • STU • TNC

Field	Description	Valid Values
Termination Mode	Sets the termination mode. When a session is terminated, the signal is either reinitialized or passed through without any changes. For 400G-XP, 10x10G-LC, and OTU2-XP cards, the default mode is Transparent. For the 40E-MXP card, the default mode is Transparent but can be changed to other values as required. **Note** This parameter is not supported for the OC192 and STM64 card modes.	For SONET: • Transparent • Line • Session For SDH: • Transparent • Multiplex Section • Regeneration Section
Admin State	Sets the administrative state of the port.	—
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format:PrimaryState-PrimaryState Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance

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 65

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 42: Optical Channel Settings, on page 103 table.

Step 5 Click **Apply**.

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

Table 42: 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) • Locked, disabled (ETSI)/ OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/ OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)
Service State	Displays the service state.	—
Reach	Indicates the distance from one node to another node.	• Auto Provision • List of reach values

Parameter	Description	Options
SD FEC	Indicates the standard FEC.	• SD_FEC_15_DE_OFF • SD_FEC_15_DE_ON • SD_FEC_20 • SD_FEC_25_DE_OFF • SD_FEC_25_DE_ON • SD_FEC_7
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 • Enable • 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 • 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. **Note** You cannot configure this parameter if **Fixed Ratio** is already configured.	• Valid range: -19 dBm to +3 dBm • Default value: -2.0 dBm
Fixed Ratio	Sets the Rx VOA fixed ratio. **Note** 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 42: Optical Channel Settings, on page 103

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 65

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 43: Performance Monitoring Parameters, on page 106.
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 43: 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.

Use this parameter	to
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 65

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 44: G.709 PM Thresholds, on page 108.

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 44: 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.
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 65

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 65

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 45: RMON threshold parameters, on page 110.

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 45: RMON threshold parameters

Parameter	Description
Port ID	The identifier for the port that you configure the RMON threshold for.
Variable	The specific MIB variable to be sampled. This variable must be any of these ASN.1 primitive type: • INTEGER\ • Counter32 • Counter64 • Gauge • TimeTicks
Alarm Type	Indicates which threshold crossing triggers the alarm: • Rising • Falling • Rising or Falling
Sampling Type	The method used to sample the variable: • **Absolute**: the threshold to use the total number of occurrences, regardless of the time period • **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. **Note** 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 65
- 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 102.

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 65

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 46: Optical safety parameters for cards, on page 112 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 46: 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. • 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: • ALS-Disabled—Deactivates ALS. • 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. • 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. **Note** OSRI configuration is not supported on the transponder and muxponder cards.	From the drop-down list, choose one of the following: • OSRI-OFF • OSRI-ON
ALS Status	(Display only) ALS status of the device.	• Working • 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.	—

Configure thresholds for SONET or SDH

Configure threshold settings for SONET or SDH payload ports (OC192, STM64) to monitor performance and to maintain network integrity.

Perform this configuration on supported line cards (e.g., OTN XP, ADM-10G, MXP, and transponders) to enable performance monitoring.

This functionality is supported on Slice-0 of the 40x10 HM configuration of the MXP-40X10G-4X100G card mode.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Follow these steps to provision SONET or SDH thresholds for OC192 and STM64 payload ports on the OTN XP card.

Procedure

Step 1 Click the **Provisioning** tab.

Step 2 Perform one of the following steps:

- Click the **SONET Trace Monitoring** section to provision thresholds for SONET.
- Click the **SDH Trace Monitoring** section to provision thresholds for SDH.

Step 3 Select the interval of the threshold to *15 Min* or *24 Hour*.

Step 4 Click the plus icon to add a new SONET or SDH threshold.
The **New SONET/SDH Threshold** dialog is displayed.

Step 5 Select the required details in the **New SONET/SDH Threshold** dialog box as described in the Table 47: New SONET/SDH Threshold Dialog, on page 114 table.

Step 6 Click **Apply**.

The system applies the configured thresholds to generate alarms or notifications when performance metrics exceed defined limits, facilitating proactive network management and fault detection.

Table 47: New SONET/SDH Threshold Dialog

Field	Description	Valid Values
TCA Types	Select the interface name.	—
Interface	Select the interface name.	—
Granularity	Sets the threshold for intervals of either 15 minutes or 24 hours.	• 15min • 24Hour
Direction	Sets the direction.	• ES • SES • UAS • EB • SEFS
Location	Sets the low threshold value.	—
PM Type	Sets the PM type.	—
PM Type Extension	Sets the PM type extension.	—
Threshold Value	Sets the threshold value.	—

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 48: 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 65

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 • 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**. **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 65

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 65

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 65

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.

View performance monitoring parameters

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds, and report performance data for early problem detection. Users can retrieve current and historical PM counters for various controllers at several intervals.

PM for optical parameters includes laser bias current, transmit and receive optical power, mean polarization mode dispersion, accumulated chromatic dispersion, and received optical signal-to-noise ratio (OSNR). These parameters facilitate troubleshooting operations and enhance the data collected directly from the equipment.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Follow these steps to view the current and historical PM parameters of a card.

Procedure

Step 1 Click the **Performance** tab.

Step 2 Select the **Interface Type** and **Interface** for which you want to retreive the PM data.

Step 3 Select the **Granularity** to *15 Min* or *24 Hour*.

Step 4 Click **Get PM**.
The PM parameters are displayed on the table.

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

Step 6 Perform one of the following from the **Clear PM** drop-down list to clear the current PM parameters on the table:

- Select **Clear Current** to clear the current PM parameters collected on the card.
- Select **Clear All** to clear the current PM parameters collected on the card.

Caution Cleared event logs on a card are not recoverable.

The current and historical PM parameters of the selected card are displayed.

Table 49: Performance monitoring parameter fields

Use this drop-down	To	Valid values
Interface Type	Select the interface type of the card.	The options available are based on the selected card.
Interface	Select the interface of the card.	The options available are based on the selected interface type.
Granularity	Select the threshold value to retrieve performance monitoring parameters for the chosen time interval.	• 1 Min • 15 Mins • 1 Hour • 24 Hours
Location	Select the location.	• nearEnd • farEnd

SVO Card

In this chapter, "SVO" refers to the NCS2K-SVO-K9 card.

The Shelf Virtualization Orchestrator (SVO) card is a two-slot card, which allows better management and control of multichassis solutions for the Cisco NCS 2000.

Cisco Optical Site Manager extends the Network Services Orchestrator (NSO) application by network topology-aware virtualization, thereby improving the management of Cisco NCS 2000 through alarms, status and connection verifications, and so on.

SVO Card enables High Availability functionality by connecting the two SFP+ 10GE optics back-to-back with another SVO Card. You can also configure the card in Geo HA mode where two SVO-LCs are installed in separate NCS2000 nodes to ensure that redundancy is maintained if one of the NCS2000 nodes fails.

SVO Card has a powerful 12 core 2GHz Intel Xeon processor with 64GB DDR4 RAM, 240GB SSD, 4x SFP+ ports, 5x 1GE copper for External Switch, 2x USB 3.0 along with Ethernet management and Console port.

On the Cisco NCS 2015 shelf, the cards can be installed in slots 2 to 15.

The following pluggables on the four front panel ports.

SFP+ (10G)	SFP (1G)
ONS-SC+-10G-SR=	ONS-SI-GE-SX=
ONS-SC+-10G-LR=	ONS-SI-GE-LX=
SFP-10G-SR=	ONS-SE-ZE-EL=
SFP-10G-LR=	

The card has the features:

- Runs in complete redundancy mode with another standby SVO Card.
- Provides selfmonitored hardware status with on board logging.
- Provides virtualization of nodes in a network.

Installing the SVO Card

Note Install and configure the SVO card before installing any other line cards into the shelf assemblies.

When you install the SVO card on the chassis, the PWR-CON-LMT alarm is raised when the power consumption limit is exceeded. We recommend that you remove the SVO card and place it in another chassis that supports the required power.

Procedure

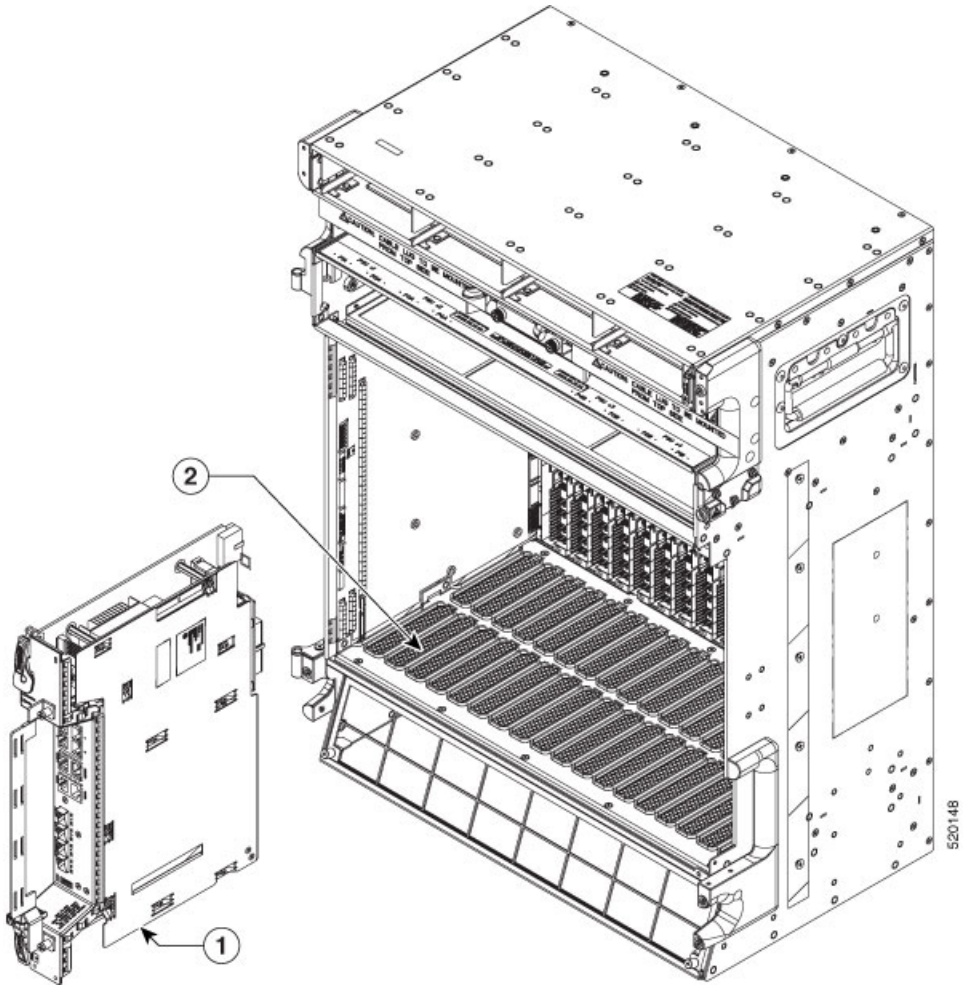
Step 1 Align the SVO card so the markings on the card and the chassis are on the same side.

Step 2 Open the latches or ejectors of the first SVO card that you will install.

Step 3 Use the latches or ejectors to firmly slide the card horizontally along the guide rails until the card plugs into the receptacle at the back of the slot (any slot from slot 2 to 6 in the shelf or slot 2 to 15 in the NCS 2015 shelf).

Step 4 Verify that the card is inserted correctly, and close the latches or ejectors on the card.

Figure 23: Installing SVO card on the NCS 2015 Shelf



1	SVO card	2	Guide Rail

Figure 24: Installed SVO Card on the NCS 2015 Shelf

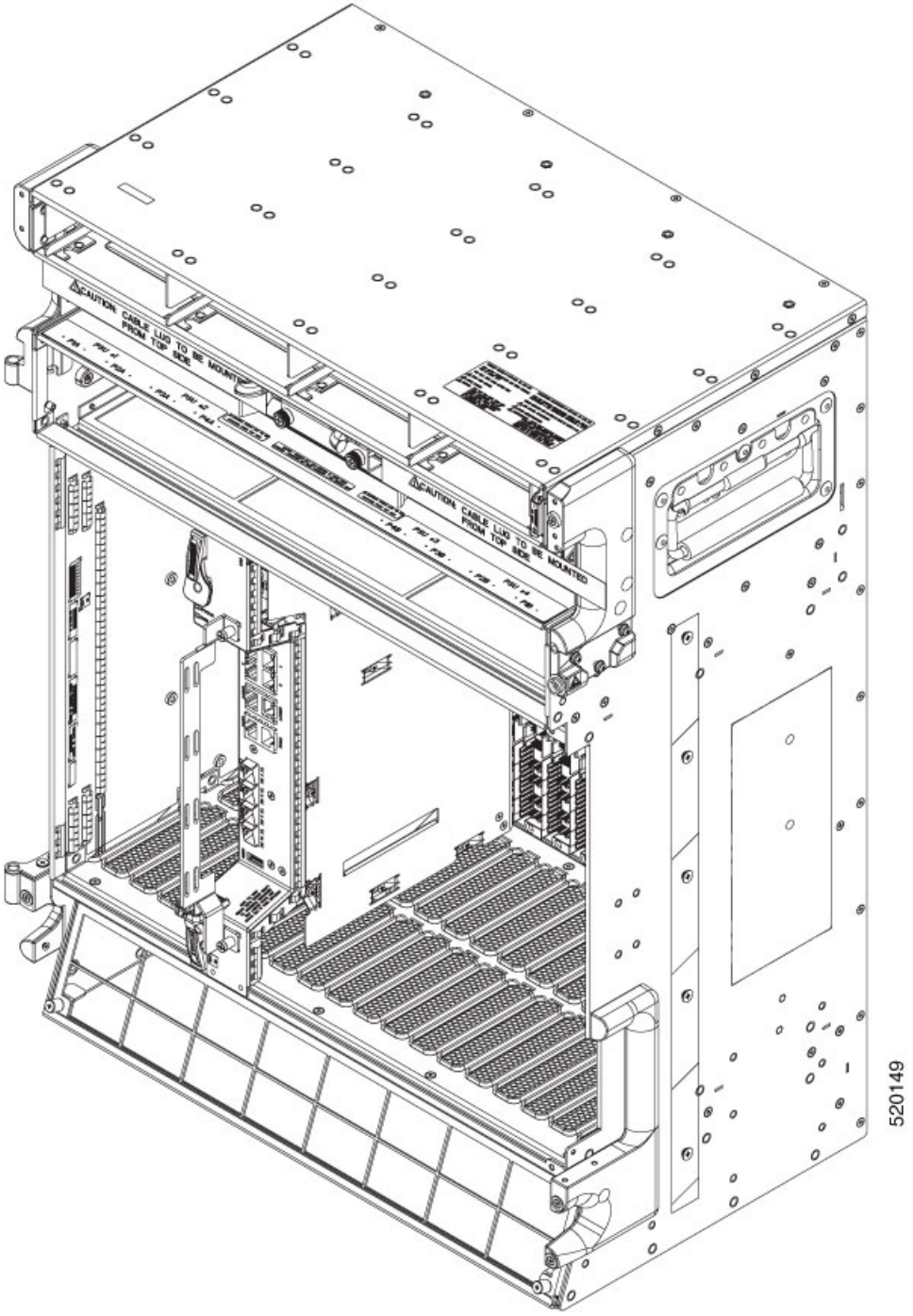
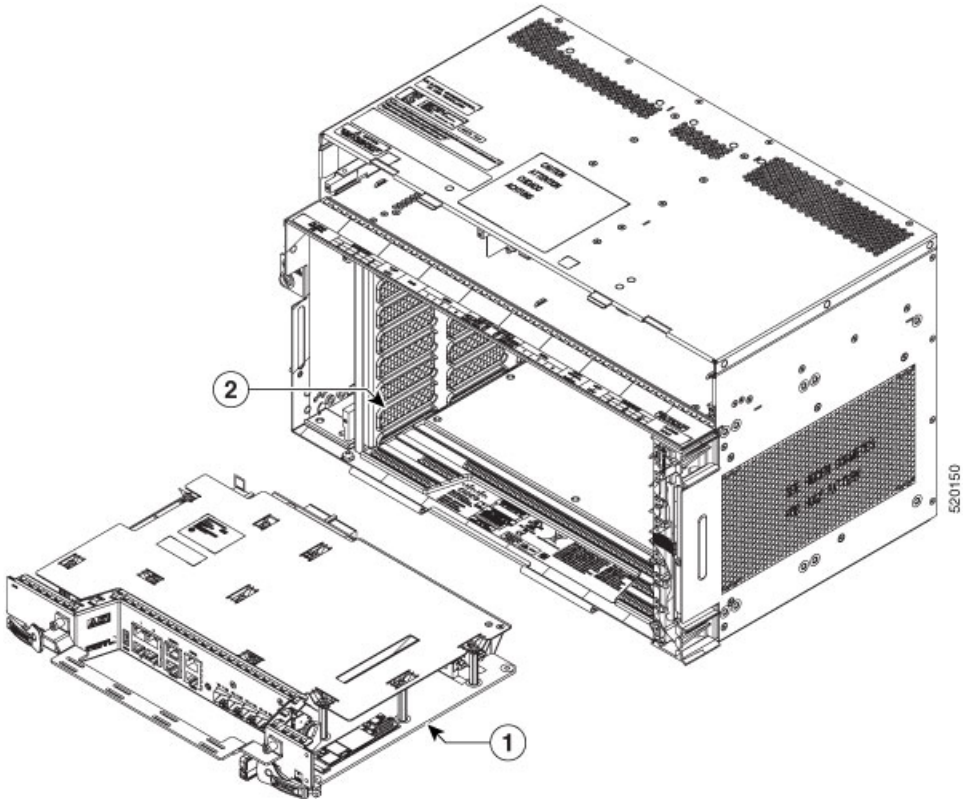
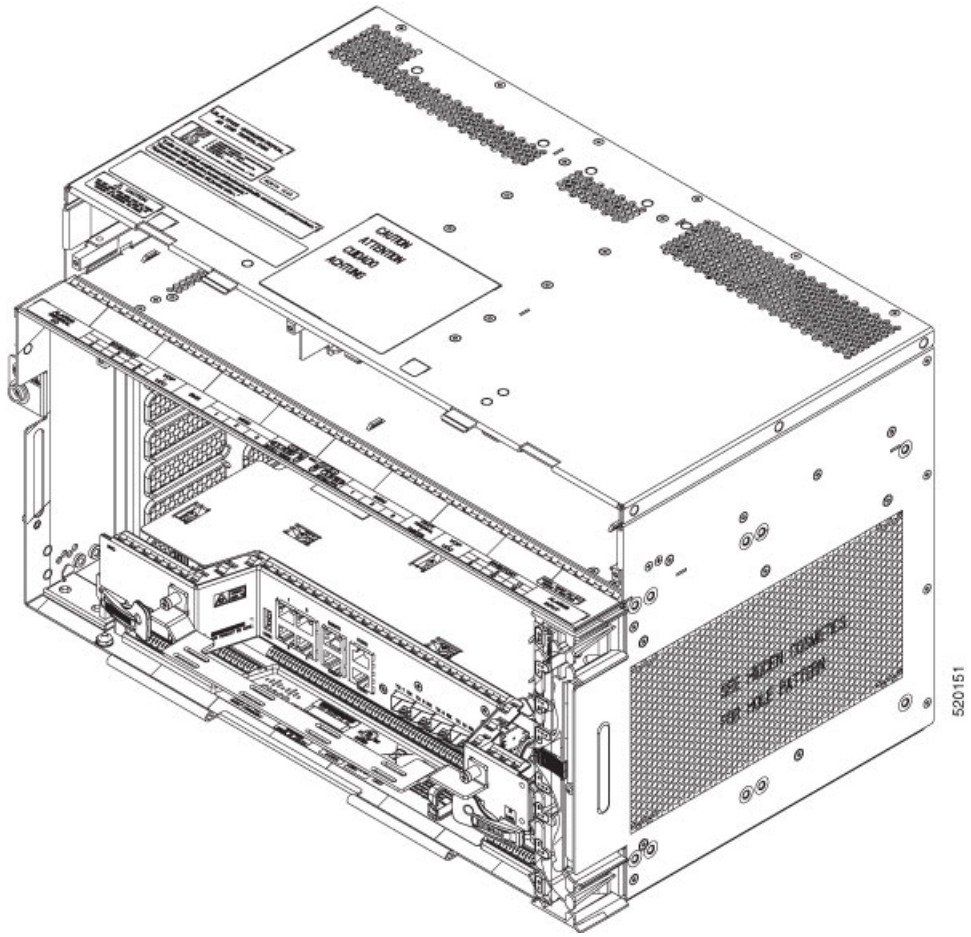


Figure 25: Installing SVO Card on the Shelf



1	SVO Card	2	Guide Rail

Figure 26: Installed SVO Card on the Shelf



View UDC details

The User Data Channel (UDC) is a 100 Mbps Ethernet-type interface available on certain cards, providing a dedicated path for management or user-defined data. Cisco Optical Site Manager allows you to view the details of a UDC channel configured through the CTC.

Use this task to view the UDC channel details of a control card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Provisioning** tab.

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

The UDC section displays the port and its service type.

View Insertion Loss Parameters

Use this task to view the insertion loss parameters of the 16-AD-CCOFS and 6AD-DD-CFS cards.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Click the **Maintenance** > **Insertion Loss** tabs to view the insertion loss parameters.

The Insertion Loss tab displays the following information:

- **Insertion Loss Path**—Displays the insertion loss path.
- **IL Value (dB)**—Displays the insertion loss value.

Note When the card is removed, the last retrieved Insertion Loss values are displayed in the Cisco Optical Site Manager web UI. When the card is replaced, the Insertion Loss values are updated in the Cisco Optical Site Manager web UI.

Manage the Protection Group

Use this task to view the protection group that is automatically created when a new PSM card is provisioned. You can also perform a switch operation on the interfaces.

Before you begin

- Log into Cisco Optical Site Manager, on page 1

- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** > **Protection** tabs to view the parameters of the PSM protection group.

The Protection tab displays the following information:

- **Name**—Name of the protection group
- **Protection Type**—The protection type is splitter
- **Active Interfaces**—The interfaces on which the traffic is present
- **Working Interfaces**—The working interfaces are the active interfaces when the protection group is created.
- **Protection Interfaces**—The protection interfaces when the protection group is created.
- **Switch Type**—The switch type is bidirectional-switching.
- **Revertive**—If set to true, the traffic reverts to the working port after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- **Reversion Time (min)**—Reversion time is the amount of time that will elapse before the traffic reverts to the working card. The reversion timer starts after conditions causing the switch are cleared. The range is from one to 12 minutes.
- **Reversion Pulse Width (sec)**—Reversion Pulse Width is between 10 to 200 seconds and is configurable only if the protection is revertive. By default, the duration is set to 60 seconds.

Note The following fields in the protection group are editable in the Chassis view > Provisioning tab:

- Name
- Revertive
- Reversion Time
- Reversion Pulse Width

Step 2 Click + to view the protection group data.

The interfaces of the protection group are displayed.

- **Interface**—displays the name of the interface
- **Entity**—Displays the entity of the interface, whether it is working or protect
- **Entity Status**—Displays the status of the entity, whether it is active or Standby
- **Switch Status**—Displays the switch status when a switch operation is performed.

Step 3 To perform a switch operation between the interfaces of a protection group, perform these steps:

Note A switch operation can only be performed if revertive is set to false.

a. Check the check box corresponding to the interface you want to perform a switch operation.

b. Click **Edit**.

The Switch Command dialog box appears.

c. Select an option from the **Action** drop-down list.

The options available are—Lock-Out, Force-Switch, Manual-Switch, and Release.

d. Click **Apply**.

Provisioning Optical Amplifier Cards

This chapter describes the optical amplifier cards used in Cisco NCS 2000 and its related tasks.

RAMAN-CTP and RAMAN-COP Cards

In this chapter, "RAMAN-CTP" refers to the 15454-M-RAMAN-CTP card and "RAMAN-COP" refers to the 15454-M-RAMAN-COP card.

The single-slot RAMAN-CTP and RAMAN-COP cards support counter and co-propagating Raman amplification on long unregenerated spans.

The cards manage up to 96 ITU-T 50 GHz spaced channels over the C-band of the optical spectrum (wavelengths from 1528.77 to 1566.72 nm). The counter-propagating RAMAN-CTP card is the primary unit. The co-propagating RAMAN-COP card is the secondary unit and can be used only when the counter-propagating unit is present. The OSC pluggable used with the cards is ONS-SC-OSC-18.0=.

The RAMAN-CTP card can be calibrated either manually or automatically from the **Maintenance** tab in the Cisco Optical Site Manager web interface. When the RAMAN-COP card is used, the RAMAN-CTP card can be calibrated only using the manual option.

The features of the RAMAN-CTP and RAMAN-COP cards include:

- Raman section: 1000-mW total pump power for four pumps and two wavelengths.
- Embedded distributed feedback (DFB) laser at 1568.77 nm to be used for optical safety and link continuity (in RAMAN-CTP card only).
- Photodiodes to enable monitoring of Raman pump power.
- Photodiodes to enable monitoring of the DFB laser and signal power (in RAMAN-CTP card only).
- Automatic laser shutdown (ALS) for optical laser safety.
- Hardware output signals for loss of signal (LOS) monitoring at input photodiodes.

- Raman pump back reflection detector to check for excessive back reflection.

When the node has either RAMAN-CTP or RAMAN-COP card, you can install the card in the following slots.

- Slots 2–7 in NCS 2006
- Slots 2–16 in NCS 2015

When the node has both RAMAN-CTP or RAMAN-COP cards, you can install the cards in the following slots.

- If the RAMAN-CTP card is installed in an even slot, the RAMAN-COP card must be installed in the next odd slot.
- If the RAMAN-COP is installed in an even slot, the RAMAN-CTP card must be installed in the next odd slot.

RAMAN-CTP and RAMAN-COP Cards Power Monitoring

Physical photodiodes P1 through P10 monitor the power for the RAMAN-CTP card.

Table 50: RAMAN-CTP Port Calibration

Photodiode	Type Name	Calibrated to Port
P1	DFB in-fiber Output Power	LINE-TX
P2	DWDM RX Input Power	LINE-RX
P3	Pump 1 in-fiber Output Power	LINE-RX
P4	Pump 2 in-fiber Output Power	LINE-RX
P5	Total Pump in-fiber Output Power	LINE-RX
P6	Back-Reflected Pump Power	LINE-RX
P7	DWDM TX Input Power	COM-RX
P8	Total Co-Pump in-fiber Output Power	LINE-TX
P9	DFB Input Power	LINE-RX
P10	ASE Input Power	LINE-RX

Physical photodiodes P3 through P6 monitor the power for the RAMAN-COP card.

Table 51: RAMAN-CTP Port Calibration

Photodiode	Type Name	Calibrated to Port
P3	Pump 1 in-fiber Output Power	RAMAN-TX
P4	Pump 2 in-fiber Output Power	RAMAN-TX

Photodiode	Type Name	Calibrated to Port
P5	Total Pump in-fiber Output Power	RAMAN-TX
P6	Back-Reflected Pump Power	RAMAN-TX

For more information about the RAMAN-CTP and RAMAN-COP cards, see the data sheet.

Clear the Raman Laser Shutdown Condition

The Raman Laser Shutdown (RLS) condition is raised during the Raman link turn-up phase on the RAMAN-TX port of the RAMAN-CTP and RAMAN-COP cards when excessive back reflection is detected. When the RLS condition is raised, the Raman pump laser inside the card is automatically shut down and the optical link turn-up procedure is terminated. The RLS condition must be cleared before proceeding with further provisioning.

Use this task to clear the RLS condition for RAMAN-CTP and RAMAN-COP cards.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** > **Safety** tabs.

Step 2 Click **Manual Safety Restart** to clear the RLS condition.

A confirmation dialog box appears and is service-affecting.

Step 3 Click **Yes** to proceed.

Collect Failure Logs

Use this task to collect the failure log information for the cards. This task can be used to debug the cards before RMA.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Right-click the card and choose **OBFL** to collect the On Board Failure Logs (OBFL).

The failure log information is displayed in the **Maintenance** > **OBFL Status** tabs.

Perform Automatic Calibration

Use this task to perform automatic calibration for the RAMAN-CTP, EDRA1-xx, and EDRA2-xx cards.

The automatic calibration automatically runs on the cards upon fiber restoration, power cycle, and so on.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** > **Automatic Calibration** tabs.

All the values in this pane are read-only and reflects the status of last automatic calibration.

Table 52: Parameters of Automatic Calibration

Parameter	Description
Port	Displays the port number, port type, and direction (TX or RX).
Timestamp	Displays the date and time of calibration.
Calibration Gain (dB)	Displays the Raman gain that is obtained with calibration of total pump power.
Calibration Total Pumps (mW)	Displays the reference power level used throughout calibration. The default value is 700 mW. If Raman gain is too low, the power value is automatically increased to 850 mW.
Target Gain (dB)	Displays the target spectrum gain.
Obtained Gain (dB)	Displays the obtained spectrum gain.
Target Tilt (dB)	Displays the target spectrum tilt.
Obtained Tilt (dB)	Displays the obtained spectrum tilt.
Raman Noise Floor (dBm)	Displays the optical power measured at the LINE-RX port when Raman pumps are at calibration total pumps power level and incoming signal is not received from the neighboring node. It is noise generated by the Raman amplification process.

Parameter	Description
Incoming Power Pumps Off (dBm)	Displays the power level of probe signal with Raman pumps off.
Incoming Power Pumps On (dBm)	Displays the power level of probe signal with Raman pumps on (combined with Raman noise floor).
Power Source	Displays the type of power source that is used for calibration. The possible values of Power Source are as follows: • Broadband Optical Power—Raman automatic calibration used broadband optical power, typically, Amplified Spontaneous Emission (ASE) generated by an optical amplifier. • Active Optical Services—Raman automatic calibration used active services. • Active Optical Services (Unbalanced)—Raman automatic calibration used active services;however, they do not properly cover the whole C-Band spectrum.
Result	Displays the result of automatic Raman calibration. The possible values of Result are as follows: • No Target Gain—Raman target gain is not configured. • Not Enough Gain—Raman gain obtained from calibration is too low. • Lower Than Target Gain (Need Accept)—Raman gain obtained from calibration is below the target but might be acceptable. The user must accept the Raman gain. • Lower Than Target Gain (Accepted)—Raman gain obtained from calibration is below the target and the user has accepted the Raman gain. • Target Gain Reached—Raman target gain is reached. • User Override—User has overridden the calibration result and uses configured setpoint of Raman pumps manually.

Parameter	Description
Status	Displays the status of automatic Raman calibration. The possible values of Status are as follows: • Not Scheduled—Raman automatic calibration is not scheduled. • Invalid—Raman automatic calibration reports invalid data. • Pending—Raman automatic calibration is scheduled and pending. • Running On User Request—Raman automatic calibration is running on user request. • Running—Raman automatic calibration is automatically running. • Failed—Raman automatic calibration has failed. • Aborted—Raman automatic calibration has been terminated and will be re-scheduled soon. • Completed—Raman automatic calibration is completed.

Step 2 Click **Run Calibration** to start the automatic calibration.

A confirmation message appears.

Step 3 Click **Yes**.

When you start the automatic calibration, the Status column in the Automatic Calibration tab changes to "Running on User Request."

The calibration result can be success, failure, or lower than target gain.

- If the calibration result is success, the obtained target gain value is applied to the node.
- If the calibration result is failure, the old target gain value is restored.
- If the calibration result is lower than target gain, it implies that the obtained gain is + or –2 dB from the target gain. The gain is degraded. The RAMAN-GAIN-NOT-REACHED alarm is raised on the node to inform the user of a lower target gain. The user can accept this lower target gain by clicking the **Accept Degraded Gain** button. This clears the RAMAN-GAIN-NOT-REACHED alarm and the lower target gain value is applied to the node.

Step 4 (Optional) (Not applicable for RMN-CTP-CL card) Click **Get All Calibration Reports** to display the last 10 calibration reports with the timestamp and result in a table.

Step 5 (Optional) Click **Get Last Calibration Error** to identify the reason for the last calibration failure.

The automatic calibration typically completes without user intervention. However, the automatic calibration fails upon certain conditions such as loss of communication between two nodes and OSC failure. You can

identify the reason for the last calibration failure by clicking the **Get Last Calibration Error** button. The reason is displayed only when the Status column in the Automatic Calibration tab is Failure.

Perform Manual Calibration

Use this task to perform manual calibration for the RAMAN-CTP and RAMAN-COP cards.

The RAMAN-COP card supports only manual calibration. The RAMAN-CTP card supports both automatic and manual calibration. However, if a node has both RAMAN-CTP and RAMAN-COP cards, the RAMAN-CTP card supports only manual calibration.

For complete information on the specific setup that is required for manual calibration, see DLP-G690 Configure the Raman Pump Using Manual Day-0 Installation.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** > **Manual Calibration** tabs.

All the values in this pane are read-only and reflects the status of last manual calibration.

Table 53: Parameters of Manual Calibration

Parameter	Description
Port	Displays the port number, port type, and direction (TX or RX).
Time Stamp	Displays the date and time of calibration.
Pump 1 Low Power (dBm)	Displays the measured incoming power with only pump 1 on at low power level.
Pump 2 Low Power (dBm)	Displays the measured incoming power with only pump 2 on at low power level.
Pump 1 High Power (dBm)	Displays the measured incoming power with only pump 1 on at high power level.
Pump 2 High Power (dBm)	Displays the measured incoming power with only pump 2 on at high power level.
Target Gain (dB)	Displays the target spectrum gain.
Obtained Gain (dB)	Displays the obtained spectrum gain.

Parameter	Description
Target Tilt (dB)	Displays the target spectrum tilt.
Obtained Tilt (dB)	Displays the obtained spectrum tilt.
Result	Displays the result of manual Raman calibration. The possible values of Result are as follows: • No Target Gain—Raman target gain is not configured. • Not Enough Gain—Raman gain obtained from calibration is too low. • Lower Than Target Gain—Raman gain obtained from calibration is below the target but is acceptable. • Target Gain Reached—Raman target gain is reached. • User Override—User has overridden the calibration result and uses the configured setpoint of Raman pumps manually.
Status	Displays the status of manual Raman calibration. The possible values of Status are as follows: • Not Calibrated—Raman calibration was not run. • In Progress—Raman calibration is being run by the user. • Completed—Raman calibration is completed. • Using pumps-power-setpoint—Raman pumps are regulated according to the user configuration.

Step 2 Click **Run Calibration**.

A confirmation message appears.

Step 3 Click **Yes**.

Step 4 Click **Run Pump Test** for each individual pump.

The pump test cannot be run if active circuits are present in the node. When you run the pump test, the Status column in the Manual Calibration tab changes to "In Progress."

Step 5 Enter the optimum power value of individual pump in the Power Value (dBm) field.

Step 6 Click **Calibrate Pump** to start the manual calibration.

The calibration progress appears in the **Calibration Result** area. The calibration result can be a success, failure, or lower than target gain.

- If the calibration result is success, the obtained target gain value is applied to the node.

- If the calibration result is a failure, the old target gain value is restored.
- If the calibration result is lower than the target gain, it implies that the obtained gain is + or –2 dB from the target gain. The gain is degraded. However, the calibration is still accepted and the obtained target gain value is applied to the node.

Provision FPD Upgrade

Whenever the firmware version on the card is earlier than the FPGA firmware version, an alarm "FPD-UPG-REQUIRED" is raised on the card in the **Alarms** tab.

You can view the running firmware version and the NCS 2000 FPGA firmware version under the **Maintenance** > **FPD upgrade** tabs.

Use this task to upgrade the RMN-CTP-CL card with the latest firmware released as part of the NCS 2000 software release.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** > **FPD Upgrade** tabs.

Step 2 Click **FPD upgrade** to perform firmware upgrade for the card.

After the firmware upgrade is completed successfully, the "FPD-UPG-REQUIRED" alarm gets cleared in **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

Retrieve MAC Addresses through LLDP

Use this task to retrieve the source MAC address of the host connected to the 100GE or 400GE ports of 1.2T-MXP card, after a Link Layer Discovery Protocol (LLDP) packet is received on the client port.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

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

Step 3 Click **Refresh**.

The table displays the following fields:

- Port—Displays the port number.
- Source MAC Address—Displays the MAC address of the node to which the port is connected.

Limitations of LLDP Support on the 1.2T-MXP Card

The LLDP support on the 1.2T-MXP card has the following limitations:

- The 1.2T-MXP card can handle only one LLDP packet of 2000byte size per client every four seconds.
- LLDP packet is not detected when the client ports if moved to from IS to OOS.
- After the trunk port transits from OOS to IS, there is a delay of 12 to15 seconds to detect the LLDP packet and display it on the GUI.
- LLDP capture does not happen when CFP2 DCO associated with the client port is not plugged in.
- The 1.2T-MXP card captures the LLDP packets only when:
  1. The value of ETH TYPE header is 0x88CC.
  2. The destination Multicast addresses are:
     - 01:80:C2:00:00:00
     - 01:80:C2:00:00:0e
     - 01:80:C2:00:00:03

Provision FPD Upgrade for the Ports

When the firmware version on the DCO trunk port is earlier than the NCS 2000 package firmware version, an alarm "FPD-UPG-REQUIRED" is raised on that trunk port in the **Alarms** tab. Each trunk port has separate upgrade alarm.

You can view the DCO running firmware version and the NCS 2000 package firmware version under the **FPD upgrade** section of the **Maintenance** tab.

Use this task to upgrade DCO (trunk ports) on the 1.2T-MXP card with the latest firmware released as part of the NCS 2000 software release.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

Step 2 Click the **FPD Upgrade** section to expand it.

Step 3 Choose the DCO ports that you want to upgrade.

You can consider the following use cases to choose the DCO ports for upgrade:

- When the DCO ports have both traffic-affecting and non-traffic affecting upgrade alarms, you can select only the DCO ports with non-traffic affecting upgrade alarms and proceed with the firmware upgrade without affecting traffic on the node.
- If the upgrade is required only for a DCO on a specific circuit, you can select that particular DCO and perform the upgrade without disturbing any other DCO ports.

Step 4 Click **FPD upgrade** to perform firmware upgrade for the chosen ports.

After the firmware upgrade is completed successfully, the "FPD-UPG-REQUIRED" alarm gets cleared in the **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

Provision FPD Upgrade for MR-MXP Card

When the firmware version on the MR-MXP card is earlier than the NCS 2000 package firmware version, an alarm "TRAF-AFFECT-RESET-REQUIRED" is raised on that card in the **Alarms** tab.

You can view the running firmware version and the NCS 2000 package firmware version under the **FPD upgrade** section of the **Maintenance** tab.

Use this task to upgrade the MR-MXP card with the latest firmware released as part of the NCS 2000 software release.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

Step 2 Click the **FPD Upgrade** section to expand it.

Step 3 Click **FPD upgrade** to perform firmware upgrade for the card.

After the firmware upgrade is completed successfully, the "TRAF-AFFECT-RESET-REQUIRED" alarm gets cleared in the **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

Enable Proactive Protection

Use this task to modify the proactive protection settings of the card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Provisioning** tab.

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

Step 3 Modify required settings described in the following table.

Table 54: Proactive Protection Regen Settings

Parameter	Description	Options
Port	(Display only) Displays the port name.	—
Trigger Threshold	Sets the maximum BER threshold to trigger proactive protection.	• 1E-3 • 9E-2 to 1E-2 • 9E-3 to 1E-3 • 9E-4 to 1E-4 • 9E-5 to 1E-5 • 9E-6 to 1E-6 • 9E-7 to 1E-7

Parameter	Description	Options
Trigger Window (ms)	Sets the duration when BER is monitored before triggering the proactive protection. The trigger window value must be a multiple of: • 10 ms for trigger thresholds between 1E-3 and 6E-6 • 100 ms for a trigger threshold between 5E-6 to 1E-7 Trigger window must be less than or equal to 500 ms for trigger thresholds between 1E-3 and 6E-6. The trigger window must be less than or equal to 3900 ms for trigger thresholds between 5E-6 to 1E-7.	Time in milliseconds.
Revert Threshold	Sets the revert threshold value of BER. **Note** The revert threshold settings must be less than the trigger threshold values.	• 1E-4 • 9E-3 to 1E-3 • 9E-4 to 1E-4 • 9E-5 to 1E-5 • 9E-6 to 1E-6 • 9E-7 to 1E-7 • 9E-8 to 5E-8
Revert Window (ms)	Sets the duration when BER is monitored for settings that are less than the revert threshold value before which, proactive protection that is provided to the router is removed. The revert window value must be at least 2000 ms and a multiple of: • 10 ms for a revert threshold of 1E-4 to 6E-7. • 100 ms for a revert threshold of 5E-7 to 5E-8. The revert window must be less than or equal to 3900 ms.	Time in milliseconds.
Enable Proactive Protection	Enables proactive protection.	• Disabled • FRR Proactive Protection • Pre-FEC PSM Proactive Protection

Step 4 Click **Apply**.

Provision ODU Circuit

Use this task to provision ODU circuit created through NETCONF client, in the OTNXC mode of the 400G-XP card.

Both unprotected and protected ODU connections or OTNXC circuits that are created in CTC will be available in the Cisco Optical Site Manager. The user interface after the NCS2000 device is upgraded from CTC to Cisco Optical Site Manager and the device sync is completed. The ODU connection data that is displayed in the Cisco Optical Site Manager user interface has the following discrepancies:

- When ODU connections are discovered, Cisco Optical Site Manager autogenerates the connection name as "device-name/object index" (an integer number) and displays the connection name as Circuit ID.
- CTC allows creating a protected ODU connection with two trunk ODU sources and one client ODU destination. But Cisco Optical Site Manager considers this protected ODU connection as invalid. Hence as part of discovery, Cisco Optical Site Manager recreates the protected ODU connection with one source client and two destination trunk ODUs, by swapping.

Use this task to provision ODU circuit created in the OTNXC mode of the 400G-XP card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

Step 2 Click the **OTN Circuit** section to expand it.

The **OTN Circuit** tab displays the following information:

- Circuit ID—Unique identifier for the end-to-end circuit
- Connection label—Unique identifier for ODU connections
- Bandwidth—Bandwidth of the circuit. Supported values are ODU4, ODU2, ODU2e
- Direction—Only bidirectional is supported
- Source—Source ODU port
- Destination—Destination ODU port
- Protection Reference—Displays the Protection port
- Admin State—Displays the admin state
- Service State—Displays the service state

- ILK Usage—Displays interlink port usage

Step 3 Click the plus icon to view the **Protection Attributes** of the circuit.

Step 4 (Optional) Edit the **Connection label** and the **Admin State**.

Step 5 (Optional) Click **ODU Utilization** to view ODU Utilization information.

An ODU utilization window for the 400G-XP-LC card is displayed where you can get information about the availability of each port for ODU circuit creation. All ODU ports are displayed according to the slice configuration that was configured. Each row represents 100G or ODU4 bandwidth. The client ports are listed first followed by the trunk ports. The ports that are already used by the ODU circuit are displayed in green, the ports that are available for circuit creation are displayed in orange and the ports that are not applicable nor configured are displayed in gray.

To view Bandwidth Utilization using the NETCONF client, use the following RPCs:

- To show the utilization under odu-interface which is part of otn-xc connection:

```
<action xmlns="urn:ietf:params:xml:ns:yang:1">
    <svo xmlns="http://cisco.com/yang/svo">
      <odu-connection-commands>
        <interface-otnxc-utilization>
          <interface-name>1/3/11/1-1</interface-name>
        </interface-otnxc-utilization>
      </odu-connection-commands>
    </svo>
  </action>
```

- To show card level utilization (You enter the shelf and slot info.):

```
<action xmlns="urn:ietf:params:xml:ns:yang:1">
    <svo xmlns="http://cisco.com/yang/svo">
      <odu-connection-commands>
        <module-otnxc-utilization>
          <uid>1</uid>
          <module-id>3</module-id>
        </module-otnxc-utilization>
      </odu-connection-commands>
    </svo>
  </action>
```

Step 6 Click **Apply**.

You can edit only the Admin State and the Connection label in the Cisco Optical Site Manager user interface. For protected ODU connection, Protection group Name, Revertive mode, and Revertive time can be edited from NETCONF, and web user interface (under the **Protection** section of the **Provisioning** tab in the shelf view). The other parameters such as Holdoff Timer can be edited only through the NETCONF client.

Functional Module Group

Functional Module Group (FMG) stepper simplifies the process of configuring the operating modes for transponder and muxponder cards. In the previous releases, you must navigate through multiple tabs in the Cisco Optical Site Manager application to make the appropriate selections. With the FMG stepper, you can

configure the operating modes and sub operating modes of different cards with specific client payloads in simple steps.

Configure Card Mode using Functional Module Group

Use this task to configure the operating mode and sub operating modes of a card while adding it to the NCS 2006 or NCS 2015 chassis.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

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

The Topology view is displayed.

Step 2 Click the rack title to zoom into the required rack in the left panel.

The enlarged view of the rack appears.

Step 3 Left-click the empty slot in the chassis where you want to add the card.

The dialog box for the selected slot appears.

Note Configuration of card mode cannot start from slot 16 in NCS 2015 chassis.

Step 4 Click **FMG Provision** to add a card to the chassis and configure its card mode.

The **Functional Module Group** wizard appears.

Step 5 In **Add primary module**, perform the steps to choose a primary card.

a) Choose a primary card from the **Select primary module** drop-down list.

Note When adding the NCS2K-400G-XP or NCS2K-100GS-CK-C card, ensure to follow the correct slot combinations in NCS 2006 and NCS 2015 chassis. If correct slot combinations are not available, the **Select primary module** drop-down list does not display the NCS2K-400G-XP or NCS2K-100GS-CK-C card.

A preview of the selected card appears below the drop-down list.

b) Click **Next**.

Step 6 In **Select card mode**, perform the steps to configure a card mode.

a) Choose the required card mode configuration from the drop-down list.

Note The number of available card mode configurations differ based on the primary card selected. For more information on the card mode configurations, see Configuring card modes for NCS 2000 line cards, on page 80.

b) Click **Add**.

When adding the 15454-M-10x10G-LC card, you can choose multiple card mode configurations. You must choose trunk ports for the RGN-10G, TXP-10G, Low Latency and TXPP-10G card modes, and client port for TXP-10G card mode.

When adding the NCS2K-400G-XP card, you must choose slice configurations for the card mode selected.

c) Click **Next**.

Step 7 In **Add secondary modules**, perform the steps to configure the required peer card.

a) Choose the peer card from the **Select secondary modules** drop-down list.

Note The **Functional Module Group** wizard lists the compatible peer cards for the selected primary card and its card mode configuration. For NCS2K-100GS-CK-C and NCS2K-200G-CK-C cards, you must choose sub operating modes for MXP-200G card mode from the **Submode** drop-down list.

A preview of the selected peer card appears below the drop-down list.

b) Click **Next**.

Note For standalone card modes, the **Functional Module Group** wizard skips the **Add secondary modules** step.

Step 8 In **Add pluggables**, perform the following steps to configure the pluggable parameters.

Note You need to configure the pluggable port modules and pluggables ports for the primary card followed by the secondary cards.

a) In the **Pluggable Port Modules** pane, choose from the **PPM** drop-down list and click **Add**.

The added port modules appear below the drop-down list.

b) In the **Pluggable Ports** pane, choose from the **Port ID** and **Port Type** drop-down lists and click **Add**.

The added Port ID and Port Type appear below the drop-down list.

c) Click **Next**.

A preview of the configured cards, pluggable port modules and pluggable ports appear in **Configuration recap**. If sub modes and slices are configured, then a preview of the sub modes and slices are also displayed.

Step 9 Click **Finish**.

Note Errors are displayed if the configuration is inaccurate.

Provision ZR Plus Interfaces

Use this task to provision the parameters for the ZR Plus interfaces of the 1.2T-MXP card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

Step 2 Click the **ZR Plus Interfaces** section to expand it.

Step 3 Modify any of the ZR Plus settings as described in the following table. These parameters depend on the card mode.

Table 55: Card ZR Plus Settings

Parameter	Description	Options
Port	(Display only) Displays the port number	—
Squelch Mode	(Display only) Displays the squelch mode	• 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	• Disable
FEC	Sets the FEC mode	OFEC_15_DE_ON
GroupId	Sets the GroupId that uniquely identifies a group of physical ports in a ZR frame. This makes sure that noncompliant groups do not interoperate. When a mismatch in the group is identified, GIDM alarm is raised.	1–255

Step 4 Click **Apply**.

Provision ZR Plus Interfaces

Use this task to provision the parameters for the ZR Plus interfaces of the 1.2T-MXP card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

Step 2 Click the **ZR Plus Interfaces** section to expand it.

Step 3 Modify any of the ZR Plus settings as described in the following table. These parameters depend on the card mode.

Table 56: Card ZR Plus Settings

Parameter	Description	Options
Port	(Display only) Displays the port number	—
Squelch Mode	(Display only) Displays the squelch mode	• 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	• Disable
FEC	Sets the FEC mode	OFEC_15_DE_ON
GroupId	Sets the GroupId that uniquely identifies a group of physical ports in a ZR frame. This makes sure that noncompliant groups do not interoperate. When a mismatch in the group is identified, GIDM alarm is raised.	1–255

Step 4 Click **Apply**.

Provision ZR Plus Trail Trace Monitoring

This task provisions the trail trace monitoring parameters that are supported for the ZR plus payloads on the 1.2T-MXP card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

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

Step 3 Modify any of the ZR Plus settings as described in the following table.

Table 57: ZR plus Trail Tracing Settings

Parameter	Description	Options
Port	(Display only) Displays the port number.	—
Send-Tti	Sets the transmit TTI String.	0–32 Bytes
Expected-Tti	Sets the expected TTI String.	0–32 Bytes
Received-Tti	(Display only) Displays the received TTI String.	0–32 Bytes

Note
- When the trunk port is in OOS-DSBL state, its received TTI is not displayed in the GUI.
- Sometimes, the received TTI value takes up to ten seconds to get displayed in the GUI.

Step 4 Click **Apply**.

Provision ZR Plus Trail Trace Monitoring

This task provisions the trail trace monitoring parameters that are supported for the ZR plus payloads on the 1.2T-MXP card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65

Procedure

Step 1 Click the **Maintenance** tabs.

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

Step 3 Modify any of the ZR Plus settings as described in the following table.

Table 58: ZR plus Trail Tracing Settings

Parameter	Description	Options
Port	(Display only) Displays the port number.	—
Send-Tti	Sets the transmit TTI String.	0–32 Bytes
Expected-Tti	Sets the expected TTI String.	0–32 Bytes
Received-Tti	(Display only) Displays the received TTI String.	0–32 Bytes

Note
- When the trunk port is in OOS-DSBL state, its received TTI is not displayed in the GUI.
- Sometimes, the received TTI value takes up to ten seconds to get displayed in the GUI.

Step 4 Click **Apply**.

Provision Pluggable Ports

Use this task to provision the payloads supported on the card.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 65
- Configuring card modes for NCS 2000 line cards, on page 80

Procedure

Step 1 Click the **Provisioning** tab.

Step 2 Click the **Pluggable Ports** section to expand it.

Step 3 In the Pluggable Ports area, click the + button.

The Create Port dialog box appears.

Step 4 Choose the port number from the **Port ID** drop-down list.

Step 5 Choose the supported payload from the **Port Type** drop-down list.

Note For 1.2T-MXP card, if you try to choose a payload which is not supported by the sub operating mode of the pluggable, you will see an error message.

Step 6 Choose the number of lanes from the drop-down list.

This field is visible only in specific configurations.

Step 7 Click **Apply**.

Step 8 Repeat Step 1 through Step 6 to configure the rest of the port rates as needed.

View Circuit Protection Parameters

Use this task to display the protection parameters of ODU circuit created in the OTNXC mode of the 400G-XP card. The protection parameters are defined when a protected ODU circuit is created through NETCONF client.

Before you begin

Log into Cisco Optical Site Manager, on page 1

Procedure

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

The Topology view is displayed.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Maintenance Protection** tabs to view the following protection parameters:

- **Name**—Name of the protection group.
- **Protection Type**—Type of the protection.
- **Active Interfaces**—The interfaces on which the traffic is present.
- **Working Interfaces**—The working interfaces are the active interfaces when the protection group is created.
- **Protection Interfaces**—The protection interfaces when the protection group is created.
- **Switch Type**—The switch type is bidirectional-switching.
- **Revertive**—Choose True or False. If set to true, the traffic reverts to the working port after failure conditions remain corrected for the amount of time that is entered in the Reversion Time field.
- **Reversion Time (min)**—Reversion time is the amount of time that will elapse before the traffic reverts to the working port. The reversion timer starts after conditions causing the switch are cleared. The range is from one to 12 minutes.
- **Reversion Pulse Width (sec)**—Reversion Pulse Width is not applicable for the ODU circuit.



Note The following fields in the protection group are editable in the **Chassis view Provisioning** tab:

- Name
- Revertive
- Reversion Time
- Reversion Pulse Width

Step 5 Click + to view the protection group data.

The interfaces of the protection group are displayed.

- **Interface**—Displays the name of the interface
- **Entity**—Displays the entity of the interface, whether it is working or protect
- **Entity Status**—Displays the status of the entity, whether it is active or Standby
- **Switch Status**—Displays the switch status when a switch operation is performed.

Step 6 To perform a switch operation between the interfaces of a protection group, perform these steps:

a. Check the check box of the interface that has **Entity Status** as active.

b. Click **Edit**.

The **Switch Command** dialog box appears.

c. Select an option from the **Action** drop-down list.

The options available are—Lock-Out, Force-Switch, Manual-Switch, and Release.

d. Click **Apply**.

Note Cisco Optical Site Manager does not support the Y-cable protection type. If a Y-cable protected circuit is available in the system, Cisco Optical Site Manager cannot fetch the data when you expand the protection data.

NCS 2000 Cards

Table 59: Feature History

Feature Name	Release Information	Description
Flexible Migration Options for NCS 2000 Management	Cisco NCS 2000 Release 25.1.1	This release improves flexibility and migration options for NCS 2000 management. Network-level and node-level functionalities can now be managed through Cisco Optical Network Controller or Cisco Optical Site Manager using SVO-LC. Transition to Cisco Optical Network Controller or Cisco Optical Site Manager at your own pace while continuing to use TL1, EPNM 8.1.1, and CTC. When ready, you can disable these legacy tools and adopt Cisco Optical Network Controller or Cisco Optical Site Manager as the primary management platform.

This section describes the NCS 2000 cards that can be configured using Cisco Optical Site Manager.

In release 25.1.1, CTC card-level and node-level functionalities are limited due to the availability of the Cisco Optical Site Manager web UI. The TL1 interface remains fully supported.

Note Before making any configuration changes to the NCS 2000 cards using CTC or TL1, ensure that the Cisco Optical Site Manager interface is disabled through the device lock/unlock feature. This step is essential to avoid potential conflicts during the configuration process.

10x10G-LC Card

In this section, "10x10G-LC" refers to the 15454-M-10x10G-LC card.

The 10x10G-LC card is a DWDM client card, which simplifies the integration and transport of 10 Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. The 10x10G-LC card is supported on ONS 15454 M2, ONS 15454 M6, and Cisco NCS 2000 Series platforms.

The 10x10G-LC card is a single-slot card and can be installed in any service slot of the chassis. The 10x10G-LC card consists of a 10-port SFP+ based (with gray-colored, coarse wavelength division multiplexing ([CWDM] and DWDM optics available) and one 100 G CXP-based port.

The 10x10G-LC card interoperates with 200G-CK-C card through a chassis backplane.

The 10x10G-LC card supports the following signal types:

- 10 Gigabit Ethernet LAN PHY (10.3125 Gbps)
- OC-192/STM-64 (9.95328 Gbps)
- OTU-2
- G.709 overclocked to transport 10 Gigabit Ethernet as defined by ITU-T G. Sup43 Clause 7.1 (11.0957 Gbps)

Operating Modes for 10x10G-LC Card

The 10x10G-LC card supports RGN-10G (5x10G Regenerator)/TXP-10G (5x10G Transponder) operating mode:

Each operating mode can be configured using specific set of cards and client payloads.

RGN-10G (5x10G Regenerator)/TXP-10G (5x10G Transponder)

The 10x10G-LC card works as a standalone card, supporting the multitransponder functionality. The 10 Gbps SFP+ ports should be paired to provide the 10 G transponder functionality for each port of the port pair. By using the grey optics SFP+ to provide the client equipment connectivity and DWDM SFP+ on the WDM side, up to five 10 G transponders are supported by a single 10x10G-LC card. Up to six 10x10G-LC cards are supported on the chassis allowing for 30 10 Gbps transponders in a single shelf.

All ports can be equipped with or without the G.709 Digital Wrapper function that provides wide flexibility in terms of the supported services.

As the client and trunk ports are completely independent, it is also possible to equip both SFP+ of the same pair of ports with the DWDM SFP+. The CXP pluggable is unused in this configuration.

Each of the SFP+ ports can be provisioned as a client or trunk. When one port is selected as a trunk, the other port of the pair is automatically selected as the client port. The allowed port pairs are 1-2, 3-4, 5-6, 7-8, or 9-10.

For RGN-10G mode, both ports are trunk ports.

It is not a constraint to provision five pairs of TXP-10G mode or five pairs of RGN-10G mode. A mix of TXP-10G and RGN-10G modes can be configured. For example, pairs 1-2 and 5-6 can be configured as TXP-10G mode and the remaining pairs as RGN-10G mode.

Table 60: Supported Payload Mapping Between Two SFP+ Ports

SFP+ Payload (Peer-1)	SFP+ Payload (Peer -2)
10GE-LAN (CBR Mapped)	OTU2e or 10GE-LAN (CBR Mapped)
OTU2	OC192 or OTU2

200G-CK-C Card

In this section, "200G-CK-C" refers to the NCS2K-200G-CK-C card.

The 200G-CK-C cards simplify the integration and transport of 200-Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. This card is supported on Cisco NCS 2006 and Cisco NCS 2015 platforms.

The cards interoperate with 10x10G-LC card through a chassis backplane.

Note The 200G-CK-LC cards do not operate with the CFP-LC card.

The cards provide the following benefits:

- Provide 100-Gbps wavelengths transport over fully uncompensated networks, with more than 2,500 km of unregenerated optical links
- Enable 100-Gbps transport over very high Polarization Mode Dispersion (PMD)
- Improve overall system density of up to 100-Gbps per slot, which is five times greater than what can be achieved with 40-Gbps units

You can install up to six cards per Cisco NCS 2006 shelf, supporting up to 42 100-Gbps interfaces per 42-rack units (RU) bay frame. It is possible to place up to two 100G TXPs, one 100 G Regen, or one 100 G MXP on a Cisco NCS 2006 shelf.

The 200G-CK-C cards are tunable DWDM trunk cards, which simplify the integration and transport of 100 and 200- Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. The 200G-CK-C card is an enhancement of the 100GS-CK-C card.

The 200G-CK-C cards provide the following benefits:

- Allow choosing 16 QAM and QPSK as the modulation formats at the line side
- Provide Standard G-FEC (Reed-Solomon), Soft Decision FEC (SD-FEC) encoding with 20% overhead, and Hard Decision FEC (HD-FEC) encoding with 7% overhead
- Provide Nyquist filtering for best performance and optimal band usage
- Support gridless tunability
- Allow client access either through the local 100G CPAK interface or through backplane lines
- In MXP-10X10G operating mode, allow 10GE clients (multiplexed on 100G trunk)

Key Features of 200G-CK-C and 10x10G-LC Cards

The 200G-CK-C and10x10G-LC cards support the following key feature:

- Operating Modes—You can configure the cards into multiple operating modes. The cards can be equipped with pluggables for client and trunk options, and offer large variety of configurations. When you configure the card into multiple operational modes, make sure that you complete the following tasks:
  - The card must be preprovisioned and the modes must be configured. None of the modes are provisioned on the card by default. All operating modes are created on the card level. These are card-specific provisioning, which decides the behavior of a particular card.
  - Depending on the card mode selected, the supported payload for that particular card mode must be provisioned on the PPMs. The payloads can be provisioned after configuring the operational mode on the card.

- Protocol Transparency—The 200G-CK-C cards deliver any 100-Gbps services for cost-effective, point-to-point networking. The 10x10G-LC card delivers any 10-Gbps services for cost-effective, point-to-point networking. In case of 100 G muxponder clients that are mapped into OTU4 DWDM wavelength.

Table 61: Transponder Client Configurations and Mapping for a 10x10G-LC Card

Client		Mapping
Format	**Rate (Gbps)**	
10GE LAN-PHY (MXP-10x10G mode)	10.3125	CBR-BMP clause 17.2.4 (ex G sup43 7.1) + GMP ODU2e to OPU3e4
10GE LAN-PHY (MXP-10x10G mode)	10.3125	GFP-F clause 17.4.1 (ex G sup43 7.3) + GMP ODU2 to OPU3e4
10GE LAN-PHY (TXP-10G mode)	10.3125	CBR-BMP clause 17.2.4 (ex G sup43 7.1)
10GE LAN-PHY (TXP-10G mode)	10.3125	GFP-F clause 17.4.1 (ex G sup43 7.3)
OTU2	10.709	ODU transparent + GMP ODU2 to OPU3e4
OTU2e	11.095	ODU transparent + GMP ODU2e to OPU3e4

- Flow-Through Timing—The cards allow the timing to flow through from the client to line optical interface. The received timing from the client interface is used to time the line transmitter interface. This flow-through timing allows multiple cards to be placed in the same shelf but be independently timed fully, independent of the NE timing.
- Far-End Laser Control (FELC)—FELC is supported on the cards.
- Performance Monitoring—The 100-Gbps DWDM trunk provides support for both transparent and non-transparent signal transport performance monitoring. The Digital Wrapper channel is monitored according to G.709 (OTN) and G.8021 standards. Performance Monitoring of optical parameters on the client and DWDM line interface include loss of signal (LOS), Laser Bias Current, Transmit Optical

Power, and Receive Optical Power. Calculation and accumulation of the performance monitoring data is supported in 15-minute and 24-hour intervals as per G.7710. Physical system parameters measured at the wavelength level, like Mean PMD, accumulated Chromatic Dispersion, or Received OSNR, are also included in the set of performance monitoring parameters. These measurements can greatly simplify troubleshooting operations and enhance the set of data which can be collected directly from the equipment.

- Loopback—The terminal, facility, or backplane loopback can be provisioned on all the ports of the 10x10G-LC and 200G-CK-C cards, configured in any operating mode except for the low latency mode. The backplane facility loopback cannot be configured on the 10x10G -LC card that is configured in the MXP-10x10G mode. The loopback can be provisioned only when the port is in OOS-MT state. A new port cannot be provisioned when the backplane loopback is configured on the 10x10G-LC card.
- Fault propagation on 10GE, 40GE, and 100GE clients—A new squelch option that is named LF is supported for GigE payloads. A local fault (LF) indication is fowarded to the client port in the downstream direction when a failure on the trunk port occurs. The LF option is supported for:
  - 10GE payloads on 10x10G-LC cards configured in the:
    - RGN-10G or TXP-10G mode
    - MXP-10x10G mode
  - 100GE payloads on:
    - 200G-CK-C cards configured in the TXP-100G mode
- Trail Trace Identifier—The Trail Trace Identifier (TTI) in the path monitoring overhead is supported in OTU, and ODU OTN frames.
  - 10x10G-LC—OTU4 and ODU4 payloads
  - 200G-CK-C—OTU4 and ODU4 payloads

  The Trail Trace Identifier Mismatch (TTIM) alarm is raised after checking only the SAPI bytes.
- Automatic Laser Shutdown (ALS) can be configured on all ports. ALS is supported only on the ports that are configured with OTU2 and OTU4 payloads.
- GCC channels—can be provisioned on the OTU2 client and trunk ports of the 10 x10G-LC card.
- Pseudo Random Binary Sequence (PRBS)—PRBS allows you to perform data integrity checks on their encapsulated packet data payloads using a pseudo-random bit stream pattern. PRBS generates a bit pattern and sends it to the peer router that uses this feature to detect whether the sent bit pattern is intact or not. The supported PRBS patterns are PRBS_NONE and PRBS_PN31.
- Multivendor Interoperability - The 200G-CK line card can be configured to interoperate with other vendor interfaces. A new option called, Interop Mode is available to disable or enable interoperability. This option is available when the:
  - Modulation format is 100G-QPSK.
  - FEC is set to 7% High Gain FEC.
  - Admin state of the trunk port is set to OOS-DSBLD (Out of service and disabled).

  The behavior and performance of the card that is configured with HG-FEC Multivendor FEC is the same as the old HG-FEC mode. There is no optical performance variation.

Operating Mode for 200G-CK-C Card

Each operating mode can be configured using the specific set of cards and client payloads.

200G Operating Modes

The 200G-CK-LC cards support these 100G operating modes. You can perform the operating mode configuration for the 100G operating modes on the client card.

- TXP-100G (Standalone 100GE Transponder)
- RGN-100G (100G Regenerator)

TXP-100G (Standalone 100GE Transponder)

You can configure the cards as a standalone 100-Gigabit Ethernet transponder. CXP or CPAK and coherent optical trunk supports the 100-Gigabit Ethernet traffic. The 100-Gigabit Ethernet or OTU4 payload traffic is routed from the CXP or CPAK to the optical trunk, passing through the T100 framer and the opposite way. The supported client signals in this mode are 100-Gigabit Ethernet LAN-PHY or OTU4 data rates.

RGN-100G (100G Regenerator)

You can configure the cards as a regenerator. You can connect the two cards to work in back-to-back mode connecting through the chassis backplane in the same shelf. The allowed slot pairs are 2–3, 4–5, 6–7, 8–9, 10–11, 12–13, or 14–15.

The card supports 100-Gigabit Ethernet or OTU4 client signals. Regeneration is performed leveraging on the OTU4 backplane interconnection. OTU4 overhead is terminated, allowing ODU4 to transparently pass through. GCC0 is terminated, while GCC1 and GCC2 are allowed to pass through.

The CXP client is not required because communication between the two cards acting as a regeneration group is supported through the chassis backplane.

400G-XP Card

In this section, "400G-XP" refers to the NCS2K-400G-XP card.

The 400G-XP card is a tunable DWDM trunk card that simplifies the integration and transport of 10 Gigabit and 100 Gigabit Ethernet interfaces and services to enterprises and service provider optical networks. The card is a double-slot unit that provides 400 Gbps of client and 400 Gbps of trunk capacity. The card supports six QSFP+ based client ports that can be equipped with 4x 10 Gbps optics and four QSFP28 or QSFP+ based client ports that can be equipped with 100 Gbps QSFP28 and 4x 10 Gbps QSFP+ optics. The card is capable of aggregating client traffic to either of the two 200 Gbps coherent CFP2 trunk ports.

Note For any card mode except REGEN with slide mode as OPM-10x10G, you can configure a mix of 10G payloads (OTU2, 10GE) on the same slice or client port with the exception of CDR ports (7, 8, 9, and 10). On CDR ports, the first configured 10G lane would determine the configurable payloads for the other three port lanes.

Note If a slice is configured using the OPM_10x10G slice mode, it can be used only for 10G circuit creation whereas if a slice is configured using the OPM_100G slice mode, it can be used only for 100G circuit creation.

Note GCC Rate in the Edit GCC Termination Window is shown as 192K instead of the supported 1200K. This is a known behavior.

Note The maximum short term operating temperature of the shelf must not exceed 50 degrees when the card is installed.

Key Features

The card supports the following key feature:

- • Operating Modes—The card can be configured in various operating modes. The cards can be equipped with pluggables for client and trunk ports, and offer a large variety of configurations. When you configure the card, make sure that the following tasks are completed:
  - The trunk port PPMs must be preprovisioned before configuring the card operating mode. When the card is paired with the 10x10G-LC card, all the operating mode provisioning must performed on the card. The client payloads can be provisioned after configuring the operational mode on the card.

  The table below details the configurations supported on the card for the supported card modes.

  Table 62: Configuration Options for the Card Modes

Configuration	Options		
Card configuration	MXP	REGEN	
Trunk configuration (per trunk)	M_100G	M_100G	
	M_200G	M_200G	
Slice configuration	None	Slice configuration is not supported	None
	OPM_2x40G_2x10G		OPM_100G
	OPM_100G		OPM_10x10G

- Each trunk port functions as a muxponder instance has the following features:
  - The trunk port supports Analog Coherent Optical (ACO) CFP2 coherent pluggable.

Note Before removing the CFP2 pluggable from any of two trunk ports, ensure that the relevant trunk port is set to the OOS (Out-of-service) state. Wait until the trunk port LED turns off. Wait for a further 120 seconds before extracting the CFP2 pluggable.

- Configurable trunk capacity:
  - 100 Gbps coherent DWDM transmission with quadrature phase shift keying (QPSK)modulation.
  - 200 Gbps coherent DWDM transmission with 16-state quadrature amplitude modulation (16-QAM) modulation.
- Configurable trunk FEC: SD-FEC with 15% or 25% overhead.
- Configurable differential/non-differential line encoding.
- Nyquist shaping if channels at trunk TX.
- Flex spectrum tunability over the full extended C-Band.
- 100 Gbps through 100 Gbps QSFP28 client ports.
- 10 Gbps through 4x 10 Gbps QSFP+ client ports.
- 16 Gbps through 4 x 16 Gbps QSFP+ client ports.

- The supported CD ranges are detailed in the table below:

Table 63: CD Range for Card

	200G 16-QAM		100G QPSK	
	Low	High	Low	High
Default Working CD Range	-10000	50000	-20000	90000
Default CD Thresholds	-9000	45000	-18000	72000
Allowed CD Range (Working and Thresholds)	-60000	60000	-280000	280000

- Loopback—The following loopback types are supported:
  - Client ports - Terminal (Inward), Facility (Line)
  - Trunk ports - Terminal (Inward)
- Automatic Laser Shutdown (ALS) can be configured on all the ports.
- 100GE ethernet client ports can be provisioned with or without IEEE 802.3 bj FEC. The options are Auto, Force-Fec-On, Force-Fec-Off.
- Trail Trace Identifier (TTI)—TTI in the section monitoring overhead is supported . Source Access Point Identifer (SAPI), Destination Access Point Identifer (DAPI), and User Operator Data fields are supported in Release 10.6.2 and later releases.
- Trunk Port Interworking—The two CFP2 trunk ports can interoperate with each other when the source and destination cards have the same trunk mode and slice mode configuration.

- GCC0 Support—The card supports provision of GCC0 channel on the trunk port.
- Interoperability—The card is interoperable with the NC55-6X200-DWDM-S card supported on NCS 5500 and the NCS4K-4H-OPW-QC2 Card supported on NCS 4000.

  The following table describes the configurations, payload types, and pluggables supported for interoperability between the card and the NCS4K-4H-OPW-QC2 card.

Table 64: Interoperability with the NCS4K-4H-OPW-QC2 card.

Payload type	Trunk configuration	Pluggables for trunk ports on	Pluggables for client ports on	Pluggables for trunk ports on 4H-OPW-QC2	Pluggables for client ports on 4H-OPW-QC2
100GE	OTU4	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S
100GE	OTU4C2	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S
OTU2	OTU4	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP28-LR4
OTU2	OTU4C2	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP28-LR4
10GE	OTU4	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP-4X10 MLR
10GE	OTU4C2	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP-4X10 MLR

The following table describes the configurations, payload types, and pluggables supported for interoperability between the card and the NC55-6X200-DWDM-S card.

Table 65: Interoperability with the NC55-6X200-DWDM-S card.

Payload type	Trunk configuration	Pluggables for trunk ports on	Pluggables for client ports on	Pluggables for trunk ports on 6X200-DWDM-S	Pluggables for client ports on 6X200-DWDM-S
100GE	OTU4	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S
100GE	OTU4C2	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S

For a detailed list of the supported pluggables, see .

Interoperability

The card has two trunk ports, each supporting up to 20 ODU2es. These ODU2es are numbered from 1 through 20. ODU2es from 1 through 10 belong to the first ODU4 slice and ODU2es from 11 through 20 belong to the second ODU4 slice. Each ODU number has a pre-defined group of timeslots as seen in the following table.

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
Trunk 1 (FAC 10)	Slice 1	1	96	1	1 11 21 31 41 51 61 71
		2	97	2	2 12 22 32 42 52 62 72
		3	98	3	3 13 23 33 43 53 63 73
		4	99	4	4 14 24 34 44 54 64 74
		5	100	5	5 15 25 35 45 55 65 75
		6	101	6	6 16 26 36 46 56 66 76
		7	102	7	7 17 27 37 47 57 67 77
		8	103	8	8 18 28 38 48 58 68 78
		9	104	9	9 19 29 39 49 59 69 79
		10	105	10	10 20 30 40 50 60 70 80
	Slice 2	11	106	1	1 11 21 31 41 51 61 71
		12	107	2	2 12 22 32 42 52 62 72
		13	108	3	3 13 23 33 43 53 63 73
		14	109	4	4 14 24 34 44 54 64 74
		15	110	5	5 15 25 35 45 55 65 75
		16	111	6	6 16 26 36 46 56 66 76
		17	112	7	7 17 27 37 47 57 67 77

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
		18	113	8	8 18 28 38 48 58 68 78
		19	114	9	9 19 29 39 49 59 69 79
		20	115	10	10 20 30 40 50 60 70 80
Trunk 2 (FAC 11)	Slice 1	1	116	1	1 11 21 31 41 51 61 71
		2	117	2	2 12 22 32 42 52 62 72
		3	118	3	3 13 23 33 43 53 63 73
		4	119	4	4 14 24 34 44 54 64 74
		5	120	5	5 15 25 35 45 55 65 75
		6	121	6	6 16 26 36 46 56 66 76
		7	122	7	7 17 27 37 47 57 67 77
		8	123	8	8 18 28 38 48 58 68 78
		9	124	9	9 19 29 39 49 59 69 79
		10	125	10	10 20 30 40 50 60 70 80
	Slice 2	11	126	1	1 11 21 31 41 51 61 71
		12	127	2	2 12 22 32 42 52 62 72
		13	128	3	3 13 23 33 43 53 63 73
		14	129	4	4 14 24 34 44 54 64 74

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
		15	130	5	5 15 25 35 45 55 65 75
		16	131	6	6 16 26 36 46 56 66 76
		17	132	7	7 17 27 37 47 57 67 77
		18	133	8	8 18 28 38 48 58 68 78
		19	134	9	9 19 29 39 49 59 69 79
		20	135	10	10 20 30 40 50 60 70 80

When the card interoperates with NCS4K-4H-OPW-QC2 card, the first ODU4 slice of the trunk is connected to the second ODU4 slice of the same NCS4K-4H-OPW-QC2 trunk.

Note The ODU circuit between the and NCS4K-4H-OPW-QC2 cards is created even when the ODU number is incorrect. Please ensure that the correct source and destination ODU numbers are selected.

Regeneration Mode for 400G-XP-LC

From Release 10.8.0, the 400G-XP-LC can be configured as a regenerator. The regeneration functionality is available only on the trunk ports. A new card operating mode, REGEN, is available. No client ports are involved. The two trunk ports must have the same rate to achieve regeneration (wavelengths and FEC of the trunks can vary).

Note For traffic to flow in the REGEN mode, it is mandatory that the 400G-XP-LC should be running on firmware (SCP) version 5.24 or later.

We recommend that you use the REGEN mode only with the MXP operating mode (the output from the MXP trunk of a can be connected to trunk ports in REGEN mode).

1.2T-MXP Card

Table 66: Feature History

Feature	Release Information	Description
1.2T-MXP Card		This card triples the per slot throughput of the NCS 2000 system from 200 Gbps to 600 Gbps. The DCO trunk ports of the card can support up to 400-Gbps data-rate with multiple modulation formats, encoding types, and FEC options. This card can be installed in the NCS 2006 and NCS 2015 chassis.

In this section, "1.2T-MXP" refers to the NCS2K-1.2T-MXP card.

The 1.2Tbps Transponder or Muxponder line card (1.2T-MXP) is the first line card to have a 400G trunk and 400GE client interface in the NCS 2000 platform. It is a two-slot card that triples the per slot throughput of the NCS 2000 system from 200 Gbps to 600 Gbps.

The 1.2T-MXP card has three QSFPDD56 or QSFP28 client ports, five QSFP28 client ports, and three CFP2 DWDM Digital Coherent Optics (DCO) trunk ports. The QSFPDD56 client ports can also be used alternately as QSFP28 ports on an individual port. The DCO ports can support up to 400-Gbps data-rate with multiple modulation formats, encoding types, and FEC options. You can configure the 1.2T-MXP card in different ways with a maximum of 1.2Tbps total traffic on the client side (QSFP-DD/28) and the 1.2Tbps total traffic on the trunk side.

The 1.2T-MXP card can be installed in:

- NCS 2006 chassis that can accommodate a maximum of three 1.2T-MXP cards.
- NCS 2015 chassis that can accommodate a maximum of seven 1.2T-MXP cards.

The 1.2T-MXP card coexists with other NCS 2000 line cards without restricting their functionalities. However, it does not interoperate with any other line cards.

Key Features of 1.2T-MXP

The key features are:

- Enhanced muxponder or transponder capabilities while enabling double-slot card with 100GE or 400GE client type.
- O-FEC encoding on the trunk interface.
- Nyquist filtering for OSNR.
- Supports configurable modulation format such as 300 8QAM, 400 16QAM, PAM4, and 16QAM in both Open ROADM and 400ZR+ framing mode.
- Flex spectrum support with Nyquist filtering.
- ZR+ based framing on trunk.

- 3x400GE client bandwidth using QSFP-DD or 12x100GE client bandwidth using QSFP-DD (break-out mode)
- LLDP support on 100GE or 400GE clients.
- Supports secure boot.
- Alarms for ZR interface and, Alarms, Performance, and Statistics for GE interface as well as Optical Pluggable.
- Diagnostics and maintenance support.
- Supports GroupId that uniquely identifies a group of physical ports in a ZR frame.

Supported Pluggables

The supported pluggables are:

- Three CFP2 400G DCO trunk pluggables
- Eight QSFP28 or three QSFP-DD pluggables
- Five QSFP28 client pluggables

Limitations of 1.2T-MXP Card

The following are the limitations of the 1.2T-MXP card:

- Optics PMs are not supported by Active Optical Cable (AOC) PPM.
- GroupID feature is not supported for 400GE transponder configuration.
- I-port management is not supported.
- OTN is not supported on trunk.
- Traffic does not go down when FlexO-SR Interface Trail Trace Identifier Mismatch (FOIC-TIM) alarm is raised.
- There might be traffic fluctuations affecting some switches and routers due to the following scenario:

  When there is a 400GE or 4x100GE traffic congestion on the pluggables, an electrical squelch or unsquelch is performed for one second on the transmit side of the pluggables. This operation relocks the transmit Clock and Data Recovery (CDR) of the pluggables. This results in an out-of-range frequency on the client for four to six seconds before the traffic clears.

  This issue occurs in pluggables such as QSFP-DD DR4, QDD-400G-FR4, QDD-400G-LR8, QDD-400-AOC1M, QDD-400-AOC2M, QDD-400-AOC3M, QDD-400-AOC5M, QDD-400-AOC7M, QDD-400-AOC10M, and QDD-400-AOC15M.

Operating Modes and Slice Definition in the 1.2T-MXP Card

Operating Modes

You can configure the 1.2T-MXP card in the TXPMXP mode. The following are the suboperating modes:

- OPM-400G—Enables 400GE client on the QSFP DD port, when the trunk is at 400G rate.

- OPM-4x100G-DD—Enables four 100GE clients that use four-level Pulse Amplitude Modulation (PAM4), on one QSFP DD port, when the trunk is at 400G rate.
- OPM-3x100G-DD—Enables three 100GE clients that use PAM4, on one QSFP DD port, when the trunk is at 300G rate.
- OPM-4x100G—Enables 100GE clients over four QSFP28 ports, when the trunk is at 400G rate.
- OPM-3x100G—Enables 100GE clients over three QSFP28 ports, when the trunk is at 300G rate.

The slices are configured based on the required data path configuration. The following table explains the suboperating modes that are enabled on trunk ports for each slice:

Table 67: Sub-Operating Modes

Slice	Trunk Port	Supported Sub-Operating Modes
Slice 1	9	• OPM-400G • OPM-4x100G-DD • OPM-3x100G-DD
Slice 2	10	• OPM-400G • OPM-4x100G • OPM-4x100G-DD • OPM-3x100G
Slice 3	11	• OPM-400G • OPM-4x100G • OPM-3x100G

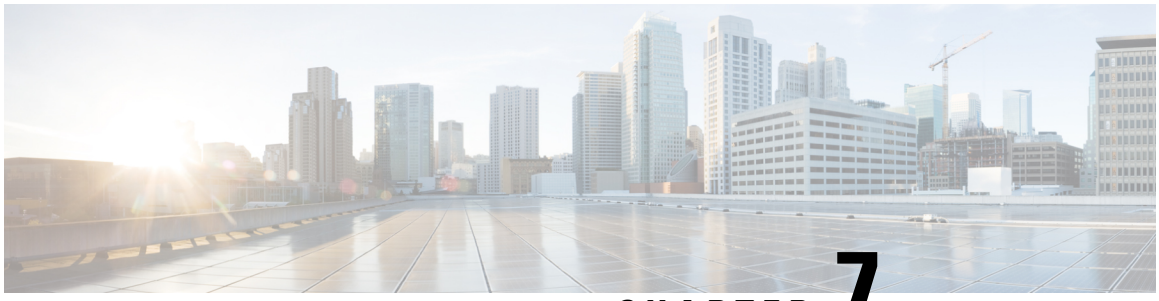
You can use the 1.2T-MXP card in different configurations. The following table describes the combinations of suboperating modes, the trunk ports, and client ports for each slice:

Note In the combinations described, you can also choose to configure only one of the slices 1–3.

Table 68: Different Combinations of Sub-Operating Modes

Configuration	Sub-Operating Modes	Trunk Ports	Client Ports
400GE Transponder—Includes 3x400G trunk, 3x400GE client with 3xQSFP-DD pluggables	Slice 1: OPM-400G	9	6
	Slice 2: OPM-400G	10	7
	Slice 3: OPM-400G	11	8

Configuration	Sub-Operating Modes	Trunk Ports	Client Ports
12x100GE Muxponder—Includes 3x400G trunk, 12x100GE client with 2xQSFP-DD breakout + 4xQSFP28 pluggables	Slice 1: OPM-4x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3, 6.4)
	Slice 2: OPM-4x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3, 7.4)
	Slice 3: OPM-4x100G	11	2, 3, 4, 8
9x100GE Muxponder—Includes 3x300G trunk, 9x100GE client with 1xQSFP-DD breakout + 6xQSFP28 pluggables	Slice 1: OPM-3x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3) 6.4 is unused.
	Slice 2: OPM-3x100G	10	1, 5, 7
	Slice 3: OPM-3x100G	11	3, 4, 8
Mixed Configuration 1	Slice 1: OPM-400G	9	6
	Slice 2: OPM-4x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3, 7.4)
	Slice 3: OPM-3x100G	11	3, 4, 8



CHAPTER 7

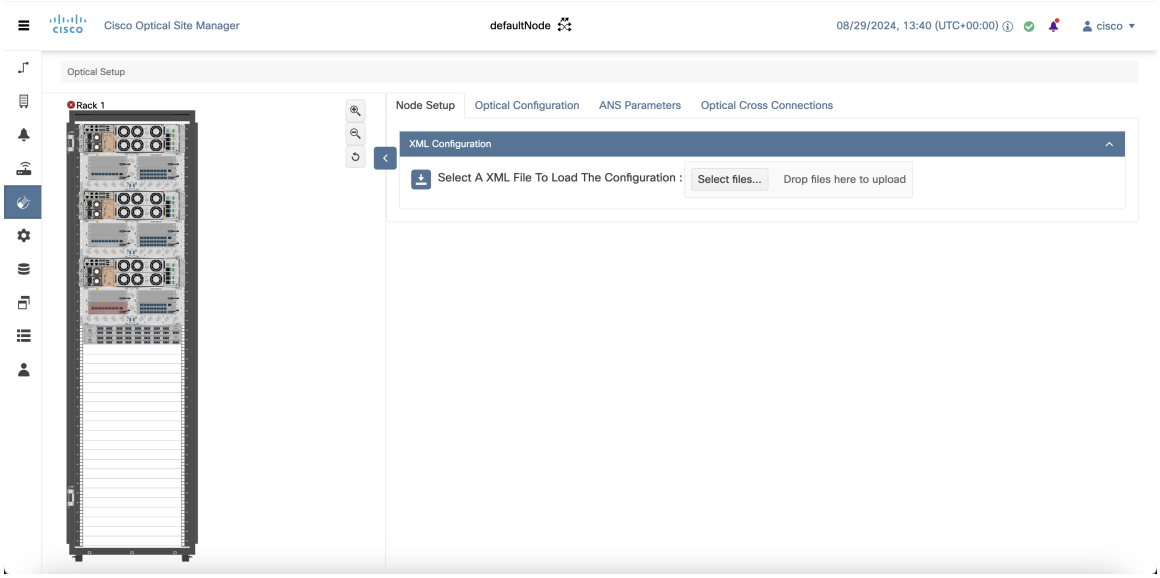
Configure the Node

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 27: Configure the Node



- Import a Cisco Optical Network Planner configuration file, on page 168
- Optical Degrees, on page 170
- Internal patch cords, on page 171
- Automatic Power Control, on page 174

- Span Loss Measurement, on page 178
- Configure amplifier parameters, on page 180
- Provision interface parameters, on page 183
- Provision Raman Amplifier Parameters, on page 185
- Manage Raman Interface Parameters, on page 187
- Optical cross-connect circuits, on page 189
- Submarine Line Terminating Equipment mode, on page 198
- GMPLS UNI, on page 200
- DCN Extension, on page 208
- Remote Node Management Using GCC, on page 210

Import a Cisco Optical Network Planner configuration file

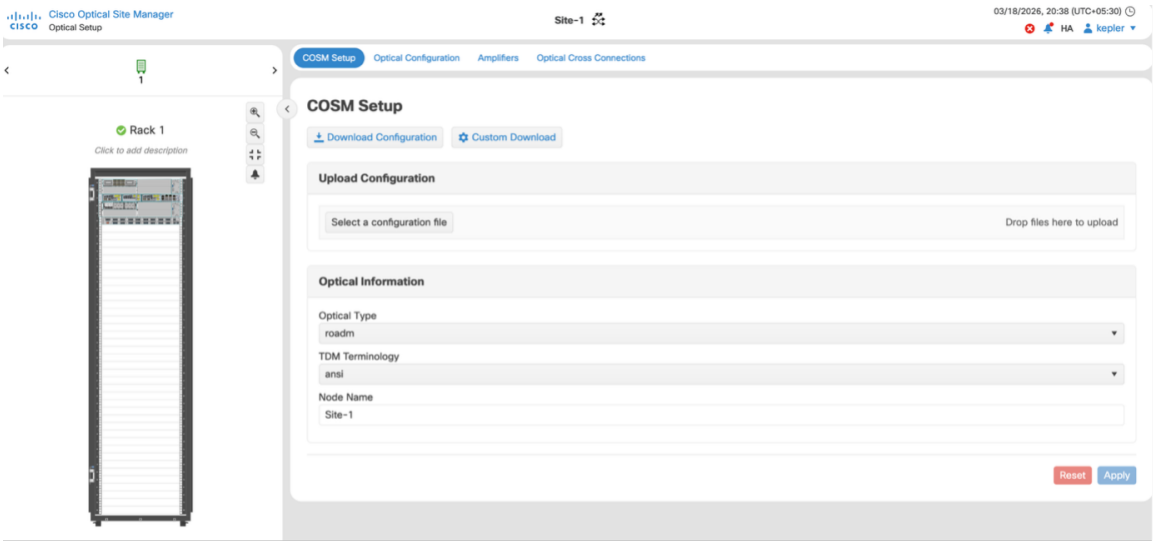
Use this task to import a Cisco Optical Network Planner NETCONF file (.xml) into Cisco Optical Site Manager to configure device parameters automatically.

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 28: 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 47

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.

You can also create IPC between trunk ports of one line card and the client ports of another line card, optimizing data flow across various line cards. These IPC can be viewed in the NFV, where optical types are selected as **txp** and **roadm**.

Additional information

Table 69: Feature History

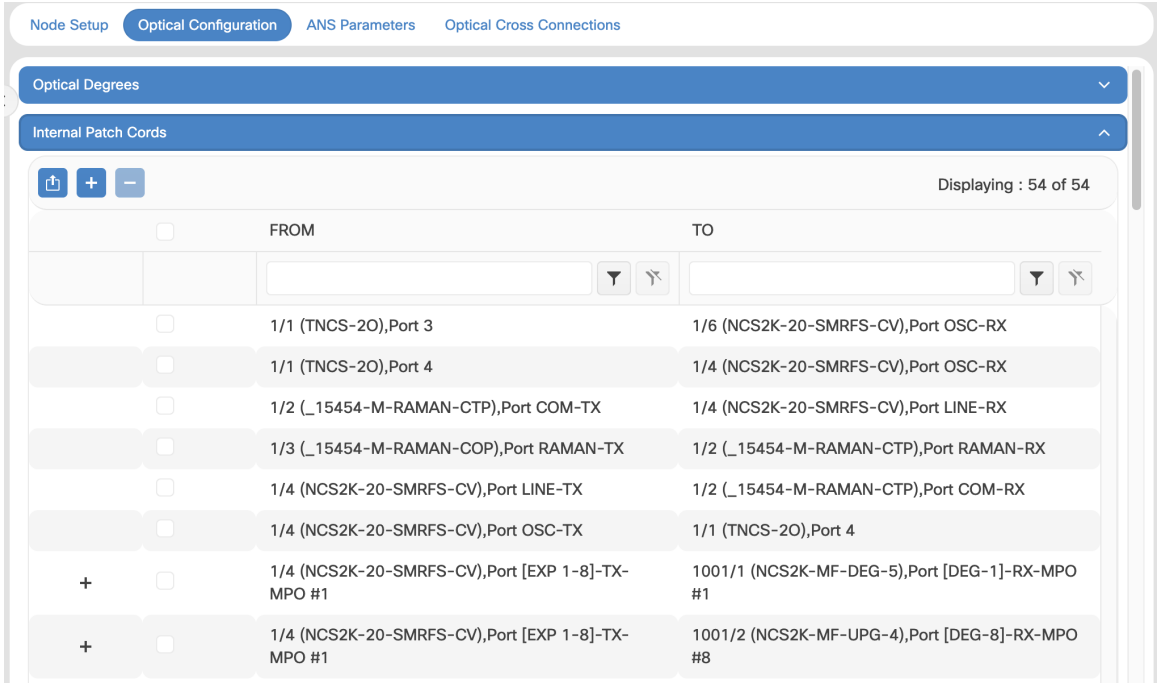
Feature Name	Release Information	Description
Support for Trunk and Client Port Connections	Cisco IOS XR Release 25.1.1	Cisco Optical Site Manager now allows one or more trunk ports on line cards to feed multiple line cards via client ports. This feature supports real and pre-provisioned line cards and is visible in NFV view with optical types **txp** and **roadm**. It enables IPC connections between trunk ports and client ports, allowing for efficient data flow across various line cards.

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 29: Internal Patch Cords



Before you begin

Log into Cisco Optical Site Manager, on page 1

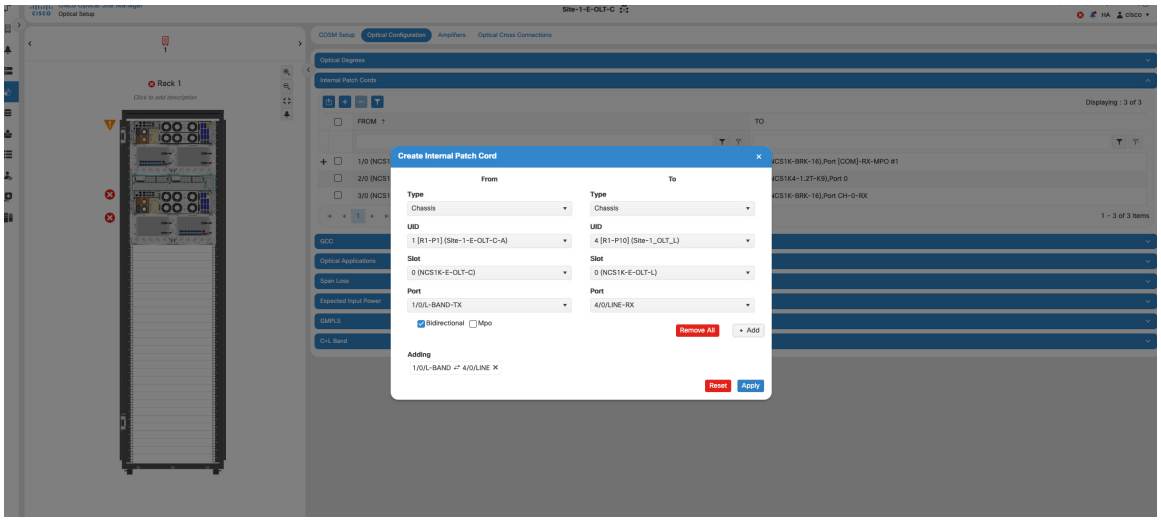
Follow these steps to create internal patch cords.

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.

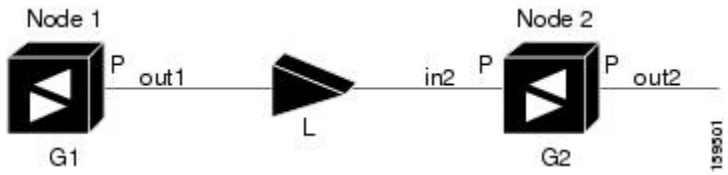
The amplifier software uses a control gain loop to keep channel power constant regardless of the number of channels. It monitors input power changes and adjusts output power proportionately. The shelf controller software emulates the control output power loop to compensate for fiber degradation.

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 30: 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. 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.
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.

Table 70: Feature History

Feature Name	Release Information	Description
Amplifier Working Mode Support for NCS 1001	Cisco IOS XR Release 25.4.1	You can now choose between **Channel Power** and **Fixed Gain** modes when configuring the working mode for Cisco NCS 1001 cards in the **Amplifier** section of the **Provisioning** tab. In **Channel Power** mode, the amplifier keeps each channel at a set power.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Open the card view, on page 31

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 71: 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.	• Channel Power: Available for NCS 1001 crads • Total Power • Optimized • Fixed Gain: Available for NCS 1001 crads • Start and Hold
Role	Role of the amplifier.	• Preamplifier • Booster
Actual Gain (dB)	Actual gain setpoint.	—
Target Gain (dB)	Target gain setpoint.	—
Tilt Setpoint (dB)	Target output tilt requested by the user.	—

Parameter	Description	Displayed Values
PSD Setpoint (dBm/12.5 GHz)	Set this when **Working Mode** is selected as **Channel Power**. Target output power requested by the user for each circuit. **Note** • This option is only available for NCS 1001 cards. • If **Channel Power Setpoint (dBm)** is set, do not set **PSD Setpoint (dBm/12.5 GHz)**.	Valid range: Upto *+10dBm*
Channel Power Setpoint (dBm)	Set this when **Working Mode** is selected as **Channel Power**. Channel Power Setpoint defines the target transmit power level for an individual optical channel (wavelength). It's essential for optimizing signal strength, preventing overload, and maintaining overall signal quality across the optical network. **Note** • If **PSD Setpoint (dBm/12.5 GHz)** is set, do not set **Channel Power Setpoint (dBm)**. • This option is only available for NCS 1001 cards.	Valid range: - *40dBm* to *+30dBm*
PSD Optimized (dBm/GHz)	Optimized PSD	—
Gain Setpoint (dB)	Set this when **Working Mode** is selected as **Fixed Gain**. Target amplifier gain requested by the user.	—
Gain Range	Sets the gain range of the amplifier.	• Gain Range 1 • Gain Range 2 • No Gain Range
Power Degrade Threshold (High) (dBm/GHz)	Shows the current value of the optical power degrade high threshold.	—

Parameter	Description	Displayed Values
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. 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.	—
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. 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 31

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 72: Interface Options

Parameter	Description	Options
Port	Displays the port number, port type, and direction (RX or TX).	All RX and TX ports (Display only)
Admin State	Sets the administrative state of the port.	• Unlocked / IS • Locked, disabled / OOS, DSBLD • Locked, maintenance / OOS, MT • 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 • OOS-AU, AINS / Unlocked-disabled, automaticInService • OOS-MA, DSBLD / Locked-enabled, disabled • 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.	—

Parameter	Description	Options
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.	—
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 31

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 73: 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. • Co-Propagating for the RAMAN-COP card.
Calibration Type	Calibration type that the card uses. 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 • Manual • 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 74: 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).
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 31

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 75: 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
Admin State	Sets the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • 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/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ 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. 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. 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 76: 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.
	b. Run the **cosm** command from the IOS XR prompt.
	`RP/0/RP0/CPU0:ios#cosm`
	`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.
	`RP/0/RP0/CPU0:ios#bash`
	`[node0_RP0_CPU0:~]$`
	b. Access the **COSM** container.
	`[node0_RP0_CPU0:~]$ docker exec -it COSM bash`
	`[COSM:/]$`
	c. Log in to the Cisco Optical Site Manager CLI by using the **ncs_cli -C -u** command and the Cisco Optical Site Manager username.
	`[COSM:/]$ ncs_cli -C -u cisco1`
	`User cisco1 last logged in 2026-05-13T07:36:57.343064+00:00, to COSM, from 127.0.0.1 using cli-console`
	`cisco1 connected from 127.0.0.1 using console on COSM`
	`NODE01:cosm#`
	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.

Submarine Line Terminating Equipment mode

The NCS 1010 optical line system supports SLTE mode configuration through Cisco Optical Site Manager, enhancing compatibility and control for subsea deployments.

SLTE configuration in Cisco Optical Site Manager

Cisco Optical Site Manager allows you to configure these parameters for SLTE mode, streamlining subsea system management and optimization.

- Manual ASE loading: Controls ASE source injection for channels.
- ASE attenuation setpoint: Sets attenuation level for ASE channels.
- OXC restoration soak time: Defines restoration timing after failures.
- ASE guard band: Configures protection bandwidth for ASE.

Enable or disable submarine mode

The Submarine Mode toggle button, located in the Optical Degrees panel, allows you to enable or disable Submarine Line Terminal Equipment (SLTE) parameters.

- Enabling Submarine Mode disables Link Power Control, Gain Estimator, and Link Tuner, sets static-ASE-disable, and shuts down OSC ports.
- Disabling Submarine Mode enables Link Power Control, Gain Estimator, and Link Tuner, activates OSC ports, and removes static-ASE-disable from XR.

The Manual Ase loading parameter in the interface panel (under OLT-C > Amplifier) is directly linked to the Submarine Mode toggle. If Manual Ase loading is enabled from the interface panel, the Submarine Mode button will show as enabled, and vice versa.

Activating Submarine Mode can disrupt network traffic if it is not performed by an optical expert. When you activate Submarine Mode, the system displays a confirmation message that lists the functionalities disabled by this change.

Before you begin

- Log into Cisco Optical Site Manager, on page 1
- Provision these interface parameters:
  - Manual Ase loading
  - Ase Attenuation Setpoint
  - OSC Restoration Soak Time, and
  - Ase Guard Band

Procedure

Step 1 Click **Optical Setup** in the left panel, then click the **Optical Configuration** tab.

Step 2 Expand **Optical Degrees** section, then click the **Edit** button.

Step 3 Locate the desired optical degree in the table.

Step 4 Under the **Submarine Mode** column, toggle the button to either enable or disable the mode.

A confirmation dialog box appears, warning that activating submarine mode will disable functionalities such as Link Power Control, Gain Estimator, and Link Tuner.

Step 5 Click **Yes** to enable submarine mode, or **No** to cancel the operation.

Step 6 Under the **Optical Cross Connections** tab, select **signal** from the **Power Source** column for the optical degree.

Step 7 (Optional) Follow these steps to initiate manual ASE loading:

a) Open the OLT-C card from the topology view.
b) Expand the **Alarms** tab at the bottom of the screen. Next, select the **OCM** tab.
c) Click the **Manual Attenuation Tuning** button.
The **Attenuation Tuning** window appears.
d) Click a channel in the graph and set the values for **Optical Attenuation** and **Ase Attenuation**.
e) Click **Continue**.
The system processes and applies the configuration. This may take a few minutes.

The system applies the selected Submarine Mode setting and automatically adjusts the associated network parameters.

GMPLS UNI

Table 77: Feature History

Feature Name	Release Information	Description
GMPLS UNI Circuit Connection	Cisco IOS XR Release 25.1.1	You can now establish circuit connections between two clients within an optical network using the Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI). This connection is facilitated through signaling exchanges between UNI Client (UNI-C) nodes, which are router nodes, and UNI Network (UNI-N) nodes, which are optical nodes. This integration enables effective usage of the DWDM grid with minimal wastage of spectral bandwidth and allows the transmission of mixed bit-rate or mixed modulation data in a grid with different channel widths.

The Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI) creates a circuit connection between two clients (UNI-C) of an optical network.

GMPLS UNI Advantages

GMPLS UNI plays a crucial role in connecting and optimizing network functionalities:

- GMPLS UNI allows packet networks to directly access the optical transport control plane, enabling coordination of resource requirements with the optical transport network.
- By leveraging open standards, GMPLS UNI optimizes network resources and enhances utilization across both packet and optical networks.

Channel Spacing Types in GMPLS

GMPLS supports two types of channel spacing, each affecting the capacity and flexibility of traffic management:

- **Fixed Grid Channel Spacing:** This spacing is fixed at 50 GHz, supporting traffic rates of 100 and 200 Gbps.
- **Flexible Grid Channel Spacing:** This spacing is set at 6.25 GHz, accommodating all data rates.

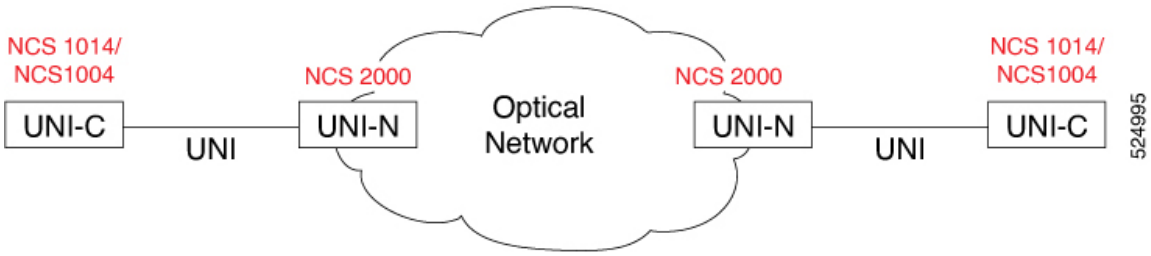
How to Create a GMPLS UNI Tunnel

Before you begin

- The NCS 2000 node must possess a valid license for ROADM and WSON support.
- Management IP addresses for both NCS 1014/NCS 1004 and NCS 2000 nodes must be accessible.
- The administrative state of the trunk port of the optics controller on the NCS 1014 or NCS 1004 node must not be in the shutdown state.

Workflow

Figure 31: GMPLS UNI Tunnel Between two NCS 1014/NCS 1004 Nodes



Creating a tunnel between two NCS 1014 or NCS 1004 nodes on a network involves establishing a connection from the headend to the tailend. The tunnel can be created between the source and destination NCS 1014 or NCS 1004 nodes without involving NCS 2000 nodes in the middle. The NCS 2000 provides GMPLS control plane support and enables dynamic provisioning and rerouting of lightpaths.

These stages describe how to create a connection between the NCS 1014 and NCS 2000 at the headend of the network.

1. Add a card mode on the NCS 1014 or NCS 1004 card. For more details, see NCS 1000 line card modes, on page 67.
2. Create internal patch cords, on page 172 between the NCS 1014 or NCS 1004 and NCS 2000 ports.
3. Create static Link Management Protocol link for GMPLS, on page 202 to establish connectivity between a NCS 2000 node and a NCS 1014 or NCS 1004 node.
4. Create Optical Cross Connections using Cisco Optical Network Controller.

Repeat the same steps at the tailend of the network to ensure complete connectivity.

Create static Link Management Protocol link for GMPLS

Table 78: Feature History

Feature Name	Release Information	Description
Static Link Management Protocol configuration for GMPLS	Cisco IOS XR Release 25.1.1	You can now configure static Link Management Protocol (LMP) using the Cisco Optical Site Manager web UI to establish connectivity between an NCS 2000 node and NCS 1004 and NCS 1014 nodes for GMPLS UNI. This protocol efficiently manages the control channel across GMPLS UNIs, ensuring smooth Traffic Engineering (TE) link connectivity between interfaces. Furthermore, it performs fault management functions, helping in fault isolation, link property correlation, and verifying link connectivity.

Link Management Protocol (LMP) manages and maintains the control and data links between nodes while overseeing the channels and links necessary for routing, signaling, and comprehensive link management. The LMP link is created to establish connectivity between an NCS 2000 node and an NCS 1004 node.

LMP effectively manages the control channel across the GMPLS UNIs, ensuring seamless Traffic Engineering (TE) link connectivity between these interfaces. Also, it performs fault management, aiding in fault isolation, link property correlation, and verifying link connectivity.

To to create LMP to establish connectivity between an NCS 2000 node and an NCS 1004 node, using the **LMP Configuration Wizard** in Cisco Optical Site Manager, perform these tasks:

- Select the LMP type, on page 202
- Select the optical parameters for LMP, on page 203
- Select the End Points for LMP, on page 204
- Verify the LMP configurations, on page 205
- Create LMP regeneration pair, on page 205

Select the LMP type

The **LMP Type** area in the Cisco Optical Site Manager **LMP Configuration Wizard** allows users to choose from various LMP Types.

Use this task to enter the **LMP Configuration Wizard** and select a card mode.

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 **GMPLS** > **LMP** to expand it.

Step 3 Click the + button to open LMP Configuration Wizard.

a) From the **LMP Type** drop-down list, choose the type of LMP.

If the LMP link is going to be established with	Select...
NCS 1004 or 1014 device	LOCAL TXP/OCHNC
NCS 1004 or NCS 4000 routers	Signaled
a TXP in a remote NCS 2000 ROADM node	Remote TXP

Note The LOCAL TXP/OCHNC and Remote TXP systems support a multi-carrier configuration, which involves bundling two Add & Drop ports to enable inverse multiplexing of traffic across trunks. This approach optimizes bandwidth distribution. However, the Signaled LMP does not support multi-carrier configuration.

Step 4 Click **Next**.

Select the optical parameters for LMP

Use this task to configure various optical parameters for different LMP types:

Before you begin

Select the LMP type, on page 202

Procedure

Step 1 Enter a name for the LMP in the Description field.

NCS 1014 does not support GMPLS-UNI.

Step 2 Choose the **TXP Controller Mode**.

This field is available only for **Local TXP/ OCHNC** LMP type. The available options are:

TXP mode	Applicable for
RSVP (GMPLS)	NCS 1004
Local	NCS 1004

TXP mode	Applicable for
Controller	NCS 1014

Step 3 Choose the **Alien ID**, **Trunk Mode**, and **FEC Mode**. See FEC modes and Trunk modes supported for Alien IDs, on page 206 for the list of aline ids and its corresponding trunk modes and FEC modes.

This field is available only for **Local TXP/ OCHNC** LMP type, and **Signaled** LMP type with Add/Drop End-Point Type.

Step 4 Choose the UNI Control Mode as UNI-Clinet or UNI-Netwrok.

This field is available only for **Signaled** LMP type.

Step 5 Select the **Channel Mode** as **Flex** or **DWDM**.

Step 6 If required, enter the **Remote Node Address** and **Remote IF Index**.

Step 7 Check the **Is Local** checkbox, to configure the UNI parameters on the client port of the TXP card

This check-box is available only for **Signaled** LMP type.

Step 8 Click **Next**.

Select the End Points for LMP

Use this task to select the end points for the LMP:

Before you begin

Select the optical parameters for LMP, on page 203

Procedure

Step 1 In the Ingress Port Selection and Egress Port Selection areas:

a) From the **Type** drop-down list, select **Chassis**, **Passive Unit**, or **Passive Chassis**.
b) From the **UID** drop-down list, select the UID.
c) From the **Slot** drop-down list, select the slot.
d) From the **Port** drop-down list, select the port.
e) Enter a name in the **Remote Description** field.

Step 2 Click **Next**.

What to do next

Verify the LMP configurations, on page 205.

Verify the LMP configurations

In the **Configuration Recap** window, verify the selected configurations across the various windows of the **LMP Configuration Wizard**.

Before you begin

Select the End Points for LMP, on page 204

Procedure

Step 1 Click to expand the **Type**, **Optical Parameters**, and **End Points** sections to verify the configured details.

Step 2 Click **Finish** to complete the LMP configuration.

What to do next

Create LMP regeneration pair, on page 205.

Create LMP regeneration pair

You can create regeneration pair to create a regeneration path for longer link. Use this task to create a regeneration pair.

Before you begin

Create the required number of LMP links using these tasks:

- Select the LMP type, on page 202
- Select the optical parameters for LMP, on page 203
- Select the End Points for LMP, on page 204
- Verify the LMP configurations, on page 205

Procedure

Step 1 Select the LMPs to be added to the regeneration path.

Note You can add only the RSVP type of LMPs into the pair.

Step 2 Click **Regen Pair**.

The regen pair gets created and you can view the same under the **LMP Regen** tab.

FEC modes and Trunk modes supported for Alien IDs

This table lists the optical interfaces (Alien IDs) supported for all LMP types, along with their corresponding trunk modes and FEC modes.

Table 79: Alien IDs supported for LMP

Alien ID	Trunk Mode	FEC Modes
100G-LC-C	Default-Mode	STANDARD_FEC, HG_FEC_7, SD_FEC_20
100G-CK-C	Default-Mode	STANDARD_FEC, HG_FEC_7, SD_FEC_20
200G-CK-LC	100G-Mode	STANDARD_FEC, HG_FEC_7, SD_FEC_20
	200G-Mode	SD_FEC_20
100GS-CK-LC	100G-Mode	STANDARD_FEC, HG_FEC_7, SD_FEC_20
	200G-Mode	SD_FEC_20
400G-XP-LC-CFP2	100G-Mode	SD_FEC_15_DE_ON, SD_FEC_15_DE_OFF, SD_FEC_25_DE_ON, SD_FEC_25_DE_OFF
	150G-Mode	SD_FEC_15_DE_ON, SD_FEC_15_DE_OFF, SD_FEC_25_DE_ON, SD_FEC_25_DE_OFF
	200G-Mode	SD_FEC_15_DE_ON, SD_FEC_15_DE_OFF, SD_FEC_25_DE_ON, SD_FEC_25_DE_OFF
NCS10x4 (NCS1K4-1.2T-K9, NCS1K4-2-QDD-C-K9)	200G-Mode	SD_FEC_27
	200G-2dot3125-BPS-Mode	SD_FEC_27
	300G-3-BPS-Mode	SD_FEC_27
	300G-3dot4375-BPS-Mode	SD_FEC_27
	400G-Mode	SD_FEC_27
	400G-4dot4375-BPS-Mode	SD_FEC_27
	500G-Mode	SD_FEC_27
	600G-Mode	SD_FEC_27

Alien ID	Trunk Mode	FEC Modes
ONS-CFP2D-400G-C-FOIC(NCS1K4-OTN-XP)	400G-Mode	OFEC
	300G-Mode	OFEC
	200G-4-BPS-Mode	OFEC
	200G-2-BPS-Mode	OFEC
	200G-3-BPS-1-E-Mode	OFEC
	200G-4-BPS-1-E-Mode	OFEC
	100G-1-S-Mode	OFEC
DP04QSDD	100G-Mode	OFEC
	200G-Mode	OFEC
	200G-4-BPS-Mode	OFEC
	200G-6-BPS-Mode	OFEC
	200G-8-BPS-Mode	OFEC
	200G-0-S-Mode	OFEC
	300G-0-S-Mode	OFEC
	400G-0-S-Mode	OFEC
NCS1K(NCS1002-K9)	100G-Mode	STANDARD_FEC, HG_FEC_7, SD_FEC_20
DCO-CFP2-8QAM-200G	200G-Mode	SD_FEC_15_DE_ON
QSFP-DD-ZR	400G-Mode	CFEC
QSFP-DD-ZR+	100G-Mode	OFEC
	300G-Mode	OFEC
	200G-4-BPS-Mode	OFEC
	200G-6-BPS-Mode	OFEC
	200G-8-BPS-Mode	OFEC
	200G-0-S-Mode	OFEC
	300G-0-S-Mode	OFEC
	400G-Mode	CFEC, OFEC
	400G-0-S-Mode	OFEC

Alien ID	Trunk Mode	FEC Modes
ONS-CFP2D-400G-C (NCS1K4-1.2T-MXP)	100G-Mode	OFEC
	300G-Mode	OFEC
	200G-4-BPS-Mode	OFEC
	200G-6-BPS-Mode	OFEC
	200G-8-BPS-Mode	OFEC
	200G-0-S-Mode	OFEC
	300G-0-S-Mode	OFEC
	400G-Mode	OFEC
	400G-0-S-Mode	OFEC
• CIM8-C-K9 • CIM8-CE-K9 • CIM8-LE-K9	• 400G-Mode • 500G-Mode • 600G-Mode • 700G-Mode • 800G-Mode • 900G-Mode • 1000G-Mode • 1100G-Mode • 1200G-Mode	SD_FEC_15

DCN Extension

External links are the logical links between two optical degrees that belong to two adjacent nodes. From this release, you can add one or more external links on a node using different optical degrees configured on that node. The creation of an external link allows the management of a remote node and these external links are used when it is not possible to create an optical-service-channel (OSC) communication.

Cisco Optical Site Manager enables you to create and provision external logical links between a source local node and a destination remote node. These nodes use local and remote degrees and require IP addresses of the NCS 2000 devices.

Limitations for DCN Extension

- If any external link is already configured for a degree on a device, then you cannot use that degree for another external link on the same node or device. To achieve this, you should delete the existing external link and create a new external link on the same degree of the device.

- You cannot delete the degree if that degree is already used by an external link.

Manage DCN Extension

Use this task to add, view, or delete external links on the node.

Before you begin

Log into Cisco Optical Site Manager, on page 1

Ensure that the degrees are existing in the node before configuring external links.

Procedure

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

Step 2 Click the **Optical Configuration** > **External Links** tabs.

Step 3 Perform these steps, as needed.

a) To add a new external link, perform these steps:

1. Click the + button.

   The **New External Link** dialog box appears.

2. In the **Local IP** field, the Local IP address of Cisco Optical Site Manager instance that you are connected gets displays.
3. Enter username of the remote user who is allowed to perform configuration on the remote Cisco Optical Site Manager instance in the **Remote Username** field.
4. Enter password of the remote user who is allowed to perform configuration on the remote Cisco Optical Site Manager instance in the **Remote Password** field.
5. Enter the IP address of an Cisco Optical Site Manager instance that you want to get connected in the **Remote IP** field.
6. Click the refresh (image) button at the end of the **Remote IP** field. The details from the remote node are fetched to allow the configuration.
7. From the **Local Degrees** drop-down list, select the available local degrees to create a starting point for the external link connection.
8. From the **Remote Degrees** drop-down list, select the available remote degrees to create an ending point for the external link connection.

Note If no degree is displayed, check the remote Cisco Optical Site Manager instance to configure the degrees.

9. Click **Add**.

The external link is added to the table of the local and remote Cisco Optical Site Manager **Node Configuration** pages. The table displays the following information under the **External Links** section of the **Node Configuration** page:

- **Local Degrees**—Specifies the local degree on which the external link is created.
- **Interfaces**—Specifies the interfaces on which the external link is created.
- **Connected To**—Specifies the remote node instance to which it is connected. You can click the remote node instance link that is connected and it opens the remote node Cisco Optical Site Manager instance. If nothing is displayed, then the local endpoint is not connected.
- **Local IP**—Specifies the IP address of the NCS 2000 device on which the external link is created.
- **Remote IP**—Specifies the NCS 2000 remote device IP address which is the end of the external link connection.

b) To delete the external link, perform these steps:

1. Check the check boxes corresponding to the external link that you want to delete.
2. Click the - button to delete the selected external link.

   A confirmation message appears. You must authenticate with the username and password for the remote Cisco Optical Site Manager instance to which the external links are connected.
3. Click **Yes**.

   The external link is deleted from both the local and remote Cisco Optical Site Manager instances.

Remote Node Management Using GCC

The remote node management feature allows you to remotely manage NCS 2000 devices with transponder cards using the in-band General Communication Channel (GCC) channels with fiber optics from OTN clients. You can only use the Cisco Light Web UI on the NCS 2000 node to create and manage the GCC channel to the remote NCS 2000 node.

The transponder cards that are supported for remote node management using GCC on Cisco web UI are 200G-CK-LC, and 400G-XP and 10x10-LC cards.

Limitations

For remote node using a GCC0 channel, the Cisco Optical Site Manager and NCS 2000 router should be in different subnets.

Manage Remote Node Using GCC

To manage a remote node, perform the following steps:

1. Bring up the remote node using the Light web UI. For more information, see Cisco Light Web User Interface.

2. Insert the transponder cards and pluggables in the NCS 2000 device at the remote site.
3. Provision a Node in GCC Using Light Web UI for Remote Node, on page 211.
4. Add a NCS 2000 Node

Provision a Node in GCC Using Light Web UI for Remote Node

Use this task to provision a node in GCC using the Cisco Light web UI.

Procedure

From the Cisco light web UI, click **Provisioning** > **GCC Configurations**.

a) In the **GCC Configuration** section, enter the following details:

- Shelf Number—Choose the shelf number.
- Slot Number—Choose the slot number.
- Port Number—Choose the port number. The options are:
  - **200G**—Port 2
  - **400G**—Port 11 or 12 pluggable
- Port Mode—Choose the transponder card port mode.
  - **200G**—The option is MXP 10x10G.
  - **400G**—The options are M100 or M200.
    - **M100**
      - First Slice—First slice should be configured when you are using M_200G as the port mode.
      - Second Slice—Choose the slice on which the card is configured. The options are OPM 100G or OPM 10 X 10G.
    - **M200**
      - First Slice—Choose the slice on which the card is configured. The options are OPM 100G or OPM 10 X 10G.
      - Second Slice—Choose the slice on which the card is configured. The options are OPM 100G or OPM 10 X 10G.
- GCC Rate—Choose the GCC rate for the channel.
  - **200G**—192K and 1200K
  - **400G**—1200K
- FEC—Choose the FEC rate.

- **200G**—Standard, HG_FEC_7, or SD_FEC_20.
- **400G**—SD_FEC_15_DE_OFF, SD_FEC_15_DE_ON, SD_FEC_25_DE_OFF, or SD_FEC_25_DE_ON.

- Wavelength—Choose the wavelength for the GCC channel.

View the GCC channel added under the GCC once the status of the GCC channel changes to Sync Completed. You can view the status of the GCC channel from both the Cisco Optical Site Manager web UI and light web UI.

- For Cisco Optical Site Manager web UI, see Add a NCS 2000 Node.
- For the light web UI, you can check if the node is provisioned properly under the **Summary** table.

Now the GCC channel is created from remote to local node and the GCC channel is up.

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 32: 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 80: 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.

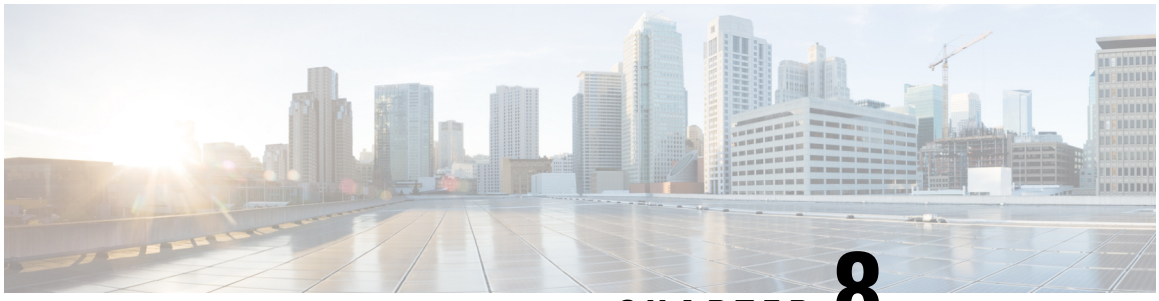
Step 9 Click **Add**.

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.



CHAPTER 8

Backup and Restore Database

This chapter describes the tasks to backup and restore Cisco Optical Site Manager database.

Table 81: 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. When unexpected failures occur, such as hardware malfunctions or software corruption, your data is securely backed up and easily recoverable.

Figure 33: Back Up and Restore Database

• Database Backup and Restore, on page 219

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.

To restore	click the *Restore* button
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.
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

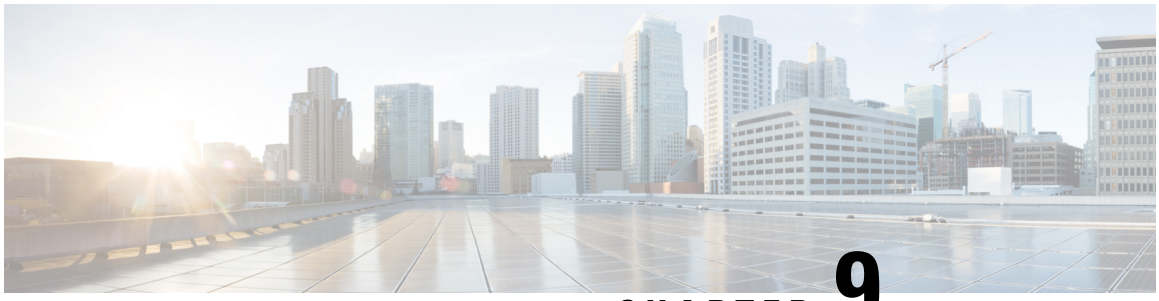
Step 1 Click **Database** in the left panel.

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 9

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 223
- Workflow for Software Upgrade, on page 224
- Download GISO image, on page 225
- Download Software Package on Device, on page 226
- Activate NCS 1000 and NCS 2000 device software, on page 227
- Activate Cisco Optical Site Manager and Admin Plane Image for the SVO-LC , on page 228
- Delete software package, on page 229

Cisco Optical Site Manager software packages

Table 82: 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. 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.

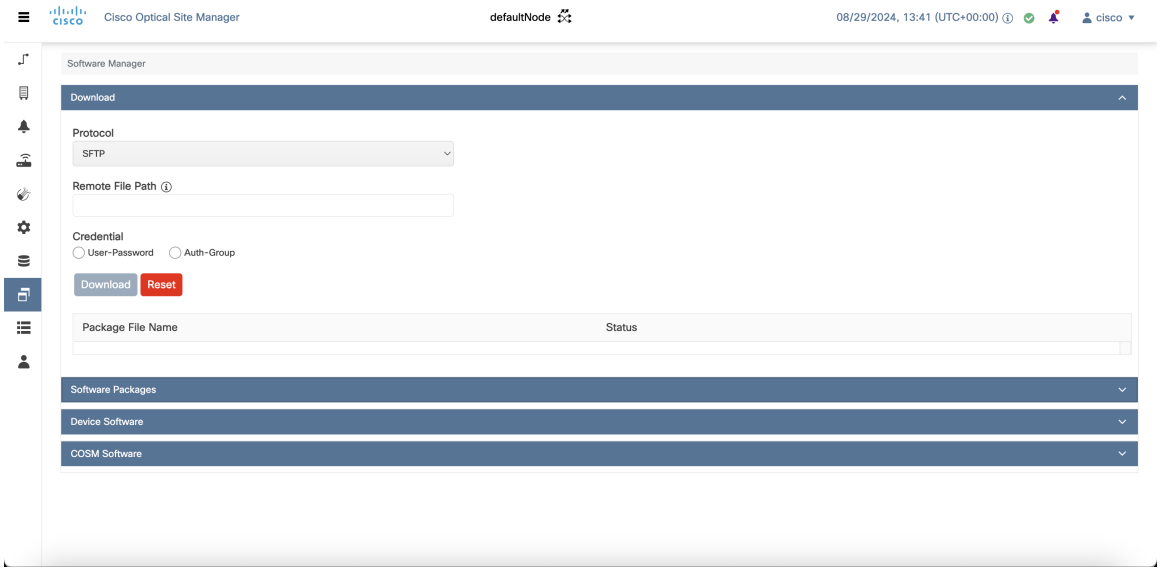
Important If you manually revert IOS XR after upgrading Cisco Optical Site Manager, remove the `migration-done` file at the `/misc/disk1/data/software` location before reinstalling Cisco Optical Site Manager. Otherwise, the subsequent Cisco Optical Site Manager upgrade might not complete correctly.

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 225. 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 226.
3. **Activate Device Software**: Activate the device software. For more details, see Activate NCS 1000 and NCS 2000 device software, on page 227.

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 34: 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.

Note When you perform the download action targeting a device that hosts the Cisco Optical Site Manager application, you may see a message indicating that the software image is already present on the device. This is expected because the package is stored in the device's local Cisco Optical Site Manager software repository. The download operation completes successfully without copying the package again.

Before you begin

- Download GISO image, on page 225

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 83: Device Software Fields

Field	Description
Name	Displays the IP address of the device.
Component	Displays the platform component name.

Field	Description
App Status	Displays the status of the Cisco Optical Site Manager application on the device. • *Active*: Cisco Optical Site Manager is currently active on the device. • *Standby*: 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 and NCS 2000 device software, on page 227

Activate NCS 1000 and NCS 2000 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 or NCS 2000 device software package.

Procedure

Step 1 Click **Software Manager**.

Step 2 Click the **Device Software** section.

Step 3 Select the NCS 1000 or NCS 2000 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.

Activate Cisco Optical Site Manager and Admin Plane Image for the SVO-LC

Use this task to upgrade OS, activate Cisco Optical Site Manager and Admin Plane image for the SVO-LC.

Before you begin

- Download Software Package on Device, on page 226

Procedure

Step 1 Click **Software Manager** from the left panel.

Step 2 Click the **Device Software** section.

Step 3 Select the **CardController** or **OS** component to be activated, and click **Activate**.

Note The activation for the **CardController** and **OS** components is only applicable to SVO-LC. If both SVO-LC cards are present (local HA configuration), you must update the **OS** component on both cards. An error occurs if you select only the **Active** card for the update.

Caution As the SVO-LC host multiple Cisco Optical Site Manager applications, the OS upgrade affects all active instances on the card being upgraded, temporarily resulting in a loss of manageability.

Step 4 To activate the Cisco Optical Site Manager and Cisco Optical Site Manager Admin Plane instance, perform these steps in the **Software** and **Admin Plane Software** sections.

a) Click the **Activate** button.
The **Software Image Activation** dialog box is displayed.

b) Select the software image you want to activate from the drop-down list and click **Activate**.

Note It is recommended to activate the **Administrative Plane Software** first, before activating other components in the system.

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.

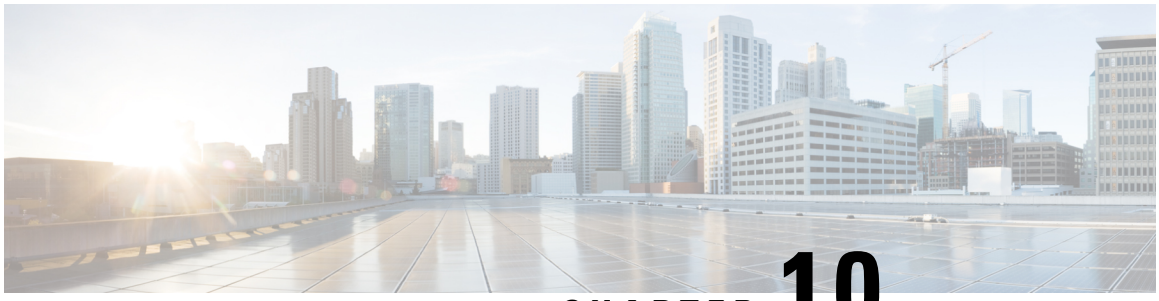
Step 3 Select the checkbox corresponding to the *SW Package ID* of the Cisco Optical Site Manager package you want to delete.

Step 4 Click **Delete**.

A confirmation message appears.

Step 5 Click **Ok**.

The selected software package is deleted.

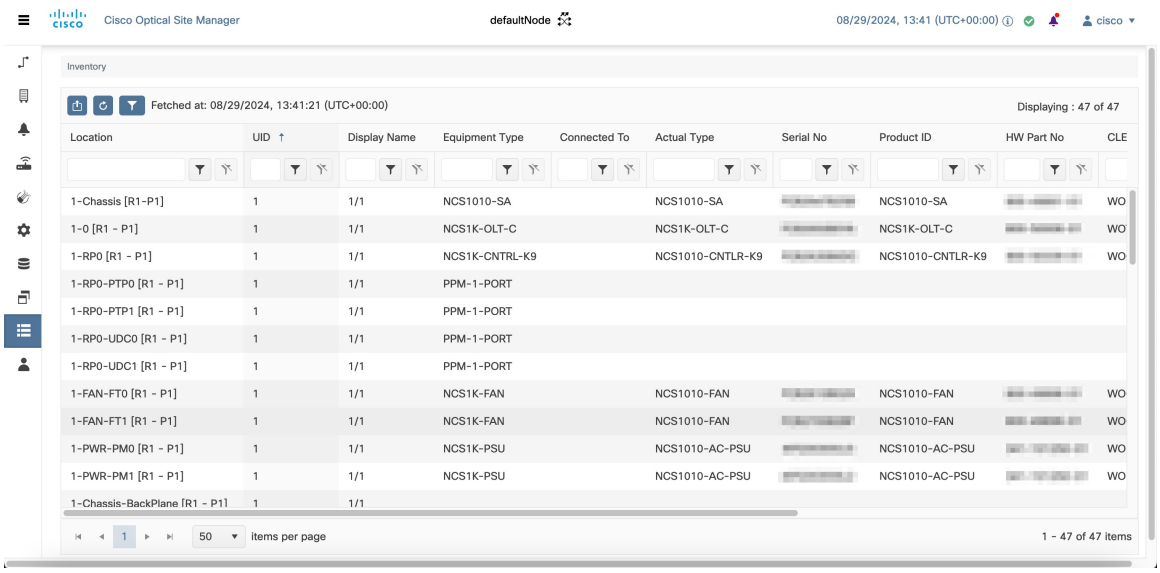


CHAPTER 10

View Inventory

This chapter describs the tasks to view the inventory details of a single or multiple racks.

Figure 35: View Inventory



- View inventory of all racks or chassis, on page 231
- View inventory of a rack or chassis, on page 232

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.

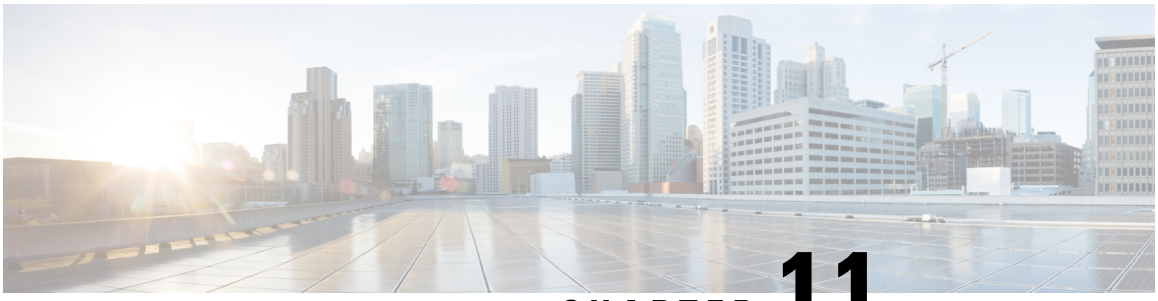
Step 2 Perform one of these steps:

- 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.



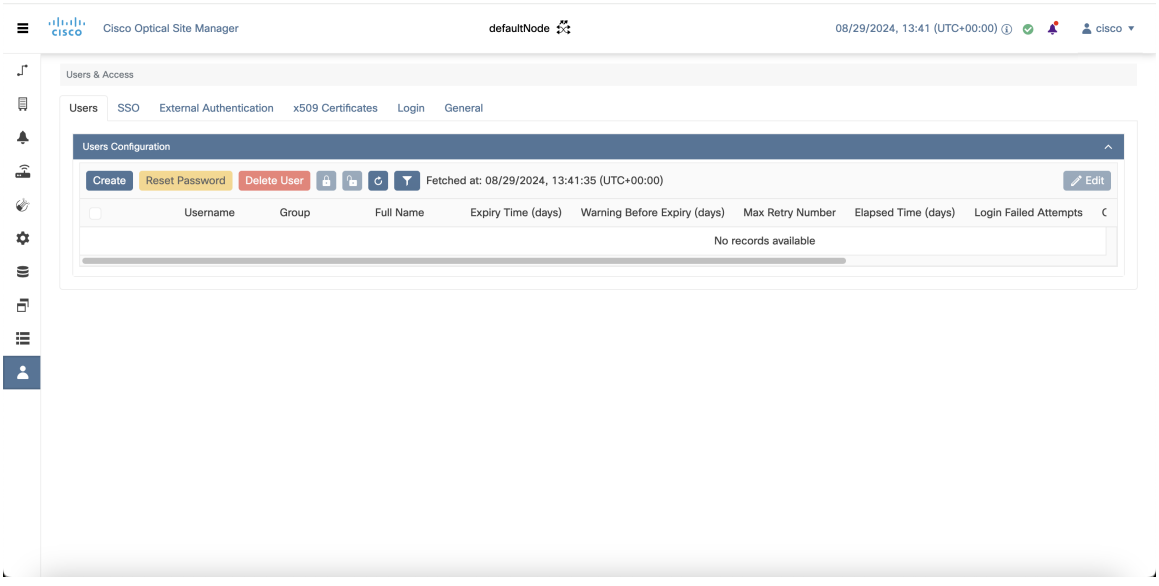
CHAPTER 11

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 36: Manage User Access and Authentication



- User configuration settings, on page 234
- Single sign-on (SSO), on page 237
- Manage External Authentication, on page 240
- x509 certificates, on page 251
- Active login user details, on page 253
- Session timeout, on page 255

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 84: User details, on page 234 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 84: User details

Field	Description / Requirements
User Name	Type the user name. User name requirements: • Must be 6–40 characters long. • Can include alphanumeric characters (a-z, A-Z, 0-9) and special characters: @, - (hyphen), . (dot).

Field	Description / Requirements
Password	Enter the login password. Password requirements: • Must be 8–127 characters long. Must include alphanumeric (a-z, A-Z, 0-9) and special characters (+, #, %). • 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. Example: • If set to 20 days, the user must change the password before 20 days are over. • 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. Available options: • admin • editor • maintenance • snmp • 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 84: User details, on page 234 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 85: SSO fields, on page 238 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 85: SSO fields

Field	Description
IDP Entity ID	A globally unique identifier for the Identity Provider within an SSO federation. 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. 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 86: 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. 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 87: 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 245

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 245

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 248

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 248

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 250

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 88: 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. 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. **b.** Select the *.cert* or *.crt* file from the **Certificate File** field and click **Upload**. **c.** Select the *.key* file in the **Key File** field and click **Upload**.	**a.** Select *PFX + PASSWORD* from the **Certificate Type** drop-down list. **b.** Select the *.pfx* file from the **Certificate File** field and click **Upload**. **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.

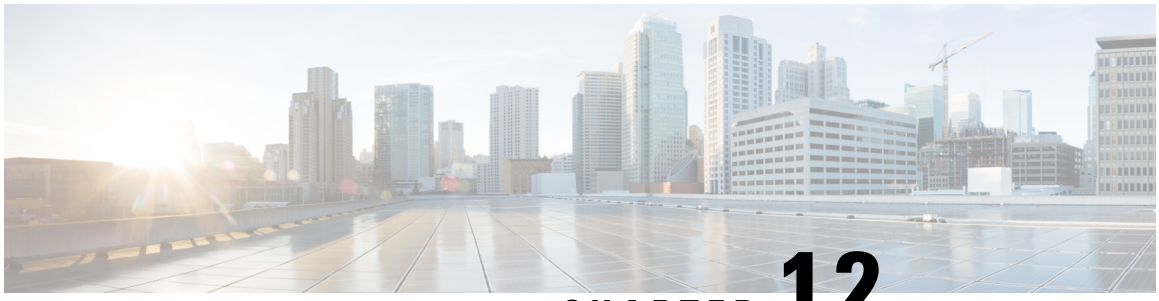
Step 3 Select the time and hours from the respective drop-down lists as described in this table:

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. 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. 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. 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.



CHAPTER 12

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 257
- Download device diagnostics, on page 258
- Configure NTP servers for node time synchronization, on page 259
- View Audit Logs, on page 260
- Smart licensing for Cisco Optical Site Manager, on page 261
- Configure smart licensing workflow, on page 263
- Smart transport mode, on page 264
- Smart licensing CSLU mode, on page 265
- Create a Token, on page 265
- Configure DNS to Access Cisco Optical Site Manager, on page 266
- Configure transport mode, on page 267
- Establish trust, on page 269
- Smart licensing offline mode, on page 270

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 89: 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.

Fields	Description
History Logs	Collects the alarms history logs.
Inventory Logs	Collects the hardware inventory logs.
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.

Configure NTP servers for node time synchronization

Set up primary and secondary NTP servers so the node always maintains the correct time.

Accurate time synchronization ensures reliable alarm reporting, generates log entries, and supports coordination across network devices. If the primary NTP server is unreachable, the node switches to the backup server. If neither server is available, the system raises an alarm.

Before you begin

Log into Cisco Optical Site Manager, on page 1

Follow these steps to configure NTP servers for the node:

Procedure

Step 1 Click **Settings**.
Step 2 Click the **NTP** tab.
Step 3 Click **Edit**.

The NTP fields become editable.

Step 4 Enter the **Server Address** and **Backup Server Address**.

- **Server Address**—Enter the IP address of the primary NTP server.
- **Backup Server Address**—Enter the IP address of the secondary NTP server.

The node checks the availability of the primary NTP server first. If it is unavailable, the node checks the secondary NTP server.

Table 90: NTP Server Behavior

If...	Then...
The primary NTP server is reachable	The node synchronizes its date and time with the primary server.
The primary NTP server fails or is unreachable	The node uses the secondary NTP server to synchronize date and time.
Both NTP servers are unreachable	The SNTP-FAIL alarm is raised until synchronization is restored.

The node retries synchronization at regular intervals and synchronizes its date and time every hour. The system clears the SNTP-FAIL alarm upon successful synchronization.

Step 5 Click **Apply**.

A confirmation message appears.

Step 6 Click **Yes** to confirm the update to initiate synchronization.

The node synchronizes its date and time with the configured NTP server.

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 91: 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.



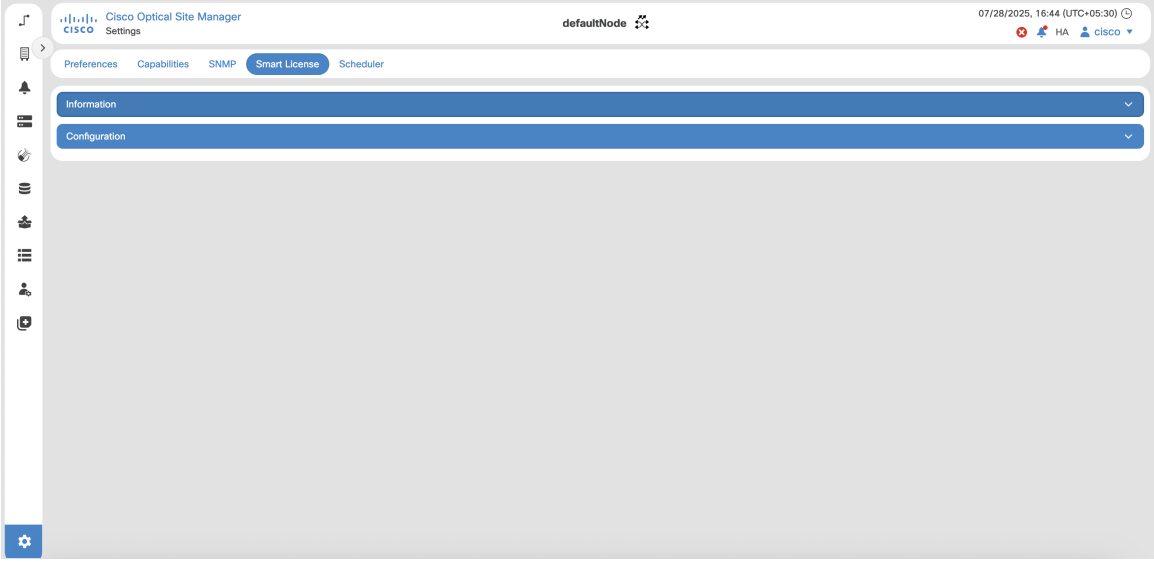
Restriction For NCS 2000, Cisco Optical Site Manager must be running on the SVO line card.

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 37: 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 265
CSLU mode	Smart licensing CSLU mode workflow, on page 265
Offline mode	Smart licensing offline mode workflow, on page 270

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 267.

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 267
- Establish trust, on page 269

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 267
- Establish trust, on page 269

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
%0ANzY4Njl8ZVJSckxKN2pFV2tIeHVoMUkxbGxTazFDVm9kc1B5MGlHQmlFWUJi%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.

Select	To configure
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.

If..	Then..
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.