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 appplications.

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

Step 4 Export the current table.

a) Click **Export** to export the details of any table from any application screen to a spreadsheet file.

b) 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 5 Export all data relevant to the current application.

a) Click **Export** to export the details of any table from any application screen to a spreadsheet file.

b) 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.

c) Click **Generate** to initiate file generation.

Step 6 Use the **Sort** option to sort the table values.

Step 7 Use the **Filter** option to filter the table content as per requirement in each application screen.

Topology

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 **OTS** or **OMS** layers as options in the display. 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 **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.

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.

On the top of this screen, there is a panel for displaying the different alarm types and the count of each type of alarm that are part of the network. 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
RED	Critical alarms are displayed in red color.
ORANGE	Major alarms are displayed in orange color.
YELLOW	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.

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. Right click on any node in the map to select **Resync**, **View in Node UI** and **View Alarms** options.

Table 2: Topology Node Options

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

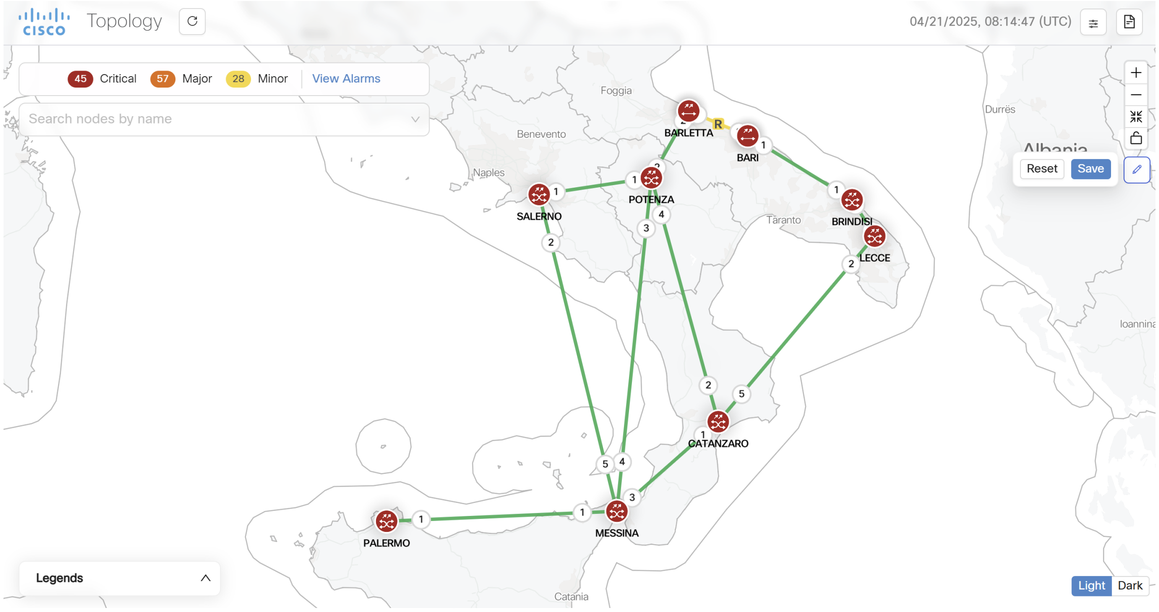
You can also view the information related to the different nodes, links, and the states of each node in the network at any point in time by clicking the **Legends** option. To select any node in the network, use the drop-down box to select the node.

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.

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

Figure 1: Topology Application



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 Raman 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 atleast 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 om 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.

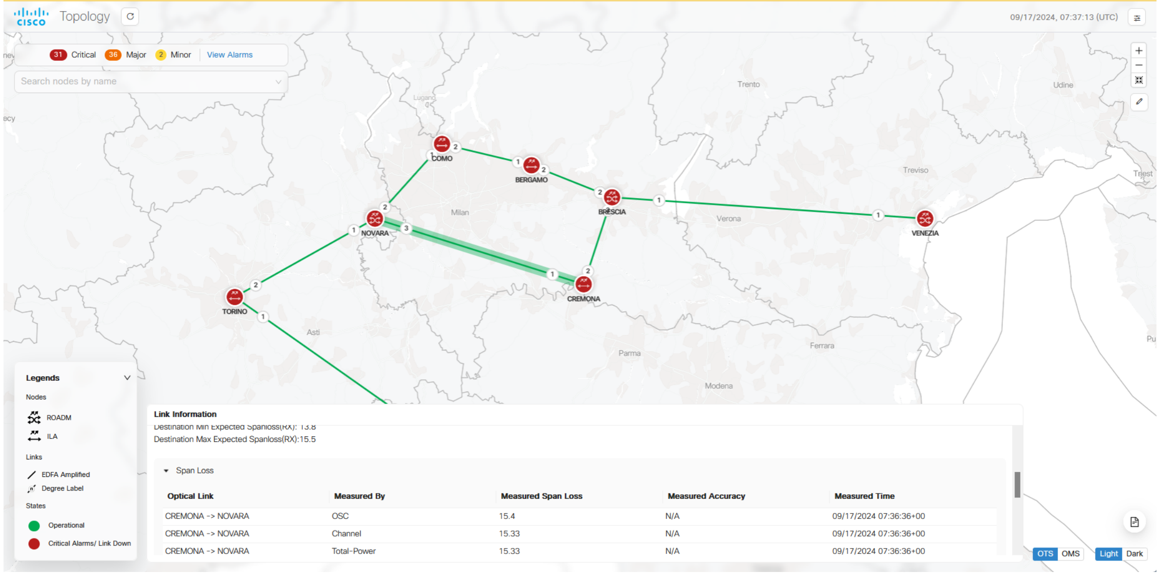
From Cisco Optical Network Controller 24.3.1 release onwards, fiber information and span loss details are added newly to the **Topology** live PM tool tip. When you click on the fiber sapn link in the map, you will see the following details appearing in the tool tip information:

- **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.

Note

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

Figure 2: Topology Live PM



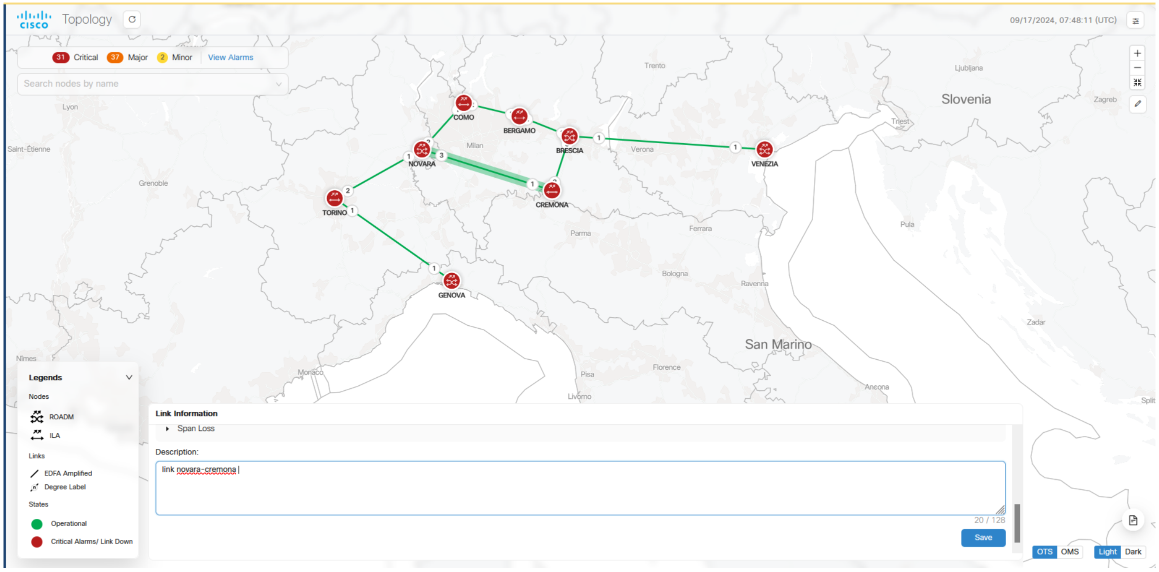
Link Information

Destination Min Expected Spanloss(RX): 13.8
Destination Max Expected Spanloss(RX):15.5

▾ Span Loss

Optical Link	Measured By	Measured Span Loss	Measured Accuracy	Measured Time
CREMONA -> NOVARA	OSC	15.4	N/A	09/17/2024 07:36:36+00
CREMONA -> NOVARA	Channel	15.33	N/A	09/17/2024 07:36:36+00
CREMONA -> NOVARA	Total-Power	15.33	N/A	09/17/2024 07:36:36+00

Figure 3: Tool Tip



Link Information

▸ Span Loss

Description:

link novara-cremona

20 / 128

Save

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 that is part of a service at any given point in time. 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, the original node name in the network is used by Cisco Optical Network Controller.
- **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 Location**: 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.

Note

- 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 go localtion 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 operations, Cisco Optical Network Controller pushes the current node name to the node, ensuring consistency even if changes were missed while the device was offline.

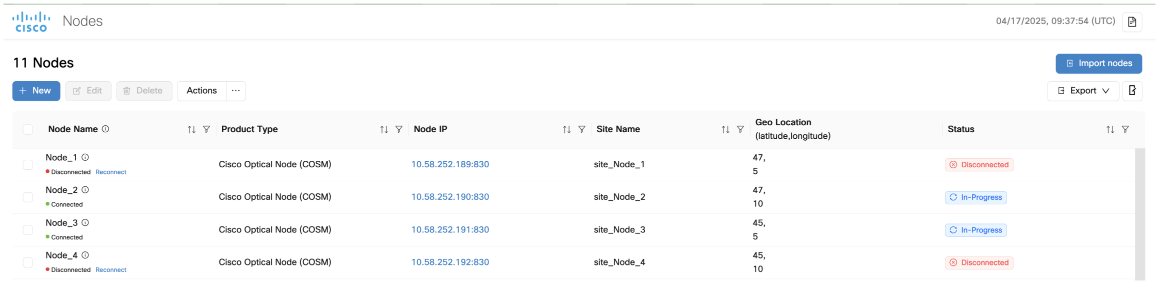
- **Status**: The status of each node within the network to know whether it is discovered or disconnected.

Use the information icon that appears along with each node in this table for viewing the additional details pertaining to each node. The tooltip contains these details:

- Site Description
- Message: Information about any error conditions
- Created by: The user who added the node
- Created Date

- Modified Date

Figure 4: Nodes



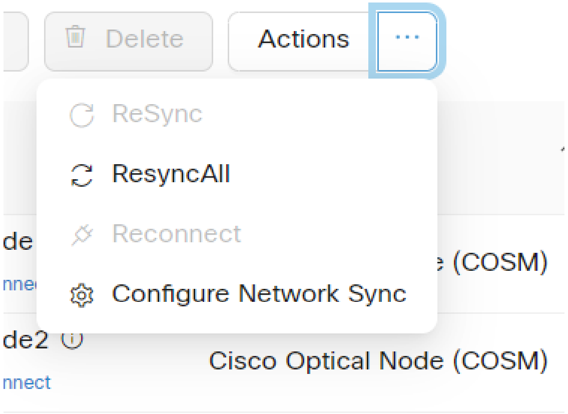
Node Name	Product Type	Node IP	Site Name	Geo Location (latitude,longitude)	Status
Node_1 Disconnected Reconnect	Cisco Optical Node (COSM)	10.58.252.189:830	site_Node_1	47, 5	Disconnected
Node_2 Connected	Cisco Optical Node (COSM)	10.58.252.190:830	site_Node_2	47, 10	In-Progress
Node_3 Connected	Cisco Optical Node (COSM)	10.58.252.191:830	site_Node_3	45, 5	In-Progress
Node_4 Disconnected Reconnect	Cisco Optical Node (COSM)	10.58.252.192:830	site_Node_4	45, 10	Disconnected

Use the sort or filter options to sort and filter values in the table. You can also cross launch to other supported pages 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. There are four options available for this purpose.

- **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 **Periodic Network Full Sync**.

Figure 5: Actions



Note

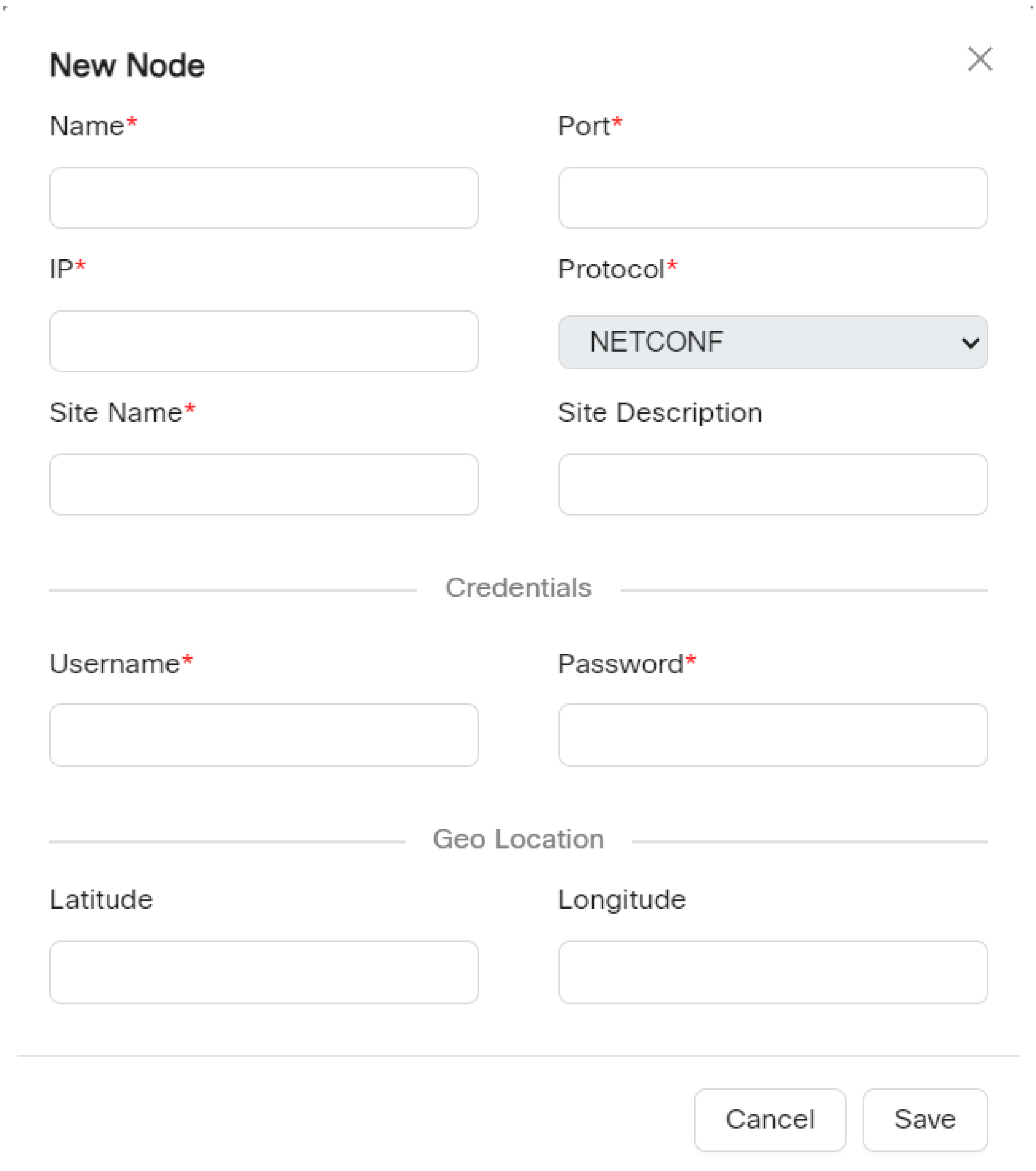
- Latitude and longitude values can be set in both Cisco Optical Site Manager and Cisco Optical Network Controller. The following scenarios are possible:
  - **Geo location is set in both Cisco Optical Site Manager and Cisco Optical Network Controller**: Cisco Optical Network Controller geo location 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 coming from Cisco Optical Site Manager have more than four digits, they are shortened to up to four digits only and displayed.

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 6: Add New Node



Protocol* NETCONF

Before you begin

To add nodes to Cisco Optical Network Controller:

- Cisco Optical Site Manager must be installed on the node.
- All 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 create 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 Enter the device details necessary connect to the device as given in the table below.

Table 3: Add new node

Name	Description	Mandatory
Name	Name of the new node you are adding	Yes
IP	IP address of the new node which you are adding.	Yes
Port	The port number of the new node which you are adding.	Yes
Protocol	The protocol used for the new node which you are adding.	Yes
Site Name	The name of the site to which the new node belongs.	Yes
Username	The username you want to set for accessing the new node.	Yes
Password	The password you want to set 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 you which you want to assign for the new node to set its location.	No
Longitude	The Longitude co-ordinate value you which you want to assign for the new node to set its location.	No

Note

- Ensure that you enter valid a username and password of the device to enable Cisco Optical Network Controller to connect to the device.

Step 4 Click **Save**.The new node or device is onboarded successfully and added to the **Nodes** table. Cisco Optical Network Controller validates the connection with the onboarded device.

Import Nodes on Cisco Optical Network Controller

Before you begin

For importing the node details from any spreadsheet into the table, use the procedure given below.

Procedure

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

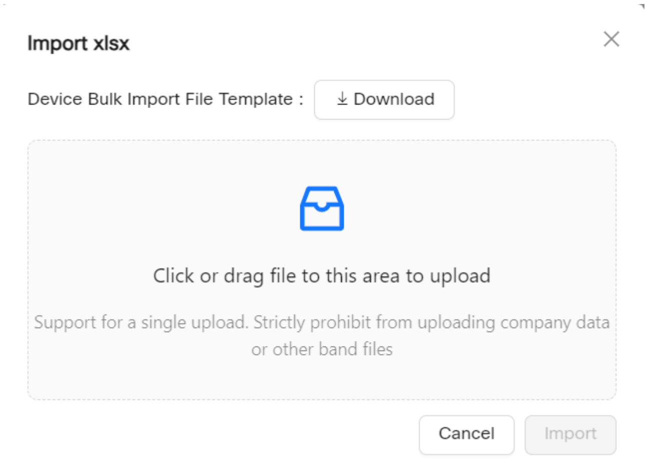
Step 2 Click **Import** to import the table details from external files.

Step 3 Select the spreadsheet which has all the node details and click **Open**. The new nodes are onboarded and added to the **Nodes** table.

To add the details of the nodes in a bulk format use the **Import nodes** option.

Note
Click **Download** option to get the sample template of the bulk import file.

Figure 7: Import Nodes

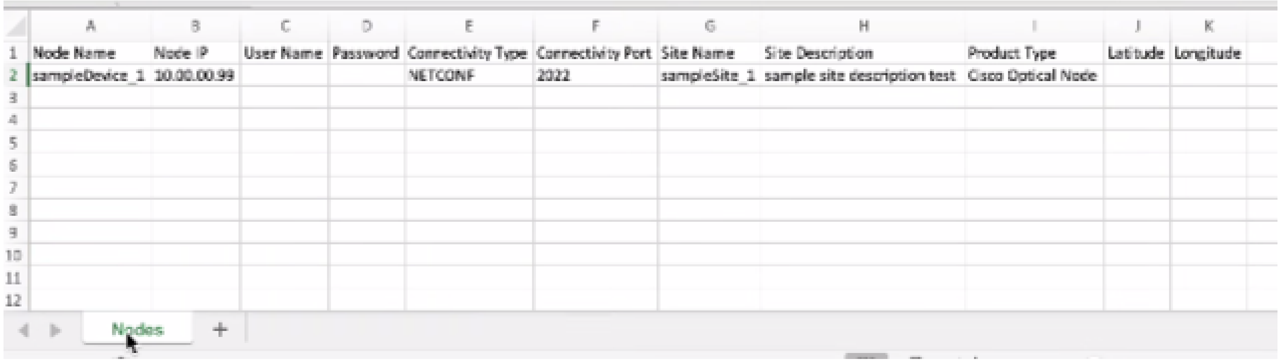


Import xlsx

Device Bulk Import File Template :

Click or drag file to this area to upload

Support for a single upload. Strictly prohibit from uploading company data or other band files



	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											
10											
11											
12											

The sample bulk import template has the following fields which need to be filled before importing node details.

Table 4: Bulk Import File Template

Name	Description
Node Name	Name of the host node.
Node IP	The IP address of the node you are adding.
User Name	The username you want to set for accessing the new node.
Password	The password you want to set for accessing the new node.
Connectivity Type	The type of the protocol used for connecting the node.
Connectivity Port	The port number of the node. Port number 2022 for NCS 1000 series nodes. Port number 830 for NCS 2000 series nodes.
Site Name	The name of the site to which the new node belongs.
Site Description	The description of the site to which the new node belongs.
Product Type	Type of the node.
Latitude	The Latitude co-ordinate value you which you want to assign for the new node to set its location.
Longitude	The Longitude co-ordinate value you which you want to assign for the new node to set its location.

Cisco Optical Network Controller shows a messsage `Import in progress` during the import process.

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

Before you begin

Use the **Delete** option to delete one or more nodes at any given time. Follow the procedure given below.

Procedure

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

Step 2 Select the node or nodes to be deleted.

Step 3 Click **DELETE**.

This will delete the selected node from the table.

Note

- We recommend to wait at least two minutes after device discovery completes before deleting the device.
- You cannot delete more than 5 nodes at a time.
- If the circuits are active and flowing over the nodes or if the resync is in progress, then deletion of the node fails. In this case you will receive an error message for the **Node Deletion Failure** when the circuit is spanning through the node.

  For example: <Device A> cannot be deleted because circuit spanning across the device.
- Do not perform delete operations and Geo-Redundancy Switchover simultaneously. Make sure there is no switchover taking place before you perform delete operations.

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.

Discovery Completed	All information has been collected from the device and it is ready for operations. **Note** It is recommended to wait for 60 secs once the device is turned to Discovery Completed state which ensures the device is ready for accepting requests.	

- **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.

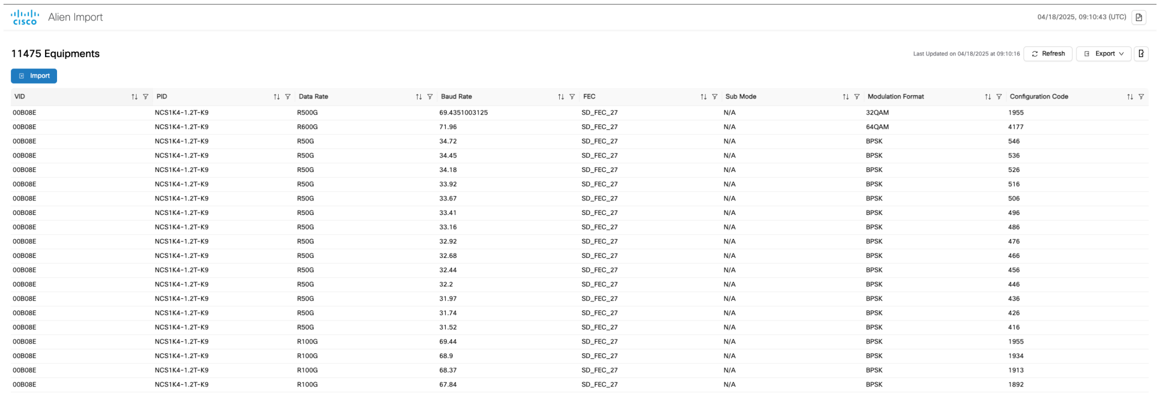
Alien Import

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 8: Alien Import



11475 Equipments

Last Updated on 04/18/2025 at 09:10:16

VID	PID	Data Rate	Baud Rate	FEC	Sub Mode	Modulation Format	Configuration Code
00B08E	NCS1K4-1.2T-K9	R500G	69.4351003125	SD_FEC_27	N/A	32QAM	1955
00B08E	NCS1K4-1.2T-K9	R600G	71.96	SD_FEC_27	N/A	64QAM	4177
00B08E	NCS1K4-1.2T-K9	R50G	34.72	SD_FEC_27	N/A	BPSK	546
00B08E	NCS1K4-1.2T-K9	R50G	34.45	SD_FEC_27	N/A	BPSK	536
00B08E	NCS1K4-1.2T-K9	R50G	34.18	SD_FEC_27	N/A	BPSK	526
00B08E	NCS1K4-1.2T-K9	R50G	33.92	SD_FEC_27	N/A	BPSK	516
00B08E	NCS1K4-1.2T-K9	R50G	33.67	SD_FEC_27	N/A	BPSK	506
00B08E	NCS1K4-1.2T-K9	R50G	33.41	SD_FEC_27	N/A	BPSK	496
00B08E	NCS1K4-1.2T-K9	R50G	33.16	SD_FEC_27	N/A	BPSK	486
00B08E	NCS1K4-1.2T-K9	R50G	32.92	SD_FEC_27	N/A	BPSK	476
00B08E	NCS1K4-1.2T-K9	R50G	32.68	SD_FEC_27	N/A	BPSK	466
00B08E	NCS1K4-1.2T-K9	R50G	32.44	SD_FEC_27	N/A	BPSK	456
00B08E	NCS1K4-1.2T-K9	R50G	32.2	SD_FEC_27	N/A	BPSK	446
00B08E	NCS1K4-1.2T-K9	R50G	31.97	SD_FEC_27	N/A	BPSK	436
00B08E	NCS1K4-1.2T-K9	R50G	31.74	SD_FEC_27	N/A	BPSK	426
00B08E	NCS1K4-1.2T-K9	R50G	31.52	SD_FEC_27	N/A	BPSK	416
00B08E	NCS1K4-1.2T-K9	R100G	69.44	SD_FEC_27	N/A	BPSK	1955
00B08E	NCS1K4-1.2T-K9	R100G	68.9	SD_FEC_27	N/A	BPSK	1934
00B08E	NCS1K4-1.2T-K9	R100G	68.37	SD_FEC_27	N/A	BPSK	1913
00B08E	NCS1K4-1.2T-K9	R100G	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.

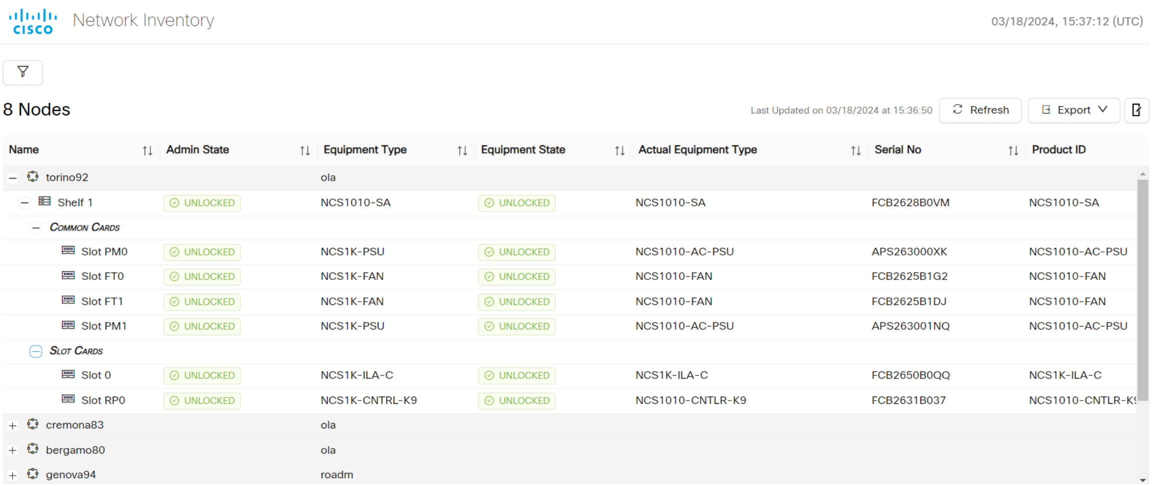
Step 6 Use the sort or filter options to sort and filter values in the table.

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 9: Network Inventory



8 Nodes

Last Updated on 03/18/2024 at 15:36:50

Name	Admin State	Equipment Type	Equipment State	Actual Equipment Type	Serial No	Product ID
– torino92		ola				
– Shelf 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-CNTLR-K9	FCB2631B037	NCS1010-CNTLR-K
+ 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-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 10: Select multiple toggle

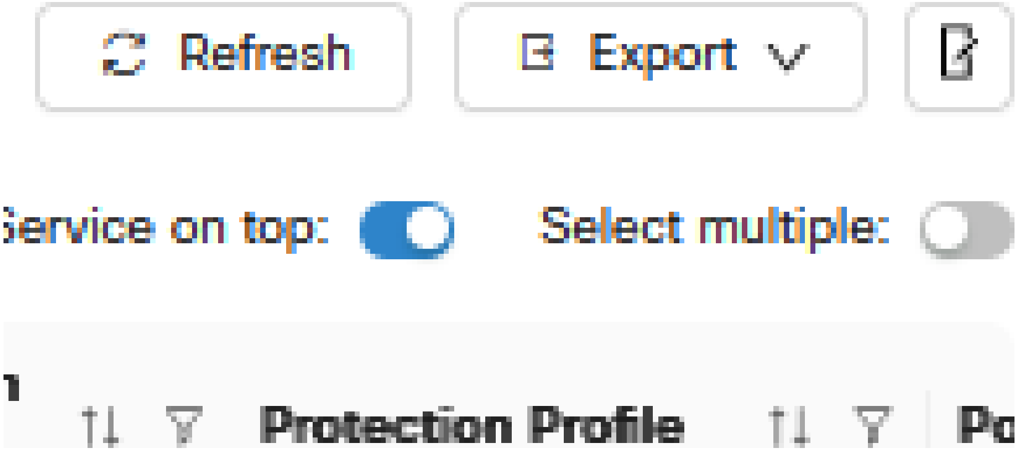
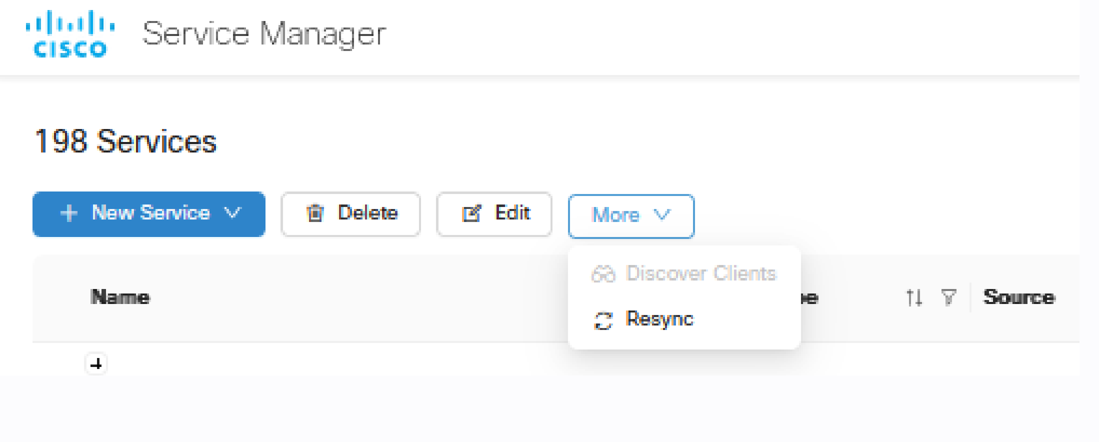


Figure 11: Resync option for GMPLS circuits

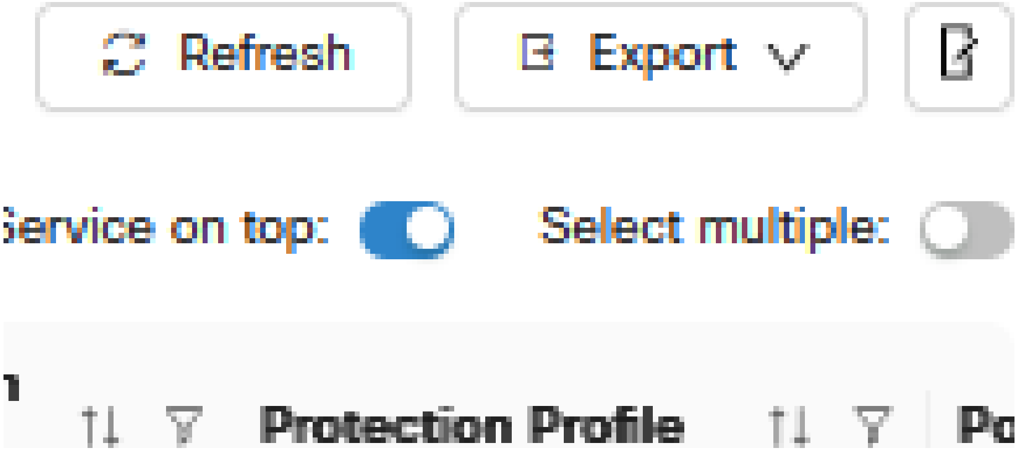


- Resyncing can resolve lifecycle state issues, for example, when the circuit is in PARTIAL, where clients are not discovered properly or are in an ambiguous state.
- When multiple services are selected, the **More** button is replaced with a **Resync** button.
- Resyncing a trail service also resyncs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

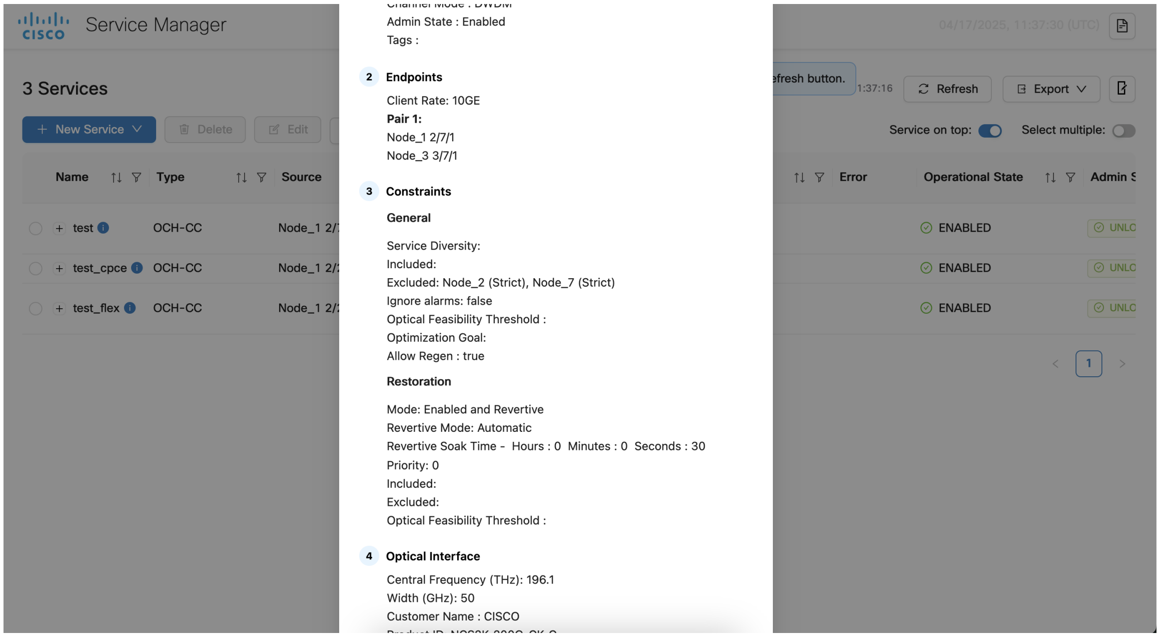
Figure 12: Service on top and Select multiple toggles



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 13: Service Manager



Name	Type	Source	Error	Operational State	Admin S
test	OCH-CC	Node_1 2/		ENABLED	UNLO
test_cpce	OCH-CC	Node_1 2/		ENABLED	UNLO
test_flex	OCH-CC	Node_1 2/		ENABLED	UNLO

Channel Mode : DWDM
Admin State : Enabled
Tags :

2 **Endpoints**

Client Rate: 10GE
Pair 1:
Node_1 2/7/1
Node_3 3/7/1

3 **Constraints**

General

Service Diversity:
Included:
Excluded: Node_2 (Strict), Node_7 (Strict)
Ignore alarms: false
Optical Feasibility Threshold :
Optimization Goal:
Allow Regen : true

Restoration

Mode: Enabled and Revertive
Revertive Mode: Automatic
Revertive Soak Time - Hours : 0 Minutes : 0 Seconds : 30
Priority: 0
Included:
Excluded:
Optical Feasibility Threshold :

4 **Optical Interface**

Central Frequency (THz): 196.1
Width (GHz): 50
Customer Name : CISCO

Service manager table fields

Column	Values	Description
Name		Name of the service

Column	Values	Description
Type	OCH-NC	Type of the service
	OCH-Trail	
	OCH-CC	
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_HANDOVER	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. **Note** Cisco Optical Network Controller does not support circuit repair in release 25.1.1.
	GMPLS_SYNC_IN_PROGRESS	GMPLS controller has acceptedthe 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	The circuit is configured with PSM protection to ensure service availability in case of failure.
	UNPROTECTED	The circuit is not configured with any protection mechanism, and may be subject to service disruption 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
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.

Provision CPCE services

Use the following procedure to create and manage 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.

Before you begin

Table 5: Supported transponder cards and modes

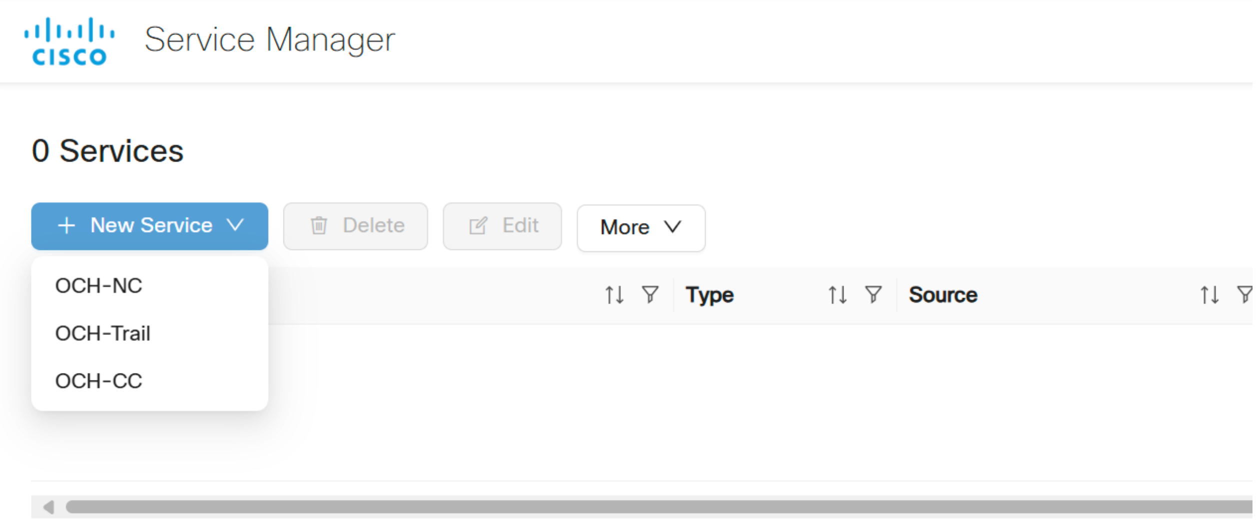
Card	Modes Supported
NCS1K4-2-QDD-C-K9	MXP-SLICE: 200G, 300G, 400G trunk and 100G and OTU4 client
NCS1K4-QXP-K9	MXP-SLICE: 400G trunk with 400G and 100G client
NCS1K4-OTN-XP	MXP: 4x100G TXP: 400G 400G trunk with 100G, 10G and OTU2 clients
NCS1K14-2.4T-X-K9	MXP-SLICE: 400G, 600G, 800G, 1T, 1.2T trunk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

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**.

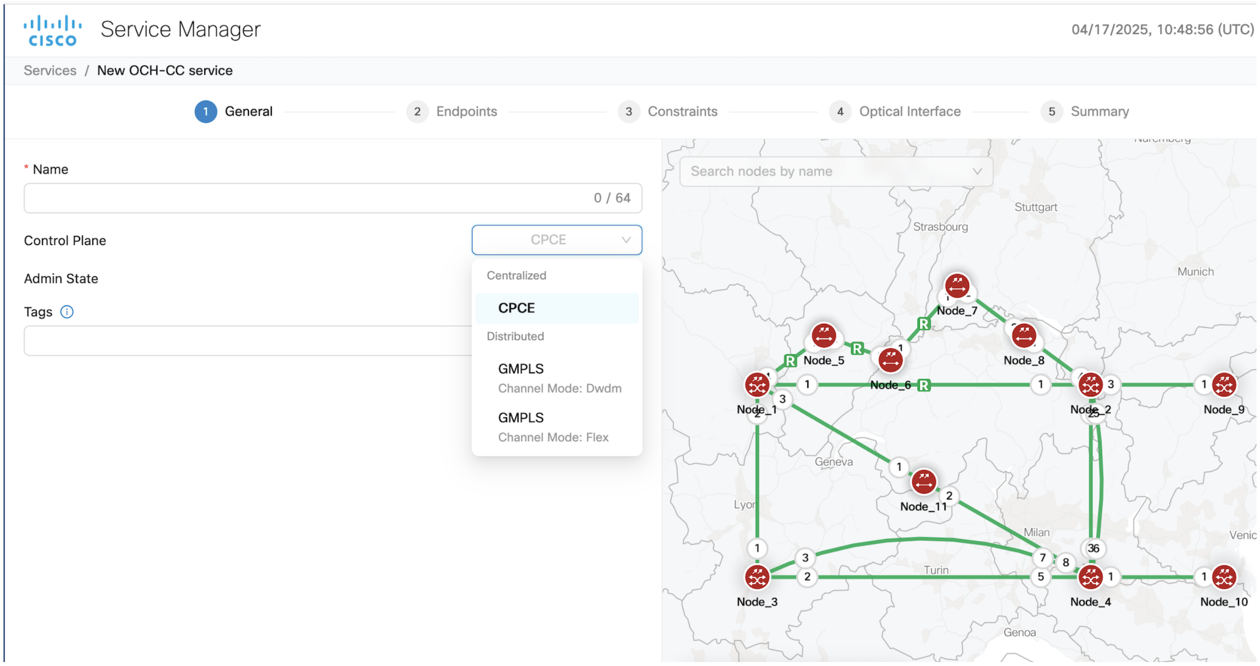


Step 2 Select **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

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 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.

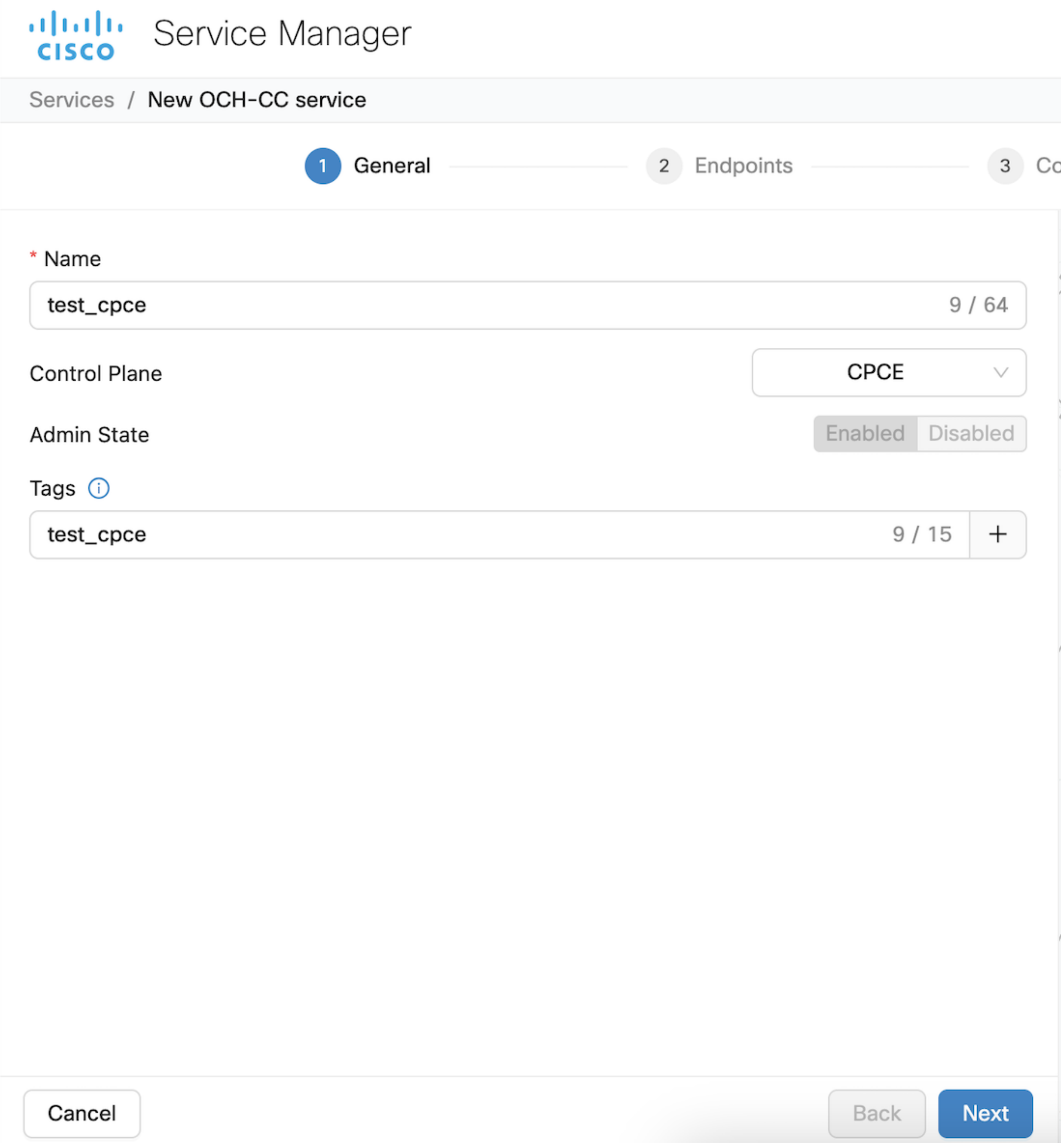
Figure 14: Service Manager



Service Manager launches the new service wizard.

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

Figure 15: Service Manager



* Name: test_cpce 9 / 64

Control Plane: CPCE

Admin State: Enabled Disabled

Tags: test_cpce 9 / 15

Table 6: General Parameters

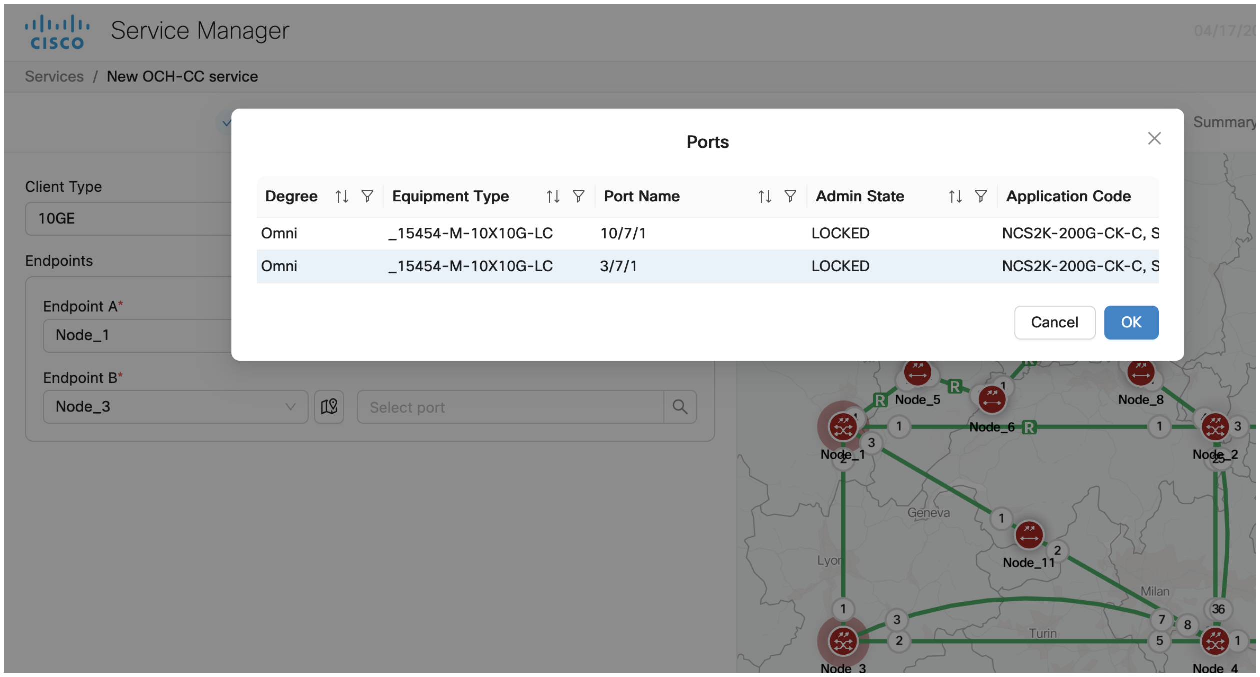
Field	Description	Values/restrictions
Name	The unique user defined name of the link.	(Allowed characters are a-z, A-Z, 0-9 and _. <Space not allowed>).

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 16: Service Manager



Service Manager

Services / New OCH-CC service

Client Type: 10GE

Endpoints

Endpoint A*: Node_1

Endpoint B*: Node_3

Ports

Degree	Equipment Type	Port Name	Admin State	Application Code
Omni	_15454-M-10X10G-LC	10/7/1	LOCKED	NCS2K-200G-CK-C, S
Omni	_15454-M-10X10G-LC	3/7/1	LOCKED	NCS2K-200G-CK-C, S

Table 7: Endpoints Parameters

Field	Description	Values/restrictions
Carrier Type		
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
Endpoints		
Endpoint A	Node and port of first endpoint	—

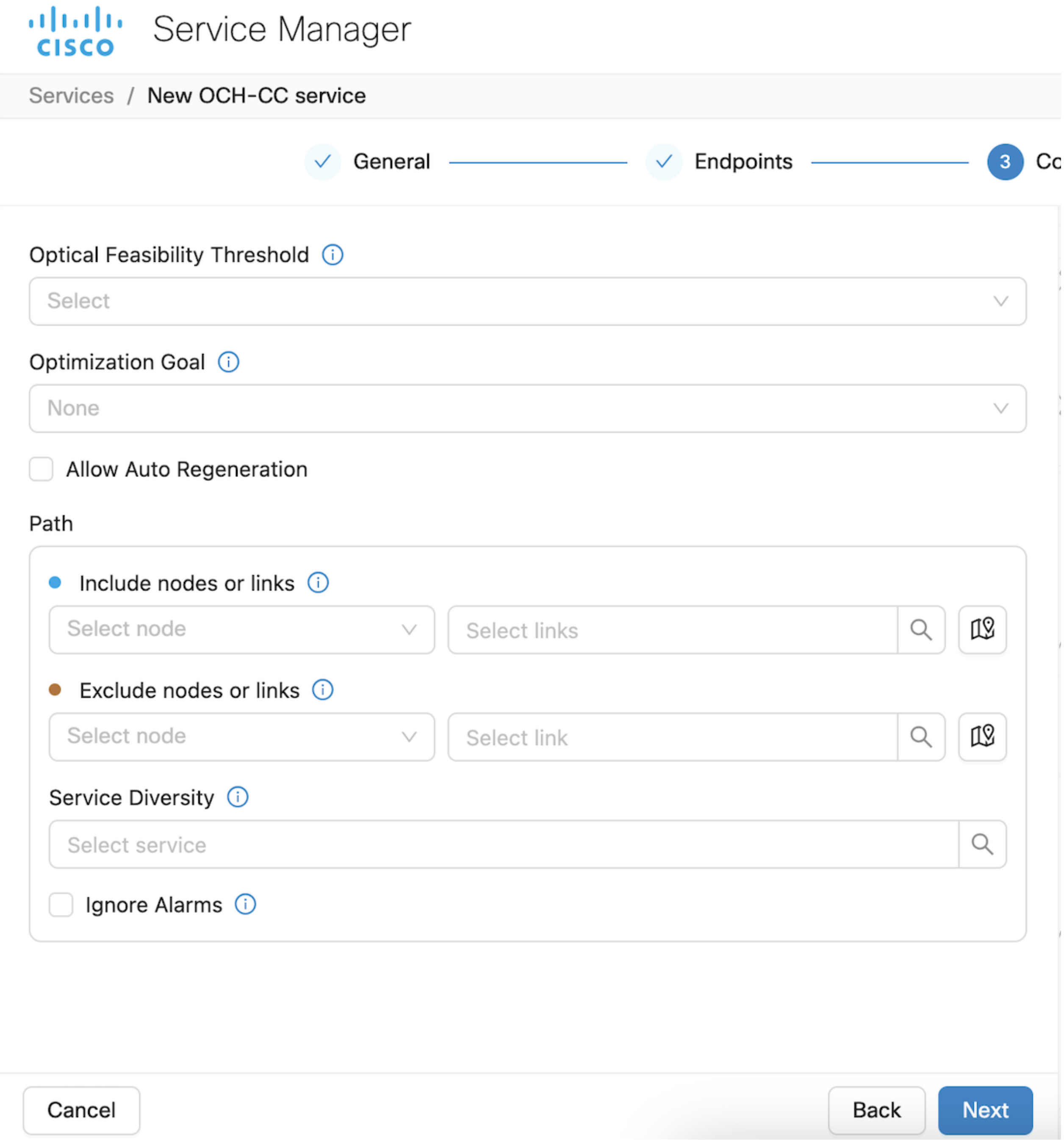
Field	Description	Values/restrictions
Endpoint B	Node and port of second endpoint	—

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 17: Service Manager



Service Manager

Services / New OCH-CC service

✓ General ✓ Endpoints 3 Co

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 dropdownfor 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.
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.

a) Update the name.

b) Click **Save**.

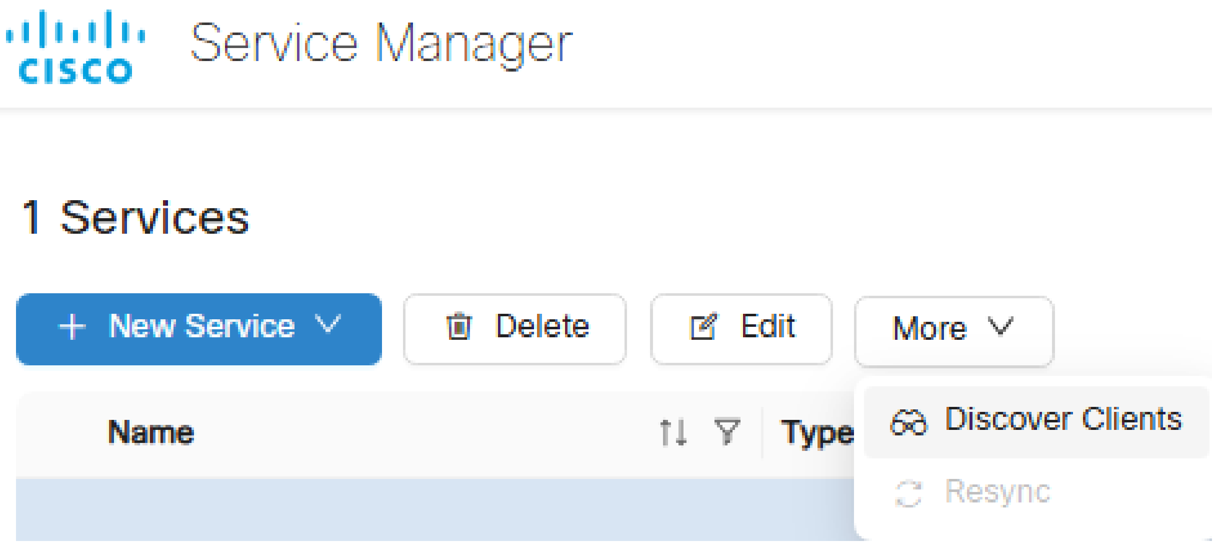
Step 11 Click **Delete** option to delete a selected service from the table.

Note

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

Step 12 Select an OCH-Trail circuit and click **More** > **Discover Clients** to discover all OCH-CC circuits over the selected trail.

Figure 18: Service Manager



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.

Step 14

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-XXXXX (XXXX.XX)) and Destination one (XXXXXXXX-XXXXX (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
COSM Node gets disconnected as soon as a service is provisioned in CONC	Config Failure	Delete the circuit and reprovision from the CONC.
COSM nodes are in sync state during CONC provisioning.	Config Failure	Check the COSM node and wait for synchronisation to complete.
NCS 1010 Devices under COSM Nodes are locked	Config Failure	• Check COSM and unlock the NCS 1010 device. • Verify COSM synchronisation status to be completed.
COSM node Restart during provisioning	Config Failure	Wait for CONC to re-establish the connection successfully after restart and its status moved to Discovery Completed in CONC.

Reload of the NCS 1010 device during provisioning from CONC	Config Failure	• Wait for the reload to complete on NCS 1010 device. • Verify the synchronisation is complete on COSM Node. • Wait for CONC to reestablish the connection successfully with COSM Node and its status moved to Discovery Completed.
Stale entries present in NCS 1010 while no cross connects present on COSM Nodes	Config Failure	• Clear the NCS1010 stale entries. • Wait for COSM node to complete the synchronisation.
Xcons Present in COSM Node along with NCS 1010	Config Failure	• Clear the XCONS on COSM and NCS 1010. • Wait for COSM node to complete the synchronisation and Discovery completed status.

Provision GMPLS services

Use the following procedure to create and manage circuits.

Before you begin

Table 10: Supported transponder cards and modes

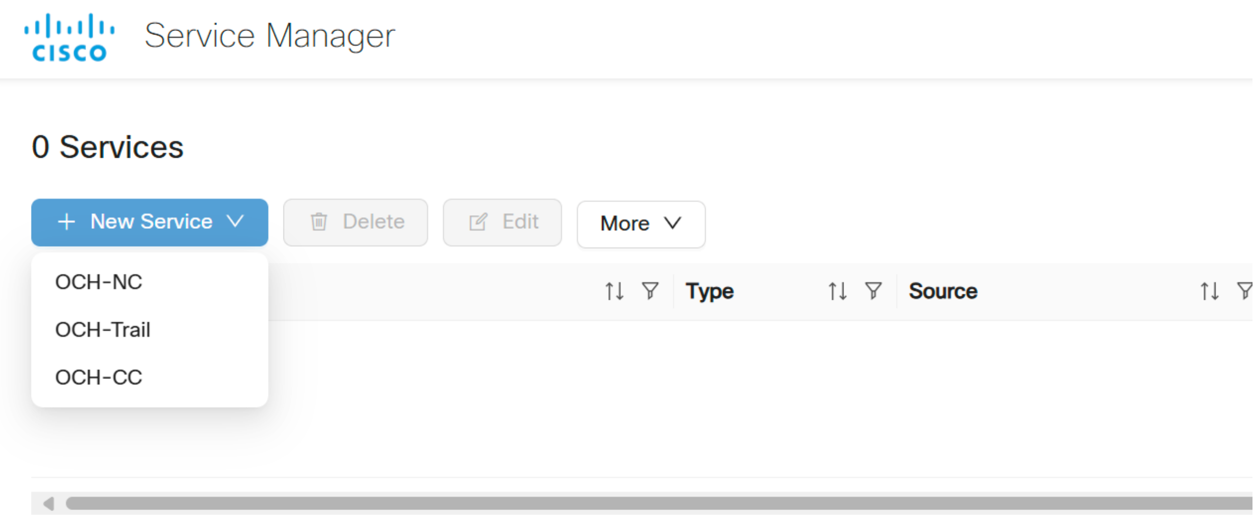
Card	Modes Supported
NCS1K4-2-QDD-C-K9	MXP-SLICE: 200G, 300G, 400G trunk and 100G and OTU4 client
NCS1K4-QXP-K9	MXP-SLICE: 400G trunk with 400G and 100G client
NCS1K4-OTN-XP	MXP: 4x100G TXP: 400G 400G trunk with 100G, 10G and OTU2 clients
NCS1K14-2.4T-X-K9	MXP-SLICE: 400G, 600G, 800G, 1T, 1.2T trunk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

Card	Modes Supported
NCS1K4-1.2T-K9	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
15454-M-10X10G-LC=	MXP 10x10G (with backplane connection to NCS2K-200G-CK-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients

Note Cisco Optical Network Controller supports OCH-CC circuits between client ports that have the same port number at both endpoints from release 25.1.1.

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**.

- **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.

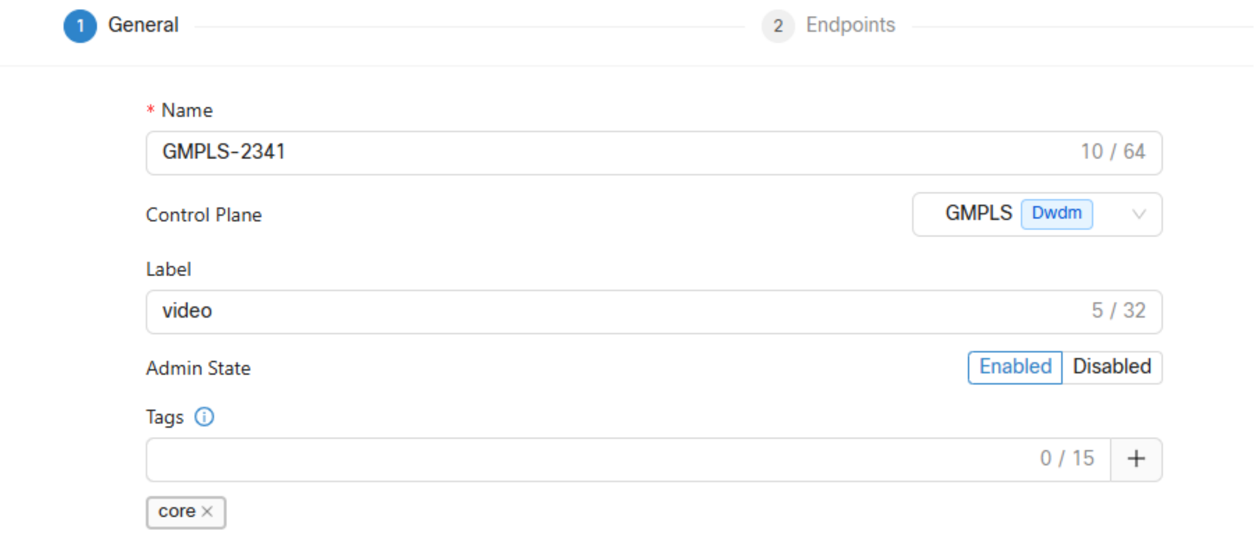
- **OCH-Trail**: An OCH-Trail is a circuit established between trunk ports of transponders or muxponders. This type of circuit typically transports aggregated traffic across the optical core network.

- **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 19: Service Manager



* Name: GMPLS-2341 10 / 64

Control Plane: GMPLS Dwdm

Label: video 5 / 32

Admin State: Enabled Disabled

Tags 0 / 15 +

core ×

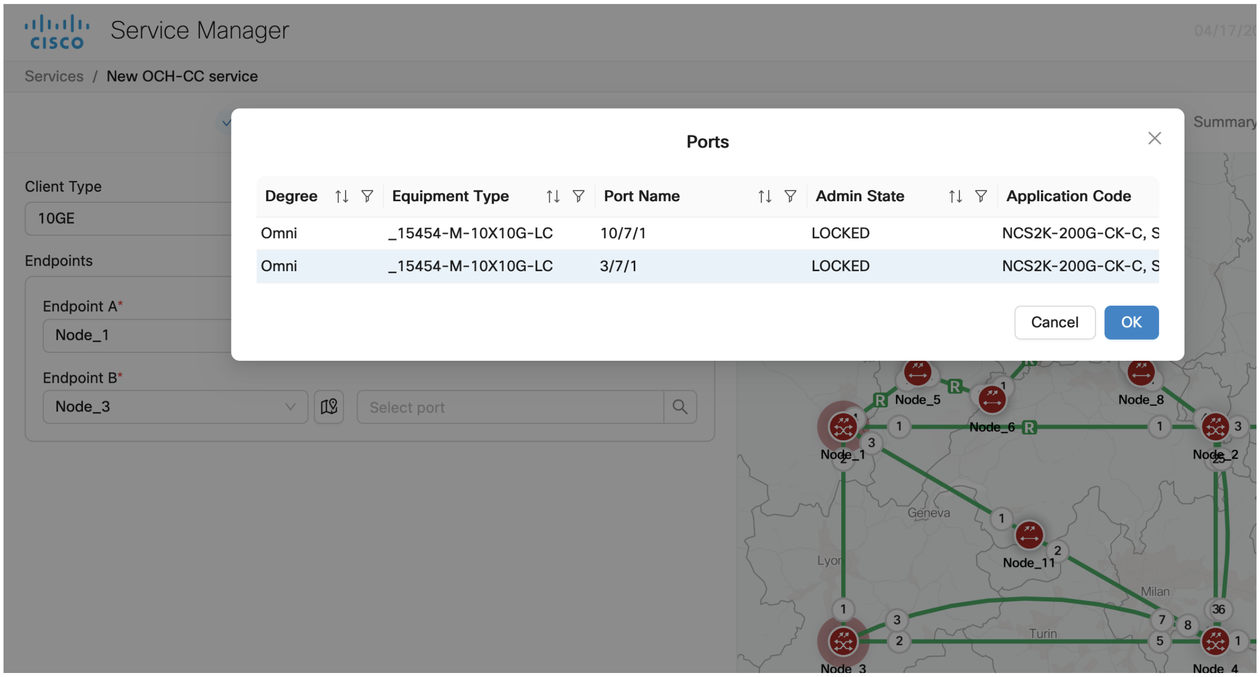
Table 11: General Parameters

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	Enabled or Disabled

Field	Description	Values/restrictions
Tags	Tags can be attached to the Service for better management, to group them together	—

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

Figure 20: Service Manager



Service Manager

Services / New OCH-CC service

Client Type

10GE

Endpoints

Endpoint A*

Node_1

Endpoint B*

Node_3

Select port

Ports

Degree	Equipment Type	Port Name	Admin State	Application Code
Omni	_15454-M-10X10G-LC	10/7/1	LOCKED	NCS2K-200G-CK-C, S
Omni	_15454-M-10X10G-LC	3/7/1	LOCKED	NCS2K-200G-CK-C, S

Table 12: Endpoints Parameters

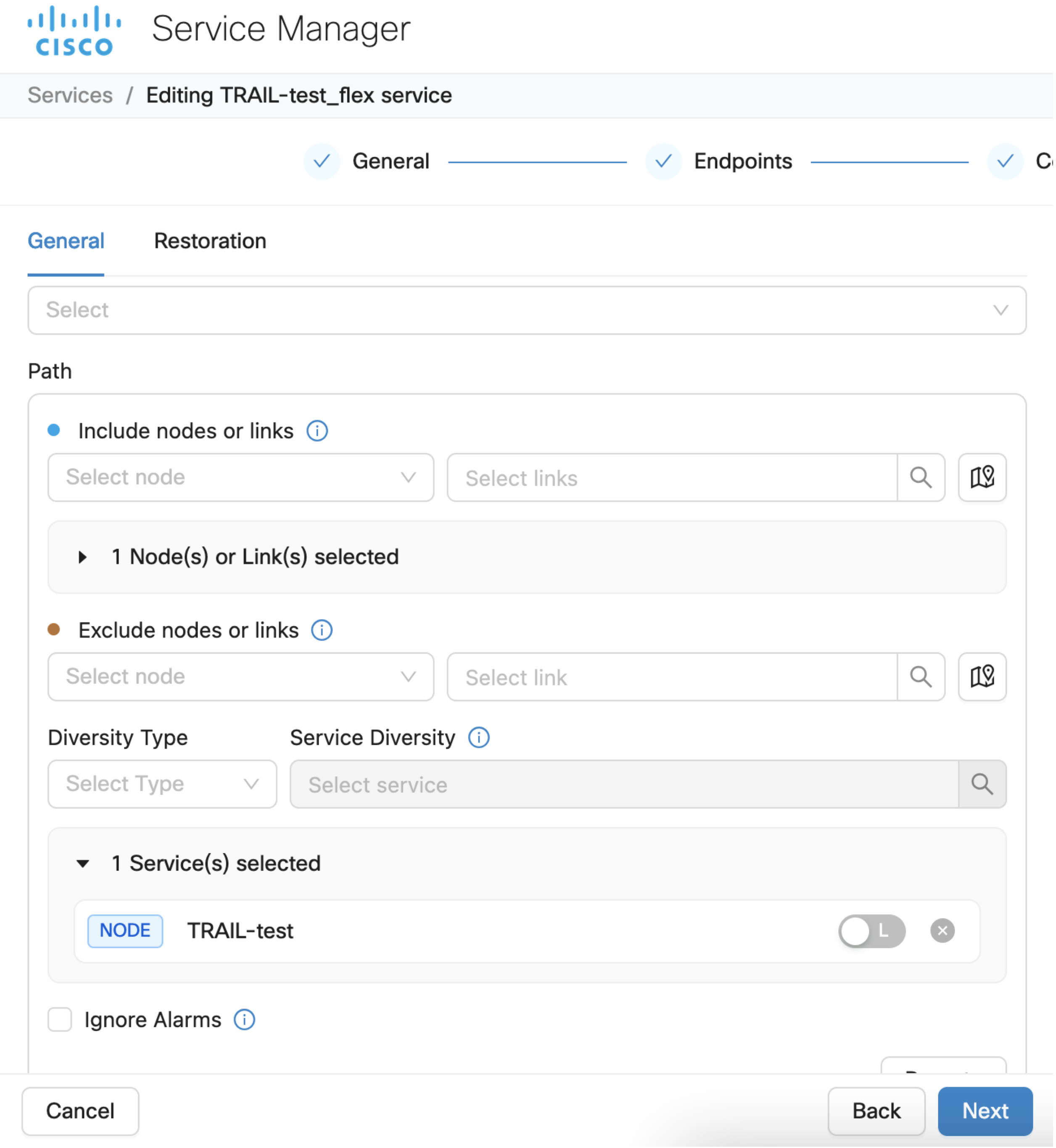
Field	Description	Values/restrictions
Client Type	Select the client type	10GE, 40GE, 100GE, 400GE, OTU2, OTU2E, OTU4, OC192/STM64
Endpoints		
Endpoint A	Node and port of first endpoint	—
Endpoint B	Node and port of second endpoint	—

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 21: Service Manager



Service Manager

Services / Editing TRAIL-test_flex service

✓ General ✓ Endpoints ✓ C

General | Restoration

Select

Path

● Include nodes or links

Select node | Select links

1 Node(s) or Link(s) selected

● Exclude nodes or links

Select node | Select link

Diversity Type: Select Type

Service Diversity: Select service

1 Service(s) selected

NODE TRAIL-test L

□ Ignore Alarms

Table 13: General constraints

Field	Description	Values/restrictions

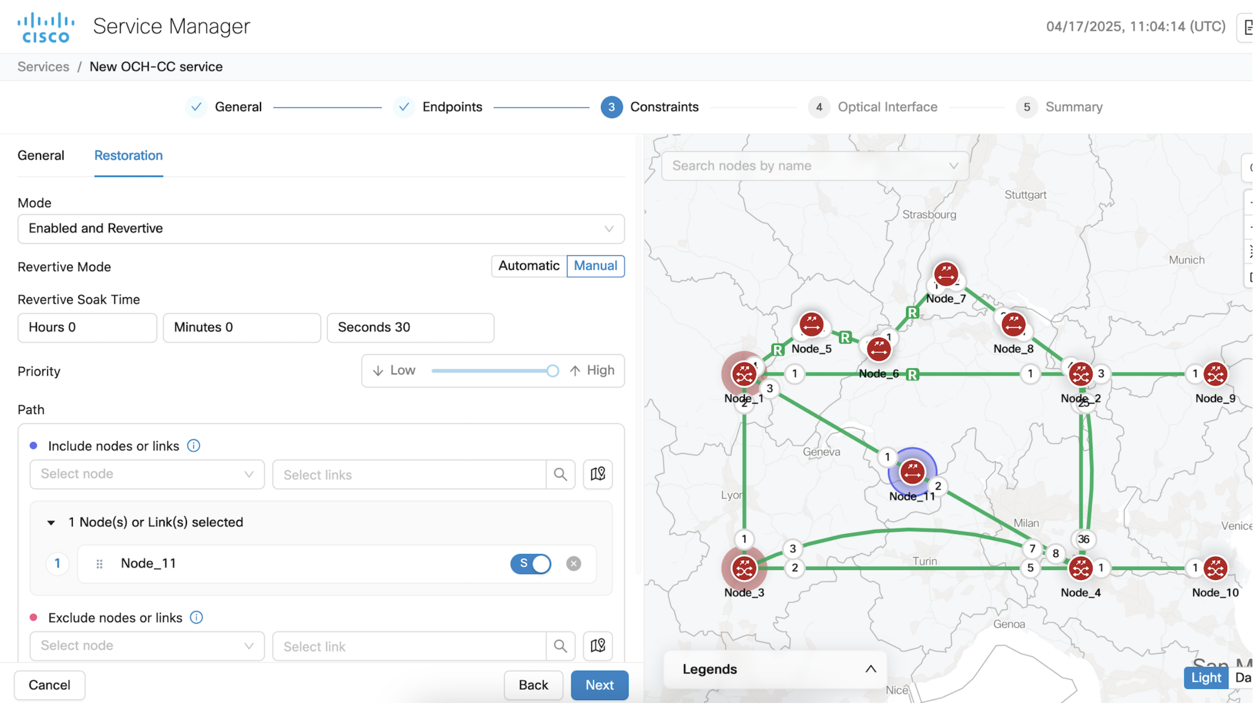
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	Select RED, GREEN, YELLOW or ORANGE.
		GREEN = mean value
		YELLOW = +1 sigma
		ORANGE = +2 sigma RED = +3 sigma

Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	—
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 dropdownfor 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.

Step 6 Choose the constraints in the **Constraints** > **Restoration** tab, and click **Next**.

Figure 22: Service Manager



Service Manager

04/17/2025, 11:04:14 (UTC)

Services / New OCH-CC service

✓ General — ✓ Endpoints — 3 Constraints — 4 Optical Interface — 5 Summary

General | Restoration

Mode: Enabled and Revertive

Revertive Mode: Automatic | Manual

Revertive Soak Time: Hours 0 | Minutes 0 | Seconds 30

Priority: ↓ Low — ↑ High

Path

● Include nodes or links ⓘ

Select node | Select links

1 Node(s) or Link(s) selected

1 Node_11 S

● Exclude nodes or links ⓘ

Select node | Select link

Cancel | Back | Next

Table 14: Restoration constraints

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 restorationshould 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.
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.	

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

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

Table 15: Optical interface parameters

Field	Description
Wavelength	
Central Frequency (THz)	Choose a central frequency for the service.
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

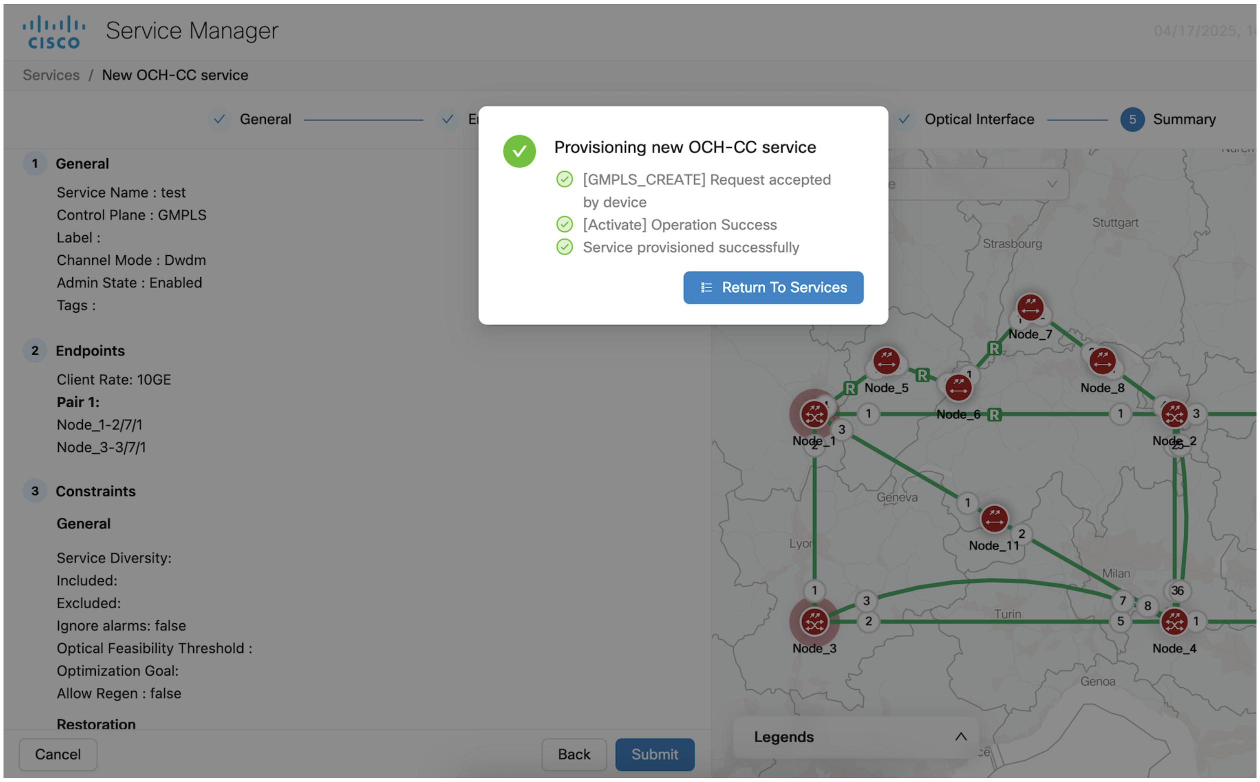
Note

- For OCH-trail,Optical Interface fields are auto populated and non-editable.

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

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

Figure 23: Service Manager



Service Manager

04/17/2025, 1

Services / New OCH-CC service

✓ General — ✓ E — ✓ Optical Interface — 5 Summary

1 General

Service Name : test
Control Plane : GMPLS
Label :
Channel Mode : Dwdm
Admin State : Enabled
Tags :

2 Endpoints

Client Rate: 10GE
Pair 1:
Node_1-2/7/1
Node_3-3/7/1

3 Constraints

General

Service Diversity:
Included:
Excluded:
Ignore alarms: false
Optical Feasibility Threshold :
Optimization Goal:
Allow Regen : false

Restoration

Provisioning new OCH-CC service

✓ [GMPLS_CREATE] Request accepted by device
✓ [Activate] Operation Success
✓ Service provisioned successfully

Return To Services

Cancel | Back | Submit

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**.

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 contraints to reroute the circuit.
A status pop-up appears showing the progress of the reroute process.
b) Go to **Constraints** > **Restoration** and update the constraints.
c) Click **Upgrade Restored** to make a restored circit 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 24: Service Manager

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 16: Deletion failure scenarios

Reason	Troubleshooting
Cross connect was deleted outside Cisco Optical Network Controller	• Retry deleting the service • Use the resync option in Service Manager and try again • Perform an full network resync and try again • Try deleting the service from Cisco Transport Controller
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.

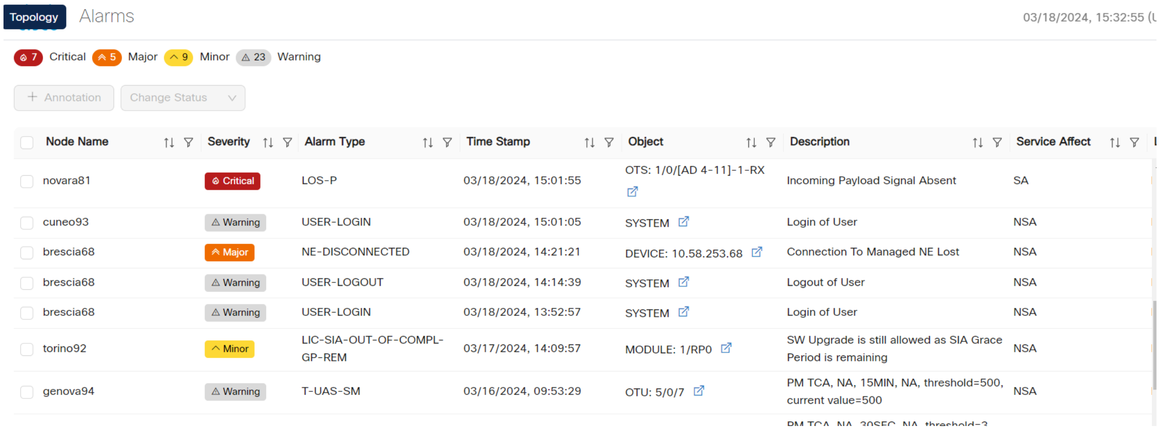
Error	Description
No wavelength available on path	The optical path in the node terminates on a port not matching the requested protection mode.
Reroute Failed	The requested action can not be executed as the selected circuit is already in rolled state
Optical Validation	The partial path evaluated during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

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.

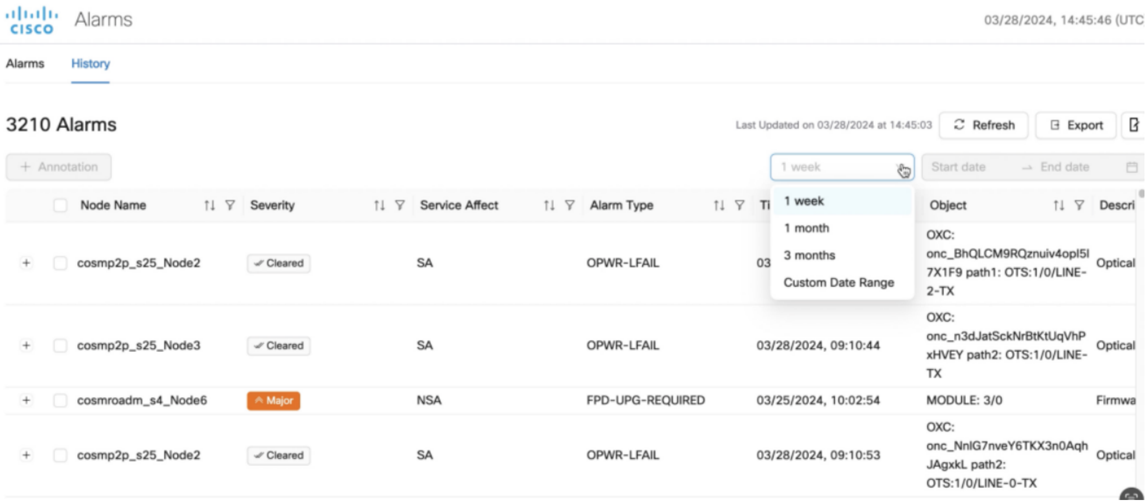
Figure 25: Alarms



Node Name	Severity	Alarm Type	Time Stamp	Object	Description	Service Affect
novara81	Critical	LOS-P	03/18/2024, 15:01:55	OTS: 1/0/[AD 4-11]-1-RX	Incoming Payload Signal Absent	SA
cuneo93	Warning	USER-LOGIN	03/18/2024, 15:01:05	SYSTEM	Login of User	NSA
brescia68	Major	NE-DISCONNECTED	03/18/2024, 14:21:21	DEVICE: 10.58.253.68	Connection To Managed NE Lost	NSA
brescia68	Warning	USER-LOGOUT	03/18/2024, 14:14:39	SYSTEM	Logout of User	NSA
brescia68	Warning	USER-LOGIN	03/18/2024, 13:52:57	SYSTEM	Login of User	NSA
torino92	Minor	LIC-SIA-OUT-OF-COMPL-GP-REM	03/17/2024, 14:09:57	MODULE: 1/RP0	SW Upgrade is still allowed as SIA Grace Period is remaining	NSA
genova94	Warning	T-UAS-SM	03/16/2024, 09:53:29	OTU: 5/0/7	PM TCA, NA, 15MIN, NA, threshold=500, current value=500	NSA
					PM TCA, NA, 30SEC, NA, threshold=3	

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

Figure 26: Alarms History



Node Name	Severity	Service Affect	Alarm Type	Ti	Object	Descri
cosmp2p_s25_Node2	Cleared	SA	OPWR-LFAIL	03	OXC: onc_BhQLCM9RQznuiv4opl5l7X1F9 path1: OTS:1/0/LINE-2-TX	Optical
cosmp2p_s25_Node3	Cleared	SA	OPWR-LFAIL	03/28/2024, 09:10:44	OXC: onc_n3dJatSckNrBtKtUqVhPxHVEY path2: OTS:1/0/LINE-TX	Optical
cosmroadm_s4_Node6	Major	NSA	FPD-UPG-REQUIRED	03/25/2024, 10:02:54	MODULE: 3/0	Firmwa
cosmp2p_s25_Node2	Cleared	SA	OPWR-LFAIL	03/28/2024, 09:10:53	OXC: onc_NnlG7nveY6TKX3n0AqhJAgxkL path2: OTS:1/0/LINE-0-TX	Optical

Table 17: Alarm Table Fields

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 Alarm Categories.	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,
User Tag	User-defined tags for categorizing and filtering alarms. **Note** • 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. • User Tag information comes from Cisco Optical Site Manager. See User Tags. • User tags are not supported on system-level and device alarms. • 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.	Custom tags/labels
User Notes	User-added notes or comments related to the alarm.	Free-form text

Field Name	Description	Example/Values
Acknowledge	Indicates whether the alarm has been acknowledged.	Acknowledged, Unacknowledged
UUID	Unique Universal Identifier for the alarm.	UUID string
Correlation Type	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 **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**.

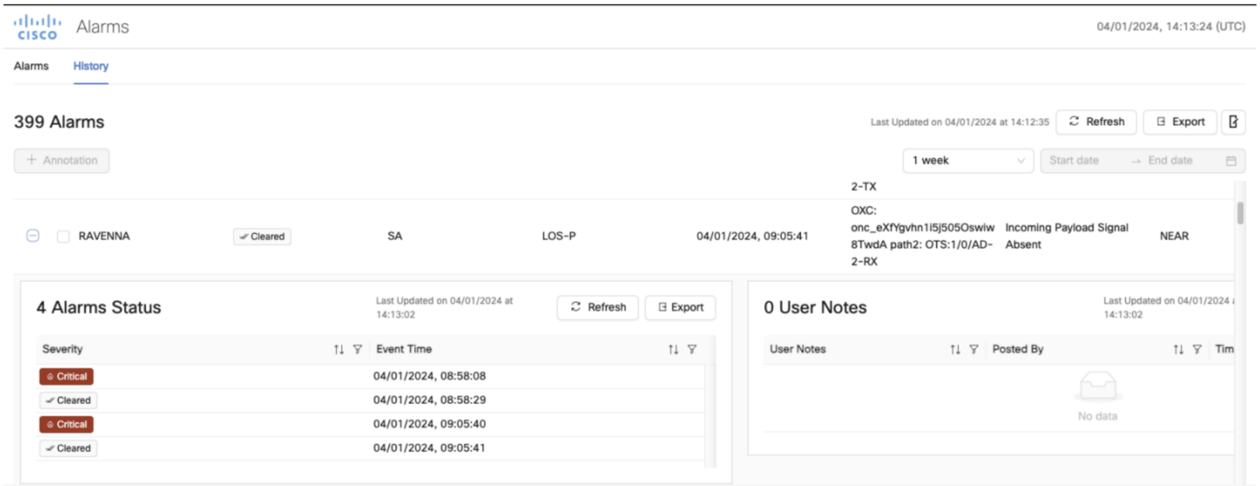
Note
You can add a user note to up to 500 alarms at once. You can add multiple notes to multiple alarms in the form of a list.

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** 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 27: Alarm History Expanded View



Alarms 04/01/2024, 14:13:24 (UTC)

Alarms History

399 Alarms

Last Updated on 04/01/2024 at 14:12:35 Refresh Export

+ Annotation 1 week Start date → End date

2-TX

RAVENNA | Cleared | SA | LOS-P | 04/01/2024, 09:05:41 | OXC: onc_eXfYgvhn1i5j505Oswiw 8TwdA path2: OTS:1/0/AD-2-RX | Incoming Payload Signal Absent | NEAR

4 Alarms Status

Last Updated on 04/01/2024 at 14:13:02 Refresh Export

Severity	Event Time
Critical	04/01/2024, 08:58:08
Cleared	04/01/2024, 08:58:29
Critical	04/01/2024, 09:05:40
Cleared	04/01/2024, 09:05:41

0 User Notes

Last Updated on 04/01/2024 a 14:13:02

User Notes	Posted By	Tim

No data

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

- 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 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

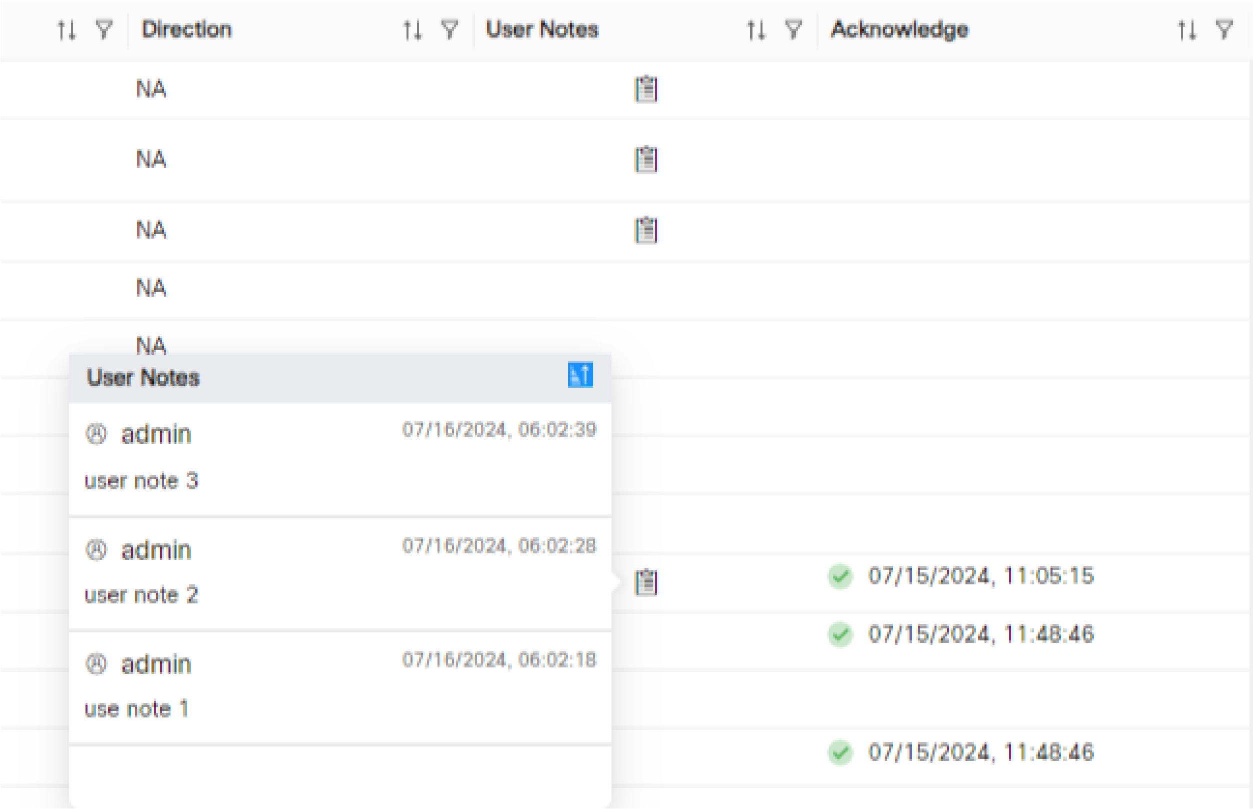
- To acknowledge or unacknowledge any particular alarm, select the node from the table and then click on **Change Status**. From the drop down, select **Acknowledge** or **Unacknowledge** option to acknowledge or unacknowledge the alarm of the selected node.
- If an alarm is acknowledged, it appears 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 28: User Notes



Direction	User Notes	Acknowledge
NA	📋	
NA	📋	
NA	📋	
NA		
NA		
	📋	✓ 07/15/2024, 11:05:15
		✓ 07/15/2024, 11:48:46
		✓ 07/15/2024, 11:48:46

User Notes

admin 07/16/2024, 06:02:39
user note 3

admin 07/16/2024, 06:02:28
user note 2

admin 07/16/2024, 06:02:18
use note 1

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.

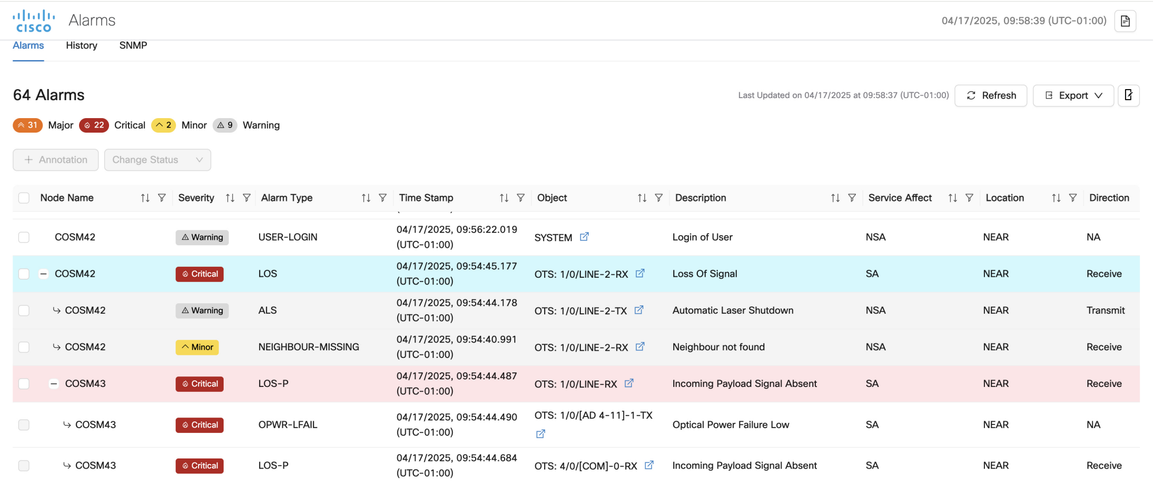
Note

- 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 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 higlighted 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 higlighted in red color.
- Alarms correlated at the node level cannot be acknowledged or have user notes added in Cisco Optical Network Controller.

Figure 29: Alarms History



64 Alarms

31 Major 22 Critical 2 Minor 9 Warning

Last Updated on 04/17/2025 at 09:58:37 (UTC-01:00)

□	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 18: 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 supppressed 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 30: Mute Acknowledged Alarms in Topology

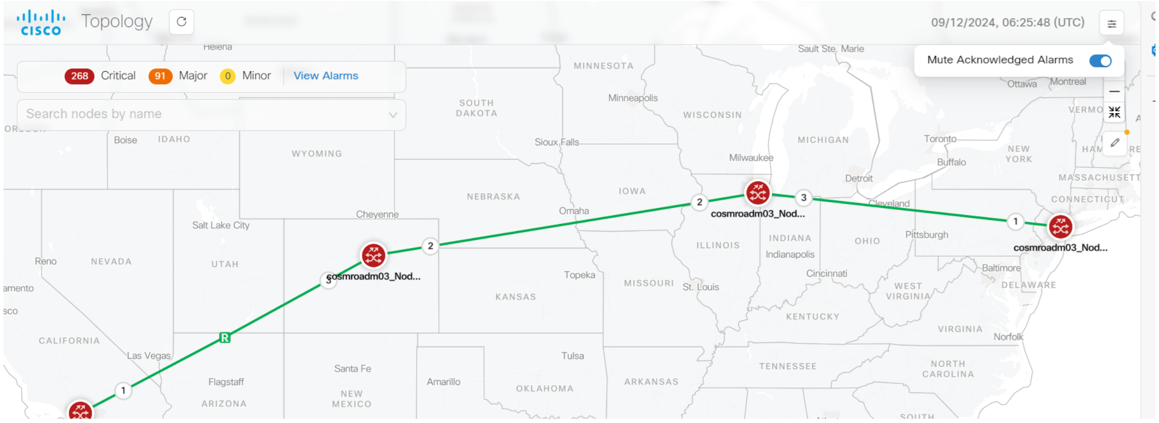
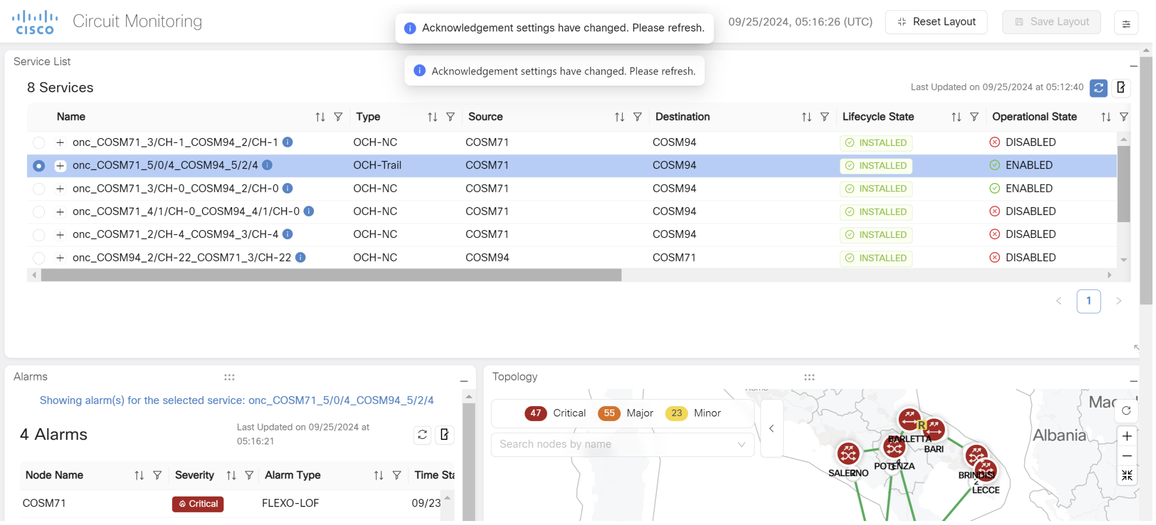


Figure 31: Mute Acknowledged Alarms in Circuit Monitoring



Circuit Monitoring

Acknowledgement settings have changed. Please refresh.

09/25/2024, 05:16:26 (UTC)

Acknowledgement settings have changed. Please refresh.

Service List

8 Services

Last Updated on 09/25/2024 at 05:12:40

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

Alarms

Showing alarm(s) for the selected service: onc_COSM71_5/0/4_COSM94_5/2/4

4 Alarms

Last Updated on 09/25/2024 at 05:16:21

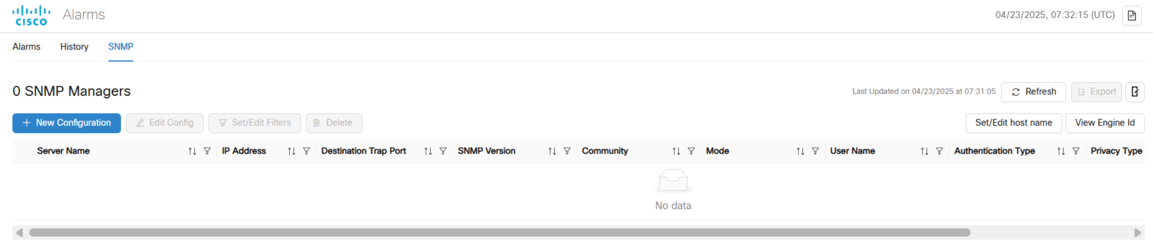
Node Name	Severity	Alarm Type	Time Sta
COSM71	Critical	FLEXO-LOF	09/23

Topology

47 Critical 55 Major 23 Minor

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.



Alarms

04/23/2025, 07:32:15 (UTC)

0 SNMP Managers

Last Updated on 04/23/2025 at 07:31:05

Server Name	IP Address	Destination Trap Port	SNMP Version	Community	Mode	User Name	Authentication Type	Privacy Type

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**.

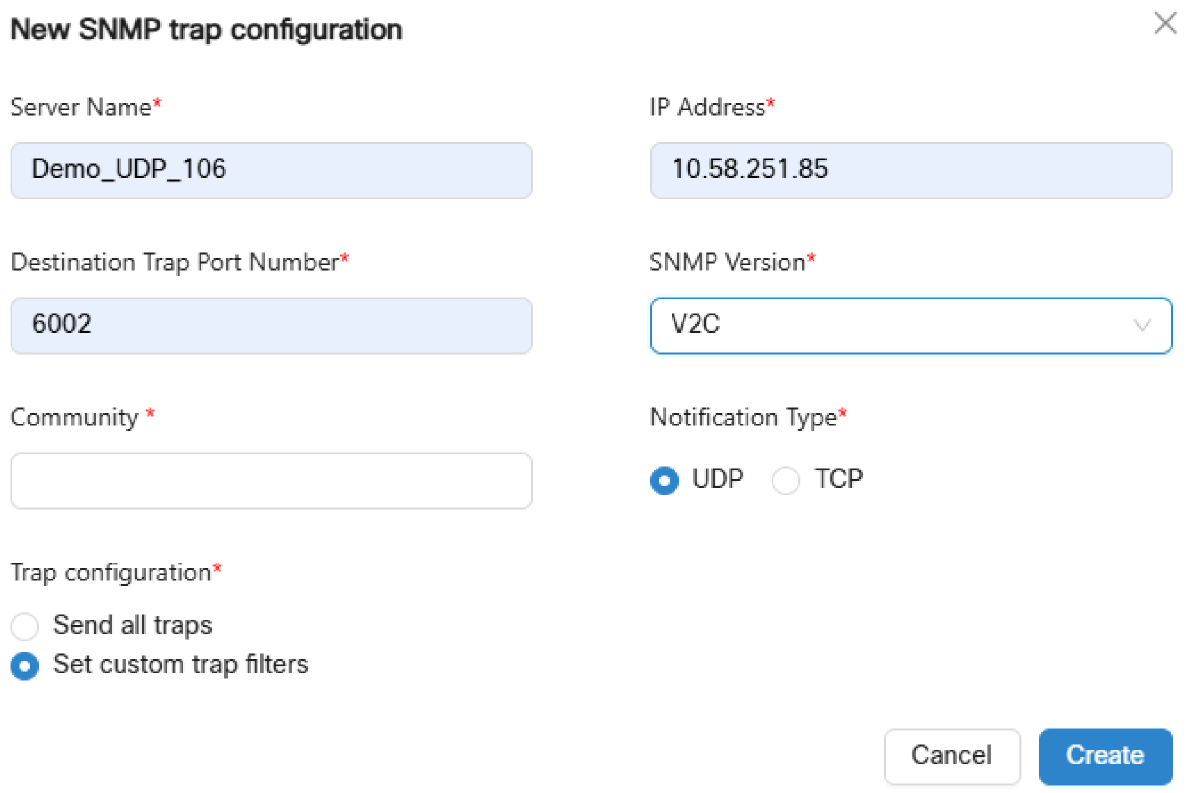
Step 2 Create a New SNMP Manager.

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

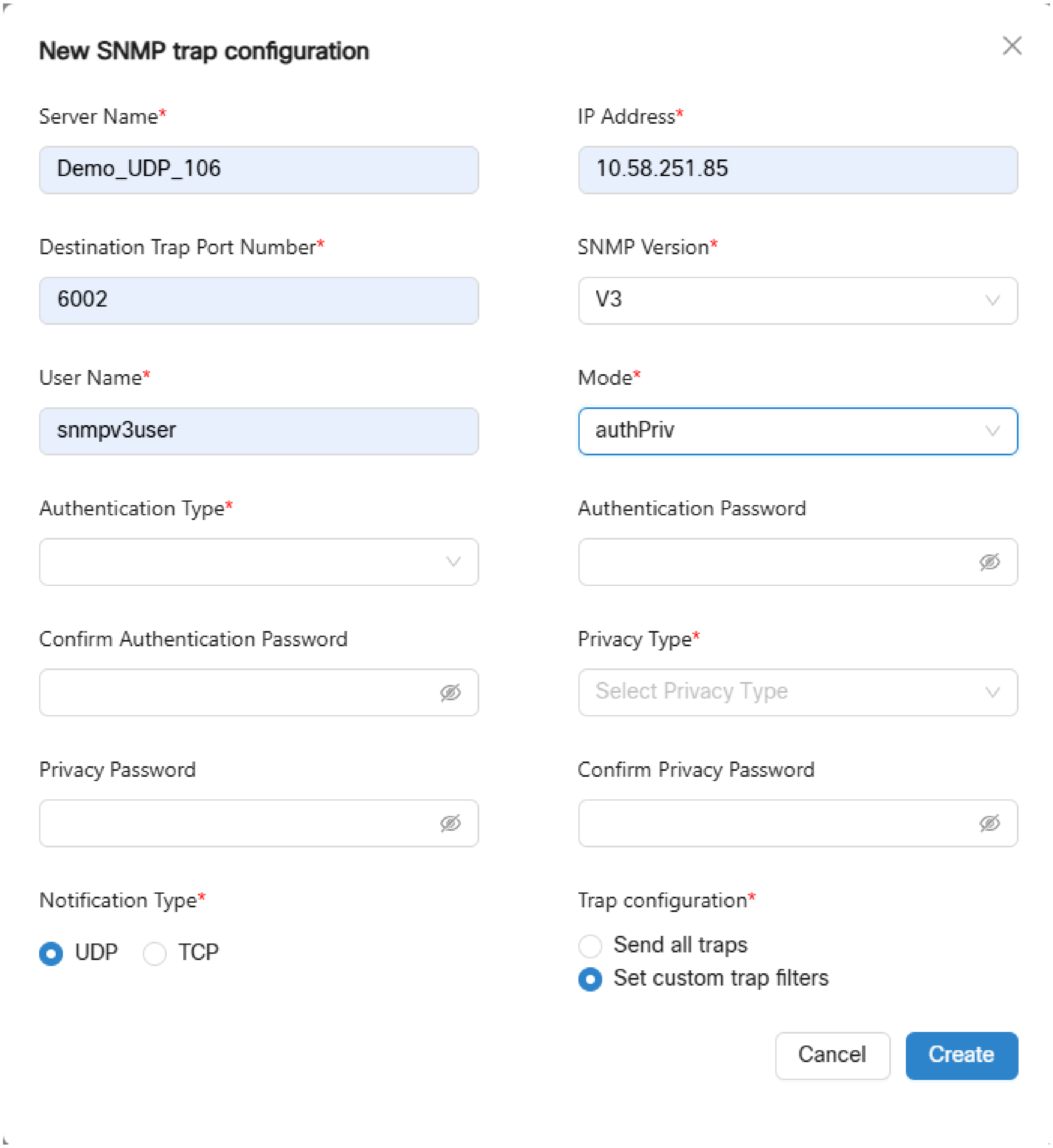
SNMP Version*: V2C

Community *:

Notification Type*: ● UDP ○ TCP

Trap configuration*:
○ Send all traps
● Set custom trap filters

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

Server Name*: Demo_UDP_106

IP Address*: 10.58.251.85

Destination Trap Port Number*: 6002

SNMP Version*: V3

User Name*: snmpv3user

Mode*: authPriv

Authentication Type*:

Authentication Password:

Confirm Authentication Password:

Privacy Type*: Select Privacy Type

Privacy Password:

Confirm Privacy Password:

Notification Type*: ● UDP ○ TCP

Trap configuration*: ○ Send all traps ● Set custom trap filters

e) Choose the **Notification Type**, TCP or UDP.

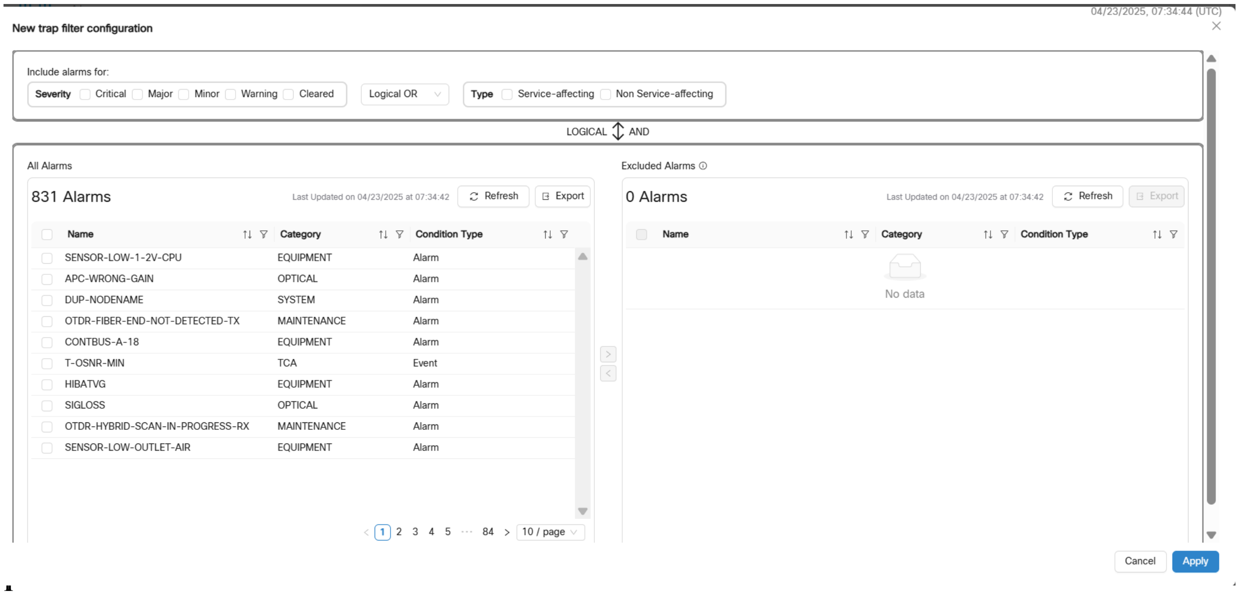
f) Choose the **Trap Configuration**, Send all traps or Set custom trap filters.
If you choose custom trap filters follow3.c, on page 59

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



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

New trap filter configuration

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

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

< 1 2 3 4 5 ··· 84 > 10 / page

Excluded Alarms ⓘ

0 Alarms

Last Updated on 04/23/2025 at 07:34:42

Name	Category	Condition Type

No data

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 Controllerserver has network connectivity to the SNMP manager.

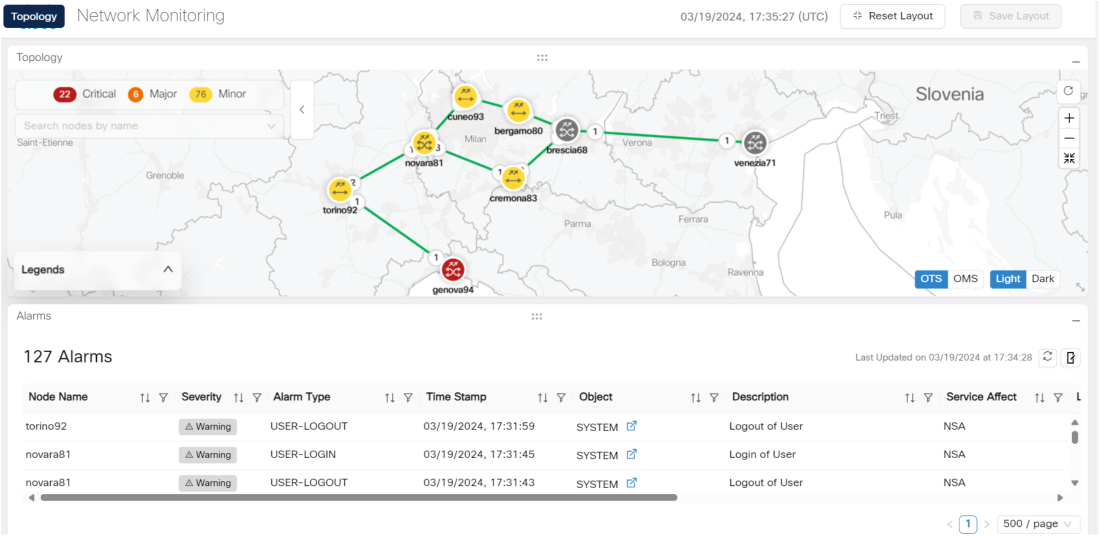
Workspaces

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.

Types of Workspaces

- **Network Monitoring Workspace:** Provides a comprehensive view of the network, including node status, alarms, and performance metrics.

Figure 32: Workspaces Network Monitoring



127 Alarms

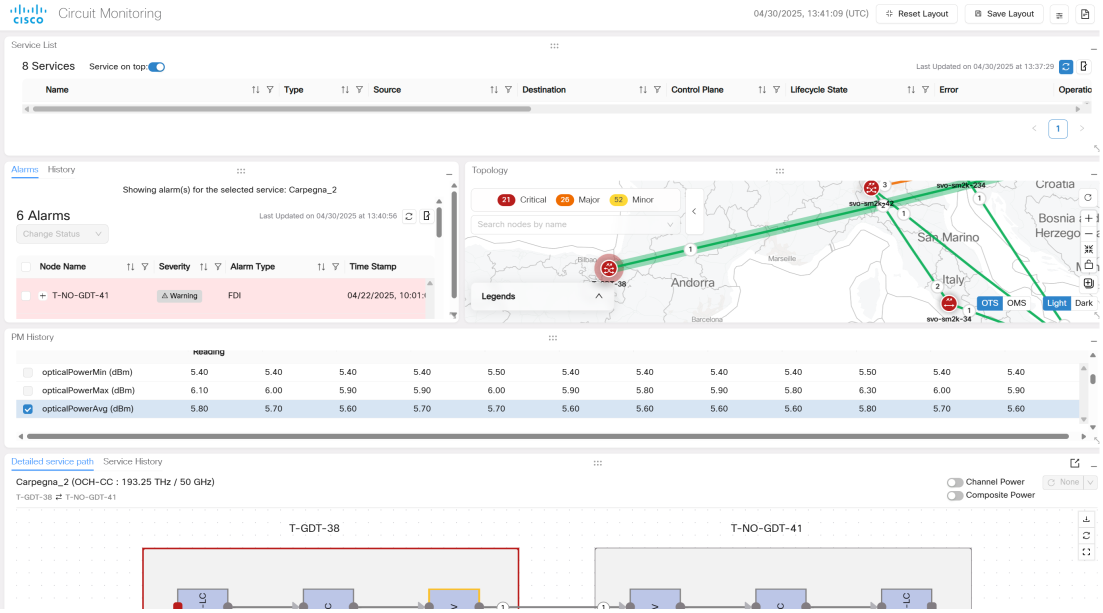
Last Updated on 03/19/2024 at 17:34:28

Node Name	Severity	Alarm Type	Time Stamp	Object	Description	Service Affect
torino92	⚠ Warning	USER-LOGOUT	03/19/2024, 17:31:59	SYSTEM	Logout of User	NSA
novara81	⚠ Warning	USER-LOGIN	03/19/2024, 17:31:45	SYSTEM	Login of User	NSA
novara81	⚠ Warning	USER-LOGOUT	03/19/2024, 17:31:43	SYSTEM	Logout of User	NSA

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

- **Circuit Monitoring Workspace:** Focuses on individual circuits, displaying their path, associated alarms, and performance history.

Figure 33: Circuit Monitoring



8 Services Service on top:

Last Updated on 04/30/2025 at 13:37:29

Name	Type	Source	Destination	Control Plane	Lifecycle State	Error	Operatio

Showing alarm(s) for the selected service: Carpegna_2

6 Alarms

Last Updated on 04/30/2025 at 13:40:56

Node Name	Severity	Alarm Type	Time Stamp
+ T-NO-GDT-41	⚠ Warning	FDI	04/22/2025, 10:01:(

Reading												
□ opticalPowerMin (dBm)	5.40	5.40	5.40	5.40	5.50	5.40	5.40	5.40	5.40	5.50	5.40	5.40
□ opticalPowerMax (dBm)	6.10	6.00	5.90	5.90	6.00	5.90	5.80	5.90	5.80	6.30	6.00	5.90
☑ opticalPowerAvg (dBm)	5.80	5.70	5.60	5.70	5.70	5.60	5.60	5.60	5.60	5.80	5.70	5.60

Carpegna_2 (OCH-CC : 193.25 THz / 50 GHz)

T-GDT-38 ⇄ T-NO-GDT-41

Note

- In the **Alarms** screen above, select any alarm and right click followed by **Show Affected service(s)**. This will display all the services related to the selected alarm in the services layout.
- From release 24.3.1, PM tab is available in the **Circuit Monitoring** workflow 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 toggle to select the segment type.
  3. Click the nodes or links you want to select.

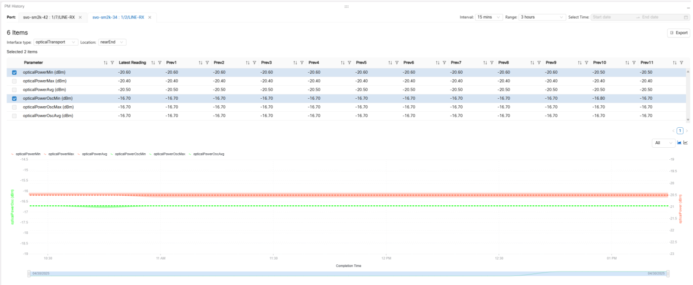
     You can select up to 20 entities at a time.
  4. Click **Show services**.

     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.
- **Detailed service path**
  - Select a service from the service list to view its detailed service path.
  - Use the **Channel Power** and **Composite Power** toggles to enable and disable the power display for all ports in the detailed service path.
  - Hover over a port or equipment in the detailed service path to view a tooltip with additional information.
  - PM history
    - Select a service from the service list.

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

Figure 34: PM History in Circuit Monitoring



PM History

Port: svo-sm2k-42 : 1/7/LINE-RX   svo-sm2k-34 : 1/2/LINE-RX

Interval: 15 mins   Range: 3 hours   Select Time: Start date → End date

6 Items

Export

Interface type: opticalTransport   Location: nearEnd

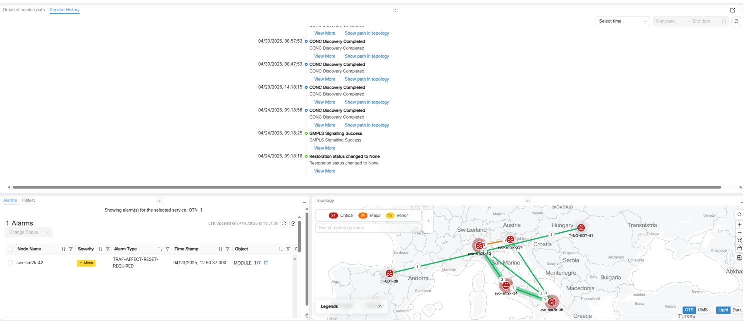
Selected 2 items

	Parameter	Latest Reading	Prev1	Prev2	Prev3	Prev4	Prev5	Prev6	Prev7	Prev8	Prev9	Prev10	Prev11
☑	opticalPowerMin (dBm)	-20.60	-20.60	-20.60	-20.60	-20.60	-20.60	-20.60	-20.60	-20.60	-20.60	-20.50	-20.50
□	opticalPowerMax (dBm)	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40	-20.40
□	opticalPowerAvg (dBm)	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50	-20.50
☑	opticalPowerOscMin (dBm)	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.80	-16.70
□	opticalPowerOscMax (dBm)	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70
□	opticalPowerOscAvg (dBm)	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70	-16.70

- **Interface type Selection**: 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 dropdown.
- **Location selection for up to two ports PM report**: You can choose to view the nearEnd or farEnd PM history for the port.
- You can view PM history for up to two ports at a time.

- **Service History**
  - Select an OCH-CC or OCH-Trail service to get a timeline view of events and actions performed on a circuit.

Figure 35: PM History in Circuit Monitoring



Detailed service path   Service History

Select time   Start date → End date

View More   Show path in topology

04/30/2025, 08:57:53 CONC Discovery Completed
CONC Discovery Completed
View More   Show path in topology

04/30/2025, 08:47:53 CONC Discovery Completed
CONC Discovery Completed
View More   Show path in topology

04/29/2025, 14:18:15 CONC Discovery Completed
CONC Discovery Completed
View More   Show path in topology

04/24/2025, 09:18:58 CONC Discovery Completed
CONC Discovery Completed
View More   Show path in topology

04/24/2025, 09:18:25 GMPLS Signalling Success
GMPLS Signalling Success
View More

04/24/2025, 09:18:16 Restoration status changed to None
Restoration status changed to None
View More

Alarms   History

Showing alarm(s) for the selected service: OTN_1

1 Alarms

Change Status

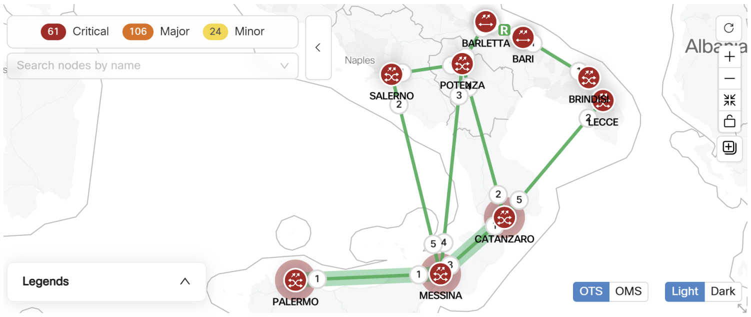
Last Updated on 04/30/2025 at 13:31:35

	Node Name	Severity	Alarm Type	Time Stamp	Object
□	svo-sm2k-42	Minor	TRAF-AFFECT-RESET-REQUIRED	04/23/2025, 12:50:37.000	MODULE: 1/7

  - Includes details such as the user who initiated the action, the timestamp, and the status of the operation.
  - Offers a "view more" option to display detailed diagnostic logs related to the event.

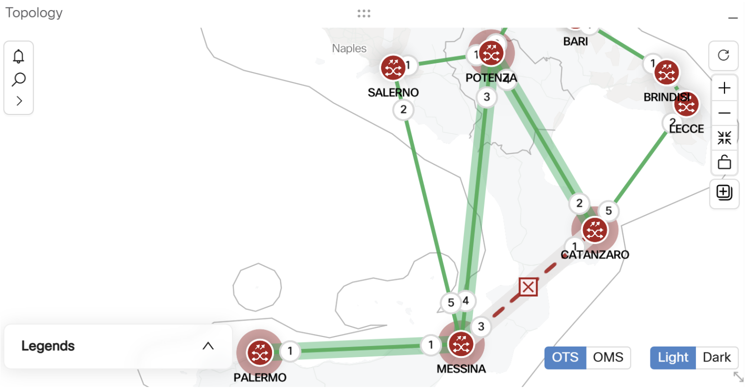
- **Visualise Circuit Restoration**
  - Select a Service from the Service List to highlight the circuit in the topology.

    Figure 36: Topology in circuit monitoring workspace

  - If the circuit has undergone restoration due to a fiber cut, topology shows the new path and the main path. The main path is represented by dotted lines.

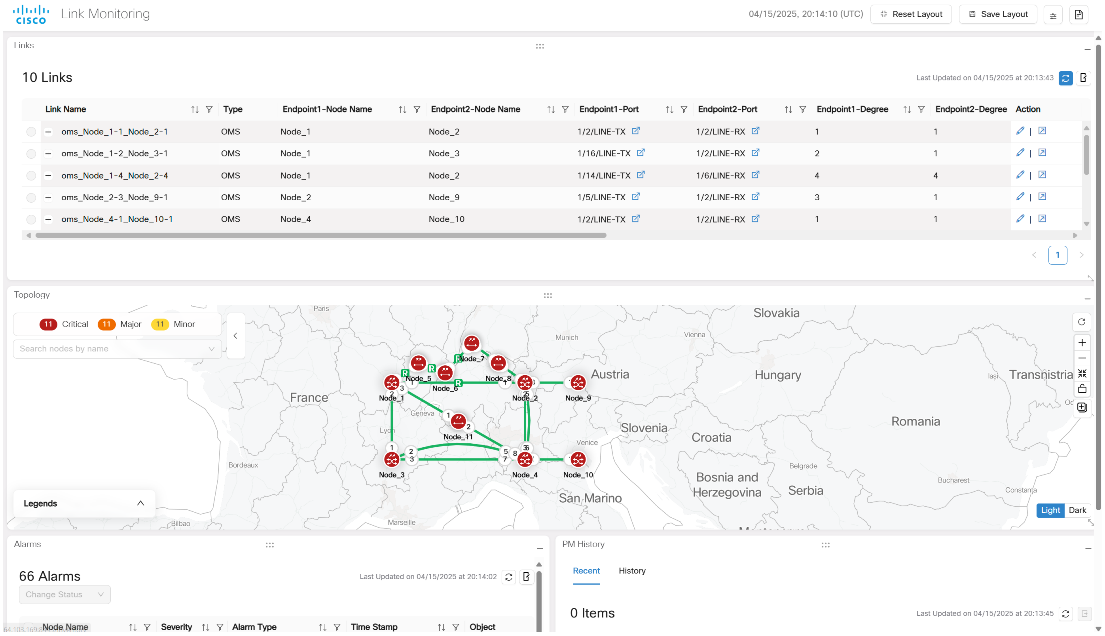
    Figure 37: Topology in circuit monitoring workspace

  - You can also see the service restoration and related events in Service History.
  - Restoration State column in the Service list also displays the restoration state of the service.

- **Link Monitoring Workspace:** Focuses on individual links, displaying their alarms, performance history, topology, and associated circuits.

Figure 38: Link Monitoring workspace



Link Monitoring

04/15/2025, 20:14:10 (UTC)

Links

10 Links

Last Updated on 04/15/2025 at 20:13:43

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	
oms_Node_1-2_Node_3-1	OMS	Node_1	Node_3	1/16/LINE-TX	1/2/LINE-RX	2	1	
oms_Node_1-4_Node_2-4	OMS	Node_1	Node_2	1/14/LINE-TX	1/6/LINE-RX	4	4	
oms_Node_2-3_Node_9-1	OMS	Node_2	Node_9	1/5/LINE-TX	1/2/LINE-RX	3	1	
oms_Node_4-1_Node_10-1	OMS	Node_4	Node_10	1/2/LINE-TX	1/2/LINE-RX	1	1	

Alarms

66 Alarms

Last Updated on 04/15/2025 at 20:14:02

Node Name	Severity	Alarm Type	Time Stamp	Object

PM History

0 Items

Last Updated on 04/15/2025 at 20:13:45

- In Links monitoring, Links table is primary.
- 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`.

  Your selection is bidirectional. The link you select from the Links list is highlighted in topology. The nodes and links you select in topology are filtered in the links list.
- In links table, click **edit link** in the action column to edit link details.
- You can cross launch circuit monitoring for circuits using a link by clicking **View Circuit Monitring** in the action column.
- In links table only forward/reverse ots can be selected.
- You can select multiple links or nodes in the topology.
  1. Click **Select node(s)/link(s)**in topology.
  2. Use the OTS/OMS 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. Multiple selection is available only for ots links.
  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.

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

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.

Software Image Management and Upgrade

The Software Image Management and Upgrade (SWIMU) is a Cisco Optical Network Controller appliction 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 19: 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 20: External SFTP Server Storage Formula Parameters

Parameter	Description
Network Total Devices	The number of onboarded devices.
Size of the Device	The size of an individual device.
Requested Archive Period	The duration for which the backup files are stored in days
Backup Reoccurrence	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 21: Internal SFTP Server Storage Formula Parameters

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

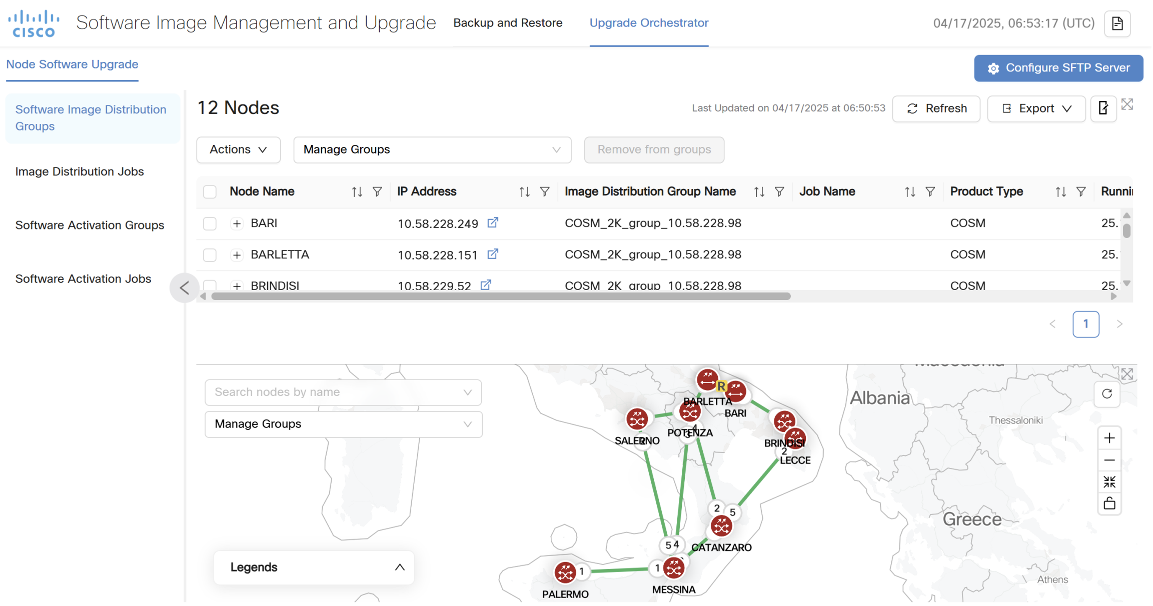
What to do next

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 39: Node Backup and Restore



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.

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

a) Click **Backup, Restore and Group Management** > **Manage Groups** > **Create Group**

b) Enter the **Group Name** and **Description** and click **Save**.

c) Select the nodes from the **Nodes** table.

d) 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.

a) 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.

b) 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.

a) 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.

b) Click **Edit** to edit the schedule of the existing scheduled backup jobs.
c) Click **Delete** to delete the selected job from the backup scheduled job list.
d) 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

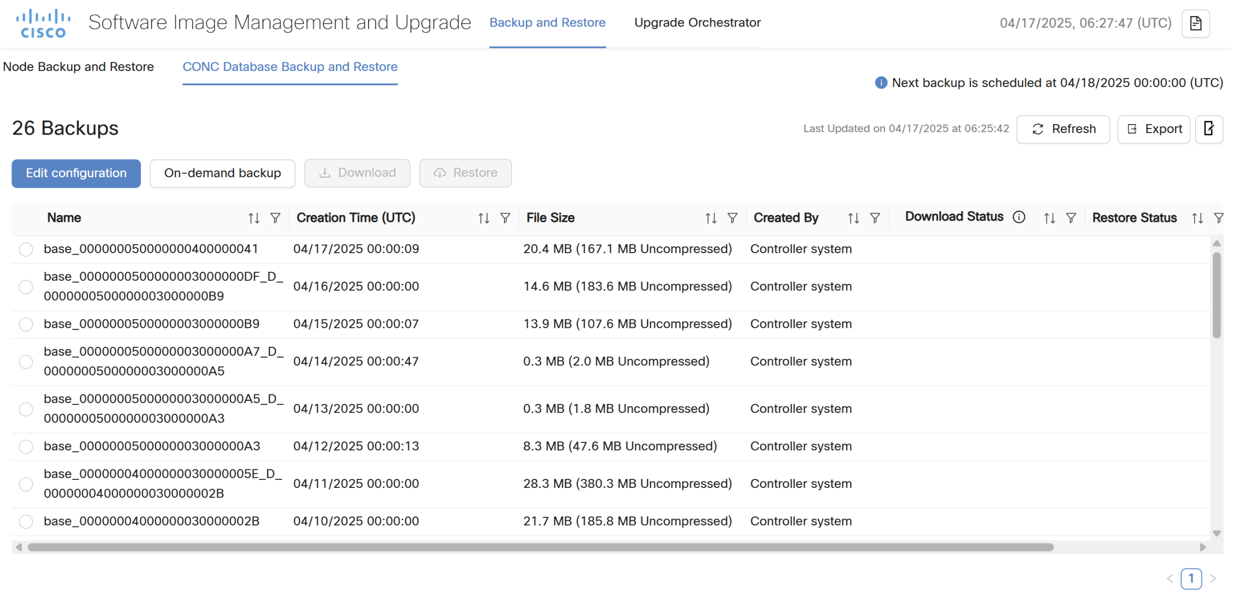
- The Cisco Optical Network Controller Database Backup and Restore feature relies on a properly configured SFTP server.
- Ensure that the SFTP server has sufficient storage space for the backups.
- If a backup fails, the BACKUP-FAILURE alarm is raised.
- If the upload of a backup to the SFTP server fails, the UPLOAD-FAILURE alarm is raised.

Procedure

Step 1 Perform an **On-demand** backup.

a) Navigate to **Backup and Restore** > **CONC Database Backup and Restore**.

Figure 40: 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_0000000500000000400000041	04/17/2025 00:00:09	20.4 MB (167.1 MB Uncompressed)	Controller system		
○	base_00000005000000003000000DF_D_00000005000000003000000B9	04/16/2025 00:00:00	14.6 MB (183.6 MB Uncompressed)	Controller system		
○	base_00000005000000003000000B9	04/15/2025 00:00:07	13.9 MB (107.6 MB Uncompressed)	Controller system		
○	base_00000005000000003000000A7_D_00000005000000003000000A5	04/14/2025 00:00:47	0.3 MB (2.0 MB Uncompressed)	Controller system		
○	base_00000005000000003000000A5_D_00000005000000003000000A3	04/13/2025 00:00:00	0.3 MB (1.8 MB Uncompressed)	Controller system		
○	base_00000005000000003000000A3	04/12/2025 00:00:13	8.3 MB (47.6 MB Uncompressed)	Controller system		
○	base_000000040000000030000005E_D_000000040000000030000002B	04/11/2025 00:00:00	28.3 MB (380.3 MB Uncompressed)	Controller system		
○	base_000000040000000030000002B	04/10/2025 00:00:00	21.7 MB (185.8 MB Uncompressed)	Controller system		

b) 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

a) Navigate to **Backup and Restore** > **CONC Database Backup and Restore**.
b) Select the backup you want to download from the table.
c) 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 -zvxf <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 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>
```

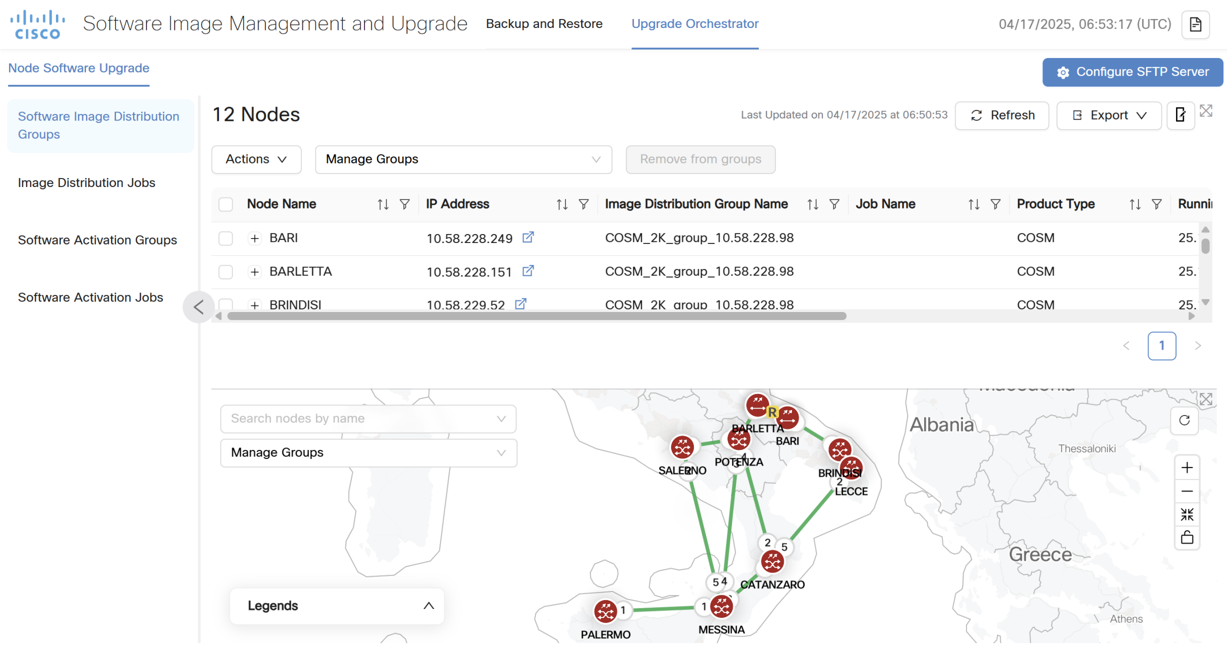
- `<file-name>`: The name of the file to delete.

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

Step 2 Create Image Distribution Groups.

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

Figure 41: Upgrade Orchestrator



Software Image Management and Upgrade | Backup and Restore | Upgrade Orchestrator | 04/17/2025, 06:53:17 (UTC)

Node Software Upgrade | Configure SFTP Server

Software Image Distribution Groups
Image Distribution Jobs
Software Activation Groups
Software Activation Jobs

12 Nodes | Last Updated on 04/17/2025 at 06:50:53 | Refresh | Export

Actions | Manage Groups | Remove from groups

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.

1

Search nodes by name
Manage Groups
Legends

b) Click **Actions** and select **Expand all** to expand nodes in the table to view the subtended devices under the node.

c) Click **Manage Groups** and select **New Group**.

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

d) Enter a Group Name and Description.

e) Select the nodes 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 autogenerated by Cisco Optical Network Controller.

You cannot edit NCS 2000 groups.

You cannot add NCS 2000 nodes to NCS 1000 groups.

Step 3 Create an Image Distribution Job.

a) 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.

d) Select an SFTP server from the dropdown 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
For NCS 2000 nodes, Image distribution takes place for all nodes in a group. You cannot select a subset of nodes to distribute images to.

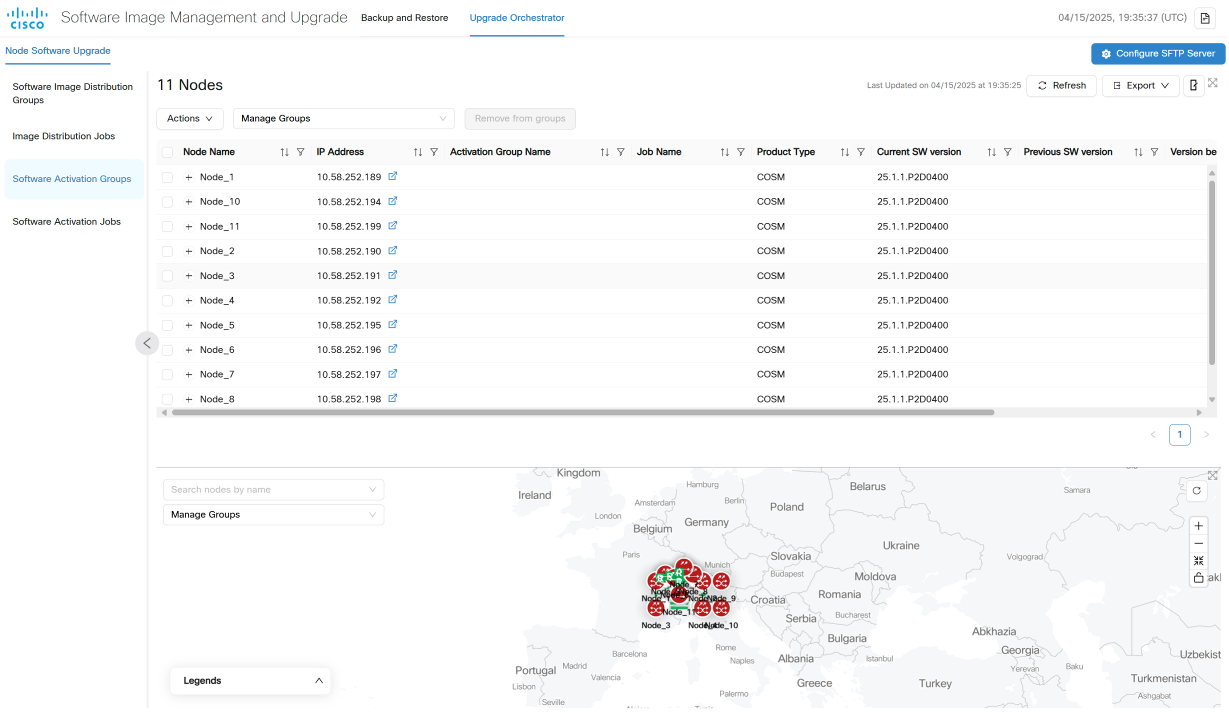
If a job status is **PARTIAL**, it means the job succeeded for some of the nodes, but failed for other nodes in the group of devices that the job was initiated for.

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 42: Upgrade Orchestrator



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		

You can also Mange 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 autogenerated by Cisco Optical Network Controller.

You cannot edit NCS 2000 groups.

You cannot add NCS 2000 nodes to NCS 1000 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.
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.

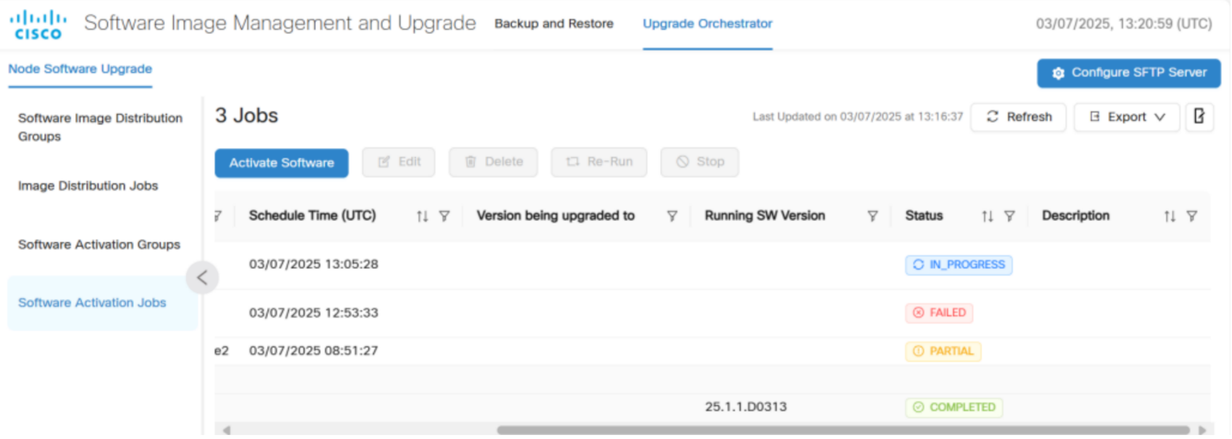
   The job continues on the nodes on which it was in progress.

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.

Figure 43: Upgrade Orchestrator



3 Jobs

Last Updated on 03/07/2025 at 13:16:37

	Schedule Time (UTC)	Version being upgraded to	Running SW Version	Status	Description
	03/07/2025 13:05:28			IN_PROGRESS	
	03/07/2025 12:53:33			FAILED	
e2	03/07/2025 08:51:27			PARTIAL	
			25.1.1.D0313	COMPLETED	

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

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 22: Benefits of PM History

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

Table 23: Time Range for Fetching Data

Time Range	Limit
PM Data Interval for 15 mins	Active data retention - 1 day + current day Archive data retention - 3 days
PM Data Interval for 24 hours	Active data retention - 31 days + current day Archive data retention - 93 days

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.

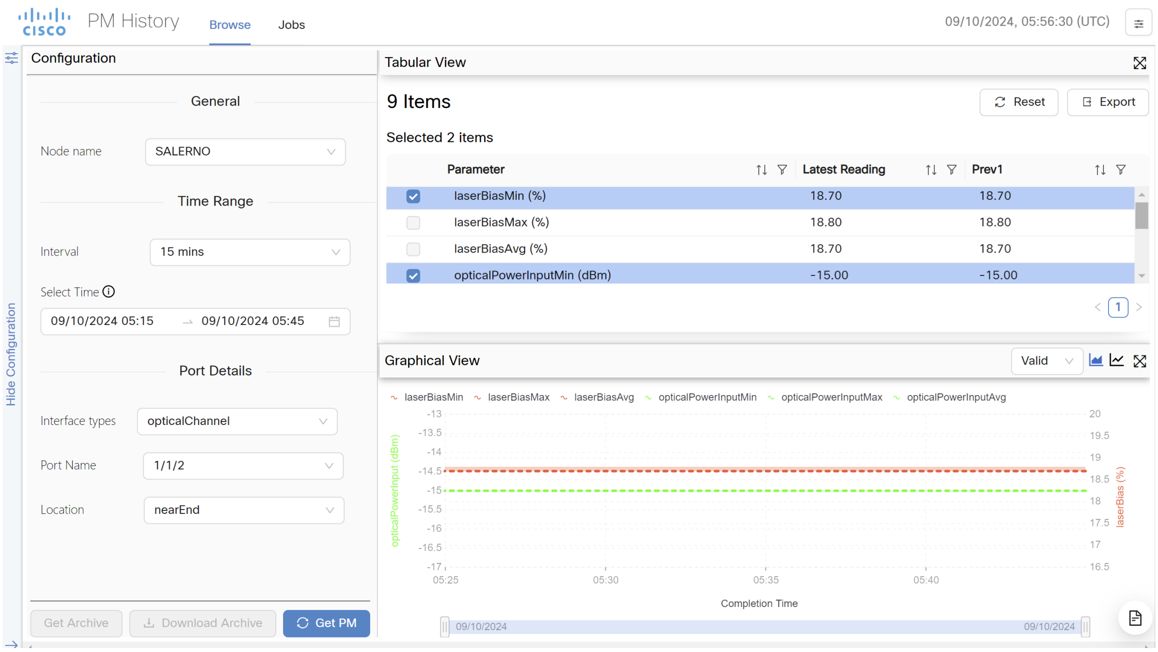
Table 24: Types of PM History Report

Type of PM History Report	Description
15-Minute Granularity PM Report	• **Availability**: Real-time reports are accessible for up to one + current day, from the time the report is generated. • **Archiving**: Data is archived and accessible for up to active (current day - 2) up to (current day - 5). Overall data is available for 5 days.
24-Hour Granularity PM Report	• **Availability**: Real-time reports are accessible for up to 31 days from the time the report is generated. • **Archiving**: Data is archived and accessible for up to 93 days from the time the report was first generated.

Note

- For both 15-Minute or 24-Hour granularity PM report, you can use the horizonal scroll bar to adjust the dates as per your need. For 15-Minute granularity archive data is available for download from 3 to 5 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 44: 15-Minute Granularity PM Report



General

Node name: SALERNO

Time Range

Interval: 15 mins

Select Time: 09/10/2024 05:15 → 09/10/2024 05:45

Port Details

Interface types: opticalChannel

Port Name: 1/1/2

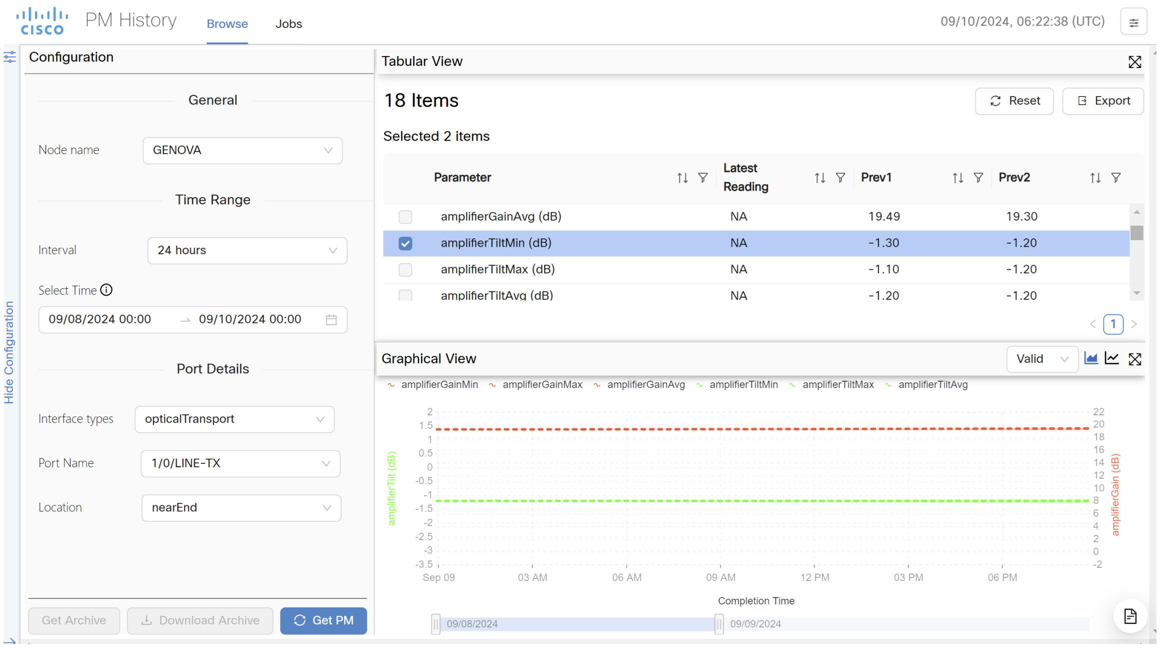
Location: nearEnd

9 Items

Selected 2 items

	Parameter	Latest Reading	Prev1
☑	laserBiasMin (%)	18.70	18.70
□	laserBiasMax (%)	18.80	18.80
□	laserBiasAvg (%)	18.70	18.70
☑	opticalPowerInputMin (dBm)	-15.00	-15.00

Figure 45: 24-Hour Granularity PM Report



General

Node name: GENOVA

Time Range

Interval: 24 hours

Select Time: 09/08/2024 00:00 → 09/10/2024 00:00

Port Details

Interface types: opticalTransport

Port Name: 1/0/LINE-TX

Location: nearEnd

18 Items

Selected 2 items

	Parameter	Latest Reading	Prev1	Prev2
□	amplifierGainAvg (dB)	NA	19.49	19.30
☑	amplifierTiltMin (dB)	NA	-1.30	-1.20
□	amplifierTiltMax (dB)	NA	-1.10	-1.20
□	amplifierTiltAvg (dB)	NA	-1.20	-1.20

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.

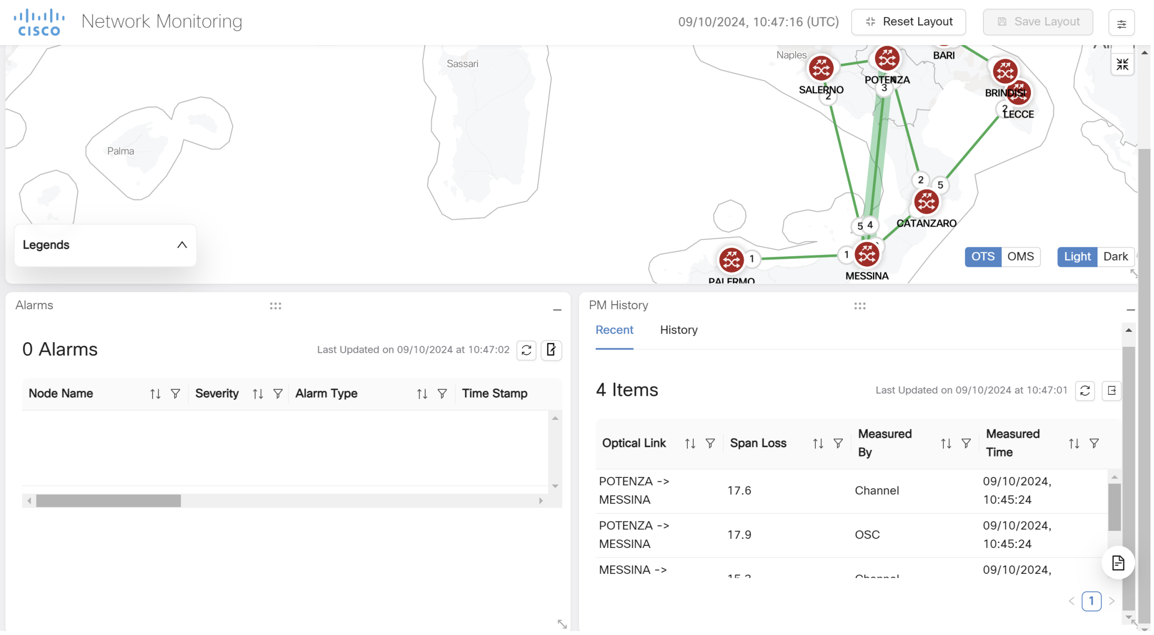
- Reports are sent through email which is configured through SMTP server and which are not password protected.

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 46: PM History in Network Monitoring



0 Alarms

Last Updated on 09/10/2024 at 10:47:02

Node Name	Severity	Alarm Type	Time Stamp

4 Items

Last Updated on 09/10/2024 at 10:47:01

Optical Link	Span Loss	Measured By	Measured Time
POTENZA -> MESSINA	17.6	Channel	09/10/2024, 10:45:24
POTENZA -> MESSINA	17.9	OSC	09/10/2024, 10:45:24
MESSINA ->	15.3	Channel	09/10/2024,

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

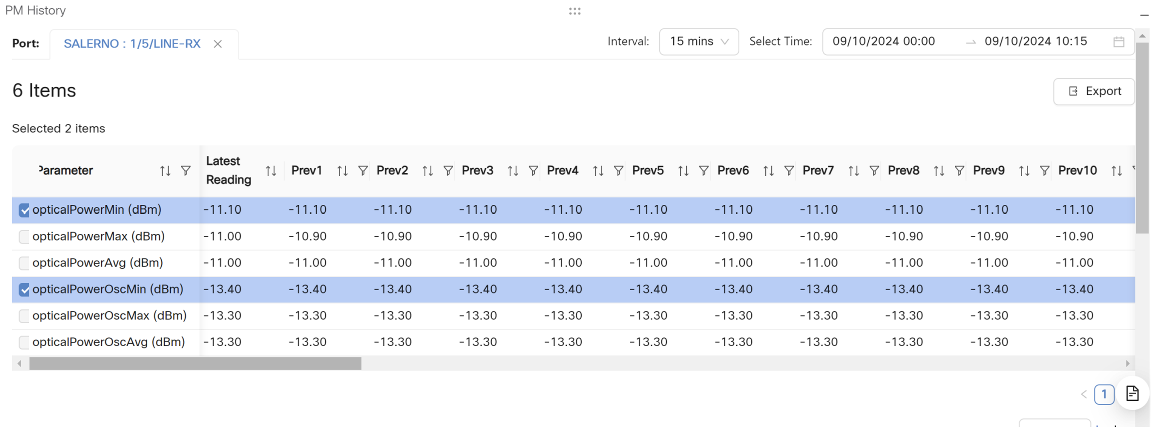
The **Circuit Monitoring** workspace will now feature a new dashboard in the detailed service path component, displaying PM History data. This new add-on dashboard has the **Detailed Service Path** component which displays the PM values based on selected port.

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.

Figure 47: 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

?arameter	Latest Reading	Prev1	Prev2	Prev3	Prev4	Prev5	Prev6	Prev7	Prev8	Prev9	Prev10
☑ opticalPowerMin (dBm)	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10
□ opticalPowerMax (dBm)	-11.00	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90
□ opticalPowerAvg (dBm)	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00
☑ opticalPowerOscMin (dBm)	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40
□ opticalPowerOscMax (dBm)	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30
□ 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.

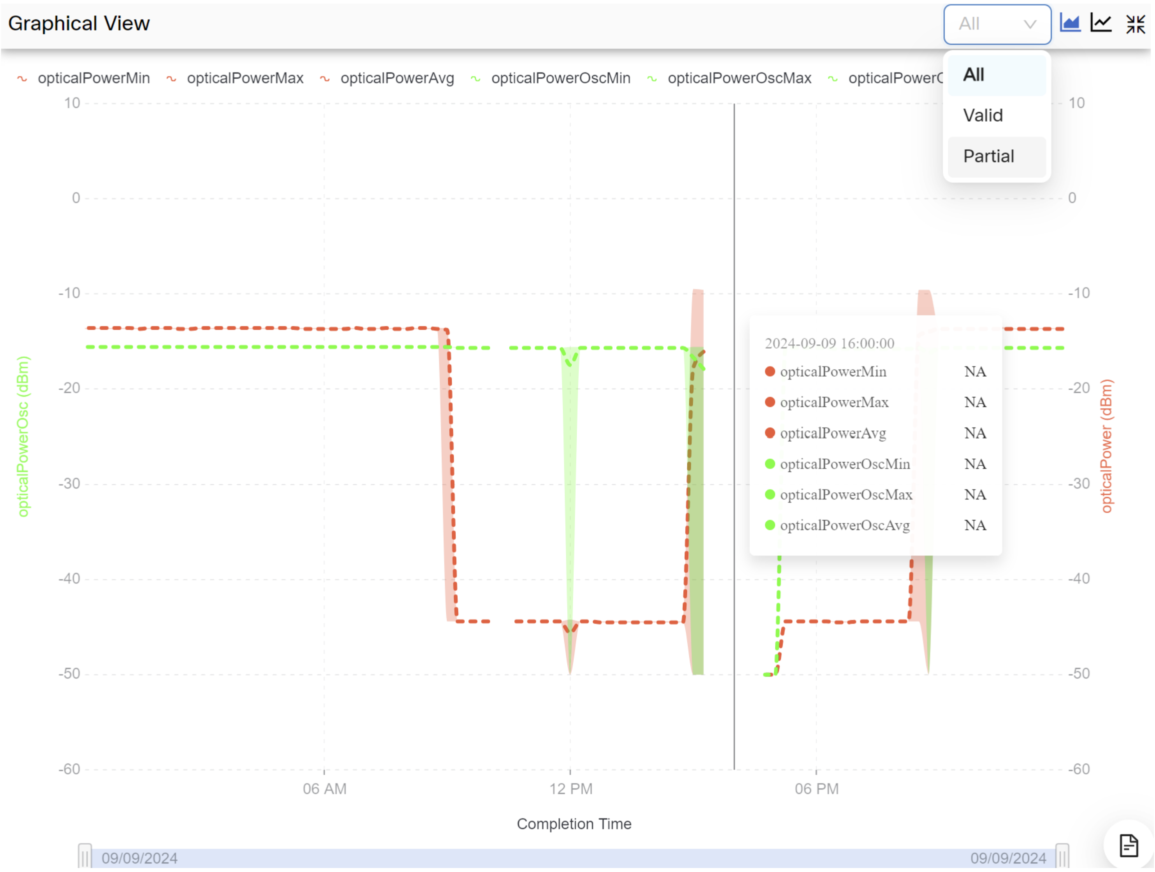
Graphical Representation within PM History Application

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 48: NA Values in Linear Graph



Accessing PM History Report

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

Procedure

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

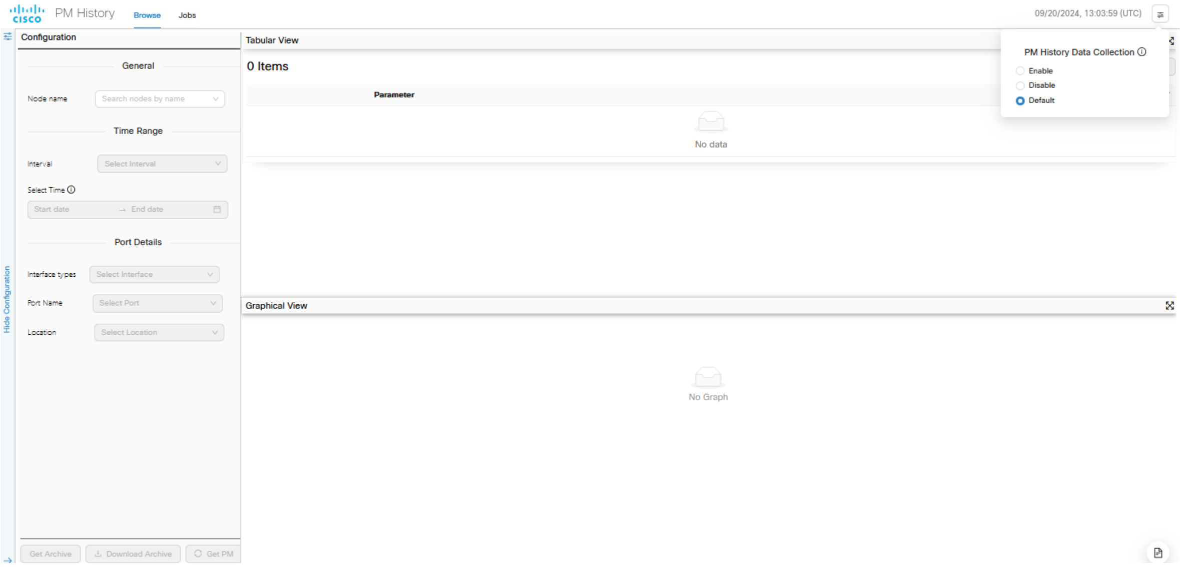
To browse or view the general PM History details follow the steps given:

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.
- You can enable, disable or select default values for PM History data collection using the **PM History Data Collection** option which appears on the top right corner of the **PM History** screen.
- 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**.

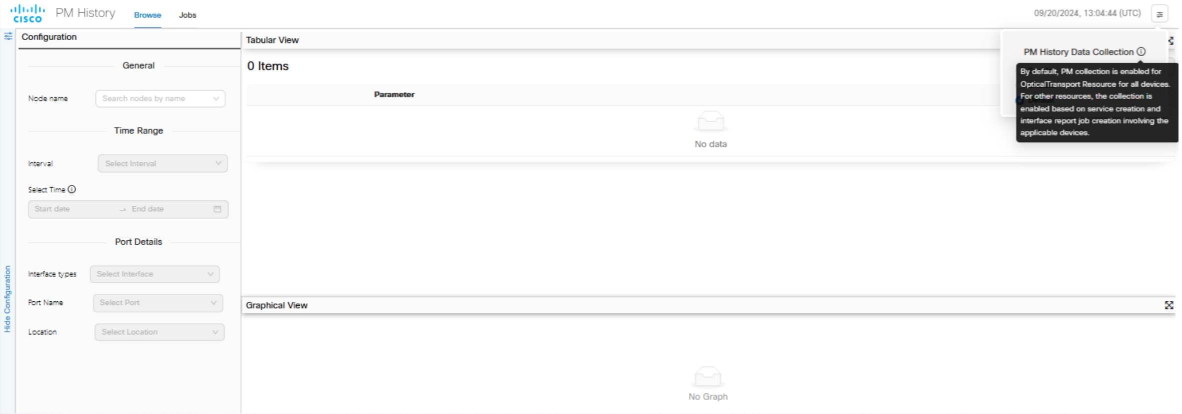
Figure 49: PM History Data Collection



PM History Data Collection

○ Enable
○ Disable
● Default

Figure 50: More Information about PM History Data Collection



By default, PM collection is enabled for OpticalTransport Resource for all devices. For other resources, the collection is enabled based on service creation and interface report job creation involving the applicable devices.

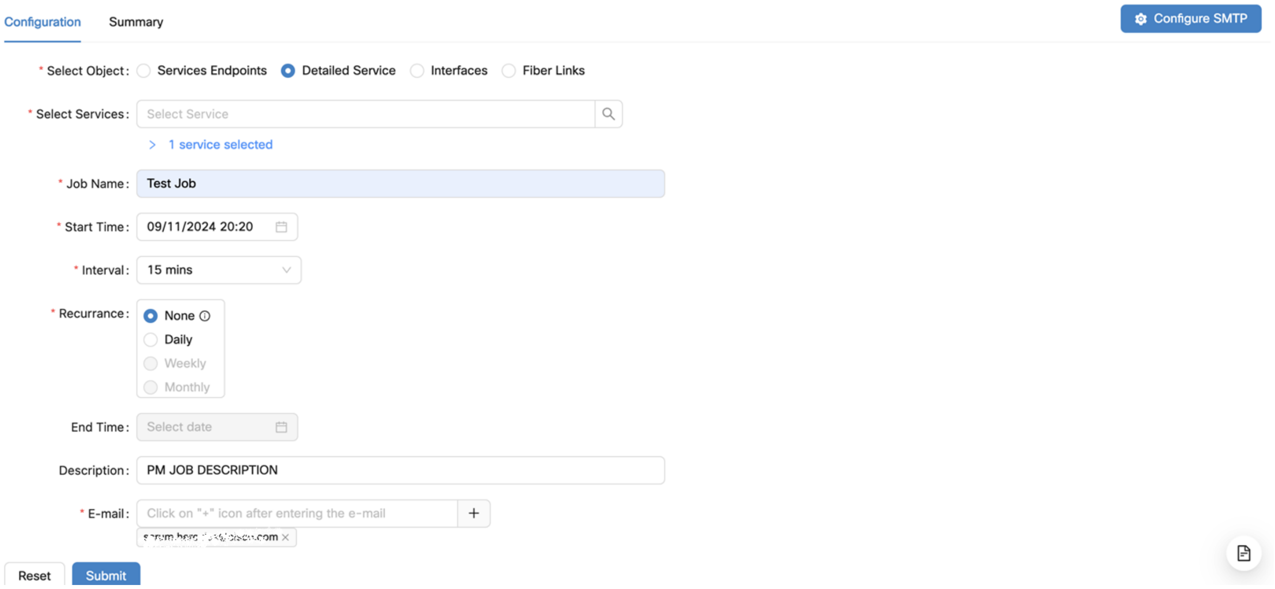
To browse or view the job scheduling details follow the steps given:

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 51: Configure SMTP



* Select Object: ○ Services Endpoints ● Detailed Service ○ Interfaces ○ Fiber Links

* Select Services: Select Service

› 1 service selected

* Job Name: Test Job

* Start Time: 09/11/2024 20:20

* Interval: 15 mins

* Recurrance: ● None ○ Daily ○ Weekly ○ Monthly

End Time: Select date

Description: PM JOB DESCRIPTION

* E-mail: Click on "+" icon after entering the e-mail +

[redacted] ×

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

To schedule the jobs follow the steps given:

a) 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.

b) Enter **Job Name**.

c) Enter **Start Time**.

d) Enter **Interval** which can be 15 mins or 24 Hours.

e) Enter **Recurrence** which can be either None, Daily, Weekly or Monthly.

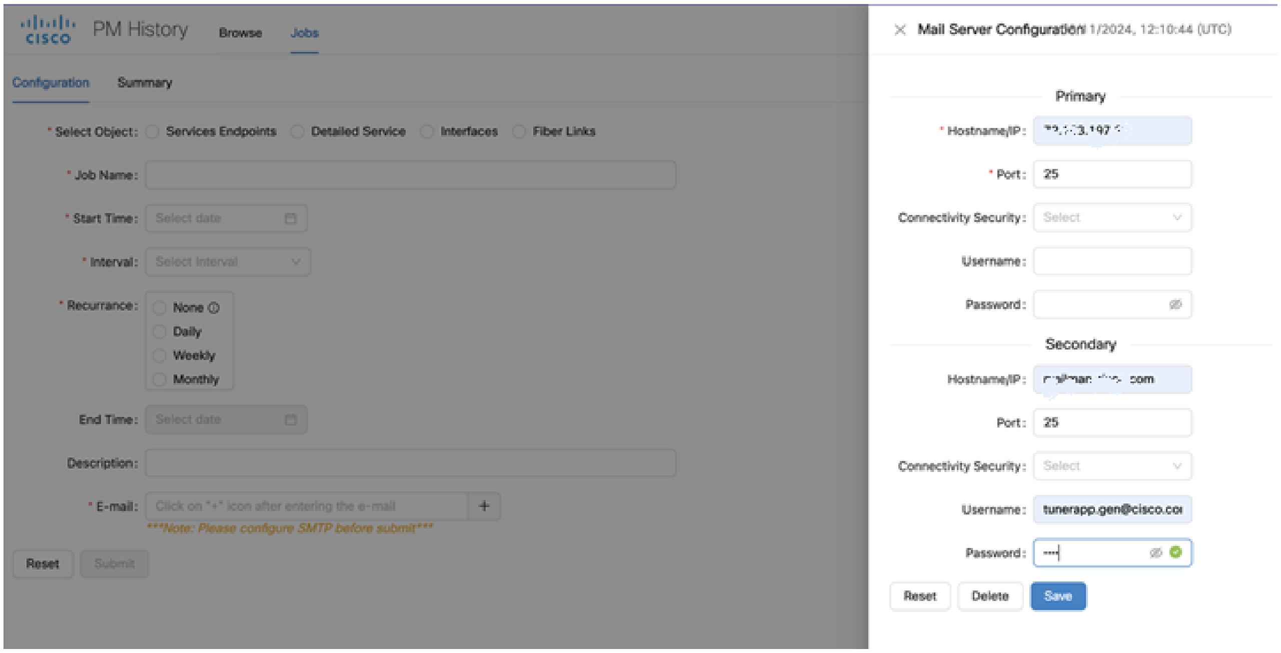
f) Enter **End Time**.

g) Enter **Description**.

h) 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 52: Jobs



PM History — Browse | Jobs

Configuration | Summary

* Select Object: ○ Services Endpoints ○ Detailed Service ○ Interfaces ○ Fiber Links
* Job Name:
* Start Time: Select date
* Interval: Select Interval
* Recurrance: ○ None ○ Daily ○ Weekly ○ Monthly
End Time: Select date
Description:
* E-mail: Click on "+" icon after entering the e-mail +
Note: Please configure SMTP before submit

Reset | Submit

Mail Server Configuration 1/2024, 12:10:44 (UTC)

Primary
* Hostname/IP: [redacted]
* Port: 25
Connectivity Security: Select
Username:
Password:

Secondary
Hostname/IP: [redacted]
Port: 25
Connectivity Security: Select
Username: tunerapp.gen@cisco.coı
Password: ····

Reset | Delete | Save

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 25: Audit Logs Category

Category Field	Description
System	The events that are part of this category are: • Login. • Logout. • Create user. • Delete user. • CONC database backup and restore
Inventory	The events that are part of this category are: • Card create/delete/state update. • Physical port and logical port create/delete/state update. • Interfaces create/delete/state update. • Chassis create/delete. • IPC add and delete. • Degree add and delete. • Passive unit add/delete • Port Frequency

Category Field	Description
Node	The events that are part of this category are: • Device add/delete/resync/reconnect. • Device state for discovered and disconnected status. • Connection loss or reconnect audit logs status.
Service	The events that are part of this category are: • Circuit add/delete/edit/update or state change. • Link up and down.
Topology	The events of this category include the OMS and OTS interfaces.
Site_Audit	The events that are part of this category are: • COSM login/logout/login failed. • COSM devices version. • All COSM provisions, notifications which are traffic impacting and audited under site audit category. • COSM backup/Restore
Alarm	All the events related to **Alarms**.
Alien_Import	All the events related to **Alien_Import**.
SNMP	• Add SNMP Manager • Delete SNMP Manager • Update SNMP Manager

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-xxxxxxxx.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  │
└──────────────────────────────┴───────────────┴────────────────────────────────┘
```

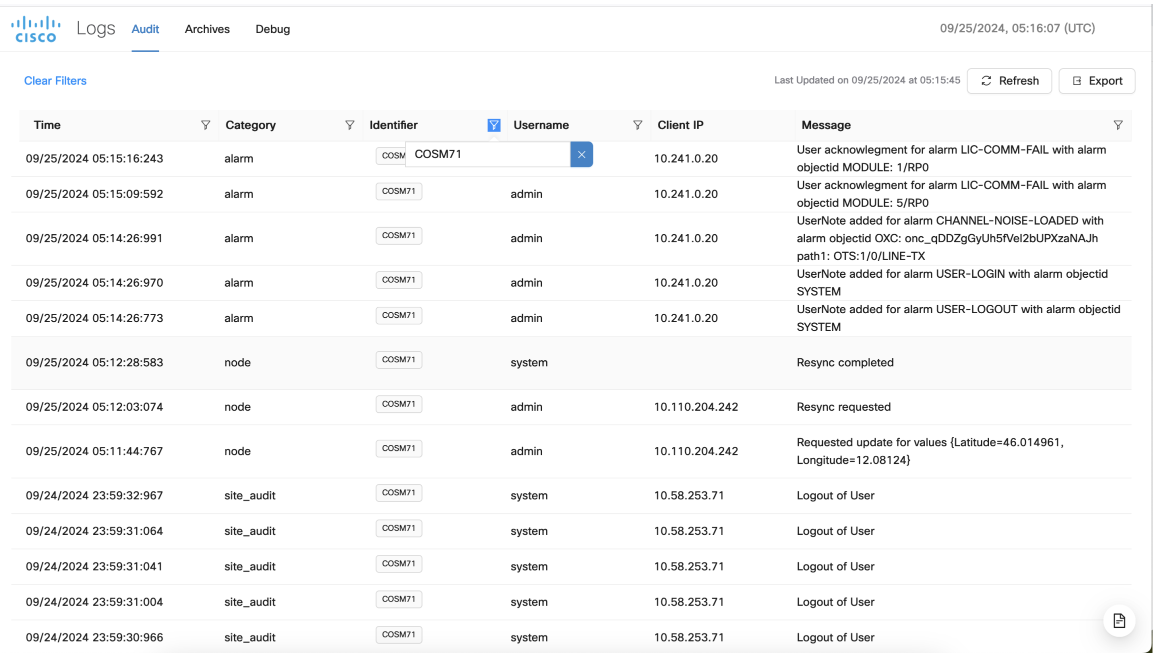
2. Step 2:

   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 53: Audit Logs

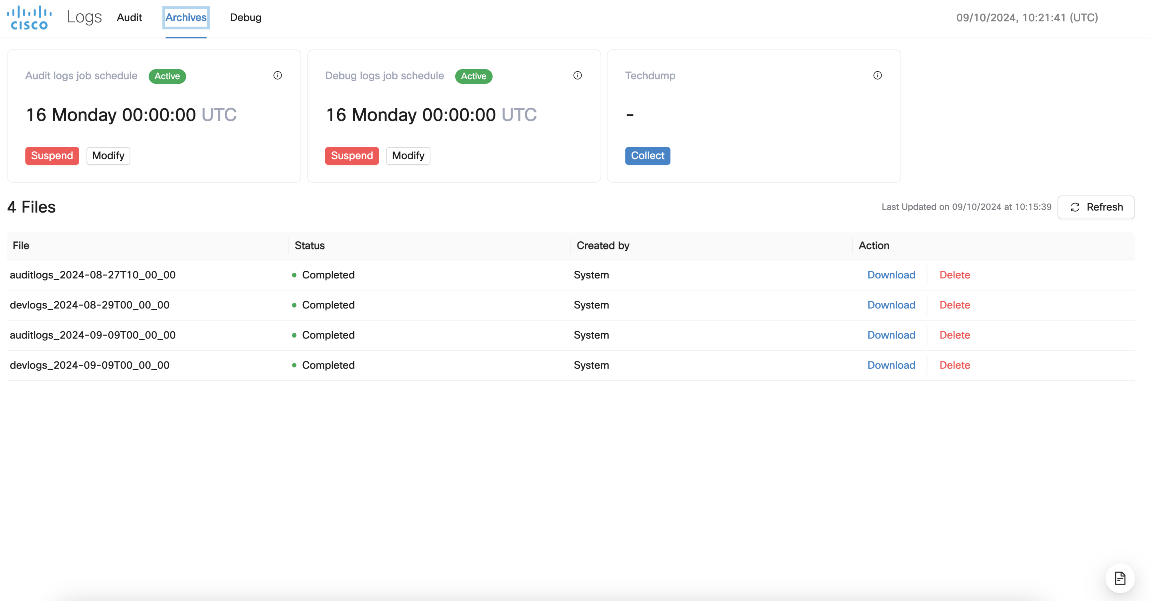


09/25/2024, 05:16:07 (UTC)

Last Updated on 09/25/2024 at 05:15:45

Time	Category	Identifier	Username	Client IP	Message
09/25/2024 05:15:16:243	alarm	COSM COSM71		10.241.0.20	User acknowlegment 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 acknowlegment 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_qDDZgGyUh5fVel2bUPXzaNAJh 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 54: Archive Logs



09/10/2024, 10:21:41 (UTC)

Audit logs job schedule Active

16 Monday 00:00:00 UTC

Debug logs job schedule Active

16 Monday 00:00:00 UTC

Techdump

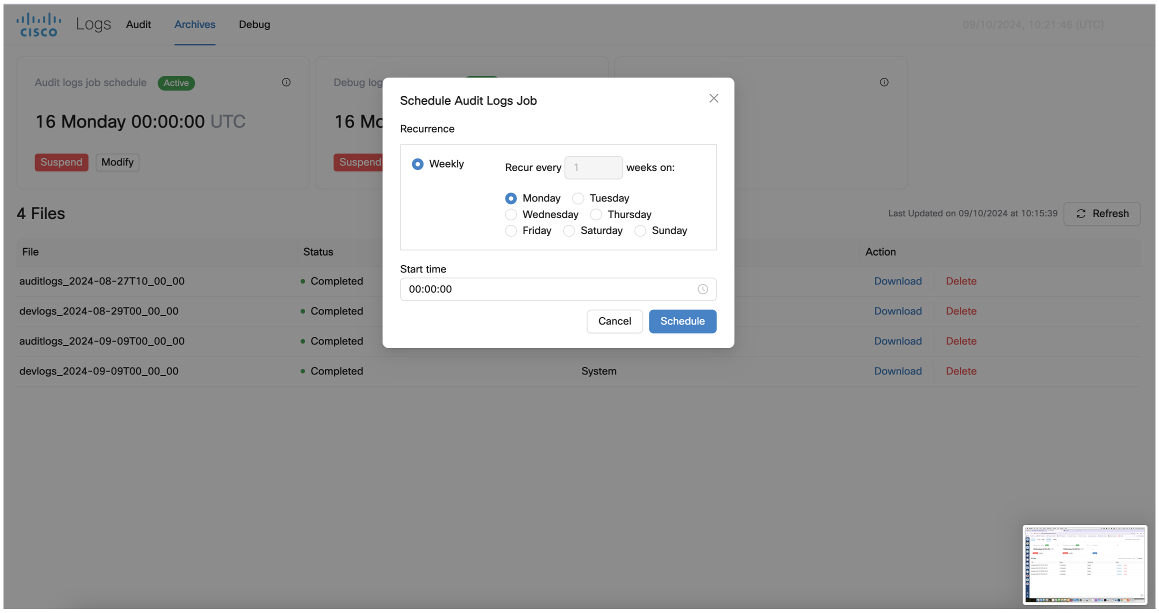
-

4 Files

Last Updated on 09/10/2024 at 10:15:39

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 55: Scheduling Audit Logs Job



Audit logs job schedule Active

16 Monday 00:00:00 UTC

Debug log…

16 Mo…

Schedule Audit Logs Job

Recurrence

● Weekly   Recur every 1 weeks on:

● Monday ○ Tuesday
○ Wednesday ○ Thursday
○ Friday ○ Saturday ○ Sunday

Start time

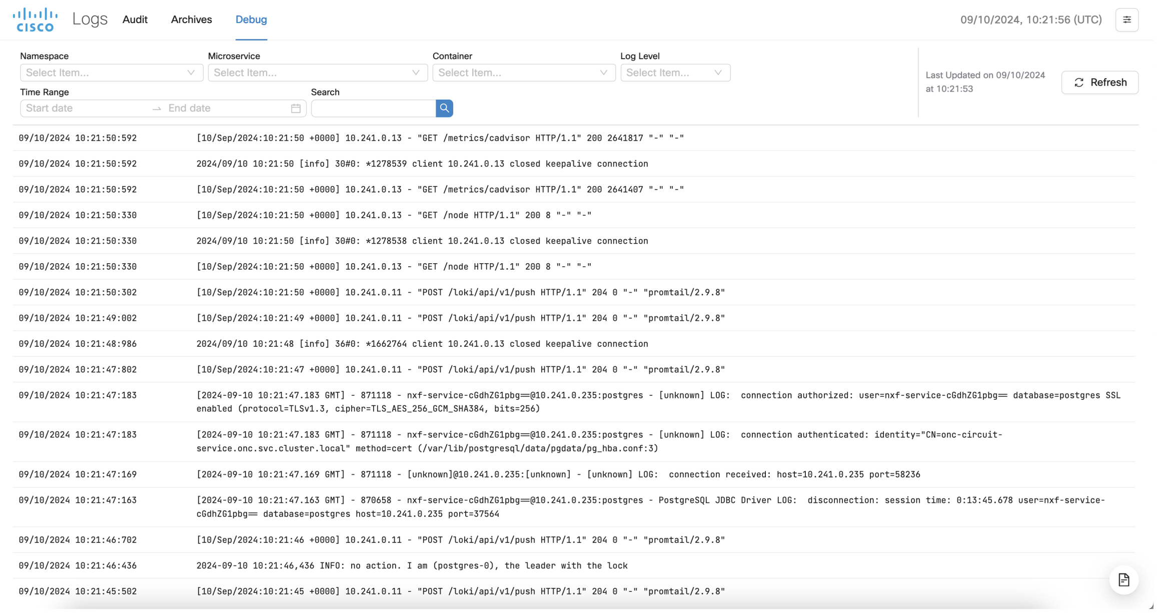
00:00:00

4 Files

Last Updated on 09/10/2024 at 10:15:39

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

Figure 56: Debug Logs



Namespace: Select Item...
Microservice: Select Item...
Container: Select Item...
Log Level: Select Item...
Time Range: Start date → End date
Search

Last Updated on 09/10/2024 at 10:21:53

```
09/10/2024 10:21:50:592    [10/Sep/2024:10:21:50 +0000] 10.241.0.13 - "GET /metrics/cadvisor HTTP/1.1" 200 2641817 "-" "-"
09/10/2024 10:21:50:592    2024/09/10 10:21:50 [info] 30#0: *1278539 client 10.241.0.13 closed keepalive connection
09/10/2024 10:21:50:592    [10/Sep/2024:10:21:50 +0000] 10.241.0.13 - "GET /metrics/cadvisor HTTP/1.1" 200 2641407 "-" "-"
09/10/2024 10:21:50:330    [10/Sep/2024:10:21:50 +0000] 10.241.0.13 - "GET /node HTTP/1.1" 200 8 "-" "-"
09/10/2024 10:21:50:330    2024/09/10 10:21:50 [info] 30#0: *1278538 client 10.241.0.13 closed keepalive connection
09/10/2024 10:21:50:330    [10/Sep/2024:10:21:50 +0000] 10.241.0.13 - "GET /node HTTP/1.1" 200 8 "-" "-"
09/10/2024 10:21:50:302    [10/Sep/2024:10:21:50 +0000] 10.241.0.11 - "POST /loki/api/v1/push HTTP/1.1" 204 0 "-" "promtail/2.9.8"
09/10/2024 10:21:49:002    [10/Sep/2024:10:21:49 +0000] 10.241.0.11 - "POST /loki/api/v1/push HTTP/1.1" 204 0 "-" "promtail/2.9.8"
09/10/2024 10:21:48:986    2024/09/10 10:21:48 [info] 36#0: *1662764 client 10.241.0.13 closed keepalive connection
09/10/2024 10:21:47:802    [10/Sep/2024:10:21:47 +0000] 10.241.0.11 - "POST /loki/api/v1/push HTTP/1.1" 204 0 "-" "promtail/2.9.8"
09/10/2024 10:21:47:183    [2024-09-10 10:21:47.183 GMT] - 871118 - nxf-service-cGdhZG1pbg==@10.241.0.235:postgres - [unknown] LOG:  connection authorized: user=nxf-service-cGdhZG1pbg== database=postgres SSL
                           enabled (protocol=TLSv1.3, cipher=TLS_AES_256_GCM_SHA384, bits=256)
09/10/2024 10:21:47:183    [2024-09-10 10:21:47.183 GMT] - 871118 - nxf-service-cGdhZG1pbg==@10.241.0.235:postgres - [unknown] LOG:  connection authenticated: identity="CN=onc-circuit-
                           service.onc.svc.cluster.local" method=cert (/var/lib/postgresql/data/pgdata/pg_hba.conf:3)
09/10/2024 10:21:47:169    [2024-09-10 10:21:47.169 GMT] - 871118 - [unknown]@10.241.0.235:[unknown] - [unknown] LOG:  connection received: host=10.241.0.235 port=58236
09/10/2024 10:21:47:163    [2024-09-10 10:21:47.163 GMT] - 870658 - nxf-service-cGdhZG1pbg==@10.241.0.235:postgres - PostgreSQL JDBC Driver LOG:  disconnection: session time: 0:13:45.678 user=nxf-service-
                           cGdhZG1pbg== database=postgres host=10.241.0.235 port=37564
09/10/2024 10:21:46:702    [10/Sep/2024:10:21:46 +0000] 10.241.0.11 - "POST /loki/api/v1/push HTTP/1.1" 204 0 "-" "promtail/2.9.8"
09/10/2024 10:21:46:436    2024-09-10 10:21:46,436 INFO: no action. I am (postgres-0), the leader with the lock
09/10/2024 10:21:45:502    [10/Sep/2024:10:21:45 +0000] 10.241.0.11 - "POST /loki/api/v1/push HTTP/1.1" 204 0 "-" "promtail/2.9.8"
```

Benefits of Logs Enhancement

Log enhancements help in:

Table 26: 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.

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.

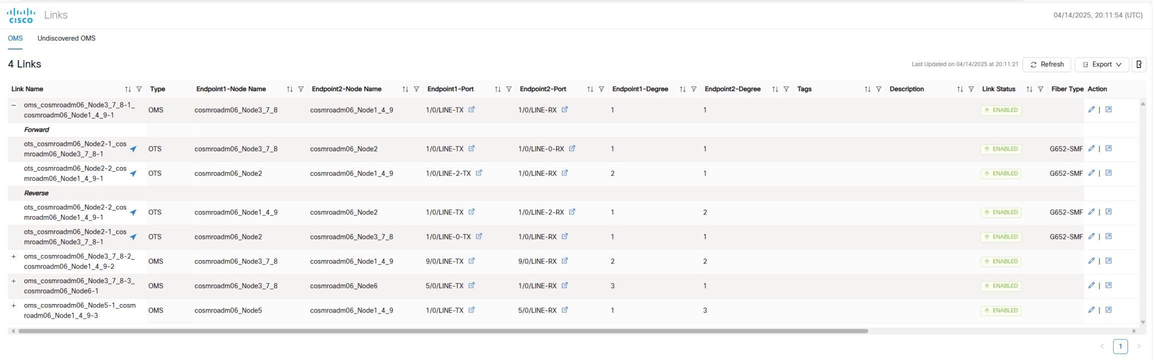
Procedure

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 57: Links App



04/14/2025, 20:11:54 (UTC)

4 Links

Last Updated on 04/14/2025 at 20:11:21

Link Name	Type	Endpoint1-Node Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port	Endpoint1-Degree	Endpoint2-Degree	Tags	Description	Link Status	Fiber Type	Action
− 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		✎ | ↗
Forward												
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-RX	2	1			↑ ENABLED	G652-SMF	✎ | ↗
Reverse												
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-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-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-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-RX	1	3			↑ ENABLED		✎ | ↗

1

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.

Links table

The table includes these columns:

- Link Name
- Type (OMS or OTS)
- 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.

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.
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.

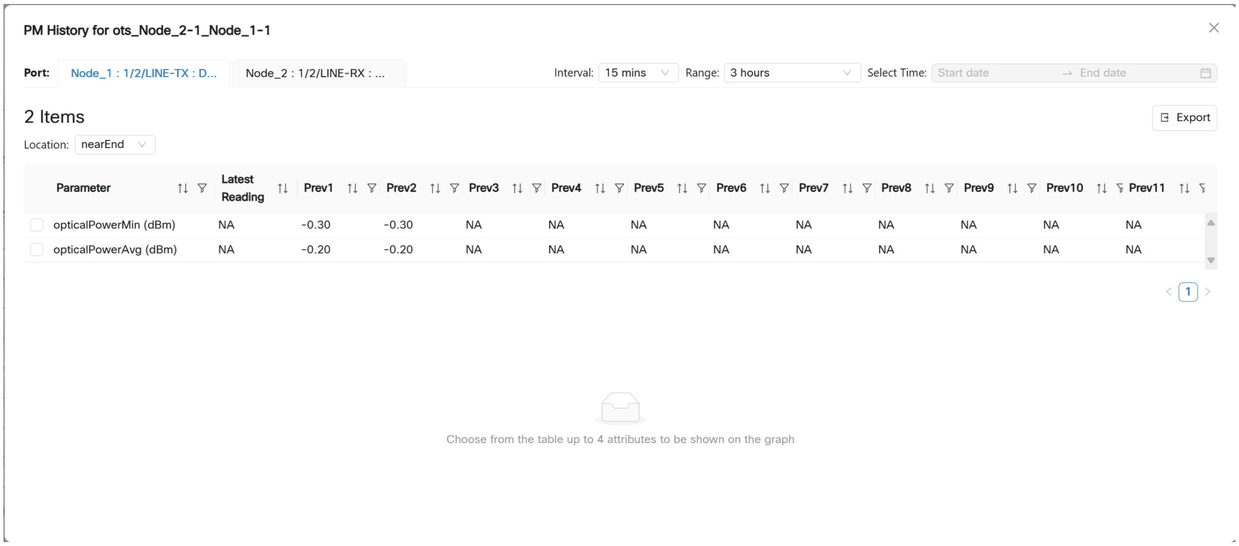
a) Select a link in the OMS or Undiscovered OMS tab.
b) Click the circuit monitoring icon in the Action column.

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 58: Links App



PM History for ots_Node_2-1_Node_1-1

Port: Node_1 : 1/2/LINE-TX : D... | Node_2 : 1/2/LINE-RX : ...

Interval: 15 mins Range: 3 hours Select Time: Start date → End date

2 Items

Location: nearEnd

Parameter	Latest Reading	Prev1	Prev2	Prev3	Prev4	Prev5	Prev6	Prev7	Prev8	Prev9	Prev10	Prev11
□ opticalPowerMin (dBm)	NA	-0.30	-0.30	NA	NA	NA	NA	NA	NA	NA	NA	NA
□ opticalPowerAvg (dBm)	NA	-0.20	-0.20	NA	NA	NA	NA	NA	NA	NA	NA	NA

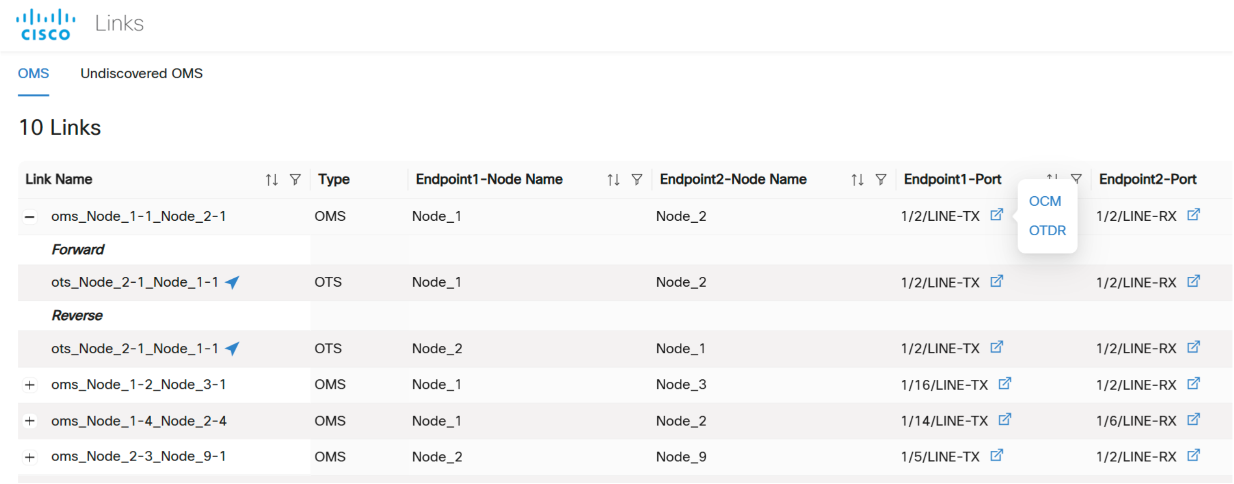
Choose from the table up to 4 attributes to be shown on the graph

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.

a) In the OMS tab, expand an OMS link to view its OTS links.
b) Click the cross-launch icon in the **Endpoint1-Port** or **Endpoint2-Port**.

Figure 59: Links App



10 Links

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
Forward					
ots_Node_2-1_Node_1-1	OTS	Node_1	Node_2	1/2/LINE-TX	1/2/LINE-RX
Reverse					
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

c) 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.

a) Click **Export**.
b) (Optional) Select **Table View** and click **Export** to export and download the data currently displayed in the table.
c) Select **Network Links** to export all network links.
d) Click **Generate**.
e) 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.

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:

  ```
  sedo diagnostics archive-logs
  ```

  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 60: Unmanaged Equipment Support in Topology

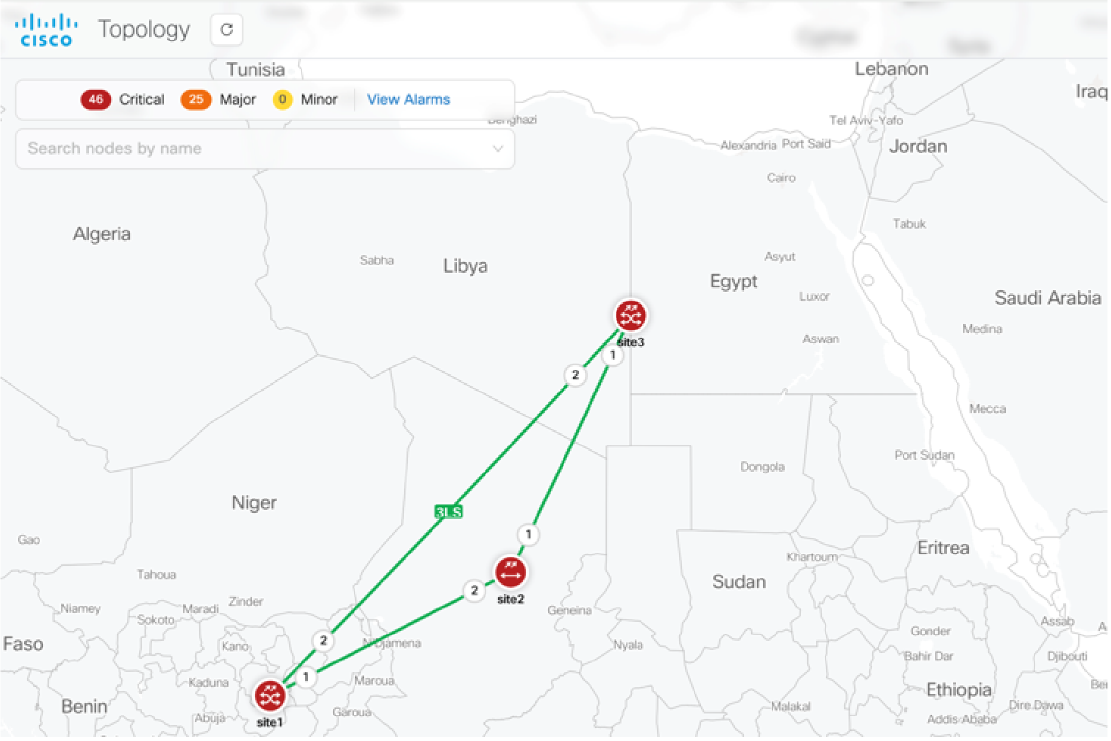
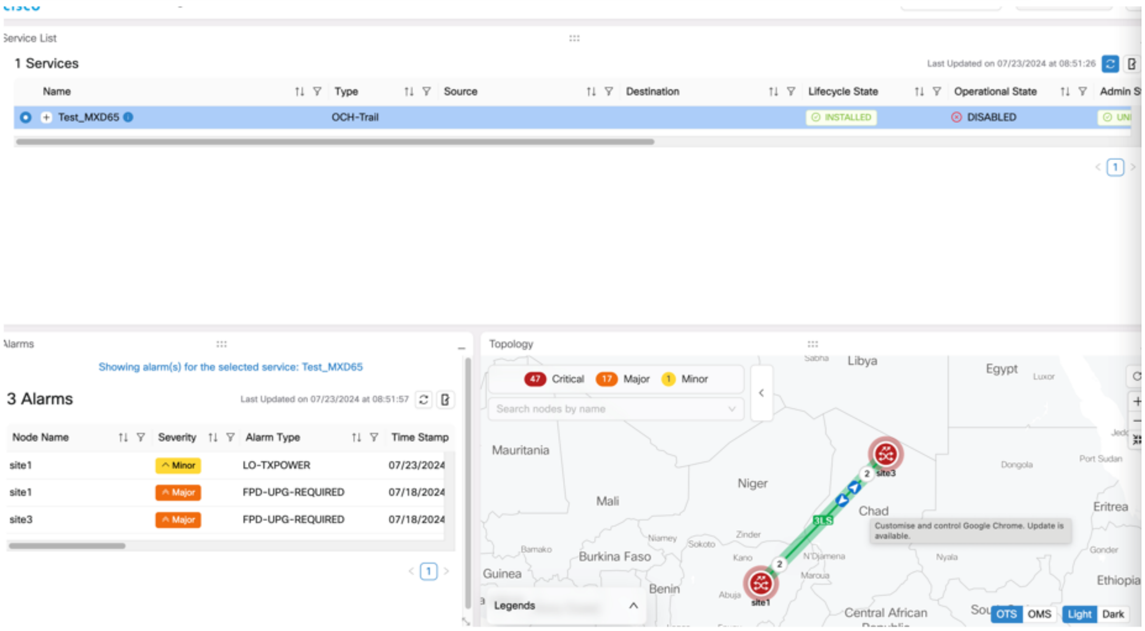


Figure 61: Unmanaged Equipment Support in Service Assurance



Service List

1 Services

Last Updated on 07/23/2024 at 08:51:26

Name	Type	Source	Destination	Lifecycle State	Operational State	Admin S
Test_MXD65	OCH-Trail			INSTALLED	DISABLED	UNI

Alarms

Showing alarm(s) for the selected service: Test_MXD65

3 Alarms

Last Updated on 07/23/2024 at 08:51:57

Node Name	Severity	Alarm Type	Time Stamp
site1	Minor	LO-TXPOWER	07/23/2024
site1	Major	FPD-UPG-REQUIRED	07/18/2024
site3	Major	FPD-UPG-REQUIRED	07/18/2024

PSM Fiber 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

- 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 fiber 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 ILA sites are not supported in 24.3.1 release, refer to the P2P scenario.

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 Fiber Protection

- Cisco Optical Network Controller does not support PSM Protection switching in optical circuits with NCS 1010 ILA modules between NCS 1010 OLT nodes.
- Cisco Optical Network Controller does not support 3-way PSM Protection switching.
- The W-RX and P-RX thresholds for the 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. Fiber protection is not supported.
- You must perform a resync if you onboard devices, add or modify IPCs, or add or remove degrees to the netwwork 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 Click **Circuit Monitoring**.

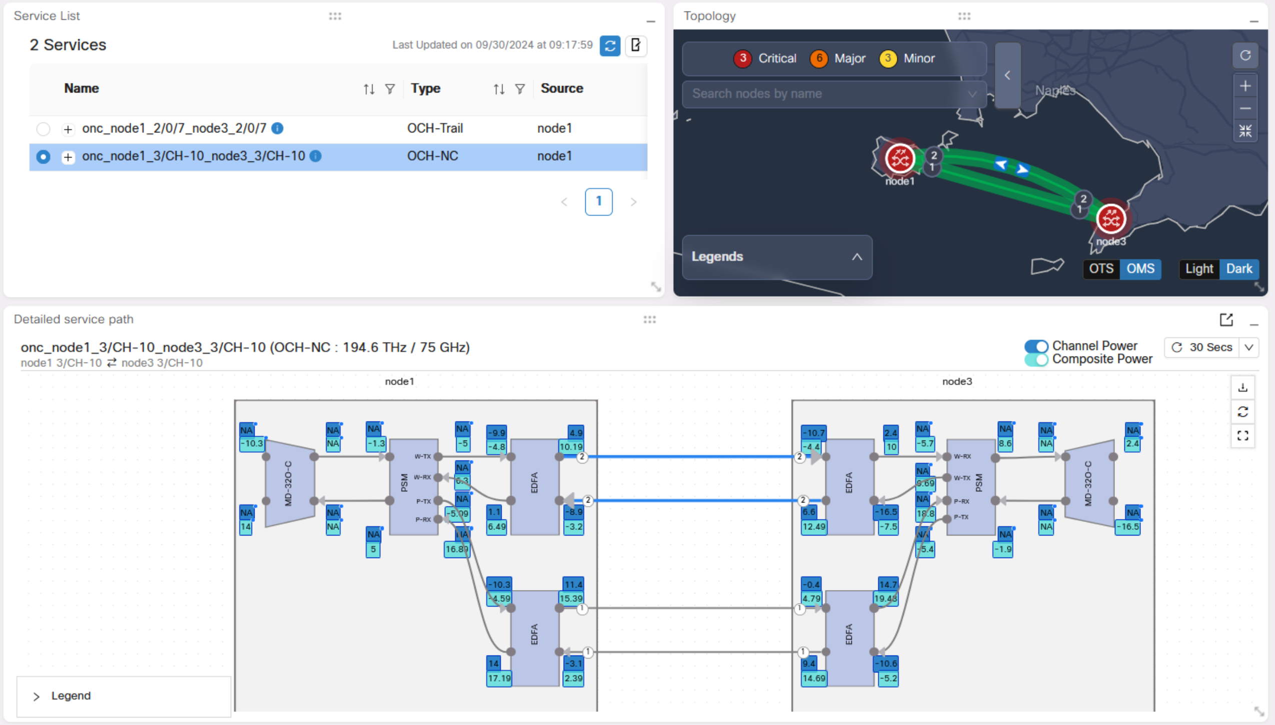
Step 3 Select the PSM circuit.

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.

Figure 62: PSM Circuit in Workspace



Service List

2 Services

Last Updated on 09/30/2024 at 09:17:59

	Name	Type	Source
○	+ onc_node1_2/0/7_node3_2/0/7	OCH-Trail	node1
●	+ onc_node1_3/CH-10_node3_3/CH-10	OCH-NC	node1

Topology

3 Critical 6 Major 3 Minor

Search nodes by name

Detailed service path

onc_node1_3/CH-10_node3_3/CH-10 (OCH-NC : 194.6 THz / 75 GHz)

node1 3/CH-10 ⇄ node3 3/CH-10

Channel Power

Composite Power

30 Secs

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 apllication 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>
```