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

**First Published:** 2025-03-30

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

# CONTENTS

CHAPTER 12

CHAPTER 1

# Cisco Optical Site Manager Overview

This chapter gives us an overview of the Cisco Optical Site Manager.

## Cisco Optical Site Manager Overview

Cisco Optical Site Manager is an application that allows you to view and access the topology of all the optical devices located in the same optical site. It represents a ROADM functionality by aggregating any transponder or muxponder (or optical transceiver in general) present in the same location.

Cisco Optical Site Manager enables software-defined networks to automate site operations. Its site aggregation feature for Optical Sites includes any NCS 1000 devices connected to the network.

Cisco Optical Site Manager provides the following features:

1. **Site Aggregation for Optical Sites:** Cisco Optical Site Manager allows site aggregation for Optical Sites with NCS 1010, NCS 1014, NCS 1004, and NCS 1001 devices. This feature provides a clear view of the topology of the optical site the devices connected to it. Cisco Optical Site Manager also allows abstraction of OLS site (Optical Line System), OT site (Optical Terminal), or and OLS+OT site.

2. **Site-Level Management:** Cisco Optical Site Manager collects and manages site-level information, including inventory details, site topology, performance monitoring, and correlated alarms.

3. **Web-Based User Interface:** Cisco Optical Site Manager offers a web-based user interface (Web UI) that provides improved management control for NCS 1000 devices and their configurations. This interface allows you to easily view the layout of chassis, cards, and passive devices. Additionally, you can check the active and acknowledged alarms for the NCS 1000 devices.

4. **Performance Monitoring:** Cisco Optical Site Manager enables you to keep track of the performance of different cards and chassis that are hosted on the device. You can access both current and historical performance monitoring counters at various intervals. Additionally, you can verify connections and perform loopbacks.

For more information about Cisco Optical Site Manager, see the data sheet.

# Log into Cisco Optical Site Manager

To log into Cisco Optical Site Manager web interface, follow these steps:

### Procedure

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

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

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

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

CHAPTER 2

# Node Functional View

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

*Table 1: Feature History*

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

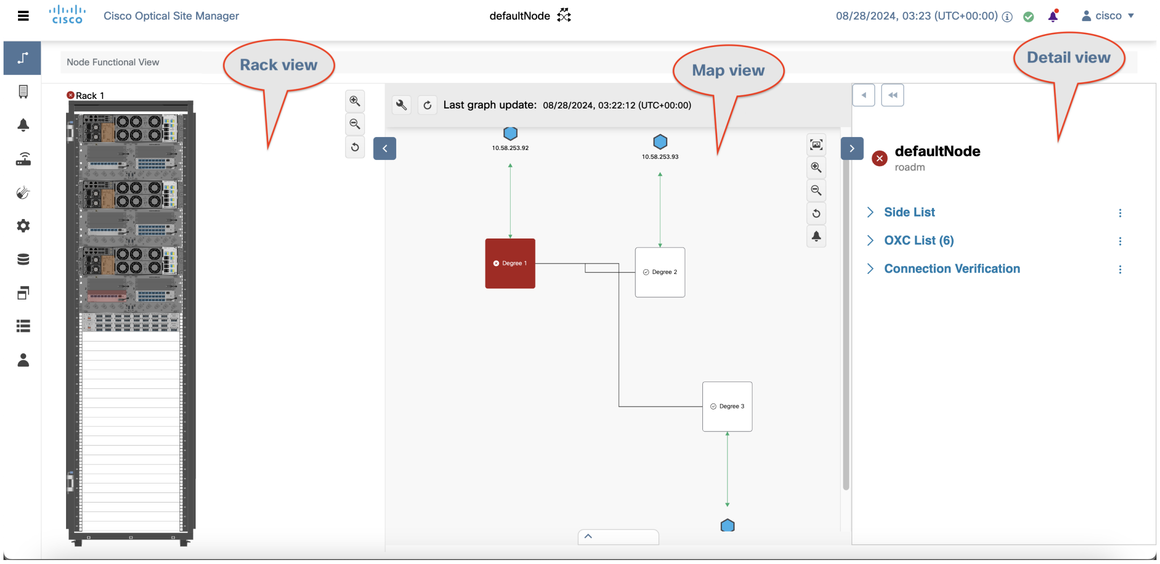
# Understanding Node Functional View

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

Using NFV, you can:

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

*Figure 1: Node Functional View*



## Node Functional View panels

This table describes the NFV panels.

*Table 2: Overview of NFV panels*

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

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

# NFV icons

This table describes the action icons used in the NFV.

*Table 3: Icon used on NFV*

| Icon | Description |
|---|---|
| ↺ | Resets the zoomed view to normal view. |
| Refresh<br>↻ | Refreshes the map view with current information. |
| > < | Expands or collapses the rack or Detailed view. |
| 🔔 | Displays or hides the alarms icon in the map and detailed view.<br>**1.** Click this button.<br>**2.** Select or deselect the alarm icons in the drop-down list to display or hide the alarms icon in the map and detailed view. |

| Icon | Description |
|---|---|
| User Settings<br>🔧 | Sets the user preferences.<br>For more details, see Customize NFV layout, on page 23. |
| Zoom In<br>⊕ | Zooms in the rack or map view. |
| Zoom Out<br>⊖ | Zooms out the rack or map view. |
| Zoom Out<br>◀◀ | Navigates to the default view in the map view. |
| Zoom Out<br>◀ | Navigates to the previous page in the map View. |
| Zoom Out<br>⌃ | Expands or collapses the Alarms section. |
| Zoom Out<br>⛶ | Magnifies the selected area of the map view, providing a closer and more detailed view of that specific section. |

# 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 2

### Procedure

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

The Node Functional View page appears.

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

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

*Table 4: Node details*

| Section | Description |
|---|---|
| Side List | Displays a list of the nodes along with its details, such as span loss value, the IP address of the device it is connected to, and its degree. |
| OXC List | Displays a list of active circuits passing through a particular card.<br>For more details, see View active circuit list, on page 24. |
| Connection Verification | Displays a list of the connections between the line cards and all passive modules.<br>For more details, see Connection verification, on page 21. |

# 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 2

### Procedure

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

The **Node Functional View** page appears.

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

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

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

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

You can view these details in the right panel:

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

# Optical Channel Monitoring

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

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

### Key features of OCM

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

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

### OCM tab icons and elements

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

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

# View Optical Channel Monitoring data

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

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

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

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

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

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

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

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

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

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

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

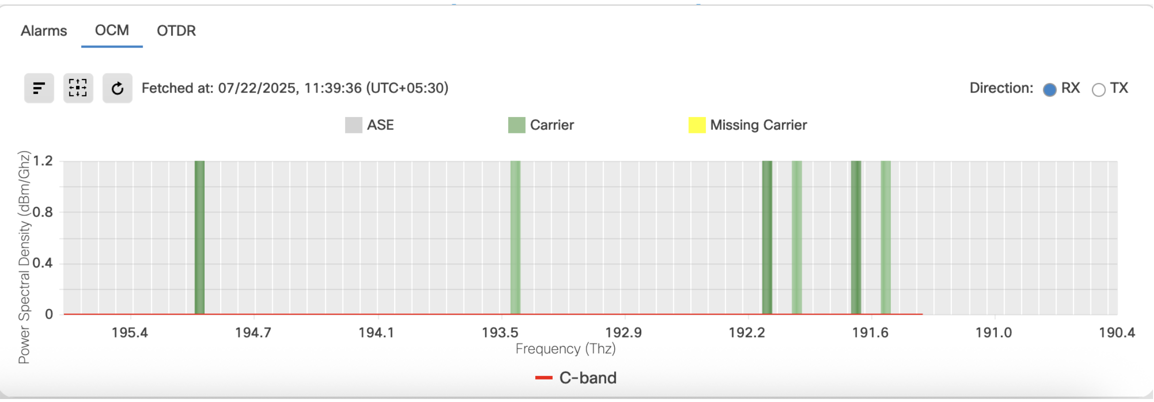
You can view the transmission or reception power levels for the optical degree you selected in the OCM data and spectrum occupancy graph and table.

# OCM spectrum graph

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

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

*Figure 2: OCM spectrum graph*



Fetched at: 07/22/2025, 11:39:36 (UTC+05:30)

Direction: ● RX ○ TX

## 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). |

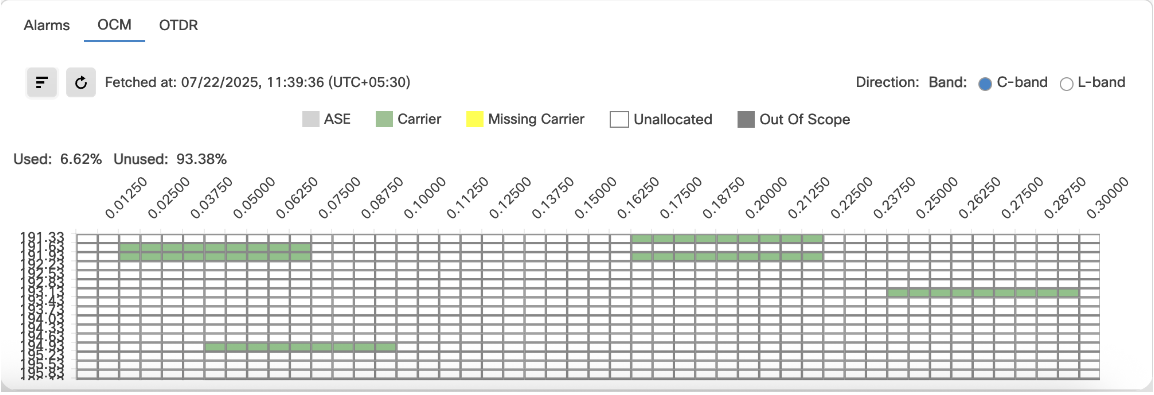
# OCM utilization table

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*



Fetched at: 07/22/2025, 11:39:36 (UTC+05:30)

Used: 6.62% Unused: 93.38%

### OCM utilization table color elements

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

*Table 5: 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 in NCS 1010 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 enables you to assess fiber quality during system installation (prior to activating traffic) using the Optical Time Domain Reflectometer (OTDR) feature.

The OTDR feature offers several advantages for fiber management:

- Real-time loss and back reflection measurements for the fiber pair connected to the TX and RX ports.
- Monitoring of the fiber during live system operation.
- Inspection of the fiber following cable cut and repair events.

# OTDR icons

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

### OTDR icon descriptions

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

*Table 6: 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. |

| Icon | Description |
|---|---|
| 💾 | Save the current OTDR scan results as a baseline. |
| ^ Clear Alarms | Clear the reflections or losses alarms. |
| 🔧 | Enable or disable automatic OTDR scan after a fiber cut or Raman Turn Up. |

# Enable automatic OTDR scan

In the automatic mode, OTDR automatically triggers a scan after events such as span faults, fiber restorations, device power cycles, or line card reloads.

Follow these steps to enable or disable the automatic OTDR scan.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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 and then click the **OTDR Settings** icon.
**OTDR Configurations** dialog box is displayed.

**Step 5** Click the **Global** tab.

**Step 6** Select these checkboxes in the **Automatic OTDR Scans Settings** section:

| If you want to enable automatic OTDR scan | then select this check box |
|---|---|
| after a system startup, fiber cut or repair | **System Startup, Fiber Cut & Repair** |
| after the Raman turn-up process is completed | **Raman Turn Up** |
| if span loss increases | **Span Loss Increase** |
| if an excessive ORL is detected from the span | **Excessive ORL from span** |

**Step 7** Specify the delay time in the **Start Delay (Min)** field.

**Step 8** Specify the threshold in dB in the **Span Loss Increase Threshold (dB)** field.

**Step 9** Click **Apply**.

# Run a manual OTDR scan

Manually run an OTDR scan during fiber installation or troubleshooting to verify link quality and locate faults.

Follow these steps to manually run an OTDR scan.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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** Scroll to the bottom of the panel.

**Step 6** Select **RX** or **TX** to run the OTDR scan in the RX or TX directions, respectively.

**Step 7** Click the **Direction** button to set the OTDR scan sensitivity and threshold values.

*Table 7: OTDR scan sensitivity and threshold*

| Use this option | To |
|---|---|
| Loss Sensitivity | enable the OTDR scan to detect small signal losses (attenuation) along the fiber. Higher loss sensitivity helps the OTDR identify minor attenuation caused by factors like bends or splices. |
| Reflection Sensitivity | enable the OTDR scan to detect reflected signals from events such as connector interfaces, splices, or breaks.<br>High reflection sensitivity is crucial for accurately locating and analyzing reflective faults in the fiber. |
| Absolute Threshold | ensure that the OTDR scan can reliably detect and measure the lowest signal strength, allowing the OTDR to provide accurate and meaningful data essential for identifying weak signals or long-distance faults. |
| Unprovision | delete the OTDR scan results in the selected direction. |

**Step 8** Click **Start Scan** button to start OTDR scan.
The OTDR-SCAN-IN-PROGRESS-RX alarm is raised and displayed ion the **Alarms** tab of the **Fault Monitoring** menu.

**Step 9** Click **Stop Scan** button to terminate the OTDR scan.

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

The scan results are displayed in the graph.

# 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 2

### Procedure

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

The Node Functional View page appears.

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

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

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

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

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

# View side details for an OLS node

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

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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 2

### 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 2

### Procedure

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

The Node Functional View page appears.

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

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

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

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

You can view these port information in the right panel:

| Section/Field | Description |
|---|---|
| Name | Displays the name of the port. |
| Location | Displays the shelf, rack, or slot of the card. |
| Powers | Displays the list of all the links with their aggregate power.<br>The aggregate power displays the current power in case of a single port. The aggregate power displays a list of all the different power levels in case of an MPO port or logical group. |
| 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 2

### 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 8: 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 21. |

# 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 2

### 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 9: Patch cord details*

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

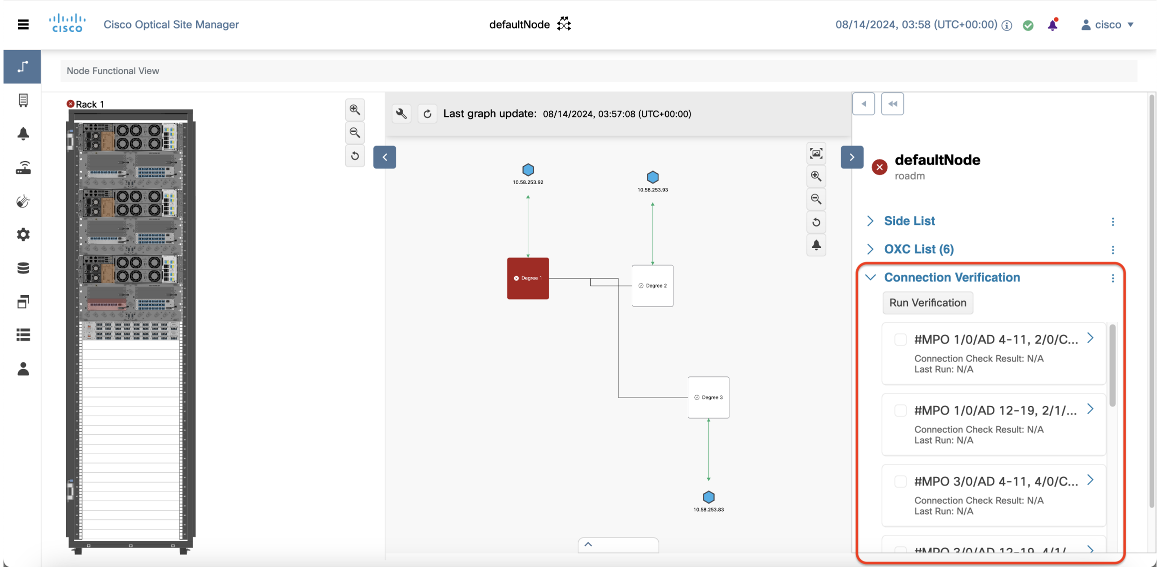
# Connection verification

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

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

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

*Figure 4: Connection Verification*


Cisco Optical Site Manager
defaultNode
08/14/2024, 03:58 (UTC+00:00)
cisco
Node Functional View
Rack 1
Last graph update: 08/14/2024, 03:57:08 (UTC+00:00)
10.58.253.92
10.58.253.93
Degree 1
Degree 2
Degree 3
10.58.253.83
defaultNode
roadm
Side List
OXC List (6)
Connection Verification
Run Verification
#MPO 1/0/AD 4-11, 2/0/C...
Connection Check Result: N/A
Last Run: N/A
#MPO 1/0/AD 12-19, 2/1/...
Connection Check Result: N/A
Last Run: N/A
#MPO 3/0/AD 4-11, 4/0/C...
Connection Check Result: N/A
Last Run: N/A
#MPO 3/0/AD 12-19, 4/1/...

### 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 2

### 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 2

### Procedure

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

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

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

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

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

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

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

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

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

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

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

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

# View active circuit list

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

### Before you begin

Log into Cisco Optical Site Manager, on page 2

## 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

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.

## Create a rack

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

Use this task to add a rack to Cisco Optical Site Manager.

**Before you begin**

- Log into Cisco Optical Site Manager, on page 2

**Procedure**

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

The COSM 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 value from 1 through 32767.

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

The rack is added to the rack and table views.

# 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 2

**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 2

### Procedure

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

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

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

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

The table displays a list of passive devices.

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

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

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

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

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

# View voltage, temperature and current details

*Table 10: 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 2

#### 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 2

#### 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

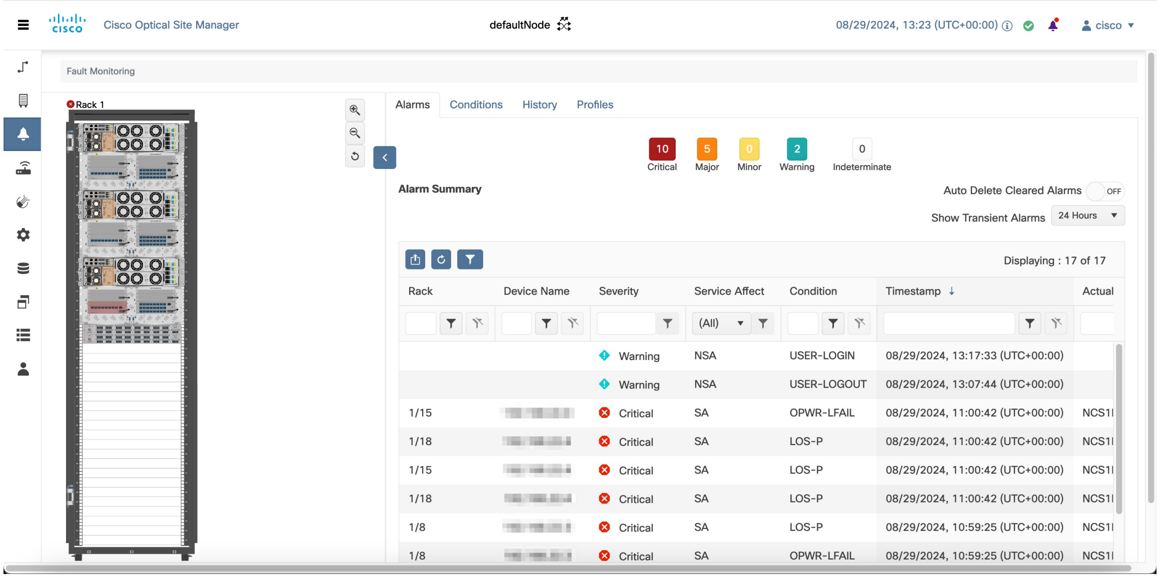
# Monitor Faults

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

# Fault Monitoring

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 5: Fault Monitoring*



Alarm Summary

Auto Delete Cleared Alarms OFF

Show Transient Alarms 24 Hours

Displaying : 17 of 17

| Rack | Device Name | Severity | Service Affect | Condition | Timestamp ↓ | Actual |
|---|---|---|---|---|---|---|
| | | (All) | | | | |
| | | Warning | NSA | USER-LOGIN | 08/29/2024, 13:17:33 (UTC+00:00) | |
| | | Warning | NSA | USER-LOGOUT | 08/29/2024, 13:07:44 (UTC+00:00) | |
| 1/15 | [redacted] | Critical | SA | OPWR-LFAIL | 08/29/2024, 11:00:42 (UTC+00:00) | NCS1I |
| 1/18 | [redacted] | Critical | SA | LOS-P | 08/29/2024, 11:00:42 (UTC+00:00) | NCS1I |
| 1/15 | [redacted] | Critical | SA | LOS-P | 08/29/2024, 11:00:42 (UTC+00:00) | NCS1I |
| 1/18 | [redacted] | Critical | SA | LOS-P | 08/29/2024, 11:00:42 (UTC+00:00) | NCS1I |
| 1/8 | [redacted] | Critical | SA | LOS-P | 08/29/2024, 10:59:25 (UTC+00:00) | NCS1I |
| 1/8 | [redacted] | Critical | SA | OPWR-LFAIL | 08/29/2024, 10:59:25 (UTC+00:00) | NCS1I |

# 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 2

## 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

You can view all alarms for all components such as racks, chassis, cards, and ports to monitor system-wide status and detect issues.

Follow these steps to view all alarms and transient conditions:

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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 to view all the alarms.
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 **Conditions** tab to view all the transient conditions.

**Step 4** Click the **History** tab to view the alarms.

**Step 5** (Optional) Click the **Auto Delete Cleared Alarms** toggle button to automatically delete the cleared alarms.

**Step 6** (Optional) Click the **Excel Export** button to export the alarms to an Excel sheet.

---

# View correlated alarms

*Table 11: 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 2

### 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 2

### 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:

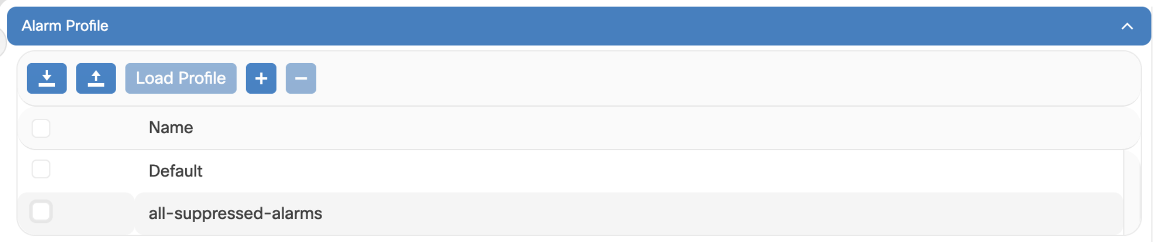
- The default alarm profile is preprovisioned on the node and contains all alarms.
- It sets alarm severities according to standard Telcordia GR-474-CORE guidelines, which cannot be changed.
- Default severities are applied to all alarms and conditions until a new custom profile is created and applied.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



| | Name |
|---|---|
| □ | Default |
| □ | all-suppressed-alarms |

### 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 2

### 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 2

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 12: 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.<br>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 2

### 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.

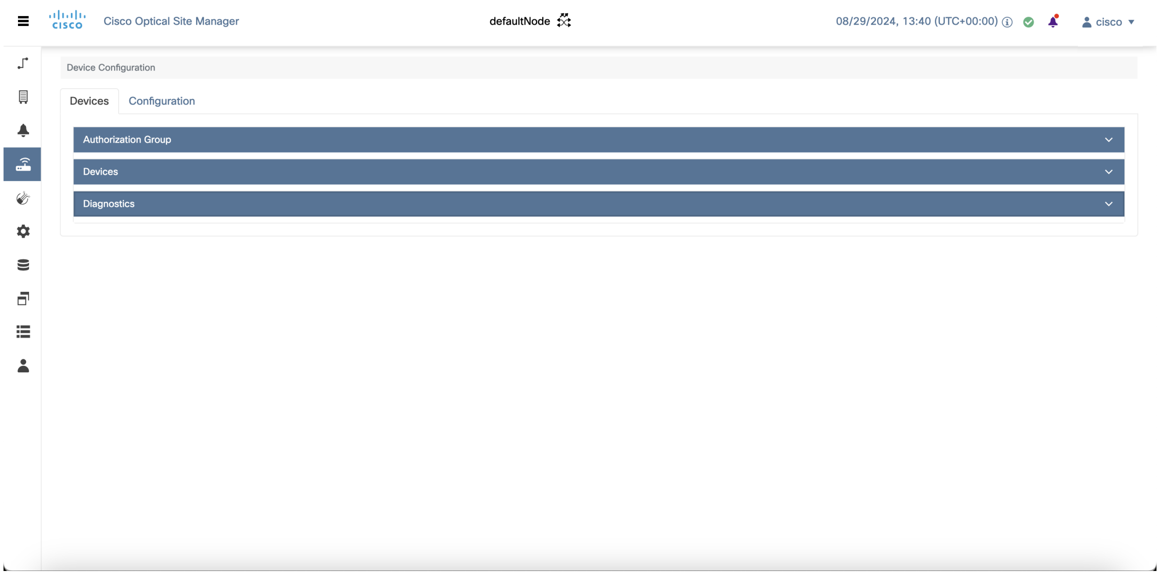
View the tag name in the **User Tag** column under the **Alarms** tab to easily identify the affected device.

CHAPTER 5

# Configure Devices

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

*Figure 7: Configure Devices*



# Manage authorization groups

Authorization groups are used to manage user and group attributes for authentication and authorization processes.

Follow these steps to create, edit, or delete authorization groups for devices.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

## Procedure

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

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

The table lists all the available groups.

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

| To | perform these steps |
|---|---|
| Create a new authorization group | **a.** Click the **Add Auth Group** button.<br>The **Add Authorization Group** dialog box appears.<br>**b.** Enter the **Auth Group Name**, **Remote User Name**, and **Remote Password** in their respective fields.<br>**c.** Click **Add**.<br>The new auth group is added to the table. |
| Edit an authorization group | **a.** Click the **Add Auth Group** button.<br>The **Add Authorization Group** dialog box appears.<br>**b.** Enter the **Auth Group Name**, **Remote User Name**, and **Remote Password** in their respective fields.<br>**c.** Click **Add**.<br>The authorization group is added to the table. |
| Delete an authorization group | **a.** Select the check box next to the authorization group you want to edit.<br>**b.** Click the **Delete Auth Group** button.<br>A confirmation message appears.<br>**c.** Click **OK**.<br>The authorization group is deleted from the table. |

# Add a device

Cisco Optical Site Manager automatically detects and onboards directly connected peer devices on the network. However, if you've added a new device after configuring Cisco Optical Site Manager, you can manually add the device for management using the application.

*Figure 8: 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 2

## 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**.

**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.

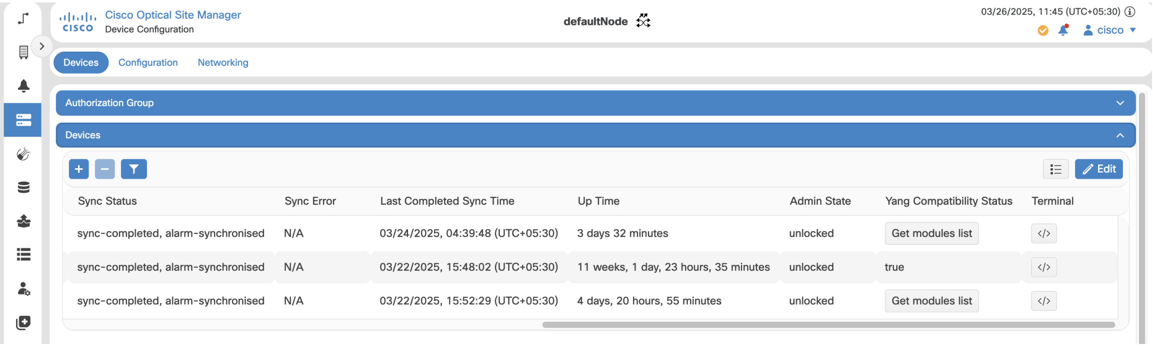
# Manage a device using IOS XR CLI

*Table 13: 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 9: Manage a Device Using IOS XR CLI*



| Sync Status | Sync Error | Last Completed Sync Time | Up Time | Admin State | Yang Compatibility Status | Terminal |
|---|---|---|---|---|---|---|
| sync-completed, alarm-synchronised | N/A | 03/24/2025, 04:39:48 (UTC+05:30) | 3 days 32 minutes | unlocked | Get modules list | </> |
| sync-completed, alarm-synchronised | N/A | 03/22/2025, 15:48:02 (UTC+05:30) | 11 weeks, 1 day, 23 hours, 35 minutes | unlocked | true | </> |
| sync-completed, alarm-synchronised | N/A | 03/22/2025, 15:52:29 (UTC+05:30) | 4 days, 20 hours, 55 minutes | unlocked | Get modules list | </> |

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 2

## Procedure

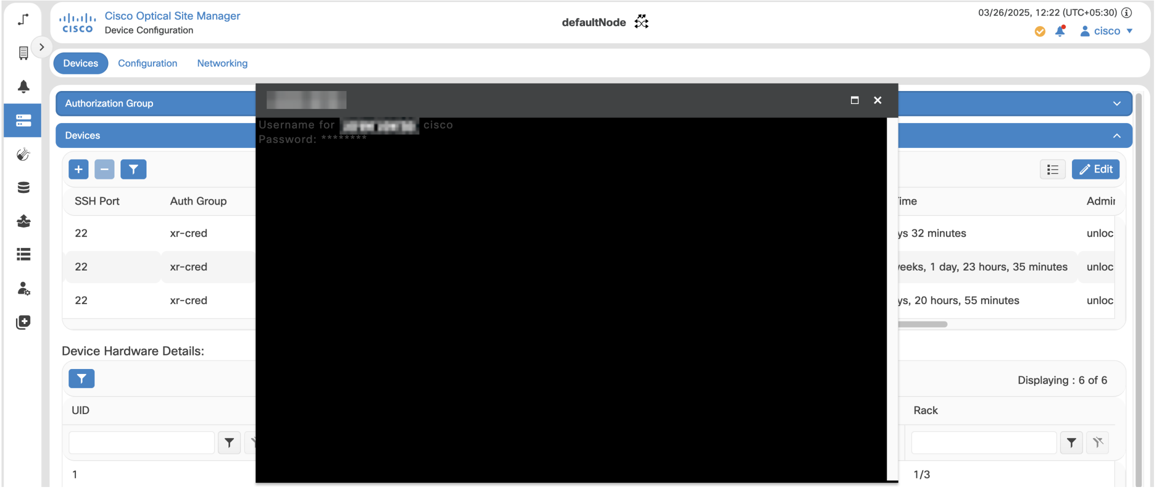
**Step 1** Click **Devices** in the left panel.
The *Device Configuration* page appears.

**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.



[redacted]

```
Username for [redacted] cisco
Password: ********
```

| SSH Port | Auth Group | ime | Admi |
|---|---|---|---|
| 22 | xr-cred | ys 32 minutes | unloc |
| 22 | xr-cred | eeks, 1 day, 23 hours, 35 minutes | unloc |
| 22 | xr-cred | ys, 20 hours, 55 minutes | unloc |

**Step 4** Type the username and press **Enter**.

The system prompts you to enter the password.

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

# Add unmanaged devices

*Table 14: Feature History*

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

Unmanaged devices are those not actively managed by NCS 1000 or NCS 2000. Add an unmanaged device to Cisco Optical Site Manager. Examples include switches, LAN controllers, and passive optical devices.

Follow these steps to add an unmanaged device.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

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

**Step 5** In the rack view, perform these steps.

a) Right-click an empty rack unit and select **Add a Passive Unit**
The **Add Passive Unit in Ru Position** dialog box is displayed.
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 is displayed.

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

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

# Delete devices

Delete devices that are no longer used in the network.

Follow these steps to delete an NCS 1000, NCS 2000, passive device, or an external controller.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

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

The table lists all the configured devices.

**Step 3** Select the check box next to the devices you want to delete.

**Step 4** Click the **Delete Device(s)** button to delete the selected devices.
A confirmation message appears.

**Step 5** Click **Yes**.

# 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 2

## Procedure

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

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

The configured devices are listed in a table.

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

**Step 4** Click **Retrieve**.

A confirmation message appears.

**Step 5** Click **Yes** to proceed.

A **Request Accepted** message appears.

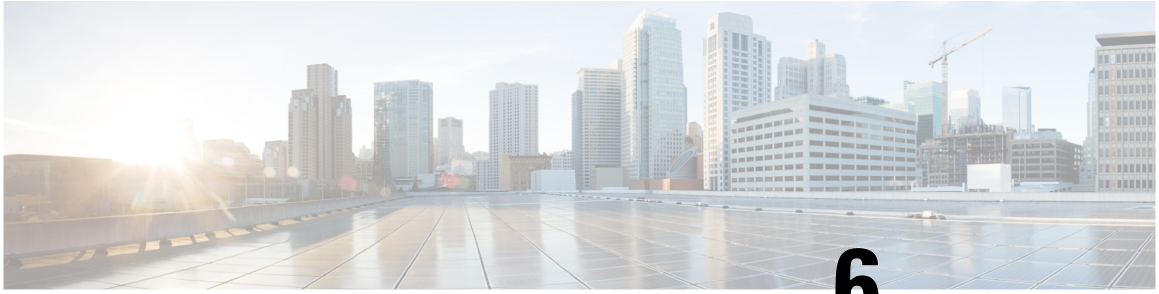
**Step 6** Click **OK**.

A message appears when the diagnostic action is completed.

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

The system downloads a zip file containing the logs.

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

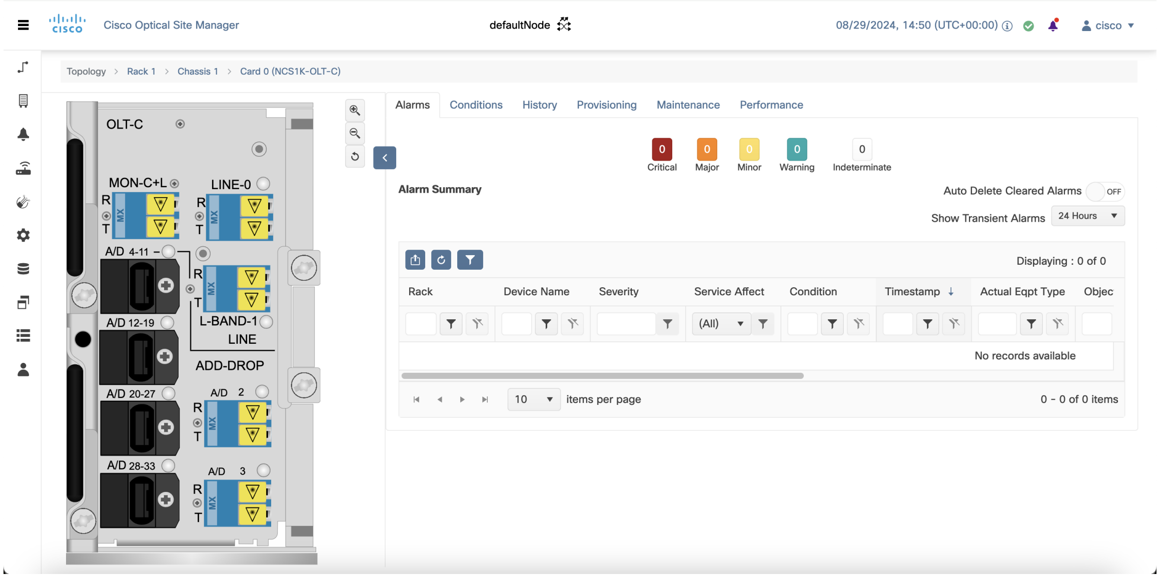


CHAPTER 6

# Provision Line Cards

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

*Figure 10: Provision Line Cards*



# Supported Line Cards

*Table 15: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for NCS1K-OTDR Line Card | Cisco IOS XR Release 25.1.1 | Cisco Optical Site Manager now allows you to manage the NCS1K-OTDR line card. |
| Support for NCS 1001 and Cards | Cisco IOS XR Release 24.3.1 | Cisco Optical Site Manager now allows you to manage the NCS 1001 node and its following cards:<br>• NCS1K-PSM<br>• NCS1K-EDFA |

Cisco Optical Site Manager supports configuration and management of various NCS 1000 cards.

For detailed information about the supported cards, you can refer to the following topics:

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

# Provision Pluggable Port Module

Use this task to provision the Pluggable Port Module (PPM) on the control card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

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

The fields in the table become editable.

**Step 4** Choose the admin state in the **Admin State** column from the drop-down list and click **Apply**.

# Open the Card View

Use this task to open the card view.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

The COSM Topology page appears.

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

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

# Add Card Mode for NCS 1000 Cards

*Table 16: Feature History*

| 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:<br>• 800G<br>• 900G<br>• 1000G<br>• 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:<br>• FC-MXP<br>• MXP-4x100G-TXP-400G with 400GE and 100GE/OTU4 client rates<br>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:<br>• NCS1K4-1.2T-K9<br>• NCS1K4-1.2TLCW-K9 |

| Feature Name | Release Information | Description |
|---|---|---|
| Support for NCS2000 Cards | Cisco IOS XR Release 25.1.1 | The **Card Configuration Wizard** now supports configuration of card mode for these cards:<br>• 10x10G-LC<br>• 200G-CK-C<br>• 400G-XP-LC<br>• 1.2T-MXP |
| Additional Card Mode and Trunk Rates for the NCS1K4-OTN-XP Card | Cisco IOS XR Release 24.3.1 | The **Select Card Mode** page of the **Card Configuration Wizard** is updated to include the **1.2T Splitted** configuration on the **Trunk 0** port.<br>You can also use the wizard to configure these trunk rates in the muxponder mode:<br>• 100-GE client traffic for 600-G and 1000-G<br>• 500-G and 900-G |
| Support for NCS 1004 Card and Card Modes | Cisco IOS XR Release 24.3.1 | The **Card Configuration Wizard** now supports configuring these card modes for NCS1K4-OTN-XP cards:<br>• 10G-GREY-MXP<br>• 40x10G-4x100G-MXP<br>You can also use the wizard to configure card mode for the NCS1K4-2-QDD-C-K9 card. |
| 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. |

Cisco Optical Site Manager allows you to configure NCS 1000 line cards in various modes, including Muxponder and Slice configurations. These modes determine how the line card processes data and manages traffic, facilitating efficient client-to-trunk mapping.

# How to Add a Card Mode

To add a card mode using the **Card Configuration Wizard** in Cisco Optical Site Manager, perform these tasks:

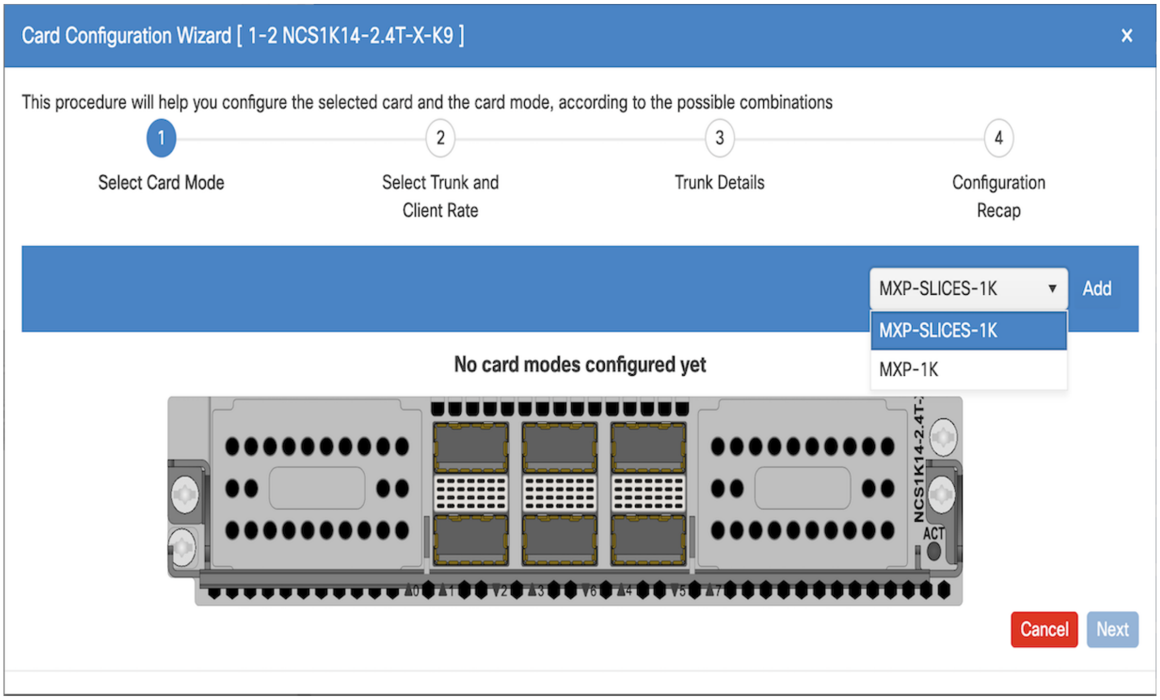
1. Select Card Mode, on page 58
2. Select Trunk and Client Data Rate, on page 59
3. Add Internal Patch Cords, on page 61
4. Add Trunk Details, on page 62
5. Verify Configuration Details, on page 63

# Select Card Mode

The **Select Card Mode** in the Cisco Optical Site Manager **Card Configuration Wizard** allows users to choose from various card modes.

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

***Figure 11: Select Card Mode***



Card Configuration Wizard [ 1-2 NCS1K14-2.4T-X-K9 ]

This procedure will help you configure the selected card and the card mode, according to the possible combinations

No card modes configured yet

### Before you begin

- Log into Cisco Optical Site Manager, on page 2

### Procedure

**Step 1** Open the **Card Configuration Wizard**.

- To open the **Card Configuration Wizard** from Rack view, perform these steps:

  **a.** Right-click a line card in the Rack view.

  **b.** Click **Card Mode**.

  **c.** Select **Install**.

- To open the **Card Configuration Wizard** from Card view, perform these steps:

  **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 17: 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**.

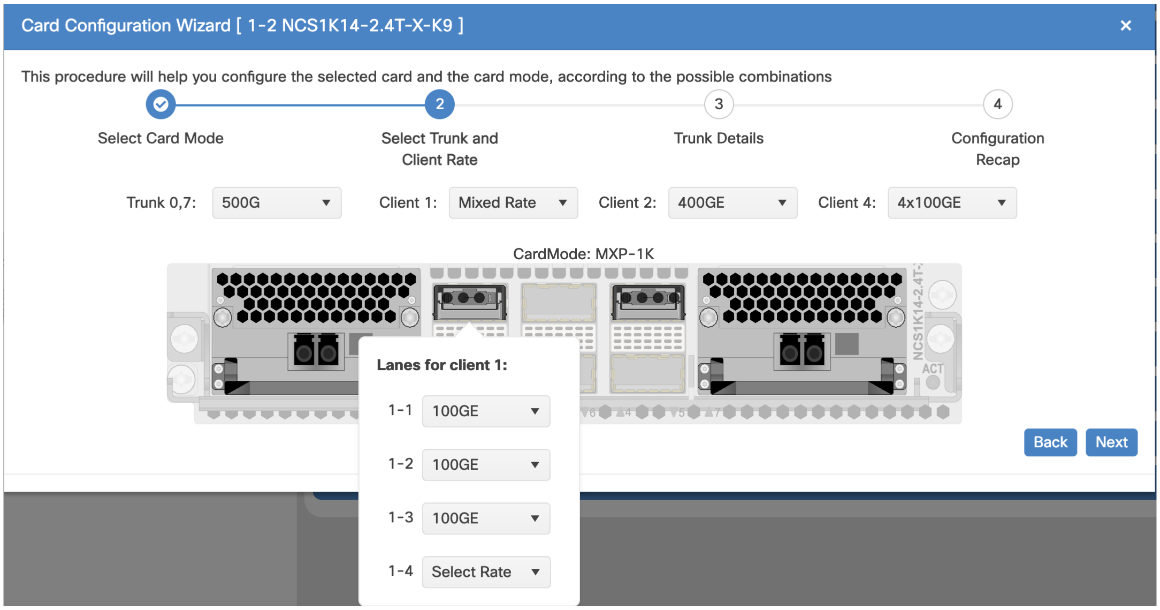
#### What to do next

Select the Trunk and Client Data Rates.

## Select Trunk and Client Data Rate

Use this task to select the trunk and client port data rates in the **Card Configuration Wizard**.

*Figure 12: Select Trunk and Client Data Rate*



Card Configuration Wizard [ 1-2 NCS1K14-2.4T-X-K9 ]

This procedure will help you configure the selected card and the card mode, according to the possible combinations

Trunk 0,7: 500G
Client 1: Mixed Rate
Client 2: 400GE
Client 4: 4x100GE

CardMode: MXP-1K

Lanes for client 1:

1-1 100GE
1-2 100GE
1-3 100GE
1-4 Select Rate

## Before you begin

- Select Card Mode, on page 58

## 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.

*Table 18: Client Data Rate Options*

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

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

### What to do next

- If optical type is configured as *txp*, see Add Trunk Details, on page 62.
- If optical type is configured as *roadm*, see Add Internal Patch Cords, on page 61.

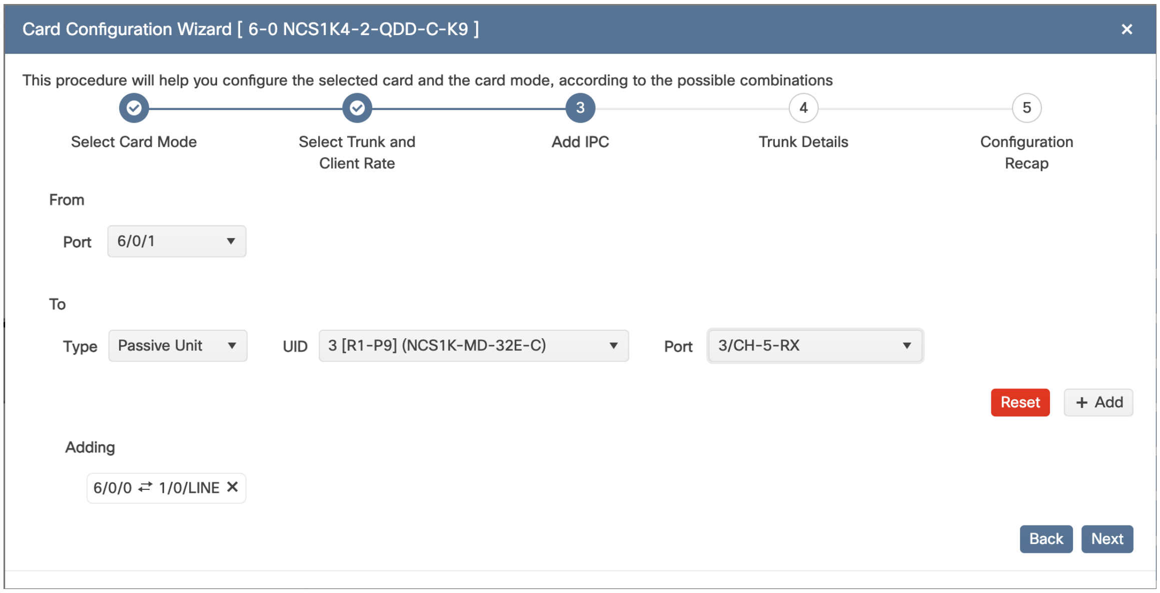
# Add Internal Patch Cords

Adding Internal Patch Cords (IPC) in the **Card Configuration Wizard** establishes virtual links between network termination points, such as OSC ports, transponder or muxponder trunk ports, line ports, and passive device ports.

Use this task to add IPC in the **Card Configuration Wizard**.

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

*Figure 13: Add Internal Patch Cords*



Card Configuration Wizard [ 6-0 NCS1K4-2-QDD-C-K9 ]

This procedure will help you configure the selected card and the card mode, according to the possible combinations

From

Port: 6/0/1

To

Type: Passive Unit
UID: 3 [R1-P9] (NCS1K-MD-32E-C)
Port: 3/CH-5-RX

Adding

6/0/0 ⇄ 1/0/LINE ✕

### Before you begin

- Select Trunk and Client Data Rate, on page 59

### 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:

*Table 19: IPC Drop-down Lists Displayed Based on Device Type*

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

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

**Step 4** (Optional) Do one of the following to remove internal patch cord:

- 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**.

### What to do next

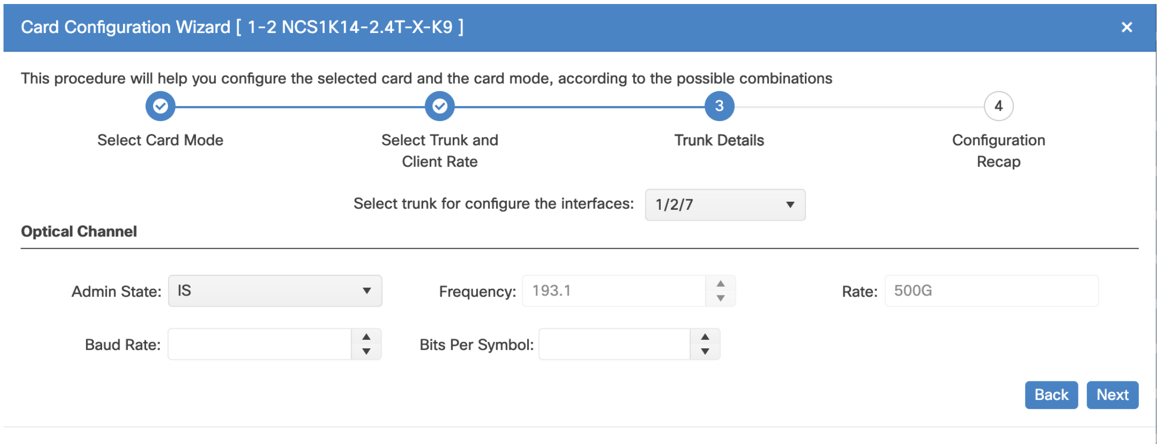
Add the Trunk Details to configure the interfaces.

# Add Trunk Details

Adding trunk details in the **Card Configuration Wizard** specifies the parameters and configurations necessary for establishing trunk connections.

Use this task to add select the trunk details in the **Card Configuration Wizard** to configure the interfaces.

*Figure 14: Add Trunk Details*



Card Configuration Wizard [ 1-2 NCS1K14-2.4T-X-K9 ]

This procedure will help you configure the selected card and the card mode, according to the possible combinations

Select trunk for configure the interfaces: 1/2/7

Optical Channel

Admin State: IS

Frequency: 193.1

Rate: 500G

Baud Rate:

Bits Per Symbol:

### Before you begin

- If optical type is configured as *roadm*, make sure to Add Internal Patch Cords, on page 61
- If optical type is configured as *txp*, make sure to Select Trunk and Client Data Rate, on page 59

## Procedure

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

**Step 2** In the **Optical Channel** section, select the following from their corresponding drop-down lists:

- **Admin State**
- **Frequency**
- **Baud Rate**
- **Bits Per Symbol**
- **Rate**

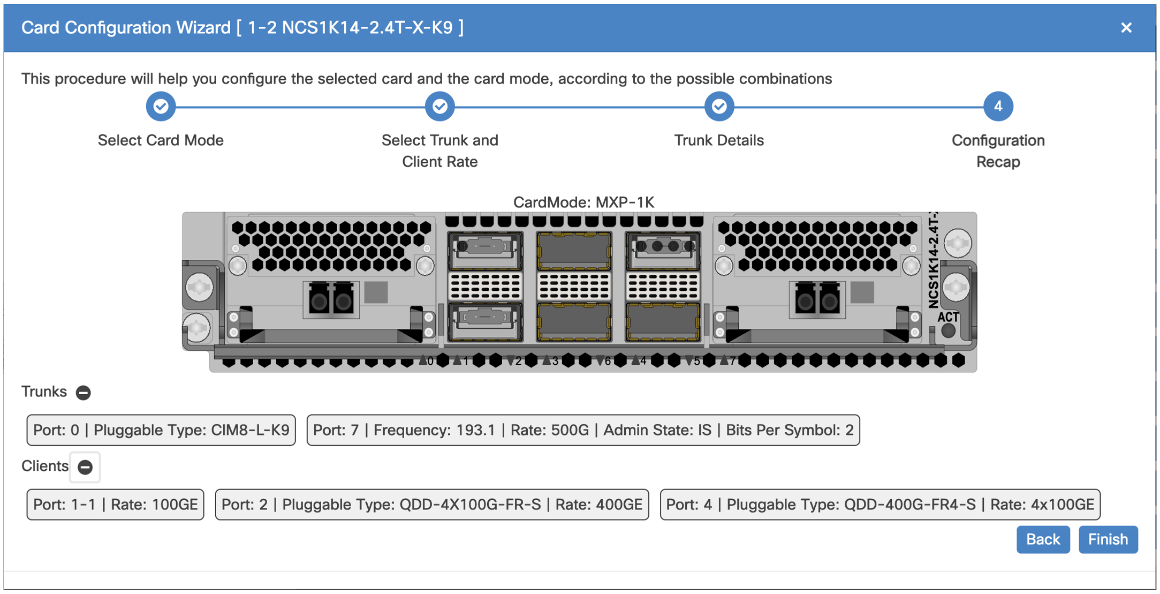
### What to do next

Verify Configuration Details, on page 63

# Verify Configuration Details

In the **Configuration Recap** window, verify the selected configuration across the various windows of the **Card Configuration Wizard**.

*Figure 15: Verify Configuration Details*



Card Configuration Wizard [ 1-2 NCS1K14-2.4T-X-K9 ]

This procedure will help you configure the selected card and the card mode, according to the possible combinations

CardMode: MXP-1K

Trunks

Port: 0 | Pluggable Type: CIM8-L-K9

Port: 7 | Frequency: 193.1 | Rate: 500G | Admin State: IS | Bits Per Symbol: 2

Clients

Port: 1-1 | Rate: 100GE

Port: 2 | Pluggable Type: QDD-4X100G-FR-S | Rate: 400GE

Port: 4 | Pluggable Type: QDD-400G-FR4-S | Rate: 4x100GE

### Before you begin

Add Trunk Details, on page 62

### 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.

# Edit Card Mode for NCS 1000 Cards

Use this task to edit the trunk and client port data rates for a card mode configured on a for a NCS 1000 line card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2

### Procedure

**Step 1** Open the **Card Configuration Wizard** using any of these options.

- To open the **Card Configuration Wizard** from Rack view, perform these steps:

  **a.** Right-click a line card in the Rack, Chassis or Card view.

b. Click **Card Mode**.

c. Select **Edit**.

- To open the **Card Configuration Wizard** from Card view, perform these steps:

  a. Click the **Provisioning** tab.

  b. Click the **Card Modes** section to expand it.

  c. Select the check box corresponding to the card mode you want to edit and click the **Edit card mode** button.

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

For more details about selecting trunk and client data rates, see Select Trunk and Client Data Rate, on page 59.

# Provision SONET or SDH Trace Monitoring

Use this task to provision the trace monitoring parameters that are supported for both the OC192 and STM64 payloads. SONET and SDH trace monitoring is supported on OTN XP card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

**Step 2** Perform one of the following steps:

- Click the **SONET Trace Monitoring** section to provision trace monitoring parameters for SONET.
- Click the **SDH Trace Monitoring** section to provision trace monitoring 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 following table.

*Table 20: SONET and SDH Trace Monitoring Parameters*

| Parameter | Description | Options |
|---|---|---|
| Port | Displays the port number. | — |
| Tx-String | Sets a new transmit string. | 0–15 bytes |

| Parameter | Description | Options |
|---|---|---|
| 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<br>• False |
| Trace-Format | Sets the format in which the received string is displayed. | • 1BYTE<br>• 16BYTE<br>• 64BYTE |

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

# Provision Trail Trace Monitoring

This task allows you to configure the parameters for trail trace monitoring.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### 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, choose **Section** to list all the OTU interfaces and **Path** to list all the ODU interfaces.

**Step 4** Modify required settings as described in the following table.

*Table 21: Trail Trace Identifier Settings*

| Parameter | Description | Options |
|---|---|---|
| Port | Displays the port number. | — |
| Legacy Tx-TTI | Displays the current transmit string of the TTI or sets a new transmit string. | 0-64 bytes |

| Parameter | Description | Options |
|---|---|---|
| Legacy Expected-TTI | Displays the current expected string or sets a new expected string. | 0-64 bytes |
| Legacy Rx-TTI | (Display only) Displays the current received string. | — |
| 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. | • True<br>• False |
| Detect Mode | Sets the mode for detecting the discrepancy between the expected and received trace. | • Disabled<br>• Enabled<br>• SAPI<br>• DAPI<br>• SAPI-and-DAPI |

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

# Provision ODU Interfaces

Use this task to modify the ODU settings of the card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

**Step 3** Modify required settings described in the following table.

*Table 22: ODU Interface Settings*

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

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

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

# Provision OTU Interfaces

Use this task to modify the OTU settings of the card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

**Step 3** Modify required settings described in the following table.

*Table 23: 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<br>• EFEC<br>• EFEC_14<br>• EFEC_17<br>• HG_FEC_20<br>• HG_FEC_7<br>• STANDARD_FEC |
| Interop Mode | Enables interoperability between line cards and other vendor interfaces. | • InteropNone<br>• InteropEnable |
| Supports Sync | (Display only) Displays the SupportsSync card parameter. If the value is true, the card is provisioned as a NE timing reference. | • true<br>• false |
| Sync Msg In | Sets the EnableSync card parameter. Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source. | • true<br>• false |

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

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

# Provision Ethernet Interfaces

Use this task to provision the parameters for the Ethernet interfaces of the card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### 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 following table. These parameters appear depends on the card mode.

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

*Table 24: Card 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/locked state. | Numeric. Default: 1548<br>Range 64–9700 |
| FEC | Sets the FEC mode. When set to On, FEC is enabled. | • NA<br>• Auto (default)<br>• On<br>• Off |
| Duplex | Sets the expected duplex capability of ports. | • Full<br>• Half |
| Mapping | Sets the mapping mode. | • CBR<br>• GFP |
| Auto Negotiation | Enables or disables autonegotiation on the port. | • Disabled<br>• Enabled |
| Squelch Mode | Sets the squelch mode. | • Disable<br>• Squelch<br>• LF |

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

# Provision SONET or SDH Interfaces

Use this task to provision the parameters for the SONET or SDH interfaces of a card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

## Procedure

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

**Step 2** Perform one of the following 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 following table.

*Table 25: SONET or SDH Interface Parameters*

| Field | Description | Valid Values |
|---|---|---|
| Port | Displays the port number. | — |
| Description | Displays the description of the port.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | — |

| Field | Description | Valid Values |
|---|---|---|
| Type | Displays the current payload for the port. OC192 is displayed for SONET systems and STM64 is displayed for SDH systems. | • OC192<br>• STM64 |
| SF BER | Sets the signal fail (SF) bit error rate (BER). | • 1E-3<br>• 1E-4<br>• 1E-5 |
| SD BER | Sets the signal degrade (SD) bit error rate (BER). | • 1E-5<br>• 1E-6<br>• 1E-7<br>• 1E-8<br>• 1E-9 |
| Squelch Mode | When a LOS is detected on the near-end client input, the far-end client laser is turned off. It is said to be squelched.<br>Alternatively, an AIS can be invoked.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | • Squelch<br>• AIS |
| 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.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | • Disable<br>• 50 ms<br>• 100 ms<br>• 250 ms<br>• 500 ms |
| ProvidesSync | (Display only) Displays the ProvidesSync card parameter.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | • true<br>• false |
| Send DoNotUse | When checked, sends a “Do Not Use for Synchronization (DUS)” message on the S1 byte.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | • true<br>• false |

| Field | Description | Valid Values |
|---|---|---|
| Sync SyncMsgIn | Sets the ProvidesSync card parameter. Enables synchronization status messages, which allow the node to choose the best timing source.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | • true<br>• 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.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | • DUS<br>• PRS<br>• RES<br>• SMC<br>• ST2<br>• ST3<br>• ST3E<br>• ST4<br>• STU<br>• TNC |
| Termination Mode | Sets the termination mode. When a session is terminated, the signal is reinitialized or is passed through without any changes.<br>For 400G-XP, 10x10G-LC, and OTU2-XP cards it is Transparent by default.<br>For 40E-MXP card, it is Transparent by default but can be set to the other values as required.<br>**Note**<br>This parameter is not supproted for the OC192 and STM64 card modes. | For SONET:<br>• Transparent<br>• Line<br>• Session<br>For SDH:<br>• Transparent<br>• Multiplex Section<br>• Regeneration Section |
| Admin State | Sets the administrative state of the port. | — |

| Field | Description | Valid Values |
|---|---|---|
| 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<br>• OOS-AU,AINS/ Unlocked-disabled, automaticInService<br>• OOS-MA,DSBLD/ Locked-enabled,disabled<br>• OOS-MA,MT/ Locked-enabled,maintenance |

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

# Provision Optical Channels

Use this task to configure the parameters for the optical channels on the card.

### Before you begin

*Table 26: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| **Optical Channel** Section Enhancements | Cisco IOS XR Release 24.3.1 | The **Optical Channel** section is now updated to allow the configuration of the **Target Power** and **Fixed Ratio** parameter values. |

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

**Step 3** Click the **Edit** button and modify required parameters in the table.

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

This table describes the parameters displayed in the **Optical Channel** section.

*Table 27: Optical Channel Settings*

| Parameter | Description | Options |
|---|---|---|
| Port | (Display only) Displays the port name. | — |
| Reach | Indicates the distance from one node to another node. | • Auto Provision<br>• List of reach values |
| SD FEC | Indicates the standard FEC. | • SD_FEC_15_DE_OFF<br>• SD_FEC_15_DE_ON<br>• SD_FEC_20<br>• SD_FEC_25_DE_OFF<br>• SD_FEC_25_DE_ON<br>• SD_FEC_7 |
| Tx Power (dBm) | Sets the Tx power on the trunk port. | The range is –10.0 to 0.25 dBm. |
| PSM Info | When enabled on a TXP or MXP trunk port that is connected to a PSM card, it allows fast switching on the cards. | • NA<br>• Enable<br>• Disable |
| Frequency (THz) | Sets the frequency in THz | - |
| Wavelength (nm) | Displays the wavelength is set based on the **Frequency**. | - |
| Tx Shutdown | (Display only) | • true<br>• false |
| Width (GHz) | (Display only) | - |
| CD (Working Range) High (ps/nm) | Sets the threshold for maximum chromatic dispersion. | - |
| CD (Working Range) Low (ps/nm) | Sets the threshold for minimum chromatic dispersion. | - |

| Parameter | Description | Options |
|---|---|---|
| Admin State | Sets the port service state unless network conditions prevent the change. | • Unlocked (ETSI)/ IS (ANSI)<br>• Locked, disabled (ETSI)/ OOS, DSBLD (ANSI)<br>• Locked, maintenance (ETSI)/ OOS, MT (ANSI)<br>• Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI) |
| Service State | Displays the service state. | — |
| Target Power | Sets the Rx VOA target power.<br>**Note**<br>You cannot configure this parameter if **Fixed Ratio** is already configured. | • Valid range: -19 dBm to +3 dBm<br>• Default value: -2.0 dBm |
| Fixed Ratio | Sets the Rx VOA fixed ratio.<br>**Note**<br>You cannot configure this parameter if **Target Power** is already configured. | • Valid value: 0.0 dBm |
| Rate | Displays the rate. | — |

# Change Trunk Port Parameters

You can directly change the trunk port parameters from the Rack, Chassis, or Card view. These parameter values can then be viewed in the **Optical Channel** section of the **Provisioning** tab.

Use this task to configure the trunk port parameters, such as admin state, frequency, baud rate, and bits per symbol.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2

### Procedure

**Step 1** Right-click the trunk ports 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 the table Table 27: Optical Channel Settings, on page 76

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

The parameter values are saved and displayed in the **Optical Channel** section of the **Provisioning** tab.

# Provision Optical Threshold Settings

Use this task to set the threshold crossing alert values on the card.

**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 2
- Open the Card View, on page 55

### 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.

*Table 28: Performance Monitoring Parameters*

| Use this parameter | to |
|---|---|
| amplifierTilt | configure the thresholds for ingress or egress amplifier tilt. |
| amplifierGain | configure the thresholds for ingress or egress amplifier gain. |
| opticalPower | configure the thresholds for total Rx or Tx power. |
| opticalPowerOSC | configure the thresholds for total Rx or Tx OSC power. |
| opticalPowerBackReflection | configure thresholds for optical power back reflection. |
| opticalPowerBackReflectionRatio | |
| Raman - 1 | |

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

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

# Provision G.709 Thresholds

Use this task to provision the G.709 PM thresholds for the OTN ports.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

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

You can set the thresholds for Near End or Far End, for 15 minutes or 1 day intervals, or for SM (OTUk) or PM (ODUk).

*Table 29: G.709 PM Thresholds*

| Parameter | Description |
|---|---|
| ES | Errored Seconds shows the number of errored seconds recorded during the PM time interval. |
| SES | Severely Errored Seconds shows the severely errored seconds recorded during the PM time interval. |
| UAS | Unavailable Seconds shows the unavailable seconds recorded during the PM time interval. |
| BBE | Background block error shows the number of background block errors that are recorded during the PM time interval. |
| FC | Failure Counter shows the number of failure counts recorded during the PM time interval. |

# Provision FEC Thresholds

Use this task to provision the FEC thresholds for the card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

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

You can set the FEC thresholds for 15 minutes or one-day intervals.

The possible PM types are:

- BIT-EC—Sets the value for bit errors corrected.
- UNC-WORDS—Sets the value for uncorrectable words.

# Provision RMON Thresholds

Use this task to provision the RMON thresholds on the control card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

**Step 1** Click the **Provisioning** > **RMON Thresholds** tabs.

**Step 2** Click the + button.

The Create RMON Threshold dialog box appears.

**Step 3** From the **Port ID** drop-down list, choose the port number.

**Step 4** From the **Variable** drop-down list, choose a variable.

**Step 5** From the **Alarm Type** drop-down list, indicate whether the event is triggered by the rising threshold, falling threshold, or both thresholds.

The available options are **Rising Threshold**, **Falling Threshold**, and **Rising and Falling Threshold**.

**Step 6** From the **Sampling Type** drop-down list, choose either **Relative** or **Absolute**.

**Relative** restricts the threshold to use the number of occurrences within the user-set sample period.

**Absolute** sets the threshold to use the total number of occurrences, regardless of the time period.

**Step 7** Enter the appropriate number of seconds in the **Sampling Period** field.

**Step 8** Enter the appropriate number of occurrences in the **Rising Threshold** field.

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 1000 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

**Step 9** Enter the appropriate number of occurrences in the **Falling Threshold** field.

In most cases, a falling threshold is set lower than the rising threshold.

**Step 10** Click **Apply**.

# Provision Loopback

Use this task to provision loopback on the card.

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

**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 2
- Open the Card View, on page 55
- Perform the loopback configuration only in the maintenance service state. To place the trunk ports in the Locked, maintenance state, see Provision Optical Channels, on page 75.

### 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, choose Terminal, Facility, Terminal-Drop, or Facility-Drop for each port required.

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

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

# Provision Optical Safety

Use this task to provision the optical safety parameters for cards.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

**Step 2** Click the **Live Data** section to expand it.

**Step 3** Modify required settings described in the following table:

*Table 30: Optical Safety Parameters for Cards*

| Parameter | Description | Options |
|---|---|---|
| Interface | (Display only) Displays the port name, port type, and direction. | — |
| Supported Safety | (Display only) Displays the supported safety mechanism. | • ALS for line cards and control cards.<br>• ALS-OSRI for amplifier cards. |
| ALS Mode | Automatic laser shutdown mode. The ALS mode is disabled for RX ALS interfaces. | From the drop-down list, choose one of the following:<br>• ALS-Disabled—Deactivates ALS.<br>• Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired.<br>• Manual Restart |
| OSRI | Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down.<br>**Note**<br>OSRI configuration is not supported on the transponder and muxponder cards. | From the drop-down list, choose one of the following:<br>• OSRI-OFF<br>• OSRI-ON |
| ALS Status | (Display only) ALS status of the device. | • Working<br>• Shutdown |
| Recovery Pulse Interval (Sec.) | Displays the interval between two optical power pulses. | 60 to 300 seconds. |
| Recovery Pulse Duration (Sec.) | Displays the duration of the optical power pulse that begins when an amplifier restarts. | 2 to 100 seconds |

| Parameter | Description | Options |
|---|---|---|
| Manual Restart | Triggers manual restart action for the ALS interface. However, manual restart does not happen if Mode is set to Automatic Restart or Disabled. | — |

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

# Provision SONET or SDH Thresholds

Use this task to provision SONET or SDH thresholds for OC192 and STM64 payload ports on the OTN XP card. 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 2
- Open the Card View, on page 55

### 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** In the **New SONET/SDH Threshold** dialog, select these details:

*Table 31: 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 either 15-minute or 24-hour intervals. | • 15min<br>• 24Hour |

| Field | Description | Valid Values |
|---|---|---|
| Direction | Sets the direction. | • ES<br>• SES<br>• UAS<br>• EB<br>• 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. | — |

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

# Enable Attention LED

*Table 32: 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 is particularly helpful for troubleshooting and maintenance by locating the device in its installed location.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

**Step 2** Click the **Attention Led** section to expand it.

**Step 3** Perform any one of the following steps:

a) To turn on the Attention LED of a chassis provisioned on the rack, perform these steps:

1. Select *true* from the **Attention Led for** drop-down list and click **Apply**.

b) To turn on the Attention LED of all the ports of a line card, perform these steps:

1. Select *true* from the **Attention Led for** drop-down list and click **Apply**.

c) To turn on the Attention LED of a specific port of a line card, perform these steps:

1. Click **Edit**.
2. Select *true* corresponding to the port you want to blink the Attention LED and click **Apply**.

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

# PSM card protection switching

| Feature Name | Release Information | Description |
|---|---|---|
| Protection Switching on PSM Card | Cisco IOS XR Release 24.3.1 | Protection switching provides protection mechanism against optical fiber faults or signal failure. In case a failure is detected, live traffic is automatically moved from the working path to the protection path to prevent any data loss.<br>You can enable this feature from the **Protection** section of the **Maintenance** tab. |

Cisco Optical Site Manager enables the configuration of protection switching on the PSM card, ensuring uninterrupted traffic flow by automatically switching traffic from a failed path to a working path.

Protection switching provides a mechanism to safeguard traffic in the event of a signal failure:

- The working path is the active path that typically carries traffic.
- In the event of a signal failure on the working path, traffic is immediately switched to the protection path to maintain service continuity.

### 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 revertive protection switching

Protection switching offers a safeguard against optical fiber faults. When a failure is detected, live traffic is automatically switched from the working path to the protection path, ensuring uninterrupted data transmission.

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

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### 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.

# Enable or disable 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.

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

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

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

**Step 4** Perform these steps to enable non-revertive switching:

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**.

a)

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

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

b) Click **Apply**.

# Perform a manual switch

If changes are required during a scheduled maintenance window on the working or protection path, you can manually switch traffic between the two paths.

Follow these steps to perform a manual switch:

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

### Procedure

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

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

**Step 3** Click 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 selected interface becomes active and is displayed under the **Active Interfaces** column.

# 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.

Use this task to view the current and historical PM parameters of a card.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the Card View, on page 55

## Procedure

**Step 1** Click the **Performance** tab.

**Step 2** Select the interval of the threshold to *15 Min* or *24 Hour*.

**Step 3** Click the plus icon to add a new SONET or SDH threshold.
The **New SONET/SDH Threshold** dialog is displayed.

**Step 4** In the **New SONET/SDH Threshold** dialog, select these details:

*Table 33: New SONET/SDH Threshold Dialog*

| Use this drop-down | To | Valid Values |
|---|---|---|
| Granularity | Select the threshold for either 15-minute or 24-hour intervals. | • 15min<br>• 24Hour |
| Interface Type | Select the interface type of the card. | The options available are based on the selected card. |
| Interface | Select the port of the card. | The options available are based on the selected card. |
| Location | Select the location. | • nearEnd<br>• farEnd |

**Step 5** Click **Get PM**.
The PM parameters are displayed on the table.

**Step 6** (Optional) Click the **Excel Export** button to export the parameters to an Excel sheet.

**Step 7** 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.

CHAPTER 7

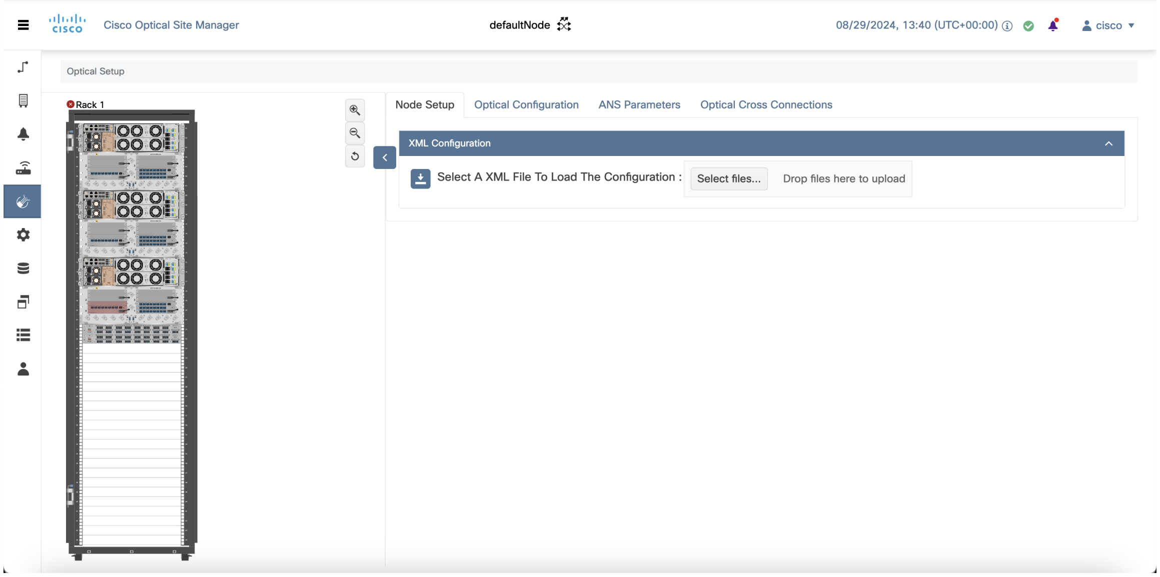
# Configure the Node

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

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

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

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


Cisco Optical Site Manager
defaultNode
08/29/2024, 13:40 (UTC+00:00)
cisco
Optical Setup
Rack 1
Node Setup
Optical Configuration
ANS Parameters
Optical Cross Connections
XML Configuration
Select A XML File To Load The Configuration :
Select files...
Drop files here to upload

# Import the Cisco Optical Network Planner Configuration File

If you have a configuration file NETCONF file (.xml) exported from Cisco Optical Network Planner, you can import it to Cisco Optical Site Manager. The file includes parameters for the node, shelf, card type, port (including the wavelength of the card), pluggable port module (PPM), OTN, and FEC parameters.

Only the values present in XML format appear in the configuration file parameters. If the values are not in XML format, a column appears blank. The XML file values are independently reported and do not affect any configuration changes that you apply.

Use this task to import the Cisco Optical Network Planner NETCONF file (.xml) into Cisco Optical Site Manager.

### Before you begin

Before importing the NETCONF file (.xml), ensure that:

1. The NETCONF file (.xml) contains the following parameters available on Cisco Optical Site Manager:
   - device name
   - uid
   - rack id
   - chassis/passive unit id
2. You are logged in to Cisco Optical Site Manager. For details, see Log into Cisco Optical Site Manager, on page 2.

.

### Procedure

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

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

**Step 3** Click **Select Files**, navigate to the location where the NETCONF file (.xml) is present and select it.
A confirmation message appears.

**Step 4** Click **Yes**.

**Step 5** Click **Upload**.
A confirmation message appears after the upload is complete.

**Step 6** To export the XML file, click the **Download Node Configuration as XML** button.

# 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 2

### 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

*Table 34: 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. |

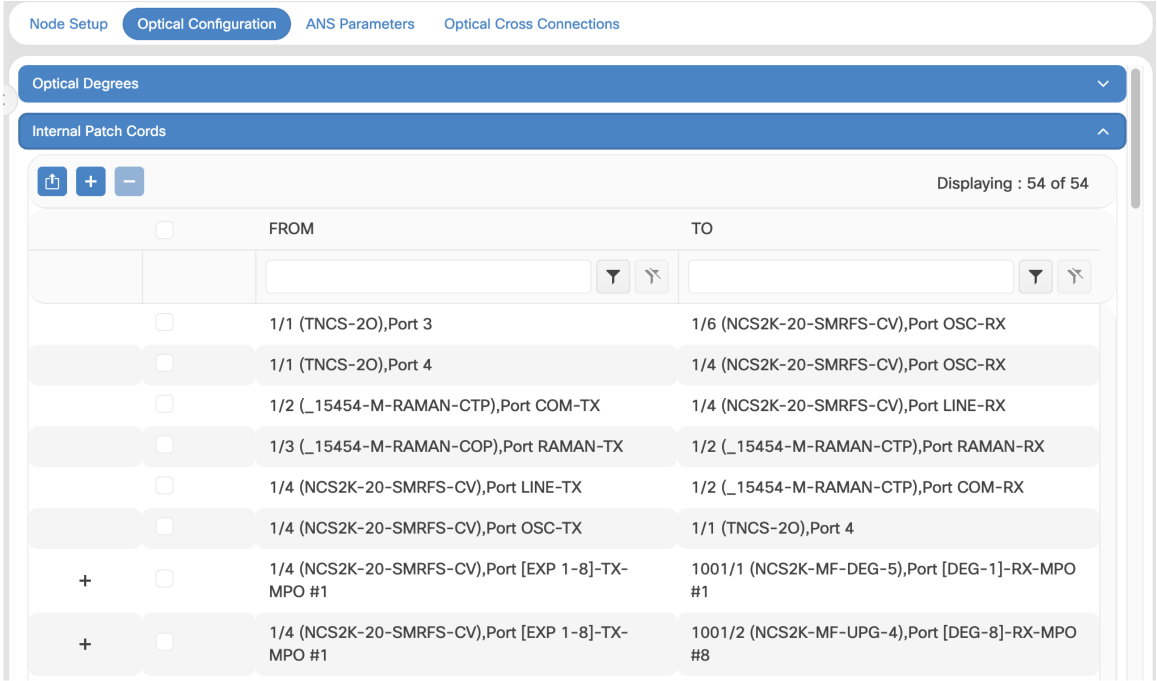
Virtual links can be created between network termination points using Internal Patch Cords (IPC). These termination points include OSC ports, transponder or muxponder trunk ports, line ports, and passive device ports.

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**.

# Create Internal Patch Cords

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

***Figure 17: Internal Patch Cords***



Displaying : 54 of 54

|  | □ | FROM | TO |
|---|---|---|---|
|  | □ | 1/1 (TNCS-2O),Port 3 | 1/6 (NCS2K-20-SMRFS-CV),Port OSC-RX |
|  | □ | 1/1 (TNCS-2O),Port 4 | 1/4 (NCS2K-20-SMRFS-CV),Port OSC-RX |
|  | □ | 1/2 (_15454-M-RAMAN-CTP),Port COM-TX | 1/4 (NCS2K-20-SMRFS-CV),Port LINE-RX |
|  | □ | 1/3 (_15454-M-RAMAN-COP),Port RAMAN-TX | 1/2 (_15454-M-RAMAN-CTP),Port RAMAN-RX |
|  | □ | 1/4 (NCS2K-20-SMRFS-CV),Port LINE-TX | 1/2 (_15454-M-RAMAN-CTP),Port COM-RX |
|  | □ | 1/4 (NCS2K-20-SMRFS-CV),Port OSC-TX | 1/1 (TNCS-2O),Port 4 |
| + | □ | 1/4 (NCS2K-20-SMRFS-CV),Port [EXP 1-8]-TX-MPO #1 | 1001/1 (NCS2K-MF-DEG-5),Port [DEG-1]-RX-MPO #1 |
| + | □ | 1/4 (NCS2K-20-SMRFS-CV),Port [EXP 1-8]-TX-MPO #1 | 1001/2 (NCS2K-MF-UPG-4),Port [DEG-8]-RX-MPO #8 |

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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. of the patch cord from the **From** and **To** drop-down lists.

   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 **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) the **Reset** button to remove all the 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.

**Tip** 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.

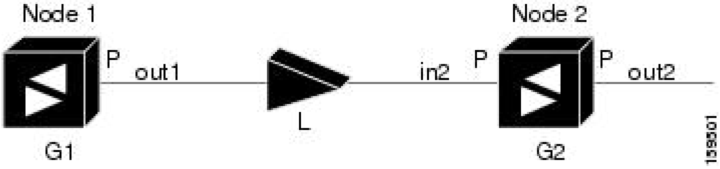
The amplifier software uses a control gain loop to keep channel power constant regardless of the number of channels. It monitors input power changes and adjusts output power proportionately. The shelf controller software emulates the control output power loop to compensate for fiber degradation.

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 18: 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 2

### 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 2

### 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 view or modify span loss parameters.

**Note** 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 2

### 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 + button corresponding to a degree in the list and then click **Span Loss Measured Data** to expand it.

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

A message appears. Click **OK**.

**Step 5** Click the Retrieve button to view the updated **Measured Span Loss**, **Measured Accuracy**, and **Measured time** values.

**Step 6** Enter the values for **Min. Exp. Span Loss** or **Max. Exp. Span Loss** in dB. The range is from 0 to 99.

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

A confirmation message appears.

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

The span loss range is extended including the Accuracy value. A Span Loss Out of Range condition is raised when the measured span loss is higher than the extended range.

**Step 9** (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

---

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

- **Degree**—Displays the side for which span loss information appears.
- **Measured By**—Displays whether the measurement was executed with or without channels. Values are OSC or CHANNEL.
- **Min Exp. Span Loss (dB)**—Displays the minimum expected span loss (in dB) for the incoming span.
- **Max Exp. Span Loss (dB)**—Displays the maximum executed span loss (in dB) for the incoming span.
- **Measured Span Loss (dB)**—Displays the measured span loss value.
- **Measured Accuracy (dB)**—Displays the resolution or accuracy of the span loss measurement. The resolution is +/-1.5 dB if the measured span loss is 0–25 dB. The resolution is +/-2.5 dB if the measured span loss is 25–38 dB.
- **Measured Time**—Displays the time and date when the last span loss measured value is changed.

# Configure Amplifier Parameters

Use this task to configure the optical amplifier parameters.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the card view, on page 28

### Procedure

---

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

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

**Step 3** Modify any of the settings described in the following table.

*Table 35: Amplifier Parameters for Amplifier Cards*

| Parameter | Description | Options |
|---|---|---|
| Working Mode | Shows the working mode. | • Channel Power<br>• Total Power<br>• Optimized<br>• Fixed Gain<br>• Start and Hold |
| Tilt Setpoint (dB) | Target output tilt requested by the user. | — |
| PSD Setpoint (dBm/GHz) | Power Spectral Density. Target output power requested by the user for each circuit. | — |
| Gain Setpoint (dB) | Target amplifier gain requested by the user. | — |
| Gain Range | Sets the gain range of the amplifier. | • Gain Range 1<br>• Gain Range 2<br>• No Gain Range |

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

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

*Table 36: Amplifier 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. | — |

| Parameter | Description | Displayed Values |
|---|---|---|
| Working Mode | Shows the working mode. | • Channel Power<br>• Total Power<br>• Optimized<br>• Fixed Gain<br>• Start and Hold |
| Role | Role of the amplifier. | • Preamplifier<br>• Booster |
| Actual Gain (dB) | Actual gain setpoint. | — |
| Target Gain (dB) | Target gain setpoint. | — |
| Tilt Setpoint (dB) | Target output tilt requested by the user. | — |
| PSD Setpoint (dBm/GHz) | Power Spectral Density. Target output power requested by the user for each circuit. | — |
| PSD Optimized (dBm/GHz) | Optimized PSD | — |
| Gain Setpoint (dB) | Target amplifier gain requested by the user. | — |
| Gain Range | Sets the gain range of the amplifier. | • Gain Range 1<br>• Gain Range 2<br>• No Gain Range |
| Power Degrade Threshold (High) (dBm/GHz) | Shows the current value of the optical power degrade high threshold. | — |
| Power Degrade Threshold (Low) (dBm/GHz) | Shows the current value of the optical power degrade low threshold. | — |
| Status | Shows the current status of the amplifier. | — |

| Parameter | Description | Displayed Values |
|---|---|---|
| Gain Degrade High (dB) | (Display only) Shows the current value of the gain degrade high threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode.<br>Gain Degrade High refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up. | — |
| Gain Degrade Low (dB) | (Display only) Shows the current value of the gain degrade low threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode.<br>Gain Degrade Low refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up. | — |

# Provision Interface Parameters

Use this task to change the optical interface parameters.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the card view, on page 28

### 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 settings described in the following table. The provisionable parameters are listed in the *Options* column in the table.

*Table 37: 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:<br>• Unlocked / IS<br>• Locked, disabled/OOS, DSBLD<br>• Locked, maintenance/OOS, MT<br>• Unlocked, automaticInService/IS, AINS |
| Service State | (Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State. | • IS-NR/<br>Unlocked-enabled<br>• OOS-AU,AINS/<br>Unlocked-disabled, automaticInService<br>• OOS-MA,DSBLD/<br>Locked-enabled,disabled<br>• OOS-MA,MT/<br>Locked-enabled,maintenance |
| Optical Power (dBm) | (Display only) Displays the optical power for each port. | — |
| OSC Power (dBm) | (Display only) Displays the service-channel power level for each port. | — |
| Optical PSD Setpoint (dBm/GHz) | Target output Power Spectral Density requested by the user. | -50 to 10 |
| Attenuator Value (dB) | Sets the attenuator value. | — |
| Optical Power Threshold Low (dBm) | Fail low threshold used to detect the LOS alarm on the port. | — |
| OSC Power Threshold Low (dBm) | (Display only) Displays the OSC power level for each port. | — |

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

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

**Note**

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

# 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 2
- Open the card view, on page 28

### 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 38: Raman Amplifier Parameters for Amplifier Cards*

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

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

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

*Table 39: RAMAN Pump Power Parameters*

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

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

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

# Manage Raman Interface Parameters

Use this task to manage the Raman interface parameters.

### Before you begin

- Log into Cisco Optical Site Manager, on page 2
- Open the card view, on page 28

### 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 40: Interface Options*

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

| Parameter | Description | Options |
|---|---|---|
| Admin State | Sets the administrative state of the port. | From the drop-down list, choose one of the following:<br>• Unlocked (ETSI)/ IS (ANSI)<br>• Locked, disabled (ETSI)/OOS, DSBLD (ANSI)<br>• Locked, maintenance (ETSI)/OOS, MT (ANSI)<br>• Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI) |
| Service State | (Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State. | • IS-NR/<br>Unlocked-enabled<br>• OOS-AU,AINS/<br>Unlocked-disabled, automaticInService<br>• OOS-MA,DSBLD/<br>Locked-enabled,disabled<br>• OOS-MA,MT/<br>Locked-enabled,maintenance |
| Optical Power (mW) | (Display only) Displays the optical power for each port. | — |
| Current Optical Power Setpoint (mW) | (Display only) Shows the current value of the optical power setpoint that must be reached. | — |
| Current Power Degrade High (mW) | (Display only) Shows that the current value of the optical power degrade high threshold.<br>Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card. | — |

| Parameter | Description | Options |
|---|---|---|
| Current Power Degrade Low (mW) | (Display only) Shows that the current value of the optical power degrade high threshold configured in the card.<br>Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card. | — |
| Current Power Failure Low (mW) | (Display only) Shows the optical power failure low threshold for the port. | — |

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

# Optical Cross-connect Management

Optical cross-connect (OXC) circuits are used to connect two optical nodes on a specified C-band wavelength. These circuits are created using data models and are bidirectional in nature. The connection is established through the ports present on the wavelength selective switches, multiplexers, demultiplexers, and add/drop cards.

In an OXC circuit, the wavelength from a source interface port enters to a DWDM system and then exits from the DWDM system to the destination interface port.

The administrative states are:

- IS/Unlocked
- IS, AINS/Unlocked, AutomaticInService
- OOS, DSBLD/Locked, disabled

## View Optical Cross-connect Circuits

Use this task to view the details of the optical cross-connects that are created for a node using data models.

**Note** The optical cross-connects are read-only and cannot be modified.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

**Step 2** Click the **Optical Cross Connections** tab.

**Step 3** To delete an optical cross-connect, select the check box corresponding to the OXC you want to delete and click the - button.

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

**Step 5** (Optional) Click the **Download OXC as XML** button to download the details of the optical cross-connects as a XML file.

**Step 6** (Optional) Click the **Sync from device** button to synchronize the optical cross-connect information with the associated NCS 1000 device.

The **Optical Cross Connections** tab displays the following details for each cross-connect.

- **Connection Label**—Displays the name of the cross-connect.
- **Type**—Displays the type of cross-connect. It is bidirectional.
- **Admin Status**—Displays the admin state on the circuit.
- **Service Status**—Displays the status of the service.
- **Central Frequency (THz)**—Displays the spectral position of the circuit.
- **Allocation Width (GHz)**—Displays the bandwidth occupied by the service. The range is 25 to 300GHz.
- **Signal Width (GHz)**—Displays the carrier bandwidth.
- **Path 1 End-points**—Displays the source and destination interfaces of the path.
- **Path 2 End-points**—Displays the source and destination interfaces of the path.

To view Path 1 or Path 2, click the + icon to expand the cross-connect. Click the down arrow on the right to view the internal details of Path 1 or Path 2. The details are:

- **Interface Name**—Displays the interface name.
- **Optical Power**—Displays the value of the optical power.
- **Power Failure Low**—Displays the threshold for power failure.
- **Optical PSD Setpoint (dBm/GHz)**—Displays the configured optical power spectral density setpoint. This setpoint is independent of the width of the circuit.
- **Current PSD Setpoint**—Displays the current optical power spectral density setpoint. This setpoint is independent of the width of the circuit.
- **Optical Power Setpoint**—Displays optical power setpoint. This setpoint is scaled to the width of the circuit and matches the value of the optical power parameter.

CHAPTER 8

# Backup and Restore Database

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

*Table 41: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Backup and Restore Database | Cisco IOS XR Release 24.3.1 | Cisco Optical Site Manager now supports backup and restore for both its own database and the databases of the devices it manages.<br>When unexpected failures occur, such as hardware malfunctions or software corruption, your data is securely backed up and easily recoverable. |

*Figure 19: Back Up and Restore Database*

# 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.

Use this task 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 2

### 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.

## 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.

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 2

### Procedure

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

**Step 2** Click the **Restore Options** button.
The **Choose a Restore Option** dialog box appears.

**Step 3** Do one of the following to restore the database:

**Note**
When restoring the Cisco Optical Site Manager or full database on the host device, the Cisco Optical Site Manager becomes temporarily unavailable.

| To restore | click the *Restore* button |
|---|---|
| only Cisco Optical Site Manager database, | in the *COSM* section. |
| only the managed devices database, | in the *Devices* section after selecting the one or all check boxes corresponding to the devices for which you want to restore the data. |
| 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 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 2

### 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

*Table 42: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| SSH Upgrade | Cisco IOS XR Release 25.1.1 | The Cisco Optical Site Manager software package now includes integrated SSH libraries. When you upgrade to Release 25.1.1, these libraries are automatically incorporated into the NCS 2000 Cisco Optical Site Manager software package.<br>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.

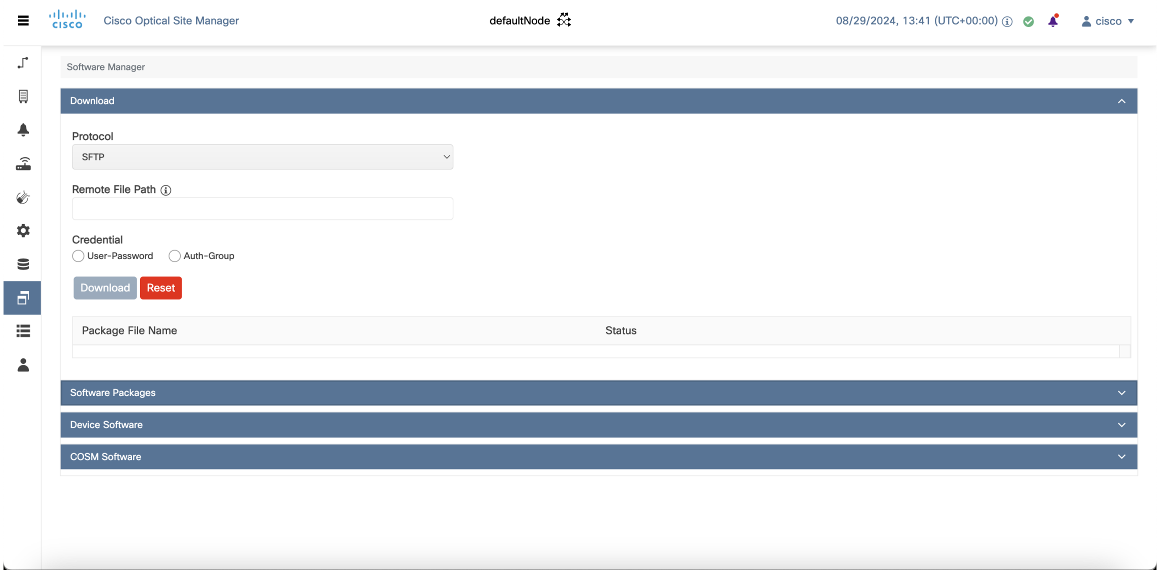
# Workflow for Software Upgrade

You can upgrade NCS 1000 device and Cisco Optical Site Manager application software using the Software Manager.

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 card. For more details, see Download ISO line card image, on page 120. The downloaded packages appear in the **Software Packages** tab.
2. **Download Software Package to Device**: Download the software package from Cisco Optical Site Manager card to the NCS 1000 device. For more details, see Download Software Package on Device, on page 121.
3. **Activate Device Software**: Activate the device software. For more details, see Activate NCS 1000 device software, on page 122.

***Figure 20: Software Upgrade***



Protocol: SFTP

# Download ISO line card image

Before

Download the necessary ISO line card image from the Cisco repository to the Cisco Optical Site Manager card.

Follow these steps to download the ISO line card image.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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

•

### Before you begin

•

### Procedure

**Example:**

*Table 43:*

| If.. | Then.. |
|---|---|
| | |
| | |

*Table 44:*

| When.. | And.. | Then.. | And.. |
|---|---|---|---|
| | | | |

•

*Figure 21:*

-

Example

What to do next

-

# Activate NCS 1000 device software

Activate the Cisco Optical Site Manager software immediately after downloading it to ensure proper operation.

Follow these steps to activate the NCS 1000 device software package.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

**Step 1** Click **Software Manager**.

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

**Step 3** Select the NCS 1000 device for which you want to activate the software, then click **Activate**.

**Step 4** For the NCS 1000 device, select the ISO to be activated.

**Note**
If the device hosting the Cisco Optical Site Manager application is activated, manageability is temporarily lost while the new device image is loaded and the updated Cisco Optical Site Manager application restarts.

**Caution**
Do not install a base ISO without Cisco Optical Site Manager component on the device that already has Cisco Optical Site Manager. This will remove the Cisco Optical Site Manager application and leave the device in an inconsistent state.

The selected software is activated.

# Delete software package

Log into Cisco Optical Site Manager, on page 2

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.

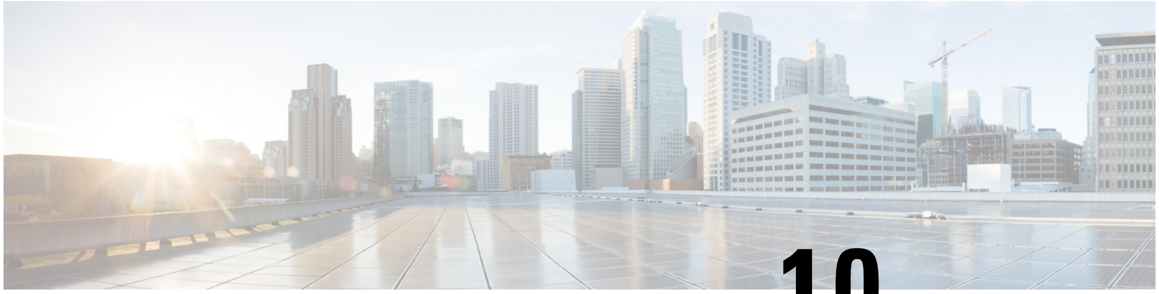
**Step 3** Select the checkbox corresponding to the *SW Package ID* of the Cisco Optical Site Manager package you want to delete.

**Step 4** Click **Delete**.

A confirmation message appears.

**Step 5** Click **Ok**.

The selected software package is deleted.

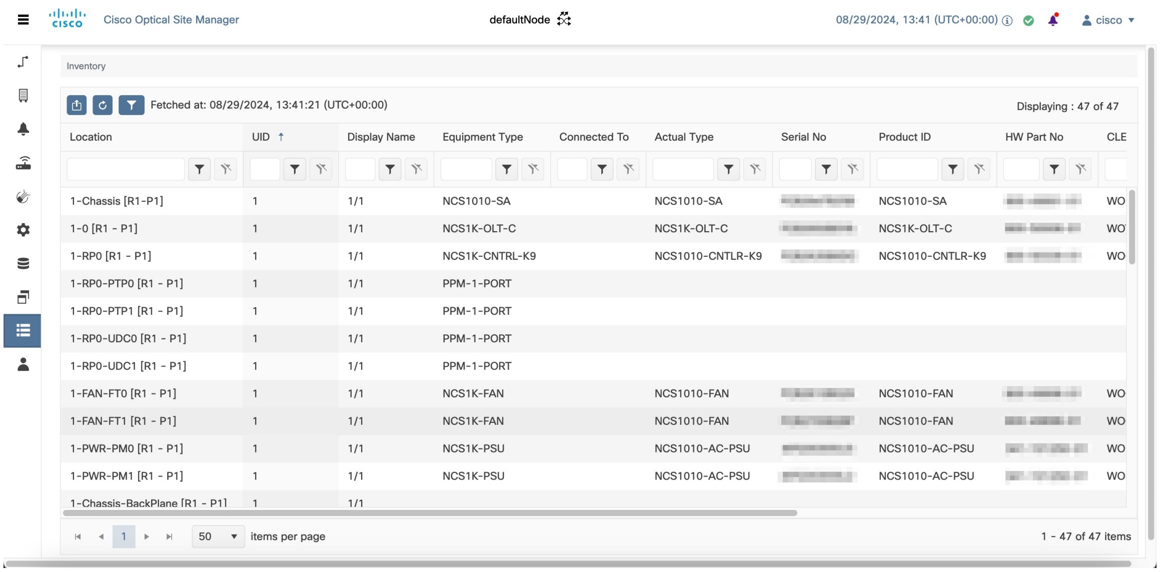


CHAPTER 10

# View Inventory

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

*Figure 22: View Inventory*



Fetched at: 08/29/2024, 13:41:21 (UTC+00:00)

Displaying : 47 of 47

| Location | UID | Display Name | Equipment Type | Connected To | Actual Type | Serial No | Product ID | HW Part No | CLE |
|---|---|---|---|---|---|---|---|---|---|
| 1-Chassis [R1-P1] | 1 | 1/1 | NCS1010-SA | | NCS1010-SA | [redacted] | NCS1010-SA | [redacted] | WO |
| 1-0 [R1 - P1] | 1 | 1/1 | NCS1K-OLT-C | | NCS1K-OLT-C | [redacted] | NCS1K-OLT-C | [redacted] | WO |
| 1-RP0 [R1 - P1] | 1 | 1/1 | NCS1K-CNTRL-K9 | | NCS1010-CNTLR-K9 | [redacted] | NCS1010-CNTLR-K9 | [redacted] | WO |
| 1-RP0-PTP0 [R1 - P1] | 1 | 1/1 | PPM-1-PORT | | | | | | |
| 1-RP0-PTP1 [R1 - P1] | 1 | 1/1 | PPM-1-PORT | | | | | | |
| 1-RP0-UDC0 [R1 - P1] | 1 | 1/1 | PPM-1-PORT | | | | | | |
| 1-RP0-UDC1 [R1 - P1] | 1 | 1/1 | PPM-1-PORT | | | | | | |
| 1-FAN-FT0 [R1 - P1] | 1 | 1/1 | NCS1K-FAN | | NCS1010-FAN | [redacted] | NCS1010-FAN | [redacted] | WO |
| 1-FAN-FT1 [R1 - P1] | 1 | 1/1 | NCS1K-FAN | | NCS1010-FAN | [redacted] | NCS1010-FAN | [redacted] | WO |
| 1-PWR-PM0 [R1 - P1] | 1 | 1/1 | NCS1K-PSU | | NCS1010-AC-PSU | [redacted] | NCS1010-AC-PSU | [redacted] | WO |
| 1-PWR-PM1 [R1 - P1] | 1 | 1/1 | NCS1K-PSU | | NCS1010-AC-PSU | [redacted] | NCS1010-AC-PSU | [redacted] | WO |
| 1-Chassis-BackPlane [R1 - P1] | 1 | 1/1 | | | | | | | |

1 | 50 items per page | 1 - 47 of 47 items

- View inventory of all racks or chassis, on page 125
- View inventory of a rack or chassis, on page 126

# 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.

Follow these steps to view the inventory of all the racks and chassis:

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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 2

### 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).

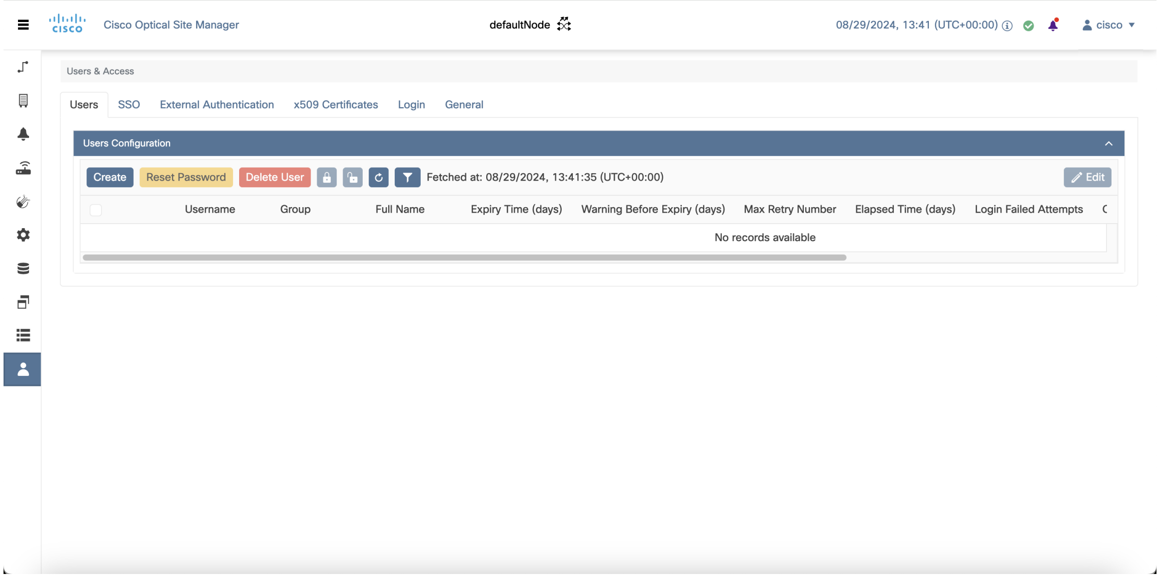
The **Inventory** page appears and displays the inventory details.

CHAPTER 11

# Manage User Access and Authentication

This chapter describes the tasks to manage users accounts, SSO authentication, external authentication, web certificates.

*Figure 23: Manage User Access and Authentication*



Fetched at: 08/29/2024, 13:41:35 (UTC+00:00)

| | Username | Group | Full Name | Expiry Time (days) | Warning Before Expiry (days) | Max Retry Number | Elapsed Time (days) | Login Failed Attempts | C |
|---|---|---|---|---|---|---|---|---|---|
| | | | | No records available | | | | | |

# Users Configuration

This section describes the tasks to manage users and user profile passwords.

# Create Users

Use this task to create new users. Only an admin can create new users.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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 following details in the **Create User** dialog box.

a) **User Name**—Type the user name. The user name must be a minimum of six and a maximum of 40 characters. It can include alphanumeric characters (a-z, A-Z, 0-9) and special characters @, " - " (hyphen), and " . " (dot).

b) **Password**—Enter the password that will be used by the user to log into Cisco Optical Site Manager. 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 number is 127. The password must not contain the user name.

c) Retype the password in the **Retype Password** field.

d) **Expiry Time (days)**—Enter the time period in days before which the user needs to change the password. For example, if the user has set the expiry time to be 20 days, the user must change the password before 20 days are over.

The user is automatically moved to the *Password* group after this time elapses. The user must change the password before performing any other action.

e) **Warning Before Expiry (days)**—Enter the number of days the user is warned of the expiry of the password.

f) **Max Retry Number**—Specify the maximum number of consecutive unsuccessful login attempts that are allowed. When the maximum number of failed login attempts is reached, the account is automatically moved to the *Password* group.

g) **Group**—Select the group from the drop-down list. The available options are *admin*, *editor*, *maintenance*, *snmp* and *viewer*.

**Step 5** Click **Create**.

The new user is added to the list.

# Change User Password

Use this task to change password for a user. Only an admin or superusers can change the password.

### Before you begin

Log into Cisco Optical Site Manager, on page 2.

### 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**.

A confirmation message appears.

**Step 8** Click **OK**.

# Delete Users

Use this task to delete users. Only an admin or superuser can delete users. Superusers cannot be deleted using this task.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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.

# Single sign-on (SSO)

This chapter describes the tasks to create and enable Single Sign On in Cisco Optical Site Manager using Security Assertion Markup Language (SAML) and Central Authentication Service (CAS).

## Create and Enable SSO with SAMLv2

Use this task to configure and enable SSO SAMLv2 details. Only an admin can configure 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** Perform any one of the following:

- Type the entity ID and metadata URL of the identity provider in the **IDP Entity ID** and **IDP Metadata Url** fields respectively.
- Type the entity ID and metadata of the identity provider in the **IDP Entity ID** and **IDP Metadata** fields respectively.

**Step 5** (Optional) Type the **Proxy Address** and **Proxy Port**.

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

## Create SSO with CAS

Use this task to add an SSO user with CAS. Only an admin can add SSO users.

Ensure that both SSO users and other users are different.

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **SSO CAS** section to expand it

**Step 3** In the **SSO Users** area, perform these steps:

a) Click the **+** button.

The **Creat SSO User** dialog box appears.

b) Enter the username in the **Username** field.

c) Choose the user group from the **Group** drop-down list.

The options are *viewer* and *editor*. The viewer when mapped for SSO, can only view the Cisco Optical Site Manager configurations. The Editor when mapped for SSO, can configure devices.

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

A confirmation message appears.

**Step 5** Click **Yes**.

## Enable SSO with CAS

Use this task to enable SSO. Only an admin or superuser can enable SSO.

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **SSO CAS** tab.

**Step 3** In the **SSO CAS** page, perform these steps:

a) Click **SELECTION** to expand the section.
b) Select the **Enable CAS** check box to enable SSO with CAS on Cisco Optical Site Manager.
c) Enter the Cisco Optical Network Controller server IP address in the **IP Address** field.
d) (Optional)You can change the port number in the **Port** field. The default port number is 443.

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

A confirmation message appears.

**Step 5** Click **Yes**.

# 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 .

The following table lists some external authentication scenarios that describe some possible authentication errors, causes, and actions.

*Table 45: External and Local Authentication Scenarios*

| External and Local Authentication Combination | Possible Authentication Scenario | Possible Cause | Action to be Taken |
|---|---|---|---|
| • External Authentication Enabled and Local Authentication Disabled | Server denies authentication | External username or password is incorrect | Enter the correct username and password to log in to the system. |
| | Server not reachable | IP address, shared secret or port number is not configured correctly although username or password could be correct | You are locked out of the system. Ensure that you have configured correct IP address, shared secret, and port number. |
| • External authentication enabled and Local authentication enabled | Server denies authentication (although location authentication is enabled) | External username or password is incorrect | Enter the correct username and password to log in to the system.<br>Local authentication only works when the RADIUS or TACACS external servers are not reacheable. |
| | Server not reachable (Local authentication is enabled) | IP address, shared secret, port number is not configured correctly although username or password could be correct | Use local authentication credentials to log in to Cisco Optical Site Manager. |

# Limitations for RADIUS or TACACS Authentication

- External user list is maintained with username and its respective group (admin, editor, or viewer). 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 (501th 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.

- External authentication is applicable only on Cisco Optical Site Manager web user interface. External authentication using logging into the Netconf console is not supported.

# RADIUS Authentication

Use the following tasks to manage RADIUS authentication on Cisco Optical Site Manager.

**Note** Only an admin or superuser 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 2

Ensure that you have added Cisco Optical Site Manager instances with RADIUS IP addresses in the Cisco Secure ACS server.

### 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 or superuser 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 2
- Create RADIUS Server Entry, on page 133

### 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 **SELECTION** 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 RADIUS server is reacheable** check box to enable the RADIUS server as a final authentication option.

**Note**

When you enable external authentication, local authentication is enabled by default to avoid lock out scenarios (such as configuration errors). Until external authentication is enabled, local authentication can be enabled or disabled based on your requirement.

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 or superuser can modify RADIUS server settings.

### Before you begin

Log into Cisco Optical Site Manager, on page 2 and Create RADIUS Server Entry, on page 133

### 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:

- **Name**
- **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 2

### 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 **SELECTION** 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 RADIUS server is reacheable** 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 2

### 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 or superuser can add TACACS+ server. You can add upto ten TACACS+ server.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

Ensure that you have added Cisco Optical Site Manager instances with TACACS+ IP addresses in the Cisco Secure ACS server.

### 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 2
- Create TACACS+ Server Entry on Cisco Optical Site Manager, on page 136

### 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 **SELECTION** 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 TACACS+ server is reacheable** check box to enable the TACACS+ server as a final authentication option.

**Note**

When you enable external authentication, local authentication is enabled by default to avoid lock out scenarios (such as configuration errors). Until external authentication is enabled, local authentication can be enabled or disabled based on your requirement.

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 or superuser can modify TACACS+ server settings.

### Before you begin

Log into Cisco Optical Site Manager, on page 2 and Create TACACS+ Server Entry on Cisco Optical Site Manager, on page 136

### 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:

- **Name**
- **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 2

### 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 **SELECTION** 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 TACACS+ server is reacheable** 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 138

### 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 **-** .

# Manage x509 Certificates

*Table 46: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Improved x509 Certificate Handling | Cisco IOS XR Release 24.1.1 | You can now upload an x509 certificate in the Personal Information Exchange (PFX) format, which improves the security of the connection between the Cisco Optical Site Manager and its server. PFX files can be password-protected, offering an extra layer of protection against potential attackers.<br>The options to automatically generate and upload certificates are available in the new **x509 Certificates** tab under the **Users & Access** menu. |

x509 certificates are used to establish a secure communication channel between a client and a server. In Cisco Optical Site Manager, you have the option to either automatically generate a self-signed x509 certificate or upload CA authorized certificate in digital or PFX format. This certificate is essential for building trust between the client and server, and it helps protect sensitive information from unauthorized parties. Additionally, x509 certificates provide the ability to detect any tampering or modification of data during transmission.

## Generate and Upload x509 Certificates

Use this task to automatically generate and apply a x509 certificate. You can also use this task to upload the certificate in digital (.cert) or PFX (.pfx) file formats.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### 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:

a) Click **Auto Generate and Apply Certificate** to generate and apply a self signed certificate automatically.

b) To upload a digital certificate, perform these steps:

1. Select *CERT + KEY* from the **Certificate Type** drop-down list.
2. Select the *.cert* or *.crt* file from the **Certificate File** field and click **Upload**.
3. Select the *.key* file from the **Key File** field and click **Upload**.
4. Click **Apply**.

c) To upload a Personal Information Exchange (PFX) certificate, perform these steps:

1. Select *PFX + PASSWORD* from the **Certificate Type** drop-down list.
2. Select the *.pfx* file from the **Certificate File** field and click **Upload**.
3. Type the password in the **Password** field if the input private key file is password protected.
4. Click **Apply**.

# View Active Login User Details

This chapter describes the procedures involved in monitoring active users and their login records.

## View Active Login Sessions

You can view the currently logged in users and their details, such as username, login time, interface name, and IP address. To view the list of currently logged in users, perform these steps:

### Before you begin

Log into Cisco Optical Site Manager, on page 2.

### 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.

## View User Login History

You can view the user login history and their details, such as login ID, username, last login and logout date, interface name, and IP address. To view the user login history, perform these steps:

### Before you begin

Log into Cisco Optical Site Manager, on page 2.

### 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 their details.

# Manage Web Configurations

## Configure Netconf and Nodal Craft Session Timeout

To configure timeout for Netconf and Nodal Craft sessions, follow these steps:

### Before you begin

Log into Cisco Optical Site Manager, on page 2.

### Procedure

**Step 1** Click **Users & Access** in the left panel.

**Step 2** Click the **General** tab.

**Step 3** To configure the Nodal Craft session timeout, perform these steps in the **Nodal Craft Session Timeout Configuration** section:

a) Select the time in minutes from the **Idle Session Timeout** drop-down.

This setting configures how long users are inactive before they are signed out of the Nodal Craft session.

b) Select the time in hours from the **Absolute Session Timeout** drop-down.

This setting configures the maximum amount of time a session can be active.

c) Click **Apply**.

**Step 4** To configure the Netconf session timeout, perform these steps in the **Netconf Session Timeout Configuration** section:

a) Select the time in minutes from the **Idle Session Timeout** drop-down.

This setting configures how long users are inactive before they are signed out of the Netconf session.

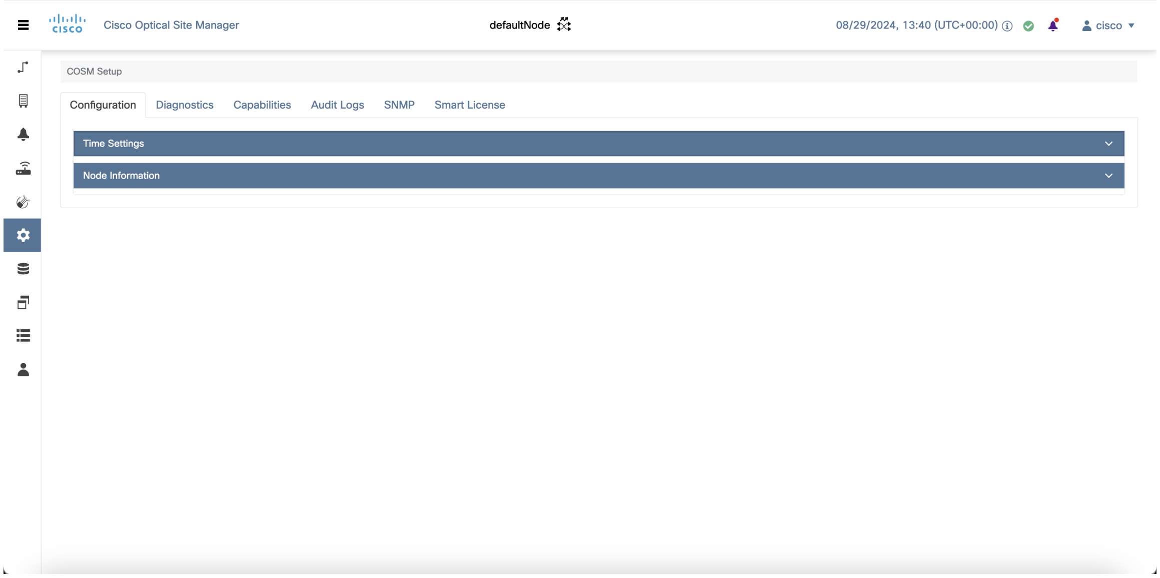
b) Click **Apply**.

CHAPTER 12

# Set up Cisco Optical Site Manager

This chapter covers the tasks for configuring the Cisco Optical Site Manager's timezone and node information. Additionally, you'll learn how to view diagnostic and audit logs, as well as configure smart licensing.

*Figure 24: Set up Cisco Optical Site Manager*



## Configure Timezone

Use this task to configure the time zone.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

**Step 2** Click the **Configuration** tab and then click **Time Settings** to expand it.

**Step 3** Type the name of the city or press space in the **Time Zone** field and select a time zone from the drop-down list.

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

A confirmation message appears.

**Step 5** Click **Yes**.

# View Cisco Optical Site Manager Diagnostics

Use this task to retrieve and download Cisco Optical Site Manager diagnostics information.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

**Step 2** Click the **Diagnostics** tab.

**Step 3** To retrieve Cisco Optical Site Manager diagnostic logs, perform these steps:

a) Select the check boxes for which you want to retrieve the logs.

**Note**
By default, all the check boxes are selected except **NCS Callback Log**.

*Table 47: Fields Description*

| Fields | Description |
|---|---|
| Alarms | Collects the active alarms |
| Audit Logs | Collects NSO audit logs |
| Conditions | Collects the active conditions |
| Admin Logs | Collects the Admin logs |

| Fields | Description |
|---|---|
| Engineer Logs | Collects all the system software logs |
| 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 entire NSO data tree |

b) Click **Retrieve** to retrieve the diagnostics report.

A confirmation message appears.

c) Click **Yes**.

d) Click **Download** to download the diagnostics report.

A zip file containing the logs is downloaded.

# View Audit Logs

Use this task to retrieve and download Cisco Optical Site Manager audit logs.

### Before you begin

Log into Cisco Optical Site Manager, on page 2

### Procedure

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

**Step 2** Click the **Audit Logs** tab.

**Step 3** Select the search criteria from the **Search filters** section and click **Search**.

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 48: 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. |

This chapter provide information about Smart Licensing (SL) solutions and their deployment on Cisco Optical Site Manager.

Smart Software Licensing is a solution for managing software across the Cisco portfolio and your organization. It provides complete visibility into your software usage and gives you full control over your licensing status.

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

## Efficient Cloud-Based Software Licensing with Smart Licensing

Smart Licensing (SL) is a cloud-based, flexible software licensing model that allows you to activate and manage Cisco software licenses across your organization. This solution enables you to easily track the status of your licenses and software usage trends. Smart Licensing allows pooling of licenses or entitlements that you can use across the entire organization in a flexible and automated manner.

## Benefits of Smart Licensing

These are the key benefits of Smart Licensing.

- **Easy activation**: establishes a pool of software licenses that can be used across your company.
- **Unified management**: provides a complete view into all of your products and services in an user-friendly portal.
- **License flexibility**: enables you to transfer licenses as needed easily, because the software is not restricted to a specific hardware.

## Key Features of Smart Licensing

These are the key features of Smart Licensing:

- **Direct and proxy registration**: registers your device directly with the Cisco Smart Software Manager (CSSM) portal or through a proxy for restricted internet access environments.

- **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.

# Deploying Smart Licenses

Smart Licensing solution makes it easier for you to procure, deploy, and manage your license. Cisco Smart Software Manager (CSSM) is your primary licensing server and portal where you can create your smart accounts and manage licenses.

Smart Software Manager On-Prem is your locally installed on-premises user portal that work with CSSM.

### License consumption

Each NCS 1010 consumes one license.

For NCS 2000, NCS 1014, NCS 1004, and NCS 1001 the license count is based 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.

# Smart Licensing Workflow

These are the stages for deploying Smart Licenses:

### Procedure

**Step 1** Order licenses

a) Order your license from Cisco Commerce Workspace (CCW).
b) Access CSSM and create the smart account and virtual accounts to organize your licenses.

**Step 2** Activate licenses.

a) Select the deployment methods.

- Direct Deployments: Direct Cloud Access (CSSM)
- On-Premises Deployments: Locally installed servers on your premises
- Offline Deployments: No connectivity to CSSM

b) Configure the smart license transport mode and register the device with CSSM.

**Step 3** Manage licenses.

a) Generate your report from the device. Synchronize the report with CSSM either automatically or manually.

b) Monitor the license usage and compliance status through the CSSM portal.

# Smart Transport

Devices send usage information directly over the internet to the Cisco Smart Software Manager (CSSM).

## Configure Smart Transport method

**Before you begin**

- Create Token
- DNS Configuration

### Create a Token

Use this task to create a new token using Cisco Smart Software Manager.

**Procedure**

**Step 1** Log in to the Cisco Smart Software Manager.

https://software.cisco.com/software/csws/ws/platform/home#SmartLicensing-Inventory

**Step 2** Click the Inventory tab, and select your virtual account from the **Virtual Account** drop-down list.

The **Create Registration Token** pane appears.

**Step 3** Click the **General** tab, and click **New Token**.

**Step 4** Enter the token description. Specify the number of days the token must be active.

**Step 5** Check the **Allow export-controlled functionality on the products registered with this token** check box.

**Step 6** Click **Create Token**.

**Step 7** Copy the token and register Cisco Optical Site Manager with the same token ID.

An example of the token ID: YzY2ZjYyNjktY2NlOS00NTc4LWIxNTAtMjZkNmNiNzMxMTY1LTE2NjAzNjQ3
%0ANzY4Njl8ZVJSckxKN2pFV2tIeHVoMUkxbGxTazFDVm9kc1B5MGlHQmlFWUJi%0Ac3VNRT0%3D%0A

## Configure DNS to Access Cisco Optical Site Manager

Provide Domine Name System(DNS) must be configure, as Cisco Optical Site Manager will not be accessible from outside the network.

### Procedure

Use this sample configuration to connect to the Cisco Optical Site Manager from your network.

**Example:**

```
Config

admin server-information networking dns-configuration dns-server <ipaddress> of DNS

commit

exit
```

## Configure Smart Transport mode

Use this task to configure Smart Transport Licensing Mode.

### Procedure

**Step 1** Click **Cisco Optical Site Manager Setup** in the left pane, and then click **Smart License**.

**Step 2** Click the **Configuration** to expand it.

**Step 3** Under **Transport Settings**, select the **Transport Mode** as **Smart Transport** from the drop-down list.

Go to Smart Transport User Interface Field descriptions, on page 152 for field descriptions.

**Step 4** Add *https://smartreceiver.cisco.com/licservice/license* under **Smart Transport URL** field.

**Step 5** Under the **Proxy Setting**

a) Populate these fields.

1. HTTPS Proxy *(Optional)*
2. HTTP Proxy *(Optional)*
3. Username *(Optional)*
4. Password *(Optional)*

**Step 6** Under **Reports Settings**, add **Reporting Interval (days)**

**Step 7** Check the **Send Hostname** check box to receive the hostname information.

**Step 8** Check the **Send Product Version** check box to receive the product version.

**Step 9** Click **Apply** to apply the settings.

**Step 10** Click **Check Connection** to check the connection with the new settings.

If the **Check Connection** button turns **Green**, it indicates that the connection is good.

If the **Check Connection** button turns **Yellow**, it indicates that there is an issue with the connection.

## Smart Transport User Interface Field descriptions

*Table 49: CSLU UI field descriptions*

| Field name | Field descriptions |
|---|---|
| Transport Mode | Specifies the mode of transport. |
| CSLU URL | Specifies the CSLU URL |
| HTTPS Proxy(Optional) | Specifies the HTTPS Proxy Address. |
| HTTP Proxy(Optional) | Specifies the HTTP Proxy Address. |
| Username(Optional) | Specifies the Username. |
| Password(Optional) | Specifies the Password |
| Reporting Interval (Days) | Specifies the reporting interval in days. |
| Hostname | Specifies the hostname that will be included in the report. |
| Product Version | Specifies the product version that will be included in the report. |

# Establish Trust for Smart Transport

Use this procedure to establish trust for smart transport.

### Procedure

**Step 1** Navigate to **Information Tab**, click **Establish Trust**.

The **Establish Trust** dialog box appears.

**Step 2** Copy the **Token** text from the **Virtual Account**, paste under the **ID Token** dialog box and click **Trust**.

**Step 3** Configuration Verification

- Under **Trust** tab **Trust Established** time and **Last Attempt Result** as **Success** displays, indicating that the **Trust Established.**

- Click **Sync**, under **Reporting** it displays **Last Report Pushed** time and **Last Acknowledgment Received** time indicating synchronization is done.
- Under **License Usage**, license count displays.

# Cisco Smart License Utility

Cisco Smart License Utility (CSLU) is a application that enables customers to administer licenses and their associated Product Instances from their premises instead of having to directly connect their Smart Licensed enabled Product Instances to Cisco Smart Software Manager (CSSM).

## Configure CSLU

### Before you begin

1. Install CSLU Application on Windows or Linux System.

## Configure CSLU Licensing Mode

Use this task to configure CSLU licensing mode.

### Procedure

**Step 1** Click **Settings** in the left panel, and then click **Smart License**.

**Step 2** Click the **Configuration** to expand it.

**Step 3** Under **Transport Settings**, select the **CSLU/OnPrem** from the drop-down list.

Go to CSLU User Interface Field descriptions, on page 154 for field descriptions.

**Step 4** Under the **CSLU URL** enter *http://<Device IP>:8182/cslu/v1/pi* under.

*Device IP* is the Ethernet2 IP address of the computer in which the CSLU application is installed.

**Step 5** Under **Proxy Setting**

a) Perform these steps as needed.

   1. HTTPS Proxy *(Optional)*
   2. HTTP Proxy *(Optional)*
   3. Username *(Optional)*
   4. Password *(Optional)*

**Step 6** Under **Reports Settings**, add **Reporting Interval (Days)**

a) Enter *<1–30>*

**Step 7** Check the check box **Send Hostname** to receive the hostname information.

**Step 8** Check the check box **Send Product Version** to receive the product version.

**Step 9** Click **Apply** to apply the settings.

**Step 10** Click **Check Connection** to check the connection with the new settings.

If the **Check Connection** button turns **Green**, it indicates that the connection good.

If the **Check Connection** button turns **Yellow**, it indicates that there is an issue with the connection.

### CSLU User Interface Field descriptions

*Table 50: CSLU UI field descriptions*

| Field name | Field descriptions |
|---|---|
| Transport Mode | Specifies the mode of transport. |
| CSLU URL | Specifies the CSLU URL |
| HTTPS Proxy(Optional) | Specifies the HTTPS Proxy Address. |
| HTTP Proxy(Optional) | Specifies the HTTP Proxy Address. |
| Username(Optional) | Specifies the Username. |
| Password(Optional) | Specifies the Password |
| Reporting Interval (Days) | Specifies the reporting interval in days. |
| Hostname | Specifies the hostname that will be included in the report. |
| Product Version | Specifies the product version that will be included in the report. |

## Establish Trust for CSLU

Establishing trust enables you to access and view license usage data.

1. In the Cisco Optical Site Manager application, click the **Sync** button.
2. CSLU displays **COMPLETE: Sync response acknowledgement to product instance** when the **Sync** is complete from the CSLU.

### Configuration Verification

Verify the configuration to check trust is established.

### Procedure

**Step 1** Under **Trust** tab **Trust Established**  time and **Last Attempt Result** as **Success** displays, indicating that the **Trust Established.**

**Step 2** When **Sync** is done, under **Reporting** it displays **Last Report Pushed** time and **Last Acknowledgement Received** time indicating synchronization is done.

**Step 3** Under **License Usage**, license count displays indicating trust is established.

# Offline

Offline mode allows you to manage your devices on premises without connecting to CSSM. You can set up your devices without internet access, and they do not require communication with Cisco, making it suitable for highly secure environments.

The offline mode involves a manual exchange of files between Cisco Optical Site Manager (COSM) and Cisco Smart Software Manager (CSSM) to establish trust and report license usage. The workflow is the same for both trust establishment and usage reporting.

### Offline Trust Establishment Workflow

1. Download Request File from COSM.
2. Import and Process File in CSSM.
3. Download Acknowledgement File from CSSM.
4. Import Acknowledgement File into COSM.

**Note** If you perform a usage report before establishing trust, the usage-file.xml generated by COSM automatically includes a trust request. This allows you to establish trust and report usage in a single operation.

## Configure Offline

Use this task to configure offline licensing mode.

### Procedure

**Step 1** Click **Settings** in the left panel, and then click **Smart License**.

**Step 2** Click the **Configuration** tab to expand it.

**Step 3** Under **Transport Settings**, select **Offline** mode from**Transport Mode** drop-down list.

**Step 4** Check the **Send Hostname** check box to send the hostname information.

**Step 5** Check the **Send Product Version** check box to send the product version.

**Step 6** Click **Apply** to apply the settings.

**Check Connection** is disabled for **Offline** mode.

# Download Request File from COSM

Perform these steps to establish trust for Cisco Optical Site Manager offline licensing.

## Procedure

**Step 1** Click the **Information** tab to expand it.

**Step 2** Click the **Save** button and choose **Trust Request trust-request** XML file downloads

**Step 3** Establish Trust by performing these steps in sequential order.

a. Upload Usage Data to CSSM, on page 156

b. Download Acknowledgement from CSSM, on page 156

c. Import Acknowledgement in COSM, on page 157

# Upload Usage Data to CSSM

Perform these steps at CSSM.

## Procedure

**Step 1** Go to Cisco Smart Software Manager then go to **Reports** then click **Usage Data Files** then click **Upload Usage Data** and select the **Virtual Account** and click **Ok**.

**Step 2** **Upload Usage Data** window opens, click the **Browse** button and upload the **trust-request** file.

**Step 3** Check under the **Reporting Status** tab to see **No Errors**.

It may take a few minuets to show **No Errors**. If it shows **Errors**, you have to fix them.

# Download Acknowledgement from CSSM

Perform these steps at CSSM.

## Procedure

**Step 1** In the CSSM, under **Usage Data Files** click **Upload Usage Data**.

**Step 2** It opens a **Upload Usage Data** window, click **Browse** and select **rum-report-xxx** click **Open** then click **Upload Data** In the **Select Virtual Accounts** window, select the appropriate account and click **ok**.

It may take a few minuets to show **No Errors**. If it shows **Errors**, you have to fix them.

**Step 3** When **No Errors** appears, **Download** the **Ack_rum-report-xxx**.

**Step 4** In the Cisco Optical Site Manager click **Import** button, it opens **Establish Trust** click **Select files..** and select **Ack_rum-report-xxx** click **Open** then click **Done**.

## Import Acknowledgement in COSM

Perform these steps at Cisco Optical Site Manager.

### Procedure

**Step 1** Click **Download** under **Acknowledgment** tab.

**Step 2** In the Cisco Optical Site Manager click **Import** button, it opens a **Establish Trust** window.

**Step 3** Click **Select files...** and upload **Ack_trust-request-xxxx** click **Open** then click **Upload**.

**Step 4** Click **Save**, then **Usage**, it opens a **Select what to save** window, then choose any one option.

- unreported
- all
- days

**rum-report-xxx** downloads

**Step 5** Click the **Refresh** button to see updated information.

**Step 6** Configuration Verification

- Under the **Trust** tab, you will see a **Trust Established** time, indicating that the trust has been established.
- Under **Reporting** it displays **ACK Report Time** .
- Under **License Usage**, license count displays.