



# Use Cisco Optical Network Controller

---

Cisco Optical Network Controller offers different applications to manage and optimize your optical network. These applications provide a centralized interface for various tasks, such as visualizing network topology, provisioning circuits, monitoring performance, and troubleshooting issues. By leveraging these applications, you can gain greater visibility into your network, streamline operations, and ensure reliable service delivery.

1. Topology
2. Nodes
3. Alien Import
4. Inventory
5. Service Manager
6. Alarms
7. Workspaces
8. SWIMU
9. PM History
10. Logs
11. Monitoring
12. Links



---

**Note** Timezone configuration has been added in Release 25.1.2. Cisco Optical Network Controller webUI now displays time in the configured timezone. Change the timezone using the CLI. The timestamps in the UI differ between Releases 25.1.1 and 25.1.2. See [Update Timezone Configuration](#).

---

These steps describe how to use the common options across all these applications.

## Before you begin

[Log in to Cisco Optical Network Controller](#)

## Procedure

---

- Step 1** View the timestamp.
- The timestamp appears on the top right corner of the screen in all the screens. It follows the UTC time zone. The current date is displayed along with the time.
- Step 2** Click the **Refresh** button to refresh the status of the table content or topology in each of the application screens anytime.
- Step 3** Click the **Column Preferences** icon display, hide, or reorder columns on any application page:
- To display or hide a column from the table view, select or deselect the corresponding check box.
  - Use the drag handle next to the column name to move the column to a new position in the table.
  - Click **Reset** to revert the view to its default settings.
- Note**  
The position of the columns with a lock icon is fixed and cannot be changed. The preferences and changes remain saved until you reset them to default.
- Step 4** To resize the columns:
- Hover your cursor over the boundary line between two column headers until the resize cursor appears
  - Click and drag left or right to adjust the column width as needed.
- Step 5** Export the current table.
- Click **Export** to export the details of any table from any application screen to a spreadsheet file.
  - Choose table view and click **Export** to download the current table with the filters enabled as an excel spreadsheet.
- Note**  
When you export a table, the resulting spreadsheet contains all the columns of the table, not just the fields that you have selected from **Show or hide columns** dropdown.
- Step 6** Export all data relevant to the current application.
- Click **Export** to export the details of any table from any application screen to a spreadsheet file.
  - Choose **All items**.
- Note**  
This label changes based on the app you are using. For example, All Nodes in the Nodes app, All Services in Service Manager, and so on.
- Click **Generate** to initiate file generation.
- Step 7** Use the **Sort** option to sort the table values.
- Step 8** Use the **Filter** option to filter the table content as per requirement in each application screen.
- 

- [Topology, on page 3](#)
- [Nodes, on page 11](#)
- [Alien Import, on page 24](#)
- [Network Inventory, on page 25](#)
- [Service Manager, on page 26](#)
- [Alarms, on page 60](#)

- [Workspaces](#), on page 80
- [Software Image Management and Upgrade](#), on page 102
- [PM History](#), on page 119
- [Logs](#), on page 134
- [Monitoring](#), on page 144
- [Links](#), on page 144
- [General Troubleshooting](#), on page 151
- [Unmanaged Equipment Support](#), on page 151
- [PSM OMS Protection](#), on page 153
- [Forwarding Syslogs](#) , on page 168

## Topology

The **Topology** screen is an interactive screen which allows you to click on each node to fetch its information. The links between the nodes are the fiber links connecting each node. You can click on each fiber link to fetch its information when the OTS view is enabled. There can be multiple links connecting each node at any given point in time.

The Topology screen is responsible for maintaining and exposing the optical/OTN network topology for ONC, including:

- Network devices (sites, nodes, interfaces).
- Physical links (fiber spans, OMS/OTS/OTN links).
- Optical protection groups.
- OTDR configuration and SOR files.
- Span-loss metrics and integration with PM flows.

**Topology** displays the network along with the nodes and the associated network links on a map. You can toggle between the **Light** and **Dark** modes to view this screen. You can zoom in zoom out the entire screen to view the network and its components. You can select the **OTN**, **OMS** or **OTS** layers as options in the display.

### Layer segment buttons

The **OTS option** is used to show all fiber span between all type of nodes, OLT or ILA.

The **OMS option** is used to display only the ROADMs and the links between the ROADMs in the given network.

The **OTN option** is used to display the OTN links present between Transponders that support OTN, for example, NCS2K-400G-XP with card mode OTNXC.

### Map control icons

#### Last time refreshed

The **EDIT** icon allows you to dynamically move any node to any Geo location on the screen. You can click on the **RESET** or **SAVE** button to reset or save the network status that is being displayed in the Topology screen anytime. Use the **CENTER** icon to position the map in the center.

The disconnected nodes are displayed with a cross mark. To cross launch to other related pages use the options appearing when you right click from anywhere on the map. You can click on the **REFRESH** button to refresh the Topology screen with the current status anytime.

**Reload** icon: This icon reloads the topology screen with the current status anytime.

**Configurations** icon: This icon provides these toggle switches.

- **Mute Acknowledged Alarms:** Enable to mute the alarms.
- **Display Degree Descriptions:** Enable to display the first character of the degree description configured in COSM for every node degree. If the description is missing, the degree number will be shown. When you hover over the node, a pop up displays the full description of the degree. To add a degree description:

1. Right-click the required node and select **View in Nodal UI** to cross-launch COSM.  
COSM opens.
2. Select **Optical Setup > Optical Configurations > Optical Degrees**
3. Click **Edit**, change description and click **Apply**.

The degree description changes reflects in the topology view after a refresh.

For more information, see the *Configuration Guide for Cisco Optical Site Manager*.

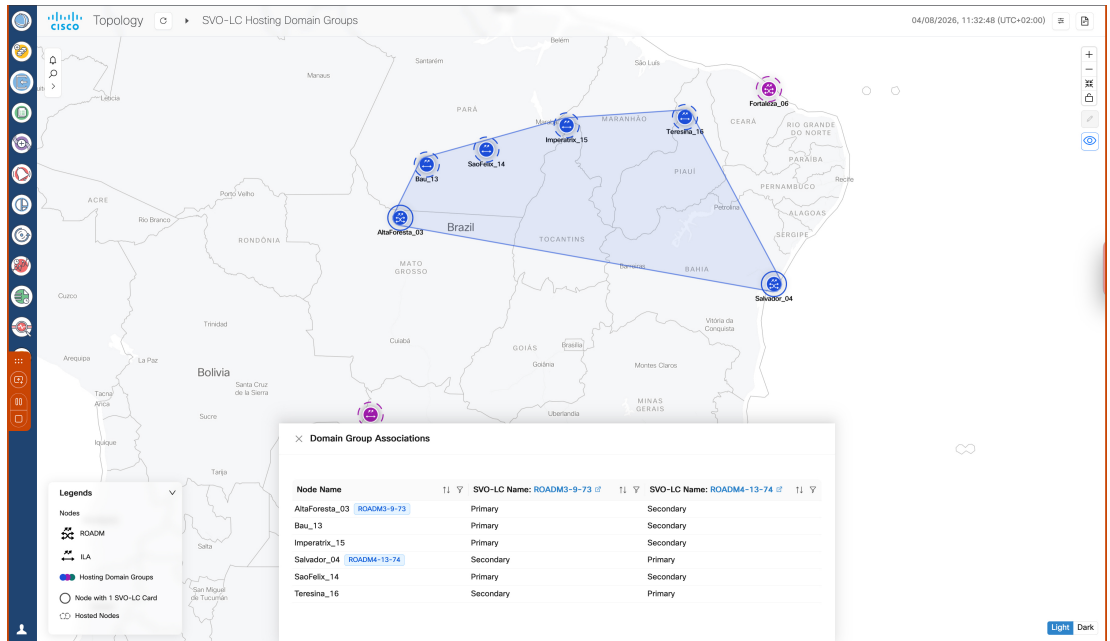
**Documentation** icon: Opens the Cisco Optical Network Controller configuration guide.

**Default view:** The topology view zooms on the world map to show all the nodes by default. If you have a specific set of nodes that you are interested in, zoom and pan the map to the view that you want, and click **Lock default view** button to make it your default view. The default view persists across reloads and logins on the same browser. The default view shows the world map if there are no nodes. The topology view across Cisco Optical Network Controller shows the default view.

**Eye icon:** From R26.1.1, the topology view includes an eye icon that allows you to choose an SVO hosting map and submarine links map. This icon provide these check boxes.

- **Show SVO-LC Hosting Domain Groups:** Displays the NCS 2000 nodes hosting SVO line cards. Click on the node to discover the domain groups associated to the same SVO line cards in HA. In the SVO domain groups view, the **Domain Group Associations** table appears displaying the **Node Name, SVO-LC Name**. In this map view, the **Legends** are updated with new icons such as circle (for nodes with one SVO line card) and pentagon (for nodes with more than one SVO line card).

Figure 1: Domain Group Associations



- **Filter Submarine Links:** Displays the submarine connections.

**Alarm severity bar**

On the top of this screen, there is an alarms bar for displaying the different alarm types and the count of each type of alarm that are part of the network. The **View Alarm** hyperlink opens the **Alarm** app. The alarm types are color coded based on the types of severity as seen in the table below.

Table 1: Alarm Severity

Alarm Type	Description
<b>RED</b>	Critical alarms are displayed in red color.
<b>ORANGE</b>	Major alarms are displayed in orange color.
<b>YELLOW</b>	Minor alarms are displayed in yellow color.



**Note** Alarm severity type for any warning will appear as **Warning** and for cleared alarms they severity is displayed as **Cleared**.

**Note**

- In the **Topology** screen, the alarms reported at the top left are related to only those nodes that have the Geo location defined. Due to this there can be a discrepancy between the alarms reported in the **Topology** and the **Alarms** screen related to these nodes.
- In the **Topology** screen only the critical, major and minor count alarms are reported, unlike the **Alarms** screen which reports the warnings or cleared alarms.

Use the **Search nodes by name** search bar to search for nodes in the topology network. This will fetch and locate the exact node in the map.

**Individual node pop-up options**

You can get the node name along with the COSM site name it belongs to and its current state by hovering over each node in the **Topology** map anytime.

1. Hover over a node and right click on it.  
The pop-up options appear.
2. Select of the options: **Resync**, **View in Node UI** and **View Alarms** options.

**Table 2: Topology Node Options**

Options	Description
<b>Resync</b>	Resync starts the resync of the selected node.
<b>View in Node UI</b>	This option takes you to the COSM site from where you can view the node details.
<b>View Alarms</b>	This option opens the <b>Alarms</b> application in a new tab, from where you can view all the alarms details.

You can also view the information related to the different nodes, links, and the states of each node in the network at any point in time by clicking the **Legends** option. To select any node in the network, use the drop-down box to select the node.

Figure 2: OTS view in Topology screen

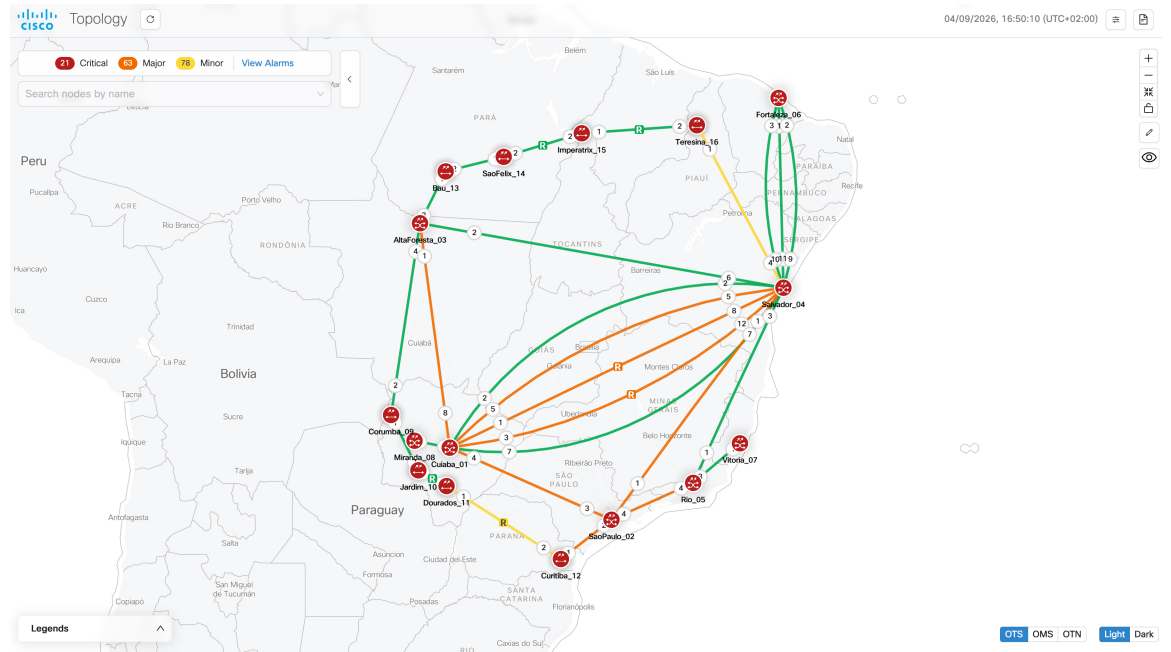
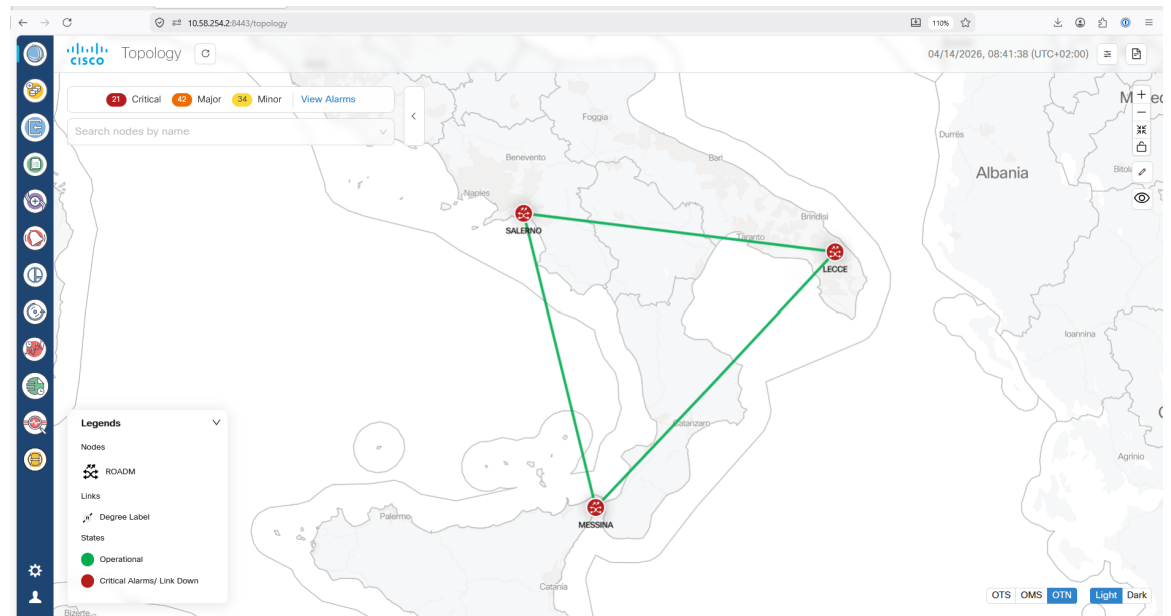


Figure 3: OTN view in Topology screen



**Note**

- The links between each node in the network in the **Topology** map displays the degree numbers which can be right clicked to navigate to the particular **Node UI**. The '**R**' in the link refers to Rama Amplified. This is not visible when you select the **OMS** layer option to view the map.

Click **Legends** in the bottom of the **Topology** screen to view the various representations used in the map as shown below.

- **Nodes**: The different nodes that are part of the network at any given time.
- **Links**: The different links between nodes along with the amplifier and degree labels.
- **States**: The different states like operational, critical alarms, link down and minor alarms.
- In the **Topology** map if two nodes have the same Geo location then they appear as a single node due to overlapping with each other which is a constraint.
- If any node in the **Topology** screen does not have a Geo location specified, the button in the upper right corner which is used to enter the Geo location value displays an orange highlight or dot. This orange dot is used to represent that there is at least one node which does not have any Geo location specified. When you click this orange dot a pop-up menu appears displaying all such nodes that are lacking Geo locations. Click the **Edit** icon and then select any node to move it to any desired location on the map. This will add the Geo locations to the node. You can move the node and the **Topology** maps the Geo location automatically for these node based on the location.
- Once the Geo location is selected, Cisco ONC displays a message to indicate that the **Topology** has been updated and to view the updated changes you must refresh the page by clicking the **Refresh** or **Reload** button.

From Cisco Optical Network Controller 24.3.1 release onwards, fiber information and span loss details are added newly to the **Topology** live PM tool tip. When you click on the fiber span link in the map, you will see the following details appearing in the tool tip information:

- **Fiber Type**: The type of fiber link.
- **Length**: The length of the fiber link.
- **Source Min Expected Spanloss**: Source node's minimum expected span loss value.
- **Source Max Expected Spanloss**: Source node's maximum expected span loss value.
- **Destination Min Expected Spanloss**: Destination node's minimum expected span loss value.
- **Destination Max Expected Spanloss**: Destination node's maximum expected span loss value.
- **Span Loss**: Span loss table.

**Check span utilization summary for OTN links**

1. In the left panel, click the **Links** app.
2. Go to the **OTN** tab and click the required *OTN link*.

Figure 4: Links app

Link Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port	Tags	Description	Link Status	Span Utilization	Action
OTNXC1	SaoPaulo	5/8/11	1/8/11			ENABLED		View summary
OTNXC2	AltaForesta	1/8/12	5/8/11			ENABLED		View summary
OTNXC3	AltaForesta	5/8/12	5/8/12			ENABLED		View summary

- Click **View summary** to open *Span Utilization Summary* for the selected OTN link.

Figure 5: Span utilization summary in Topology screen

ODU Number	SALERNO	MESSINA	Bandwidth	Service Name
1-8				
1-9				
1-4				
1-5				
1-6				
1-7				
1-10				
2			100G	100ge_protect
1-2				
1-1			10G	10ge_unprotect
1-3				

ODU Utilization (%) 55%

In this summary, these parameters appear:

**Note**

- ODU Number
- Source endpoint
- Destination endpoint
- Bandwidth
- Service Name for all ODU connection present.

ODU Utilization (%) in percentage is also available with respect to total bandwidth available in OTN-link.

- (Optional) Click **Export** to export the ODU span utilization table in an Excel.

**Note**

On **Topology** tool tip information, it is possible to add a description and save.

Figure 6: Topology Live PM

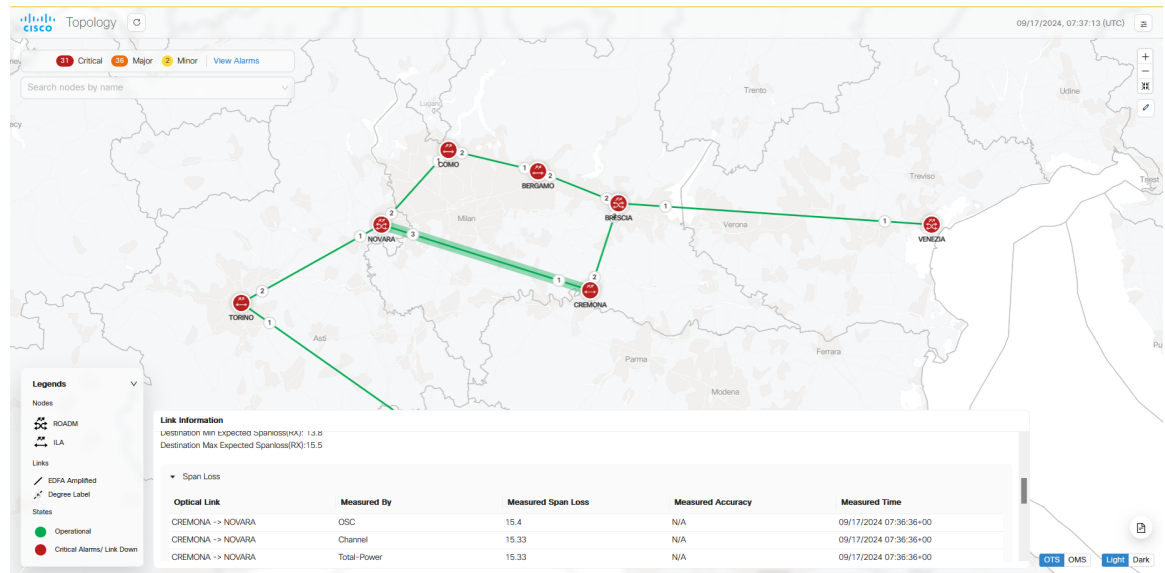
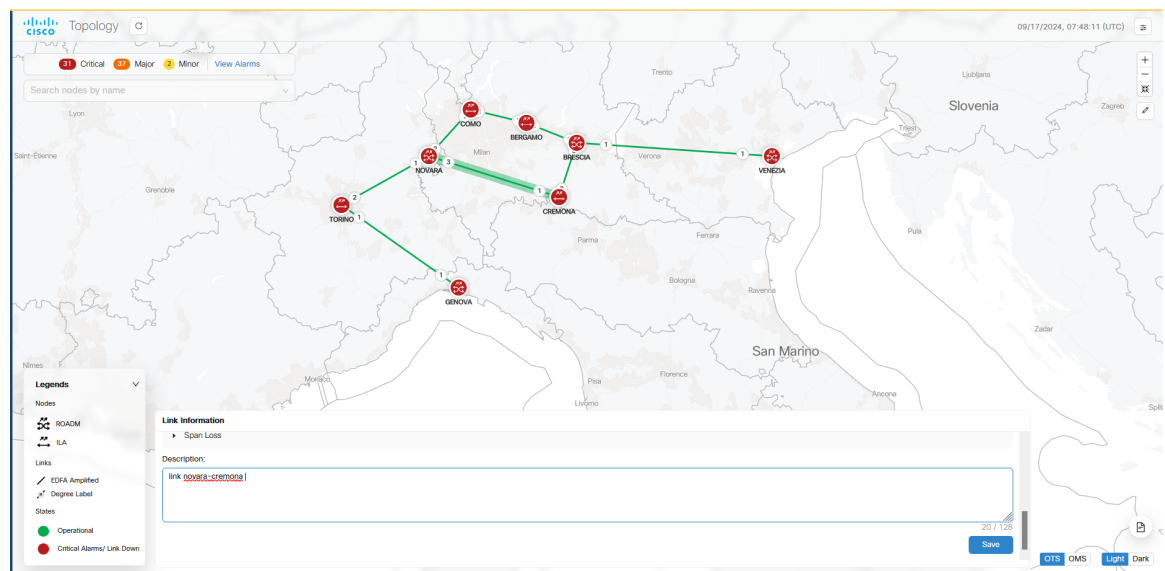


Figure 7: Tool Tip



## Troubleshooting in Topology

The most common problems encountered while using the **Topology** application is given below.

- **A pop-up message:** Asking to reload the page appears in the following scenarios.
  - New node onboarded or deleted
  - Geo locations changed

- In case the node, link or icons of the nodes are missing and not displayed in the **Topology** screen then refresh the page.

## Nodes

A node refers to a device in the network. You can add a single node or a set of nodes in the form of a batch at any given point in time.

Use the **Nodes** screen to view the details of each node. The **Nodes** table displays the following details for each node:

- **Node Name:** The name of the node. The node name provided by you must match the original node name used in Cisco Optical Site Manager. In case of any mismatch or discrepancy issues, user given name is configured on Cisco Optical Site Manager.
- **Product Type:** The type of product the node belongs to. For example: Cisco Optical Site Manager.
- **IP: Port (NETCONF):** The IP address of each node along with the port number.
- **Site Name:** The location of the site that each node belongs to. For example: ROADM\_Site\_Bengaluru\_33
- **Geo Location:** The Geo location of each node in terms of the latitude and longitude values based on where exactly the node is situated in the world at any given time.
- **Status:** The status of each node within the network to know whether it is active or disconnected.
- **Number of Hosting Servers:** Define the number of SVO Line Cards present in the COSM NCS 2000 node.
- **Primary Hosting Server:** Displays the active SVO line card hyperlink. Click the hyperlink to open the COSM admin plane for the hosting server.
- **Secondary Hosting Server:** Displays the standby SVO line card hyperlink. Click the hyperlink to open the COSM admin plane for the hosting server.
- **Up Time:** Displays the duration the COSM node is active.
- **Host Sync Error:** Displays the sync error details.

Hover over the information (i) icon that appears along with each node in this **Node Name** column to view these additional details of a node:

Figure 8: Additional details of a node

**14 Nod**

[+ New](#)

<input type="checkbox"/>	Name
<input type="checkbox"/>	Site_4 ● Connect
<input type="checkbox"/>	Site_5 ● Connect

**Site Description :**  
**Message :** Device is not reachable  
**Failure Reason :** Socket connectivity check failed with error - [connection timeout after 2s to 10.64.103.128:2022] and Ping failed with error - [no response from 10.64.103.128]  
**Created By :** admin  
**Created Date :** 03/26/2026, 14:31:06.870 (UTC+00:00)  
**Last Successful connection :** 04/08/2026, 20:50:16.675 (UTC+00:00)  
**Last Retried :** 04/09/2026, 15:10:25.292 (UTC+00:00)  
**Last Resync Reason :** Manual Resync  
**Last Resync Time :** 04/07/2026, 07:15:46.474 (UTC+00:00)

- **Site Description:** A brief description of the site associated with the node.
- **Message:** Displays information about any error conditions related to the node.
- **Failure Reason:** Indicates why the node cannot connect or is unreachable. This field is only visible when a node is in *Waiting\_for\_connection* state.

Here are example values for the field:

- *Socket connectivity check failed with error - [dial tcp 10.20.30.40:2020: connect: connection refused] but Ping succeeded*
- *Socket connectivity check failed with error - [connection timeout after 2s to 10.20.30.40:22] and Ping failed with error - [no response from 10.20.30.40]*
- *Socket connectivity check failed with error - [dial tcp 10.20.30.40:22: connect: no route to host] but Ping succeeded*
- **Created by:** Displays the user id that added the node.
- **Created Date:** Shows the date and time when the node was added.
- **Modified Date:** Shows the date and time when the node details were last updated.
- **Last Successful connection:** Shows the date and time when the node last connected successfully.
- **Last Retried:** Shows the date and time when the last connection attempt was made for this node. This field is only visible when a node is in *Waiting\_for\_connection* state.

- **Last Resync Reason:** Shows the reason for the most recent resync of the node.
- **Last Resync Time:** Shows the date and time when the most recent resync of the node occurred.

Figure 9: Nodes

Name	Product Type	IP	Site Name	Geo Location (latitude,longitude)	Status	Number of Hosting Servers	Primary Hosting Server
Node_1	Cisco Optical Node (COSM)	10.58.252.200:830	site_Node_1	47, 5	Active	0	MAIN
Node_2	Cisco Optical Node (COSM)	10.58.252.201:830	site_Node_2	47, 10	Active	0	MAIN
Node_3	Cisco Optical Node (COSM)	10.58.252.202:830	site_Node_3	45, 5	Active	0	MAIN
10.64.103.129	Cisco Optical Node	10.64.103.129:2022	Site45		Disconnected	0	
Node_5	Cisco Optical Node (COSM)	10.58.252.206:830	site_Node_5	47.5, 6	Active	0	MAIN
Node_6	Cisco Optical Node (COSM)	10.58.252.207:830	site_Node_6	47.25, 7	Active	0	MAIN
Node_7	Cisco Optical Node (COSM)	10.58.252.208:830	site_Node_7	48, 8	Active	0	MAIN
Node_8	Cisco Optical Node (COSM)	10.58.252.209:830	site_Node_8	47.5, 9	Active	0	MAIN
Node_9	Cisco Optical Node (COSM)	10.58.252.204:830	site_Node_9	47, 12	Active	0	MAIN

From release 26.1.1, the **Nodes** screen displays the last refreshed information for the primary hosting server. Hover over the **i** icon to get the latest refreshed information.

Figure 10: Last Refreshed information

Geo Location (latitude,longitude)	Status	Number of Hosting Servers	Primary Hosting Server	Secondary Hosting	Up Time	Host Sync Error
.87752, .17671	Active	0	10.64.103.75		4 days	
.39568, 28361	Active	0	10.64.103.204		4 days	
.74742, .02454	Active	0	10.64.103.206		4 days	

Tooltip for Primary Hosting Server IP: Last Refreshed: 04/15/2026, 04:46:19.361 (UTC+00:00)

Use the sort or filter options to sort and filter values in the table. You can also cross launch to Cisco Optical Site Manager using the links provided in this table.

Use the **Actions** button for synchronizing and configuring the network sync along with reconnecting the various nodes present in the network. These are the available options.

- **ReSync:** Used for resyncing any selected node in the network.
- **ReSync All:** Used for resyncing all the nodes in the network.
- **Reconnect:** Used to reconnect any or all the nodes.
- **Configure Network Sync:** Used for **Daily Network Full Sync**. Enable or Disable this functionality.

- **Test Connection:** Used for sending pings to the far end node.
- **Resync Host Details:** Used for resyncing NCS 2000 node with SVO line cards.

**Note**

- Latitude and longitude values can be set in both Cisco Optical Site Manager and Cisco Optical Network Controller. The following scenarios are possible:

- **Geo location is set in both Cisco Optical Site Manager and Cisco Optical Network Controller:** Cisco Optical Network Controller Geo location is used.
- **Geo location is set only in Cisco Optical Site Manager:** Cisco Optical Site Manager Geo location is used .
- **Geo location is set only in Cisco Optical Network Controller:** Cisco Optical Network Controller Geo location is used.
- **Geo location is not set in either Cisco Optical Network Controller or Cisco Optical Site Manager:** You will be prompted to add the node in **Topology** with the edit button.

For all the cases mentioned above, Cisco Optical Network Controller latitude and longitude value has a higher priority over the Cisco Optical Site Manager latitude and longitude values during the onboarding process. In case the Cisco Optical Network Controller latitude and longitude values are not provided, only then the Cisco Optical Site Manager latitude and longitude values are used.

- Even if the user updates the Geo location in Cisco Optical Network Controller, it does not get updated in the Cisco Optical Site Manager device.
- If the Geo location values that are coming from Cisco Optical Site Manager in a pre-filled format has more than four digits, then the length of the Geo location value is truncated to only four digits.
- Node names are synchronized between Cisco Optical Network Controller and the nodes it manages. During onboarding, node name provided in Cisco Optical Network Controller is pushed to the node if the node has a different name. Changes made on Cisco Optical Site Manager is reverted as Cisco Optical Network Controller pushes the original name to Cisco Optical Site Manager.

During a onboard and resync operation, Cisco Optical Network Controller pushes the current node name to the node, ensuring consistency even if changes were missed while the device was offline.

## Reserved internal IP addresses and subnets

Cisco Optical Network Controller uses specific IP addresses and subnets for its internal network. These ranges are reserved and must not overlap with the IP addresses assigned to any nodes.

Before adding nodes to the Cisco Optical Network Controller, ensure their IP addresses are planned accordingly and do not fall within any of the reserved internal IP ranges in this list.

- 10.241.x.x/24
- 10.242.x.x/24
- 10.243.x.0/24
- 10.91.0.0/16

- 10.92.0.0/16
- 10.93.0.0/16
- 172.16.0.1/32



---

**Note** Do not use the subnets configured for the control plane for any other purpose.

---

## Add nodes on Cisco Optical Network Controller

You can add a single node or a set of nodes in the form of a batch use the procedure given below.

Figure 11: Add New Node

## New Node

✕

**Node Name\***

**Port\***

**Node IP\***

**Protocol\***

NETCONF
▾

**Site Name\***

**Site Description**

---

**Credentials**

**Username\***

**Password\***

---

**Geo Location**

**Latitude**

**Longitude**

---

Test Connection

Cancel

Save

**Before you begin**

Verify these before adding to Cisco Optical Network Controller:

- Verify the Cisco Optical Site Manager is reachable from Cisco Optical Network Controller server via DCN.
- NETCONF port is enabled on the Cisco Optical Site Manager. .

- The COSM1K (NCS 1000 series) nodes must be added using port number 2022.
- All COSM2K (NCS 2000 series) nodes must be added using port number 830.
- You must add only fully configured nodes. All passives and patchcords must already be created before you add a node.

## Procedure

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

**Step 2** Click **New**.

**Step 3** In the **New Node** dialog box, enter the device details necessary connect to the device as given in the table below.

Ensure that you enter valid a username and password of the device to enable Cisco Optical Network Controller to connect to the device. For details about field descriptions, see the [Table 3: Add new node field descriptions, on page 17](#) table.

**Step 4** To test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node, perform these steps:

a) (Optional) Click **Test Connection** to test the connectivity to the node.

**Note**

The **Test Connection** button is enabled only if the **Node Name**, **Port** and **Node IP** fields are filled.

The **Test Connection** dialog opens for the selected node and shows the node name, node IP address, node port, connection status, and test duration..

b) Click **Try Again** if you want to rerun the connection test.

c) Click **Ping** if you want to verify node reachability from Cisco Optical Network Controller.

The ping result shows the reachability status and test duration for the selected Cisco Optical Site Manager node.

**Step 5** Click **Save**.

The new node or device is onboarded successfully and added to the **Nodes** table.

Cisco Optical Network Controller onboards the devices.

**Table 3: Add new node field descriptions**

Field	Description	Mandatory
<b>Name</b>	Name of the new node you are adding	Yes
<b>IP</b>	IP address of the new node which you are adding.	Yes
<b>Port</b>	The port number of the new node which you are adding.	Yes
<b>Protocol</b>	The protocol used for the new node which you are adding.	Yes

Field	Description	Mandatory
Site Name	The name of the site to which the new node belongs.	Yes
Username	The username for accessing the new node.	Yes
Password	The password for accessing the new node.	Yes
Site Description	The description of the site to which the new node belongs.	No
Latitude	The Latitude co-ordinate value that you want to assign for the new node to set its location.	No
Longitude	The Longitude co-ordinate value that you want to assign for the new node to set its location.	No

## Import multiple nodes into Cisco Optical Network Controller

Use this task to import multiple nodes into Cisco Optical Network Controller from a spreadsheet.

Use this task to import multiple nodes into Cisco Optical Network Controller by using a spreadsheet. The bulk import option enables you to add multiple nodes at the same time instead of adding them individually.

Cisco Optical Network Controller onboards nodes in batches:

- XS profile: 2 nodes at a time
- S and M profiles: 3 nodes at a time

### Before you begin

Follow these steps to import multiple nodes from any spreadsheet into Cisco Optical Network Controller.

### Procedure

- 
- Step 1** Click **Nodes** in the left panel.
  - Step 2** Click **Import nodes** to import the nodes in bulk.
  - Step 3** Click **Download** to download the node bulk import file template.
  - Step 4** For each node you want to import, enter its information in the appropriate columns in the downloaded Excel sheet.
  - Step 5** In the **Import xlsx** dialog box, select the Excel sheet.

Figure 12: Import nodes

	A	B	C	D	E	F	G	H	I	J	K
1	Node Name	Node IP	User Name	Password	Connectivity Type	Connectivity Port	Site Name	Site Description	Product Type	Latitude	Longitude
2	sampleDevice_1	10.00.00.99			NETCONF	2022	sampleSite_1	sample site description test	Cisco Optical Node		
3											
4											
5											
6											
7											
8											
9											

The sample bulk import template file includes these fields that you must fill out before importing the Excel sheet:

Table 4: Bulk Import File Template

Name	Description
<b>Node Name</b>	Name of the host node.
<b>Node IP</b>	The IP address of the node you are adding. <b>Note</b> Ensure that this IP does not overlap the <a href="#">Reserved internal IP addresses and subnets</a> .
<b>User Name</b>	The username for accessing the new node.
<b>Password</b>	The password for accessing the new node.
<b>Connectivity Type</b>	The type of the protocol used for connecting the node. Default: NETCONF
<b>Connectivity Port</b>	The port number of the node. Port number 2022 for NCS 1000 series nodes. Port number 830 for NCS 2000 series nodes.
<b>Site Name</b>	The name of the site to which the new node belongs.

Name	Description
Site Description	The description of the site to which the new node belongs.
Product Type	Set it as <i>Cisco Optical Node</i> .
Latitude	Specify the latitude co-ordinate value you want to assign to the new node to set its location.
Longitude	Specify the longitude co-ordinate value you want to assign for the new node to set its location.

After you upload the file, Cisco Optical Network Controller validates the entries and displays the message *Import in progress* while the nodes are being onboarded.

---

The new nodes are onboarded and added to the Nodes table. Wait until all nodes have completed onboarding.

#### What to do next

On the **Nodes** page, verify the total node count displayed at the top and match it with the number of nodes listed in the Excel file to ensure onboarding is complete.

## Export Nodes on Cisco Optical Network Controller

#### Before you begin

For exporting the node details from the table use the procedure given below.

#### Procedure

---

- Step 1** Click **Nodes** in the left panel.
- Step 2** Click **Export** to export the details to a spreadsheet file.
- 

## Edit Nodes on Cisco Optical Network Controller

#### Before you begin

Use the **Edit** option for editing the node details, use the procedure given below.

#### Procedure

---

- Step 1** Click **Nodes** in the left panel.
- Step 2** Click **EDIT** after selecting the node from the table.

In the edit mode the Cisco Optical Site Manager (COSM) geo location latitude and longitude values appear as separate values which can also be modified as required. Once the onboarding of the node or device is complete you can edit any selected node and modify its credentials using the **EDIT** option.

## Delete nodes on Cisco Optical Network Controller

Use this task to delete one or more nodes from Cisco Optical Network Controller.

Cisco Optical Network Controller supports node deletion even if OXC circuits. This operation does not affect traffic and you can add the same node back later.

When a node is deleted, Cisco Optical Network Controller takes these actions for the delete node.

- All alarms for the deleted node are removed from the **Current Alarms** tab and retained in the **History Alarms** tab.
- Audit logs for the deleted node are retained
- PM history for the deleted node is removed.

This table describes circuit behavior when a node is deleted:

**Table 5: Service behavior after node deletion**

Circuit type	When the deleted node is...	Service behavior in Service Manager app
CPCE	A node through which the service passes.	Service is deleted.
	The terminal node of the service.	Service is deleted.
	A combination of terminal node and a node through which the service passes.	Service is deleted.
GMPLS	A destination node or/and a node through which the service passes.	Service is not deleted and moves to the <b>PARTIAL</b> state.  <b>Note</b> For the TAPI notification northbound interface, the service is marked as <b>PENDING REMOVAL</b> when the service is in the <b>PARTIAL</b> state.
	The source node of the service.	Service is deleted.
	All nodes in the service.	Service is deleted.

Follow these steps to delete nodes on Cisco Optical Network Controller.

### Procedure

- Step 1** Click **Nodes** in the left panel.
- Step 2** Select the node or nodes that you want to delete.

**Step 3** Click **Delete**.

The selected node is deleted from the table.

**Note**

- Wait at least 2 minutes after device discovery completes before you delete the device.
- Node deletion is not allowed when the node status is *Resync In-Progress*, regardless of whether the node has any services. In this case you will receive an error message for the **Node Deletion Failure** when the circuit is spanning through the node.
- When an OXC is deleted from Cisco Optical Site Manager or the XR CLI, the **Lifecycle State** in the **Service Manager** application of the service connected to the OXC changes from **INSTALLED** to **PARTIAL**.

A warning message is displayed.

**Step 4** Review the impacted services as described in the warning message.

**Step 5** In the **Delete Node** dialog box and click **Delete**.

---

The selected nodes are deleted from Cisco Optical Network Controller.

## Troubleshooting in Nodes

The most common problems encountered while adding new nodes are given below.

- **Bulk import failure**

In this case you will get a text file describing the specific issues in the template.




---

**Note** Cisco ONC does not allow deletion of a node which involved in the collection or resync process, or while it is a part of any circuit path

---

- **Nodes possible status**

Node Status	Description	User Action
In Progress	Cisco ONC is collecting information about the onboarded device.	No action is needed, wait for the status to change.
Resync Pending	Cisco ONC has gone out of sync with device and is scheduled for a resync.	Either wait for scheduled resync or start the resync manually.
Resync In-progress	Cisco ONC is re-collecting information about the onboarded devices.	No action is needed, wait for the status to change.
Disconnected	Cisco ONC was unable to establish a session with COSM.	Attempt re-connect or resync. If the problem still persists contact Cisco TAC.

<u>Active</u>	<p>All information has been collected from the device and it is ready for operations.</p> <p><b>Note</b> It is recommended to wait for 60 secs once the device is turned to Active state which ensures the device is ready for accepting requests.</p>	
---------------	--	--

• **Nodes connection status**

Connection State	Description	User Action
Connected	Cisco ONC has successfully established the session with the COSM device provided user/password information.	No action is needed.
Disconnected	Cisco ONC was unable to establish session with COSM.	Attempt re-connect or resync. If the problem still persists contact Cisco TAC.
Waiting for connection	Cisco ONC is attempting to establish connection with COSM.	No action is needed.
Resync_needed	Cisco ONC has gone out of sync with device and is scheduled for a resync.	Either wait for scheduled resync or start the resync manually.
Resync Failed	Cisco ONC was unable to resync after multiple retries.	Attempt Resync. If problem still persists contact Cisco TAC.
Discovery Failed	Cisco ONC was not able to collect information from the device as it might have timed out or failed.	Attempt Resync. If problem still persists contact Cisco TAC.
Errored	Cisco ONC was not able to collect information from the device even after 3 retries.	Attempt Resync. If problem still persists contact Cisco TAC.

• **De-boarding of a node fails**

- Ensure no circuit is created involving this node.
- Retry deleting the node after sometime.
- In case the deletion fails even after you have retried it multiple times, contact Cisco TAC for further assistance.

## Test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node

Validate reachability and NETCONF port connectivity between Cisco Optical Network Controller to a Cisco Optical Site Manager node.

- Use **Test Connection** to verify NETCONF port connectivity.
- Use **Ping** to verify that the node is reachable from Cisco Optical Network Controller.

You can run these diagnostics while you add a node or after the node is onboarded.

### Before you begin

Follow these steps to test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node.

### Procedure

- 
- Step 1** Open the connectivity test for the node.
- To test connectivity during adding a new node, in the Node Node dialog box, click **Test Connection** after adding the node details.  
For detailed steps, see [Add nodes on Cisco Optical Network Controller, on page 15](#).
  - To test connectivity after onboarding, on the **Nodes** page, select the node, click **Actions**, and choose **Test Connection**.
- The **Test Connection** dialog opens for the selected node and shows the node name, node IP address, node port, connection status, and test duration.
- Step 2** Click **Try Again** if you want to rerun the connection test.
- Step 3** Click **Ping** if you want to verify node reachability from Cisco Optical Network Controller.  
The ping result shows the reachability status and test duration for the selected Cisco Optical Site Manager node.
- Step 4** Click **Try Again** if you want to rerun the connection test.
- 

## Alien Import

### Before you begin

To import and export the alien device data use the procedure given below.




---

**Note** For more details on how to model an alien wavelength or transceiver, etc through Cisco Optical Network Planner (CONP) see [CONP Manage Alien](#).

---

Figure 13: Alien Import

VID	PID	Data Rate	Baud Rate	FEC	Sub Mode	Modulation Format	Configuration Code
00B08E	NCS1K4-1.2T-K9	R5000	69.4351003125	SD_FEC_27	N/A	32QAM	1955
00B08E	NCS1K4-1.2T-K9	R6000	71.96	SD_FEC_27	N/A	64QAM	4177
00B08E	NCS1K4-1.2T-K9	R500	34.72	SD_FEC_27	N/A	BPSK	546
00B08E	NCS1K4-1.2T-K9	R500	34.46	SD_FEC_27	N/A	BPSK	536
00B08E	NCS1K4-1.2T-K9	R500	34.18	SD_FEC_27	N/A	BPSK	526
00B08E	NCS1K4-1.2T-K9	R500	33.92	SD_FEC_27	N/A	BPSK	516
00B08E	NCS1K4-1.2T-K9	R500	33.67	SD_FEC_27	N/A	BPSK	506
00B08E	NCS1K4-1.2T-K9	R500	33.41	SD_FEC_27	N/A	BPSK	496
00B08E	NCS1K4-1.2T-K9	R500	33.16	SD_FEC_27	N/A	BPSK	486
00B08E	NCS1K4-1.2T-K9	R500	32.92	SD_FEC_27	N/A	BPSK	476
00B08E	NCS1K4-1.2T-K9	R500	32.68	SD_FEC_27	N/A	BPSK	466
00B08E	NCS1K4-1.2T-K9	R500	32.44	SD_FEC_27	N/A	BPSK	456
00B08E	NCS1K4-1.2T-K9	R500	32.2	SD_FEC_27	N/A	BPSK	446
00B08E	NCS1K4-1.2T-K9	R500	31.97	SD_FEC_27	N/A	BPSK	436
00B08E	NCS1K4-1.2T-K9	R500	31.74	SD_FEC_27	N/A	BPSK	426
00B08E	NCS1K4-1.2T-K9	R500	31.52	SD_FEC_27	N/A	BPSK	416
00B08E	NCS1K4-1.2T-K9	R1000	69.44	SD_FEC_27	N/A	BPSK	1955
00B08E	NCS1K4-1.2T-K9	R1000	66.9	SD_FEC_27	N/A	BPSK	1934
00B08E	NCS1K4-1.2T-K9	R1000	68.37	SD_FEC_27	N/A	BPSK	1913
00B08E	NCS1K4-1.2T-K9	R1000	67.84	SD_FEC_27	N/A	BPSK	1892

## Procedure

**Step 1** Click the **Import** icon on the top of the table.

Cisco Optical Network Controller imports and displays the information of all the alien devices from the XML file. After successful import, the alien device information is available for applications that use the Cisco Optical Network Controller TAPI and REST API.

**Step 2** To export the alien device information in JSON or XML formats, click Export and choose the target format from the drop-down list.

### Note

The XML file which is imported in Cisco ONC is generated by CONP and can have some third-party restrictions on it.

**Step 3** Click the **Refresh** button to refresh the equipment status.

**Step 4** Click on the **Show or hide columns** icon to select any columns to be displayed or hidden from the table view anytime.

**Step 5** Use the page numbers and select the number of rows per page as required for the table display.

**Step 6** Use the sort or filter options to sort and filter values in the table.

# Network Inventory

## Before you begin

This task describes how to view inventory details on Cisco Optical Network Controller. To view or export the inventory details, follow the procedure given below.

Figure 14: Network Inventory

Network Inventory 03/18/2024, 15:37:12 (UTC)

8 Nodes Last Updated on 03/18/2024 at 15:36:50 Refresh Export

Name	Admin State	Equipment Type	Equipment State	Actual Equipment Type	Serial No	Product ID
torino92		ola				
Sheff 1	UNLOCKED	NCS1010-SA	UNLOCKED	NCS1010-SA	FCB2628B0VM	NCS1010-SA
COMMON CARDS						
Slot PM0	UNLOCKED	NCS1K-PSU	UNLOCKED	NCS1010-AC-PSU	APS263000XK	NCS1010-AC-PSU
Slot FT0	UNLOCKED	NCS1K-FAN	UNLOCKED	NCS1010-FAN	FCB2625B1G2	NCS1010-FAN
Slot FT1	UNLOCKED	NCS1K-FAN	UNLOCKED	NCS1010-FAN	FCB2625B1DJ	NCS1010-FAN
Slot PM1	UNLOCKED	NCS1K-PSU	UNLOCKED	NCS1010-AC-PSU	APS263001NQ	NCS1010-AC-PSU
SLOT CARDS						
Slot 0	UNLOCKED	NCS1K-ILA-C	UNLOCKED	NCS1K-ILA-C	FCB2650B0QQ	NCS1K-ILA-C
Slot RP0	UNLOCKED	NCS1K-CNTRL-K9	UNLOCKED	NCS1010-CNTRL-K9	FCB2631B037	NCS1010-CNTRL-K9
cremona83		ola				
bergamo80		ola				
genova94		roadm				

## Procedure

- Step 1** Click **Network Inventory** in the left panel.
- Cisco Optical Network Controller displays the Inventory tab. This tab displays all the inventory at the selected site.
- Step 2** Click the node that you want to view the details of.
- There is an option for selecting cascading windows for each node to view the Common Cards and the Slot Cards.
- Step 3** (Optional) To export inventory data into an excel file, click **Export**.
- Step 4** Click the **Refresh** button to refresh the inventory status.
- Step 5** Use the filter to search using **Custom Search** or **Quick Search** options.

### Note

**Custom Search:** Use this option to filter the search based on any particular field from the table. By selecting from the drop down list, the rows that are specific to the selected field appear in the search result. You can custom search using any of these options: **Admin State**, **Equipment Type**, **Software Revision**, **Equipment State**, **Actual Equipment Type**, **Serial No** or **Site Name**.

**Quick Search:** Use this option to search based on any value or field by typing it in the search box to fetch the related rows from the table.

## Service Manager

The Service Manager is an application within the Cisco Optical Network Controller that provides a centralized view and management of network services, particularly circuits. It enables users to visualize, provision, and monitor circuits, and perform actions such as editing and deleting them.

### Supported Circuit Types

- OCH-NC
- OCH-Trail
- OCH-CC

### GMPLS Support

- Supports OCH-CC with NCS1004 chassis with the following cards:
  - NCS1K4-1.2T-K9
  - NCS1K4-OTN-XP
  - NCS1K4-2-QDD-C-K9
  - NCS1K4-QXP-K9
- Support OCH-CC with NCS1014 chassis with the following cards:
  - NCS1K4-QXP-K9
  - NCS1K14-2.4T-X-K9
- Supports OCH-CC and OCH-TRAIL with the following NCS2K Transponder/Muxponder
  - NCS2K-400G-XP (with card mode: MXP)
  - 15454-M-10X10G-LC (with card mode: TXP-10G and MXP-10x10G)
  - NCS2K-200G-CK-C (with card mode TXP-100G and MXP-10x10G)
- Supports OCH-TRAIL with the following NCS2K Transponder/Muxponder
  - NCS2K-400G-XP (with card mode: OTN-XP)
- Supports OCH-NC with alien wavelength

### Existing CPCE circuits

Existing circuits are circuits that are already existing on devices. The configuration of these circuits is done either outside of Cisco Optical Network Controller, using Site Manager or CLI. It can be configured through a different instance of Cisco Optical Network Controller as well which manages the same network. The existing circuit's service names have the following format:

onc\_<SourceNode-Name>\_<Source-Port>\_<DestinationNode-Name>\_<Destination-Port>.

### Resync services

- You can select multiple services and use the resync option to resynchronize them.

Figure 15: Select multiple toggle

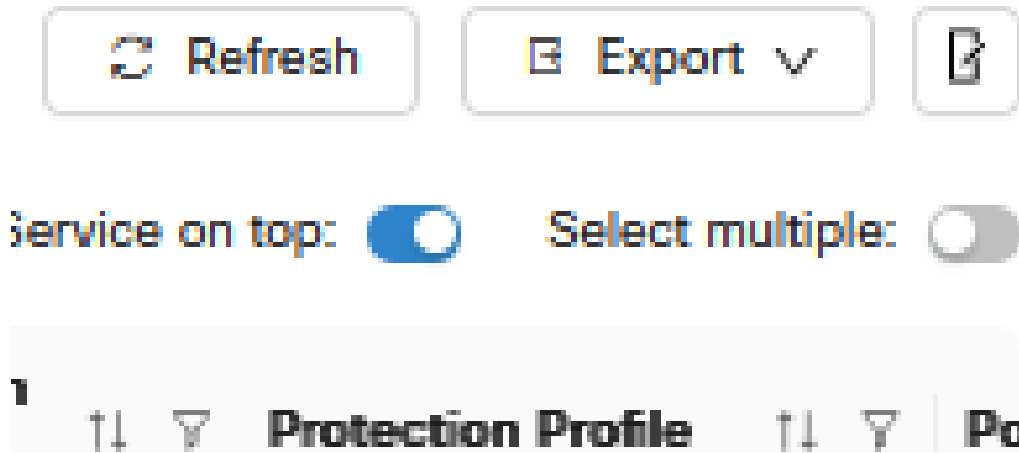
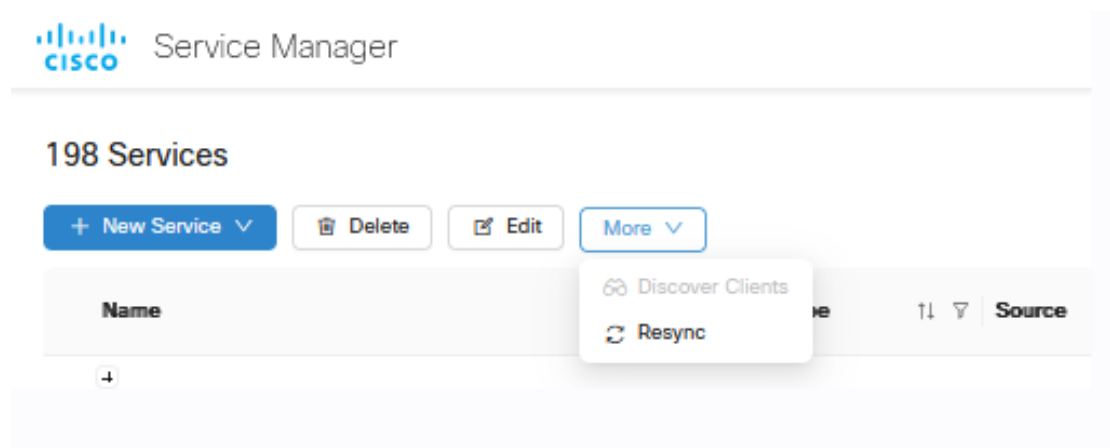


Figure 16: Resync option for GMPLS circuits

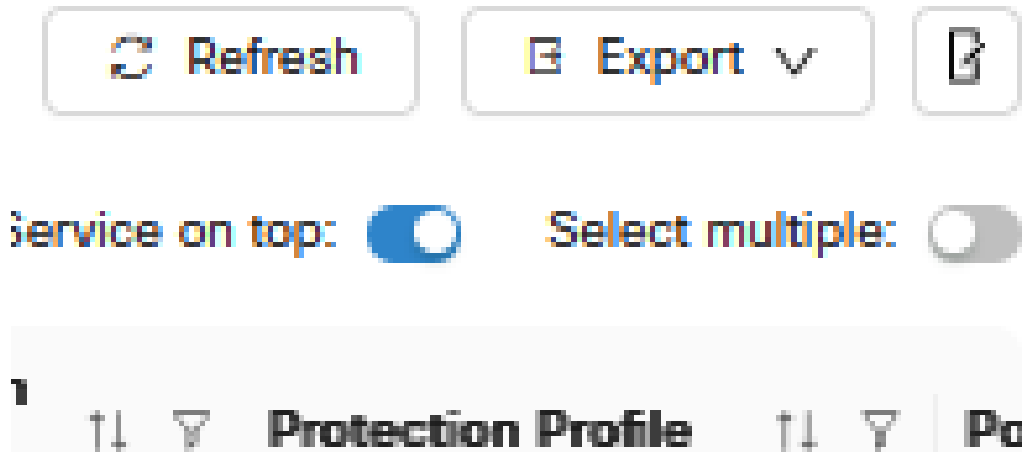


- Resyncing can resolve lifecycle state issues, for example, when the circuit is in PARTIAL, where clients are not discovered properly or are in an ambiguous state.
- When multiple services are selected, the **More** button is replaced with a **Resync** button.
- Resyncing a trail service also resyncs all its embedded OCH-CC services.

### Service Manager table view toggles

- Click **Service on top** toggle to toggle the Service on top mode on or off. When **Service on top** is enabled, the OCH-CC circuit is the main entry and its associated trail appears nested under it. When disabled, the trail becomes the main entry and the OCH-CC circuit is shown nested under it.
- Click **Select multiple** toggle to toggle multiple selection in the table on or off.

Figure 17: Service on top and Select multiple toggles



### Service summary

Click **i** next to the name of a service to view the Summary information for a circuit. This includes all the parameters set during circuit creation or edit.

Figure 18: Service summary in service manager

## Service Summary ✕

- 1
**General**

Service Name : ODU\_connection\_protected\_10GE  
 Protection Profile : PROTECTED  
 Payload Type : 10GE  
 Bandwidth : ODU2e  
 Service State : INSTALLED  
 Operational State : ENABLED  
 Admin State : UNLOCKED  
 Tags :  
 Description :
- 2
**Endpoints**

Source: site\_svo-sm2k-42 6/4/7-3  
 Destination: site\_svo-sm2k-36 6/2/7-3  
**Source protection values**  
 Source Revert Time : 5  
 Source Switch State : Released  
 Source Holdoff Timer : 0  
**Destination protection values**  
 Destination Revert Time : 5  
 Destination Switch State : Released  
 Destination Holdoff Timer : 0

**Service manager table fields**

Column	Values	Description
Name		Name of the service
Type	OCH-NC OCH-Trail OCH-CC	Type of the service

<b>Column</b>	<b>Values</b>	<b>Description</b>
Source	—	Source Node and Port
Destination	—	Destination Node and Port
Control Plane	GMPLS	Control Plane Protocol
	CPCE	

Column	Values	Description
Lifecycle State	INSTALLED	The circuit is fully provisioned and active in the network.
	PLANNED	The circuit configuration is defined but not yet provisioned on the network.
	PENDING_REMOVAL	The circuit is marked for deletion but the deletion process is not yet complete.
	DELETION_IN_PROGRESS	The circuit deletion process is in progress.
	DELETION_FAILED	The circuit deletion process failed to complete successfully.
	PARTIAL	The circuit is in a partially provisioned state, possibly due to missing or undiscovered components.
	GMPLS_ACTIVE	GMPLS circuit is successfully working, cross corrections are created, and path is available.
	GMPLS_INACTIVE	There is no valid path for creating the circuits due to frequency not available, inconsistent constraints, optical validation failure, etc.
	GMPLS_HANOVER	The circuit is configured to be upgraded from non-GMPLS to GMPLS or GMPLS to non-GMPLS.
	GMPLS_ACTIVATING	GMPLS circuit activation is in progress
	GMPLS_DEACTIVATING	GMPLS circuit deactivation is in progress.
	GMPLS_FAILED	GMPLS circuit failed (i.e. link down, node down).
	GMPLS_DEGRADED	Circuit trail failed (i.e. PSM working or protected is down or fail).
	GMPLS_RECOVERING	Temporary reboot status at circuit restart.
	GMPLS_REPAIRING	Circuit repair is in progress (i.e. node IP changed)
GMPLS_RELEASING	A downgrade from GMPLS to non-GMPLS circuit has been requested and the action is running.	
GMPLS_REPAIR_NEEDED	An IP address change is done on a node impacting the circuit, so the circuit must be repaired.  <b>Note</b> Cisco Optical Network Controller does not support circuit repair in release 25.1.1.	
GMPLS_SYNC_IN_PROGRESS	GMPLS controller has accepted the configuration, Cisco Optical Network Controller is getting the updated data from the GMPLS controller. When a circuit is discovered in a node that is onboarded to CONC, the Lifecycle state continues in this state until CONC fetches the circuit information from the GMPLS controller.	
Operational State	ENABLED	The circuit is active and functioning normally.
	DISABLED	The circuit is inactive and not functioning.

Column	Values	Description
Admin State	UNLOCKED	The circuit is administratively enabled and available for use.
	LOCKED	The circuit is administratively disabled and unavailable for use.
Frequency (THz)		Optical carrier frequency at which the circuit will operate within the DWDM spectrum.
Bandwidth (GHz)		Bandwidth used by the circuit
Protection profile	PROTECTED	OTN service has both active and standby path.
	UNPROTECTED	For OTN service, only active path is present. For PSM circuit, the circuit is configured with PSM OMS protection.
	OCH-PSM	The circuit is configured with PSM wavelength protection to ensure service availability in case of failure.
Port Rate	10GE	Data rate
	40GE	
	100GE	
	400GE	
	OTU2	
	OTU2E	
	OTU4	
	OC192/ STM-64	
	FC16	
	FC32	
Discovery Date	—	Service discovery date

Column	Values	Description
Restoration Type	None	No restoration is configured for the circuit.
	Enabled	Restoration is enabled for the circuit, and the network will automatically attempt to restore the circuit upon failure by calculating restoration path based on restoration constraints.
	Restorable Alternate	Restoration is enabled for the circuit, and the network will automatically attempt to restore the circuit upon failure by calculating restoration path based on restoration constraints and main path constraints alternatively.
	Enabled and Revertive(Automatic)	Restoration is enabled, and the circuit will automatically revert to the original (home) path after the failure is resolved and unverified alarms are manually cleared from COSM.
	Enabled and Revertive(Manual)	Restoration is enabled, and manual intervention is required to revert the circuit to the original (home) path after the failure is resolved.
Tags	—	Tags attached to the Service during circuit provisioning.

## Create and manage circuits

Consider these conditions when creating OCH-CC circuits.

- The OCH-Trail must be in installed state before an OCH-CC circuit can be created.
- When the corresponding trail is in planned state, no new OCH-CC circuits can be created.
- The number of OCH-CC circuits that you can have per trail depends on the card mode configuration of the transponder card.
- OCH-CC circuits inherit constraints from the parent trail.
- Creating an OCH-CC circuit creates the associated OCH-Trail circuit automatically.

Follow these steps to create circuits in Cisco Optical Network Controller.

### Before you begin

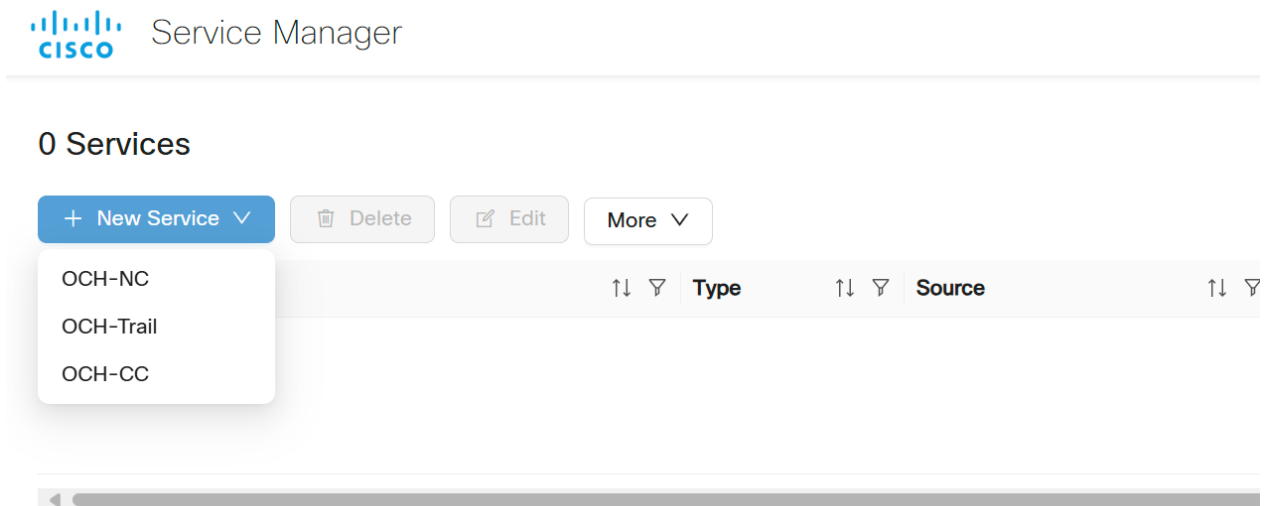


#### Note

- After changing the card mode for NCS1K4-1.2T-K9, resync the nodes from the Nodes page to ensure that the client ports are correctly displayed.
- If you do not see the ports on your target nodes during endpoint selection, we recommend you perform a resync of the nodes before creating a new service.
- If a new NCS 2000 chassis with a TXP present is added to a node already present in COSM, you must perform a resync of the node to see the endpoints during circuit provisioning.

## Procedure

**Step 1** Click **New Service** and choose **OCH-NC**, **OCH-Trail**, or **OCH-CC**.



**Step 2** Select **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

### Note

- **OCH-NC**: An OCH-NC is a circuit established between add/drop ports on terminal OLTs (Optical Line Terminals) or ROADMs (Reconfigurable Optical Add-Drop Multiplexers). This type of circuit typically connects end-user equipment to the optical network.
- **OCH-Trail**: An OCH-Trail is a circuit established between trunk ports of transponders or muxponders. This type of circuit typically transports aggregated traffic across the optical core network.
- **OCH-CC**: An OCHCC circuit is an optical service type that extends the OCH-NC to create an optical connection from the source client port to the destination client port of the transponder or muxponder cards. It also represents the actual end-to-end client service passing through the DWDM system, and enables seamless client traffic transmission across the optical network.

Figure 19: Service Manager

The screenshot displays the Cisco Service Manager web interface. At the top, the title is "Service Manager" with the Cisco logo on the left and the timestamp "04/17/2025, 10:48:56 (UTC)" on the right. Below the title, the breadcrumb trail reads "Services / New OCH-CC service". A progress indicator shows five steps: 1. General (active), 2. Endpoints, 3. Constraints, 4. Optical Interface, and 5. Summary.

The "General" tab contains the following fields:

- Name:** A text input field with a character count of "0 / 64".
- Control Plane:** A dropdown menu currently showing "CPCE". A dropdown menu is open, listing:
  - Centralized
  - CPCE** (highlighted)
  - Distributed
  - GMPLS Channel Mode: Dwdm
  - GMPLS Channel Mode: Flex
- Admin State:** A text input field.
- Tags:** A text input field with a help icon.

On the right side, there is a map of Europe with a search bar "Search nodes by name". The map shows a network topology with nodes labeled Node\_1 through Node\_11, connected by green lines. The nodes are distributed across various cities: Node\_1 (Lyon), Node\_2 (Turin), Node\_3 (Lyon), Node\_4 (Turin), Node\_5 (Strasbourg), Node\_6 (Strasbourg), Node\_7 (Stuttgart), Node\_8 (Stuttgart), Node\_9 (Munich), Node\_10 (Venice), and Node\_11 (Geneva).

**Step 3**

Service Manager launches the new service wizard.

Enter the details in the General tab and click **Next**.

Figure 20: Service Manager

The screenshot shows the 'Service Manager' interface for creating a 'New OCH-CC service'. The 'General' tab is active, showing the following configuration:

- Name:** test\_cpce (9 / 64 characters)
- Control Plane:** CPCE (dropdown menu)
- Admin State:** Enabled (radio buttons)
- Tags:** test\_cpce (9 / 15 characters, with a plus sign to add more)

At the bottom of the form, there are three buttons: 'Cancel', 'Back', and 'Next'.

Table 6: General Parameters

Field	Description	Values/restrictions
Name	The unique user defined name of the link.	(Allowed characters are a-z, A-Z, 0-9 and _ . <Space not allowed>).

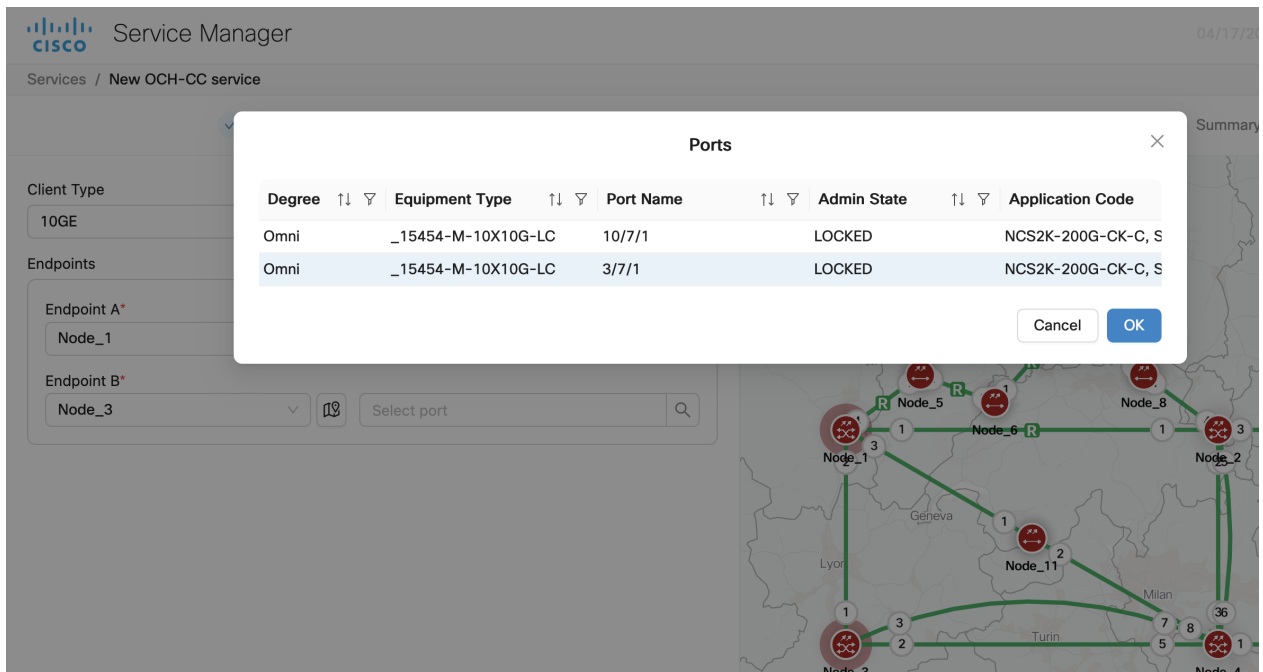
Field	Description	Values/restrictions
Control Plane	CPCE	—
Admin State	—	only ENABLED is supported
Tags	Tags can be attached to the Service for better management, to group them together	—

**Note**

Click + after entering a tag to add a tag. You can add multiple tags. If you click **Next** without clicking + the tag is not added to the service.

**Step 4**

Choose a Carrier type and the endpoints of the circuit in the **Endpoints** tab, and click **Next**.

**Figure 21: Service Manager****Table 7: Endpoints Parameters**

Field	Description	Values/restrictions
<b>Carrier Type</b>		
Single Carrier	Provision a service between 2 nodes with source and destination end points.	—
Multi-Carrier	Provision a service between 2 nodes with multiple source and destination end points.	Only for OCH-NC circuits
<b>Endpoints</b>		
Endpoint A	Node and port of first endpoint	—

Field	Description	Values/restrictions
Endpoint B	Node and port of second endpoint	—

**Note**

- Click and select any object from the map after clicking the map icon and that object's details gets added in the Endpoints automatically.
- Click **Add Endpoint** to add additional endpoints to multicarrier services.
- When you create a OCH-CC circuit for an existing trail, after selecting the first endpoint, the second endpoint is auto filled. The constraints and optical interface tabs are also skipped. You are taken directly to the summary tab. The preview option is not available.

**Step 5** Choose the constraints in the **Constraints** tab, and click **Next**.

Figure 22: Service Manager

Service Manager

Services / New OCH-CC service

General Endpoints **3** Cc

Optical Feasibility Threshold ⓘ  
Select

Optimization Goal ⓘ  
None

Allow Auto Regeneration

Path

Include nodes or links ⓘ  
Select node Select links

Exclude nodes or links ⓘ  
Select node Select link

Service Diversity ⓘ  
Select service

Ignore Alarms ⓘ

Cancel Back Next

Table 8: Constraint parameters

Field	Description	Values/restrictions
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	Select RED, GREEN, YELLOW or ORANGE. GREEN = mean value YELLOW = +1 sigma ORANGE = +2 sigma RED = +3 sigma
Optimization Goal	Defines the mechanism for the control plane to compute optimum path depending on various criteria.	LENGTH (Max): Computation criteria based on minimizing the path LENGTH HOPS(Max): Computation criteria based on minimizing the number of HOPS OSNR(Min): Computation criteria based on maximizing the OSNR
Allow Auto Regeneration	Whether to allow auto regeneration	—
Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	—
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	—
Service Diversity	Select one or more existing services from the dropdown for the control plane to exclude the resources that the services use during path computation.	—
Ignore Alarms	If true, Service manager ignores any alarms present on the path and continues to provision the service.	—

**Note**

Optical Feasibility Threshold assesses whether an optical channel is operational after provisioning based on its optical power and Optical Signal-to-Noise Ratio (OSNR). This assessment is represented by colors: RED, GREEN, YELLOW, or NONE.

**Step 6**

Choose the optical interface Parameters in the **Optical Interface** tab, and click **Next**.

Table 9: Optical interface parameters

Field	Description
Wavelength	
Central Frequency (THz)	Choose a central frequency for the service.
Nyquist Spacing	Select <b>Yes</b> to allow channels to share spectral boundaries as long as the center frequency of one channel does not fall within the spectrum of another.  <b>Note</b> This option is only enabled if central frequency is specified.

Customer Name	The Customer name
Product ID	The product ID This is the Product ID of either the pluggable optics for the TXP card with pluggable trunk or the TXP card for the TXP card with fixed trunk.
FEC	The FEC depending on the product, for example, CFEC or OFEC depending on the previous selection.
Data Rate	The Data rate supported by the selected product.
Baud rate	The Baud rate supported by the selected product.
Sub Mode	is may appear depending on the other settings

**Note**

- Click **Reload application code** to reload the list of the Application codes available for OCHNC provisioning for an Alien wavelength recently imported using Alien Import.
- Click **Reset** to reset all the fields.
- For OCH-trail, Optical Interface fields are auto populated and non-editable.

Clicking next takes you to the **Summary** tab.

**Step 7** Click **Preview** in the **Summary** tab to the preview the circuit in the topology before it is created.

**Step 8** Click **Finish** to create the circuit.

**Step 9** Click **OK** once the circuit is provisioned successfully.

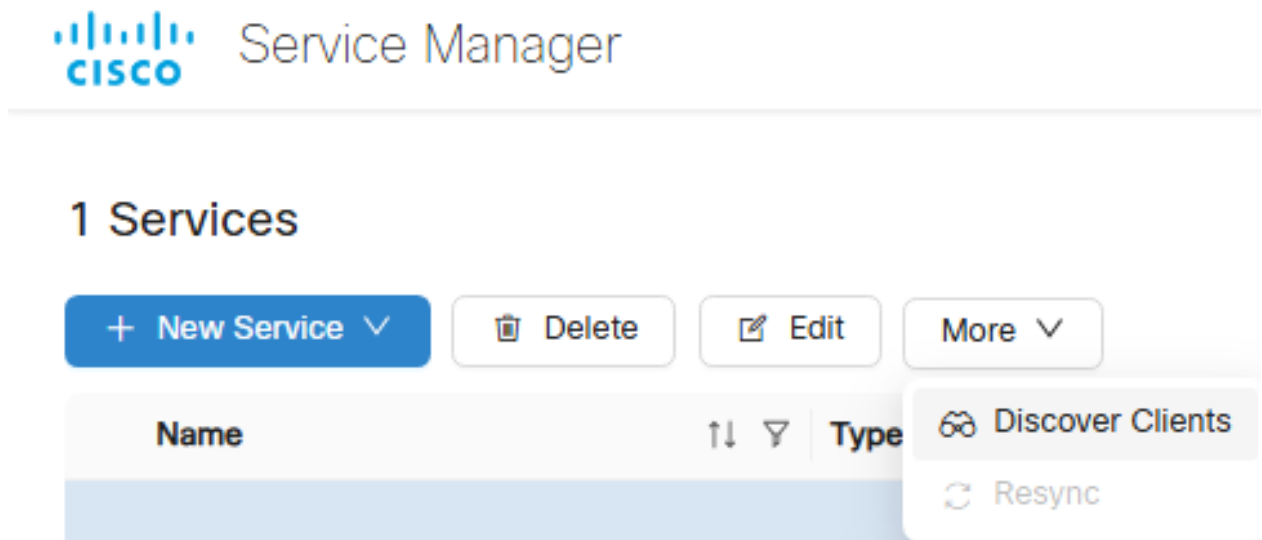
The newly provisioned circuit appears in the **Service List** table once the provisioning is complete. The **Lifecycle State** for the new circuit appears as **PLANNED** initially and later changes to **INSTALLED**.

**Step 10** Select a service and click **Edit** to edit the circuit.

- Update the name.
- Click **Save**.

**Step 11** Select an OCH-Trail circuit and click **More > Discover Clients** to discover all OCH-CC circuits over the selected trail.

Figure 23: Service Manager



**Step 12** Click **Delete** option to delete a selected service from the table.

**Note**

Delete each OCH-CC circuit associated with a service and then delete the OCH-Trail circuit.

**Note**

When cross-connect endpoints are extended or modified in Cisco Optical Site Manager or NCS 1000 topology, the existing service becomes outdated and its **Lifecycle State** moves to *Pending Removal*, while a new service with the updated endpoints is automatically rediscovered in Service Manager. After the new service is visible, the old pending-removal service can be safely deleted without affecting the network.

**Step 13** Click + icon after selecting any service to expand the service and view its carriers.

Carriers can be of either single or multiple service types. Multiple carriers can have the same Endpoints over different channels.

**Example**

This table describes the supported cards and their modes that can be used to create and manage circuits.

**Table 10: Supported transponder cards and modes**

Card	Modes Supported
NCS1K4-2-QDD-C-K9	MXP-SLICE: 200G, 300G, 400G trunk and 100G and OTU4 client
NCS1K4-QXP-K9	MXP-SLICE: 400G trunk with 400G and 100G client

Card	Modes Supported
NCS1K4-OTN-XP	MXP: 4x100G TXP: 400G 400G trunk with 100G, 10G and OTU2 clients
NCS1K14-2.4T-X-K9	MXP-SLICE: 400G, 600G, 800G, 1T, 1.2T trunk with 100G and 400G clients
NCS1K4-1.2T-K9	MXP: 100G, 200G, 300G, 400G trunk with 100G and OTU4 client MXP-SLICE: 2 trunks with 100G, 200G, 300G, 400G bandwidth and 100G and OTU4 client Supports SD-FEC-27 and SD-FEC-15
NCS2K-400G-XP-LC	MXP: 400G trunk and 100G, 10G clients FEC Modes: SD_FEC_15_DE_OFF, SD_FEC_15_DE_ON, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON
NCS2K-200G-CK-C	TXP-100G: 100G trunk and client FEC Modes: HG_FEC_7, SD_FEC_20, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON
NCS2K-1.2T-MXP	TXPMXP: 400G Trunk and 100GE, 400GE, and OTU4 clients

This table summarizes the additional supported circuit provisioning options for the 400G-XP-LC cards across CPCE configurations.

**Table 11: Supported circuit provisioning options for 400G-XP-LC cards**

Configuration	OCH-CC	OCH-Trail	OCH-NC
NCS2000 400G-XP-LC with peered ONS 15454 10x10G-LC	Yes	Yes	Yes
10X10G with MPO cable connected to 400G-XP-LC	No	Yes	Yes

## Troubleshoot CPCE Services

The most common problems encountered while using the **Service Manager** application is given below.

Some PCE error codes which you might encounter while provisioning the service are given below.

- [PCE-PR00003] - Failed for waves selector: [PCE-EXC00002] - Carrier 1 source wave (XXXXXXXX-XXXX (XXXX.XX)) and Destination one (XXXXXXXX-XXXX (XXXX.XX)) differs
- [PCE-WAL00048] - Requested central frequency XXX,XXX is out of supported range
- [PCE-WAL00026] - No free spectrum available to allocate MCH with central frequency XXX.XXX.
- [PCE-PR00001] - No routes available
- [PCE-WAL00026] - No free spectrum available to allocate MCH with central frequency XXX.XXX.x
- [PCE-PR00026] - Include constraint [Site uuid] not matched
- [PCE-PR00018] - Optical validation failed: ZONE\_RED worse than ZONE\_GREEN
- [PCE-PR00004] - Failed to evaluate optical path: [PCE-OV00016] - [Fiberspan UUID]: Invalid fiberType: [null value]

The probable scenarios in which the services can go to the **Pending Removal** State due to configuration failures and recovery steps are given below:

Failure Scenario	Cisco ONC Error	Recovery Step
Cisco Optical Site Manager Node gets disconnected as soon as a service is provisioned in CONC	Config Failure	Delete the circuit and reprovision from the CONC.
Cisco Optical Site Manager nodes are in sync state during CONC provisioning.	Config Failure	Check the Cisco Optical Site Manager node and wait for synchronisation to complete.
NCS 1010 Devices under Cisco Optical Site Manager Nodes are locked	Config Failure	<ul style="list-style-type: none"> <li>• Check Cisco Optical Site Manager and unlock the NCS 1010 device.</li> <li>• Verify Cisco Optical Site Manager synchronisation status to be completed.</li> </ul>
Cisco Optical Site Manager node Restart during provisioning	Config Failure	Wait for CONC to re-establish the connection successfully after restart and its status moved to Active in CONC.

Reload of the NCS 1010 device during provisioning from CONC	Config Failure	<ul style="list-style-type: none"> <li>• Wait for the reload to complete on NCS 1010 device.</li> <li>• Verify the synchronisation is complete on Cisco Optical Site Manager Node.</li> <li>• Wait for CONC to reestablish the connection successfully with Cisco Optical Site Manager Node and its status moved to Active.</li> </ul>
Stale entries present in NCS 1010 while no cross connects present on Cisco Optical Site Manager Nodes	Config Failure	<ul style="list-style-type: none"> <li>• Clear the NCS1010 stale entries.</li> <li>• Wait for Cisco Optical Site Manager node to complete the synchronisation.</li> </ul>
Xcons Present in Cisco Optical Site Manager node along with NCS 1010	Config Failure	<ul style="list-style-type: none"> <li>• Clear the XCONS on Cisco Optical Site Manager and NCS 1010.</li> <li>• Wait for Cisco Optical Site Manager node to complete the synchronisation and Active status.</li> </ul>

## Provision GMPLS services

Use the following procedure to create and manage circuits.

### Before you begin

**Table 12: Supported transponder cards and modes**

Card	Modes Supported
NCS1K4-2-QDD-C-K9	MXP-SLICE: 200G, 300G, 400G trunk and 100G and OTU4 client
NCS1K4-QXP-K9	MXP-SLICE: 400G trunk with 400G and 100G client
NCS1K4-OTN-XP	MXP: 4x100G TXP: 400G 400G trunk with 100G, 10G and OTU2 clients
NCS1K14-2.4T-X-K9	MXP-SLICE: 400G, 600G, 800G, 1T, 1.2T trunk with 100G and 400G clients

Card	Modes Supported
NCS1K4-1.2T-K9	<p>MXP: 100G, 200G, 300G, 400G trunk with 100G and OTU4 client</p> <p>MXP-SLICE: 2 trunks with 100G, 200G, 300G, 400G bandwidth and 100G and OTU4 client</p> <p>Supports SD-FEC-27 and SD-FEC-15</p>
NCS2K-400G-XP-LC	<p>MXP: 400G trunk and 100g, 10G clients</p> <p>FEC Modes: SD_FEC_15_DE_OFF, SD_FEC_15_DE_ON, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON</p> <p>MXP with backplane connection to 15454-M-10X10G-LC with slice 2 configured as OPM-PEER-ODU2 or OPM-PEER-ODU2E</p> <p>REGEN: 100G and 200G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits</p>
NCS2K-200G-CK-C	<p>TXP-100G: 100G trunk and client</p> <p>FEC Modes: HG_FEC_7, SD_FEC_20, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON</p> <p>RGN-100G: 100G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits</p>
15454-M-10X10G-LC	MXP 10x10G (with backplane connection to NCS2k-200G-CK-C/15454-M-100G-LC-C/15454-M-100G-ME-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients
15454-M-100G-LC-C and 15454-M-100G-ME-C	<ul style="list-style-type: none"> <li>• 10x10G client card</li> <li>• 100GE TXP mode: 100G trunk and 100GE/OTU4 clients</li> </ul>



**Note** From release 25.1.1, Cisco Optical Network Controller supports OCH-CC circuits between client ports that have the same client type and the same equipment type at both endpoints.



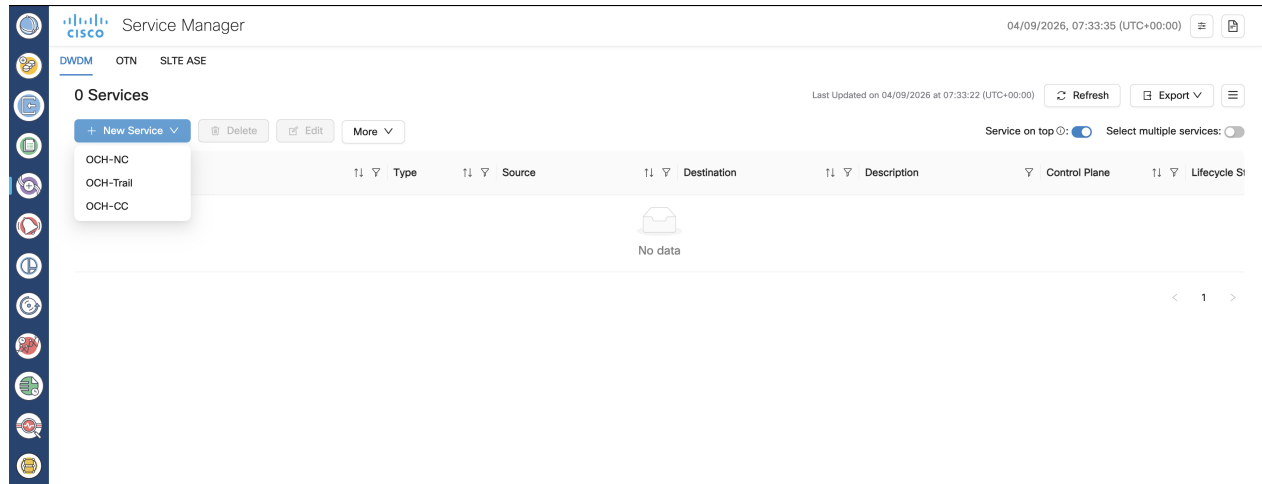
**Note** From release 26.1.1, Cisco Optical Network Controller discovers the ODU connections and builds the end-to-end protected or unprotected OTN services. Cisco Optical Network Controller automatically discovers the full OTN service when the OCH-Trail for GMPLS circuits are discovered. Additional OTN services can be added via CTC.

In release 26.1.1, OTN services are supported in the OTN-XC card mode of the NCS2K-400G-XP-LC line card only.

## Procedure

**Step 1** Click **New Service** and choose **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

**Figure 24: Service Manager**



**Step 2** Select **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

- **OCH-NC:** An OCH-NC is a circuit established between add/drop ports on terminal OLTs (Optical Line Terminals) or ROADMs (Reconfigurable Optical Add-Drop Multiplexers). This type of circuit typically connects end-user equipment to the optical network.

**Note**

You must create an LMP from COSM **GMPLS > LMP** panel before creating an OCH-NC circuit.

- **OCH-Trail:** An OCH-Trail is a circuit established between trunk ports of transponders or muxponders. This type of circuit typically transports aggregated traffic across the optical core network.
- **OCH-CC:** An OCH-CC is a circuit established between cards within optical devices, such as transponders, muxponders, or ROADMs. This type of circuit facilitates internal cross-connections within the optical equipment.

Service Manager launches the new service wizard.

**Step 3** Enter the details in the **General** tab and click **Next**.

Figure 25: Service Manager &gt; General

Services / New OCH-CC service

1 General 2 Endpoints 3 Cc

\* Name ⓘ  
 GMPLS 5 / 77

Control Plane ⓘ  
 GMPLS Fixed ▾

Label ⓘ  
 REGEN 5 / 32

Admin State ⓘ  
 UNLOCKED LOCKED

Allow Auto Regeneration

Tags ⓘ  
 Click '+' to add a tag 0 / 15 +

Description ⓘ  
 0 / 500

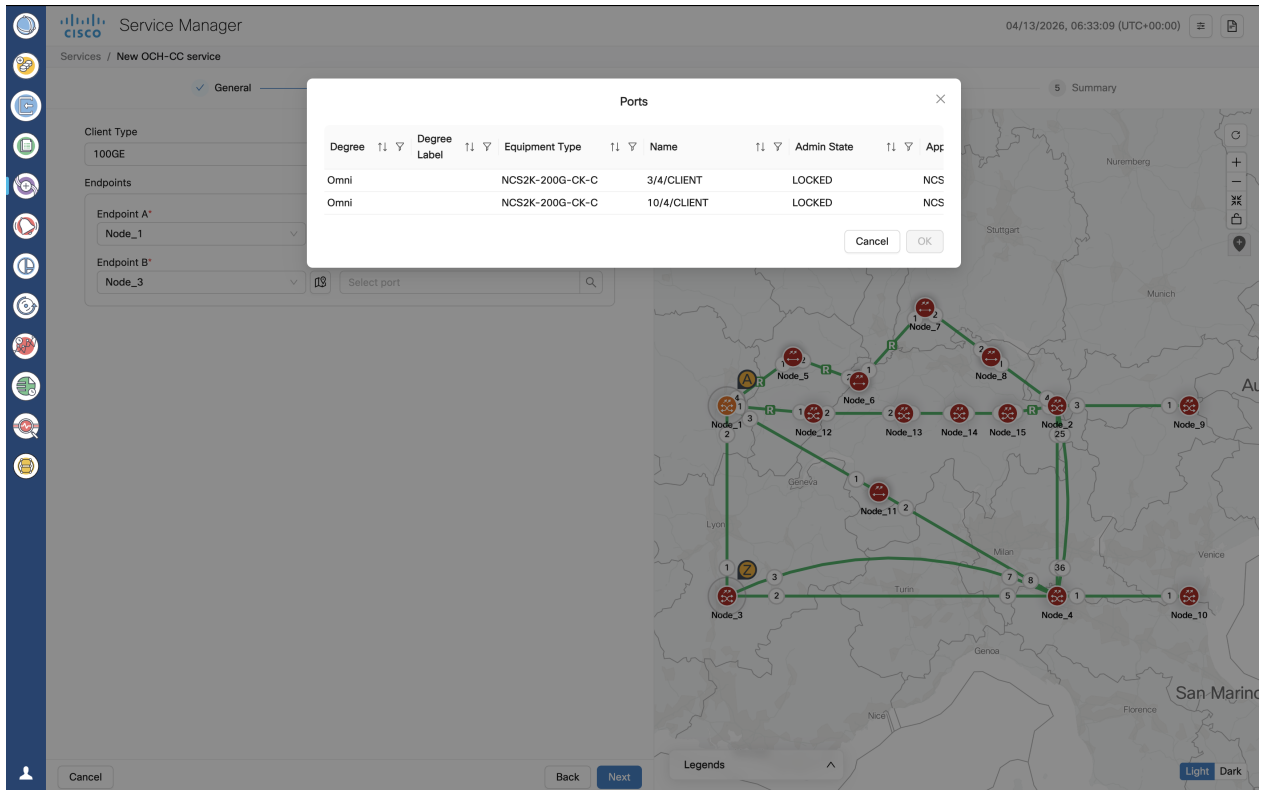
Table 13: General Parameters

Field	Description	Values/restrictions
Name	The unique user defined name of the link.	(Allowed characters are a-z, A-Z, 0-9 and _ . <Space not allowed>).
Control Plane	GMPLS Dwdm OR GMPLS Flex	—
Label	This label is assigned to the NCS 2000 cross-connects.	A label is autogenerated if the field is left blank.
Admin State	The admin state of the service	UNLOCKED or LOCKED
Allow Auto Regeneration	Allows the control plane to find a regenerator deployed in the network when a single DWDM channel is not optically feasible end to end.  <b>Note</b> This field is only displayed when GMPLS is selected in <b>Control Plane</b> .	Available for GMPLS OCH-Trail and OCH-CC circuits.

Field	Description	Values/restrictions
Tags	Tags can be attached to a service for better management, to group them together.	—
Description	Add a description about the service.	—

**Step 4** Choose a client type and the endpoints of the circuit in the **Endpoints** tab, and click **Next**.

**Figure 26: Service Manager > Endpoints**



**Table 14: Endpoints Parameters**

Field	Description	Values/restrictions
Client Type	Select the client type	10GE, 40GE, 100GE, 400GE, OTU2, OTU2E, OTU4, OC192/STM64
<b>Endpoints</b>		
Endpoint A	Node and port of first endpoint	—
Endpoint B	Node and port of second endpoint	—

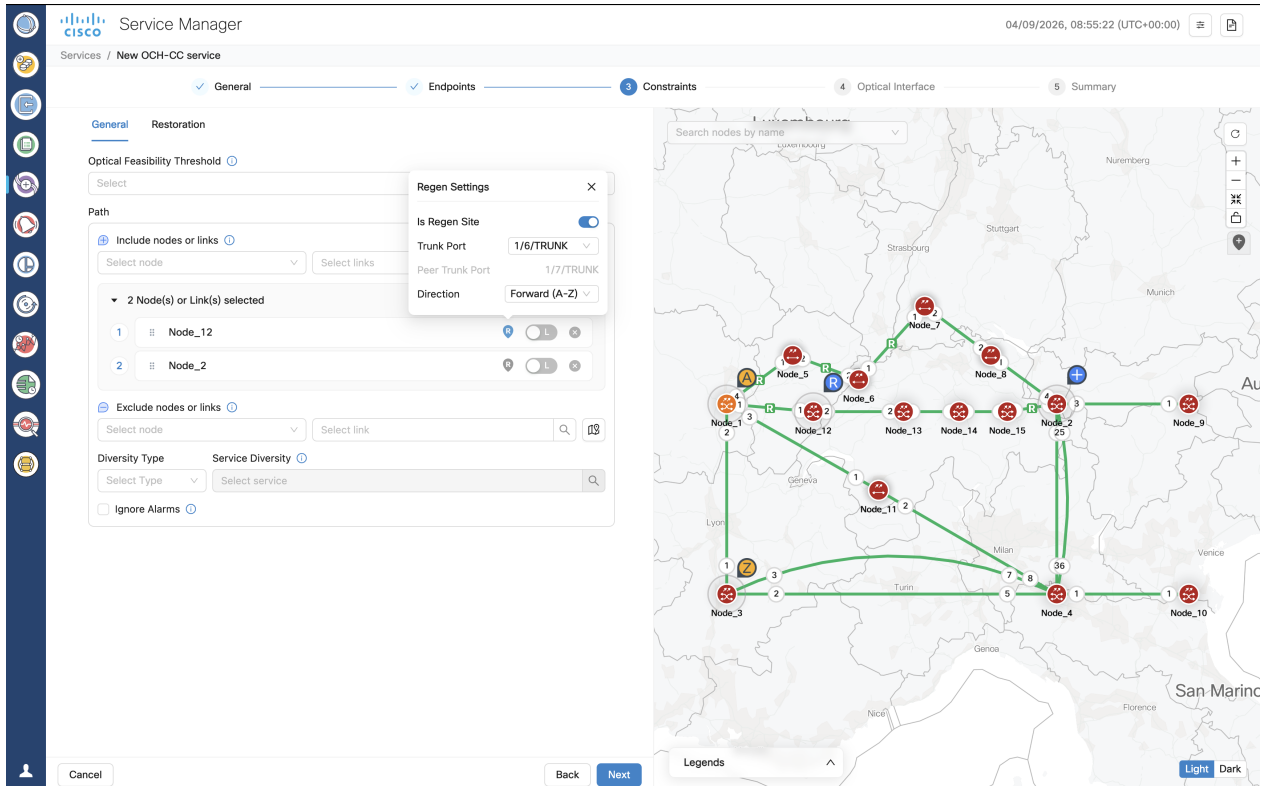
**Note**

- Click and select any object from the map after clicking the map icon and that object's details gets added in the Endpoints automatically.

- The port selection list shows the ports matching the client type selection.

**Step 5** Choose the constraints in the **Constraints > General** tab, and click **Next**.

**Figure 27: Service Manager > Constraints > General**



**Table 15: General constraints field descriptions**

Field	Description	Values/restrictions
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	Select RED, GREEN, YELLOW or ORANGE. GREEN = mean value YELLOW = +1 sigma ORANGE = +2 sigma RED = +3 sigma
Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	—
Regen (R) settings icon	Allows the control plane to include a regen node present in network to create an end-to-end circuit.	—

Field	Description	Values/restrictions
Regen Settings	Includes the selected node as a mandatory regen site in the working circuit path.	Use the <b>R</b> icon to open this dialog. <ul style="list-style-type: none"> <li>• <b>Include as regen:</b> Enable toggle button include node as regen.</li> <li>• <b>Trunk Port:</b> (Optional) Select the trunk port.</li> <li>• <b>Direction:</b> (Optional) Select the direction.</li> </ul>
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	—
Diversity Type	Choose the type of service diversity	Node, link, or srlg
Service Diversity	Select one or more existing services from the dropdown for the control plane to exclude the resources that the services use during path computation.	—
Ignore Alarms	If true, Service manager ignores unverified alarms present on the path and continues to provision the service.	—

**Note**

Optical Feasibility Threshold assesses whether an optical channel is operational after provisioning based on its optical power and Optical Signal-to-Noise Ratio (OSNR). This assessment is represented by colors: RED, GREEN, YELLOW, or NONE.

- a) For regenerated GMPLS OCH-Trail and OCH-CC circuits, add a node in the include constraint list and click the **R** icon  
Alternatively, you can click the map icon or the blue inverted teardrop icon in the map and select a node from the map.
- b) In the **Regen Settings** dialog, enable the **Is Regen Site** toggle button.
- c) You can optionally select a **Trunk Port** and **Direction** for the regen site.
  - If the node is selected as general regen node, it appears with a blue inverted teardrop **R** icon in the topology and **REGEN** icon in the **Detailed service path** tab of **Circuit Monitoring** application.
  - If the node is a normal general node, it appears with a blue inverted teardrop + icon in the topology.
  - For each regen node circuits, when you expand a service in the Service Manager table, segments are displayed and the **Regenerated** column shows **True**.

**Step 6**

Choose the constraints in the **Constraints > Restoration** tab, and click **Next**.

Figure 28: Service Manager > Constraints > Restoration

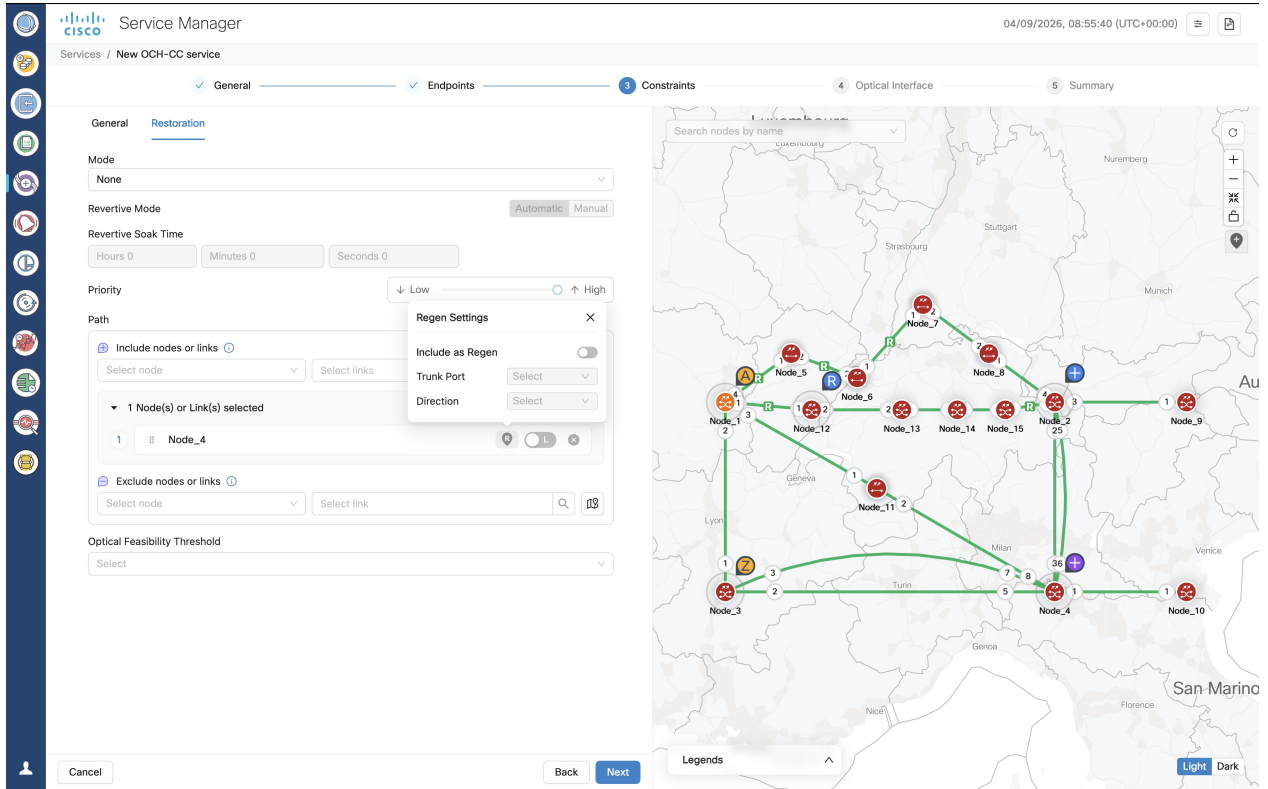


Table 16: Restoration constraints field descriptions

Field	Description	Values/restrictions
Mode	—	None, Enabled, Restorable Alternate, Enabled and Revertive
Revertive Mode	Specifies if the revert to main path after it up after a restoration should happen automatically or manually.	Automatic, Manual
Revertive Soak Time	Specifies the setup time for the restoration path. This parameter is only applicable for automatic restoration. It is the time in Hours, Minutes and Seconds for the network to switch to the restored path.	Up to 23 hours 59 minutes and 59 seconds
Priority	—	7—0 0 is the highest priority.
<b>Path</b>		
Include nodes or links	Select list of nodes & links that has to be included by the control plane during path computation.	

Field	Description	Values/restrictions
Regen (R) settings icon	Allows the control plane to include a regen node present in network to create an end-to-end circuit.	—
Regen Settings	Includes the selected node as a mandatory regen site in the working circuit path.	<p>Click the <b>R</b> icon to open this dialog.</p> <ul style="list-style-type: none"> <li>• <b>Include as regen:</b> Enable toggle button include node as regen.</li> <li>• <b>Trunk Port:</b> (Optional) Select the trunk port.</li> <li>• <b>Direction:</b> (Optional) Select the direction.</li> </ul>
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	<p>Select RED, GREEN, YELLOW or ORANGE.</p> <p>GREEN = mean value          YELLOW = +1 sigma          ORANGE = +2 sigma          RED = +3 sigma</p>

**Note**

Optical Feasibility Threshold assesses whether an optical channel is operational after provisioning based on its optical power and Optical Signal-to-Noise Ratio (OSNR). This assessment is represented by colors: RED, GREEN, YELLOW, or NONE.

- a) For regenerated GMPLS OCH-Trail and OCH-CC circuits, add a node in the include constraint list and click the **R** icon  
 Alternatively, you can click the map icon or the blue inverted teardrop icon in the map and select a node from the map.
- b) In the **Regen Settings** dialog, enable the **Include as Regen** toggle button.
- c) You can optionally select a **Trunk Port** and **Direction** for the regen site.
  - If the node is selected as restoration regen node, it appears with a purple inverted teardrop **R** icon in the topology and **REGEN** icon in the **Detailed service path** tab of **Circuit Monitoring** application after regeneration is completed.
  - If the node is a normal restoration node, it appears with a purple inverted teardrop + icon in the topology.
  - For each regen node circuits, when you expand a service in the Service Manager table, segments are displayed and the **Regenerated** column shows **True**.

**Step 7** Choose the optical interface Parameters in the **Optical Interface** tab, and click **Next**.

**Table 17: Optical interface parameters**

Field	Description
Wavelength	
Central Frequency (THz)	Choose a central frequency for the service.
Nyquist Spacing	Select <b>Yes</b> to allow channels to share spectral boundaries as long as the center frequency of one channel does not fall within the spectrum of another.  <b>Note</b> This option is only enabled if central frequency is specified.
Width	Bandwidth used by the circuit
Customer Name	The Customer name
Product ID	The product ID This is the Product ID of either the pluggable optics for the TXP card with pluggable trunk or the TXP card for the TXP card with fixed trunk.
FEC	The FEC depending on the product, for example, CFEC or OFEC depending on the previous selection.
Data Rate	The Data rate supported by the selected product.
Baud rate	The Baud rate supported by the selected product.
Sub Mode	May appear depending on the other selections

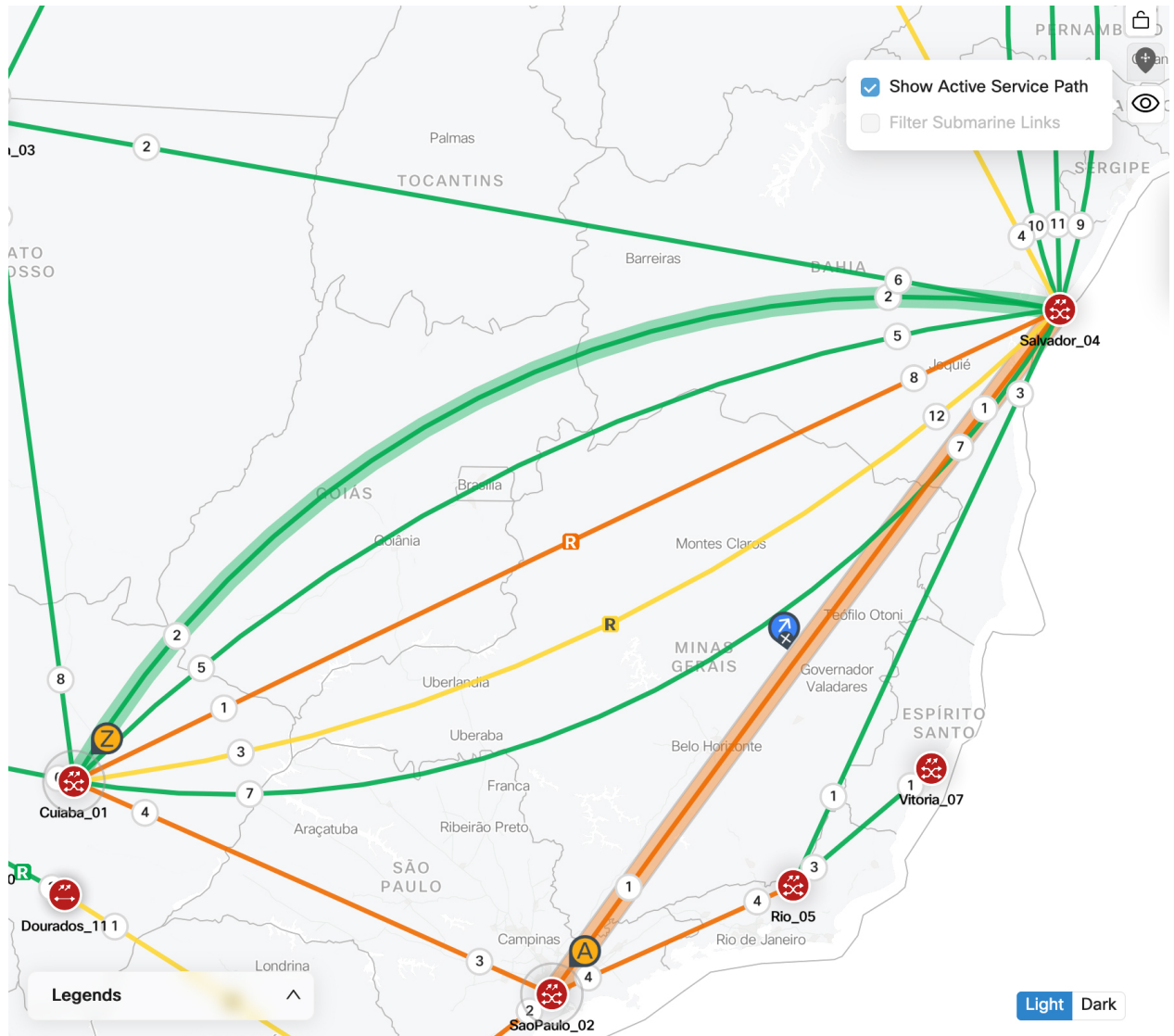
**Note**

- For OCH-trail, Optical Interface fields are auto populated and non-editable.
- For regenerated circuits, if a single wavelength is not feasible the first segment is selected and the subsequent segments use different wavelengths.

Clicking next takes you to the **Summary** tab.

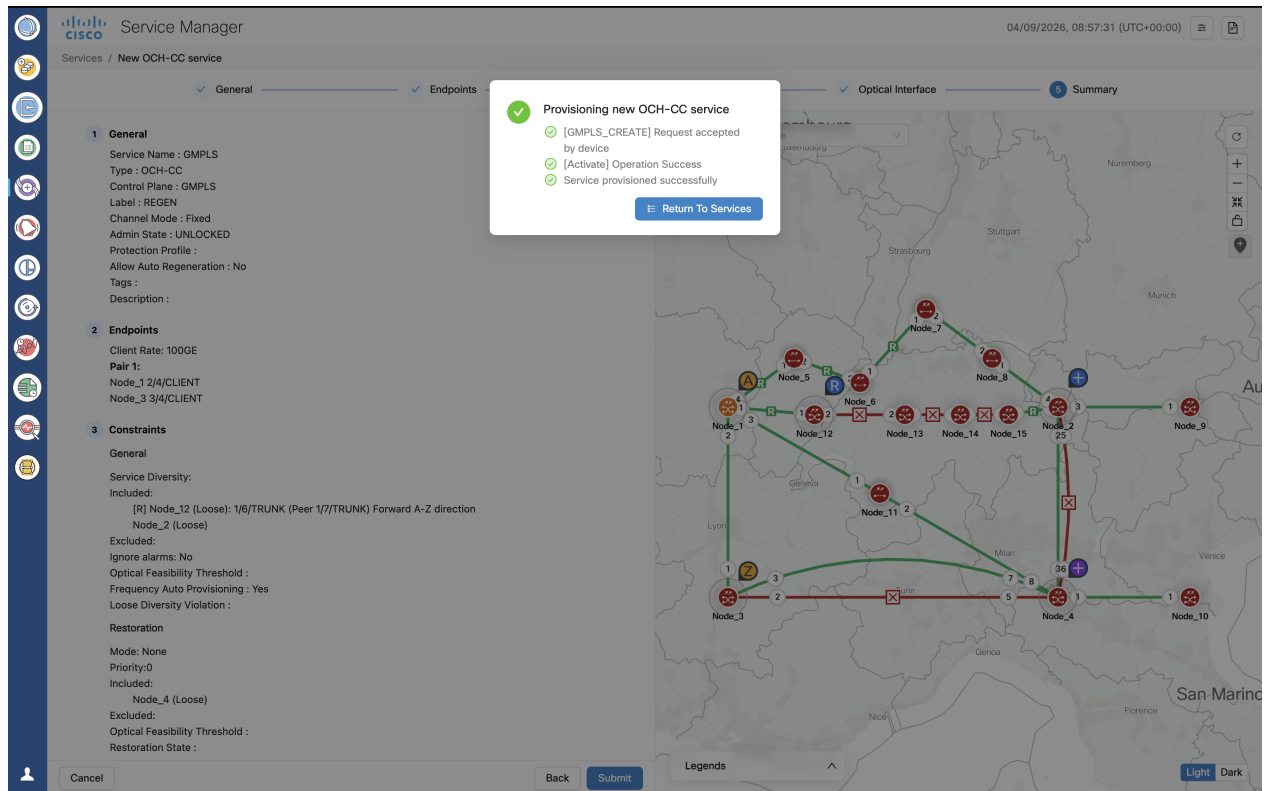
In Release 26.1.1, Topology view in Service Manager reflects the topology screen with a modified **Map View Options** eye icon. Click the eye icon and then **Show Active Service Path** to see the current active service path in the network like in Circuit monitoring screen.

Figure 29: Show Active Service Path



**Step 8** Click **Finish** to create the circuit.

Figure 30: Service Manager &gt; Summary



**Step 9** Click **Return To Services** after the circuit is provisioned successfully.

The newly provisioned circuit appears in the **Service List** table once the provisioning is complete. The **Lifecycle State** for the new circuit appears as **PLANNED** initially and later changes to **INSTALLED**.

For regenerated GMPLS OCH-Trail and OCH-CC circuits, the **Regenerated** column shows **true**. Circuit details display the service in segments, and regen sites are identified with **R** in the circuit view.

**Step 10** Select a service and click **Edit** to edit the circuit.

a) Go to **Constraints > General** and update the constraints. Click **Reroute** after updating constraints to reroute the circuit.

A status pop-up appears showing the progress of the reroute process.

For regenerated GMPLS OCH-Trail and OCH-CC circuits, you can edit regen constraints and reroute the circuit to apply the updated regen path.

b) Go to **Constraints > Restoration** and update the constraints.

You can update regen constraints for the restoration path of a regenerated circuit.

c) Click **Upgrade Restored** to make a restored circuit path the main circuit path.

d) Click **Revert Restored** to revert to the main path when **Revertive mode** is **Manual**.

Clear unverified alarms from COSM before performing this step.

e) Go to **Optical Interface**, change the wavelength parameters, and click **Retune** to change the wavelength.

*Figure 31: Service Manager > Optical Interface > Retune*

**Note**

These options are available only for GMPLS Trails and OCH-NC circuits.

For OCH-CC circuits you can edit only the name and Admin state.

**Step 11** Click **Delete** to delete a selected service from the table.

The Lifecycle state changes to DELETION\_IN\_PROGRESS and then the service is removed from the service list when deletion is complete.

**Note**

The service may go to PARTIAL state during the deletion. This is a transient state before the circuit is deleted.

The status may change to DELETION\_FAILED if the operation fails. Delete operation may fail in the following scenarios:

**Table 18: Deletion failure scenarios**

Reason	Troubleshooting
Cross connect was deleted outside Cisco Optical Network Controller	<ul style="list-style-type: none"> <li>• Retry deleting the service</li> <li>• Use the resync option in Service Manager and try again</li> <li>• Perform an full network resync and try again</li> <li>• Try deleting the service from Cisco Transport Controller</li> </ul>
Node busy	Wait for any operations on the node to complete and retry
Node disconnected	Reestablish connectivity to the node
COSM lost connection to the subtended device	Reestablish COSM connectivity to the device and try again

**Step 12** Click + icon after selecting any service to expand the service and view its carriers.

Carriers can be of either single or multiple service types. Multiple carriers can have the same Endpoints over different channels.

These are some errors you may come across when trying to provision a GMPLS circuit. Use the information to troubleshoot GMPLS errors.

Error	Description
No wavelength available on path	The optical path in the node terminates on a port not matching the requested protection mode.
Reroute Failed	The requested action can not be executed as the selected circuit is already in rolled state
Optical Validation	The partial path evaluated during route selection is outside the receiver OSNR threshold.

Error	Description
No client port available on trunk port	No available Client port matching the request constraints is found connected to the TXP Trunk port
No available optical path in node	No wavelength is available on the optical path.

### Example

This table summarizes the additional supported circuit provisioning options for the NCS 2000 100G-LC-C and 400G-XP-LC cards across GMPLS configurations.

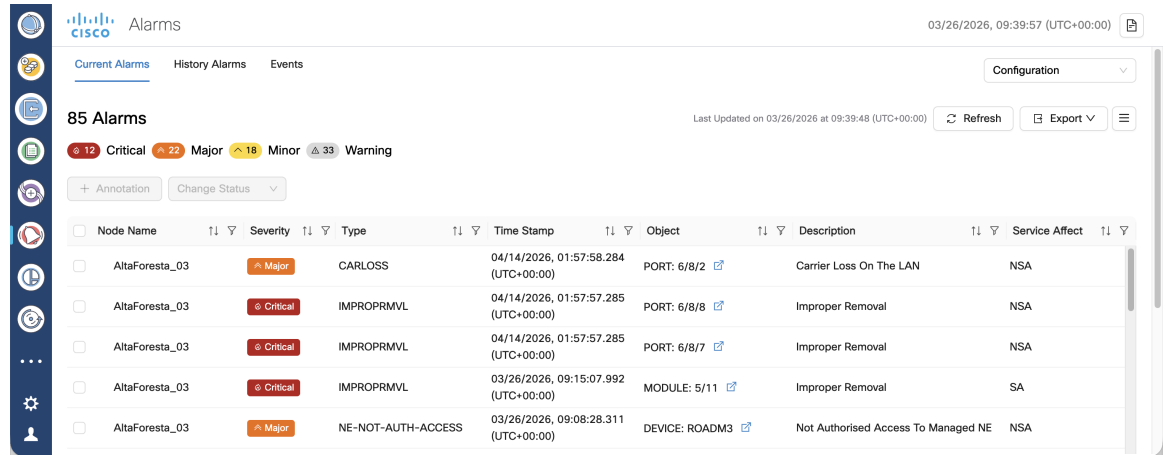
*Table 19: Supported circuit provisioning options for 100G-LC-C/100G-ME-C and 400G-XP-LC cards*

Configuration	OCH-CC	OCH-Trail	OCH-NC
NCS2000 100G-LC-C/100G-ME-C standalone	Yes	Yes	Yes
NCS2000 100G-LC-C/100G-ME-C with peered ONS 15454 10x10G-LC	Yes	Yes	Yes
NCS2000 400G-XP-LC with peered ONS 15454 10x10G-LC	Yes	Yes	Yes
10X10G with MPO cable connected to 400G-XP-LC	No	Yes	Yes

## Alarms

The **Alarms** screen displays all the alarm details for each node based on the severity level. You can view both the active alarms and the previously active alarms in this screen.

Figure 32: Alarms



For viewing the active alarms using **AlarmsCurrent Alarms** tab and the other for previous alarms using **HistoryHistory Alarms** tab.

Table 20: Alarm table field descriptions

Field Name	Description	Example/Values
Node Name	The name of the node where the alarm originated.	Node identifier/name (e.g., NODE-001)
Severity	The severity level of the alarm.	Critical, Major, Minor, Warning, Cleared
Alarm Type	The type of alarm.	LOSP, NODE-DISCONNECT
Time Stamp	The date and time when the alarm was raised.	YYYY-MM-DD HH:MM:SS.SSS
Object	The object associated with the alarm.	NODE: Node_1, SYSTEM, CHASSIS: 5
Description	A detailed description of the alarm.	Text describing alarm details
Alarm Category	The category of the alarm. See <a href="#">Alarm categories</a> .	CONC_SYSTEM, SECURITY, EQUIPMENT
Service Affect	Indicates whether the alarm is service affecting or non-service affecting.	NSA, SA
Location	The physical location of the affected equipment.	
Direction	The direction of the alarm.	Receive,

Field Name	Description	Example/Values
<b>User Tag</b>	<p>User-defined tags for categorizing and filtering alarms.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• User tags propagate from parent to child components of a chassis by default. A user tag on a child component overrides the inherited tag from its parent.</li> <li>• User Tag information comes from Cisco Optical Site Manager. See <a href="#">User Tags</a>.</li> <li>• User tags are not supported on system-level and device alarms.</li> <li>• User tags can 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.</li> </ul>	Custom tags/labels
<b>User Notes</b>	User-added notes or comments related to the alarm.	Free-form text
<b>Acknowledge</b>	Indicates whether the alarm has been acknowledged.	Acknowledged, Unacknowledged
<b>UUID</b>	Unique Universal Identifier for the alarm.	UUID string
<b>Correlation Type</b>	The type of correlation applied to the alarm.	Network Level, Node Level



**Note** You can filter the alarms table based on the fields. You can filter alarms to show only network-level or node-level correlated alarms.

## Procedure

- Step 1** Click **Alarms** in the left panel.
- Step 2** Select the **AlarmsCurrent Alarms** tab to view the active alarms of each node.
- Step 3** Select an alarm or multiple alarms and click **Annotation** to add user notes to any alarm
- a) Enter the user notes and click **Add**.

**Note**

You can add a user note to up to 500 alarms at once. You can add multiple notes to multiple alarms in the form of a list.

This will send a notification for the alarm.

**Step 4** Click **Change Status** and choose an option from the dropdown list to acknowledge or unacknowledge alarms.

**Step 5** Click **History** **History Alarms** to view the inactive or previous alarms. The details of each alarm based on each node and alarm type are displayed in the form of a cascading list and tables. Use the **Custom Date Range** Custom Date Range drop down option to view the history alarms based on different dates or time periods.

**Figure 33: Alarm History Expanded View**

Choose a time period for which you want to view the alarm history from the **Select Time period** drop down list, or choose a custom date range.

The history displays both cleared and active alarms for the selected circuit within the specified time range.

**Note**

- You can select any 3-month range from the past 78 weeks to retrieve alarm history data.
- Alarm history queries are rate limited. You can query up to 5 alarms history in a minute.

**Step 6** Click any cross-launch icon available under the Object column for any node to cross-launch to the corresponding Cisco Optical Site Manager panel.

**Step 7** Click **Export** to export the alarms details.

**Note**

You can export the table content to an excel file using the **Table View** option which has only the visible portion of the table appearing in the file or export the entire table content at once.

**Step 8** Click **Refresh** button to refresh the alarms status.

**Note**

If you apply a filter and click the **Refresh** button, the status is refreshed as per the filter you have applied.

**Step 9** Use the **Filter** option by clicking on the filter icon appearing in each column.

**Note**

- The filter option allows you to search the alarm details based on the selected filter.

- When you apply any filter in the **Alarms** screen, the **Critical**, **Major**, **Minor** and **Warning** counters they do not update their values as per the individual status of the alarms but only the count of each type of alarm.

**Step 10** Use the **Sort** option by clicking on the sort icon appearing in each column.

**Note**

The sort option allows you to sort the alarm details based on the order you have selected.

**Step 11** Click on **Critical**, **Major**, **Minor**, **Warning**, and **Cleared** alarm types to filter and display the alarms belonging to each type.

**Step 12** Use the **Acknowledge** column in the table to view the acknowledged or unacknowledged alarms.

**Note**

- To acknowledge or unacknowledge any particular alarm, select the node from the table and then click on **Change Status**. From the drop down, select **Acknowledge** or **Unacknowledge** option to acknowledge or unacknowledge the alarm of the selected node.
- If an alarm is acknowledged, it appears with a green check mark in the table.
- Acknowledged alarms also display the date and time-stamp details.
- Up to 500 alarms can be acknowledged or unacknowledged at once.

**Step 13** Use the **User Notes** column in the table to view the user notes added by any user.

**Note**

- To add a user note, select the node and click on **Annotation** option. Enter the user note details and click on **Add**. The newly added user note appears in the **User Notes** column in the table.
- Multiple user notes can be added to the same node or alarm.
- If you click on the user notes icon in the **User Notes** column, it will display all the user notes added for the selected node or alarm.



Figure 35: Events tab in Alarms application

Node Name	Severity	Service Affect	Type	Time Stamp	Object	Description
Corumba_09	Warning	NSA	USER-LOGOUT	03/26/2026, 09:39:49.000 (UTC+00:00)	DEVICE: OLA1	Logout of User
Corumba_09	Warning	NSA	USER-LOGIN	03/26/2026, 09:39:48.000 (UTC+00:00)	DEVICE: OLA1	Login of User
AltaForesta_03	Warning	NSA	T-UAS-SM	03/26/2026, 09:38:19.000 (UTC+00:00)	OTU: 5/8/11	PM TCA, FAR, 1 threshold=500, value=500
AltaForesta_03	Warning	NSA	USER-LOGOUT	03/26/2026, 09:35:50.723 (UTC+00:00)	SYSTEM	Logout of User
Jardim_10	Warning	NSA	USER-LOGOUT	03/26/2026, 09:35:35.000 (UTC+00:00)	DEVICE: OLA2	Logout of User
Teresina_16	Warning	NSA	USER-LOGOUT	03/26/2026, 09:35:35.000 (UTC+00:00)	DEVICE: OLA8	Logout of User

### Before you begin

Ensure that you are logged in to Cisco Optical Network Controller.

Follow these steps to view and manage events in Alarms application.

### Procedure

**Step 1** Click **Alarms** in the left pane.

**Step 2** Click the **Events** tab.

The table shows the latest event for each node. Event types include user login, user logout, and performance monitoring notifications. For details about the table fields, see [Table 20: Alarm table field descriptions, on page 61](#).

**Step 3** To filter events by timeframe:

- Select *Custom Date Range* and specify the start and end dates to filter the events for the selected period.

By default, *1 week* is selected to display events from the past 7 days.

- (Optional) Click the settings icon and enter the number of weeks in the **Weeks to retain events data** to define the default event data retention period.

Valid range: 1 week to 12 weeks

**Step 4** To add user notes to events, complete these steps.

- Select an alarm or multiple alarms and click **Annotation**.
- In the **Add User Notes** dialog box, enter the note text and click **Add**.

**Step 5** Optional: Use the sort and filter controls in the column headers to find specific events.

**Step 6** Click the + icon next to an event entry to view the event history and the associated user notes.

The expanded view shows the recorded event status entries for the selected node and any user notes that were added to that event.

**Step 7** Click the hamburger icon to show or hide columns.

You can review events separately from current alarms and use the available controls to filter, inspect, annotate, refresh, and export the event data.

## Network Level Alarm Correlation

The Network Level Alarm Correlation (NLAC) in Cisco Optical Network Controller is designed to reduce alarm noise and improve troubleshooting efficiency by correlating related alarms and suppressing redundant ones. When a root cause alarm is identified at the network level, NLAC suppresses all subtending alarms associated with that root cause, providing a clearer view of the network's health and focusing operator attention on the most critical issues.



### Note

- The node or site level correlation is done by Cisco Optical Site Manager and the network level correlation is done by Cisco Optical Network Controller.
- From Cisco Optical Network Controller release 25.1.1, NLAC works over a single OMS domain. Alarm correlation does not cover alarms across multiple OMS domains.

### Alarm Hierarchy Display

- The alarm display presents a hierarchical view of correlated alarms.
- The network level root cause alarm is displayed at the top level and is highlighted in blue color.
- Subtending alarms are displayed as children of the root cause alarm, accessible by clicking a plus (+) icon.
- Site-level correlated alarms are displayed at the second level of the hierarchy.
- The site level root cause alarm is in the second level and is highlighted in red color.
- Alarms correlated at the node level cannot be acknowledged or have user notes added in Cisco Optical Network Controller.

Figure 36: Alarms History

Node Name	Severity	Alarm Type	Time Stamp	Object	Description	Service Affect	Location	Direction
COSM42	Warning	USER-LOGIN	04/17/2025, 09:56:22.019 (UTC-01:00)	SYSTEM	Login of User	NSA	NEAR	NA
COSM42	Critical	LOS	04/17/2025, 09:54:45.177 (UTC-01:00)	OTS: 1/0/LINE-2-RX	Loss Of Signal	SA	NEAR	Receive
COSM42	Warning	ALS	04/17/2025, 09:54:44.178 (UTC-01:00)	OTS: 1/0/LINE-2-TX	Automatic Laser Shutdown	NSA	NEAR	Transmit
COSM42	Minor	NEIGHBOUR-MISSING	04/17/2025, 09:54:40.991 (UTC-01:00)	OTS: 1/0/LINE-2-RX	Neighbour not found	NSA	NEAR	Receive
COSM43	Critical	LOS-P	04/17/2025, 09:54:44.487 (UTC-01:00)	OTS: 1/0/LINE-RX	Incoming Payload Signal Absent	SA	NEAR	Receive
COSM43	Critical	OPWR-LFAIL	04/17/2025, 09:54:44.490 (UTC-01:00)	OTS: 1/0/(AD 4-11)-1-TX	Optical Power Failure Low	SA	NEAR	NA
COSM43	Critical	LOS-P	04/17/2025, 09:54:44.684 (UTC-01:00)	OTS: 4/0/(COM)-0-RX	Incoming Payload Signal Absent	SA	NEAR	Receive

## Alarm Correlation

Alarm correlation takes place at the network level and at the site level. Network level alarm correlation is performed by Cisco Optical Network Controller. Site level correlation is performed by COSM.

When a LOS alarm on Line is identified as the root cause, it suppresses the following alarms. This correlation is performed by Cisco Optical Network Controller. Site level correlation is independent of network level correlation. You can see site level root cause alarms and suppressed alarms without a network level root cause alarm.

*Table 21: Alarms suppressed by LOS on line*

Alarm	Object Type
LOS-P	LINE
LOS-P	OSC
ALS	LINE
PARTIAL-TOPOLOGY	LINE
APC-BLOCKED	LINE
NEIGHBOUR-MISSING	LINE
LOS-O	LINE
LOS-O	OSC



### Note

- Alarms that are the root cause display the + icon next to them and when you click this icon it displays all the suppressed alarms.
- Links and nodes that have the suppressed alarms are not included in the summary and list of alarms in **Workspaces**, **Service Assurance** and **Topology**.
- A link with suppressed alarms does not consider a suppressed alarm as its highest severity alarm.
- You cannot acknowledge alarms that Cisco Optical Site Manager correlates from Cisco Optical Network Controller
- Filters on the alarm table do not work for suppressed alarms. You cannot see suppressed alarms when you use a filter.

## Benefits of Using NLAC

The benefits of using NLAC are:

- **Reduced Alarm Noise:** NLAC significantly reduces the number of alarms displayed, making it easier for operators to identify and address critical issues.
- **Quick Fault Isolation:** Helps in quickly identifying and isolating the root cause of network issues.
- **Improved Network Reliability:** By correlating alarms effectively, it enhances the overall reliability and performance of the network.

- **Simplified Troubleshooting:** Makes it easier for network administrators to troubleshoot and resolve issues by providing clear alarm correlations.

## Acknowledged Alarm Mute

It is now possible to mute low priority alarms and disable them from appearing in the **Topology**, **Service Assurance**, **Network Monitoring**, and **Circuit Monitoring** screens.

### Purpose of Acknowledged Alarm Mute

By enabling the **Mute Acknowledged Alarms** toggle switch option to **True**, you can hide the acknowledged alarms and disable them from appearing in the **Workspaces**, **Service Assurance** and **Topology** summaries and alarms lists, even if they are available in the **Alarms** application.

### Benefits of Using Acknowledged Alarm Mute Option

The acknowledged alarm mute option allows you to have only the selected alarms appearing in the screen, instead of the entire set of all the acknowledged alarms. This helps in reducing unwanted clutter on the screen. As all the unnecessary acknowledged alarms that you do not want to be displayed can be hidden using this option.

### Muting the Acknowledged Alarms

To mute the alarms on the screen:

1. Acknowledge the alarm from the **Alarm** screen.
2. Toggle the **Mute Acknowledged Alarms** button to **True**.



#### Note

- Once an alarm is acknowledged, and the toggle switch button is set to **True**, the alarm will no longer be visible in the **Topology**, **Service Assurance**, **Network Monitoring**, and **Circuit Monitoring** screens.
- Node and link colors take the color of the highest severity unacknowledged alarms on each node and link.

### Notifications for Acknowledged Alarm Mute

Whenever the alarms are acknowledged and muted, related notifications are sent on the screen. The scenarios for the notifications are as given:

- Notifications are sent to inform all users of any toggle changes, prompting them to refresh their pages to see updates.
- When an alarm is acknowledged and the **Mute Acknowledged Alarms** button is set to **True**, notifications are sent updating device and link summaries. This occurs only if 10 or fewer alarms are acknowledged.
- Whenever a new alarm is raised, cleared or updated new notifications are sent. But when an alarm is cleared, its acknowledgement status is lost due to which you must reset it back again.
- Acknowledged alarms are excluded from the **Topology**, **Service Assurance**, **Network Monitoring** and **Circuit Monitoring** applications when the **Mute Acknowledged Alarms** toggle switch is set to **True**.

**Note**

- A restriction is placed on the number of alarms that can be acknowledged at once. This is to ensure a single notification is sent, prompting users to refresh their pages.
- When you select the circuit, the respective alarms in the circuit that are not acknowledged are displayed when the **Mute Acknowledged Alarms** is set to **ON**. In the **Topology** screen you will be able to view the count of such alarms. In the **Circuit Monitoring** screen you will be able to see these alarm details.
- The **Mute Acknowledged Alarms** option can be used in the **Network Monitoring** application as well.
- Only the admin user or the supervisor with admin access can mute the acknowledged alarms using the **Mute Acknowledged Alarms** toggle switch.

**Figure 37: Mute Acknowledged Alarms in Topology**

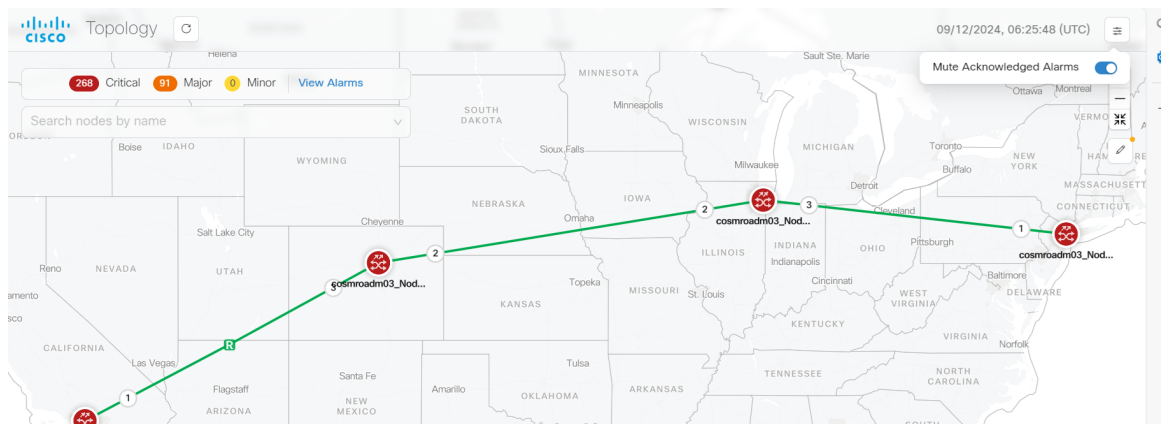


Figure 38: Mute Acknowledged Alarms in Circuit Monitoring

The screenshot displays the 'Circuit Monitoring' interface. At the top, there are notification banners: 'Acknowledgement settings have changed. Please refresh.' and a timestamp '09/25/2024, 05:16:26 (UTC)'. Below this is a 'Service List' section with a table of 8 services. The selected service is 'onc\_COSM71\_5/0/4\_COSM94\_5/2/4', which is in an 'INSTALLED' state and 'DISABLED' operationally. Below the service list, the 'Alarms' section shows 4 alarms for the selected service, with one alarm being 'Critical' and 'FLEXD-LOF'. To the right, a 'Topology' map shows a network diagram with nodes labeled 'SALENO', 'POTENZA', 'BARI', 'LECCE', and 'MARONE'.

Name	Type	Source	Destination	Lifecycle State	Operational State
onc_COSM71_3/CH-1_COSM94_2/CH-1	OCH-NC	COSM71	COSM94	INSTALLED	DISABLED
onc_COSM71_5/0/4_COSM94_5/2/4	OCH-Trail	COSM71	COSM94	INSTALLED	ENABLED
onc_COSM71_3/CH-0_COSM94_2/CH-0	OCH-NC	COSM71	COSM94	INSTALLED	ENABLED
onc_COSM71_4/1/CH-0_COSM94_4/1/CH-0	OCH-NC	COSM71	COSM94	INSTALLED	DISABLED
onc_COSM71_2/CH-4_COSM94_3/CH-4	OCH-NC	COSM71	COSM94	INSTALLED	DISABLED
onc_COSM94_2/CH-22_COSM71_3/CH-22	OCH-NC	COSM94	COSM71	INSTALLED	DISABLED

## SNMP Traps and Alarm Filters

The SNMP tab under the alarms app, allows Cisco Optical Network Controller to send alarm traps to external SNMP managers. This enables integration with external monitoring systems and provides a mechanism for forwarding alarm information. Cisco Optical Network Controller supports both SNMP v2c and v3.

The screenshot shows the 'Alarms' application with the 'SNMP' tab selected. It displays '0 SNMP Managers' and provides options to '+ New Configuration', 'Edit Config', 'Set/Edit Filters', and 'Delete'. Below these options is a table with columns for 'Server Name', 'IP Address', 'Destination Trap Port', 'SNMP Version', 'Community', 'Mode', 'User Name', 'Authentication Type', and 'Privacy Type'. The table currently contains no data.

### Alarms and Events

An event is a distinct incident that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Events can indicate an error, failure, or exceptional condition in the network. Events can also indicate the clearing of those errors, failures, or conditions. Events have associated severities which you can be adjusted.

An alarm is a response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity (Critical, Major, Minor, and so forth). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).



**Note** Cisco Optical Network Controller does not support notification replay. Hierarchical controllers miss notifications when Cisco Optical Network Controller is down or not reachable.

**SNMP manager configuration**

- Supports configuration of up to four SNMP managers.
- Supports both UDP and TCP protocols for trap transmission.
- Allows configuration of SNMP v2c and v3 managers.

**Alarm filtering**

- Provides detailed filter configuration options to control which alarms are sent to each SNMP manager.
- Supports filtering by alarm severity (Critical, Major, Minor, Warning).
- Supports filtering by alarm type (e.g., Cisco Optical Network Controller generated alarms, circuit alarms, device alarms, restoration alarms).
- Allows exclusion of specific alarm types to avoid overwhelming OSS systems.
- Provides separate filtering for transient (events) and non-transient (alarms) conditions.

**Set the Edit Host Name**

The host name is used to identify the Cisco Optical Network Controller server sending the SNMP traps.

**Before you begin**

- There is a character limit of 25 characters for the host name.
- Only alphanumeric characters, underscores, and hyphens are allowed in the host name. Spaces are not allowed.
- If you do not set a host name, the default value `CONC` is used.

**Procedure**

- 
- Step 1** Click **Set/Edit Host Name**.
- Step 2** Enter the desired hostname.
- Step 3** Click Save.
- Step 4** (Optional) Click **View Engine id**

**Note**

The Engine ID remains the same for all SNMP managers.

The Engine ID is displayed and can be copied for use in the receiver application.

---

**Configure SNMP managers**

The alarms and events are filtered based on the criteria set by user and converted to traps and sent to the trap server using the alarm model in CISCO-EPM-NOTIFICATION-MIB. For more information, see [MIB Definition For Cisco Optical Network Controller](#).

## Procedure

**Step 1** Navigate to **Alarms > SNMP**.

**Step 2** Create a New SNMP Manager.

a) Enter the Server Name and IP Address.

Cisco Optical Network Controller supports only IPv4.

b) Enter the Port Number, and choose the SNMP Version.

c) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.

### New SNMP trap configuration ✕

Server Name\*

Demo\_UDP\_106

IP Address\*

10.58.251.85

Destination Trap Port Number\*

6002

SNMP Version\*

V2C

Community\*

Notification Type\*

UDP  TCP

Trap configuration\*

Send all traps  
 Set custom trap filters

Cancel

Create

d) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth. Type**, **Auth. Password**, **Confirm Auth. Password**, **Privacy Type**, **Privacy Password**, and **Confirm Privacy Password**.

### New SNMP trap configuration ✕

<p>Server Name* <input type="text" value="Demo_UDP_106"/></p> <p>Destination Trap Port Number* <input type="text" value="6002"/></p> <p>User Name* <input type="text" value="snmpv3user"/></p> <p>Authentication Type* <input type="text" value=""/></p> <p>Confirm Authentication Password <input type="text" value=""/></p> <p>Privacy Password <input type="text" value=""/></p> <p>Notification Type*  <input checked="" type="radio"/> UDP   <input type="radio"/> TCP         </p>	<p>IP Address* <input type="text" value="10.58.251.85"/></p> <p>SNMP Version* <input type="text" value="V3"/></p> <p>Mode* <input type="text" value="authPriv"/></p> <p>Authentication Password <input type="text" value=""/></p> <p>Privacy Type* <input type="text" value="Select Privacy Type"/></p> <p>Confirm Privacy Password <input type="text" value=""/></p> <p>Trap configuration*  <input type="radio"/> Send all traps  <input checked="" type="radio"/> Set custom trap filters         </p>
--	---

- e) Choose the **Notification Type**, TCP or UDP.
- f) Choose the **Trap Configuration**, Send all traps or Set custom trap filters.  
If you choose custom trap filters follow [3.c](#), on page 75

### Step 3 Configure alarm filters.

- a) Click **Alarms > SNMP**.
- b) Select a manager and click **Set/Edit Filters**.

## The custom trap filter configuration pop-up

New trap filter configuration

04/23/2025, 07:34:44 (UTC)

Include alarms for:

Severity  Critical  Major  Minor  Warning  Cleared Logical OR

Type  Service-affecting  Non Service-affecting

LOGICAL AND

All Alarms

831 Alarms Last Updated on 04/23/2025 at 07:34:42 Refresh Export

Name	Category	Condition Type
<input type="checkbox"/> SENSOR-LOW-1-2V-CPU	EQUIPMENT	Alarm
<input type="checkbox"/> APC-WRONG-GAIN	OPTICAL	Alarm
<input type="checkbox"/> DUP-NODENAME	SYSTEM	Alarm
<input type="checkbox"/> OTDR-FIBER-END-NOT-DETECTED-TX	MAINTENANCE	Alarm
<input type="checkbox"/> CONTBUS-A-18	EQUIPMENT	Alarm
<input type="checkbox"/> T-OSNR-MIN	TCA	Event
<input type="checkbox"/> HIBATVG	EQUIPMENT	Alarm
<input type="checkbox"/> SIGLOSS	OPTICAL	Alarm
<input type="checkbox"/> OTDR-HYBRID-SCAN-IN-PROGRESS-RX	MAINTENANCE	Alarm
<input type="checkbox"/> SENSOR-LOW-OUTLET-AIR	EQUIPMENT	Alarm

Excluded Alarms

0 Alarms Last Updated on 04/23/2025 at 07:34:42 Refresh Export

No data

Cancel Apply

- c) Select the desired Severity levels and alarm types.  
Severity: Critical, Major, Minor, Warning, Cleared  
Type: Service-affecting, Non Service-affecting
- d) Choose the logical operator for the filter.  
If you choose AND, you get notifications for only the alarms that match both the severity selection and Type selection.  
If you choose OR, you get notifications for the alarms that match either the severity selection or type selection.
- e) Use the transfer list to exclude specific alarms. Use filters in the table to find the specific alarms you want to exclude.
- f) Click **Apply**.  
The custom trap filter for the SNMP manager is created.

- If traps are not being received, verify the SNMP manager configuration, including the IP address, port, protocol, and security settings.
- Check the alarm filters to ensure that the desired alarms are not being excluded.
- Verify that the Cisco Optical Network Controller server has network connectivity to the SNMP manager.

## Alarm email forwarding

A alarm email forwarding is a notification capability that

- sends alarm updates from Cisco Optical Network Controller to one or more email recipients based on subscription-specific filters,
- allows each subscription to be uniquely named, include up to five email addresses, and specify filter criteria, and
- restricts the creation, editing, or deletion of subscriptions to users with admin or supervisor roles.

### How alarm email forwarding works

Use alarm email forwarding when you want Cisco Optical Network Controller to send selected alarm notifications to distribution lists or individual recipients.

- You can create a maximum of 10 subscriptions for different recipient groups and filter criteria.
- If the same email address is used in multiple subscriptions and an alarm matches the filter criteria for more than one subscription, Cisco Optical Network Controller sends only one email notification for that alarm to that recipient.

For example, if user 1 is configured in Subscription A and Subscription B, and the same alarm matches both subscriptions, user 1 receives only one email notification for that alarm.

- The sender email address is fixed and is not user-configurable.
- Read-only users cannot create, edit, or delete alarm subscriptions.
- All notification emails are sent from the fixed sender address *noreply-conc@cisco.com*. This address cannot be changed by users.

### SMTP server requirement

The system relies on a configured SMTP server to deliver email notifications and email notifications are not delivered until the SMTP server is configured and reachable.

- SMTP settings can be configured from the **Jobs** tab of the **PM History** application. For more details, see [Accessing PM History Report, on page 132](#).
- You can specify both a primary SMTP server and, optionally, a secondary SMTP server for failover. If the primary server becomes unavailable, the system automatically attempts to send notifications using the secondary SMTP server.
- The email subscription page displays the current SMTP configuration status. If SMTP is not configured, a warning **SMTP Server is not configured** is displayed with a link to the PM Jobs configuration page.

### Alarm types that trigger notifications

These alarm events trigger email notifications:

Alarm event	Description
Alarm Raised	A new alarm occurs or an existing alarm escalates in severity.
Alarm Cleared	An alarm condition is resolved.
Alarm Updated	An alarm severity changes (other than raised or cleared).
Alarm Acknowledged	A user acknowledges or unacknowledges an alarm.
Alarm User Note	A user adds an annotation to an alarm.

## Alarm email forwarding subscription settings

Use this reference to understand the configuration values and behavior that apply to alarm email forwarding subscriptions.

### Subscription settings

The alarm email forwarding page uses these settings.

**Table 22: Alarm email forwarding settings**

Setting	Description	Notes
Subscription name	Identifies the alarm email forwarding subscription.	Each subscription name must be unique and contain no more than 50 characters.
Email recipients	Lists the email addresses that receive forwarded alarms.	Each subscription supports up to five email addresses and validates the email address format.
Alarm filters	Controls which alarms Cisco Optical Network Controller forwards for the subscription.	The filtering model is similar to the filtering model used for SNMP alarm forwarding.
SMTP configuration	Provides the mail server settings that Cisco Optical Network Controller uses to send alarm emails.	A warning is displayed if SMTP server settings to send the notifications are not configured.
Export	Exports the subscription entries from the page.	Use export to review or share the current subscription list.

## Alarm email notification format

This section describes the email format that Cisco Optical Network Controller sends for the alarm email notifications. The severity value appears in uppercase.

### Alarm email subject line format

Cisco Optical Network Controller uses these upper-case severity values in the subject: `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, and `CLEARED`.

**Table 23: Alarm email subject line format**

Condition	Subject format	Example
Alarm name and device name present	[SEVERITY] Event Type - Alarm Name on Device Name	[CRITICAL] Alarm Raised - LOS on NCS2K-Shelf1
Only alarm name present	[SEVERITY] Event Type - Alarm Name	[MAJOR] Alarm Cleared - LOS
Only device name present	[SEVERITY] Event Type on Device Name	[MINOR] Alarm Updated on NCS2K-Shelf1
Neither present	[SEVERITY] Event Type	[WARNING] Alarm Raised

### Email body format

The email body uses a plain-text format with a summary section and an alarm-details section.

Table 24: Alarm email summary fields

Field	Description
Subscription Name	Lists the matching subscription names for the recipient as a comma-separated list.
Alarm Name	Shows the name of the alarm condition when the alarm name is available.
Severity	Shows the alarm severity in uppercase when the severity value is available.
Device Name	Shows the name of the affected device when the device name is available.
Event Type	Shows one of these event types: Alarm Raised, Alarm Cleared, Alarm Updated, Alarm Acknowledged, or Alarm User Note.

**Example alarm email summary:**

```

-----
ALARM NOTIFICATION
-----
Subscription Name : Network-Ops-Team, Critical-Alerts
Alarm Name       : LOS
Severity        : CRITICAL
Device Name     : NCS2K-Shelf1
Event Type      : Alarm Raised

```

**Sender details**

Alarm notification emails always use the following sender information (these values cannot be changed):

Table 25: Alarm email sender details

Field	Value
From Address	noreply-conc@cisco.com

## Configure alarm email forwarding subscriptions

Create an alarm email forwarding subscription and apply filters that control which alarm notifications are sent to the selected recipients.

- Use different subscriptions for different recipient groups or alarm conditions.
- Use filters to limit forwarded alarms to the required severities, alarm types, or other supported criteria.

The **Alarms** page shows the existing subscriptions and provides options to create, edit, filter, delete, refresh, and export subscription entries.

If the SMTP server is not configured, Cisco Optical Network Controller shows a message on the page.

Follow these steps to configure an alarm email forwarding subscription.

## Procedure

---

**Step 1** Click **Alarms** and from the **Configuration** drop-down list, select **Email Configuration**.

The subscription list opens.

**Step 2** Click **New Subscription**.

The **Add Email Configuration** form is displayed.

**Step 3** In the **Subscription Name** field, enter a unique name for the subscription.

Use a name that identifies the recipient group or the filter purpose.

**Step 4** In the **Email(s)** field, type the email ID of the recipient and click + to add the email.

You can add up to five email addresses to a subscription.

**Step 5** In the **Alarms configuration** section, perform these steps:

- Select **Send all alarms** to send notification for all the alarms.
- Select **Set custom alarm filters** to send notification for selected alarms based on the created filters.

Use the available filter controls to include or exclude alarms based on the supported filter criteria.

To create filters, click **No filters set** and proceed with the steps outlined in the [Configure SNMP managers, on page 72](#) topic.

**Step 6** Click **Add** to save the subscription.

The new subscription appears in the subscription list and Cisco Optical Network Controller uses it for future alarm emails.

**Step 7** To manage the subscriptions, perform these optional steps:

a) To edit a subscription, select an existing subscription and click **Edit Subscription**.

**Note**

The alarm configuration option (Send all alarms / Set custom alarm filters) cannot be changed when editing a subscription. To modify filter criteria, use the **Set/Edit Filters** button.

b) To edit the filters, click **Set/Edit Filters**.

c) To delete a subscription, select a subscription and click **Delete**.

d) To export all subscription details, click **Export**.

The report is downloaded in a *.xlsx* file.

**Note**

Only one subscription can be selected at a time for editing, filtering, or deletion.

---

Cisco Optical Network Controller forwards matching alarms to the configured email recipients by using the active SMTP server settings.

# Workspaces

Workspaces provide focused environments for specific monitoring and management tasks. They integrate data and functionality from multiple applications, presenting a unified view and streamlined workflow for users. This approach reduces the need to navigate between different applications, improving efficiency and user experience.




---

**Note** From 25.1.1 release, you can acknowledge and unacknowledge alarms from the alarms tab in workspaces.

---




---

**Note** From 26.1.1 release, Circuit workspaces support PM history for OTN services that include the PM of all the ODU ports in both working and protect paths.

---

## Procedure

---

- Step 1** Click **Workspaces** in the left panel.
- Step 2** Select the workspace and click **Launch**.
- Step 3** Click **Save Layout** to save the layout at any given point in time.
- Step 4** Click **Reset Layout** to revert to the default layout.
- Step 5** Some of the other options that are available on these panels are mentioned below.
- Hovering on the nodes displays the node name and the alarm severity.
  - Hovering on the equipment displays the equipment name, service state as enabled or disabled and the count of the severity of the alarms.
  - Hovering on the port which is displayed as a round icon on the panel displays the port name, service state, and the alarms severity counts.
  - Connectivity between each equipment is highlighted with arrows.
  - If you right click at the node level it will cross launch to the Nodal UI to verify OXC's.
  - If you right click at the equipment level it will cross launch to View Nodal UI: Equipment.
  - If you right click on any port it will cross launch to View Nodal UI: Port.
  - Connectivity between the nodes are represented with arrows.
- 

## Circuit Monitoring workspace

This section describes the Circuit Monitoring workspace. This workspace focuses on individual circuits, displaying their path, associated alarms, and performance history.



**Note** AR-MXP card is supported but OCH-CC and OCH-Trail circuits cannot start from this card.

**Figure 39: Circuit Monitoring**

The screenshot displays the Cisco Circuit Monitoring workspace. At the top, it shows the date and time (04/09/2026, 16:47:39 UTC+02:00) and options to 'Reset Layout' and 'Save Layout'. Below this is the 'Service List' section, which includes tabs for 'DWDM', 'OTN', and 'SLTE ASE'. It shows 95 services with columns for Name, Type, Source, Destination, Description, Control Plane, and Lifecycle State. The services listed include OTNXK2, tkt1\_carp, th3\_car\_ar, and psm. The 'Alarms' section shows 270 alarms with a table of details including Node Name, Severity, Type, and Time Stamp. The 'Topology' section shows a map of a network with various nodes and connections.

Name	Type	Source	Destination	Description	Control Plane	Lifecycle State
OTNXK2	OCH-Trail	SaoPaulo_02	AltaForesta_03		GMPLS	INSTALLED GMPLS_Active
tkt1_carp	OCH-CC	SaoPaulo_02 1/7/1	Cuiaba_01 5/7/1		GMPLS	INSTALLED GMPLS_Active
th3_car_ar	OCH-CC	Cuiaba_01 5/3/1	Salvador_04 30/3/1		GMPLS	INSTALLED GMPLS_Active
psm	OCH-CC				GMPLS	PARTIAL GMPLS_Active

Node Name	Severity	Type	Time Stamp
Cuiaba_01	Major	CARLOSS	04/19/2026, 06:05:32.2 (UTC+02:00)
Cuiaba_01	Major	CARLOSS	04/19/2026, 06:05:32.2 (UTC+02:00)
Salvador_04	Major	CARLOSS	04/16/2026, 11:37:09.1 (UTC+02:00)
Cuiaba_01	Major	IPC-VERIFICATION-FAIL	04/09/2026, 16:28:15.0 (UTC+02:00)

In **Circuit Monitoring**, the services list is primary. This list has these tabs

- DWDM—DWDM circuit services
- OTN—OTN circuit services
- SLTE ASE—Submarine circuit services



**Note** Each services table includes an info icon, **Click to view complete summary**, next to each service. Click the info icon to get the full summary of the circuit service.

**Figure 40: Service Summary**

This image is an example of summary for OTN service.

### Service Summary ×

- 1
**General**
  - Service Name : ODU\_connection\_protected\_10GE
  - Protection Profile : PROTECTED
  - Payload Type : 10GE
  - Bandwidth : ODU2e
  - Service State : INSTALLED
  - Operational State : ENABLED
  - Admin State : UNLOCKED
  - Tags :
  - Description :
- 2
**Endpoints**
  - Source: site\_svo-sm2k-42 6/4/7-3
  - Destination: site\_svo-sm2k-36 6/2/7-3
  - Source protection values**
  - Source Revert Time : 5
  - Source Switch State : Released
  - Source Holdoff Timer : 0
  - Destination protection values**
  - Destination Revert Time : 5
  - Destination Switch State : Released
  - Destination Holdoff Timer : 0

#### OTN circuit table

The OTN circuit table provides the OTN circuit parameter information.

**Table 26: OTN circuit parameter description**

Parameter	Description
Name	Name of the OTN circuit
Source	Source node of the OTN circuit
Destination	Destination node of the OTN circuit
Lifecycle State	Lifecycle state of the discovered OTN service. supported states are Installed and Partial.
Operational State	Operational state of the node, whether enabled or disabled
Admin State	Administrative state of the node
Protection Profile	Protected for protected OTN service. Unprotected for unprotected OTN service.
Payload Type	OTN rate
Bandwidth	Bandwidth of the signal
Error	Error message
Discovery Date	Date and time of service discovery
Tags	User-defined tags
Description	Short description of the circuit

**SLTE ASE table****Table 27: STLE ASE table**

Parameter	Description
Name	Name of the service
Endpoint 1	Source endpoint
Endpoint 2	Destination endpoint
Frequency (THz)	Frequency of the circuit service in THz
Bandwidth (GHz)	Bandwidth of the circuit service in GHz
Discovery Date	Data and time when the service was discovered
Tags	User-defined tags
Source Attenuation	Signal attenuation at source node

Parameter	Description
Destination Attenuation	Signal attenuation at destination node

### Alarms table

Use the **Alarms** table to view the existing alarms in the network.

- In the **Alarms** screen, select any alarm and right click followed by **Show DWDM Affected service(s)**, **Show OTN Affected service(s)**, or **Show SLTE ASE Affected service(s)**. This will display all the services related to the selected alarm in the services layout.

**Table 28: Alarms table parameters**

Parameters	Description
Node Name	Name of the node on which the alarm is raised
Device Object Name	Name of the device object
Severity	Severity of the alarm
Type	Type of alarm
Time Stamp	Time stamp of the alarm
Object	Logical object of the alarm
Description	Description of the alarm
Category	Alarm category
Service Affect	Marks the alarm as service affecting or non service affecting
Location	Location of the node where the alarm is raised
Direction	Direction of the alarm
User Tag	User-defined tags
User Notes	User-defined notes
Acknowledge	Acknowledge or unacknowledged the alarms
UUID	Unique ID of the device
Transient	Transient or non-transient alarm
Correlation Type	Correlation type
Ru Position	Rack unit position of the device
Rack ID	Rack ID of the device

Parameters	Description
Low Device Name	Low device name

### History table

Use the **History** table in the **Alarms** pane to view the history of alarms in the network.

**Table 29: Alarms history table parameters**

Parameters	Description
Node Name	Name of the node the alarms was raised
Node State	State of the node
Device Object Name	Name of the device object
Severity	Severity of the alarm
Service Affect	Marks the alarm as service affecting or non service affecting
Type	Type of alarm
Time Stamp	Time stamp of the alarm
Object	Logical object of the alarm
Description	Description of the alarm
Category	Alarm category
Location	Location of the node where the alarm is raised
Direction	Direction of the alarm
User Tag	User-defined tags
UUID	Unique ID of the device
Transient	Transient or non-transient alarm
Ru Position	Rack unit position of the device
Rack ID	Rack ID of the device
Low Device Name	Low device name

## Release-wise circuit workspace enhancements

Figure 41: Circuit Monitoring

The screenshot displays the Cisco Circuit Monitoring workspace. At the top, it shows the date and time (04/09/2026, 16:47:39) and options to reset or save the layout. Below this, there are tabs for Service List, Alarms, and Topology. The Service List tab is active, showing a table of 95 services. The Alarms tab shows 270 alarms, and the Topology tab shows a network map with various nodes and links.

Name	Type	Source	Destination	Description	Control Plane	Lifecycle State
OTNXC2	OCH-Trail	SaoPaulo_02	AltaForesta_03		GMPLS	INSTALLED GMPLS_Active
tit1_carp	OCH-CC	SaoPaulo_02 1/7/1	Cuiaba_01 5/7/1		GMPLS	INSTALLED GMPLS_Active
tit3_car_ar	OCH-CC	Cuiaba_01 5/3/1	Salvador_04 30/3/1		GMPLS	INSTALLED GMPLS_Active
psm	OCH-CC				GMPLS	PARTIAL GMPLS_Active

Node Name	Severity	Type	Time Stamp
Cuiaba_01	Major	CARLOSS	04/19/2026, 06:05:32.2 (UTC+02:00)
Cuiaba_01	Major	CARLOSS	04/19/2026, 06:05:32.2 (UTC+02:00)
Salvador_04	Major	CARLOSS	04/16/2026, 11:37:09.1 (UTC+02:00)
Cuiaba_01	Major	IPC-VERIFICATION-FAIL	04/09/2026, 16:28:15.0 (UTC+02:00)

- From release 24.3.1, **PM** tab is available in the **Circuit Monitoring** workspace application.
- From release 25.1.1, you can select multiple links or nodes in the topology.
  1. Click **Select node(s)/link(s)** in topology.
  2. Use the OTS/OMS/OTN toggle to select the segment type.
  3. Click the nodes or links you want to select.  
You can select up to 20 entities at a time.
  4. Click **Show services**.  
The service list shows affected services for the selected nodes and links. The list shows the services that are with paths through all the selected nodes and links.
  5. Click **Refresh data and reset the layout in Service List** to reset the table to show all services.
- From release 25.1.1, alarms history can be viewed for each circuit.
  1. Select a service from the service list.
  2. Click **History** in the **Alarms** tab.
  3. Choose a time period for which you want to view the alarm history from the **Select Time period** drop down list, or choose a custom date range.  
The history tab displays both cleared and active alarms for the selected circuit within the specified time range.
    - The maximum time period is 3 months. If you select a time range more than 3 months using custom date range, Cisco Optical Network Controller throws an error.
    - Alarm history queries are rate limited. You can query up to 5 alarms history every minute.

- From release 26.1.1, the **Circuit Monitoring** workspace has these enhancements related to OTN.
  - **OTN** tab—New tab in the Services List to check the protected and unprotected services.
  - **OTN** toggle button—New toggle button in Topology pane enables OTN links of the transponder cards.

Use the OTS/OMS/OTN toggle button to select the link type.

- The *Circuit Monitoring* workspace displays the detailed OTN service path including the OTN clients, OTN trunk, OTU links, and OTN-level alarms, for example, OTN interface alarms and service history specific to OTN service.

- From release 26.1.1, the topology view highlights the constraints in the network.

1. Click the **Map View Options** eye icon.
2. Check the **Show Constraints** check box.

The active circuit path with constraint is highlighted.

**Figure 42: Show Constraints**



3. Expand the **Legends** bar to verify the configured legends. The constraints icons on the map are explained in the legends.

*Figure 43: Constraints Legends*

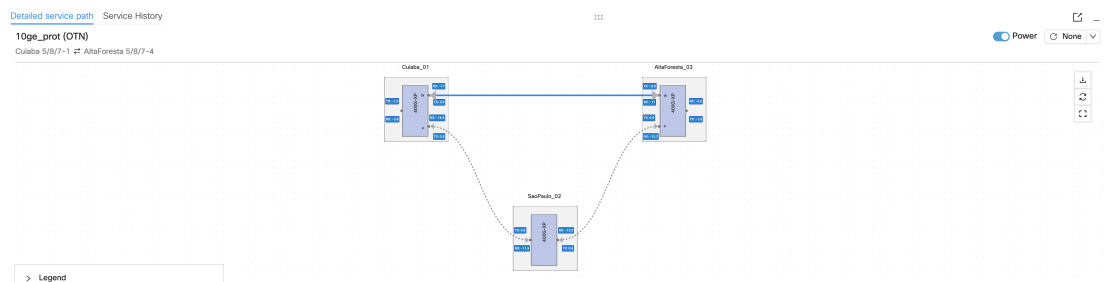
### Detailed service path

- Select a service from the service list to view its detailed service path.
- For DWDM circuits, use the **Channel Power** and **Composite Power** toggle switches to enable and disable the power display for all ports in the detailed service path.

For OTN circuits, use the **Power** toggle switch.

Power toggle switch shows the total power of relative ports for Working and Protect paths.

**Figure 44: Power toggle switch**

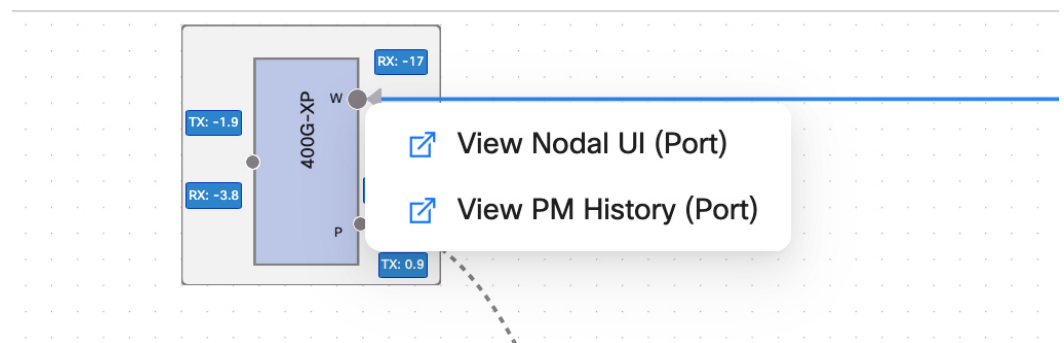


- Hover over a port or equipment in the detailed service path to view a tooltip. The tooltip displays W and P that specify the working and protected path for protected OTN service and source and destination ODU port information.

Right click on a port to cross-launch *Links* tab and *PM history* from the service detailed path.

- PM history
  - Select a service from the service list.
  - From detailed service path, right click a port and choose View PM history.

**Figure 45: Port pop-up options**



The PM History in Circuit monitoring appears.

Figure 46: PM History in Circuit workspace

PM History

Port: [Culaba\\_01 : 5/8/12](#) × [Culaba\\_01 : 5/8/12/1-1](#) ×

27 Items Export

Interface type: [opticalChannel](#) Location: [nearEnd](#)

Parameter	Latest Reading	Prev1	Prev2	Prev3	Prev4	Prev5	Prev6	Prev7	Prev8	Prev9	Prev10	Prev11
<input type="checkbox"/> FECUncorrectableBlocks	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/> PrefECBitErrorRate	0.000840082292 05641	0.000837037783 81850	0.000842441182 77459	0.000835776886 43764	0.000833031207 45781	0.000816050692 11007	0.000809881746 08633	0.000810760817 08720	0.000827422836 91265	0.000820844639 85740	0.000821532711 12249	0.000824373162 97760
<input type="checkbox"/> prefFECCorrectedErrors	206657723599	205908783706	207238003639	205598606733	204923177941	200746022107	199228479892	199444728721	203543535612	201925318871	202094582338	202793324973
<input type="checkbox"/> differentialGroupDelayMin (ps)	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00
<input type="checkbox"/> differentialGroupDelayMax (ps)	6.00	6.00	6.00	6.00	6.00	6.00	5.00	5.00	5.00	5.00	5.00	5.00
<input type="checkbox"/> differentialGroupDelayAvg (ps)	5.00	4.90	5.00	5.00	5.00	4.90	4.90	4.70	4.20	4.30	4.40	4.40

- **Interface type** drop-down list: By default, only one interface type is used to generate the report for the selected port. However, if the port has multiple interface types, you can choose the interface type from the drop-down.
- **Location** drop-down list: You can choose to view the PM history report for up to two ports based on their location, nearEnd or farEnd.
- You can view PM history for up to two ports at a time.

## Service History

- Select an OTN service from the **OTN** tab and go to **Service History** tab to get events related to the selected OTN service.

Figure 47: Service history table

Detailed service path: [Service History](#)

7 Events Last Updated on 04/09/2026 at 16:52:53 (UTC+02:00) Refresh Export

Time	Event Type	Event Name	Description	Details
04/09/2026, 16:44:48.725 (UTC+02:00)	Info	OTN_SERVICE_STATE_CHANGED	Service state changed from DISABLED to ENABLED	<a href="#">View More</a>
04/09/2026, 16:44:48.642 (UTC+02:00)	Success	OTN_SERVICE_DISCOVERED	OTN service discovered: 5/8/7-1 + 5/8/7-4 with protected circuits	<a href="#">View More</a>
04/09/2026, 16:26:59.369 (UTC+02:00)	Info	OTN_SERVICE_STATE_CHANGED	Service state changed from DISABLED to ENABLED	<a href="#">View More</a>
04/09/2026, 15:13:25.530 (UTC+02:00)	Info	OTN_SERVICE_STATE_CHANGED	Service state changed from ENABLED to DISABLED	<a href="#">View More</a>
04/09/2026, 13:32:49.144 (UTC+02:00)	Info	OTN_SERVICE_STATE_CHANGED	Service state changed from DISABLED to ENABLED	<a href="#">View More</a>
04/09/2026, 13:08:51.063 (UTC+02:00)	Info	OTN_SERVICE_STATE_CHANGED	Service state changed from ENABLED to DISABLED	<a href="#">View More</a>

- Offers a "view more" option to display detailed diagnostic logs related to the event.

## Topology panel

The **Topology** panel reflects the topology screen with a modified **Map View Options** icon.

- **Map View Options**—Provides **Show Constraints** and **Filter Submarine Links** options.

# Link Monitoring workspace

This section describes the Link Monitoring Workspace. This workspace focuses on individual links, displaying their alarms, performance history, topology, and associated circuits.

## Links monitoring workspace functionalities

Figure 48: Link Monitoring workspace

The screenshot displays the Cisco Link Monitoring workspace. At the top, there's a header with the Cisco logo, the title 'Link Monitoring', and a timestamp '04/15/2025, 20:14:10 (UTC)'. Below this, there are tabs for 'Links', 'Topology', and 'Alarms'. The 'Links' tab is active, showing a table with 10 links. The table has columns for Link Name, Type, Endpoint1-Node Name, Endpoint2-Node Name, Endpoint1-Port, Endpoint2-Port, Endpoint1-Degree, and Endpoint2-Degree. Below the table is a topology map showing nodes (Node\_1 to Node\_11) and links between them. The bottom section shows 66 alarms and a PM History section with 0 items.

Link Name	Type	Endpoint1-Node Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port	Endpoint1-Degree	Endpoint2-Degree	Action
+ oms_Node_1-1_Node_2-1	OMS	Node_1	Node_2	1/2/LINE-TX	1/2/LINE-RX	1	1	[Edit] [View]
+ oms_Node_1-2_Node_3-1	OMS	Node_1	Node_3	1/16/LINE-TX	1/2/LINE-RX	2	1	[Edit] [View]
+ oms_Node_1-4_Node_2-4	OMS	Node_1	Node_2	1/14/LINE-TX	1/6/LINE-RX	4	4	[Edit] [View]
+ oms_Node_2-3_Node_9-1	OMS	Node_2	Node_9	1/5/LINE-TX	1/2/LINE-RX	3	1	[Edit] [View]
+ oms_Node_4-1_Node_10-1	OMS	Node_4	Node_10	1/2/LINE-TX	1/2/LINE-RX	1	1	[Edit] [View]

- The Links monitoring workspace has three tabs OTS, OMS, and OTN.
- By selecting the link, its related alarms, span loss and links in topology are filtered and highlighted. The links table has a label above it specifying the current filter. For example, Showing Links for locationA 1/2/LINE-TX - locationB 1/2/LINE-RX.

In Links monitoring workspace, a selection is bidirectional. For example, the link you select from the Links table list is highlighted in the topology. The nodes and links you select in topology are filtered in the links table list.

- In links table, click the pencil icon (**edit link**) in the action column to edit link details.
- You can cross launch circuit monitoring for circuits using a link by clicking **View in Circuit Monitoring** in the action column.
- In links table, you can select only forward/reverse OTS links.
- You can select multiple links or nodes in the topology.
  1. In **Topology**, click **Select links** icon.
  2. Select the nodes or links you want to modify.  
You can select up to 20 entities at a time. Multiple selection is available only for OTS links.
  3. Click **Select Links**.  
The links list shows the selected links.
  4. Click the **Refresh data and reset the hierarchy** icon in **Links** table to reset the table to show all links.

### OMS Links tab

Use the **OMS Links** table to view the OMS link parameters in the network.

**Table 30: OMS Links table parameters**

Parameters	Description
Link Name	User-defined name for the OMS link
Type	Type of the link
Deployment Type	Location of the link deployed
Endpoint1-Node Name	Source node of the link
Endpoint2-Node Name	Destination node of the link
Endpoint1-Port	Source port that transmits the link
Endpoint2-Port	Destination port that receives the link
Endpoint1-Degree	Degrees of the source node
Endpoint1-Degree Label	User-defined label for the source node
Endpoint2-Degree Label	User-defined label for the destination node
Tags	Tags added to the link
Description	Short sentence describing the link
Link Status	Status of the link
Fiber Type	Type of fiber used between the nodes
Fiber Length (km)	Length of the fiber cable between the nodes
Total Transmit Power Tx (dBm)	Total power transmitted in the link
Total Receiver Power Rx (dBm)	Total power received in the link
Span Loss(dB)	Link span loss between the source and destination node
Action	Pencil - Edit icon - Modify the link parameters Arrow - Open icon - View circuit monitoring for a link in circuit monitoring workspace

### Link Monitoring workspace options

These action icons and button improve your interaction with the table

- **Collapse All** button—Collapses the expands tables.
- Refresh icon—Refreshes the table data.
- Export icon—Exports the table view and network report in excel.

- Column preferences icon—Enables display or removal of columns in the table.

### OTN Links tab

Use the **OTN Links** table to view the OTN link parameters in the network.

**Table 31: OMS Links table parameters**

Parameters	Description
Link Name	User-defined name for the OTN link
Rate	Speed of the link
Endpoint1-Node Name	Source node of the link
Endpoint2-Node Name	Destination node of the link
Endpoint1-Port	Source port that transmits the link
Endpoint2-Port	Destination port that receives the link
Tags	Tags added to the link
Description	Short sentence describing the link
Link Status	Status of the link
Span Utilization	View summary hyperlink opens the span utilization summary table for each ODU port
Action	Pencil - Edit icon - Modify the link parameters Arrow - Open icon - View circuit monitoring for a link in circuit monitoring workspace

### Alarms tab

Use the **Alarms** table to view the existing alarms in the network.

**Table 32: Alarms table parameters**

Parameters	Description
Node Name	Name of the node on which the alarm is raised
Device Object Name	Name of the device object
Severity	Severity of the alarm
Type	Type of alarm

Parameters	Description
Time Stamp	Time stamp of the alarm
Object	Logical object of the alarm
Description	Description of the alarm
Category	Alarm category
Service Affect	Marks the alarm as service affecting or non service affecting
Location	Location of the node where the alarm is raised
Direction	Direction of the alarm
User Tag	User-defined tags
User Notes	User-defined notes
Acknowledge	Acknowledge or unacknowledged the alarms
UUID	Unique ID of the device
Transient	Transient or non-transient alarm
Correlation Type	Correlation type
Ru Position	Rack unit position of the device
Rack ID	Rack ID of the device
Low Device Name	Low device name

### Alarm history tab

Use the **History** table in the **Alarms** pane to view the history of alarms in the network.

**Table 33: Alarms history table parameters**

Parameters	Description
Node Name	Name of the node the alarms was raised
Node State	State of the node
Device Object Name	Name of the device object
Severity	Severity of the alarm
Service Affect	Marks the alarm as service affecting or non service affecting
Type	Type of alarm
Time Stamp	Time stamp of the alarm

Parameters	Description
Object	Logical object of the alarm
Description	Description of the alarm
Category	Alarm category
Location	Location of the node where the alarm is raised
Direction	Direction of the alarm
User Tag	User-defined tags
UUID	Unique ID of the device
Transient	Transient or non-transient alarm
Ru Position	Rack unit position of the device
Rack ID	Rack ID of the device
Low Device Name	Low device name

### PM History pane

The **PM History** pane has these tabs.

- Recent—List the recent PM data
- History—List the PM history data

**Table 34: PM history table parameters**

Parameters	Description
Optical Link	Name of the optical link
Span Loss	Link span loss between the source and destination node
Measured By	Entity measured for PM data
Measured Time	PM data reported time

### Topology pane

The **Topology** pane reflects the topology screen.

- Light/Dark toggle buttons—Allows switching between light and dark themes.
- Legends—Represents the Nodes, Links, States and Node Resync in a visual format
- Map view icons—Allows zoom in, zoom out, reset and lock default view functions
- Select links icon—Selects the discovered OMS links

- Map view options icon—Pops up **Filter Submarine Links** check box to display submarine links only in the map.

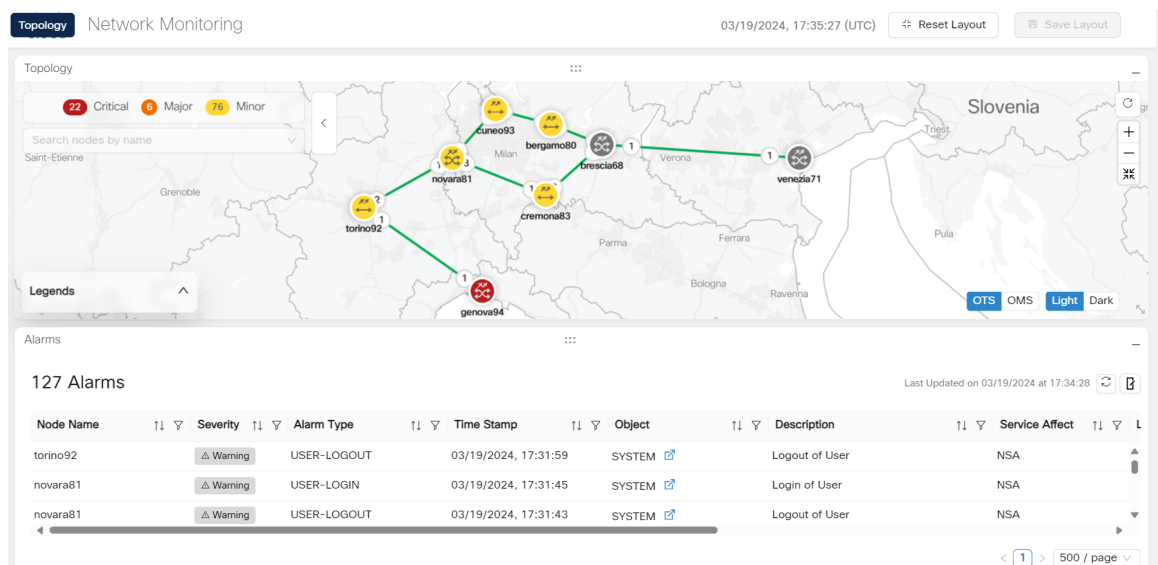
**Table 35: PM history table parameters**

Parameters	Description
Optical Link	Name of the optical link
Span Loss	Link span loss between the source and destination node
Measured By	Entity measured for PM data
Measured Time	PM data reported time

## Network Monitoring workspace

This section describes the Network Monitoring Workspace. This workspace provides a comprehensive view of the network, including node status, alarms, and performance metrics.

**Figure 49: Network monitoring workspace screen**



**Note** In the network monitoring workspace, the alarm details are displayed based on the node or link which is selected from topology.

## OTN circuits

OTN circuits are discovered on pre-existing GMPLS OCH-Trails created out of NCS2K-400G-XP-LC card in OTN-XC card mode. The OTN circuits are displayed in Service Manager , Topology views, Circuit Monitoring workspace. It supports these circuit characteristics:

- Protected circuits with an active working path and a standby protection path
- Unprotected circuits with a single active path
- GMPLS OCH-Trails

CONC supports brownfield discovery of OTN circuits that are already provisioned on the network using CTC or other tools.

- Automatic discovery of OTN services in service manager page on the *OTN* tab
- Circuit monitoring workspace with active route, protection status, and alarm visibility
- OTN link utilization summary with export to Excel option
- Service event history with event type classification and export to Excel option
- Service detailed path

## OTN circuit types and topology representation

An OTN circuit in CONC is a logical transport connection that carries client traffic over an OTN (Optical Transport Network) layer, which itself runs on GMPLS OCH-Trails. CONC discovers and displays OTN circuits with these key attributes:

- Circuit type: protected or unprotected
- Active working path and protection standby path (for protected circuits)
- Underlying OCH trail and OTS physical route

### OTN topology layers and circuit path visualization

CONC provides two main topology layers for OTN visibility:

- OTN layer: Shows OTN circuits and their paths between endpoint transponder nodes. Inline amplifier sites (OLA/ILA) that are not terminated at the OTN level are not displayed in this layer.
- OTS layer: Shows the full physical route including all nodes, links, and inline sites. OTN circuits are not directly highlighted in this layer.

The visual representation of OTN circuit paths in the circuit monitoring workspace uses these conventions:

- Solid line: The active working path of a protected circuit, or the active path of an unprotected circuit
- Dotted line: The standby protection path of a protected circuit

When a protection switch occurs, the topology highlight updates to reflect the new active route. The highlight always shows the currently active route, not the configured working route.



**Note** In release 26.1.1, ILA (Inline Line Amplifier) and OLA (Optical Line Amplifier) inline sites that are not terminated at the OTN layer are not shown in the OTN topology map. To view the full physical route including inline sites, navigate to the underlying OCH trail and switch to the OTS layer.

The following table compares OTN and OTS topology layer visibility:

**Table 36: OTN versus OTS topology layer comparison**

Attribute	OTN layer	OTS layer
OTN circuit path highlighted	Yes	No
Inline sites (OLA/ILA) visible	No	Yes
OCH trail visible	No	Yes
Protection status shown	Yes	No

## Monitor OTN circuits

Monitor OTN circuits to verify circuit health, active path routing, protection status, and any alarms affecting the circuit.

The circuit monitoring workspace provides a unified view of OTN circuits, including topology visualization, detailed service, and service history panels. The workspace displays both protected and unprotected circuits discovered from the network. You can navigate between the OTN layer and the OTS layer to correlate circuit path information with the physical network topology.

### Before you begin

OTN circuits are provisioned using CTC or other tools and discovered and displayed in CONC under the OTN tab in service manager

### Procedure

- 
- Step 1** Navigate to the circuit monitoring workspace.  
Go to **Workspace > Circuit Monitoring > Launch**.
- The circuit monitoring workspace appears displaying trails and OTN circuits in the topology panel. Trails are shown in the OTN layer and serve as the underlying transport on which OTN circuits are built.
- Step 2** Click the **OTN** toggle button in the topology to display OTN circuits.  
The OTN topology shows the OTN links and circuits between endpoint nodes. You can switch between the OTS and OTN layers using the layer selector buttons in the topology panel.
- Step 3** Select an OTN circuit to open the detailed service panel.  
For a protected circuit, the circuit detailed service panel shows:
- Active working path (solid line on topology)

- Standby protection path (dotted line on topology)
- Protection status for each path segment
- Link status pop-up when hovering over path segments

The circuit detail panel opens, showing path information, protection status, and any active alarms for the selected circuit.

**Step 4** To access device-level details, right-click a node or card in the CONC topology and select the **View in Nodel UI** option to open the component in COSM.

CONC opens the COSM interface at the specific card location. From COSM, you can perform maintenance operations such as protection switching. Direct protection switching from the CONC web UI is not available in release 2611.

**Step 5** To view performance monitoring (PM) graphs for a specific port, right-click a node or card in the CONC topology and select the **View PM History (port)** option

Clicking the port link redirects to the interface PM view. Clicking directly on a port row in the PM view opens the historical PM graph for that interface. The PM view supports range filters (for example, 3 hours) to control the time window displayed in the graph.

These PM data types are available on trunk ports:

- Optical channel PM (200G trunk only)
- OTU PM (trunk interfaces)
- ODU PM (all ODU containers)

---

The circuit monitoring workspace displays the selected OTN circuit with its active route highlighted in the topology and circuit details shown in the detail panel.

## Monitor OTN link utilization

Monitor OTN link utilization to assess bandwidth consumption and capacity across the OTN links in your network.

The link utilization view in CONC displays current bandwidth usage for all OTN links associated with a circuit. Utilization is expressed as a percentage of total link capacity.

If a port has no allocated circuit (no cross-connect installed), its bandwidth row is not populated in the OTN link utilization table. When a circuit is added, the row appears and utilization updates accordingly.



---

**Note** At least one OTN circuit must be discovered and visible.

---

### Procedure

---

**Step 1** Navigate to the link utilization view in the OTN link monitoring workspace or Links app.

For Link Monitoring workspace: Go to **Workspace > Link Monitoring > Launch**.

The link monitoring workspace appears displaying the all OMS links. Go to **OTN links** tab.

For Links app: In the left panel, click **Links**.

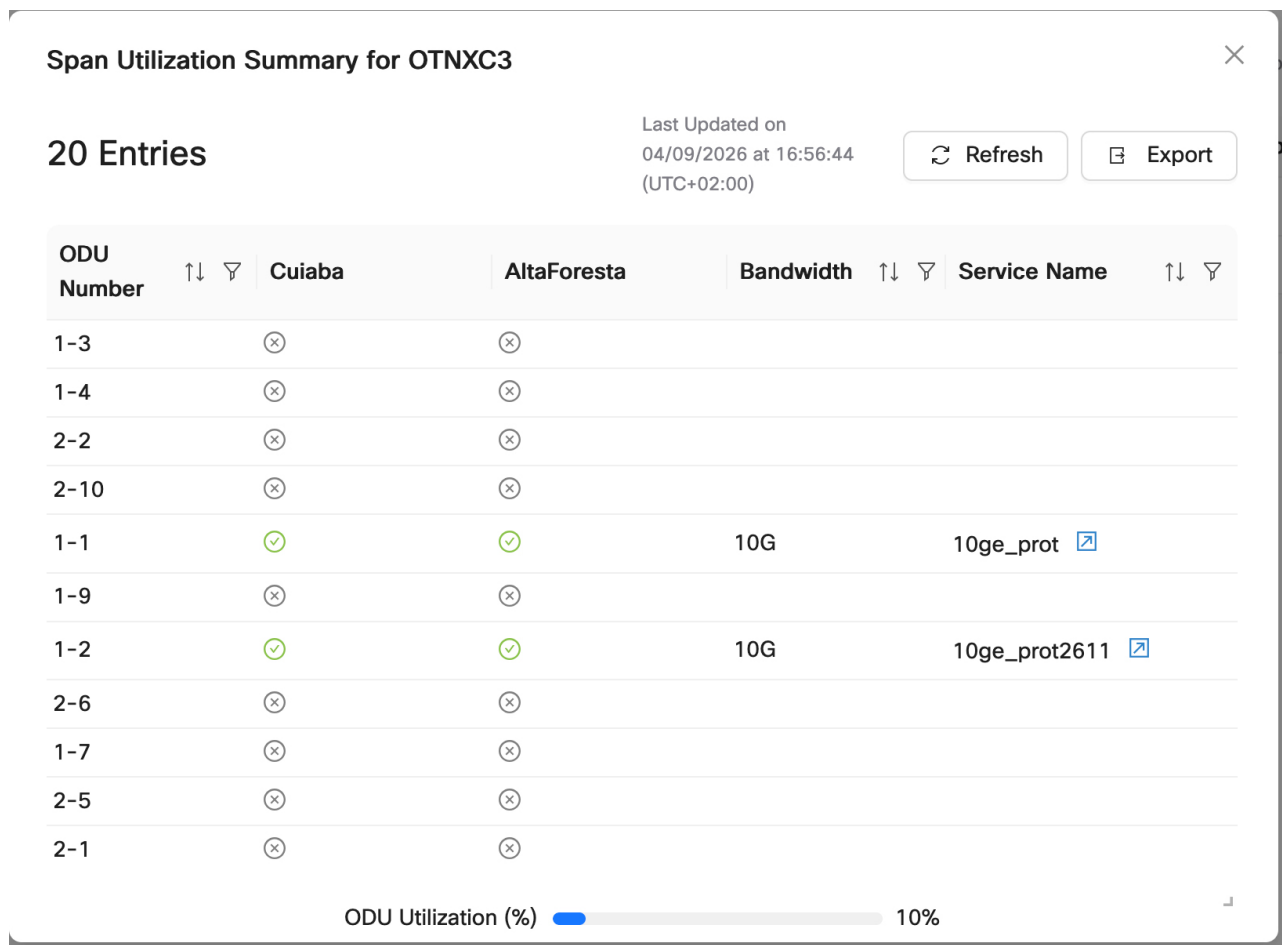
The link app opens displaying the all OMS tab. Go to **OTN** tab.

**Step 2** In the **Span Utilization** column, click **View summary**.

Span utilization summary for an OTN circuit appears displaying ODU ports and their parameters.

ODU Utilization is shown as a percentage. For example, two 10G containers on a 200G link produce a 10% utilization figure.

**Figure 50: Complete span utilization summary**



**Step 3** Review the utilization percentage for each OTN link.

The table displays these parameters for each link:

- ODU port number
- Bandwidth allocated
- Service name
- Utilization percentage

Unused ports or bandwidth that has no allocated circuit are shown with an empty bandwidth value.

---

You can view the current OTN link utilization percentages and export the data to Excel using **Excel** for offline analysis or reporting.

## View OTN service event history

view the OTN service event history for a selected OTN circuit.

The service history for an OTN circuit displays a table of events associated with that circuit. Events are classified by event type: *success*, *info*. In release 2611, success events are generated only for initial discovery events (when the OTN service is first created). Protection switch events and state changes are reported as info events. The event table supports column resizing and export to Excel.



---

**Note** The *View more* link in that column is shown only when additional event details are available.

---

### Procedure

---

- Step 1** In the circuit monitoring workspace, select an OTN circuit from the circuit list.
- The circuit detailed service list panel opens, showing topology, path information, and available tabs including service history.
- Step 2** Click the **Service History** tab to view the event log for the selected circuit.
- The event table displays these columns:
- **Timestamp:** The date and time of the event (displayed in UTC)
  - **Event name:** A description of the event, such as protection state change or successful discovery
  - **Event type:** Classifies the event as success, info, or neutral
  - **More details:** A link to additional event details, if available
- You can resize columns by dragging the column header borders.
- The service event history table loads, showing all events recorded for the selected OTN circuit.
- Step 3** (Optional) Click the **Export** icon in the service history toolbar to export the event history.
- The event history is exported to an Excel file containing all event records currently visible in the table.
-

# Software Image Management and Upgrade

Table 37: Feature history

Feature Name	Release Information	Feature Description
Software Image Management and Upgrade (SWIMU) Enhancements	Release 26.1.1	SWIMU enhancements enables you to perform granular upgrades, allowing for the independent management of the Cisco Optical Software Manager (COSM) and its associated devices. Additionally, the Cisco Optical Network Controller (CONC) supports High Availability (HA) node upgrades, ensuring seamless transitions for redundant COSM instances.

The Software Image Management and Upgrade (SWIMU) is a Cisco Optical Network Controller application which provides a centralized interface for managing and orchestrating software upgrades across Cisco Optical Site Manager managing NCS1K and NCS2K devices. It streamlines the upgrade process, offering tools for image distribution, software activation, and commit operations.

The SWIMU app also provides you the option to backup and restore the nodes and Cisco Optical Network Controller database.

## Components of SWIMU

The SWIMU App is divided into these tabs:

- **Backup and Restore:**
  - **Node Backup and Restore:** Manages node backups and restores, including on-demand backups, uploading images to nodes, and group management.
  - **CONC Database Backup and Restore:** Manages CONC database backups and restores, allowing administrators to schedule backups, trigger on-demand backups, edit backup configuration, download backup files, and restore from backups.
- **Upgrade Orchestrator:**
  - **Node Software Upgrade:**
    - **Software Image Distribution Groups:** Create and manage groups for software image distribution.
    - **Image Distribution Jobs:** Schedule and monitor image distribution jobs to copy software images to nodes and subtended devices under those nodes.
    - **Software Activation Groups:** Create and manage groups for software activation.
    - **Software Activation Jobs:** Schedule and monitor software activation jobs to upgrade nodes and subtended devices .

### Benefits of Using SWIMU

Using SWIMU you can backup the node configuration database and upload it to external or internal SFTP servers. Files can be distributed and saved to and from the Cisco Optical Site Manager devices while providing granularity to the underlying devices. It helps in:

- **Centralized Management:** Provides a single interface for managing backups, restores, and upgrades.
- **Granular Control:** Allows detailed configuration of nodes used while scheduling a backup job on top of a node.
- **Manage Tasks:** It helps manage file storage, distribution, scheduling, and monitoring based tasks.
- **Efficiency:** The distribution and scheduling prevent network overload and ensure efficient operations.
- **Flexibility:** Supports ad hoc backups with detailed scheduling options.
- **Transparency:** Allows to track the progress with notifications to keep users informed of task statuses.
- **Long-term Storage:** Ensures backup files are stored for an extended period, with configurable storage options.




---

**Note** Granularity happens at the node level but not at the device which is under the node level. Restore can be done at the device level through Cisco Optical Site Manager nodal UI using the cross-launch option in Cisco Optical Network Controller **Nodes** or **SWIM** applications.

---

### SFTP Servers

There are two types of SFTP servers allowed for backup and restore purpose.

- **Internal SFTP server:** It is the default SFTP server provided by Cisco Optical Network Controller itself which stores the backup DB in Cisco Optical Network Controller database.
- **External SFTP servers:** You can configure for Cisco Optical Network Controller DB backup or restore as part of external server storage or upload.

### Types of Backup

There are two types of backup:

**Table 38: Backup Types**

On-Demand Backup	Scheduled Backup
Immediate Backup	Regular Intervals
User-Initiated	Automated Process

### Formula for Calculating External Backup Storage Size

To calculate the storage size required for backup for external and internal SFTP servers use the given formula:

#### External SFTP Server Storage Formula

Backup Storage Size = (Network Total Devices x Size of Device x Requested Archive Period) / Backup Reoccurrence

**Table 39: External SFTP Server Storage Formula Parameters**

Parameter	Description
<b>Network Total Devices</b>	The number of onboarded devices.
<b>Size of the Device</b>	The size of an individual device.
<b>Requested Archive Period</b>	The duration for which the backup files are stored in days
<b>Backup Reoccurrence</b>	The frequency of the backup collection for devices in days.

#### Internal SFTP Server Storage Formula

Backup Storage Size = ((Number of Small Nodes \* 4.7 MB) + (Number of Medium Nodes \* 4.85 MB) + (Number of Large Nodes \* 5.1 MB) + (Number of XL Nodes \* 5.4 MB)) \* 5

**Table 40: Internal SFTP Server Storage Formula Parameters**

Parameter	Description
<b>Small Nodes</b>	Small device - 4.6 MB /4.8 MB.
<b>Medium Nodes</b>	(4 degree ROADM or (2x1010-OLT, 1x1014 - device) ) - 4.8 MB / 4.9 MB
<b>Large Nodes</b>	(6-degree ROADM) - 5.1 MB
<b>XL (8-degree ROADM) Nodes</b>	5.4 MB



**Note** Minimum allowed job interval is hourly.

For an hourly job over a period of 10 hours, file retention is 5 per node.

((Number of small nodes \* 4.7 MB) + (Number of medium nodes \* 4.85 MB) + (Number of Large nodes \* 5.1 MB) + (Number of XL nodes \* 5.4 MB)) \* 5

#### Cleanup of Storage

The cleanup of the storage in SFTP servers will be done based on the memory threshold value set by the user during the configuration of the SFTP server. The minimum threshold value is 50 and this is specific to external SFTP servers only.

## Configure SFTP server

The Software Image Management and Upgrade (SWIMU) app relies on SFTP (Secure File Transfer Protocol) servers for storing and retrieving software images and backups. You can configure up to two external SFTP servers in addition to the default local SFTP server.

### Before you begin

Before configuring an external SFTP server, ensure the following requirements are met:

- **Write Permissions:** The remote path folder must have write permissions enabled, allowing the external user to perform uploads.
- **SSH Version Compatibility:** The SFTP server SSH version must be either 7.x or 8.x. Backups and uploads fail if the SSH version is incompatible.
- **Router Static Settings:** Configure router static settings for each node separately. See [Configure Static Route on Peer Devices](#) for detailed instructions.
- **Time Synchronization:** The Cisco Optical Network Controller VM time must be synchronized with the device backend time.

### Procedure

---

- Step 1** Click the **Configure SFTP Server** in the SWIMU app. The SFTP Servers configuration screen is displayed.
- Step 2** On the SFTP Servers configuration screen, click **Add**. The Add SFTP Server screen is displayed.
- Step 3** Enter the information:
- **SFTP Server Name:** A descriptive name for the SFTP server.
  - **IP Address:** The IP address of the SFTP server.
  - **Username:** The username for accessing the SFTP server.
  - **Password:** The password for the specified username.
  - **Remote Path:** The directory path on the SFTP server where software images and backups will be stored.
  - **Disk memory space utilisation threshold for file overwrite(%):** The percentage of memory threshold allowed for each SFTP server. The minimum threshold value is 50. Anything exceeding the threshold will be cleaned up.
- Step 4** Click **Check Connectivity Status**.  
Verify that the status displays **Connection Successfully Established** before saving the configuration.  
Connectivity status check creates the directory in the remote path if it does not already exist.
- Step 5** Click **Save**.
- Step 6** Select the target SFTP server and click **Edit** to modify SFTP server details.
- a) Modify the details.
  - b) Click **Check Connectivity Status**.

c) Click **Save**.

**Note**

Do not edit or delete an SFTP server while an active job is in progress using that server.

**Step 7** Select the target SFTP server and click **Delete** to delete an SFTP server.

**What to do next**

After configuring the SFTP servers, allow a few seconds for the refresh process to complete. This delay is due to the SFTP server checking memory availability before connecting.

## Backup and Restore Nodes

Node Backup and Restore enables administrators to create and manage backups of individual nodes in the network. This feature is crucial for disaster recovery and ensuring data integrity. It allows administrators to perform on-demand backups, upload images to nodes, and organize nodes into backup/restore groups.

**Figure 51: Node Backup and Restore**

The screenshot shows the 'Node Software Upgrade' section of the Cisco Optical Network Controller. It features a table with 12 nodes and a map of Italy. The table columns are: Node Name, IP Address, Image Distribution Group Name, Job Name, Product Type, and Runn. The map shows nodes located in various parts of Italy, including Palermo, Messina, Salerno, Potenza, Catanzaro, Barletta, Bari, Brindisi, and Lecce. The interface also includes search and management options for nodes and groups.

Node Name	IP Address	Image Distribution Group Name	Job Name	Product Type	Runn
+ BARI	10.58.228.249	COSM_2K_group_10.58.228.98		COSM	25
+ BARLETTA	10.58.228.151	COSM_2K_group_10.58.228.98		COSM	25
+ BRINDISI	10.58.229.52	COSM 2K group 10.58.228.98		COSM	25

**Before you begin**

- For the backend upload to proceed you must configure the router static settings for each node separately. See [Configure Static Route on Peer Devices](#) for more details on how to configure the static routes of a node.
- The Cisco Optical Network Controller time must be the same as the device time.
- If a node backup fails, the [NODE-BACKUP-FAILURE](#) alarm is raised.

## Procedure

### Step 1

Create a nodes group

- Click **Backup, Restore and Group Management > Manage Groups > Create Group**
- Enter the **Group Name** and **Description** and click **Save**.
- Select the nodes from the **Nodes** table.
- Click **Manage Groups** and click + next to the group name to add the nodes.

#### Note

- You can also click and select any node from the **Topology** screen on the right and click the + icon appearing on top of the node and click **Update**. This will add these nodes to the group.
- Before scheduling backup jobs, you need to create a node group using the **Manage Groups** option.

### Step 2

Select a node and use options **Upload to Node** or create **On-Demand Backup** or **Manage Groups** and **Remove from Groups** by clicking each one of them.

- Before restoring the nodes you can click on **Upload to Node** option for initiating file transfer of backup files from Cisco Optical Network Controller's internal or external storage. Cisco Optical Network Controller automatically selects files for that node, based on the file name.
- You can cross launch to COSM nodal UI from any node in the **Node** table using the cross-launch option when you want to do the restoration.

- For scheduling the **On-Demand Backup** jobs. Click **On-Demand Backup** after selecting the nodes.  
This will schedule the on-demand jobs in the **Backup -Jobs** scheduler.

- Click **Remove from Groups** after selecting the nodes that you want to remove from the group.

### Step 3

Click **Jobs** to view the job summary and scheduler panel.

- Click **Schedule Backup** to schedule backup jobs.

Enter the **Job Name**, **SFTP Server**, **Groups**, **Start Date Time**, **Recurrence**, and **Description** and click **Schedule**.

#### Note

**Recurrence** option allows you to repeat the job scheduling based on **Hourly/Daily/Weekly/Monthly** intervals. The scheduling can be done using the current time + five minutes after the first occurrence.

- Click **Edit** to edit the schedule of the existing scheduled backup jobs.
- Click **Delete** to delete the selected job from the backup scheduled job list.
- Click **Refresh** to refresh the job scheduler table.

#### Note

You can track the status of each scheduled job in back up job list using the **Status** column in the table. The **Status** can be **Not Started** or **In progress** or **Completed** or **Failed**.

- If a backup or restore job fails, review the error message in the **Jobs** section.
- Ensure that the SFTP server is properly configured and accessible.

- Verify that the node is online and reachable.
- 

## Backup and Restore Database

**CONC Database Backup and Restore** enables administrators to create and manage backups of the Cisco Optical Network Controller database. This feature is crucial for disaster recovery and ensuring data integrity. It allows administrators to schedule backups, trigger on-demand backups, edit backup configurations, download backup files, and restore from existing backups.

The **CONC Database Backup and Restore** tab contains these components:

- **Backup Table:** Lists existing Cisco Optical Network Controller database backups with details such as:
  - **Name:** A unique identifier for the backup.
  - **Creation Time (UTC):** The date and time the backup was created.
  - **File Size:** The compressed and uncompressed size of the backup file.
  - **Created By:** The entity that initiated the backup (e.g., Controller system, internal).
  - **Download Status:** Indicates whether the backup has been downloaded.
  - **Restore Status:** Indicates whether a restore operation is in progress.
  - **Type:** Indicates the type of backup (delta or full).
    - **Full backup** is a complete backup of the entire Cisco Optical Network Controller database. It is taken every 7 days or after a fresh or new installation.
    - **Delta backup** is an incremental backup that captures only the changes (the difference) made to the Cisco Optical Network Controller database since the last full backup. Delta backups are taken daily at 12 AM by default, and this time and recurrence is modifiable. Hourly Recurrence can be every 6 or 12 hours and Daily recurrence can be 1, 2, or 3 days.
- **Action Buttons:** Provides the following actions:
  - **Edit configuration:** Allows editing of backup settings or scheduling.
  - **On-demand backup:** Manually triggers a new database backup.
  - **Download:** Downloads a selected backup file to Cisco Optical Network Controller VM(disabled unless a backup is selected).
  - **Restore:** Restores the Cisco Optical Network Controller database from a selected backup (disabled unless a backup is selected).
- **Scheduling Information:** Displays the next scheduled backup time.

### Before you begin

- The Cisco Optical Network Controller Database Backup and Restore feature relies on a properly configured SFTP server.

- Ensure that the SFTP server has sufficient storage space for the backups.
- If a backup fails, the [BACKUP-FAILURE](#) alarm is raised.
- If the upload of a backup to the SFTP server fails, the [UPLOAD-FAILURE](#) alarm is raised.

## Procedure

### Step 1

Perform an **On-demand** backup.

- Navigate to **Backup and Restore > CONC Database Backup and Restore**.

**Figure 52: Node Backup and Restore**

Software Image Management and Upgrade [Backup and Restore](#) Upgrade Orchestrator 04/17/2025, 06:27:47 (UTC)

Node Backup and Restore [CONC Database Backup and Restore](#) Next backup is scheduled at 04/18/2025 00:00:00 (UTC)

26 Backups Last Updated on 04/17/2025 at 06:25:42 Refresh Export 🔗

[Edit configuration](#) [On-demand backup](#) [Download](#) [Restore](#)

Name	Creation Time (UTC)	File Size	Created By	Download Status	Restore Status
base_000000050000000400000041	04/17/2025 00:00:09	20.4 MB (167.1 MB Uncompressed)	Controller system		
base_0000000500000003000000DF_D_0000000500000003000000B9	04/16/2025 00:00:00	14.6 MB (183.6 MB Uncompressed)	Controller system		
base_0000000500000003000000B9	04/15/2025 00:00:07	13.9 MB (107.6 MB Uncompressed)	Controller system		
base_0000000500000003000000A7_D_0000000500000003000000A5	04/14/2025 00:00:47	0.3 MB (2.0 MB Uncompressed)	Controller system		
base_0000000500000003000000A5_D_0000000500000003000000A3	04/13/2025 00:00:00	0.3 MB (1.8 MB Uncompressed)	Controller system		
base_0000000500000003000000A3	04/12/2025 00:00:13	8.3 MB (47.6 MB Uncompressed)	Controller system		
base_000000040000000300000005E_D_00000004000000030000002B	04/11/2025 00:00:00	28.3 MB (380.3 MB Uncompressed)	Controller system		
base_00000004000000030000002B	04/10/2025 00:00:00	21.7 MB (185.8 MB Uncompressed)	Controller system		

- Click **On-demand backup** and confirm by clicking **OK**.

#### Note

You can perform up to 10 On-demand backups per day.

A new database backup is created and the backups table is updated to show this new backup.

### Step 2

Download the database

- Navigate to **Backup and Restore > CONC Database Backup and Restore**.
- Select the backup you want to download from the table.
- Click **Download**.

#### Note

Cisco Optical Network Controller does not allow manual deletion of backups. Backups older than the retention period are automatically deleted.

- d) Enter a prefix string to be part of the downloaded file name and click **OK**.  
This prefix allows you to easily identify a backup file.
- e) Access Cisco Optical Network Controller VM CLI using SSH.
- f) Go to the path `/data/local-path-provisioner/pvc-*conc-database-backup*` to view the downloaded file.

### Step 3 Restore the database

- a) Navigate to **Backup and Restore > CONC Database Backup and Restore**.
- b) Select the backup you want to restore from the table.
- c) Click **Restore** and confirm the operation.

The Cisco Optical Network Controller database is restored from the selected backup.

### Step 4 Edit the backup configuration

- a) Click **Edit configuration**.
- b) Choose your **Preferred Backup Time (UTC)** and **Recurrence** preferences.
- c) Choose **Backup file retention time (weeks)** and set **Password to secure backup files**.

Cisco Optical Network Controller does not allow manual deletion of backups. Backups older than the retention period are automatically deleted.

- d) Enable the check box if you want to **Copy the backup files to SFTP server** and enter the SFTP Server details.
  - **SFTP Server Name:** A descriptive name for the SFTP server.
  - **IP Address:** The IP address of the SFTP server.
  - **Username:** The username for accessing the SFTP server.
  - **Password:** The password for the specified username.
  - **Remote Path:** The directory path on the SFTP server where software images and backups will be stored.
  - **Disk memory space utilisation threshold for file overwrite(%):** The percentage of memory threshold allowed for each SFTP server. The minimum threshold value is 50. Anything exceeding the threshold will be cleaned up.
- e) Click **Apply**.

### Step 5 Upload a downloaded backup file bundle to another Cisco Optical Network Controller instance.

- a) Extract the downloaded backup bundle using the following command.

```
tar -zxvf <downloaded_file_name>
```

#### Note

This step is not required if your backup file is copied from the external SFTP server.

This command extracts all the required delta and full backup files.

- b) Run the following command to generate the decryption key using your password.

```
printf "user_password" | od -A n -t x1 | tr -d ' \n' | awk '{printf "%-64s", $0}' | sed 's/ /0/g'
```

Replace `user_password` with your actual password in the command.

This command generates a 64-character key required for decryption.

- c) Decrypt the backup file using the generated key using the following command.

```
openssl enc -d -aes-256-ecb -in <encrypted_backup_file_name.tar.gz> -out  
<decrypted_backup_file_name.tar.gz> -K <key>
```

Replace the placeholders with actual file names and key.

This command generates the decrypted backup file.

- d) Upload the decrypted backup file to the Cisco Optical Network Controller server using the following sedo command.

```
sedo backup upload <decrypted_backup_file_name.tar.gz>
```

- e)

---

## Orchestrate Upgrades

Use the upgrade Orchestrator to distribute images to the nodes and activate the images on the nodes.

Cisco Optical Network Controller uses Software Image Distribution Groups and Software Activation Groups to distribute images and upgrade nodes in bulk.

### Before you begin

- For the backend upload to proceed you must configure the router static settings for each node separately. See [Configure Static Route on Peer Devices](#) for more details on how to configure the static routes of a node.
- The Cisco Optical Network Controller time must be the same as the device time.
- You must download the golden ISO from [software.cisco.com](http://software.cisco.com) and place it in the external SFTP server.
- **Image Authenticity:** Cisco Optical Network Controller does not validate the authenticity of the Golden ISO image. It is your responsibility to ensure the image is valid and trustworthy.
- **Number of Images:** There is no set limit to the number of images that can be uploaded to the local SFTP server. We recommend you store up to 5 iso images in the local sftp server.
- Software Image Distribution Groups and Software Activation Groups tables display the current software version only if CONC was used to upgrade the software in the node.

### Procedure

---

#### Step 1

Upload ISO Images to the Local SFTP Server.

- a) **Verify File Availability:** To check if a file is available on the local SFTP server, use the following command:

```
sedo object-store list onc-sw-iso
```

- b) **Upload an ISO Image:** To upload an ISO image to the local SFTP server, use the following command:

```
sedo object-store put <file> <destination> [flags]
```

- **<file>:** The path to the ISO image file on your local system.
- **<destination>:** The destination path on the SFTP server, including the bucket name and desired file name.

**Example:** `sedo object-store put <image-name.giso> onc-sw-iso/<image-name.giso>`

- c) **Delete a File:** To delete a file from the local SFTP server, use the following command:

```
sedo object-store bucket delete onc-sw-iso/<file-name>
```

- <file-name>: The name of the file to delete.

Example: `sedo object-store bucket delete onc-sw-iso/test.iso`

## Step 2 Create Image Distribution Groups.

- Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade > Software Image Distribution Groups**

**Figure 53: Upgrade Orchestrator**

- Click **Actions** and select **Expand all** to expand nodes in the table to view the subtended devices under the node.
- Click **Manage Groups** and select **New Group**.

You can also Manage groups from the topology view in the **Upgrade Orchestrator**.

- Enter a Group Name and Description.
- Select the nodes to include in the group and click **Manage Groups**.
- Click the + icon next to a group name to add the nodes to the group.
- Select a node and click **Remove from groups** to remove the node from the group it is a member of.

### Note

Groups for NCS 2000 nodes are autogenerated by Cisco Optical Network Controller.

You cannot delete the autogenerated NCS 2000 groups. You can edit the name and description of the autogenerated NCS 2000 groups.

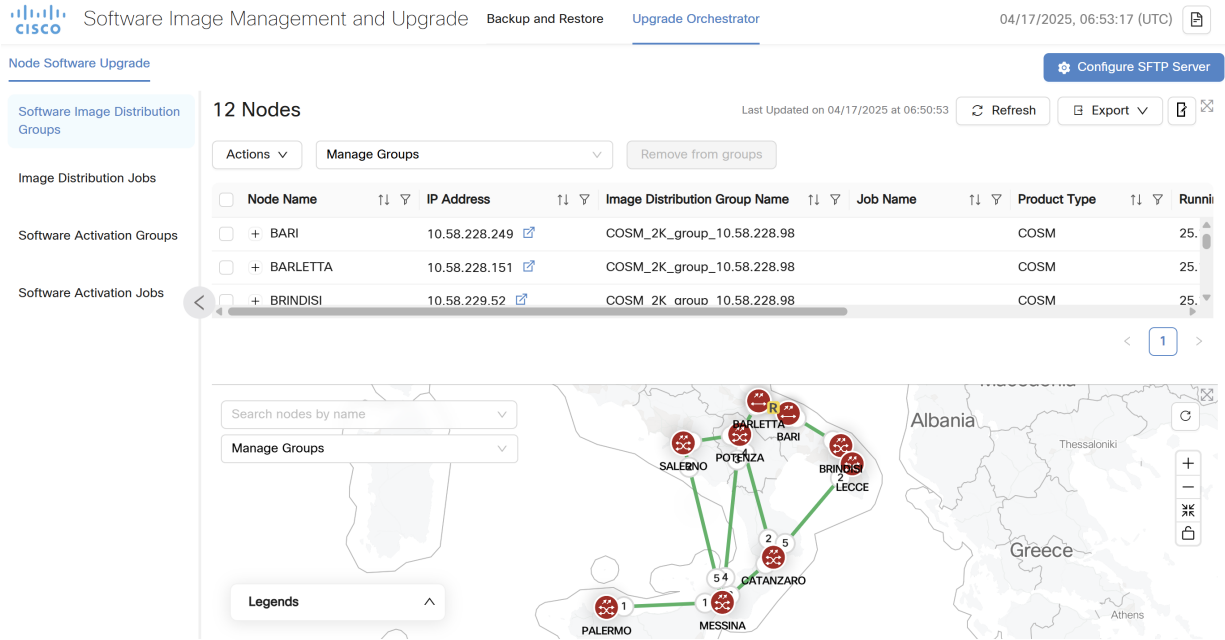
You cannot add the autogenerated NCS 2000 nodes to NCS1000 groups or NCS1000 nodes to NCS 2000 autogenerated groups.

## Step 3 Create an Image Distribution Job.

- Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade > Image Distribution Jobs**

- b) Click **Distribute Image**.
- c) Select the nodes or groups you want to distribute the images to.

**Figure 54: Upgrade Orchestrator**



**Table 41: Select node(s) or group(s) options**

UI options	Actions
Copy only to COSM radio button	Copies the image to Cisco Optical Site Manager only  <b>Note</b> COSM NCS 1000 Series: Image is copied to hosting device(s) automatically. COSM NCS 2000 Series: Image is copied to the COSM only.
Copy to COSM and device(s) under node radio button	Copies images to Cisco Optical Site Manager and sub-tended devices.
Group(s) or Node(s) search bar	Displays the list of node groups
Back	Goes back to the <b>Orchestrator Upgrade</b> tab.
Next	Moves to the next step.

- d) Select an SFTP server from the drop-down list or give the details of the SFTP server.
- e) Select the ISO image file to distribute.
- f) Schedule the job to start immediately or later.
- g) Click **Schedule** and choose a later time or schedule the job to run immediately.
- h) Click the status for a device in the status column to view detailed status.

- i) Select a job and click **Stop** to stop the job in the nodes in which the job has not started.  
The job continues on the nodes on which it was in progress.
- j) Select a job and click **Edit** to make changes to the job.  
A job that is in progress cannot be edited.
- k) Select a job and click **Delete** to delete a job that has completed or failed.

**Note**

The image distribution job table has an additional column **Type** to indicate the granular type of job.

**Note**

For NCS 2000 nodes, Image distribution takes place for all nodes in a group. You cannot select a subset of nodes to distribute images.

If a job status is **PARTIAL**, it means the job succeeded for some of the nodes, but failed for other nodes in the group of devices that the job was initiated for.

If a job fails, fix the issues in the failure status and click **Re-Run**.

**Step 4** Create Software Activation Groups.

- a) Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade > Software Activation Groups**

**Figure 55: Upgrade Orchestrator**

The screenshot displays the Cisco Upgrade Orchestrator interface. The top navigation bar includes 'Software Image Management and Upgrade', 'Backup and Restore', and 'Upgrade Orchestrator'. The current page is 'Node Software Upgrade', with a 'Configure SFTP Server' button in the top right. The main content area shows a table of 11 nodes and a topology map below it.

Node Name	IP Address	Activation Group Name	Job Name	Product Type	Current SW version	Previous SW version	Version be
+ Node_1	10.58.252.189			COSM	25.1.1.P2D0400		
+ Node_10	10.58.252.194			COSM	25.1.1.P2D0400		
+ Node_11	10.58.252.199			COSM	25.1.1.P2D0400		
+ Node_2	10.58.252.190			COSM	25.1.1.P2D0400		
+ Node_3	10.58.252.191			COSM	25.1.1.P2D0400		
+ Node_4	10.58.252.192			COSM	25.1.1.P2D0400		
+ Node_5	10.58.252.195			COSM	25.1.1.P2D0400		
+ Node_6	10.58.252.196			COSM	25.1.1.P2D0400		
+ Node_7	10.58.252.197			COSM	25.1.1.P2D0400		
+ Node_8	10.58.252.198			COSM	25.1.1.P2D0400		

The topology map below the table shows a geographical distribution of nodes across Europe, with several nodes highlighted in red, indicating a specific group or status. The map includes labels for various countries and cities such as Ireland, London, Paris, Munich, Berlin, Poland, Slovakia, Ukraine, Romania, Bulgaria, Greece, Turkey, and others.

You can also Manage groups from the topology view in the **Upgrade Orchestrator**.

- b) Click **Actions** and select **Expand all** to expand nodes in the table to view the individual devices.
- c) Click **Manage Groups** and select **New Group**.
- d) Enter a Group Name and Description.

- e) Select the nodes or individual devices to include in the group and click **Manage Groups**.
- f) Click the + icon next to a group name to add the nodes to the group.
- g) Select a node and click **Remove from groups** to remove the node from the group it is a member of.

**Note**

Groups for NCS 2000 nodes are autocreated by Cisco Optical Network Controller.

You cannot delete the autocreated NCS 2000 groups. You can edit the name and description of the autocreated NCS 2000 groups.

You cannot add the autocreated NCS 2000 nodes to NCS1000 groups or NCS1000 nodes to NCS 2000 autocreated groups.

**Step 5** (Optional) Copy a group to **Software Activation Groups** from **Software Image Distribution Groups**.

- a) Click **Software Image Distribution Groups > Manage Groups**
- b) Click the copy button next to a group name.
- c) Click **Software Activation Groups > Manage Groups**
- d) Click **Paste** at the top right corner.

**Step 6** Create a Software Activation Job.

- a) Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade > Software Activation Jobs**
- b) Click **Activate Software**.
- c) Select the target devices or groups.

**Table 42: Select Groups or Nodes or Devices options**

UI options	Actions
<b>Activate only COSM</b> radio button	<p>Activates only Cisco Optical Site Manager</p> <p><b>Note</b>            COSM NCS 1000 Series: This activation job automatically performs an upgrade of hosting device(s) as well.            COSM NCS 2000 Series: Only COSM is activated.</p>
<b>Activate both COSM and Device(s)</b> radio button	<p>Activates both Cisco Optical Site Manager and the selected subtended device(s). The activation job upgrades Cisco Optical Site Manager and selected subtended device(s).</p> <p><b>Note</b>            COSM NCS 1000 Series: The NCS 1000 hosting device(s) will be auto-selected if you have not selected the hosting device(s).            COSM NCS 2000 Series: Activation of both Cisco Optical Site Manager and device(s) works based on the selected subtended device(s).</p>

UI options	Actions
<b>Activate only Device(s)</b>	<p>Activates only the selected subtended device(s). The activation job upgrades the subtended device(s) software version.</p> <p><b>Note</b>            COSM NCS 1000 Series: The NCS 1000 hosting device(s) will be auto-selected if you have not selected the hosting device(s).            COSM NCS 2000 Series: Activation of device(s) works based on the selected subtended device(s). If COSM is not upgraded to the same, this option first upgrades the COSM and then proceed with the subtended device(s).</p>
<b>Group(s) or Node(s) or Device(s) search bar</b>	Displays the list of nodes, devices and groups
<b>Back</b>	Goes back to the <b>Orchestrator Upgrade</b> tab.
<b>Next</b>	Moves to the next step.

Figure 56: Upgrade Orchestrator

The screenshot displays the Cisco Upgrade Orchestrator interface. At the top, it shows the Cisco logo and navigation tabs: "Software Image Management and Upgrade", "Backup and Restore", and "Upgrade Orchestrator". The date and time are "04/17/2025, 06:53:17 (UTC)".

The main section is titled "Node Software Upgrade" and shows "12 Nodes". A table lists the nodes with columns for Node Name, IP Address, Image Distribution Group Name, Job Name, Product Type, and Runni. The visible nodes are:

Node Name	IP Address	Image Distribution Group Name	Job Name	Product Type	Runni
+ BARI	10.58.228.249	COSM_2K_group_10.58.228.98		COSM	25
+ BARLETTA	10.58.228.151	COSM_2K_group_10.58.228.98		COSM	25
+ BRINDISI	10.58.229.52	COSM_2K_group_10.58.228.98		COSM	25

Below the table is a map of Italy with nodes marked as red circles with numbers. The nodes shown on the map are PALERMO (1), MESSINA (1), SALERNO (1), POTENZA (2), BARLETTA (2), BARI (2), BRINDISI (2), LECCE (2), and CATANZARO (5). The map also shows neighboring countries like Albania and Greece, and cities like Thessaloniki and Athens.

**Note**

After you click **Next**, based on the selection of the radio button related to activation target, an **Information** message appears explaining the goal of the job.

Figure 57: Upgrade Orchestrator

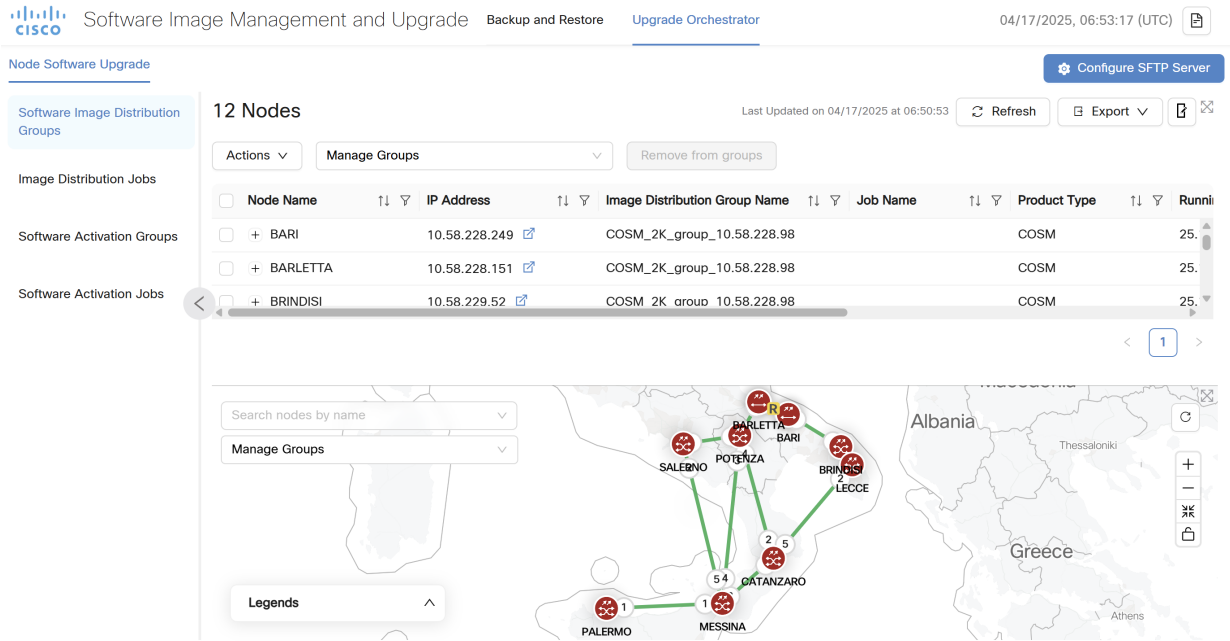


Figure 58: Upgrade Orchestrator

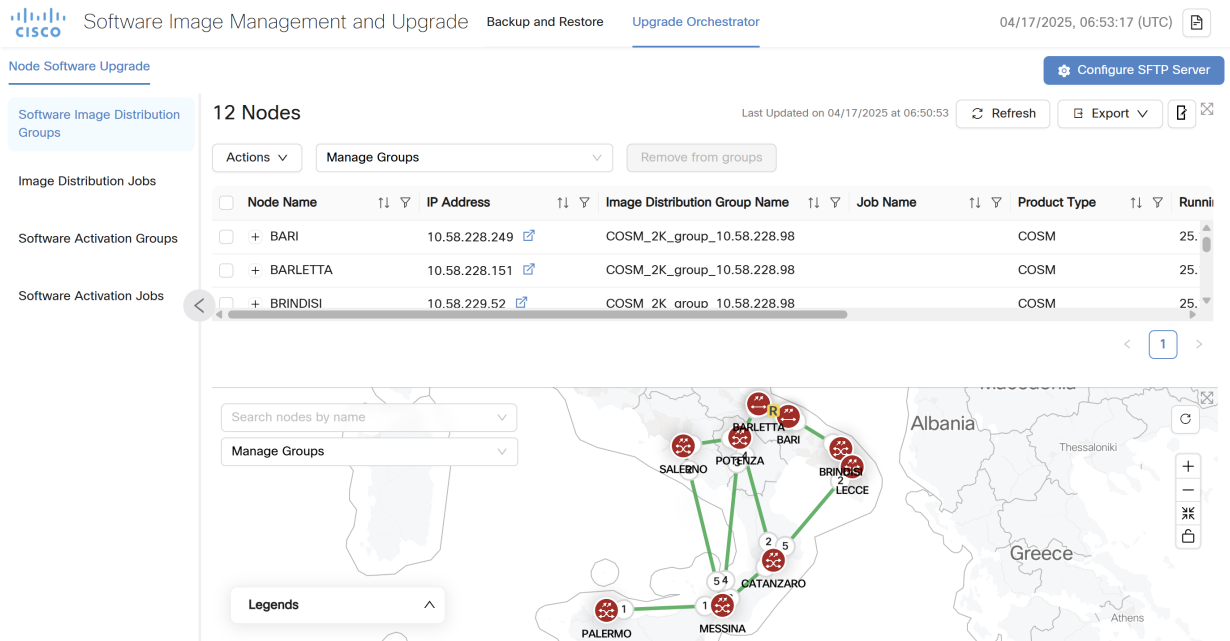


Figure 59: Upgrade Orchestrator

The screenshot displays the Cisco Upgrade Orchestrator interface. At the top, it shows the Cisco logo and navigation tabs: "Software Image Management and Upgrade", "Backup and Restore", and "Upgrade Orchestrator". The current date and time are "04/17/2025, 06:53:17 (UTC)". Below the navigation, there's a "Node Software Upgrade" section with a "Configure SFTP Server" button. A sidebar on the left lists various software management tasks. The main area features a table titled "12 Nodes" with columns for Node Name, IP Address, Image Distribution Group Name, Job Name, Product Type, and Runni. Below the table is a map of Italy with nodes marked as red circles with numbers, connected by green lines. A legend and search box are also visible.

Node Name	IP Address	Image Distribution Group Name	Job Name	Product Type	Runni
+ BARI	10.58.228.249	COSM_2K_group_10.58.228.98		COSM	25
+ BARLETTA	10.58.228.151	COSM_2K_group_10.58.228.98		COSM	25
+ BRINDISI	10.58.229.52	COSM 2K aroup 10.58.228.98		COSM	25

- d) Choose the software package from the drop-down.
- e) Schedule the job to start immediately or later.
- f) Click **Schedule** and choose a later time or schedule the job to run immediately.
- g) Click the status for a device in the status column to view detailed status.

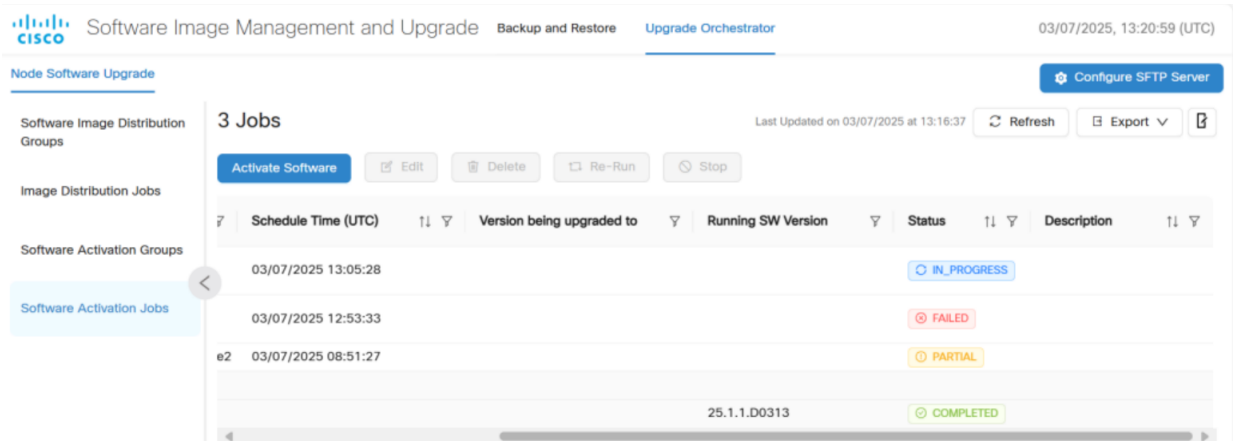
Expand the jobs displayed in a hierarchical manner to find the device activation status for every node and respective subtended devices.

- h) Select a job and click **Stop** to stop the job in the nodes in which the job has not started.  
The job continues on the nodes on which it was in progress.
- i) Select a job and click **Edit** to make changes to the job.  
A job that is in progress cannot be edited.
- j) Select a job and click **Delete** to delete a job that has completed or failed.

#### Note

The software activation jobs table has an additional column **Type** to inform about the *Activation Type*.

Figure 60: Upgrade Orchestrator



If a job status is **PARTIAL**, it means the job succeeded for some of the nodes, but failed for other nodes in the group of devices that the job was initiated for.

If a job fails, click **Troubleshoot** in the failure status to cross launch the site manager.

For NCS 2000 devices, the diagnostics page of site manager is launched. Use the logs to troubleshoot the failure.

For NCS 1000 devices, the devices tab is launched. Use the CLI to troubleshoot the failure.

**Note**

After troubleshooting the failure, click **Re-Run**.

## PM History

Table 43: Feature history

Feature name	Release information	Feature description
PM history support for the AR-MXP cards	Release 26.1.1	<p>PM history data collection is supported for the SONET and SDH interfaces type for the AR-MXP, AR-XP and AR-XPE cards. These UI enhancements are made to support the SONET and SDH interfaces of AR-MXP cards.</p> <ul style="list-style-type: none"> <li>PM browse: Added <i>sonet</i> and <i>sdh</i> interfaces in the <b>Interface</b> type drop-down list.</li> <li>PM jobs: To schedule PM jobs for AR cards, select <b>Interfaces</b> and enter <i>AR</i> in the <b>Equipment, Shelves, Cards, and Port</b> field.</li> </ul>

The Cisco Optical Network Controller 24.3.1 release includes a new application called PM History. The PM history application is made available in **Network Monitoring** workspace and it interacts with **Topology** for

links. It is also available in the **Service Monitoring** workspace interacting with the **Detailed Service Path** if circuits are available.

### Purpose of Implementing PM History Application

The **PM History** application allows you to view and generate PM history data reports for interfaces that are part of the nodes. For the sequential selection of each parameters in the order of nodes, interval, selected date time range, interface types, port name and locations.

### Benefits of Using PM History

The benefits of using **PM History** are given in the table.

*Table 44: Benefits of PM History*

Benefit	Description
<b>Enhanced Data Visibility</b>	You can now view detailed PM History reports with customizable options.
<b>Improved Network Monitoring</b>	New portlets and enhanced dashboards provide better insights into network performance.
<b>Extended Data Retention</b>	Archiving allows for long-term data analysis and historical reporting.
<b>Automated Reporting</b>	The PM job scheduler automates the generation and distribution of historical PM reports and helps improve the overall efficiency.
<b>User-Friendly Interface</b>	The standalone PM application and enhanced workspaces offer a more intuitive and responsive user experience.

### Time Range for Fetching Data

You can pick the start date or time and the end date or time based on the data stored in Cisco Optical Network Controller, for active and archive data by using the date-time input picker. The different time range options available for fetching the data are listed in the table.

Options	Description
Interval	Choose 15-min or 24-hours PM data
Range	Choose the time range for the PM history collection data
Select Time	Set start and end date for PM history collection using date picker

Table 45: Time Range for Fetching Data

Time Range	Limit
<b>PM Data Interval for 15 mins</b>	Active data retention—2 days + current day Archive data retention—29 days <b>Note</b> Archive data retention limit is on top of the active data retention limit, that is, 29 days before the active data retention days.
<b>PM Data Interval for 24 hours</b>	Active data retention—93 days + current day Archive data retention—87 days <b>Note</b> Archive data retention limit is on top of the active data retention limit, that is, 87 days before the active data retention days.

### Port Details

The **Port Details** area displays these drop-down lists.

From R26.1.1.1, the PM browser supports the SDH and SONET interface types.

Drop-down list	Description
Interface types	Type of interface on the ports. <ul style="list-style-type: none"> <li>• opticalTransport</li> <li>• opticalChannel</li> <li>• otnOtu</li> <li>• otnOdu</li> <li>• ethernetCsmacd</li> <li>• sonet</li> <li>• sdh</li> <li>• zrPlus</li> </ul>
Port Name	Port label
Location	Location of the node from where the PM is being collected. <ul style="list-style-type: none"> <li>• near-end: The current node and current port.</li> <li>• far-end: The port to which the current port is connected to</li> </ul>

### Data Collection and Storage

PM data will be collected in 15 minutes and 24 hours time intervals from the onboarded COSM nodes and stored in a database. The data and activity logs are stored in the form of storage bins. The data is fetched based on what you choose as the start or end date and time values. Any data which is more than three months old is archived. Use the **Get Archive** option to get the archived PM History data.

### Types of PM History Reports

You can download the archived data in the form of 15-minute or 24-hour granularity report type. The PM History reports are of two types based on the different granularity levels and time intervals.

*Table 46: Types of PM History Report*

Type of PM History Report	Description
<b>15-Minute Granularity PM Report</b>	<ul style="list-style-type: none"> <li>• <b>Availability:</b> Real-time reports are accessible for up to one + current day, from the time the report is generated.</li> <li>• <b>Archiving:</b> Data is archived and accessible for up to active ( current day - 2 ) up to (current day - 32). Overall data is available for 32 days.</li> </ul>
<b>24-Hour Granularity PM Report</b>	<ul style="list-style-type: none"> <li>• <b>Availability:</b> Real-time reports are accessible for up to 31 days from the time the report is generated.</li> <li>• <b>Archiving:</b> Data is archived and accessible for up to 93 days from the time the report was first generated.</li> </ul>



#### Note

- For both 15-Minute or 24-Hour granularity PM report, you can use the horizontal scroll bar to adjust the dates as per your need. For 15-Minute granularity archive data is available for download from 3 to 31 days and for 24 hours granularity from 31 to 93 days.
- If the date range falls on archive data then you will receive a message to indicate the user has chosen a time range which coincides with the archived data time range.

Figure 61: 15-Minute Granularity PM Report

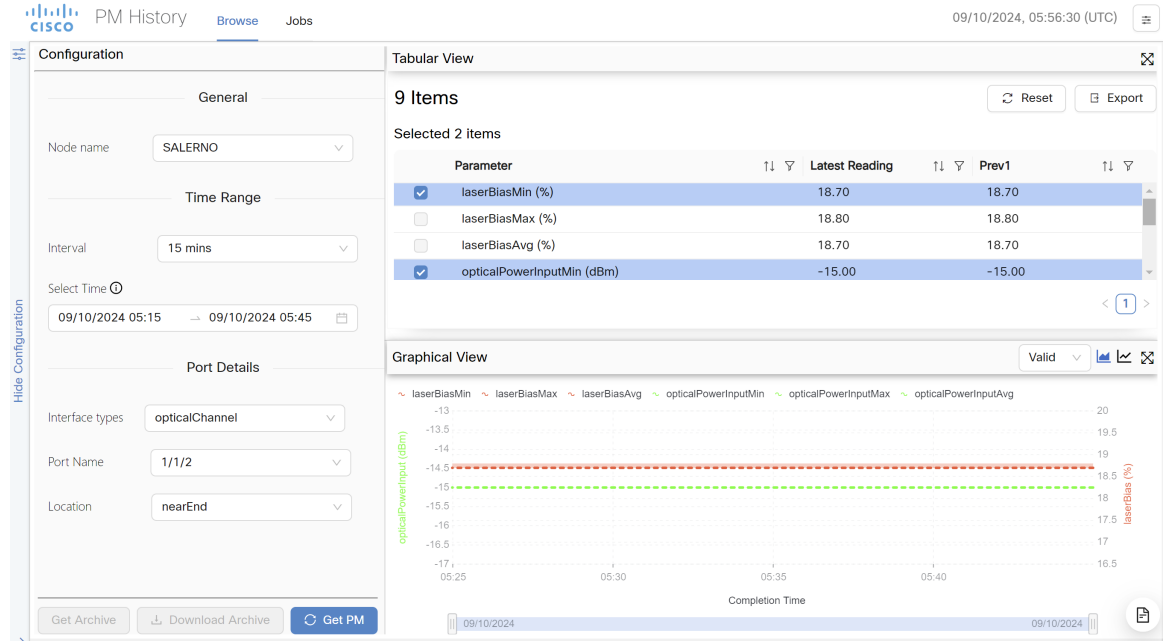
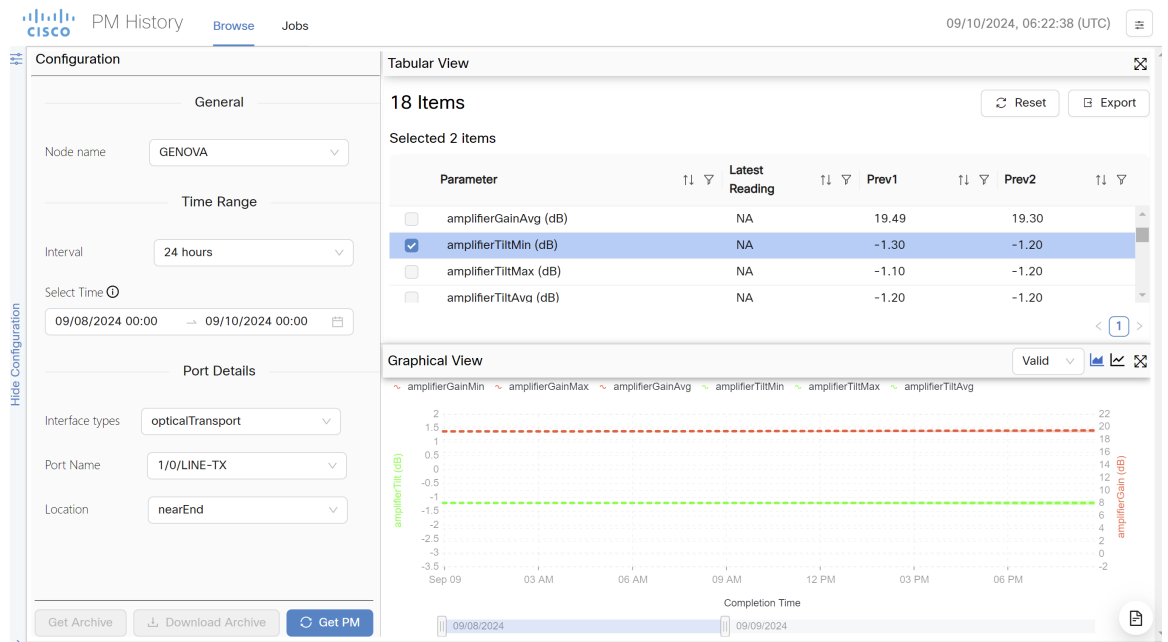


Figure 62: 24-Hour Granularity PM Report



Data Representation

The PM history data is also represented in a graphical format.

## PM Job Scheduler

The PM job scheduler manages the PM tasks as given:

- PM history.
- It generates one-time, daily, weekly, and monthly historical PM reports based on the job criteria and Cisco Optical Network Controller entities like circuits or services, links, and ports.



### Note

- **None**: one time applicable for both 15 minutes and 24 hours.
  - **Daily**: is applicable only for 15 minutes.
  - **Weekly** and **Monthly**: are applicable only for 24 hours.
- 
- Reports are sent through email which is configured through SMTP server and which are not password protected.

## PM History in Network Monitoring

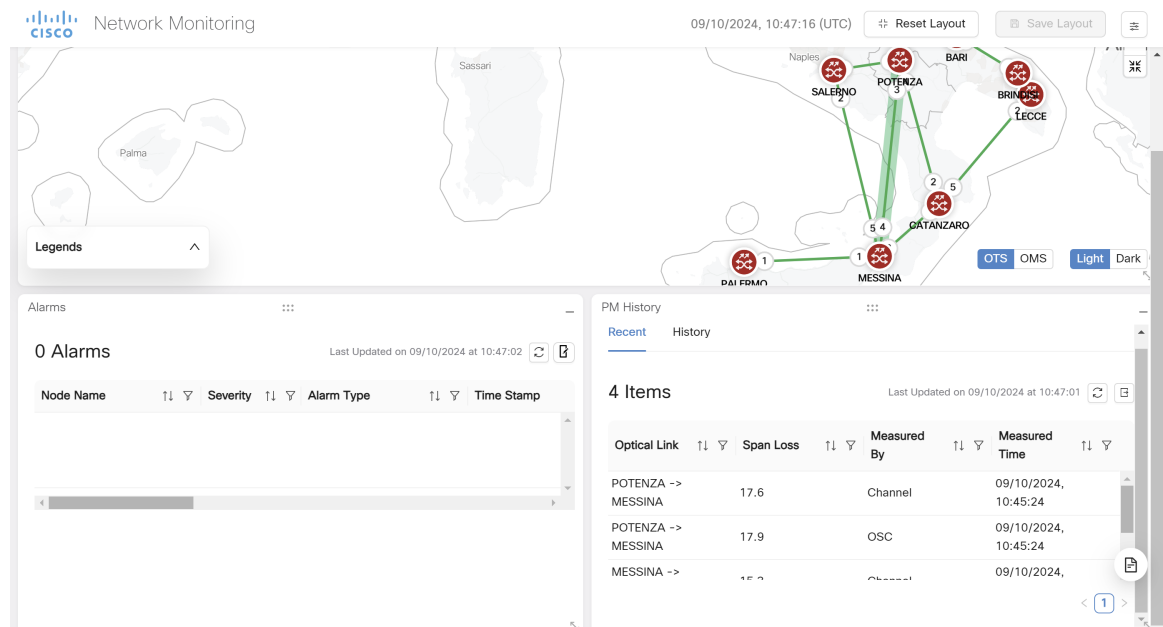
The **Network Monitoring** workspace now includes a new tab for PM History span loss reports, featuring both graphical and table representations. The dashboard display updates based on selections made in the **Topology** application and the user selected time range.



### Note

You must select the **OTS** link in the **Topology** application to view the spanloss values in the table.

**Figure 63: PM History in Network Monitoring**



## PM History in Topology

In the **Topology** application, the PM history tab:

- Interacts with the **Topology** application and its components.
- Helps in viewing the span loss changes and information.

## PM History in Circuit Monitoring

The **Circuit Monitoring** workspace will now feature a new dashboard in the detailed service path component, displaying PM History data. This new add-on dashboard has the **Detailed Service Path** component which displays the PM values based on selected port.

The historical data for a particular port from the **Detailed Service Path** can be seen for 15 minutes and 24 hours interval. You can also select the start and end date. PM values for ports are displayed in the tabular and graphical formats.



### Note

- Right click on the port on **Detailed Service Path** and use the option to launch PM History for that port. Also you can choose up to two ports.
- PM and PM history is enabled only after circuits are created on a node.
- Using *Interval* and *Select Time*, select the data range for Circuit Monitoring PM history data, based on the retention days.

**Figure 64: PM History in Circuit Monitoring**

PM History

Port: **SALERNO : 1/5/LINE-RX** Interval: **15 mins** Select Time: **09/10/2024 00:00** → **09/10/2024 10:15**

6 Items Export

Selected 2 items

Parameter	Latest Reading	Prev1	Prev2	Prev3	Prev4	Prev5	Prev6	Prev7	Prev8	Prev9	Prev10
<input checked="" type="checkbox"/> opticalPowerMin (dBm)	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10
<input type="checkbox"/> opticalPowerMax (dBm)	-11.00	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90
<input type="checkbox"/> opticalPowerAvg (dBm)	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00
<input checked="" type="checkbox"/> opticalPowerOscMin (dBm)	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40
<input type="checkbox"/> opticalPowerOscMax (dBm)	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30
<input type="checkbox"/> opticalPowerOscAvg (dBm)	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30

## Service Endpoint PM History Report

The PM History application jobs dashboard report in service endpoint helps in:

- Calculating and presenting total availability or outage time and percentage.
- Exporting to Excel and scheduling job options if available.

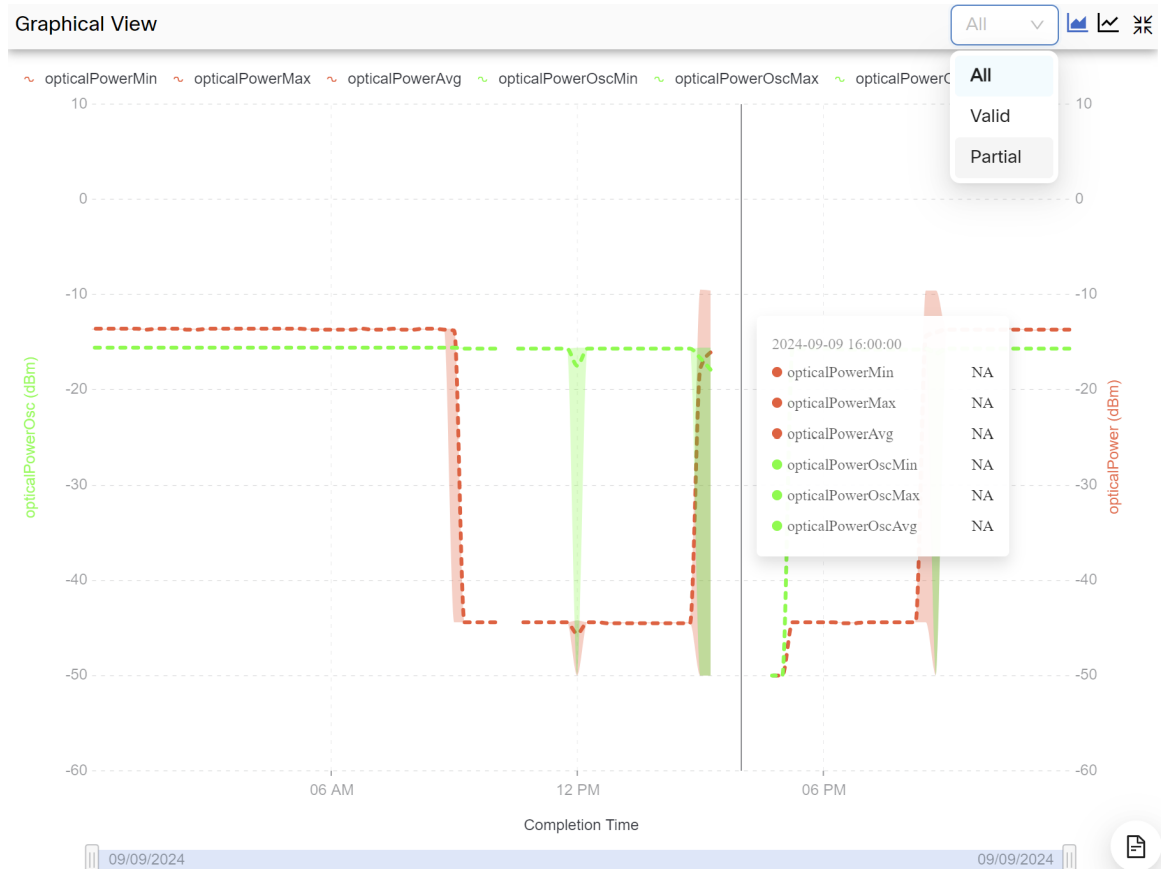
## Graphical Representation within PM History Application

The linear graph displays **ALL/VALID/PARTIAL** PM values. Also, the NA values do not have any representation in the graph.



**Note** Partial is represented in yellow.

**Figure 65: NA Values in Linear Graph**



## PM Data Retention

The PM retention configuration settings allow users to customize the period for which Performance Management (PM) data is stored. You can increment or decrement retention values for both 15-minute and 24-hour bucket data. These settings affect data availability across PM browse, jobs, and workspace history.

The **PM Data Retention** pane has these PM buckets.

- **15 Mins (Max Range 31 days):** PM data collected at 15-minute intervals.
- **Days to retain active data:** The number of days the system keeps the most recent, high-granularity data.

- **Days to retain archive data:** The number of days the system keeps historical data that has been moved to the archive.
- **24 hours (Max Range 180 days):** PM data collected at daily (24-hour) intervals.
- **Days to retain active data:** The number of days the system keeps the daily aggregated active data.
- **Days to retain archive data:** The number of days the system keeps the daily aggregated archive data.

Figure 66: PM Data Retention



Table 47:

Label	Setting Category	Data Type	Default Value	Valid Range
1	15 Mins Interval	Active Data	2 days	1–2 days
2	24 Hours Interval	Active Data	31 days	1–93 days
3	24 Hours Interval	Archive Data	93 days	1–149 days
4	15 Mins Interval	Archive Data	3 days	1–29 days

These are action buttons.

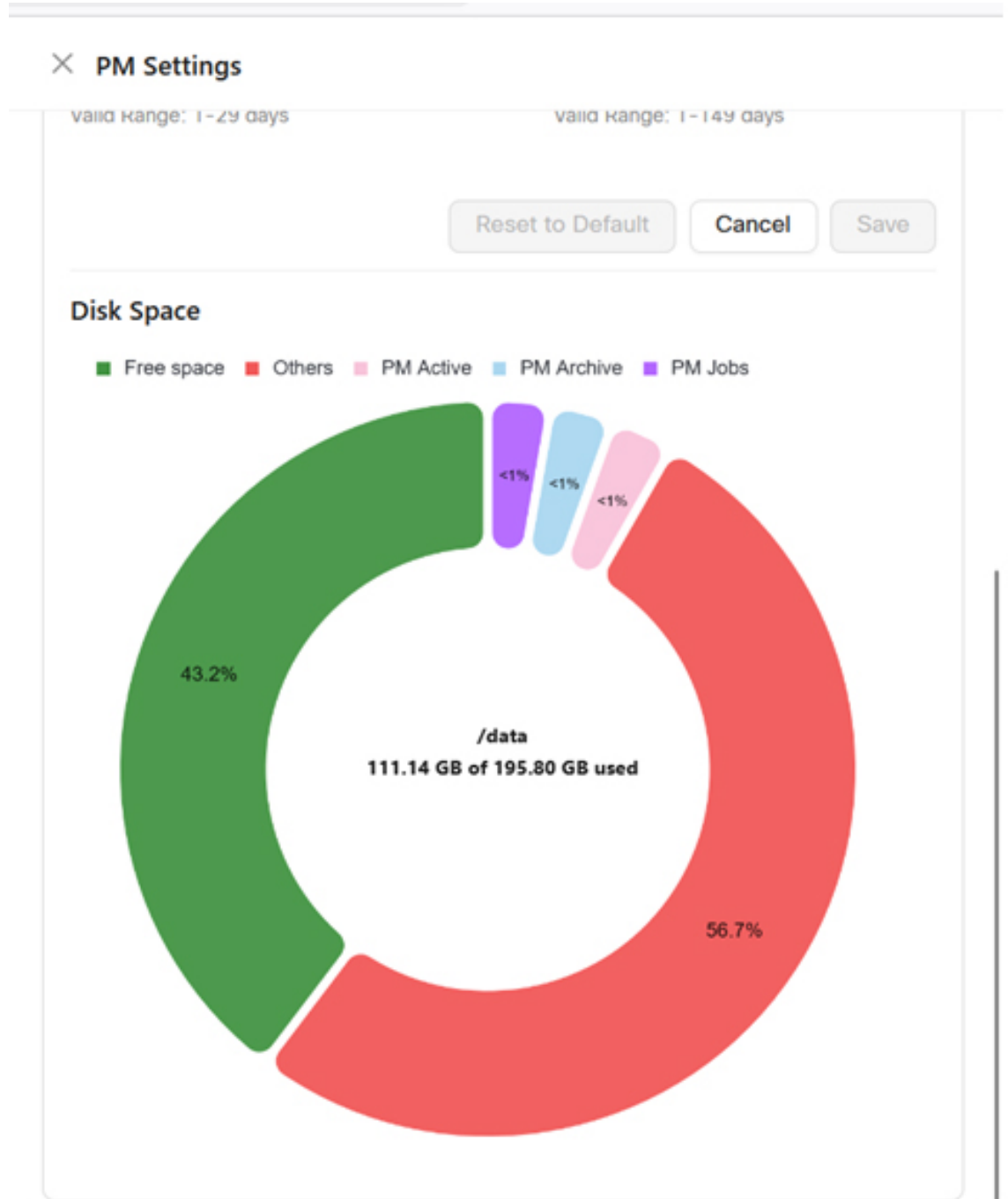
- **Reset to Default:** Restores data collection settings to their default state.
- **Cancel:** Discards any changes made to the PM data collection configuration.
- **Save:** Saves all configuration changes.

## Disk Space

The **Disk Space** pane shows the disk space usage for VMs in a pie chart.

- **Free Space:** Unused space is left in your VM.
- **Others:** Space used by files or data in the ONC VM other than PM data.
- **PM Active:** Space used by recent (active) PM data in Postgres.
- **PM Archive:** Space used by old (archived) PM data in Postgres.
- **PM Jobs:** Space used by PM job results and reports.

Figure 67: PM retention disk space



528644

### Charateresitics of PM data retention

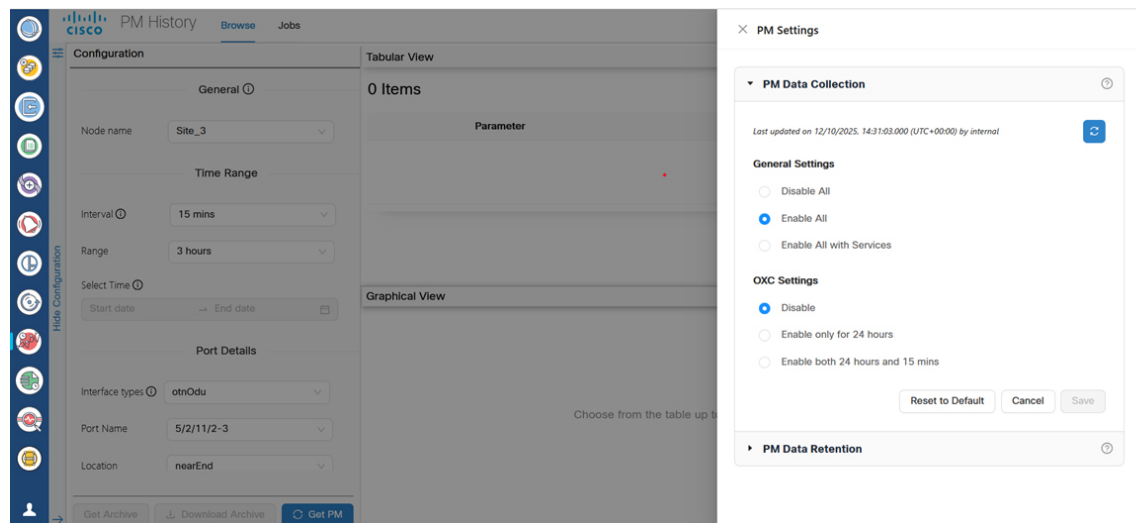
These are the characteristis of PM data retention.

- **Decrease of retention:** Reducing the retention period may cause existing jobs to fail. Jobs will move to the Paused state.
- **Increase of Retention:** Increasing the retention period increases disk space usage. For example, with 55 nodes and a retention period of 2 days (15-min), 180 days (24-hour), storage usage is 3.29 GB. Extending the retention period to 10 days (15-min), 180 days (24-hour) raises estimated storage usage to around 3.4 GB.
- **Threshold warning:** If the VM disk space utilization exceeds 80%, you cannot increase the retention period for performance metrics data. To extend retention, add storage or free up disk space.
- **PM Browse:** You can retrieve 15-minute interval PM data for up to 31 days, and 24-hour interval data for up to 180 days.
- **PM Jobs:** PM jobs update when you change the retention settings.
- **PM History Workspace:** The calendar in the circuit or link workspace changes when retention settings change. Based on the active 15 mins retention days + current day, for example, **PM History Active = 2 + Current Day**.
- **Multi-user login:** If user A updates retention values, user B in the same workspace receives a notification: "PM Data Retention has changed. Please refresh the page."

## PM Data Collection

PM Data Collection is the PM option that allows you to control the collection of performance metrics (PM) from various interface types. This option provides flexibility to enable or disable data collection for general interfaces and Optical X Connection (OXC) interfaces separately.

**Figure 68: PM History Data Collection**



### General Settings

- **Disable All:** Disables performance metric data collection for all general interfaces.
- **Enable All:** Enables performance metric data collection for all general interfaces.

- **Enable All with Services:** Enables data collection for all general interfaces except OXC and associated services.




---

**Note** In *General Settings*, **Enable All with Services** is the default option.

---




---

**Note** For the SONET/SDH PM data, it is not required to have circuits present. To view the PM counters, use the *Enable All* option in *General Settings*.

---

#### *OXC Settings*

- **Disable:** Disables data collection for OXC interfaces.
- **Enable only for 24 hours:** Enables OXC interface data collection for a 24-hour period.
- **Enable both 24 hours and 15 mins:** Enables OXC interface data collection for both 24-hour and 15-minute intervals.




---

**Note** In *OXC Settings*, **Disable** is the default option.

---




---

**Note** If you select **Disable** for general settings and **OXC** setting, everything will be disabled with no selection in the interface type.

If you select **Enable** for general settings and **OXC** setting, everything will be available in the interface selection.

If you select **Enable** for general settings and the **OXC** setting is **Disable**, then everything will present except **OpticalXConnection** will be hidden in the interface type selection.

If you select **Disable** for general settings and the **OXC** setting is **Enable**, then everything except **OpticalXConnection** will be present in the interface type selection.

---

These are action buttons.

- **Reset to Default:** Restores data collection settings to their default state.
- **Cancel:** Discards any changes made to the PM data collection configuration.
- **Save:** Saves all configuration changes.



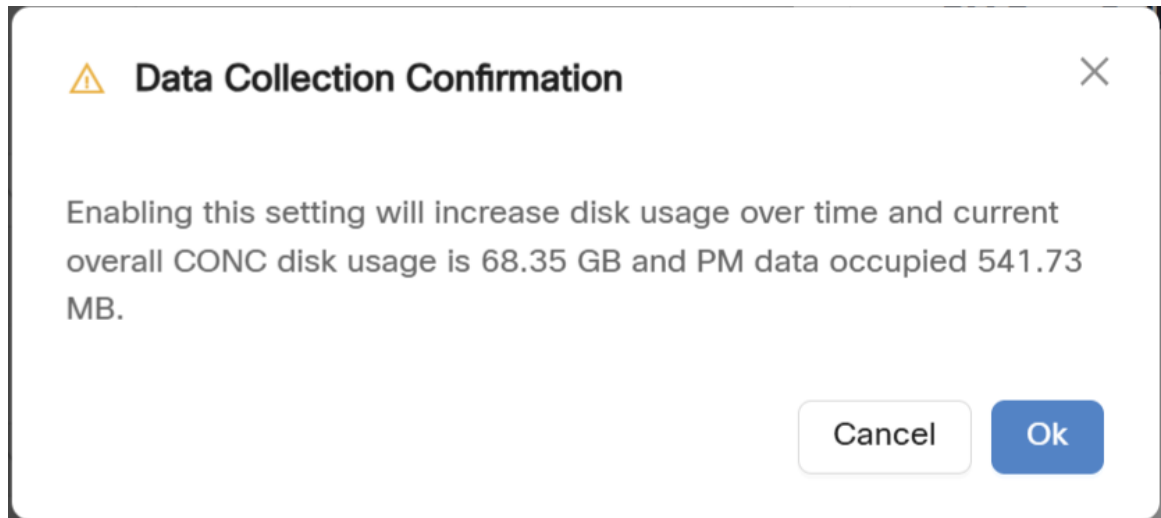

---

**Note** When you select **Enable All** in *General Settings*, then the **Data Collection Confirmation** message appears warning about disk space usage.

If the VM disk space usage exceeds 80%, you have to add storage or free up disk space.

---

Figure 69: PM History Data Collection



## Accessing PM History Report

To access the **PM History** tab follow the steps:

### Procedure

**Step 1** Click **PM History** option from the left panel.

To browse or view the general PM History details follow the steps given:

- a) Click **Browse** tab.
- b) Enter **Node name** and **Interval**. time range.
- c) **Select Time**. Select **Start date** and **End date**.
- d) Enter **Port Details** followed by **Interface types**, **Port Name** and **Location**.

#### Note

- The browse tab will open the **Configuration** screen where you can fetch the general PM History details in the tabular and graphical forms. You can choose to show or hide the configuration to see the expanded graphical and tabular view.
- Choose the required options for the PM History data collection using the **PM History Data Collection** option.
- To know more details about the **PM History Data Collection** click on the **i** icon. There are three options available here which are **Enable**, **Disable** and **Default**.

To browse or view the job scheduling details follow the steps given:

- a) Click **Jobs** tab.

This will display the **Configuration** and **Summary** tabs from where you can schedule jobs and use them for generating the reports.

**Step 2** Click **Configure SMTP** in the **Jobs** screen. Enter the primary and secondary mail server details and click **Save**.

**Figure 70: Configure SMTP**

**Step 3** Enter the job scheduling details and click **Submit**.

To schedule the jobs follow the steps given:

- Use **Select Object** from **Services Endpoint** for OCH-Trail circuit or **Detailed Service** for OCH CC, OCH NC and OCH-Trail circuits or **Interfaces** to select site, equipments, shelves, cards, ports and layers or **Fiber Links**.

**Note**

With **Services Endpoint** report, you can choose one or more than one services but with **Detailed Service** report, you can choose only one service.

**Note**

From release 26.1.1, you can schedule PM jobs for AR-MXP cards. Select **Interfaces** radio button and type **AR** in the **Equipments, Shelves, Cards, and Ports** field.

- Enter **Job Name**.
- Enter **Start Time**.
- Enter **Interval** which can be 15 mins or 24 Hours.
- Enter **Recurrence** which can be either None, Daily, Weekly or Monthly.
- Enter **End Time**.
- Enter **Description**.
- Enter **E-mail** address.

**Note**

To configure **Jobs**, you need to configure the SMTP optionally. From the mail server configuration screen, you must enter the mandatory fields host name/IP, port and then save.

Figure 71: Jobs

**Note**

- To view the PM History values you must wait for a minimum of 15 minutes after onboarding.
- For 15 minutes interval, you must wait for 20 minutes post on-boarding.
- For 24 hours interval, you must wait for 15 mins past 12 A.M post on-boarding.

# Logs

Cisco Optical Network Controller supports two sets of logs:

- The **Audit** logs.
- The developer or **Debug** logs.

Both these logs can be viewed online, using the **Logs** application's **Audit** and **Debug** tabs. These logs are archived every week on Monday around midnight by default. The archived logs are in the *.tgz* format. You can also schedule different day and time values as the archive scheduler time. These archives can be downloaded and deleted using the **Archive** tab.

**Audit Logs**

The **Audit** logs option helps in:

- Auditing all the Cisco Optical Network Controller operations which include circuit operations, Cisco Optical Network Controller and COSM user login or logout procedures and traffic related operations that are done on COSM or node.

- The logs can be used to learn about all the changes that have occurred as a result of external notifications that come from connected nodes.



**Note** **Audit** logs are not added for configurations which are done on the devices before the device discovery.

### Display Features

- Pagination and filter options are available for **Audit** logs.
- Filter option is set to **All** by default.

### Categorization of Audit Logs

**Audit** logs are categorized into:

*Table 48: Audit Logs Category*

Category Field	Description
System	<p>The events that are part of this category are:</p> <ul style="list-style-type: none"> <li>• Login.</li> <li>• Logout.</li> <li>• Create user.</li> <li>• Delete user.</li> <li>• CONC database backup and restore</li> </ul>
Inventory	<p>The events that are part of this category are:</p> <ul style="list-style-type: none"> <li>• Card create/delete/state update.</li> <li>• Physical port and logical port create/delete/state update.</li> <li>• Interfaces create/delete/state update.</li> <li>• Chassis create/delete.</li> <li>• IPC add and delete.</li> <li>• Degree add and delete.</li> <li>• Passive unit add/delete</li> <li>• Port Frequency</li> </ul>

Category Field	Description
Node	The events that are part of this category are: <ul style="list-style-type: none"> <li>• Device add/delete/resync/reconnect.</li> <li>• Device state for discovered and disconnected status.</li> <li>• Connection loss or reconnect audit logs status.</li> </ul>
Service	The events that are part of this category are: <ul style="list-style-type: none"> <li>• Circuit add/delete/edit/update or state change.</li> <li>• Link up and down.</li> </ul>
Topology	The events of this category include the OMS and OTS interfaces.
Site_Audit	The events that are part of this category are: <ul style="list-style-type: none"> <li>• COSM login/logout/login failed.</li> <li>• COSM devices version.</li> <li>• All COSM provisions, notifications which are traffic impacting and audited under site audit category.</li> <li>• COSM backup/Restore</li> </ul>
Alarm	All the events related to <b>Alarms</b> .
Alien_Import	All the events related to <b>Alien_Import</b> .
SNMP	<ul style="list-style-type: none"> <li>• Add SNMP Manager</li> <li>• Delete SNMP Manager</li> <li>• Update SNMP Manager</li> </ul>

**Note**

- Only admin or internal users can view logs, collect techdump, download or delete archive files and schedule archive.
- Only users with read-only permission and the supervisor users can view the archived files and collect techdump.
- The user names are based on the type of user.
- The **User Name** field is marked as *[Unknown]* for a few scenarios. For example: when the user login authentication fails, because of incorrect credentials you get this message: *User failed while logging in due to invalid CSRF token.*

### Debug Logs

Under **Debug** logs, all the developer logs are displayed with filters and pagination. There is also an option to enable and disable debugging of all services. Also, similar to the **Audit** logs, the **Debug** logs have the logs active for up to seven days. After seven days these logs get archived, from where they can also be downloaded.



---

**Note** **Debug** logs that are older than one month are cleared, as they are retained only for a month.

---

### Retention and Archiving and Archive Logs

The **Audit** logs can be retained and saved as given.

- **Audit** logs are retained for up to seven days which can be viewed online using the **Logs** application.
- Logs beyond seven days are archived and kept in the Cisco Optical Network Controller storage. The **Archive** logs are maintained for three months and are deleted later.
- The archived logs can be downloaded any time by using the **Archive** tab in the **Logs** application.
- The **Audit** logs archiving can be scheduled weekly using the **Audit** log scheduler.
- The active **Audit** logs are visible in the **Audit** log table for up to seven days after which they are moved to the **Archive** logs.
- The archived logs can be retrieved anytime and are available in the archive tab. Archived logs which are more than three months old are deleted by Cisco Optical Network Controller by default.
- You can download or delete the archived logs anytime. You can also suspend or resume archiving of logs anytime.

### Archive Logs

The **Archive** logs allow you to schedule the logs. It consists of two schedulers:

- **Audit logs job scheduler**: Refers to all the archived audit logs.
- **Debug logs job scheduler**: Refers to all the archived developer logs.



---

**Note** **Techdump**: It collects the data base (DB) snapshots for all the services. You can collect or download and also delete these logs from the table.

---

**Note**

- The **Archive** logs are saved as tar zip files.
- The **Suspend** and **Modify** options can be used to suspend, resume or modify the archived logs. The **Modify** option works on a weekly basis and you can also set any day as the value as per your requirement.
- The archived audit logs are stored for up to three months where as the developer logs are stored for one month.
- When one archive collection is proceeding, it is recommended to not change the scheduler time as otherwise it can lead to generation of multiple **In Progress** tasks.

**Sedo Commands**

For any issues with the logs, you can collect the techdump data and use the sedo command logs and report them.

The sedo commands are as given:

**1. Step 1:**

Use **sedo diagnostics archive-logs /tmp/logs** to collect all service 7 days logs. It collects logs and stores them in the */tmp/logs* directory with the file name *nxfos-logs-xxxxxxx.tar.gz*.

**2. Step 2:**

Use the **scp** command to copy *nxfos-logs-xxxxxxx.tar.gz* file to the local system.

Download of developer archive logs will time-out when logs are too huge, then it is recommended to use the sedo commands to download:

**1. Step 1:**

Use the command **sedo object-store list onc-torch-service-dev-log-data-archives** which lists all archived files under the developer logs.

For example:

```
Ex : root@abrageor-nxf:~# sedo object-store list onc-torch-service-dev-log-data-archives
```

OBJECT	SIZE (BYTES)	LAST MODIFIED
devlogs_2024-09-20T12_40_00	13606281	Fri, 20 Sep 2024 12:47:01 UTC
devlogs_2024-09-22T07_31_00	175939085	Sun, 22 Sep 2024 08:58:12 UTC

**2. Step 2:**

Use the command **sedo object-store get onc-torch-service-dev-log-data-archives/devlogs\_2024-09-20T12\_40\_00** to download from the current directory. *devlogs\_2024-09-20T12\_40\_00* is the file name list taken from the Step 1 output.

**3. Step 3:**

You can download the file to the local system.

Figure 72: Audit Logs

Time	Category	Identifier	Username	Client IP	Message
09/25/2024 05:15:16:243	alarm	COSM COSM71		10.241.0.20	User acknowledgment for alarm LIC-COMM-FAIL with alarm objectid MODULE: 1/RP0
09/25/2024 05:15:09:592	alarm	COSM71	admin	10.241.0.20	User acknowledgment for alarm LIC-COMM-FAIL with alarm objectid MODULE: 5/RP0
09/25/2024 05:14:26:991	alarm	COSM71	admin	10.241.0.20	UserNote added for alarm CHANNEL-NOISE-LOADED with alarm objectid OXC: onc_qDD2gGyUh5fVeI2bUPXzANAJh path1: OTS:1/0/LINE-TX
09/25/2024 05:14:26:970	alarm	COSM71	admin	10.241.0.20	UserNote added for alarm USER-LOGIN with alarm objectid SYSTEM
09/25/2024 05:14:26:773	alarm	COSM71	admin	10.241.0.20	UserNote added for alarm USER-LOGOUT with alarm objectid SYSTEM
09/25/2024 05:12:28:583	node	COSM71	system		Resync completed
09/25/2024 05:12:03:074	node	COSM71	admin	10.110.204.242	Resync requested
09/25/2024 05:11:44:767	node	COSM71	admin	10.110.204.242	Requested update for values {Latitude=46.014961, Longitude=12.08124}
09/24/2024 23:59:32:967	site_audit	COSM71	system	10.58.253.71	Logout of User
09/24/2024 23:59:31:064	site_audit	COSM71	system	10.58.253.71	Logout of User
09/24/2024 23:59:31:041	site_audit	COSM71	system	10.58.253.71	Logout of User
09/24/2024 23:59:31:004	site_audit	COSM71	system	10.58.253.71	Logout of User
09/24/2024 23:59:30:966	site_audit	COSM71	system	10.58.253.71	Logout of User

Figure 73: Archive Logs

File	Status	Created by	Action
auditlogs_2024-08-27T10_00_00	Completed	System	Download Delete
devlogs_2024-08-29T00_00_00	Completed	System	Download Delete
auditlogs_2024-09-09T00_00_00	Completed	System	Download Delete
devlogs_2024-09-09T00_00_00	Completed	System	Download Delete

Figure 74: Scheduling Audit Logs Job

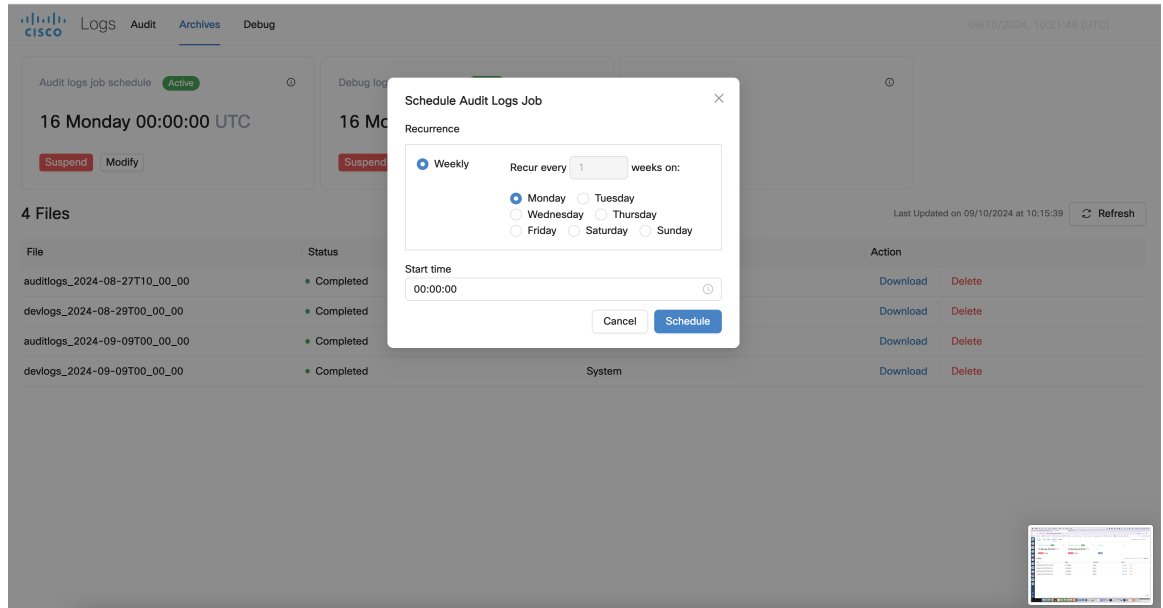
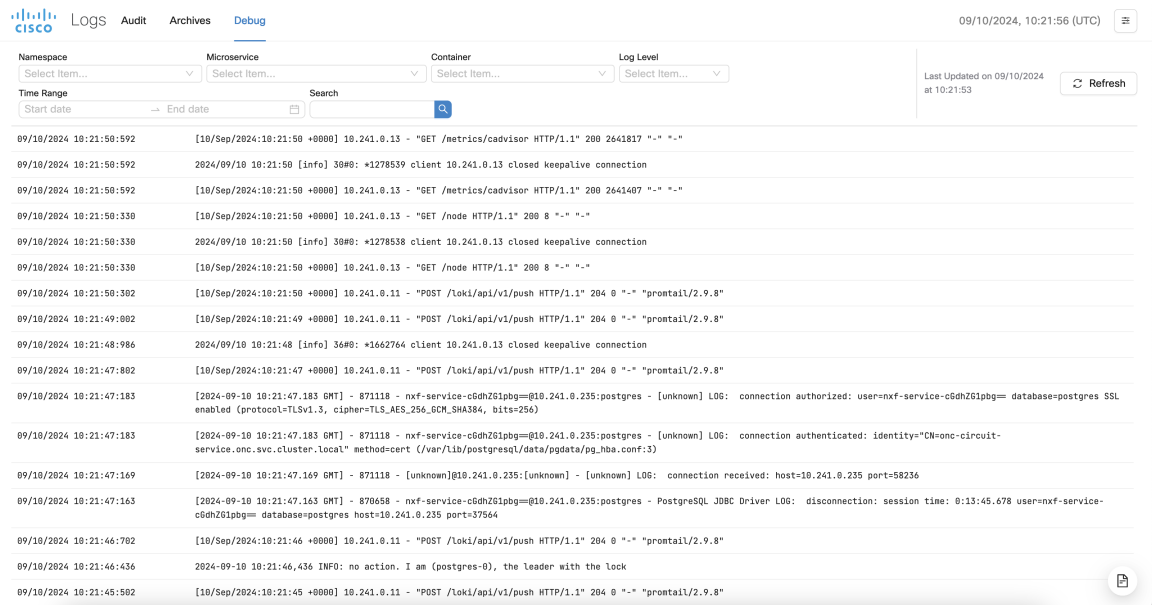


Figure 75: Debug Logs



## Benefits of Logs Enhancement

Log enhancements help in:

Table 49: Benefit of Log Enhancements

Benefit	Description
Organized Log Management	Clear categorization and sub tab structure for easy navigation.
Enhanced Usability	Pagination, filters, and export options improve user experience.
Efficient Retention	Automated scheduling and archiving ensure logs are retained and managed effectively.
User Access Control	Different permissions for admin or internal users and readonly or supervisor users enhance security and control.
Comprehensive Logging	Detailed logging for various operations ensures thorough tracking and auditing.

## Accessing Logs

To access the **Logs**, tab follow the steps:

### Procedure

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

The **Logs** screen is displayed.

**Step 2** Click **Audit** tab.

The **Audit** table is visible which has the following fields:

- **Time**: The time of audit log creation.
- **Category**: The category type of the audit log. It can be one of the following types based on your selection:
  - **System**
  - **Node**
  - **Inventory**
  - **Topology**
  - **Service**
  - **Alarm**
  - **Alien\_Import**
  - **Site\_Audit**

- **Identifier:** The names of unique Cisco Optical Network Controller identifiers like circuit names or device names, circuit tags or degree names which can be used to filter the **Audit** log table.
- **Username:** The user names based on type of user.
- **Client IP:** The IP address of the device or node. It can also have the Cisco Optical Network Controller IP address used for login or also appear as blank.
- **Message:** Messages are information pertaining to each log that are part of the **Audit**.

**Step 3** Click **Refresh** to refresh the **Audit** log table content anytime.

**Step 4** Click **Export** to export the entire **Audit** log table content to an *\*.xls* file.

**Step 5** Click **Archives** tab to view the archived data.

This will display the archives table along with the **Audit logs job scheduler**, **Debug logs job scheduler** and **Techdump** options.

For more information on each of these options you can click **i** the information icon, provided on top of each of these options.

**Step 6** Click **Debug** tab to view the developer logs.

The **Debug** table has the following filter options which you can select:

- **Namespace**
- **Microservice**
- **Container**
- **Log Level**
- **Time Range**
- **Search**

There is also an **Enable Detailed Logs** option which allows you to fetch detailed log information from this table for debugging purpose. By default, this option is disabled and must be enabled only when required.

## Generate and download tech dump logs

Tech dump logs on Cisco Optical Network Controller are diagnostic data bundles. They collect detailed system information, logs, and state files to help with troubleshooting and support.

From R26.1.1, you can collect, download, and delete tech dump logs from the **Tech Dump** tab of **Logs**.

When you generate a tech dump, Cisco Optical Network Controller compiles logs, configuration files, and operational data into a single archive file.

### Before you begin

Ensure that there is sufficient space on the VM hosting the Cisco Optical Network Controller.

Follow these steps to generate and download the tech dump logs:

## Procedure

**Step 1** Click **Logs**.

**Step 2** Click **Tech Dump** tab.

For details about the field descriptions on this tab, see [Table 50: Tech dump tab field descriptions, on page 143](#).

**Step 3** Click the **Collect** button to initiate the log collection.

A confirmation message appears, stating that starting a new log collection will delete the existing log file.

**Step 4** Click the **Collect the DB dump** check box if you also want to collect information about CONC databases.

**Note**

Selecting this check box does not collect any sensitive information, including device credentials.

**Step 5** Click **Collect** on the dialog box.

Collected log files remain local to the current active VM. If a switchover occurs, these files are not available on the new active VM.

Wait for the log collection to finish.

**Step 6** Click **Download** to download the logs or **Delete** to remove them.

**Warning**

Do not log out during the download, as it can cause the file download to fail.

A file named in the *tech\_dump\_<timestamp>.tar.gz* format is downloaded.

The **Tech Dump** tab displays these fields:

**Table 50: Tech dump tab field descriptions**

Field	Description
File Name	Displays the name of the generated tech-dump file, including timestamp and timezone.
Status	Shows the current state of the tech-dump file generation. A green check mark indicates successful completion.
File Size	Indicates the size of the generated tech-dump archive in MB.
Triggered By	Shows the user ID that triggered the tech-dump collection.
Triggered On	Shows the exact timestamp (date and time with timezone) when the tech-dump creation started.

Field	Description
Action	<p>Provides available operations for the generated file:</p> <ul style="list-style-type: none"> <li>• Download: Download the collected logs.</li> <li>• Delete: Delete the collected logs.</li> </ul> <p><b>Note</b> These options are not displayed when the log collection is in progress.</p>

## Monitoring

- **Detailed Node Resources:** You can monitor the CPU, memory or disk consumption of the host.
- **Pod Monitoring:** You can monitor the CPU, memory or disk consumption of the microservices within the kubernetes cluster.

### Before you begin

Use this app to view the log messages and other related details.

### Procedure

---

Click to view each option separately.

---

## Links

The Links App is a new application in the Cisco Optical Network Controller. It provides a centralized location for managing and monitoring network links. It offers enhanced filtering and sorting capabilities compared to the topology view, allowing you to easily differentiate between discovered and undiscovered OMS links.

Figure 76: Links App

Link Name	Type	Endpoint1-Node Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port	Endpoint1-Degree	Endpoint2-Degree	Tags	Description	Link Status	Fiber Type	Action
<b>Forward</b>												
oms_cosmroadm06_Node3_7_8-1_cosmroadm06_Node1_4_9-1	OMS	cosmroadm06_Node3_7_8	cosmroadm06_Node1_4_9	1/0/LINE-TX	1/0/LINE-RX	1	1			ENABLED		
<b>Reverse</b>												
ots_cosmroadm06_Node2-1_cosmroadm06_Node3_7_8-1	OTS	cosmroadm06_Node3_7_8	cosmroadm06_Node2	1/0/LINE-TX	1/0/LINE-0-RX	1	1			ENABLED	G652-SMF	
ots_cosmroadm06_Node2-2_cosmroadm06_Node1_4_9-1	OTS	cosmroadm06_Node2	cosmroadm06_Node1_4_9	1/0/LINE-2-TX	1/0/LINE-4-RX	2	1			ENABLED	G652-SMF	
ots_cosmroadm06_Node2-2_cosmroadm06_Node1_4_9-1	OTS	cosmroadm06_Node1_4_9	cosmroadm06_Node2	1/0/LINE-TX	1/0/LINE-2-RX	1	2			ENABLED	G652-SMF	
ots_cosmroadm06_Node2-1_cosmroadm06_Node3_7_8-1	OTS	cosmroadm06_Node2	cosmroadm06_Node3_7_8	1/0/LINE-0-TX	1/0/LINE-4-RX	1	1			ENABLED	G652-SMF	
oms_cosmroadm06_Node3_7_8-2_cosmroadm06_Node1_4_9-2	OMS	cosmroadm06_Node3_7_8	cosmroadm06_Node1_4_9	9/0/LINE-TX	9/0/LINE-4-RX	2	2			ENABLED		
oms_cosmroadm06_Node3_7_8-3_cosmroadm06_Node6-1	OMS	cosmroadm06_Node3_7_8	cosmroadm06_Node6	5/0/LINE-TX	1/0/LINE-4-RX	3	1			ENABLED		
oms_cosmroadm06_Node5-1_cosmroadm06_Node1_4_9-3	OMS	cosmroadm06_Node5	cosmroadm06_Node1_4_9	1/0/LINE-TX	5/0/LINE-4-RX	1	3			ENABLED		

## Key features of the Links app

The Links app has two tabs, OMS and Undiscovered OMS:

- **OMS tab:** Lists the discovered optical links in a hierarchical, tree-structured table. The parent row shows OMS links, which, when expanded, reveal the underlying OTS links in forward and reverse directions.
- **Undiscovered OMS tab:** Lists undiscovered OMS links, which are considered partial links. In this tab, the parent row is an OTS link.
- **OTN Links tab:** Lists the OTN links for the tranponder networks.

Figure 77: Links app

Link Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port	Tags	Description	Link Status	Span Utilization	Action
OTNXC1	SaoPaulo	5/8/11	1/8/11			ENABLED		View summary
OTNXC2	AltaForesta	1/8/12	5/8/11			ENABLED		View summary
OTNXC3	AltaForesta	5/8/12	5/8/12			ENABLED		View summary

Click the **View summary** in **Span Utilization** to open the Span Utilization table.

## Links table

The table includes these columns:

- Link Name
- Type (OMS or OTS or OTN)
- Endpoint information
  - Endpoint 1 – Node Name
  - Endpoint 2 – Node Name
  - Endpoint 1 – Port
  - Endpoint 2 – Port

- Endpoint 1 – Degree
- Endpoint 2 – Degree
- Tags
- Description
- Link Status
- Fiber Type
- OTS-specific information
  - Fiber Length [km]
  - Tx [dBm]
  - Rx [dBm]
  - Fiber Loss [dB]
- Action

The table contains these interactive options:

- **Action Column:** Provides the following actions:
  - **Edit:** Allows users to edit the Link Name, Tags, and Description.
  - **View Circuit Monitoring:** Cross-launches to the Circuit Monitoring page, filtering for circuits related to the selected link. This option is available only in the OMS tab and not in Undiscovered OMS tab.
- **PM History:** A small arrow icon for each OTS link provides access to PM history data.
- **OCM and OTDR Cross-Launch:** Each endpoint has a cross-launch icon to navigate to the relevant Cisco Optical Site Manager OCM (Optical Channel Monitoring) and OTDR (Optical Time Domain Reflectometer) measures. If OTDR is not supported, it navigates to alarms.




---

**Note** From release 26.1.1, the Links Monitoring table supports the OTN links and features a new **Span Utilization** column that provides an overview of the ODU resource utilization summary and details.

---

### Link monitoring workspace

Link monitoring in workspace integrates links table, topology, alarms and PM history, enabling cross-application interaction. You can select a link in the Topology App and highlight it in the Links App and vice versa.

## Use the Links Application

This task describes the different actions that you can perform from the Links app.

## Procedure

**Step 1** Open the Links app from the sidebar.

**Step 2** Edit Link Attributes.

- a) Select a link in the OMS or Undiscovered OMS tab.

**Note**

From release 26.1.1, for OTN networks, the Links application displays OMS Links and OTN Links attributes only.

- b) Click the edit (pencil) icon in the Action column.
- c) Modify the Link Name, Tags, or Description.
- d) Click Save to apply the changes.

**Step 3** View the Circuit Monitoring workspace for a link.

- a) Select a link in the OMS or Undiscovered OMS tab.

**Note**

From release 26.1.1, for OTN networks, the Links application displays OMS Links and OTN Links attributes only.

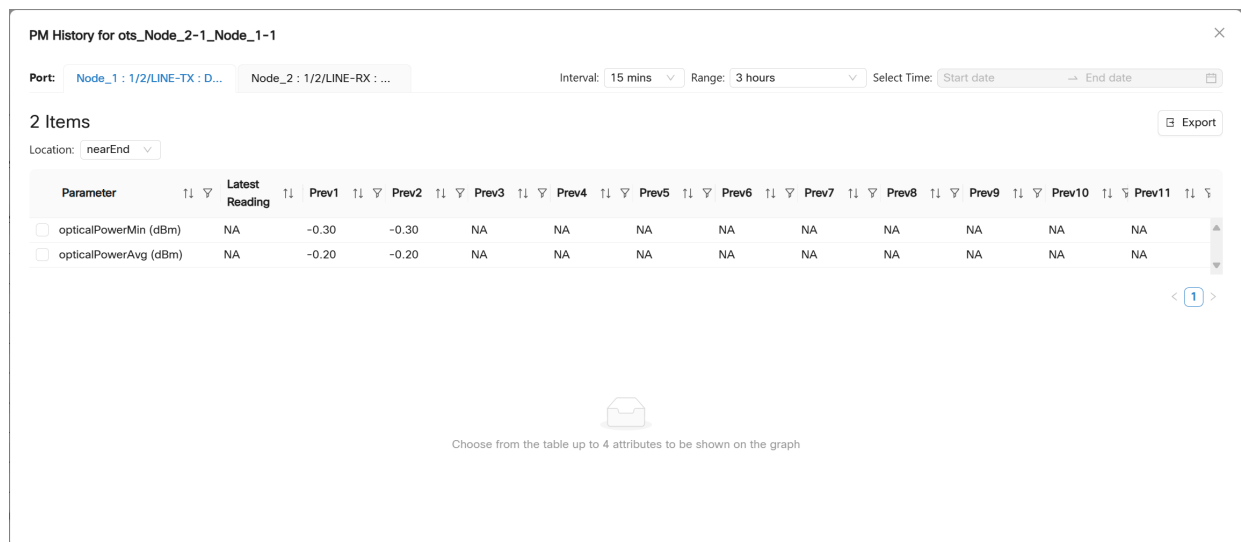
- b) Click the circuit monitoring icon in the Action column.

The Circuit Monitoring page opens, filtered to display circuits related to the selected link.

**Step 4** View PM History for a link.

- a) In the OMS tab, expand an OMS link to view its OTS links.
- b) Click the arrow icon next to an OTS link to view its PM history.

**Figure 78: Links App**

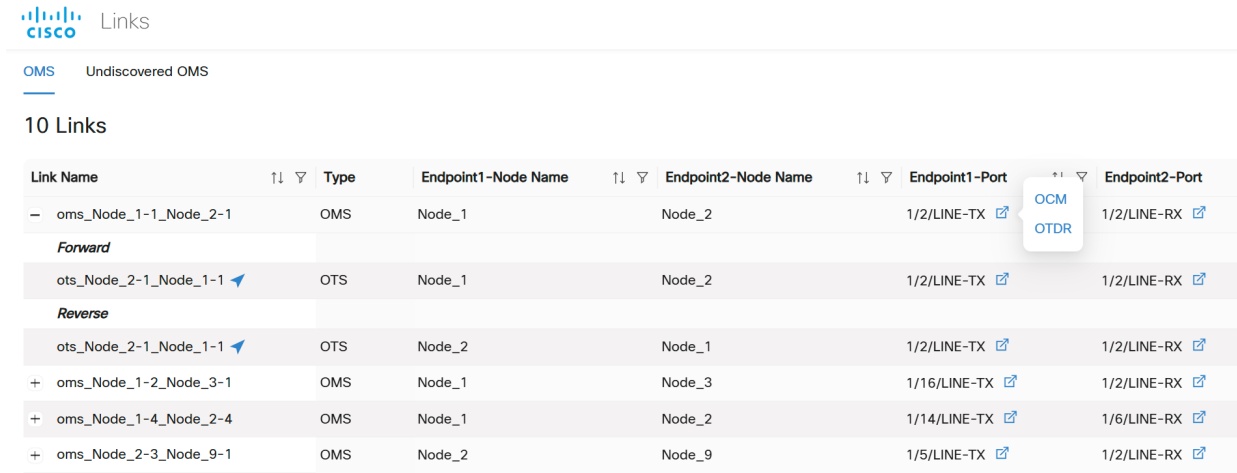


- c) Select an interval and predefined time range or choose a custom range. The PM history table is displayed.
- d) Select up to 4 parameters to view on the graph.

**Step 5** Cross-Launch to OCM/OTDR in Cisco Optical Site Manager.

- In the OMS tab, expand an OMS link to view its OTS links.
- Click the cross-launch icon in the **Endpoint1-Port** or **Endpoint2-Port**.

Figure 79: Links App



Link Name	Type	Endpoint1-Node Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port
oms_Node_1-1_Node_2-1	OMS	Node_1	Node_2	1/2/LINE-TX	1/2/LINE-RX
<b>Forward</b>					
ots_Node_2-1_Node_1-1	OTS	Node_1	Node_2	1/2/LINE-TX	1/2/LINE-RX
<b>Reverse</b>					
ots_Node_2-1_Node_1-1	OTS	Node_2	Node_1	1/2/LINE-TX	1/2/LINE-RX
oms_Node_1-2_Node_3-1	OMS	Node_1	Node_3	1/16/LINE-TX	1/2/LINE-RX
oms_Node_1-4_Node_2-4	OMS	Node_1	Node_2	1/14/LINE-TX	1/6/LINE-RX
oms_Node_2-3_Node_9-1	OMS	Node_2	Node_9	1/5/LINE-TX	1/2/LINE-RX

- Click **OCM** or **OTDR** to cross-launch the OCM or OTDR tab in Cisco Optical Site Manager for the selected endpoint. If OTDR is not supported, it navigates to alarms.

#### Step 6 Export Links data.

- Click **Export**.
- (Optional) Select **Table View** and click **Export** to export and download the data currently displayed in the table.
- Select **Network Links** to export all network links.
- Click **Generate**.
- After the file is generated, click **Export** to download the XLS file.

#### Note

After expanding links, wait for up to 60 seconds for the **Total Transmit Power Tx(dBm)** and **Total Receiver Power Rx(dBm)** values to be fetched. If you export or Generate a full report before all the values are fetched, the report contains only the power values for the links for which the values were fetched.

## SLTE links and ASE services in Cisco Optical Network Controller

An Submarine Line Terminal Equipment (SLTE) link is an optical link type that Cisco Optical Network Controller automatically discovers from Cisco Optical Site Manager configuration. This allows the different applications, such as Links, Topology, and Service Manager to distinguish submarine behavior from terrestrial behavior.

- Cisco Optical Network Controller shows SLTE links with the `Submarine` deployment type in **Links** app.
- Service Manager shows discovered ASE channels in a dedicated **SLTE ASE** tab.

For details

## How Cisco Optical Network Controller handles SLTE links and ASE services

Use the SLTE link and ASE service views to verify discovery results and to manage the transition between discovered ASE channels and provisioned user channels.

- The submarine deployment type is discovered from Cisco Optical Site Manager and can be overridden in Cisco Optical Network Controller when the discovered topology needs correction for a custom deployment.
- The link override is applied at the OTS link level, even when the **Links** app groups the view under an OMS link.
- The **SLTE ASE** tab lists the ASE services with frequency, bandwidth, and endpoint information.
- Upgrading an ASE service converts the selected ASE channel into a user channel. Deleting that user channel adds the ASE channel back so that the spectrum remains filled.
- Cisco Optical Network Controller discovers an ASE service even when only one endpoint is available. If no matching OXC with the same frequency and bandwidth is present at the far end of the fiber, Cisco Optical Network Controller displays the ASE service as a partial discovery result with a single endpoint.
- When Cisco Optical Network Controller later discovers a matching endpoint with the same frequency and bandwidth at the other end of the fiber, it completes the ASE discovery and updates the service to show both endpoints.

## Change the SLTE link deployment type

Override the deployment type on a discovered OTS link when the automatic link type does not match the actual deployment topology.

- Use this task for custom topologies where the submarine type is not derived correctly from discovery.
- Use the updated deployment type to align the **Links** app and related topology views with the actual link behavior.

Use this task in custom topologies where the submarine type is not correctly derived from link discovery. Updating the deployment type aligns the Links app and topology views with the real-world link behavior.

### Before you begin

- Configure the ASE channels on the submarine nodes by using XR CLI before onboarding the nodes in Cisco Optical Network Controller. For more details on configuring SLTE using XR CLI, see [Sub-sea Configuration](#).
- Ensure that the SLTE nodes and their links are already discovered in Cisco Optical Network Controller.

Follow these steps to change an SLTE link deployment type.

### Procedure

---

- Step 1** Click **Links** and then click the **OMS** tab.
- Step 2** Locate the required OMS link and expand the entry to show the underlying OTS links. The **Deployment Type** can be configured on the OTS link.

- Step 3** For the required OTS link, click **Edit** action.
- Step 4** In the **Edit Link** dialog box, select **Submarine** or **Terrestrial** from the **Deployment Type** drop-down list. Select **Submarine** when the link is part of an SLTE deployment and the discovered type must be corrected.
- Step 5** Save the change.  
Cisco Optical Network Controller updates the OTS link deployment type.
- Step 6** Click **Refresh** and verify the updated deployment type in the link list.

- 
- The selected OTS link uses the deployment type that you specified, and Cisco Optical Network Controller reflects the updated deployment type in the **Topology**.
  - To filter submarine links in the **Topology** application, select **OTS** or **OMS** links, click the eye icon on the right side and select the **Filter Submarine Links** check box.

## Convert SLTE ASE channel to user channel

Convert a discovered SLTE ASE channel into a user service by selecting the required service name and endpoint.

Whether you create a new user channel or upgrade an ASE channel to a user channel, you must tune the attenuation settings based on live network conditions to ensure that traffic flows correctly.

The **SLTE ASE** tab in **Service Manager** displays discovered ASE services with their endpoint, frequency, and bandwidth based on SLTE configuration.

During this upgrade, constraints used by other service types are not applicable to the SLTE ASE workflow.

- The configuration is rejected in these cases:
  - The ASE channel central frequency and channel width exactly match the user-provided central frequency and channel width for the user channel. Remove the hardware module for the ASE channel and configure the end-to-end circuit from Cisco Optical Network Controller.
  - The user channel extends beyond the ASE channel into empty spectrum. Remove the ASE channel and configure an end-to-end circuit from Cisco Optical Network Controller.
  - The user channel has a narrower width than the ASE channel but uses the same central frequency. Remove the ASE channel and configure the end-to-end circuit from Cisco Optical Network Controller.
- Cisco Optical Network Controller provisions the required user circuit when a new user channel on the same add/drop port overlaps an existing user channel, provided that only frequency slices overlap and the payloads do not overlap.
- When a submarine channel is created, CPCE performs no optical validation except for central frequency and channel width.

### Before you begin

Ensure that the SLTE nodes are onboarded and that the required ASE services are already discovered.

Follow these steps to convert an SLTE ASE channel to a user channel.

## Procedure

- 
- Step 1** Click **Service Manager** and then click the **SLTE ASE** tab.  
The list of discovered ASE services is displayed.
- Step 2** Select the endpoint of the actual user channel service that you want to convert.  
Review the endpoint, frequency, and bandwidth columns to confirm that you selected the correct ASE channel.
- Step 3** Click **Upgrade** and select a service.
- Step 4** Complete the steps in the [Create and manage circuits, on page 34](#) task to finish converting the selected ASE channel to a user channel.
- 

The selected ASE channel is converted to a user channel in Cisco Optical Network Controller, and the new user service is shown in Service Manager.



---

**Note** Deleting the user channel restores the ASE channel, ensuring the spectrum is filled.

---

## General Troubleshooting

These are some generic troubleshooting points to consider which are common across the different applications within Cisco ONC.

- **TAC case:** In order to raise a TAC case, collect the sedo diagnostic logs with the command:

```
sudo sedo diagnostics archive-logs /data
```

Collect it along with the Grafana view.

## Unmanaged Equipment Support

Unmanaged devices are third party devices that can be included in the Cisco Optical Network Controller circuit trails connected to transponders.

Cisco Optical Network Controller supports the unmanaged device MXD65-ADVA-FSP-3000-METRO-DCI-OLS in:

- **Topology,**
- **Service Assurance,**
- **Network Monitoring Workspace** and
- **Circuit Monitoring Workspace** applications.

**Note**

- The MXD65-ADVA-FSP-3000-METRO-DCI-OLS unmanaged device appears as 3LS in the circuit link.
- In case a degree between the ADVA devices is deleted and recreated, then a resync of the COSM nodes is mandatory.
- This is pre-provisioned equipment in COSM, the link status is not known since Cisco Optical Network Controller has no access to real HW.
- Alarms and PM are supported only for NCS 1014 and TXP cards.
- Power levels are reported only on the TXP card endpoint of the service, and not on the UME side.
- There is no support for automatic degree detection. The neighbouring nodes have to be configured manually through NETCONF RPC.

**Figure 80: Unmanaged Equipment Support in Topology**

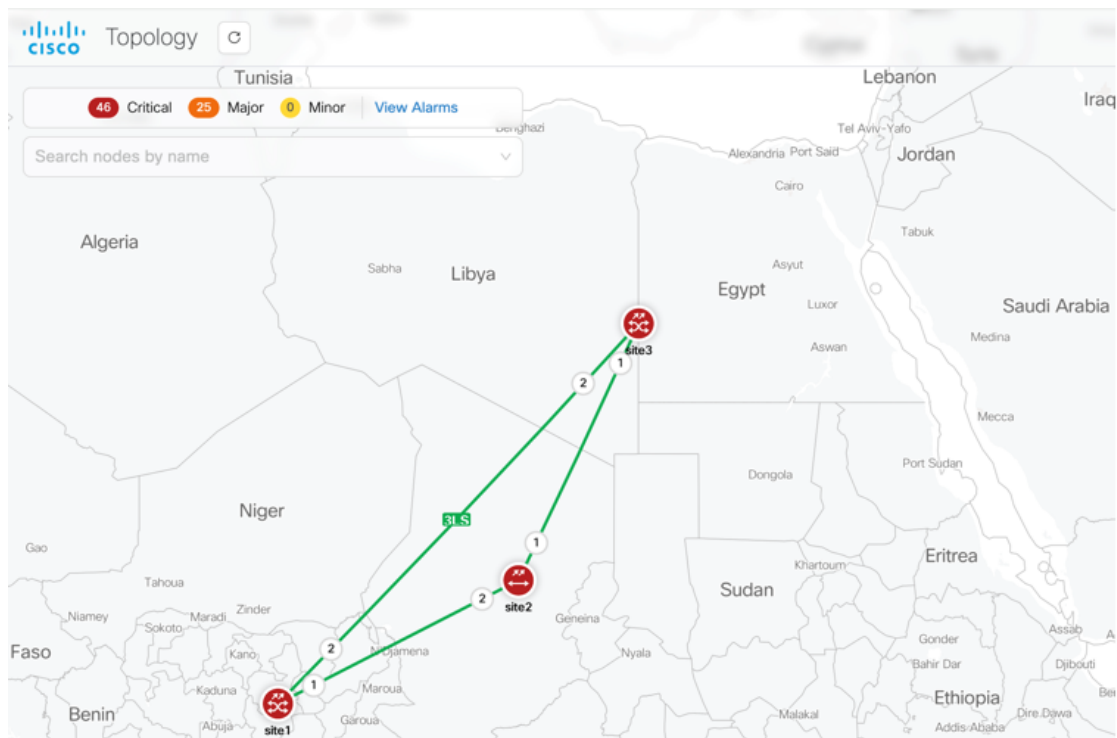
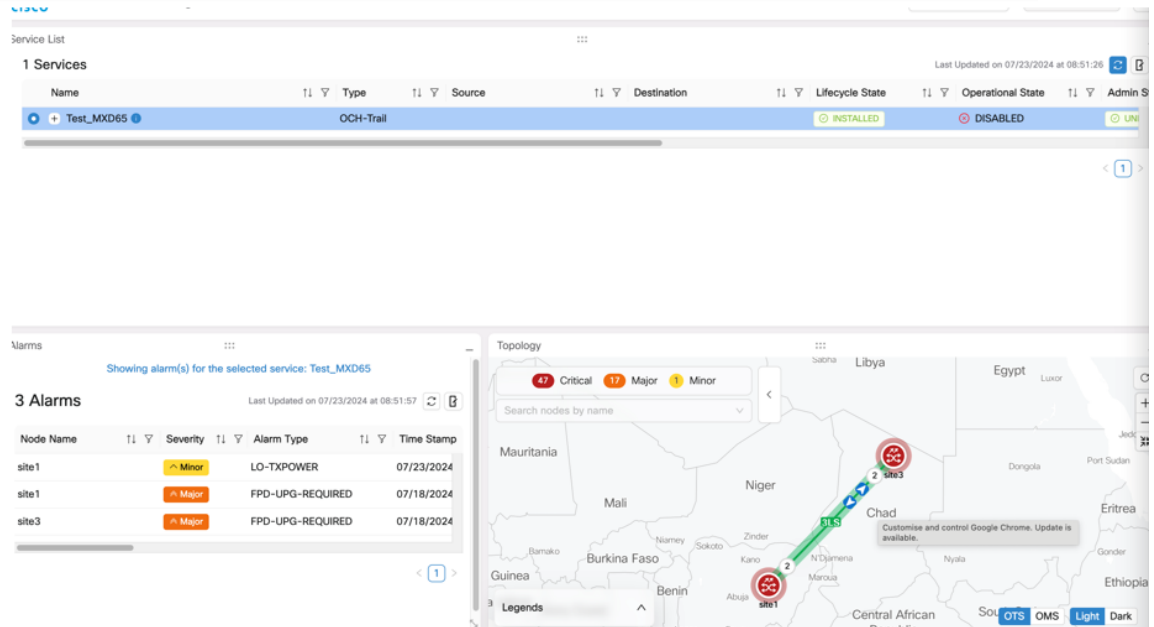


Figure 81: Unmanaged Equipment Support in Service Assurance



## PSM OMS Protection

Protection Switching Module (PSM) is a Cisco Optical Network Controller feature that protects the Optical Multiplex Section (OMS) segment in the optical network. It ensures the continuity of signal transmission by automatically switching circuit paths in case of any fiber cut.



### Note

- Cisco Optical Network Controller supports only brownfield network.
- Cisco Optical Network Controller does not support greenfield networks. From Cisco Optical Network Controller, you cannot create new PSM services.
- PSM module is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.
- NCS 1001 is supported only if it is managed by a COSM instance running over a NCS 1014 chassis.

### Configuration in PSM Circuits

PSM supports two-way configurations and can be manually configured. Out of the two paths one will be active and the other will be a standby path. Whenever the active path fails due to fiber cut then the standby path is used for receiving the signal. This is because both the active and standby paths are always used in the TX direction for transmitting the signal, but only one of them can be used to receive the signal at a time.



### Note

PSM supports both automatic and manual path switching. Once you cross launch to COSM, there is also a manual switch option provided there for you to select any path and use it as the active path in the PSM circuit.

### Benefits of PSM

The benefits of using PSM are:

- Enhanced network reliability and protection through PSM OMS protection.
- Improved network management and monitoring with clear visualization of active and standby paths in the circuits.
- Flexibility in network design with support for various connection scenarios for PSM.
- Comprehensive event logging and user-driven OAM for better operational control. See [Configuration Guide for Cisco NCS 1001](#).
- Being multiplexer-agnostic ensures compatibility with various network components.



---

**Note** Protection switching in optical circuits with NCS 1010 ILA modules between NCS 1010 OLT nodes.

---

### Additional PSM Functions

PSM generates alarms and performs automatic path switching with minimal data loss. PSM is integral to circuit creation and can be deployed in any network segment for protection. Additionally, it includes features for monitoring channel power and composite power.

### PSM Circuit in Service Manager

In the Service Manager application, the PSM circuit is created like any other circuit using the Provision Circuit option. Once the PSM circuit is installed and it appears in the Services screen it can be visualized in the Service Assurance and the Workspace applications.

### Limitations of PSM OMS protection

- Cisco Optical Network Controller does not support 3-way PSM Protection switching.
- The W-RX and P-RX thresholds for the NCS 1001 PSM must be set carefully based on the number of channels. If the number of channels is lower, a significant power drop from one channel going off may cause the PSM to switch, leading to traffic hits on other channels. See [Configuration Guide for Cisco NCS 1001](#)
- Cisco Optical Network Controller does not display the Reason for switchover.
- Cisco Optical Network Controller supports only configurations with amplifiers positioned after the PSM module. OMS protection is not supported.
- You must perform a resync if you onboard devices, add or modify IPCs, or add or remove degrees to the network after onboarding the PSM.
- If the same network is being managed by two separate active Cisco Optical Network Controller instances, the same connection service, either a discovered service in both instances, or a service provisioned in one and discovered in the other, must be deleted on both instances for all types of connection services.

## PSM Circuit in Workspace Screen

To view the selected PSM circuit follow the steps:

### Procedure

---

**Step 1** Click **Workspace** option on the left panel.

**Step 2** In **Circuit Monitoring**, click **Launch**.

**Step 3** Select the PSM circuit.

This will display the PSM circuit on the Topology screen where you can see the active PSM circuit path displayed with a blue colored arrow.

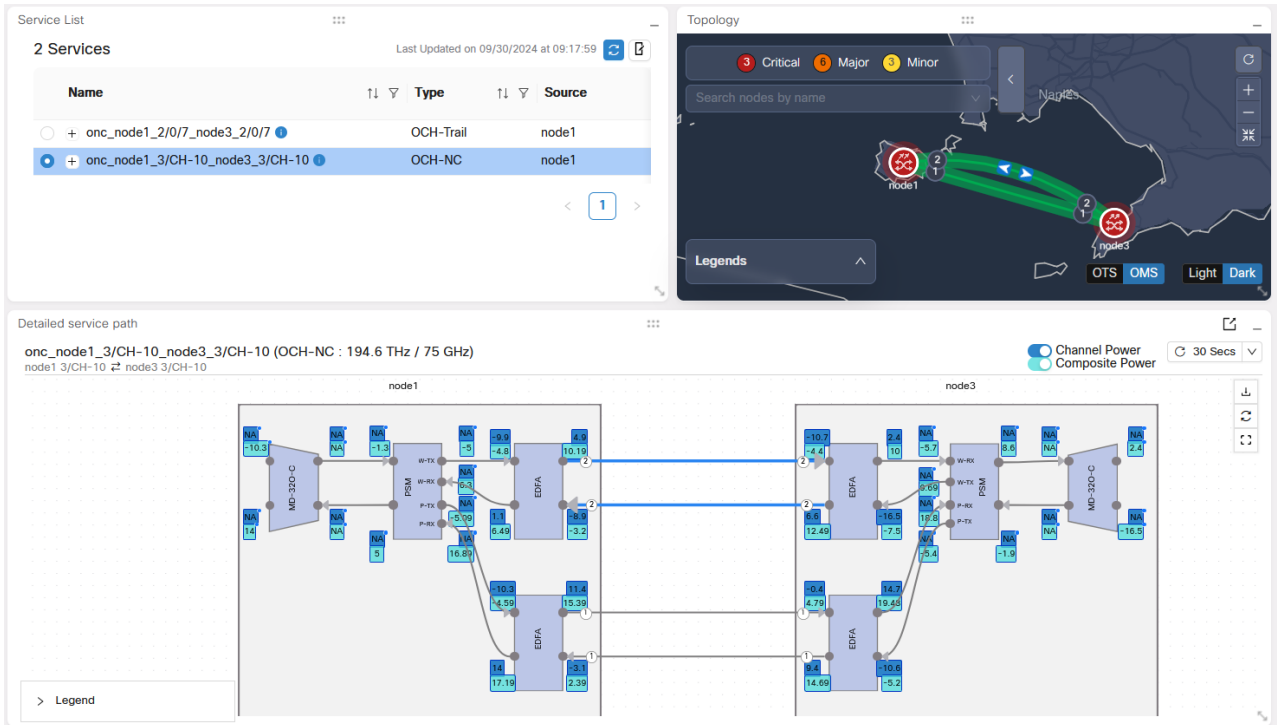
### Note

- The **Detailed Service Path** displays all the equipments crossed by the circuit. The active path appears in blue and the standby path in grey color.
- The blue arrows indicate the RX direction of the light for a given PSM.

### Note

- From Release 26.1.1, the NCS 1001 PSM Circuit Workspace has these UI enhancements.
- The **Detailed Service Path**.
  - Highlights the active path between the NCS 1001 PSM nodes.
  - Displays the equipment between the NCS 1010 OLT nodes as a cloud.
- From R26.1.1, service history is now enabled for PSM service to show discovery events, operation state changes, and switch events.
- In the **Service List** pane, the OCH-Trail services for NCS 1001 PSM cover the carrier (wavelength) information and add these new labels to each provisioned channel.
  - Work—Channel passing through nominal Work port of PSM.
  - Protect—Channel passing through nominal Protect port of PSM.
  - Forward—Traffic flow from node A to Node Z ,where Node A is the Source Node.
  - Reverse—Traffic flow from node Z to Node A ,where Node Z is the Source Node.
  - Active—This label is added before the Forward/Reverse labels to indicate that the channel is carrying traffic in that Forward/Reverse direction.
  - Standby—Channel that is not carrying any traffic

Figure 82: PSM Circuit in Workspace



- Unidirection service states are supported and displayed at channel level.
- If only one of the channel is discovered, work or protect, then the controller marks the service as PARTIAL. When that channel and carrier is INSTALLED, then the service moves to INSTALLED when other channel is discovered.
- If a path is standby in both directions, then it will show up as dotted line in topology in Circuit monitoring workspace.
- If different paths are active in different directions, then we will not see dotted line.

## PSM wavelength protection

Table 51: Feature History

Feature Name	Release Information	Feature Description
Two-way PSM wavelength protection	Release 26.1.1	<p>PSM wavelength protection is connecting the NCS 1001 PSM module COM port with the transponder trunk port.</p> <p>PSM wavelength protection supports two-way protection switching in optical circuits with NCS 1010 ILA modules between NCS 1010 OLT nodes. PSM wavelength protection does not support three-way and four-way switching.</p> <p>The Circuit Monitoring workspace UI is improved with for the PSM wavelength protection.</p> <ul style="list-style-type: none"> <li>• Only brownfield circuit discovery is supported.</li> <li>• In Services List pane, OCH-Trail services are added if an IPC between transponders and NCS 1001 PSM COM port is present. If IPC is not present, then PSM services are discovered as OCH-NC.</li> <li>• Onboard the node containing the PSM through Cisco Optical Network Controller to discover the circuit present in Cisco Optical Site Manager device.</li> <li>• In Services List pane, new labels are added to indicate the work and protect channels. The new labels are Work, Protect, Forward direction, Reverse direction, Active, Standby.</li> <li>• In Topology pane, the equipment connected between two NCS 1010 OLT nodes are represented as a cloud for a concise view. You can expand the cloud to check the equipment added between the two NCS 1010 OLT nodes.</li> </ul>

PSM wavelength protection is connecting the NCS 1001 PSM module COM port with the transponder trunk port.

### Characteristics of PSM wavelength protection



#### Note

- Cisco Optical Network Controller supports only brownfield network. You can only discover the PSM wavelength protection services as OCH-NC and OCH-Trail. To discover or add nodes to the PSM wavelength protection services, see [Discover the PSM wavelength protection, on page 158](#).
- Cisco Optical Network Controller does not support greenfield circuits, that is, circuit creation by selecting two endpoints in the circuit creation wizard in CONC service manager. From Cisco Optical Network Controller, you cannot create new PSM services.
- Create cross-connect between PSM COM port and LINE port using CLI and onboard them to COSM, then onboard all these nodes to CONC.
- Service discovery - Once you onboard all the COSM nodes with cross connects, then the CONC discovers the PSM services and displays in the service list.
- The listed services are tagged with Active, Standby, Protect, Work, Forward and Reverse.
- PSM switching is unidirectional and bidirectional, CONC will show both unidirectional and bidirectional services based on the Active and Standby labels.
- PSM switching supports only Centralized control plane circuits (CPCE) circuits. CPCE circuits are service-level circuits managed by Cisco Optical Network Controller using PCE for path computation and provisioning.
- In Circuit Monitoring workspace, you can check the service, detailed service path, and service history.
- PSM module is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.
- NCS 1001 is supported only if it is managed by a COSM instance running over a NCS 1014 chassis.

### Discover the PSM wavelength protection

Before discovering the PSM wavelength circuits, do these actions.

1. Create cross-connect between PSM COM port and LINE port of NCS 1010 or NCS1K-MD-320/E-C patch panel mux/demux using CLI commands.
2. Onboard the nodes to COSM, then onboard all these COSM nodes to CONC.

## PSM Circuit in Service Manager Screen

This section describes the PSM circuit in the Service Manager screen.

The **Service Manager** screen displays the details of PSM circuits in a format similar to the *Service List* in the *Circuit Monitoring* workspace. For NCS 1001 PSM, OCH-Trail services include information about the carrier (wavelength). In this view, the wavelength is nested under the channel that carries it, and the channel is nested under the OCH-Trail of the PSM circuit.

- These images show the PSM circuit in service manager screen.

Figure 83: PSM Circuit in Service Manager screen

Name	Type	Source	Destination	Description	Control Plane	Lifecycle State
onc_2way_node2_8/0/0_2way_node1_8/0/0	OCH-Trail	2way_node2 8/0/0	2way_node1 8/0/0		CPCE	INSTALLED
onc_2way_node2_8/0/0_2way_node1_8/0/0	OCH-Trail	2way_node2	2way_node1	PROTECT	CPCE	INSTALLED
onc_2way_node2_8/0/0_2way_node1_8/0/0	OCH-Trail	2way_node2	2way_node1	WORK	CPCE	INSTALLED
onc_2way_node2_8/0/1_2way_node1_8/0/1	OCH-Trail	2way_node2 8/0/1	2way_node1 8/0/1		CPCE	INSTALLED
onc_2way_node2_8/0/1_2way_node1_8/0/1	OCH-Trail	2way_node2	2way_node1	WORK	CPCE	INSTALLED
onc_2way_node2_8/0/1_2way_node1_8/0/1	OCH-Trail	2way_node2	2way_node1	PROTECT	CPCE	INSTALLED

### PSM wavelength protection switching services

In this example, black highlight is the service, green highlight is the channel and the blue highlight is the wavelength. In short, hierarchy of PSM service in the service list is **Service** > **Channel** > **Carrier**.

Only channels display specific labels that indicate their status and role.

- Work—Channel passing through nominal Work port of PSM.
- Protect—Channel passing through nominal Protect port of PSM.
- Forward—Traffic flow from node A to Node Z ,where Node A is the Source Node.
- Reverse—Traffic flow from node Z to Node A ,where Node Z is the Source Node.
- Active—This label is added before the Forward/Reverse labels to indicate that the channel is carrying traffic in that Forward/Reverse direction.
- Standby—Channel that is not carrying any traffic

Figure 84: PSM Circuit in Service Manager screen

Service Manager

04/15/2026, 05:48:28 (UTC+00:00)

DWDM OTN SLTE ASE

18 Services

Last Updated on 04/15/2026 at 05:38:49 (UTC+00:00) Refresh Export

+ New Service Delete Edit More

Service on top:  Select multiple services:

Name	Type	Source	Destination	Description
onc_SAS1_CLS_Port_Sudan_8/3/0_SAS1_CLS_Jeddah_8/3/0	OCH-Trail	SAS1_CLS_Port_Sudan 8/3/0	SAS1_CLS_Jeddah 8/3/0	
onc_SAS1_CLS_Port_Sudan_8/3/0_SAS1_CLS_Jeddah_8/3/0	OCH-Trail	SAS1_CLS_Port_Sudan	SAS1_CLS_Jeddah	Active Forward Reverse PROTECT
(Carrier) onc_SAS1_CLS_Port_Sudan_8/3/0_SAS1_CLS_Jeddah_8/3/0	OCH-Trail	SAS1_CLS_Port_Sudan 8/3/0	SAS1_CLS_Jeddah 8/3/0	
onc_SAS1_CLS_Port_Sudan_8/3/0_SAS1_CLS_Jeddah_8/3/0	OCH-Trail	SAS1_CLS_Port_Sudan	SAS1_CLS_Jeddah	Standby WORK
(Carrier) onc_SAS1_CLS_Port_Sudan_8/3/0_SAS1_CLS_Jeddah_8/3/0	OCH-Trail	SAS1_CLS_Port_Sudan 8/3/0	SAS1_CLS_Jeddah 8/3/0	
onc_SAS1_CLS_Port_Sudan_8/1/7_SAS1_CLS_Jeddah_8/1/7	OCH-Trail	SAS1_CLS_Port_Sudan 8/1/7	SAS1_CLS_Jeddah 8/1/7	
onc_SAS1_CLS_Port_Sudan_8/0/0_SAS1_CLS_Jeddah_8/0/0	OCH-Trail	SAS1_CLS_Port_Sudan 8/0/0	SAS1_CLS_Jeddah 8/0/0	

Cisco Confidential

Figure 85: PSM Circuit in Service Manager screen with Service on Top disabled



**Note** OCH-CC service appears at the bottom of the OCH-Trail services.

In this example, black highlight is the OCH-Trail service, green highlight is the channel and the blue highlight is the wavelength. Orange highlight is the OCH-CC service.

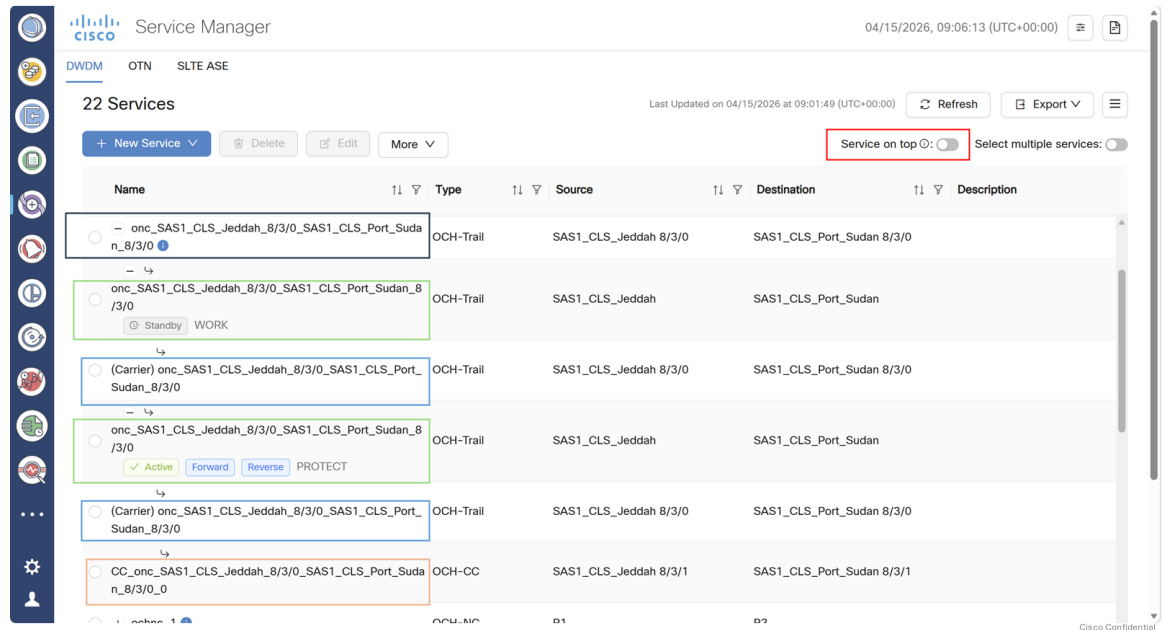
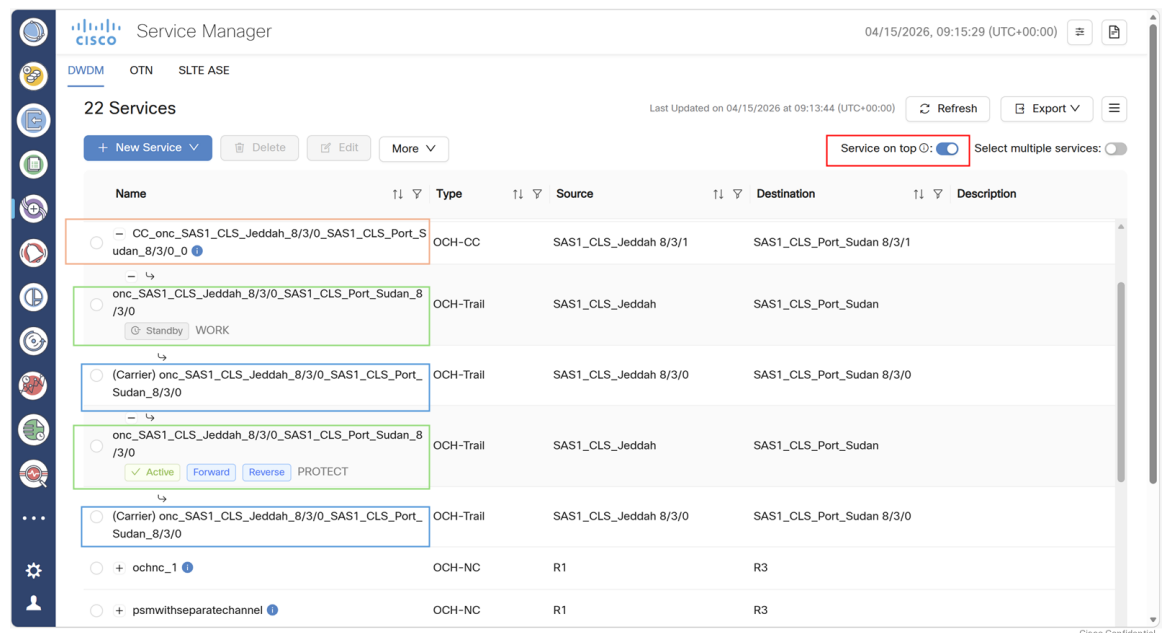


Figure 86: PSM Circuit in Service Manager screen with service on top enabled



**Note** OCH-CC service appears on top of the OCH-Trail services.

In this example, orange highlight is the OCH-CC service that appear at the top. Black highlight is the OCH-Trail service, green highlight is the channel and the blue highlight is the wavelength.



**Figure 87: OCH-PSM circuit for PSM wavelength**

The PSM wavelength circuit is defined by the **OCH-PSM** value in the **Protection Profile** column. For more information on Protection profile, see [Service Manager, on page 26](#).

Admin State	Regenerated	Frequency (THz)	Bandwidth (GHz)	Protection Profile	Port Rate	Discovery Date	Restoration Type	Restoration State	Tags	Violations
UNLOCKED	False	195.95	150	OCH PSM		04/10/2026, 15:47:43.000 (UTC+00:00)				False
UNLOCKED	False	193.1	150	OCH PSM		04/10/2026, 15:47:44.000 (UTC+00:00)				False
UNLOCKED	False	191.45	150	OCH PSM		04/10/2026, 15:47:45.000 (UTC+00:00)				False
UNLOCKED	False	195.8	150	OCH PSM		04/10/2026, 15:47:45.000 (UTC+00:00)				False
UNLOCKED	False	193.4	150	OCH PSM		04/10/2026, 15:47:45.000 (UTC+00:00)				False
UNLOCKED	False	195.95	150	OCH PSM		04/10/2026, 15:47:46.000 (UTC+00:00)				False
UNLOCKED	False	196.1	150	OCH PSM		04/10/2026, 15:47:46.000 (UTC+00:00)				False

### Trail Discovery and Upgrade Process with Transponder Connection

- After creating the services, upgrading to a trail will not work unless the transponder is connected beforehand.
- Once the transponder is connected, the trail can be discovered and subsequently upgraded.



**Note** If you are discovering a Network Channel (NC), there is no automatic way to upgrade it to a trail. Therefore, connect the transponders and create the Inter-Process Communication (IPC) before onboarding, so that the trail can be discovered.

Automatic conversion from Optical Channel Network Channel (OCH-NC) to trail is not supported. To upgrade, delete the OCH-NC and then create the trail manually.

- After creating the IPC, the trail will be discovered, and then upgrade the trail to a Circuit Channel (CC).
- However, creating the IPC between the transponder trunk and the PSM component does not automatically trigger trail discovery. You must delete the existing NC and create the trail again.
- To avoid this manual step, it is recommended that the transponder is inserted and IPCs are created before onboarding the COSM into the CONC.
- After the trail is discovered, click "Discover CC," and the CONC will discover and display the OCH-CC.

## PSM Wavelength Circuit in Workspace Screen

To view the selected PSM wavelength circuit follow the steps:

### Procedure

- Step 1** Click **Workspace** option on the left panel.
- Step 2** In **Circuit Monitoring**, click **Launch**.
- Step 3** Select the PSM wavelength circuit.

Selecting the PSM wavelength circuit shows the channel path with a blue colored arrow in the Topology panel and detailed service path with equipment patchcords in Detailed Service Path tab.

- In the **Service List** pane, the OCH-Trail services for NCS 1001 PSM cover the carrier (wavelength) information and include these new labels to each discovered channel.
  - Work—Channel passing through nominal Work port of PSM.
  - Protect—Channel passing through nominal Protect port of PSM.
  - Forward—Traffic flow from node A to Node Z, where Node A is the Source Node.
  - Reverse—Traffic flow from node Z to Node A, where Node Z is the Source Node.
  - Active—This label is added before the Forward/Reverse labels to indicate that the channel is carrying traffic in Forward/Reverse direction.
  - Standby—Channel that is not carrying any traffic.

#### Step 4

In the Alarms tab, alarms are reported for both the paths. In topology panel, you can see the Active and Standby paths and direction of the traffic flow indicated by the arrows.

**Figure 88: Alarms and topology for PSM wavelength service**

The screenshot displays the Cisco Optical Network Controller interface. The top section shows the 'Alarms' tab with a table of 8 alarms. The middle section shows the 'Topology' panel with a map of the network and a legend. The bottom section shows the 'Service List' pane with a table of 22 services.

Node Name	Severity	Type	Time Stamp	Obj
SAS1_CLS_Jeddah	Critical	IMPROPRMVL	04/10/2026, 12:56:28.000 (UTC+00:00)	
SAS1_CLS_Port_Sudan	Critical	IMPROPRMVL	04/10/2026, 12:56:27.000 (UTC+00:00)	
SAS1_CLS_Port_Sudan	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:29.000 (UTC+00:00)	
SAS1_CLS_Jeddah	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:25.000 (UTC+00:00)	
SAS1_CLS_Port_Sudan	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:19.000 (UTC+00:00)	

Name	Type	Source	Destination	Description	Control Plane	Lifecycle State	Error
CC_onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0_0	OCH-CC	SAS1_CLS_Jeddah 8/3/1	SAS1_CLS_Port_Sudan 8/3/1		CPCE	INSTALLED	
onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah	SAS1_CLS_Port_Sudan		CPCE	INSTALLED	
(Carrier) onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah 8/3/0	SAS1_CLS_Port_Sudan 8/3/0		CPCE	INSTALLED	
onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah	SAS1_CLS_Port_Sudan		CPCE	INSTALLED	
(Carrier) onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah 8/3/0	SAS1_CLS_Port_Sudan 8/3/0		CPCE	INSTALLED	

When you select the protect path, you can see the alarms for the Protect channel only and topology highlights only that protect channel.

Figure 89: Alarms and topology for PSM Protect path channel

The screenshot displays the Cisco Optical Network Controller interface. The top section shows the 'Alarms' tab with a message: 'Showing alarm(s) for the selected service: onc\_SAS1\_CLS\_Jeddah\_8/3/0\_SAS1\_CLS\_Port\_Sudan\_8/3/0'. Below this, a table lists 4 alarms, all of which are 'Major' severity and 'FPD-UPG-REQUIRED' type, occurring on 04/10/2026 at various times.

The middle section shows the 'Service List' with 22 services. The 'Service on top' checkbox is checked. The selected service is 'onc\_SAS1\_CLS\_Jeddah\_8/3/0\_SAS1\_CLS\_Port\_Sudan\_8/3/0', which is in an 'INSTALLED' state and has a 'PROTECT' status. The table below shows details for several services:

Name	Type	Source	Destination	Description	Control Plane	Lifecycle State	Error
CC_onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-CC	SAS1_CLS_Jeddah 8/3/1	SAS1_CLS_Port_Sudan 8/3/1		CPCE	INSTALLED	
onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah	SAS1_CLS_Port_Sudan		CPCE	INSTALLED	
(Carrier) onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah 8/3/0	SAS1_CLS_Port_Sudan 8/3/0		CPCE	INSTALLED	
onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah	SAS1_CLS_Port_Sudan		CPCE	INSTALLED	
(Carrier) onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah 8/3/0	SAS1_CLS_Port_Sudan 8/3/0		CPCE	INSTALLED	

The bottom section shows the 'Topology' view, which displays a map of the network with nodes and links. The selected service is highlighted in green, and the topology shows the path between SAS1\_CLS\_Jeddah and SAS1\_CLS\_Port\_Sudan.

When you select the Work path, you can see the alarms for work channel only and topology highlights only the Work channel.

Figure 90: Alarms and topology for PSM Work path channel

The screenshot displays the Cisco Optical Network Controller interface. The top section shows 'Circuit Monitoring' with a date of 04/15/2026, 11:14:53 (UTC+00:00). Below this, there are 'Alarms' and 'Topology' sections.

**Alarms Section:**

Node Name	Severity	Type	Time Stamp
SAS1_CLS_Port_Sudan	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:29.000 (UTC+00:00)
SAS1_CLS_Jeddah	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:25.000 (UTC+00:00)
SAS1_CLS_Port_Sudan	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:19.000 (UTC+00:00)
SAS1_CLS_Jeddah	Major	FPD-UPO-REQUIRED	04/10/2026, 12:54:18.000 (UTC+00:00)

**Topology Section:**

The topology map shows a geographical view of the network with nodes and links. Nodes are represented by icons for ROADM, ILA, RAMAN Amplified, and Submarine Link. Links are represented by lines with degree numbers. The map shows a path between SAS1\_CLS\_Jeddah and SAS1\_CLS\_Port\_Sudan.

**Service List Section:**

Name	Type	Source	Destination	Description	Control Plane	Lifecycle State	Error
CC_onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0_0	OCH-CC	SAS1_CLS_Jeddah 8/3/1	SAS1_CLS_Port_Sudan 8/3/1		CPCE	INSTALLED	
onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah	SAS1_CLS_Port_Sudan		CPCE	INSTALLED	
(Carrier) onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah 8/3/0	SAS1_CLS_Port_Sudan 8/3/0		CPCE	INSTALLED	
onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah	SAS1_CLS_Port_Sudan		CPCE	INSTALLED	
(Carrier) onc_SAS1_CLS_Jeddah_8/3/0_SAS1_CLS_Port_Sudan_8/3/0	OCH-Trail	SAS1_CLS_Jeddah 8/3/0	SAS1_CLS_Port_Sudan 8/3/0		CPCE	INSTALLED	

**Step 5** In the **Detailed Service Path** tab, check the selected PSM wavelength circuit.

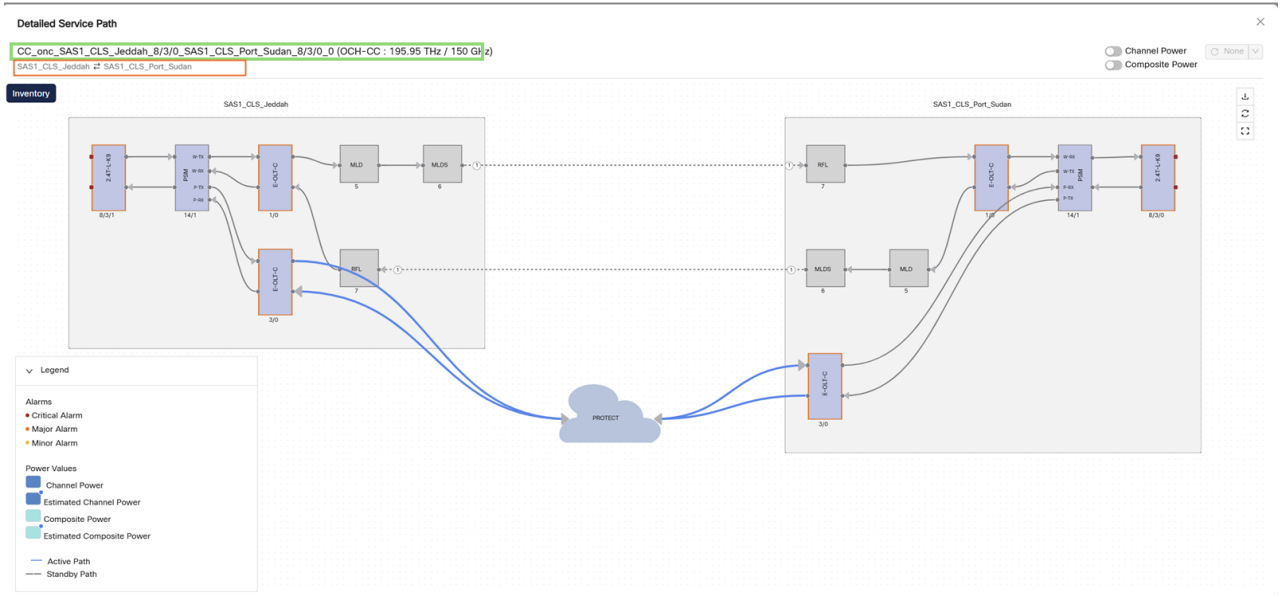
**Note**

- The **Detailed Service Path** displays all the equipments crossed by the circuit. The active path appears in blue and the standby path in Grey color.
- The blue arrows indicate the RX direction of the light for a given PSM.

**Note**

- From Release 26.1.1, the NCS 1001 PSM Wavelength Circuit Workspace has these UI enhancements.
- The **Detailed Service Path**.
  - Highlights the active path between the NCS 1001 PSM nodes.
  - Displays the equipment between the NCS 1010 OLT nodes as a cloud.

Figure 91: Detailed service path for PSM wavelength service



Cisco Confidential

Figure 92: Detailed service path for PSM work path channel

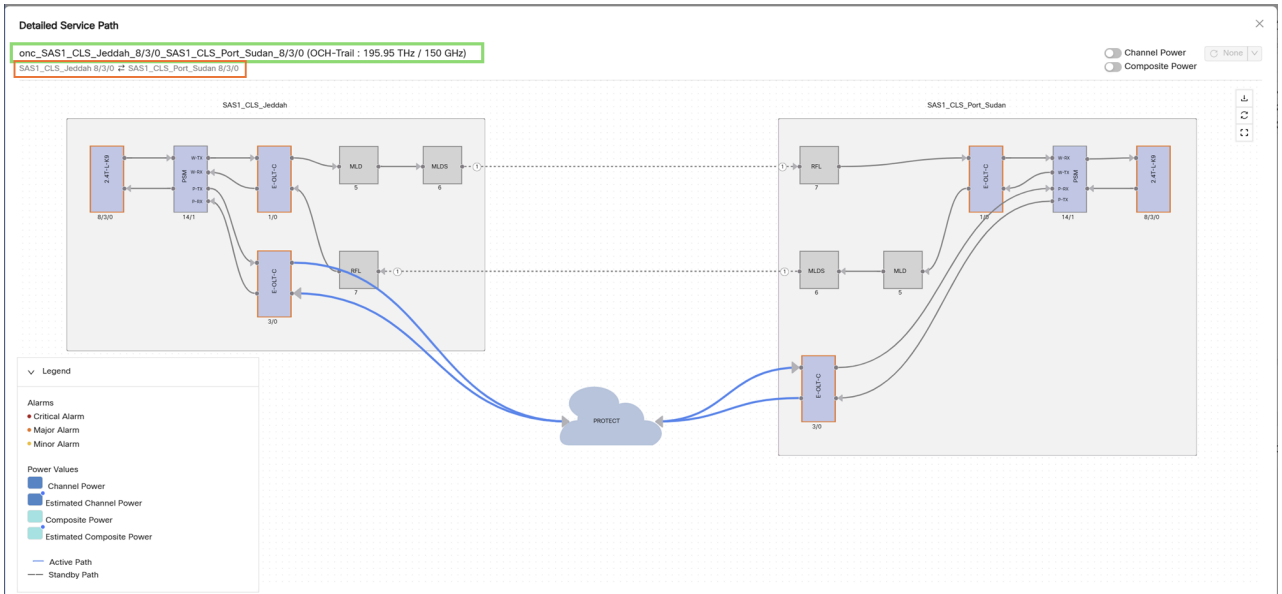
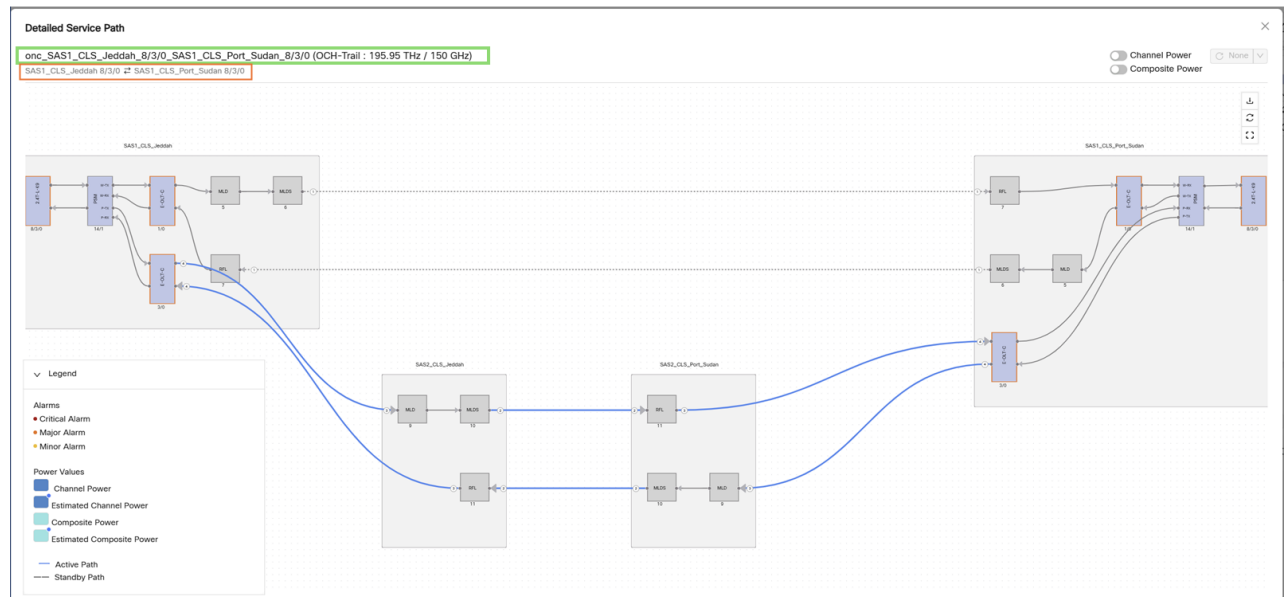


Figure 93: Detailed service path for PSM Protect path channel



Cisco Confidential

**Step 6** In the **Service History** tab, check the change of events in the PSM wavelength circuit.

- From R26.1.1, service history is now enabled for PSM service to show discovery events, operation state changes, and switch events.

Figure 94: Service History for PSM Protect path channel

The screenshot shows the Cisco Optical Network Controller interface. The top section is titled "Circuit Monitoring" and displays a list of 22 services. The selected service is "CC\_onc\_SAS1\_CLS\_Jeddah\_8/3/0\_SAS1\_CLS\_Port\_Sudan\_8/3/0\_0" of type "OCH-CC". Below the service list, the "Detailed service path" section shows "Service History" with 1 event. The event details are as follows:

Time	Event Type	Event Name	Description	Details
04/15/2026, 06:02:17.564 (UTC+00:00)	Info	SERVICE_STATE_CHANGED	Service state changed from ENABLED to DISABLED	<a href="#">View More</a>

- Unidirection service states are supported and displayed at channel level.
- If only one of the channel is discovered, work or protect, then the controller marks the service as PARTIAL. When that channel and carrier is INSTALLED, then the service moves to INSTALLED when other channel is discovered.
- If a path is standby in both directions, then it will show up as dotted line in topology in Circuit monitoring workspace.
- If different paths are active in different directions, then we will not see dotted line.

## Forwarding Syslogs

The syslog forwarding feature help in:

- Storing logs from the client VMs in the server VM.
- Allowing multiple client VMs to send logs to the same server VM.
- Server installation is done only once.
- The server's database stores all logs.

You need to run the commands from the client VMs to configure the server using the script provided.

### Install Syslog on Server

To install syslog feature on the server run the CLI commands given in the example:

Create the rsyslog server using steps provided in below website  
<https://www.makeuseof.com/set-up-linux-remote-logging-using-rsyslog/>

To create the folder structure  
 AUDIT logs here → /var/log/<host-ip>/audit.log  
 ONC service logs here → /var/log/<host-ip>/service\_logs/

Add the below lines in the rsyslog.conf file

```
$ModLoad imudp
$UDPServerRun 514

Input (type="imudp" port="514" ruleset="rs1")

template (name="ServLogLoc" type="string"
string="/var/log/%FROMHOST-IP%/service_logs/%syslogtag%.log")
template (name="AuditLogLoc" type="string" string="/var/log/%FROMHOST-IP%/audit.log")

Ruleset (name="rs1") {
:msg, contains, "audit" ?AuditLogLoc
*.* ?ServLogLoc
}
```

Restart syslog server using command,  
systemctl restart rsyslog

Check if rsyslog service is active and running using command,  
systemctl status rsyslog

### Install Syslog on Client

To install syslog server forwarding in client run the CLI commands in the example:

```
sedo syslog server create <IP> <PROTOCOL> <IP> <PORT>
IP is the address of the syslog server.
Protocol to be used - udp or tcp.
Port on which syslog server is listening to (default is 514)
```

To create a syslog query to forward the application logs of a particular Cisco Optical Network Controller app:

```
sedo syslog query create '{namespace="onc", app="<app_name>", container="app"}' LOG_INFO
LOG_USER <app_name> <IP>
```




---

**Note** The query inside single quotes is Grafana Loki's logQL, it can be tweaked according to user needs

---

To list all syslog queries:

```
sedo syslog query list
```

To list all syslog servers:

```
sedo syslog server list
```

To delete a syslog query:

```
sedo syslog query delete <QUERY_ID>
```

To delete a syslog server:

```
sedo syslog server delete <IP>
```