

Cisco Optical Network Controller Configuration Guide, Releases 25.1.x

First Published: 2025-04-28

Last Modified: 2026-09-15

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

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview of Cisco Optical Network Controller** 1

- Cisco Optical Network Controller Overview 1
- Log in to Cisco Optical Network Controller 3
- User access in Cisco Optical Network Controller 4
- Add local users to Cisco Optical Network Controller 7
- Set up authentication using LDAP 10
- Set up authentication using SAMLv2 SSO 12
- Set up Permission Mapping 14
- Manage Certificates in Cisco Optical Network Controller 16

CHAPTER 2 **Use Cisco Optical Network Controller** 19

- Topology 21
  - Troubleshooting in Topology 27
- Nodes 28
  - Reserved internal IP addresses and subnets 31
  - Add nodes on Cisco Optical Network Controller 32
  - Import multiple nodes into Cisco Optical Network Controller 35
  - Export Nodes on Cisco Optical Network Controller 38
  - Edit Nodes on Cisco Optical Network Controller 38
  - Delete nodes on Cisco Optical Network Controller 38
  - Troubleshooting in Nodes 39
- Alien Import 41
- Network Inventory 42
- Service Manager 43
  - Create and manage circuits 51
    - Troubleshoot CPCE Services 60

Provision GMPLS services 62
Alarms 73
Network Level Alarm Correlation 78
Acknowledged Alarm Mute 80
SNMP Traps and Alarm Filters 82
Set the Edit Host Name 83
Configure SNMP managers 84
Workspaces 87
Circuit Monitoring workspace 88
Link Monitoring workspace 97
Network Monitoring workspace 103
Software Image Management and Upgrade 104
Configure SFTP server 106
Backup and Restore Nodes 107
Backup and Restore Database 109
Orchestrate Upgrades 113
PM History 117
PM Data Retention 124
Disk Space 125
Charateresitics of PM data retention 126
PM Data Collection 127
Accessing PM History Report 129
Configure the SMTP mail server 131
Mail server fields 133
Connectivity security options 133
Logs 134
Accessing Logs 140
Generate and download tech dump logs 142
Monitoring 143
Links 144
Use the Links Application 146
General Troubleshooting 147
Unmanaged Equipment Support 148
PSM OMS Protection 150

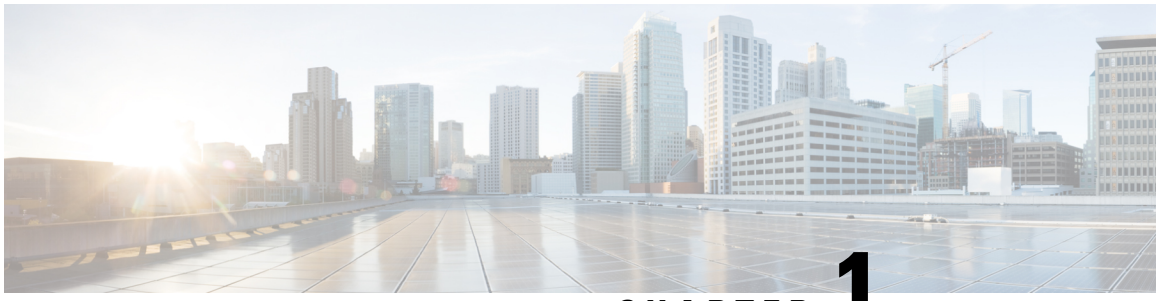
PSM Circuit in Workspace Screen 151
Forwarding Syslogs 152
Collect and download SEDO diagnostic files 154

CHAPTER 3 Alarm Troubleshooting 159
BACKUP-FAILURE 159
Clear the BACKUP-FAILURE Alarm 159
NODE-BACKUP-FAILURE 160
Clear the NODE-BACKUP-FAILURE Alarm 160
NODE-DISCONNECT 160
Clear the NODE-DISCONNECT Alarm 161
UPLOAD-FAILURE 161
Clear the UPLOAD-FAILURE Alarm 161
DISK THRESHOLD 161
Clear the DISK-THRESHOLD Alarm 162
SWITCHOVER 163
Clear the SWITCHOVER Alarm 163
FAILOVER 163
Clear the FAILOVER Alarm 163

APPENDIX A Alarm categories 165

APPENDIX B MIB Definition For Cisco Optical Network Controller 215

APPENDIX C Platforms Software Compatibility Matrix 219



CHAPTER 1

Overview of Cisco Optical Network Controller

- Cisco Optical Network Controller Overview, on page 1
- Log in to Cisco Optical Network Controller, on page 3
- User access in Cisco Optical Network Controller, on page 4
- Add local users to Cisco Optical Network Controller, on page 7
- Set up authentication using LDAP, on page 10
- Set up authentication using SAMLv2 SSO, on page 12
- Set up Permission Mapping, on page 14
- Manage Certificates in Cisco Optical Network Controller, on page 16

Cisco Optical Network Controller Overview

Cisco Optical Network Controller (Cisco ONC) is an optical SDN Controller for Cisco optical networks. Cisco Optical Network Controller behaves as a Provisioning Network Controller (PNC) and performs these functions.

- Collects information about the inventory (device types, circuits and more) and topology (node arrangment) of the managed network.
- Monitors the physical or virtual topology of the network.
- Notifies of changes in topology and service changes.
- Supports the creation and deletion of optical paths.

Optical SDN controller

Optical SDN controller is a specialized SDN controller that

- manages and controls devices within a optical technology domain, and
- communicates with the higher-level SDN controller via east-west interfaces

Core functions of Cisco Optical Network Controller

Cisco Optical Network Controller collects data necessary for optical applications. This data is used to provide abstract network information to higher layer controllers. This abstraction enables centralized control of optical network.

Cisco Optical Network Controller supports several functions.

- Optical Domain Controller

  Cisco Optical Network Controller behaves as a domain controller for Cisco optical products. The domain controller feeds data into hierarchical controllers for high-level network orchestration. Cisco Optical Network Controller has a North Bound Interface (NBI) based on the OIF transport API (T-API) standard which enables it to connect to any hierarchical controller which has a TAPI compliant South Bound Interface (SBI) and provides its functions to the controller.

- Path Compute Engine (PCE)

  PCE service provides optical path computation to ensure optically valid paths are provisioned within the supplied constraints. PCE uses the latest network status to compute the optical path.

- Model Based Network Abstraction

  Cisco Optical Network Controller supports a standardized TAPI model which enables it to abstract the device level details from the hierarchical controller.

Note

- For more details on Cisco Optical Site Manager (COSM), see COSM Configuration Guide.
- For more details on Cisco Optical Network Planner (CONP), see CONP Configuration Guide.
- For further details about Cisco Optical Network Controller, see the Cisco Optical Network Controller (CONC) Data Sheet .

Important

- TAPI is disabled by default to ensure proper device integration and data collection, enabling seamless operation. You must enable it before onboarding devices.
- You must not enable TAPI after onboarding devices in Cisco Optical Network Controller. It must be enabled only before onboarding any of the devices.
- You must enable TAPI after de-boarding all the devices.

  To enable or disable TAPI, see Enabling and Disabling the TAPI Northbound Interface

Software Requirements

Cisco Optical Network Controller, Release 25.1.x supports these software versions.

Table 1: Software Support

Hardware and Software	Version
NCS 1001	Cisco IOS XR Release 7.10.1
NCS 1004	Cisco IOS XR Release 24.3.1
NCS 1014	Cisco IOS XR Releases 25.1.1 and 24.3.1

Hardware and Software	Version
NCS 1010	Cisco IOS XR Releases 25.1.1 and 24.3.1
Cisco Optical Site Manager	
NCS 1000	Cisco IOS XR Releases 25.1.1 and 24.3.1
NCS 2000	Release 25.1.1

Log in to Cisco Optical Network Controller

Follow these steps to log into Cisco Optical Network Controller:

Procedure

Step 1 In the browser URL field, enter `https://<virtual-ip>:8443/`

Note
<virtual-ip> refers to the IP address or hostname of your Cisco Optical Network Controller deployment.

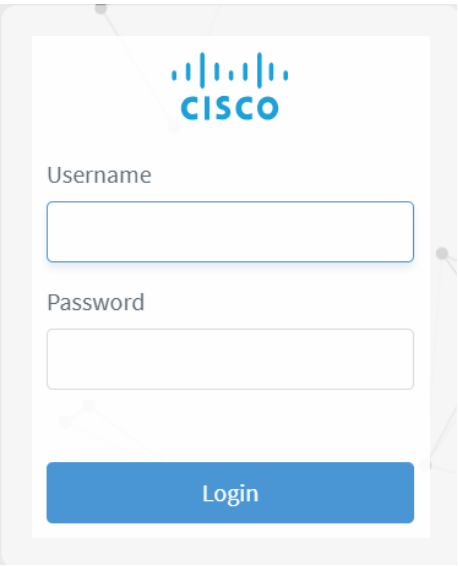
The browser displays the login page.

Step 2 Enter the username and password.

Username and password are provided by your system administrator.

Step 3 Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



Note

Cisco Optical Network Controller supports a maximum of 25 users to log in concurrently.

User access in Cisco Optical Network Controller

Users, Roles, and Permissions

Cisco Optical Network Controller allows you to manage user access and permissions. It adds an additional layer of security. It works as a Single Authentication Agent, thus sharing local, Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML) users. The Single Authentication Agent simplifies user management and provides a unified login experience across different authentication sources.

Cisco Optical Network Controller provides different permission levels for user access. See *Set up Permission Mapping*. To allow access to Cisco Optical Network Controller to a larger group of regular users, set the user authentication through LDAP or SAML Single Sign-On (SSO) protocols. You can use both protocols simultaneously, depending on your environment.

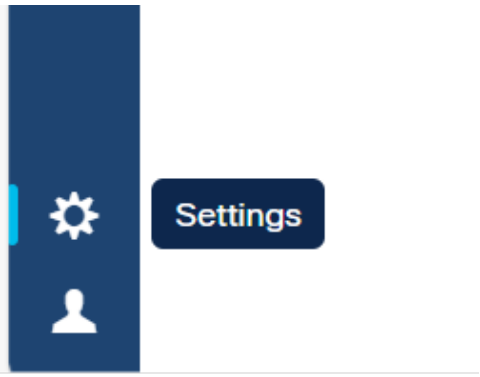
Table 2: User roles and permissions

User role	Permission	Access level
Admin	permission/admin	has no restrictions
Supervisor	permission/supervisor	has similar permission as admin but with restrictions on user management and log checks
Read-only	permission/readonly	can check data, but cannot provision.
Internal	permission/internal	collects debug logs in case of any triage or troubleshooting. **Note** We recommend using it only under the supervision of the Cisco Technical Assistance Center (TAC).

Accessing Settings

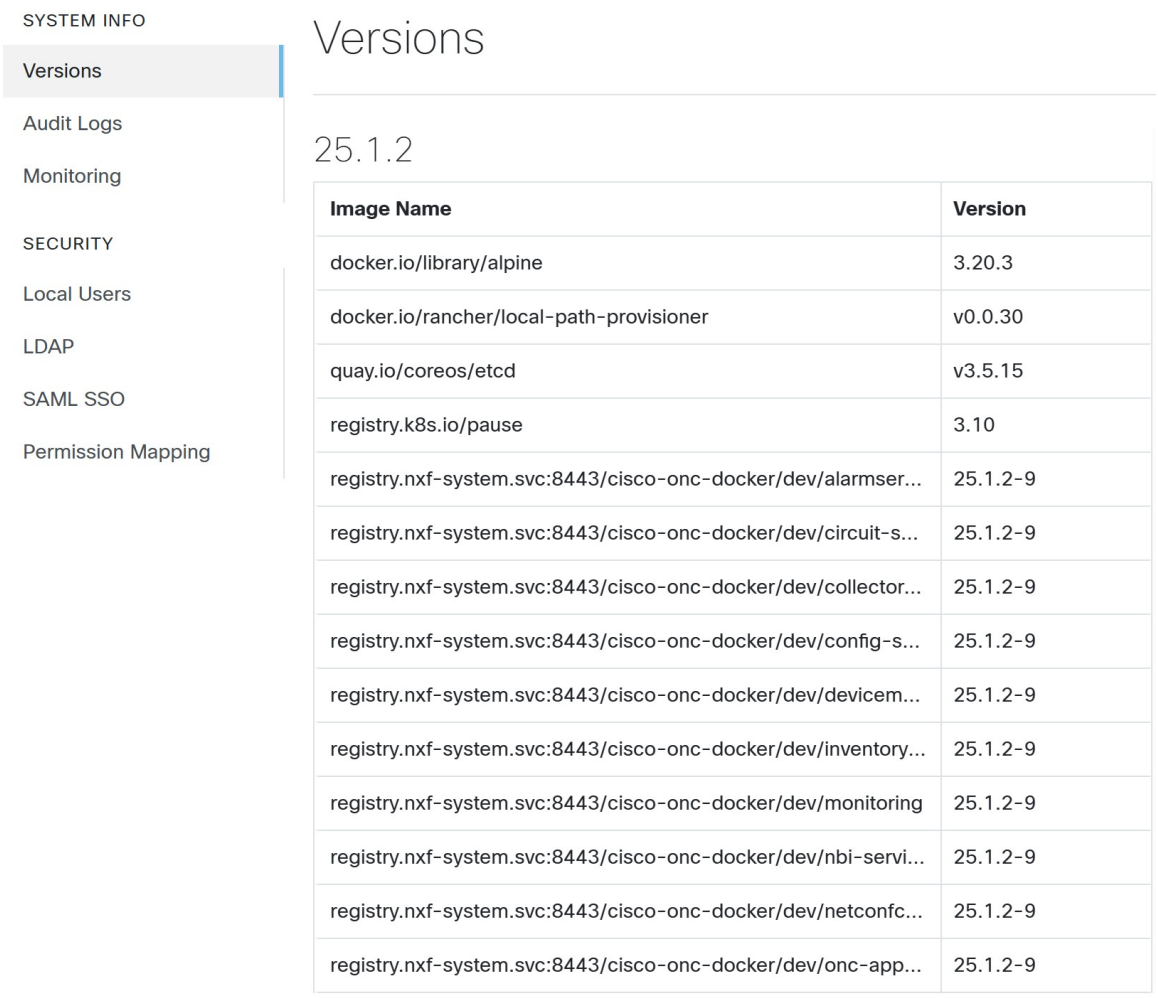
The settings button is available on the left navigation bar of Cisco Optical Network Controller.

Figure 2: Settings



After clicking **Settings** you see the settings panel.

Figure 3: Settings Options



System Info

The **System Info** section has the information about the latest versions of Cisco Optical Network Controller and the related microservices.

Security

The **Security** section is for access management and offers several options.

- **Local Users**: Display, create, and edit local users through the UI.
- **LDAP**: Set LDAP settings for user authentication.
- **SAML SSO**: Set SAML Single-Sign-On settings for user authentication.
- **Permission Mapping**: Handle permission management through the Cisco Policy Management Tool.

Note Cisco Optical Network Controller does not allow the configuration of timeout and retry client parameters for LDAP and SAML SSO authentication. Instead, it automatically applies the default values to the timeout and retry settings.

Add local users to Cisco Optical Network Controller

Add local user accounts to Cisco Optical Network Controller by completing these steps.

Before you begin

You need administrative user privileges to access Cisco Optical Network Controller.

Procedure

Step 1 From the Cisco Optical Network Controller home page click **Settings**.

Step 2 From the panel list, select **Local Users** and click **Add**.
The **Add User** screen appears.

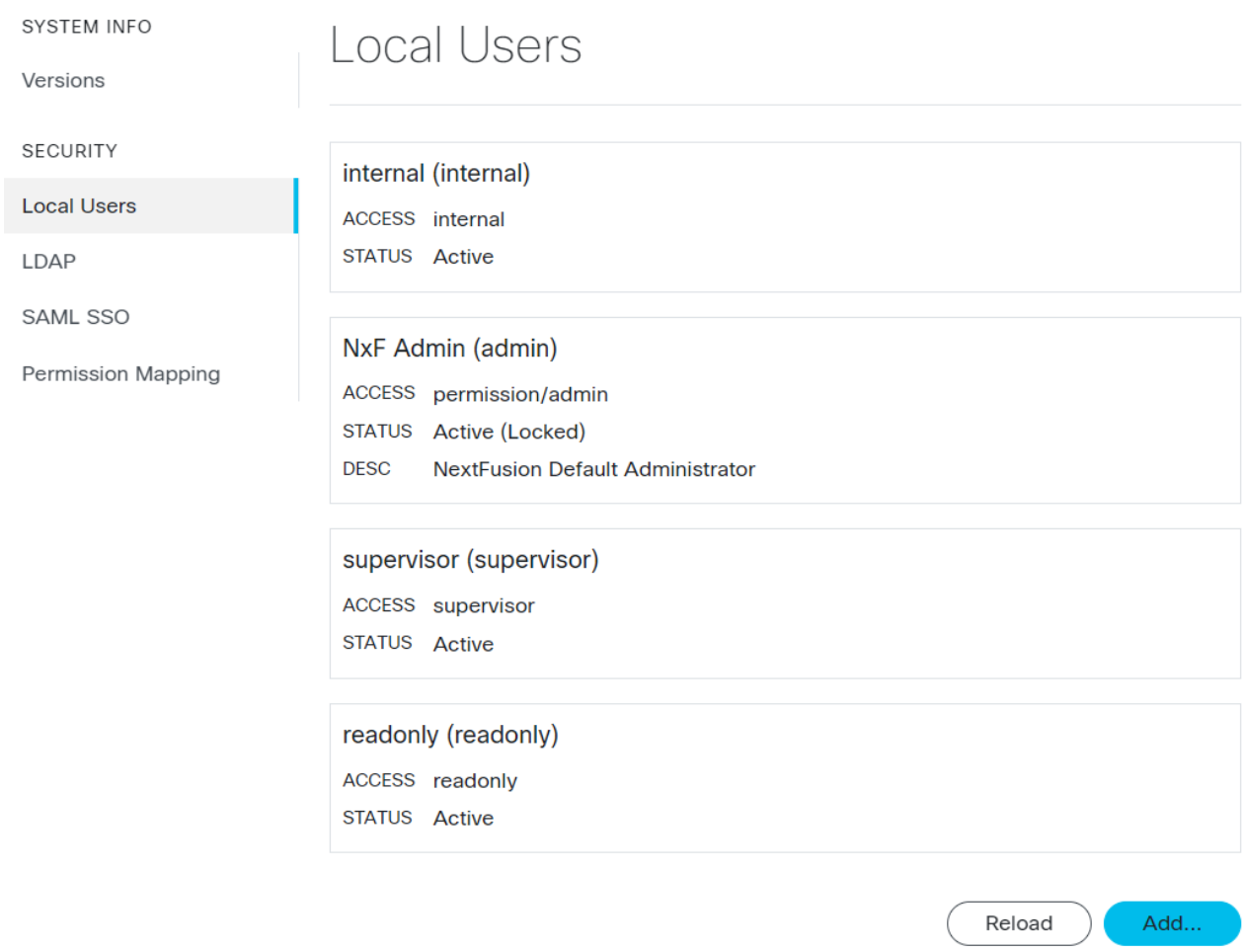
Step 3 In the **Add User** screen, fill these mandatory fields.

a) Enter a username in **Username***.
b) In **Password***, enter a password.
c) In **Confirm Password***, re-enter the password to confirm the password.

Note
Cisco Optical Network Controller uses cryptographic mechanism to secure credentials stored in the system. Cisco Optical Network Controller CLI and Web UI passwords use salted one-way hashing with yescrypt and bcrypt, respectively. Cisco Optical Site Manager device credentials saved for enrolled nodes are also stored with cryptographic protection.

Step 4 Select the access permissions from the list **Access Permissions***.

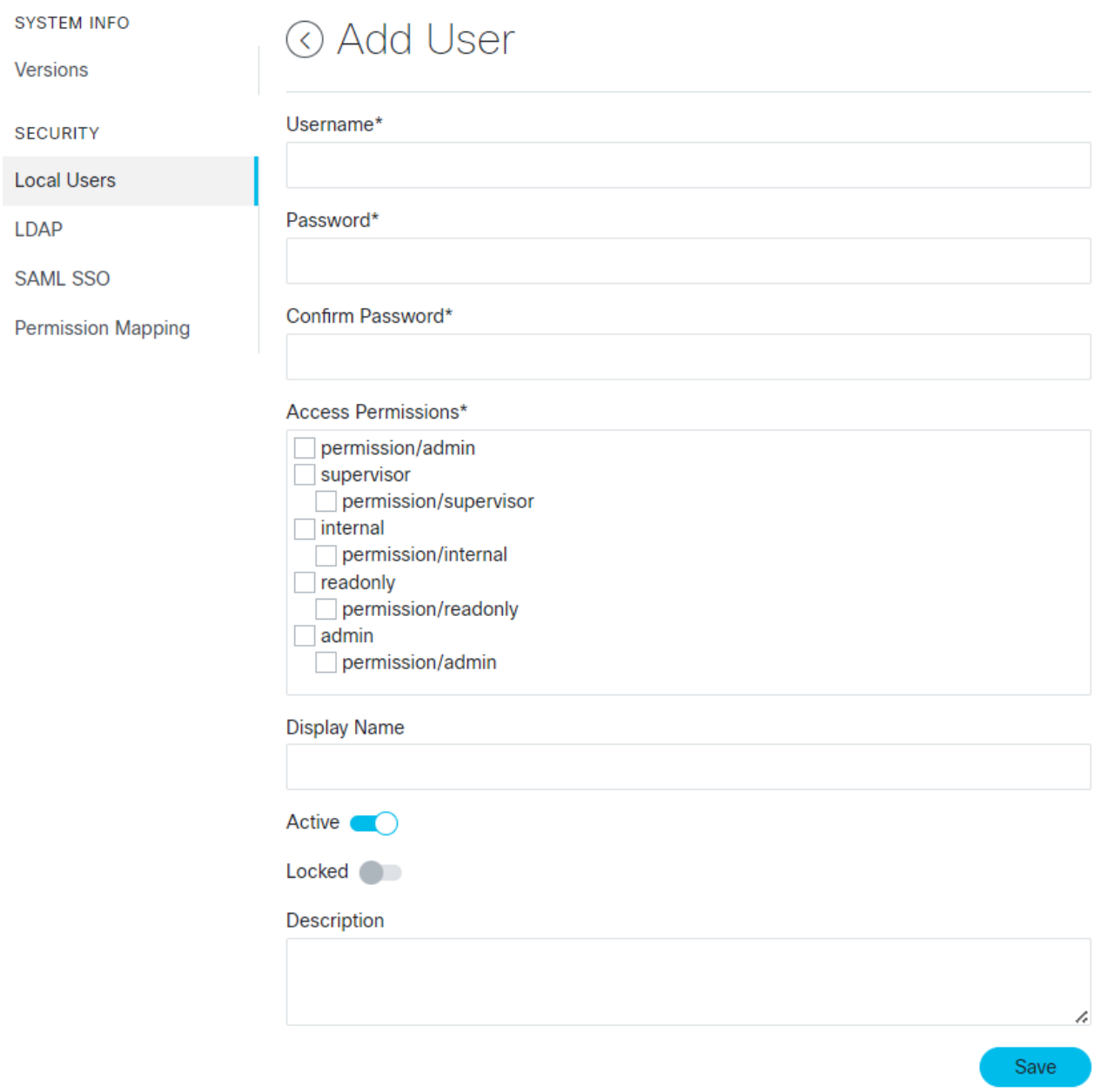
Figure 4: Local Users



For example *permission/<admin>*

Note
Description and **Display Name** are optional fields.

Figure 5: Add User



Step 5 Use the toggle switches to set the user status.

Note
The toggle switches are independent of each other, they can both be disabled or enabled at the same time.

- **Active enabled**: Allows the user to log into Cisco Optical Network Controller.
- **Active disabled**: Forbids the user from logging into Cisco Optical Network Controller.

- **Locked enabled**: Prevents deleting the user for auditing purposes or to retain historical data associated with that user.
- **Locked disabled**: Allows removal of the user

Table 3: Toggle combinations

Active status	Locked status	User status
Active enabled	Locked enabled	Prevents accidental deletion of user
Active enabled	Locked disabled	Allows user deletion
Active disabled	Locked disabled	Temporarily disables a user and allows user deletion
Active disabled	Locked enabled	Temporarily disables a user but prevent accidental deletion

Step 6 Click **Save**.

Cisco Optical Network Controller successfully saves the new user.

Set up authentication using LDAP

Set up user authentication using the Lightweight Directory Access Protocol (LDAP) on Cisco Optical Network Controller can be performed by following these instructions.

Before you begin

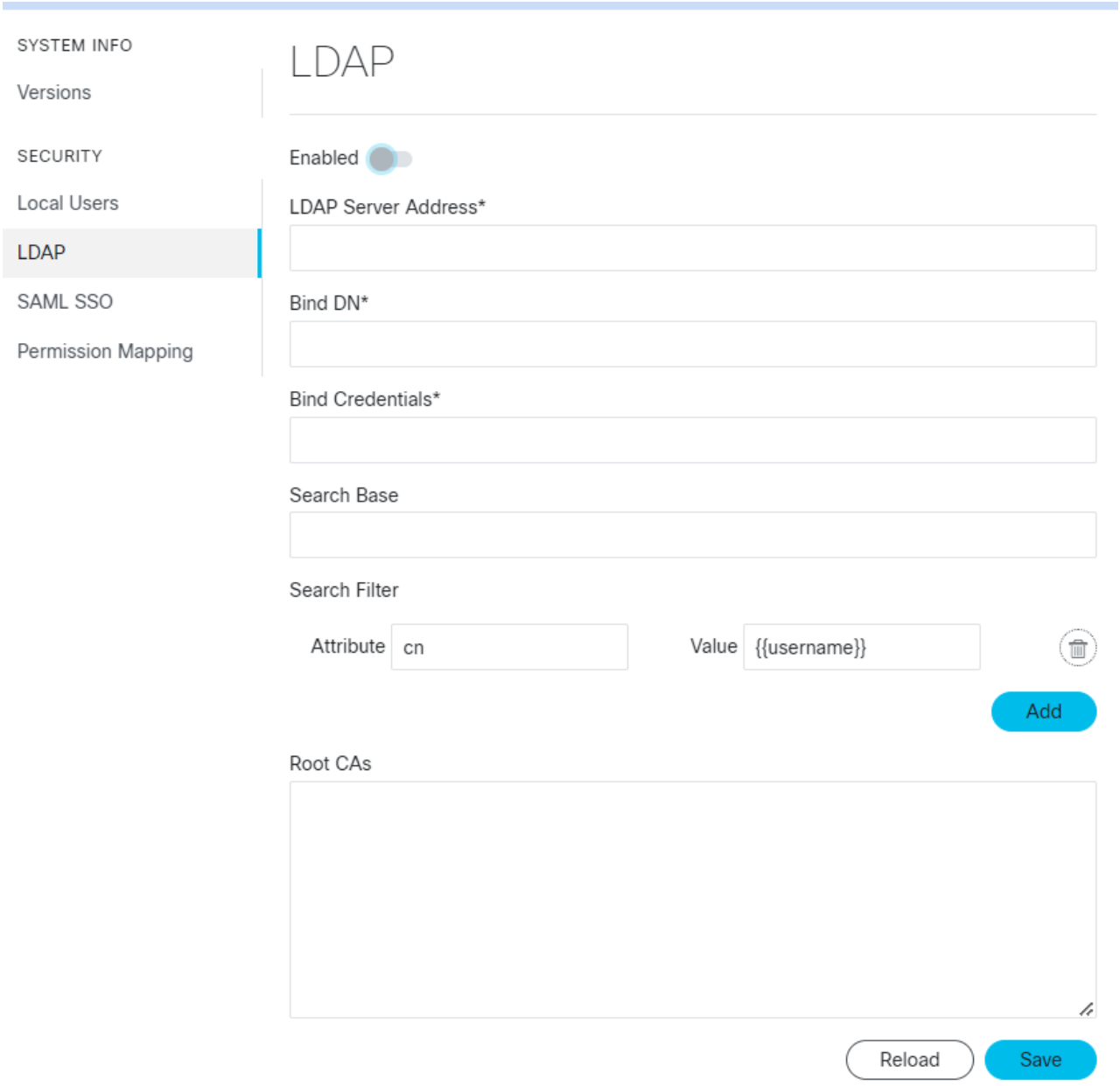
You need administrative user privileges to access Cisco Optical Network Controller.

Procedure

Step 1 From the Cisco Optical Network Controller home page click **Settings**.

Step 2 Click **LDAP**.

Figure 6: LDAP



Step 3 Enable **Enabled** toggle switch.

Step 4 Fill in the mandatory fields marked with an asterisk.

Table 4: Madatory LDAP fields

Field	Description	Value
LDAP Server Address	The IP address to your LDAP server.	This server address is set by your organization's LDAP administrator.

Field	Description	Value
Bind DN	The Distinguished Name of the user account used to connect to the LDAP directory.	This value is provided by your organization's LDAP administrator.
Bind Credentials	The password to authenticate your user account.	This value is provided by your organization's LDAP administrator.

LDAP Server Address, **Bind DN** and **Bind Credentials** are mandatory fields. The **Search Filter**, **Search Base** and **Root CAs** are optional fields.

Step 5 Click **Save**.

You have successfully completed the LDAP authentication setup.

Set up authentication using SAMLv2 SSO

The Security Assertion Markup Language (SAML) SSO allows you to gain single sign-on access based on the SAMLv2 protocol. Both local and external users can authenticate using SSO user credentials if their accounts are mapped.

Follow these instructions to set up SAML SSO authentication.

Before you begin

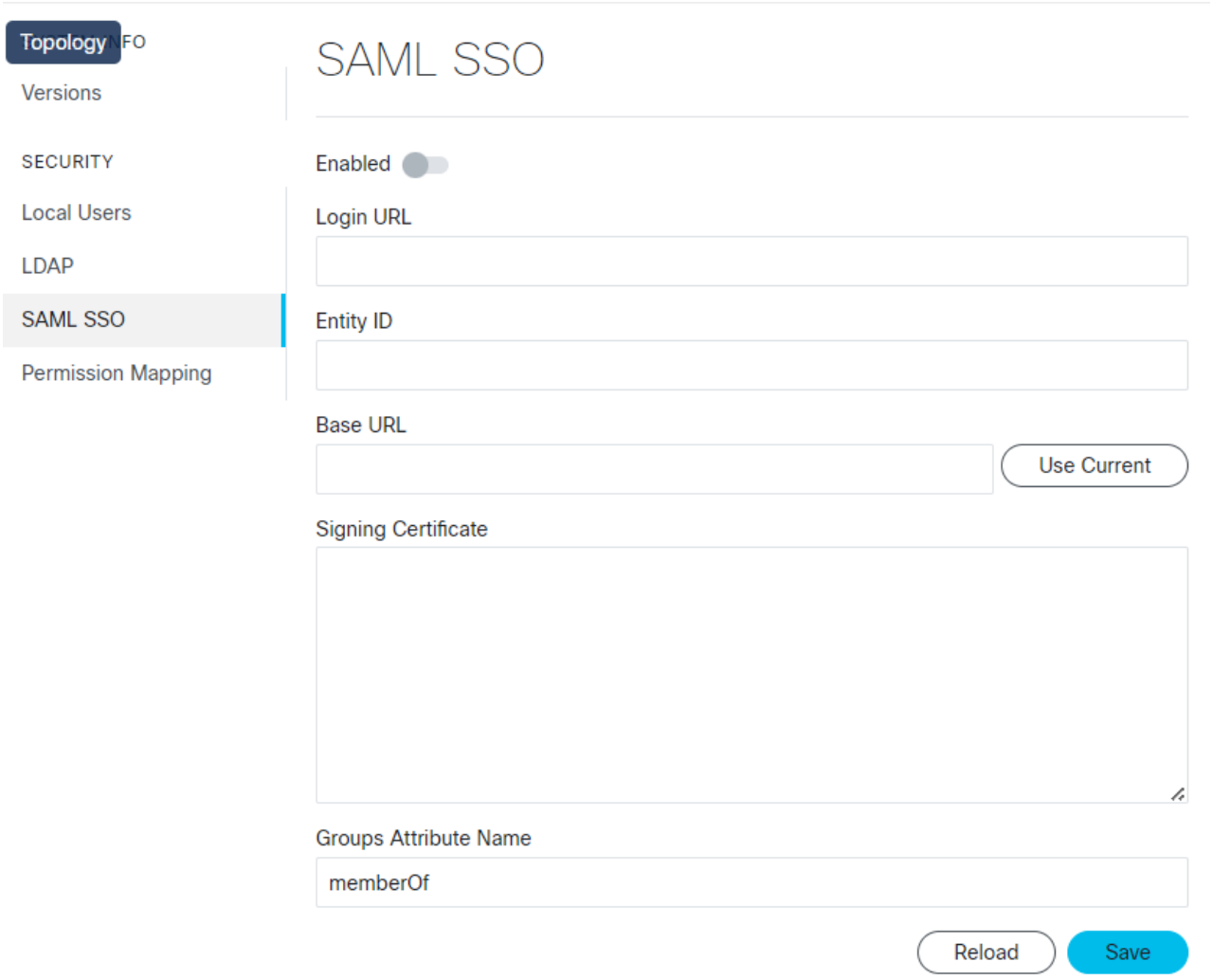
Ensure you have administrative user privileges to access Cisco Optical Network Controller.

To set up authentication using SAMLv2 SSO, ensure your SSO server is installed and configured for the application.

Procedure

Step 1 From the Cisco Optical Network Controller UI click **Settings** and select **SAML SSO**.

Figure 7: SAML SSO



Step 2 Enable **Enabled** toggle switch.

Step 3 Fill in the fields.

Table 5: SAML SSO fields

Field	Description	Value
Login URL	Sign on URL for the Cisco ONC	Cisco ONC URL
Entity ID	A unique identifier for Cisco ONC within the SAML federation, provided by your Identity Provider.	This value is provided by your organization's SSO administrator or identity provider (IdP)

Field	Description	Value
Base URL	Click **Use Current** to use the current URL.	Current URL
Signing Certificate	A downloaded certificate for Cisco ONC within the SAML federation, provided by your Identity Provider.	This value is provided by your organization's SSO administrator or identity provider (IdP)
Groups Attribute Name	Name of the group attribute that is assigned to you by your IdP.	memberOf

Step 4 Click **Save**.

You successfully completed the SAMLv2 SSO authentication setup.

Set up Permission Mapping

Cisco Optical Network Controller offers different permission levels for user access. Specific permissions can be granted to a user or group of users using this option. Follow these steps to set up permission mapping.

Before you begin

You need administrative user privileges to access Cisco Optical Network Controller.

Procedure

Step 1 From the Cisco Optical Network Controller home page click **Settings**.

Step 2 Select **Permission Mapping**.

Step 3 Click **Add**.

Step 4 In the **Add Permission Mapping** panel, choose one **Mapping Type** from the dropdown menu: **SAML User**, **SAML Group**, **LDAP User**, or **LDAP Group**.

Step 5 Fill the **Match** field.

For example, enter a specific username like 'jsmith' or a group name like 'network_admins' from your SAML/LDAP directory.

Step 6 Select the appropriate **Access Permission**.

Step 7 Click **Save**.

Figure 8: Permission Mapping

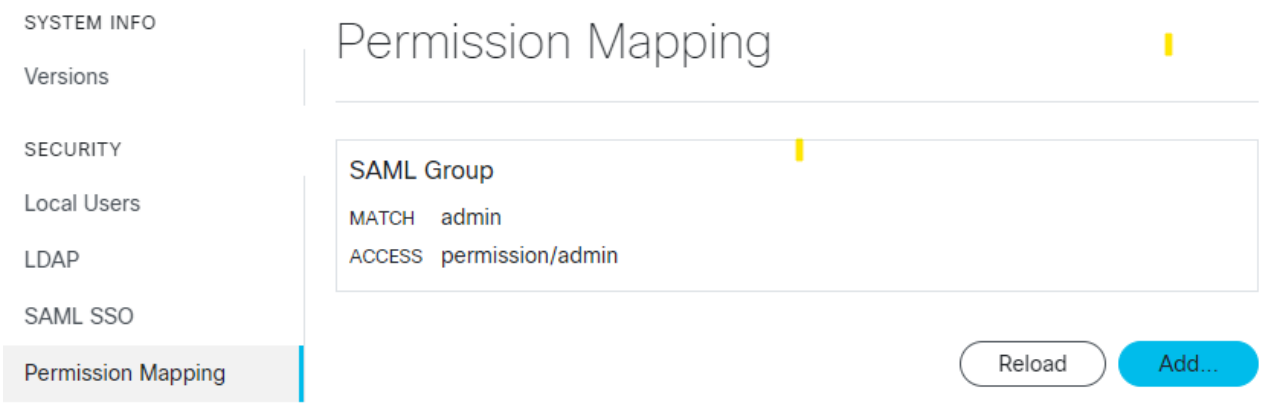
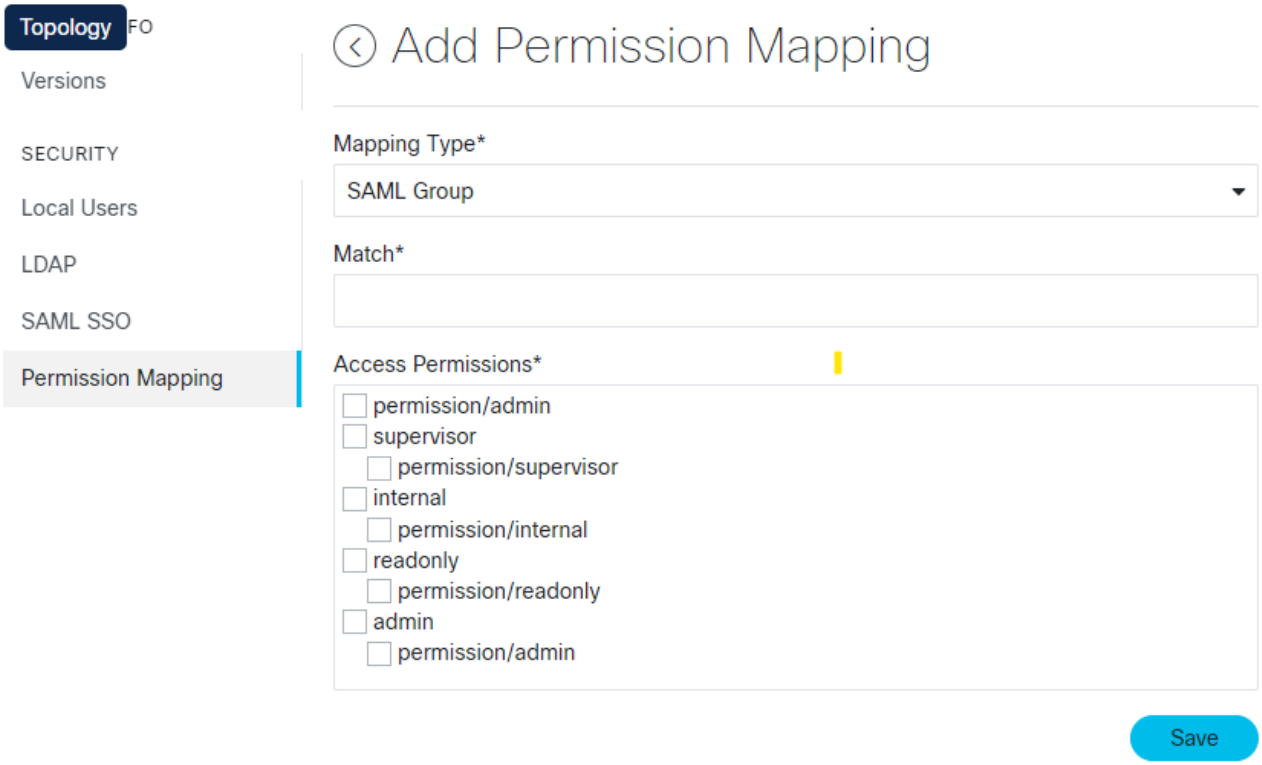


Figure 9: Add Permission Mapping



Manage Certificates in Cisco Optical Network Controller

When a Cisco Optical Network Controller cluster is created, unique self-signed EC/RSA certificates are generated for incoming HTTPS connections to the ingress-proxy. Ingress-proxy is the component that handles incoming network traffic and routes traffic to various services within the cluster. These certificates are intended for initial configuration only. From Cisco Optical Network Controller Release 24.3.1, you can create a Certificate Signing Request (CSR) and upload a signed certificate bundle using the sedo command-line interface (CLI) administration tool, a powerful tool for system administration.

Before you begin

This section requires advanced knowledge of certificate management, command-line interfaces, and security concepts.

Procedure

Step 1 Create a Certificate Signing Request (CSR) using the sedo CLI tool. You can choose between RSA and EC certificates.

Example:

For RSA:

```
sedo security certs request rsa --country <Country Name> --organization <Organization Name> <Domain
 Name or IP>
```

Example:

For EC:

```
sedo security certs request ec --country <Country Name> --organization <Organization Name> <Domain
Name or IP>
```

Step 2 Get the CSR Signed by a Certificate Authority (CA).

This is an external process. Submit the generated CSR to your organization's Certificate Authority (CA) or a trusted public CA to obtain a signed certificate.

Step 3 If your CA provides individual certificates instead of certificate chain, create a certificate chain. You must follow the exact order to create the chain. Copy the signed certificate to the CONC virtual machine location /data and create a chain of certificates in output.crt:

Example:

```
cat /data/signed_certificate.crt /path/to/issuing_ca_certificate.crt /path/to/root_ca_certificate.crt
 > /data/output.crt
```

Example:

Replace the paths with the actual paths to your Issuing CA and Root CA certificates. Ensure that the paths are accessible from the VM, and adjust the command as needed based on your specific environment and file paths.

Step 4 Upload the prepared certificate chain to the system:

Example:

```
sedo security certs upload output.crt
```

Step 5 Verify the uploaded certificates:

Example:

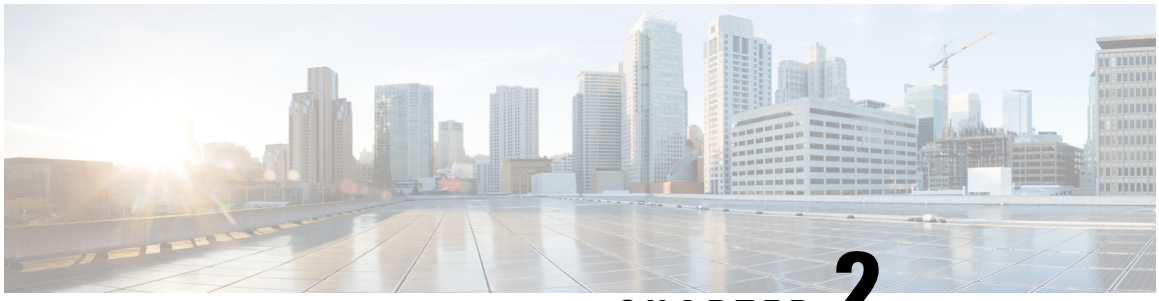
```
sedo security certs list

┌──────────────────────────────────────────────────────────────────────────┐
│ Installed Certificates
                              │
├──┬──────────────┬─────────────┬─────────┬─────────┬───┬───┬────────────────┤
│ TYPE │ SUBJECT                                    │ ISSUER                                    │ ISSUED
                       │ EXPIRES                      │ DNS SANS   │ IP SANS │ SERIAL NUMBER
                            │
├──┼──────────────┼─────────────┼─────────┼─────────┼───┼───┼────────────────┤
│ EC   │ CN=NextFusion,O=Cisco,ST=California,C=US │ CN=NextFusion,O=Cisco,ST=California,C=US │ Mon
Nov 18 22:46:18 GMT 2024 │ Thu Nov 18 22:46:18 GMT 2027 │ nxf.local │         │
1445557328950165706858003484413381754985522282604 │

│ RSA  │ CN=NextFusion,O=Cisco,ST=California,C=US │ CN=NextFusion,O=Cisco,ST=California,C=US │ Mon
Nov 18 22:46:18 GMT 2024 │ Thu Nov 18 22:46:18 GMT 2027 │ nxf.local │         │
1232594841637394522581611101986931324866857045143 │
└──┴──────────────┴─────────────┴─────────┴─────────┴───┴───┴────────────────┘
```

If you are replacing the self-signed certificate with the active `output.crt` (CA-signed chain certificate), ensure to delete any other certificates if only one certificate is being replaced. This helps avoid conflicts and ensure the system uses the newly uploaded, trusted certificate.

```
sedo security certs delete ec
```



CHAPTER 2

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, on page 3

Procedure

Step 1 View the timestamp.

The timestamp appears on the top right corner of the screen in all the screens. It follows the UTC time zone. The current date is displayed along with the time.

Step 2 Click the **Refresh** button to refresh the status of the table content or topology in each of the application screens anytime.

Step 3 Click the **Show or hide columns** icon display, hide, or reorder columns on any application page:

a) To display or hide a column from the table view, select or deselect the corresponding check box.

b) Click **Reset** to revert the view to its default settings.

Note
The position of the columns with a lock icon is fixed and cannot be changed. The preferences and changes remain saved until you reset them to default.

Step 4 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, on page 21
- Nodes, on page 28
- Alien Import, on page 41
- Network Inventory, on page 42
- Service Manager, on page 43
- Alarms, on page 73
- Workspaces, on page 87
- Software Image Management and Upgrade, on page 104
- PM History, on page 117
- Logs, on page 134

• Monitoring, on page 143
• Links, on page 144
• General Troubleshooting, on page 147
• Unmanaged Equipment Support, on page 148
• PSM OMS Protection, on page 150
• Forwarding Syslogs , on page 152
• Collect and download SEDO diagnostic files, on page 154

Topology

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

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

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

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

Layer segment buttons

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

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

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

Map control icons

Last time refreshed

Figure 10: Topology icons

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

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

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

Configurations icon: This icon provides these toggle switches.

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

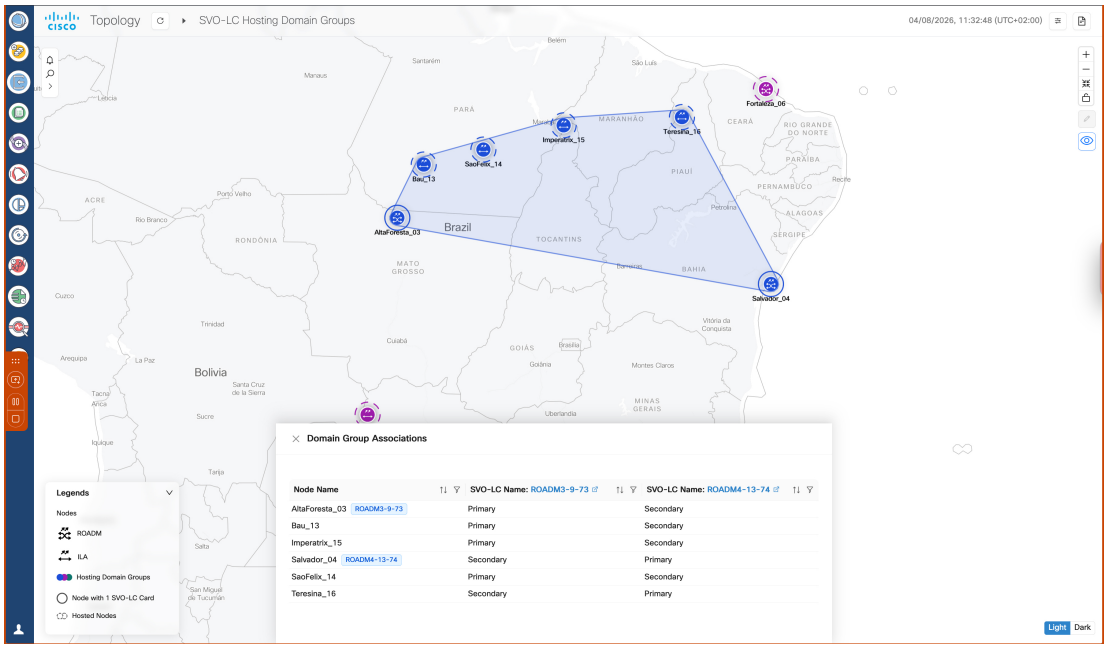
Documentation icon: Opens the Cisco Optical Network Controller configuration guide.

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

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

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

Figure 11: Domain Group Associations



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

Alarm severity bar

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

Table 6: 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.

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

Individual node pop-up options

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

1. Hover over a node and right click on it.

   The pop-up options appear.

2. Select of the options: **Resync**, **View in Node UI** and **View Alarms** options.

Table 7: 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.

Options	Description
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.

Figure 12: Topology Application

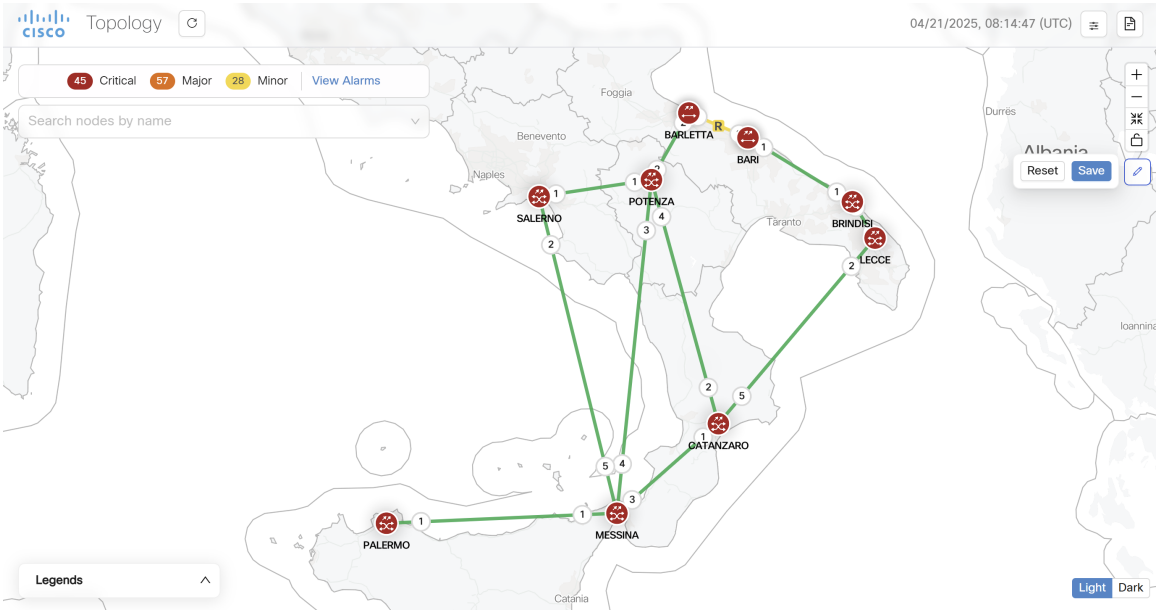


Figure 13: OTS view in Topology screen

Note

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

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

  - **Nodes**: The different nodes that are part of the network at any given time.
  - **Links**: The different links between nodes along with the amplifier and degree labels.
  - **States**: The different states like operational, critical alarms, link down and minor alarms.

- In the **Topology** map if two nodes have the same Geo location then they appear as a single node due to overlapping with each other which is a constraint.
- If any node in the **Topology** screen does not have a Geo location specified, the button in the upper right corner which is used to enter the Geo location value displays an orange highlight or dot. This orange dot is used to represent that there is at least one node which does not have any Geo location specified. When you click this orange dot a pop-up menu appears displaying all such nodes that are lacking Geo locations. Click the **Edit** icon and then select any node to move it to any desired location 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.

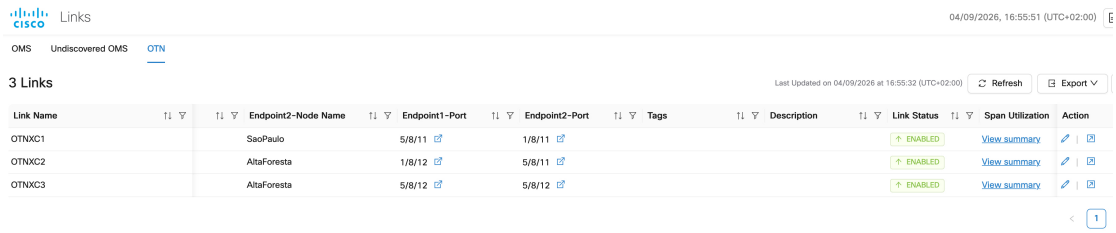
From Cisco Optical Network Controller 24.3.1 release onwards, fiber information and span loss details are added newly to the **Topology** live PM tool tip. When you click on the fiber span link in the map, you will see the following details appearing in the tool tip information:

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

Check span utilization summary for OTN links

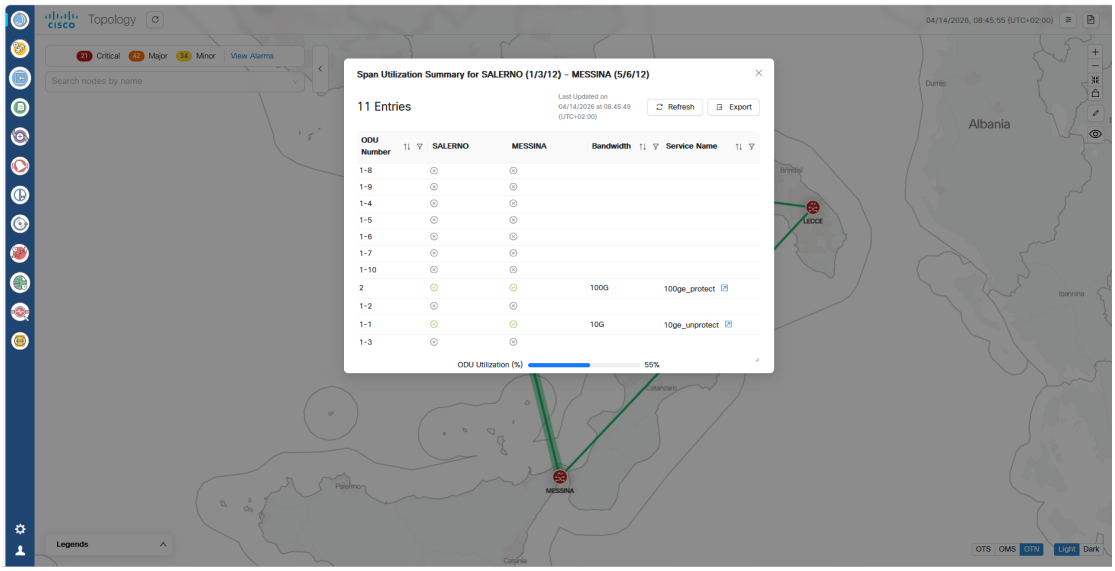
1. In the left panel, click the **Links** app.
2. Go to the **OTN** tab and click the required *OTN link*.

Figure 14: Links app



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

Figure 15: Span utilization summary in Topology screen



In this summary, these parameters appear:

Note

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

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

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

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

Figure 16: Topology Live PM

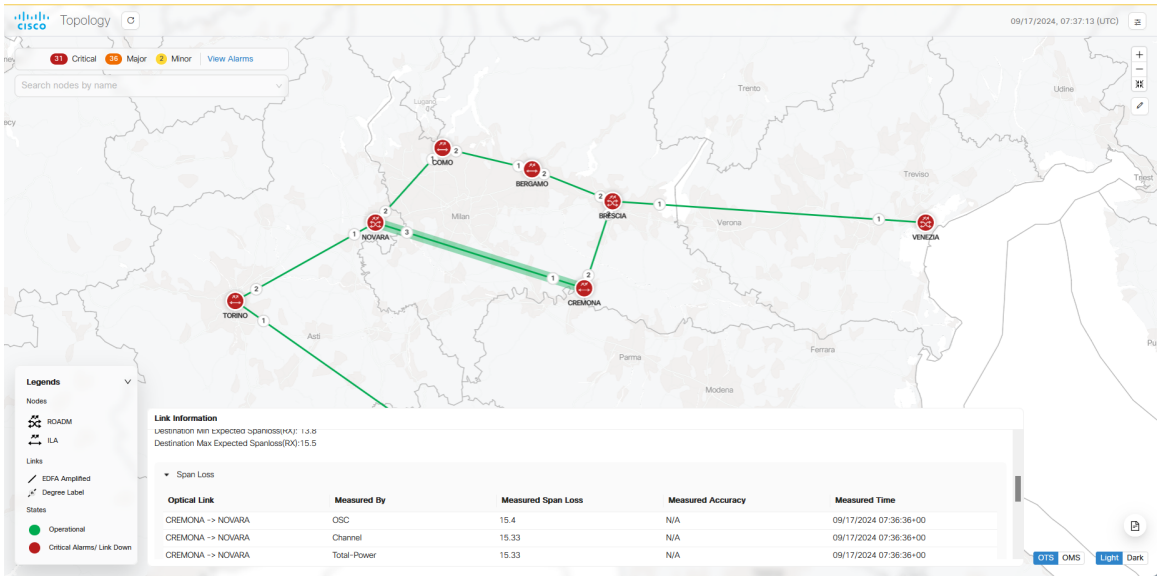
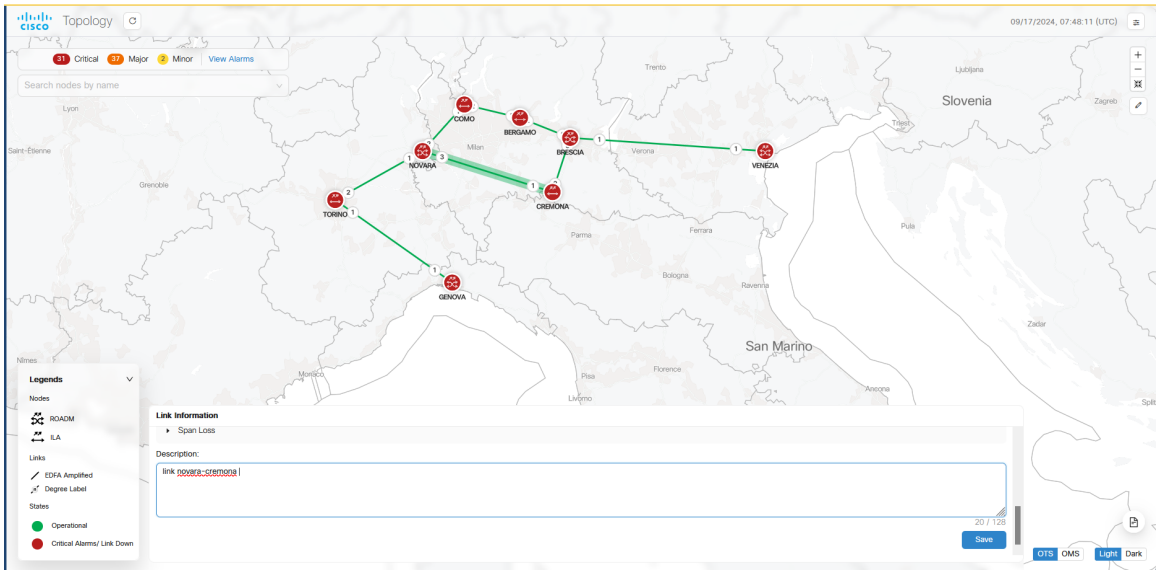


Figure 17: Tool Tip



Troubleshooting in Topology

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

- **A pop-up message**: Asking to reload the page appears in the following scenarios.

- New node onboarded or deleted
- Geo locations changed

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

Nodes

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

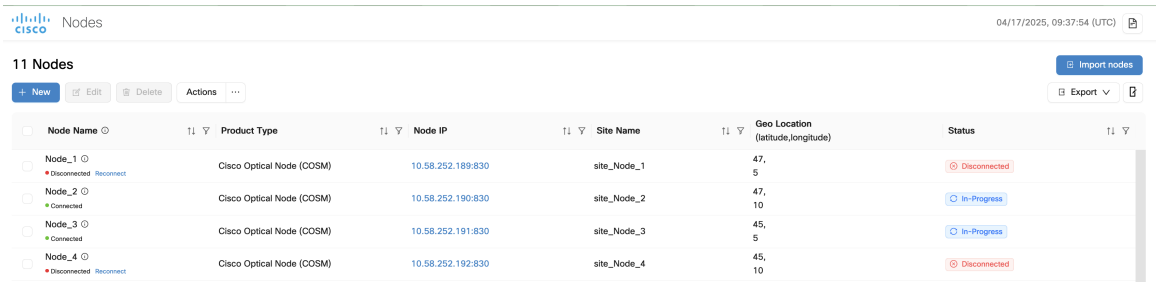
Use the **Nodes** screen to view the details of each node. The **Nodes** table displays the following details for each node:

- **Node Name**: The name of the node. The node name provided by you must match the original node name used in Cisco Optical Site Manager. In case of any mismatch or discrepancy issues, user given name is configured on Cisco Optical Site Manager.
- **Product Type**: The type of product the node belongs to. For example: Cisco Optical Site Manager.
- **IP: Port (NETCONF)**: The IP address of each node along with the port number.
- **Site Name**: The location of the site that each node belongs to. For example: ROADM_Site_Bengaluru_33
- **Geo Location**: The Geo location of each node in terms of the latitude and longitude values based on where exactly the node is situated in the world at any given time.
- **Status**: The status of each node within the network to know whether it is discovered or disconnected.

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

- **Site Description**: A brief description of the site associated with the node.
- **Message**: Displays information about any error conditions related to the node.
- **Created by**: Displays the user id that added the node.
- **Created Date**: Shows the date and time when the node was added.
- **Modified Date**: Shows the date and time when the node details were last updated.

Figure 18: Nodes



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

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

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

Figure 19: Actions

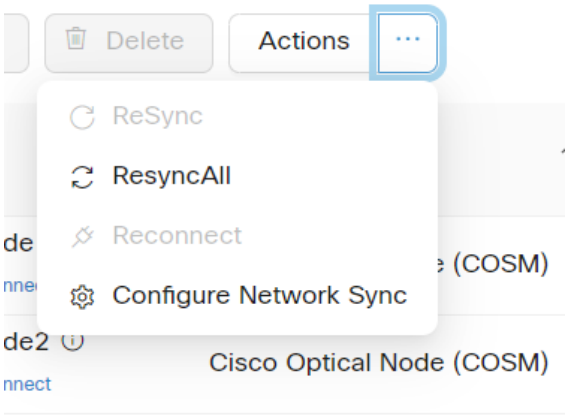
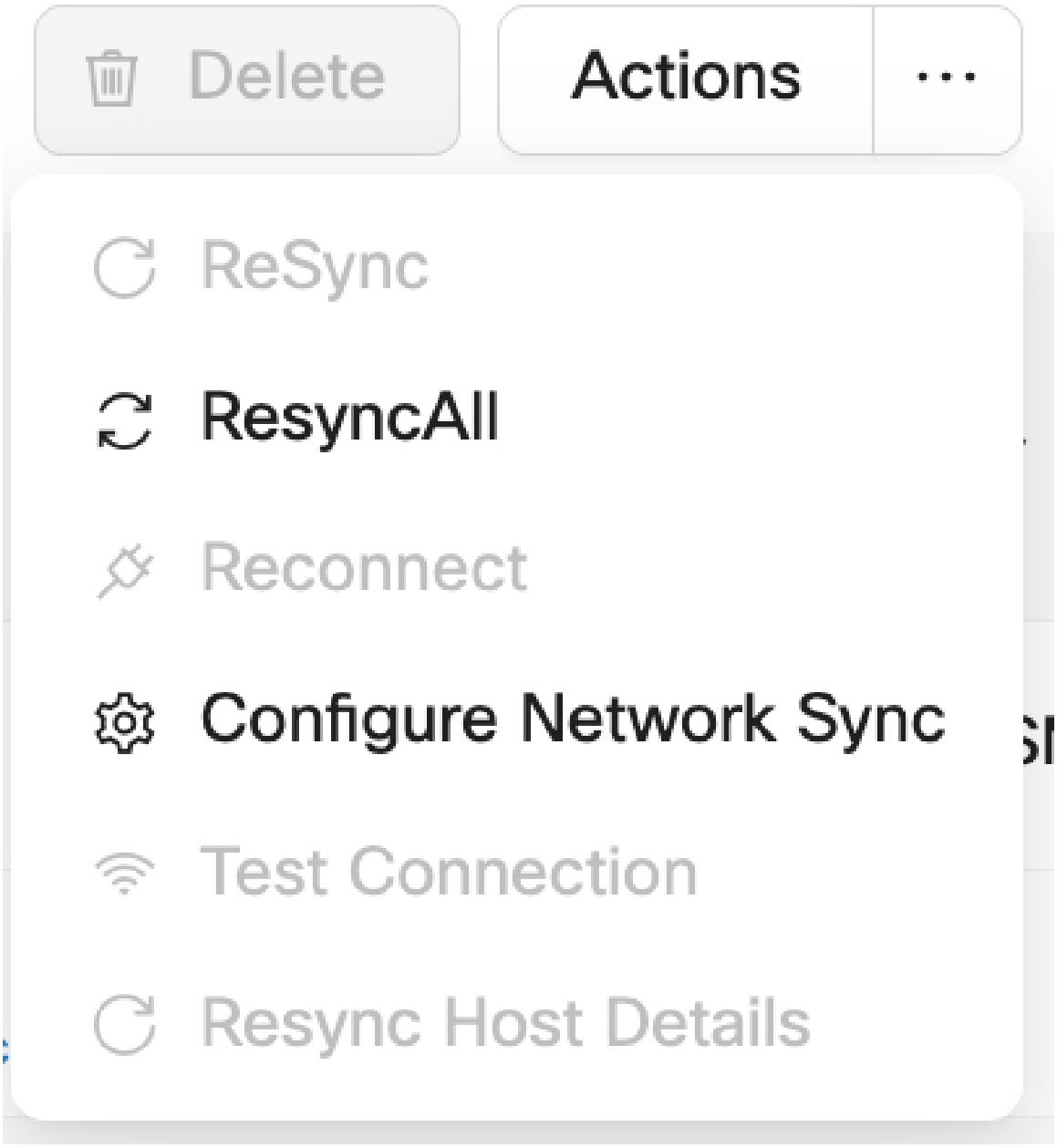


Figure 20: Actions



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 that are coming from Cisco Optical Site Manager in a pre-filled format has more than four digits, then the length of the Geo location value is truncated to only four digits.
- Node names are synchronized between Cisco Optical Network Controller and the nodes it manages. During onboarding, node name provided in Cisco Optical Network Controller is pushed to the node if the node has a different name. Changes made on Cisco Optical Site Manager is reverted as Cisco Optical Network Controller pushes the original name to Cisco Optical Site Manager.

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

Reserved internal IP addresses and subnets

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

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

- 10.241.x.x/24
- 10.242.x.x/24
- 10.243.x.0/24
- 10.91.0.0/16
- 10.92.0.0/16
- 10.93.0.0/16

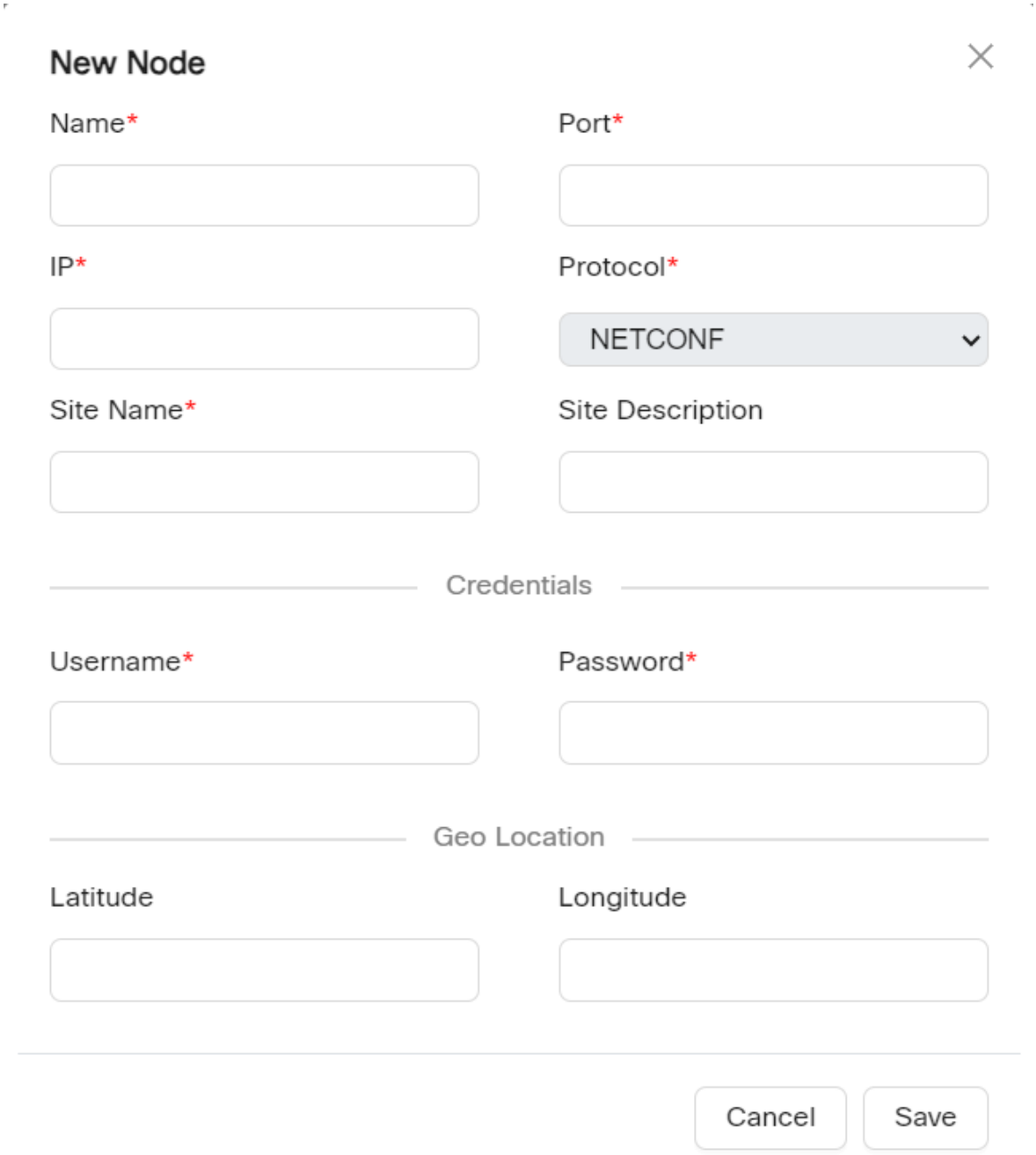
- 172.16.0.1/32

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

Add nodes on Cisco Optical Network Controller

Use this task to add a single Cisco Optical Site Manager node.

Figure 21: Add New Node



Before you begin

Verify these before addding to Cisco Optical Network Controller:

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

- NETCONF port is enabled on the Cisco Optical Site Manager. For more details, see Enable NETCONF over SSH.
- The COSM1K (NCS 1000 series) nodes must be added using port number 2022.
- All COSM2K (NCS 2000 series) nodes must be added using port number 830.
- You must add only fully configured nodes. All passives and patchcords must already be created before you add a node.

Procedure

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

Step 2 Click **New**.

Step 3 In the **New Node** dialog box, enter the details necessary connect to the node.

Ensure that you enter valid a username and password of the node to enable Cisco Optical Network Controller to connect to the node. For details about field descriptions, see the Table 8: Add new node field descriptions, on page 34 table.

Note
Use a Cisco Optical Site Manager administrator account to add and manage a Cisco Optical Site Manager node in Cisco Optical Network Controller. This account is required for onboarding and ongoing node operations, including performance monitoring collection, service provisioning and deletion, database backup and restore, and software download and activation. Other Cisco Optical Site Manager user roles are not supported for these operations.

Step 4 Click **Save**.
The new node is onboarded successfully and added to the **Nodes** table.

Cisco Optical Network Controller onboards the Cisco Optical Site Manager nodes.

Table 8: Add new node field descriptions

Field	Description	Mandatory
Node Name	Name of the new node you are adding. **Note** This name replaces the already configured Cisco Optical Site Manager node name.	Yes
Node IP	IP address of the new node which you are adding. **Note** Ensure that this IP does not overlap the Reserved internal IP addresses and subnets.	Yes

Field	Description	Mandatory
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 for accessing the new node.	Yes **Note** Use an administrator account to add and manage a Cisco Optical Site Manager node in Cisco Optical Network Controller. This account is required for onboarding and ongoing node operations, including performance monitoring collection, service provisioning and deletion, database backup and restore, and software download and activation. Other Cisco Optical Site Manager user roles are not supported for these operations.
Password	The password for accessing the new node.	Yes
Site Description	The description of the site to which the new node belongs.	No
Latitude	The Latitude co-ordinate value that you want to assign for the new node to set its location on the map.	No
Longitude	The Longitude co-ordinate value that you want to assign for the new node to set its location on the map.	No

Import multiple nodes into Cisco Optical Network Controller

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

Cisco Optical Network Controller onboards nodes in batches:

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

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

Procedure

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

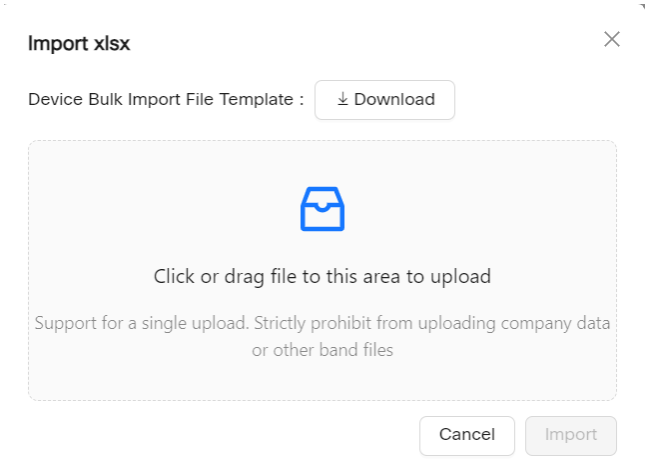
Step 2 Click **Import nodes** to import the nodes in bulk.

Step 3 Click **Dowload** to download the node bulk import file template.

Step 4 For each node you want to import, enter its information in the appropriate columns in the dowloaded Excel sheet.

Step 5 In the **Import xlsx** dialog box, select the Excel sheet.

Figure 22: Import nodes



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

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

Table 9: Bulk Import File Template

Name	Description
Node Name	Name of the node Cisco Optical Site Manager node. **Note** This name replaces the already configured Cisco Optical Site Manager node name.

Name	Description
Node IP	The IP address of the node you are adding. **Note** Ensure that this IP does not overlap the Reserved internal IP addresses and subnets.
User Name	The username for accessing the new node. **Note** Use an administrator account to add and manage a Cisco Optical Site Manager node in Cisco Optical Network Controller. This account is required for onboarding and ongoing node operations, including performance monitoring collection, service provisioning and deletion, database backup and restore, and software download and activation. Other Cisco Optical Site Manager user roles are not supported for these operations.
Password	The password for accessing the new node.
Connectivity Type	The type of the protocol used for connecting the node. Default: NETCONF
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	Set it as *Cisco Optical Node*.
Latitude	Specify the latitude co-ordinate value you want to assign to the new node to set its location on the map.
Longitude	Specify the longitude co-ordinate value you want to assign for the new node to set its location on the map.

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

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

What to do next

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

Export Nodes on Cisco Optical Network Controller

Before you begin

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

Procedure

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

Step 2 Click **Export** to export the details to a spreadsheet file.

Edit Nodes on Cisco Optical Network Controller

Before you begin

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

Procedure

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

Step 2 Click **EDIT** after selecting the node from the table.

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

Delete nodes on Cisco Optical Network Controller

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

This table describes circuit behavior when a node is deleted:

Table 10: Service behavior after node deletion

Circuit type	When the deleted node is...	Service behavior in Service Manager app
CPCE	A node through which the service passes.	Service is deleted.
	The terminal node of the service.	Service is deleted.
	A combination of terminal node and a node through which the service passes.	Service is deleted.

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

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

Procedure

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

Step 2 Select the node or nodes that you want to delete.

Step 3 Click **Delete**.

The selected node is deleted from the table.

Note

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

A warning message is displayed.

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

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

The selected nodes are deleted from Cisco Optical Network Controller.

Troubleshooting in Nodes

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

- **Bulk import failure**

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

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

- **Nodes possible status**

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

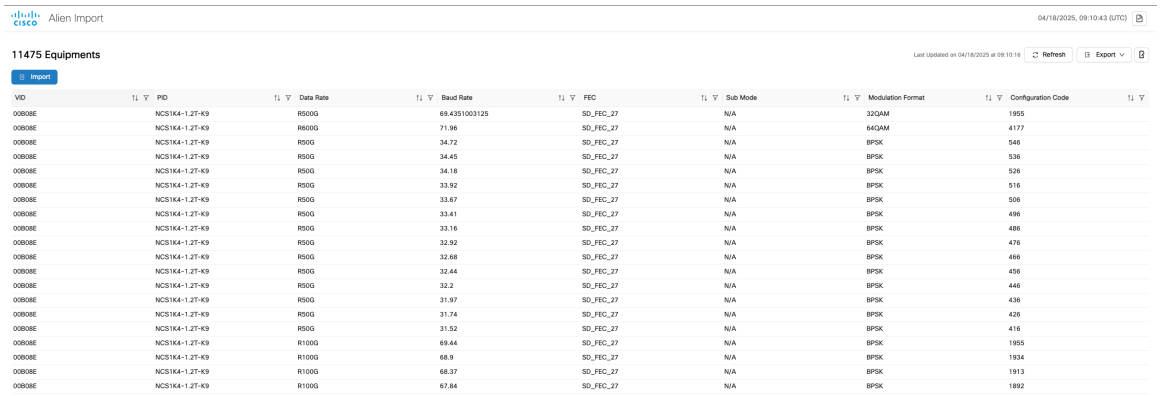
Alien Import

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 23: Alien Import



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.

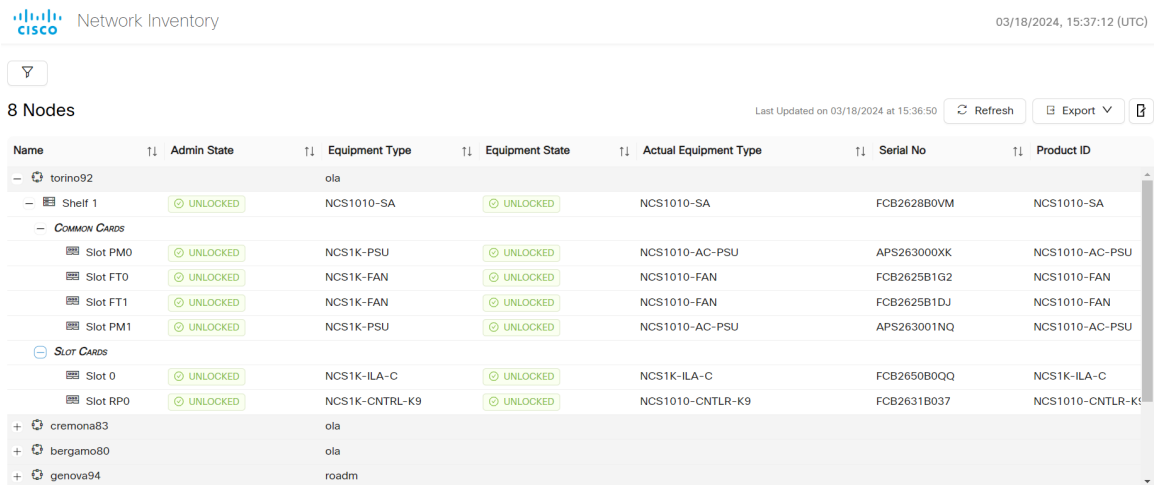
Step 6 Use the sort or filter options to sort and filter values in the table.

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 24: Network Inventory



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 25: Select multiple toggle

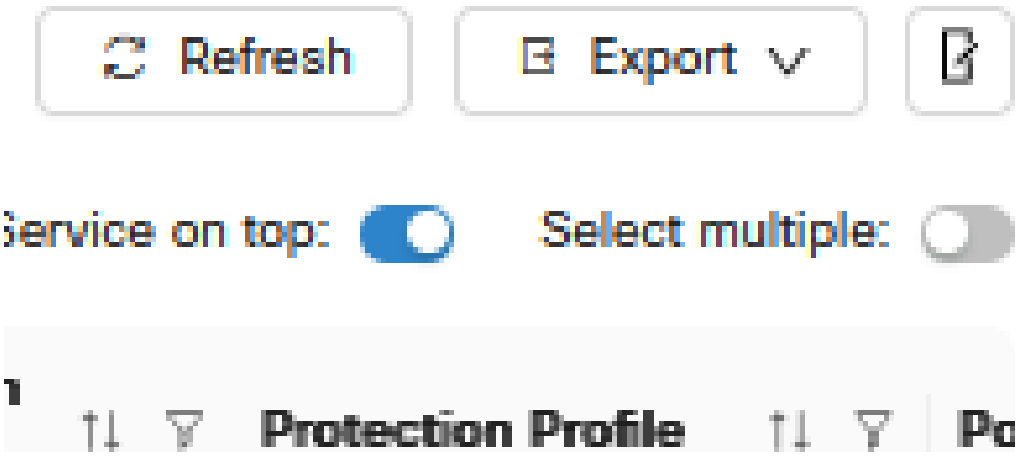
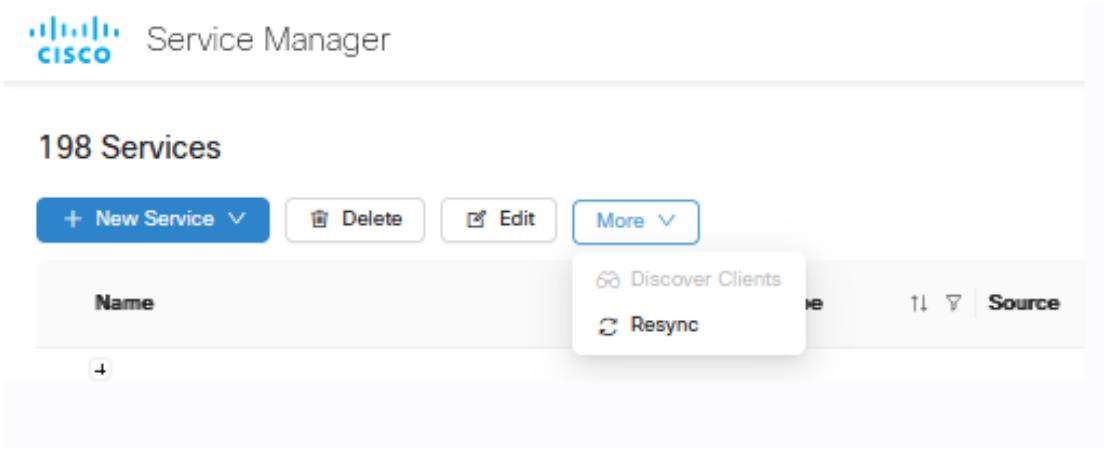


Figure 26: Resync option for GMPLS circuits

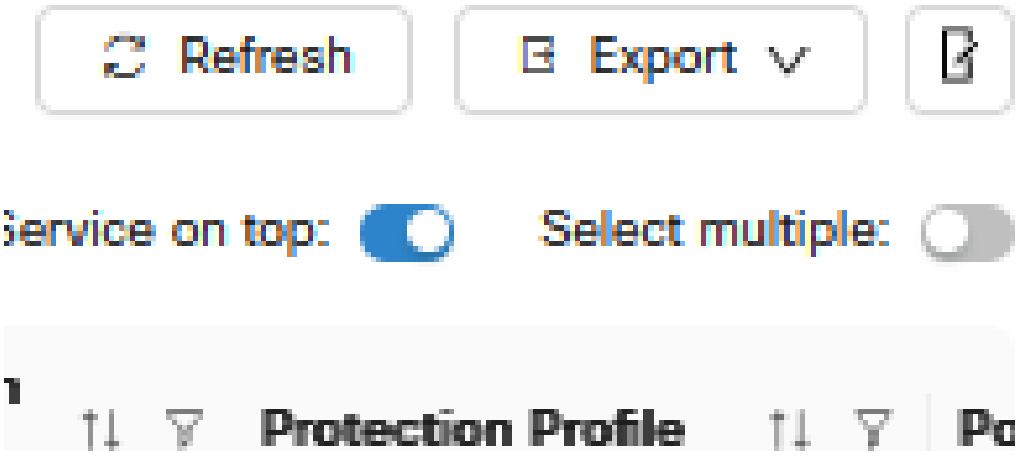


- Resyncing can resolve lifecycle state issues, for example, when the circuit is in PARTIAL, where clients are not discovered properly or are in an ambiguous state.
- When multiple services are selected, the **More** button is replaced with a **Resync** button.
- Resyncing a trail service also resyncs 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 27: 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 28: Service Manager

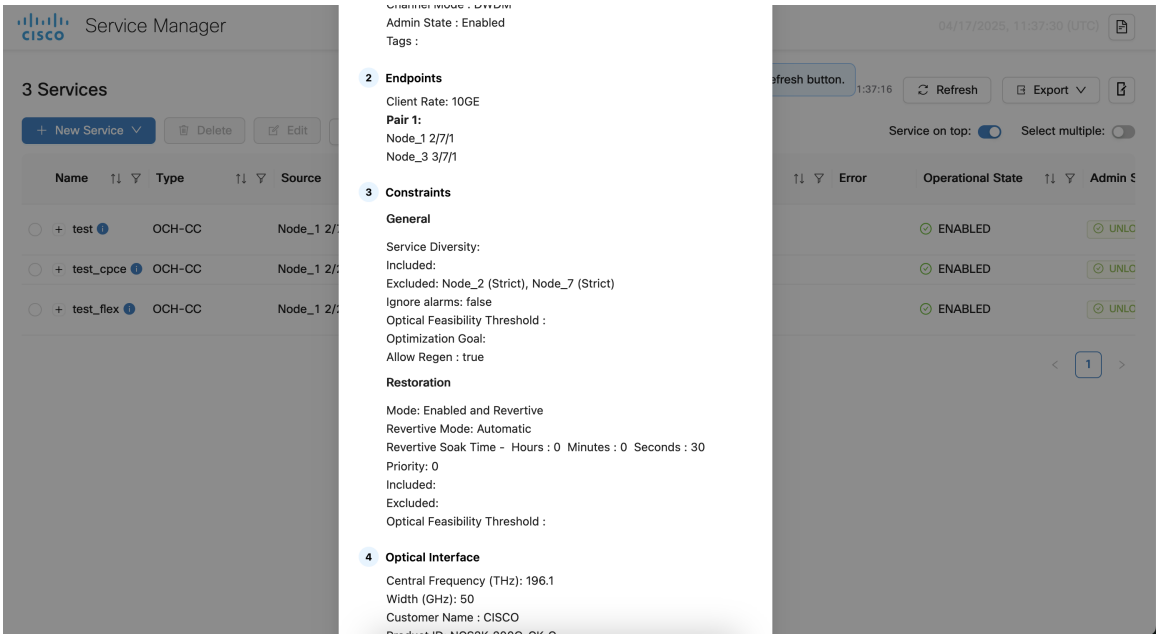
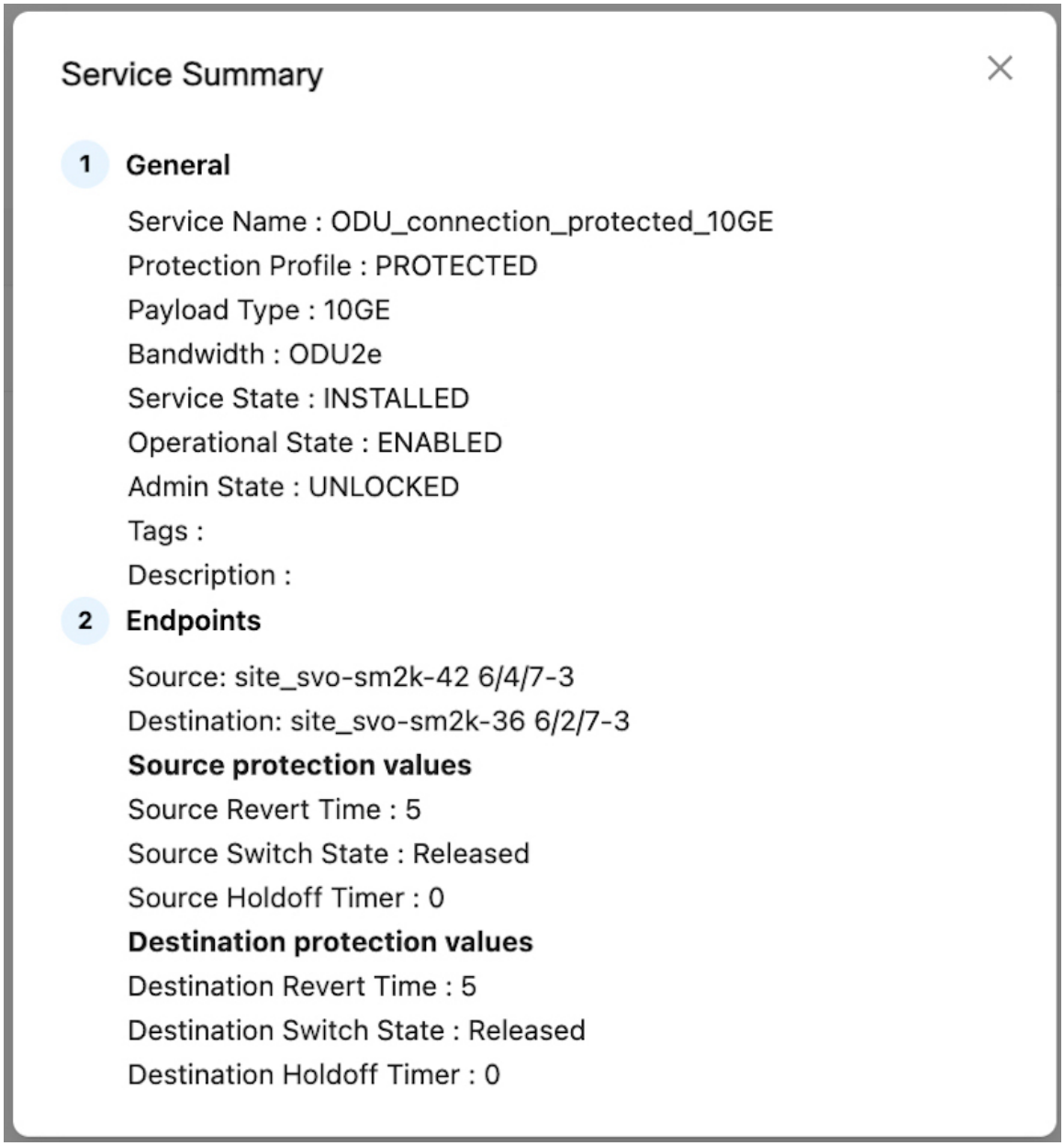


Figure 29: Service summary in service manager



Service manager table fields

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

Column	Values	Description
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.

Column	Values	Description
Operational State	ENABLED	The circuit is active and functioning normally.
	DISABLED	The circuit is inactive and not functioning.
Admin State	UNLOCKED	The circuit is administratively enabled and available for use.
	LOCKED	The circuit is administratively disabled and unavailable for use.
Frequency (THz)		Optical carrier frequency at which the circuit will operate within the DWDM spectrum.
Bandwidth (GHz)		Bandwidth used by the circuit
Protection profile	PROTECTED	OTN service has both active and standby path.
	UNPROTECTED	For OTN service, only active path is present. For PSM circuit, the circuit is configured with PSM OMS protection.
	Port Rate	10GE
40GE		
100GE		
400GE		
OTU2		
OTU2E		
OTU4		
OC192/ STM-64		
FC16		
FC32		
Discovery Date	—	Service discovery date

Data rate

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

Create and manage circuits

Consider these conditions when creating OCH-CC circuits.

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

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

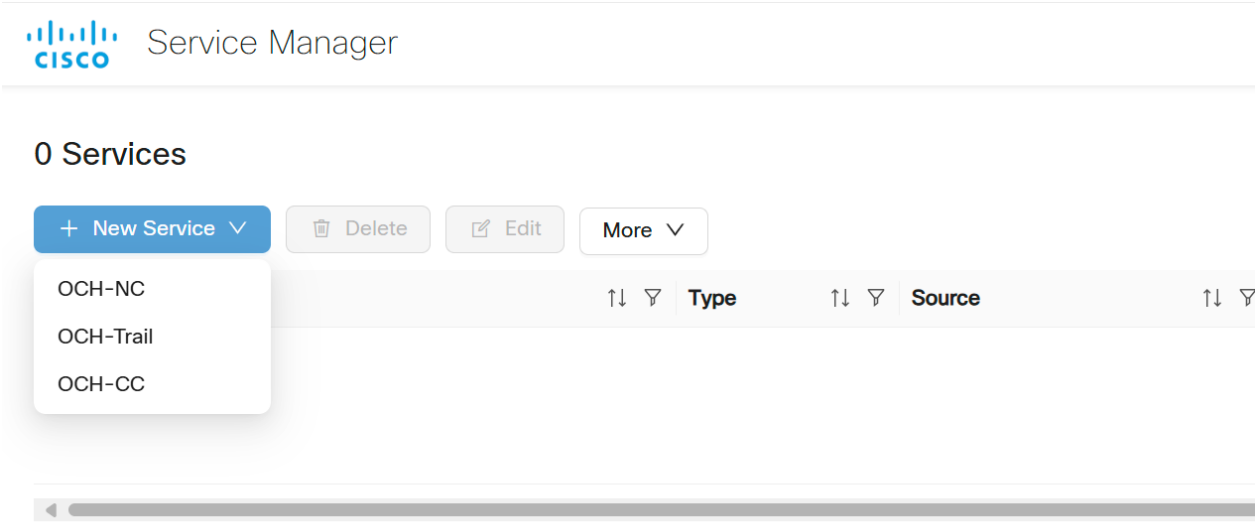
Before you begin

Note

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

Procedure

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

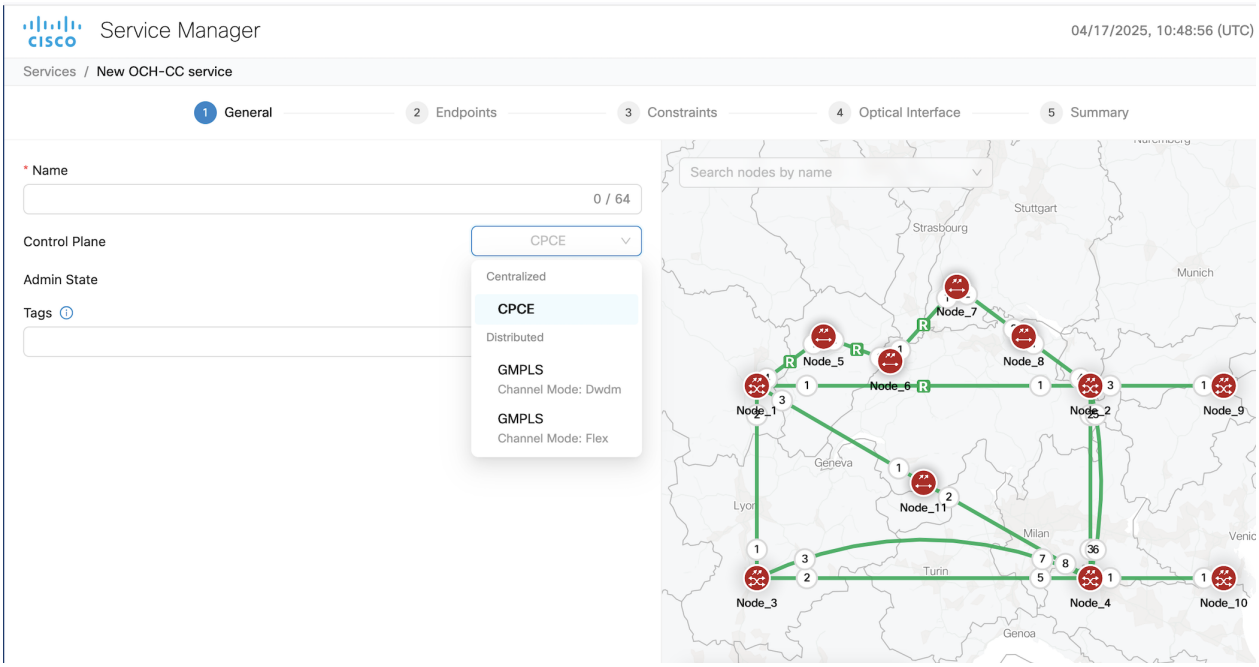


Step 2 Select **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

Note

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

Figure 30: Service Manager



Service Manager launches the new service wizard.

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

Figure 31: Service Manager

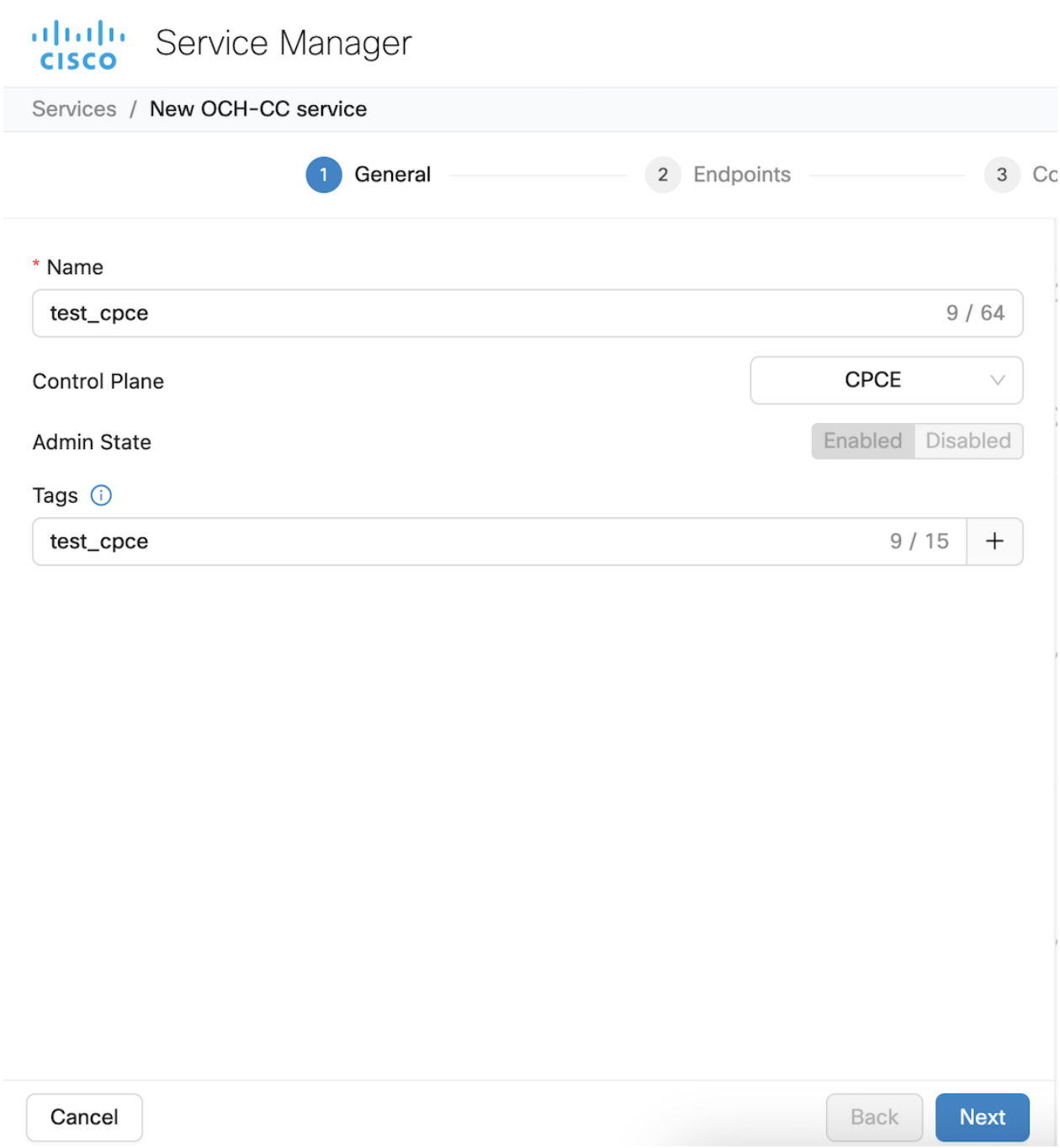


Table 11: General Parameters

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>).

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 32: Service Manager

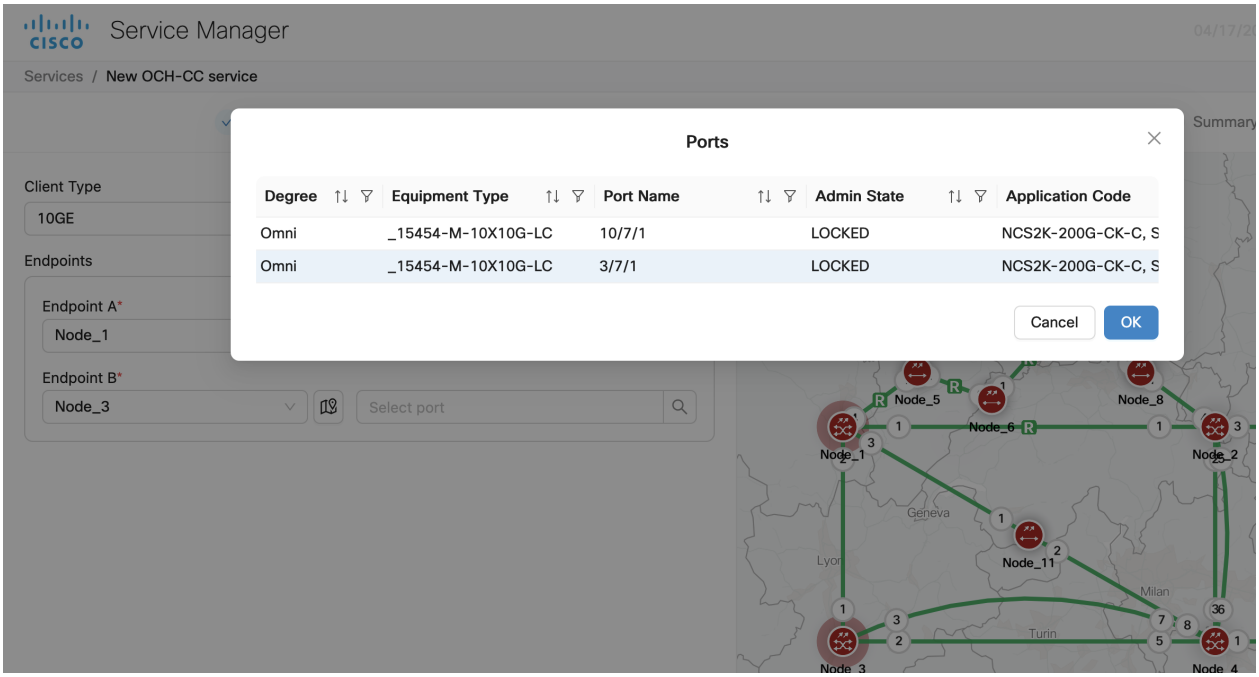


Table 12: Endpoints Parameters

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 33: Service Manager

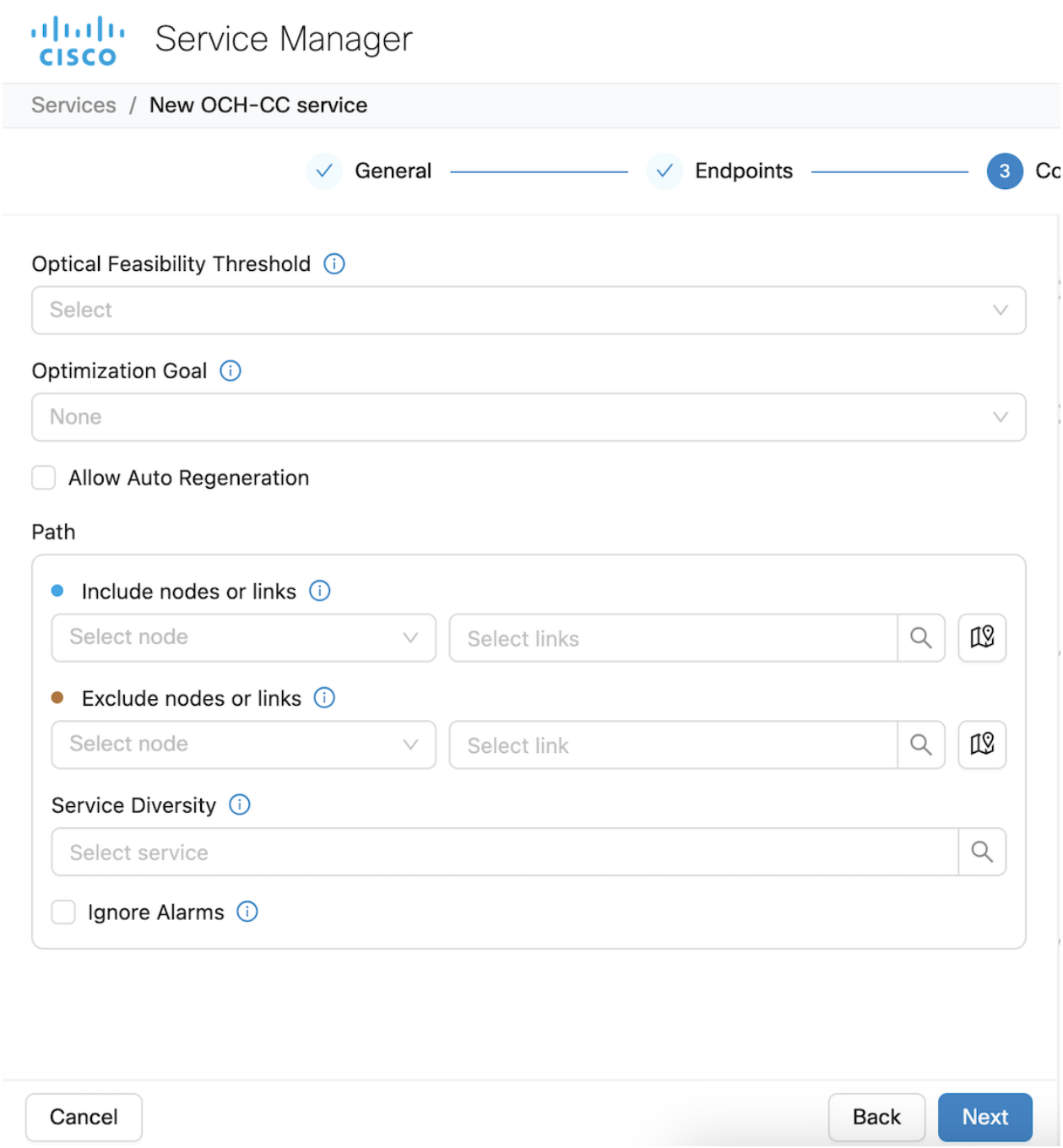


Table 13: Constraint parameters

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 14: 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.

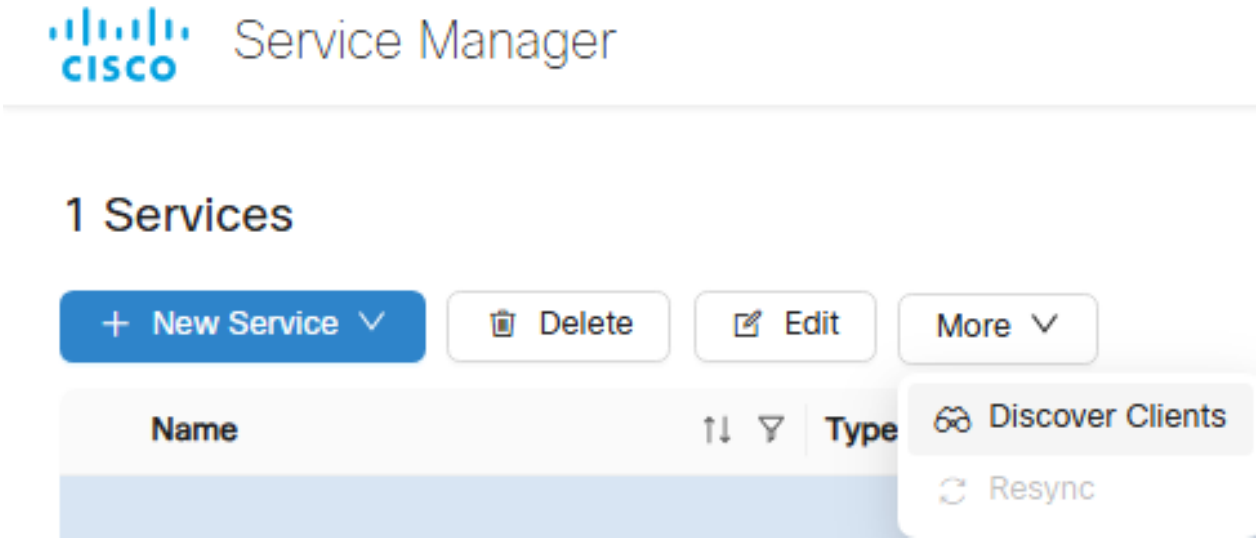
The newly provisioned circuit appears in the **Service List** table once the provisioning is complete. The **Lifecycle State** for the new circuit appears as **PLANNED** initially and later changes to **INSTALLED**.

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

a) Update the name.
b) Click **Save**.

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

Figure 34: Service Manager



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

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

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

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

Example

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

Table 15: 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

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
Cisco Optical Site Manager Node gets disconnected as soon as a service is provisioned in CONC	Config Failure	Delete the circuit and reprovision from the CONC.
Cisco Optical Site Manager nodes are in sync state during CONC provisioning.	Config Failure	Check the Cisco Optical Site Manager node and wait for synchronisation to complete.
NCS 1010 Devices under Cisco Optical Site Manager Nodes are locked	Config Failure	• Check Cisco Optical Site Manager and unlock the NCS 1010 device. • Verify Cisco Optical Site Manager synchronisation status to be completed.
Cisco Optical Site Manager node Restart during provisioning	Config Failure	Wait for CONC to re-establish the connection successfully after restart and its status moved to 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 Cisco Optical Site Manager Node. • Wait for CONC to reestablish the connection successfully with Cisco Optical Site Manager Node and its status moved to Discovery Completed.
Stale entries present in NCS 1010 while no cross connects present on Cisco Optical Site Manager Nodes	Config Failure	• Clear the NCS1010 stale entries. • Wait for Cisco Optical Site Manager node to complete the synchronisation.
Xcons Present in Cisco Optical Site Manager node along with NCS 1010	Config Failure	• Clear the XCONS on Cisco Optical Site Manager and NCS 1010. • Wait for Cisco Optical Site Manager 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 16: Supported transponder cards and modes

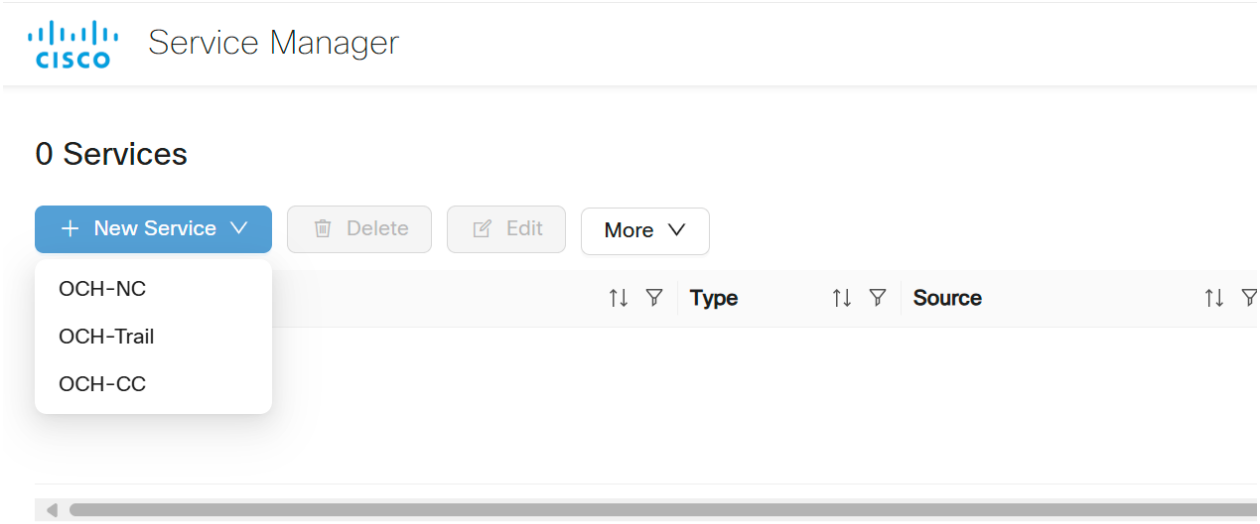
Card	Modes Supported
NCS1K4-2-QDD-C-K9	MXP-SLICE: 200G, 300G, 400G trunk and 100G and OTU4 client
NCS1K4-QXP-K9	MXP-SLICE: 400G trunk with 400G and 100G client
NCS1K4-OTN-XP	MXP: 4x100G TXP: 400G 400G trunk with 100G, 10G and OTU2 clients
NCS1K14-2.4T-X-K9	MXP-SLICE: 400G, 600G, 800G, 1T, 1.2T trunk 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 MXP with backplane connection to 15454-M-10X10G-LC with slice 2 configured as OPM-PEER-ODU2 or OPM-PEER-ODU2E
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/15454-M-100G-LC-C/15454-M-100G-ME-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients

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

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 35: Service Manager > General

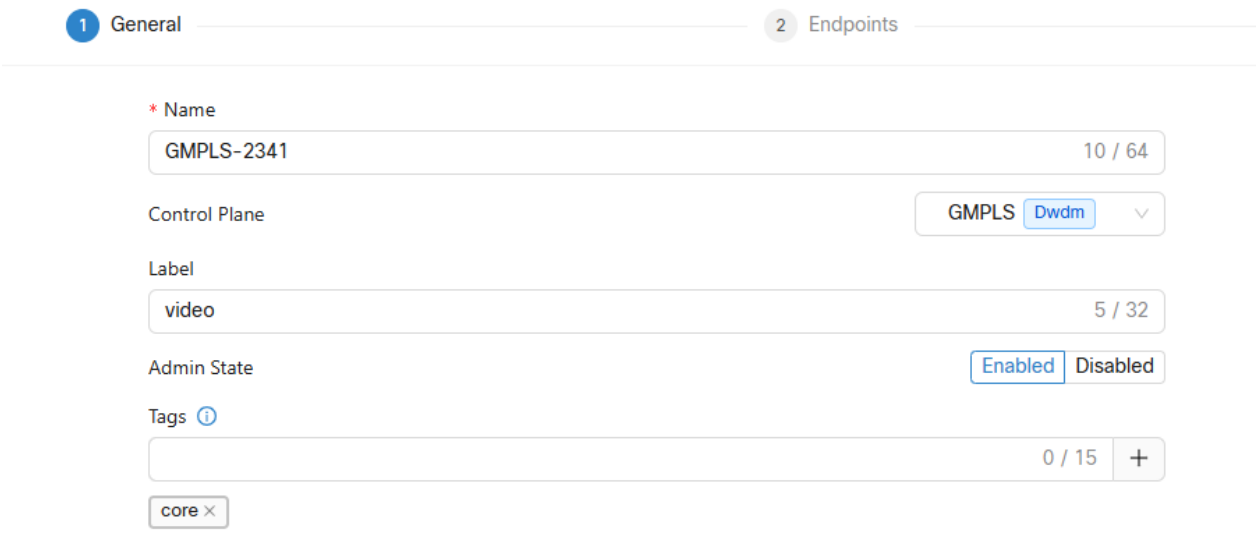


Table 17: General Parameters

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 a 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 36: Service Manager

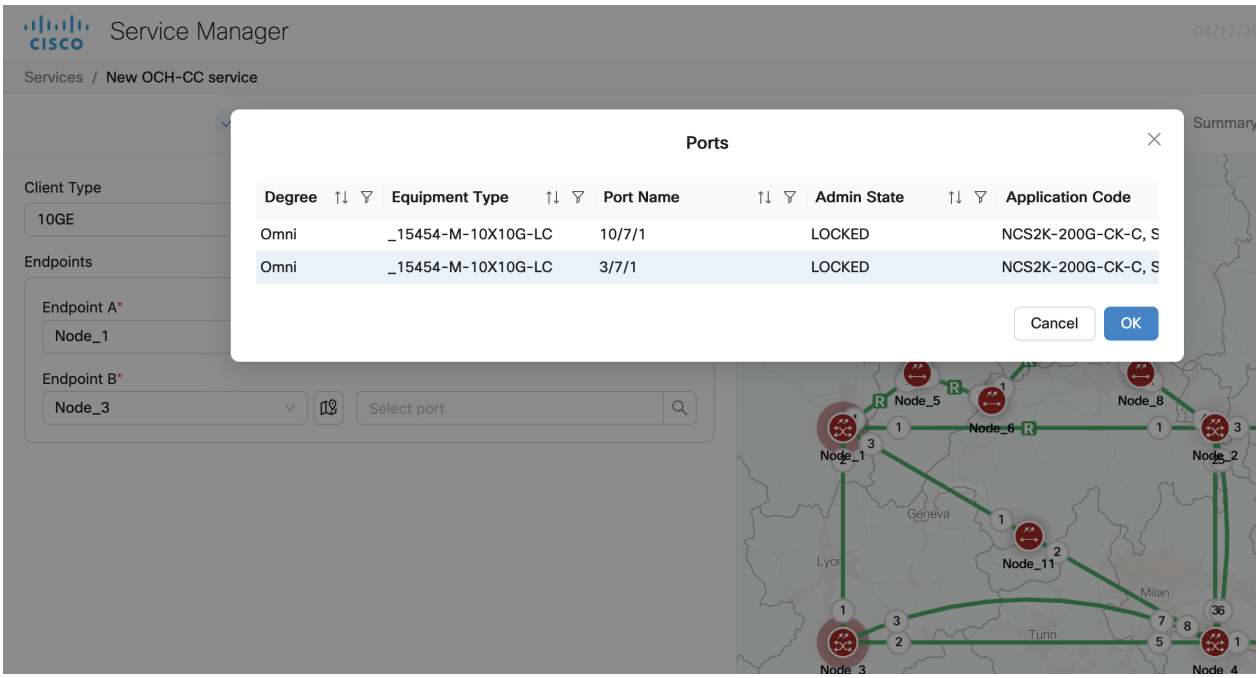


Table 18: Endpoints Parameters

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 37: Service Manager

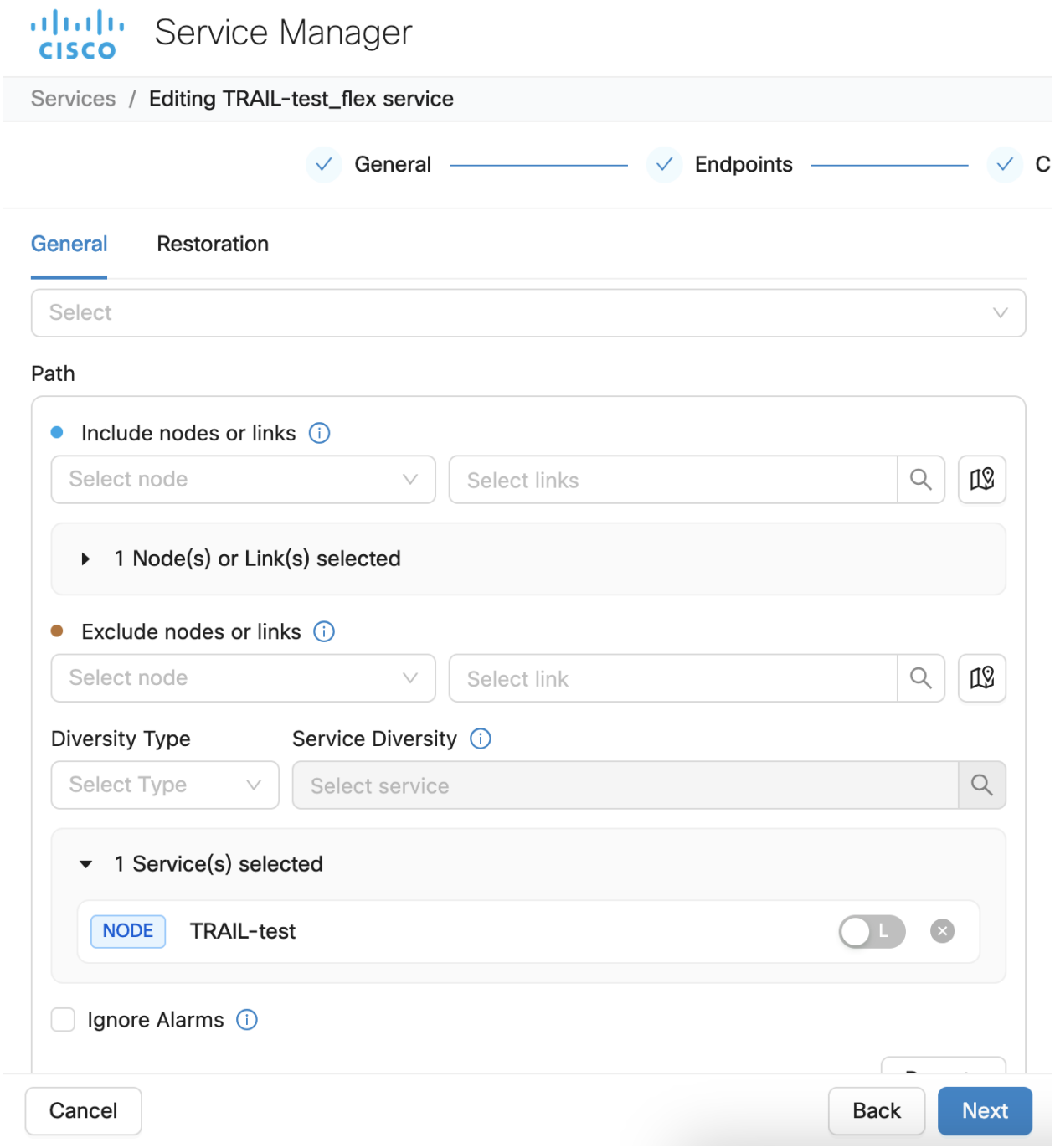


Table 19: General constraints field descriptions

Field	Description	Values/restrictions
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	Select RED, GREEN, YELLOW or ORANGE. GREEN = mean value YELLOW = +1 sigma ORANGE = +2 sigma RED = +3 sigma
Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	—
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	—
Diversity Type	Choose the type of service diversity	Node, link, or srlg
Service Diversity	Select one or more existing services from the dropdown for the control plane to exclude the resources that the services use during path computation.	—
Ignore Alarms	If true, Service manager ignores unverified alarms present on the path and continues to provision the service.	—

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

- If the node is selected as general regen node, it appears with a blue inverted teardrop **R** icon in the topology and **REGEN** icon in the **Detailed service path** tab of **Circuit Monitoring** application.
- If the node is a normal general node, it appears with a blue inverted teardrop **+** icon in the topology.

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

Figure 38: Service Manager > Constraints > Restoration

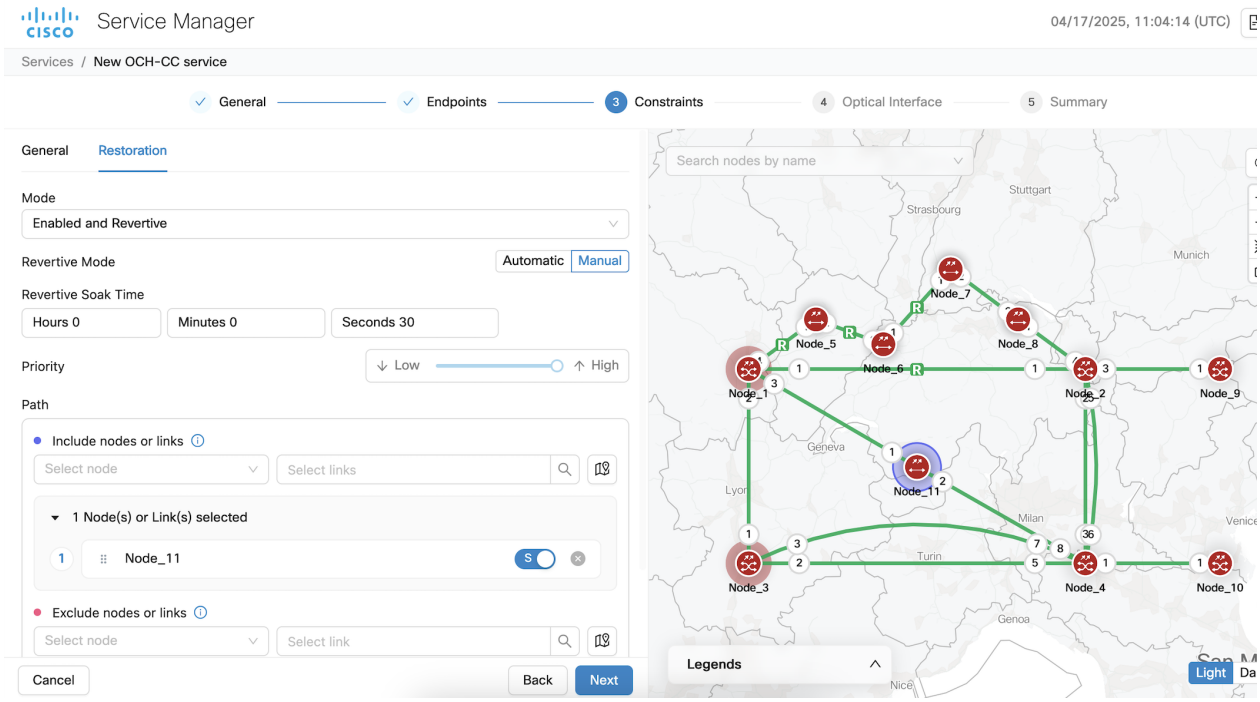


Table 20: Restoration constraints field descriptions

Field	Description	Values/restrictions
Mode	—	None, Enabled, Restorable Alternate, Enabled and Revertive
Revertive Mode	Specifies if the revert to main path after it up after a restoration should happen automatically or manually.	Automatic, Manual
Revertive Soak Time	Specifies the setup time for the restoration path. This parameter is only applicable for automatic restoration. It is the time in Hours, Minutes and Seconds for the network to switch to the restored path.	Up to 23 hours 59 minutes and 59 seconds
Priority	—	7—0 0 is the highest priority.
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.

- If the node is a normal restoration node, it appears with a purple inverted teardrop + icon in the topology.

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

Table 21: Optical interface parameters

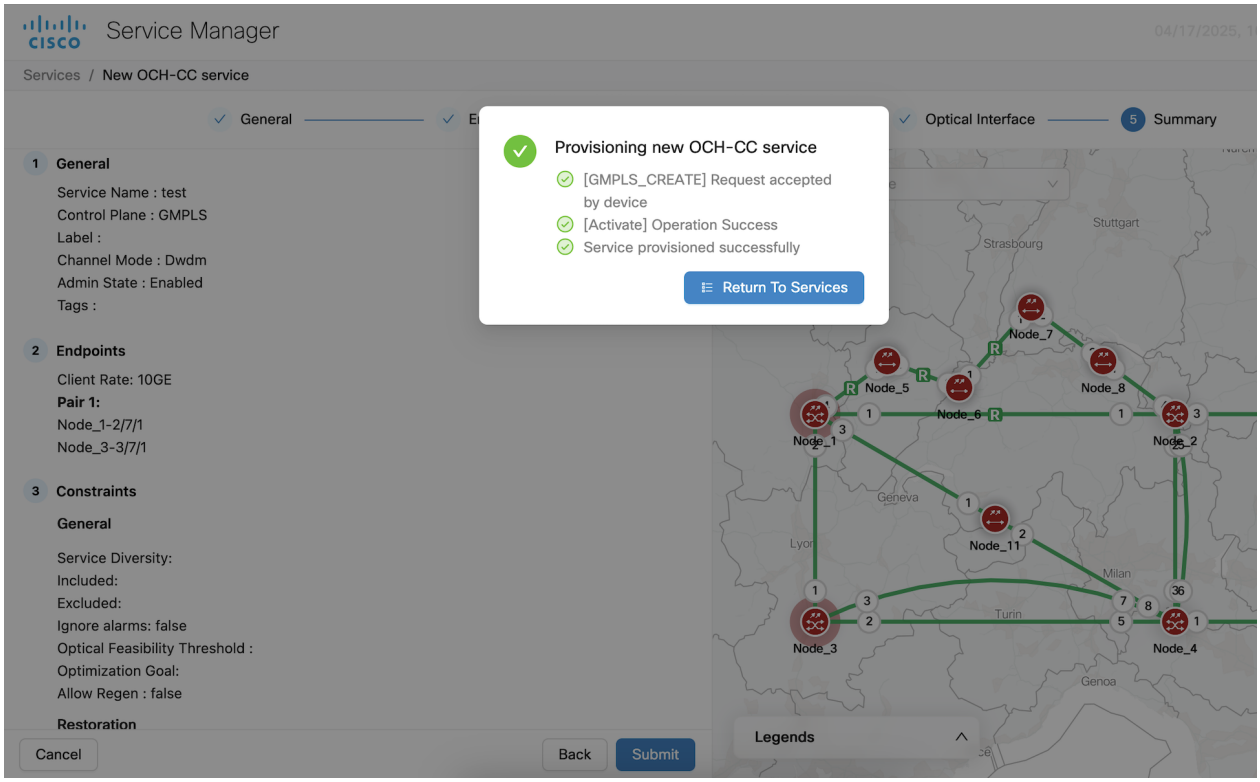
Field	Description
Wavelength	
Central Frequency (THz)	Choose a central frequency for the service.
Width	Bandwidth used by the circuit
Customer Name	The Customer name
Product ID	The product ID This is the Product ID of either the pluggable optics for the TXP card with pluggable trunk or the TXP card for 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 39: Service Manager



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 constraints 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 circuit path the main circuit path.

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

Clear unverified alarms from COSM before performing this step.

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

Figure 40: Service Manager > Optical Interface > Retune

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

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

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

The Lifecycle state changes to DELETION_IN_PROGRESS and then the service is removed from the service list when deletion is complete.

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

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

Table 22: 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.

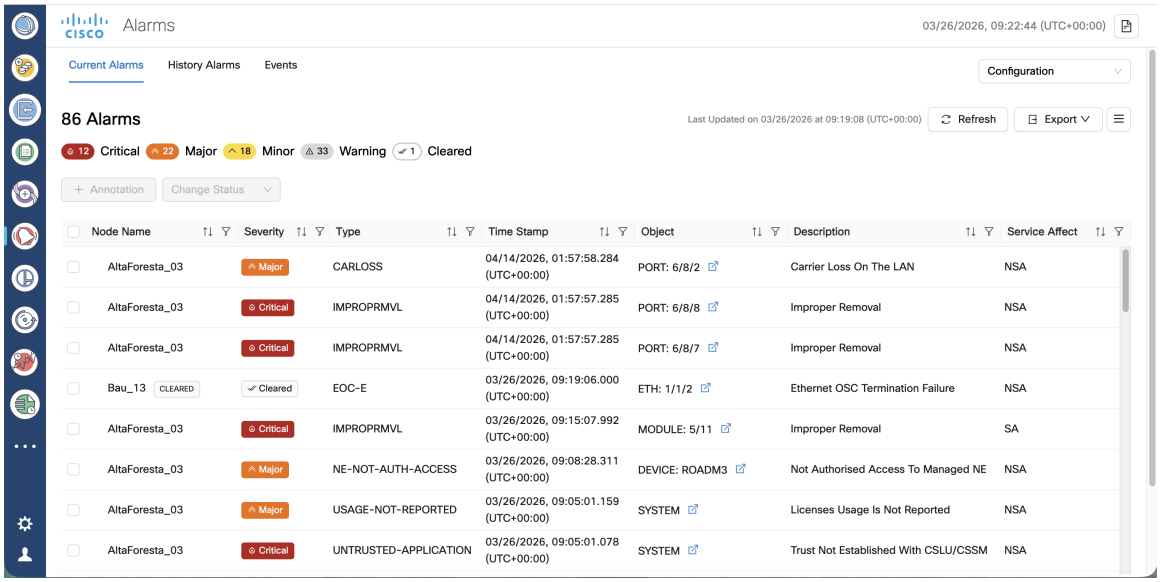
Error	Description
No client port available on trunk port	No available Client port matching the request constraints is found connected to the TXP Trunk port
No available optical path in node	No wavelength is available on the optical path.

Example

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 41: Alarms



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

Figure 42: Alarms History

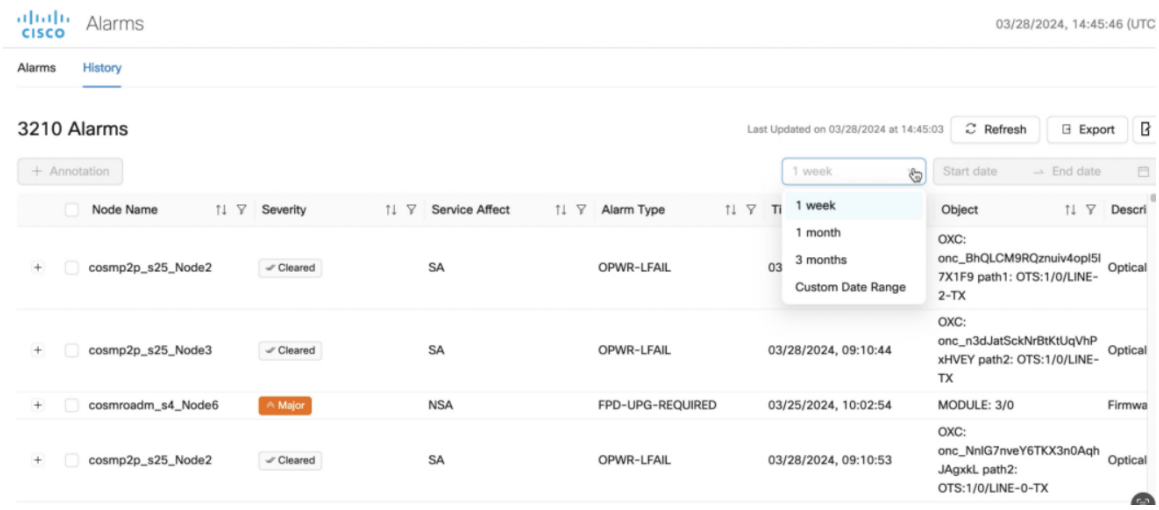


Table 23: Alarm table field descriptions

Field Name	Description	Example/Values
Node Name	The name of the node where the alarm originated.	Node identifier/name (e.g., NODE-001)
Severity	The severity level of the alarm.	Critical, Major, Minor, Warning, Cleared
Alarm Type	The type of alarm.	LOSP, NODE-DISCONNECT
Time Stamp	The date and time when the alarm was raised.	YYYY-MM-DD HH:MM:SS.SSS
Object	The object associated with the alarm.	NODE: Node_1, SYSTEM, CHASSIS: 5
Description	A detailed description of the alarm.	Text describing alarm details
Alarm Category	The category of the alarm. See 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,

Field Name	Description	Example/Values
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
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 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**.

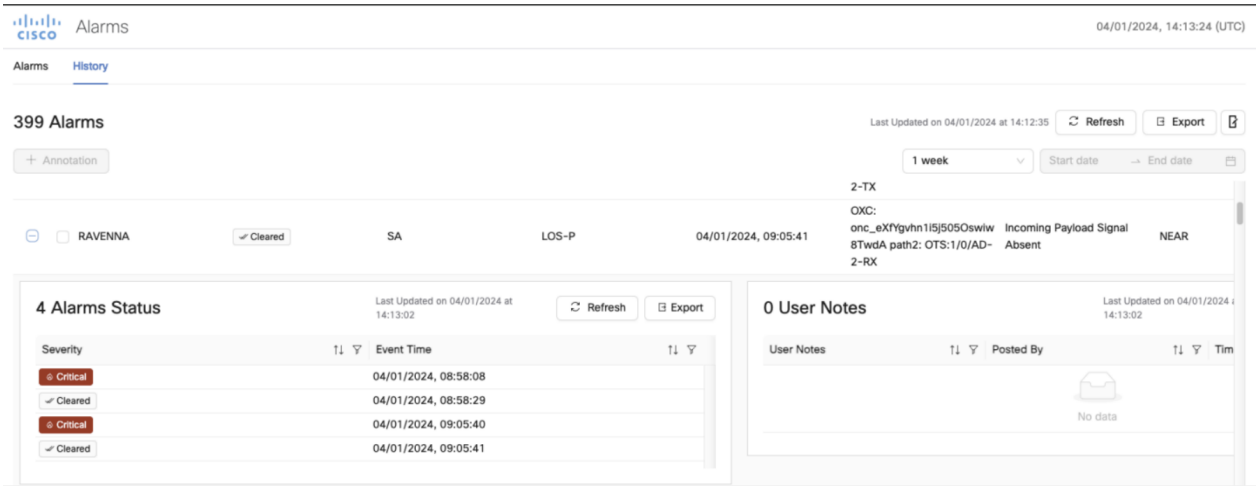
Note
You can add a user note to up to 500 alarms at once. You can add multiple notes to multiple alarms in the form of a list.

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 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 43: Alarm History Expanded View



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

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

Note

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

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

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

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

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

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

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

Note

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

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

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

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

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

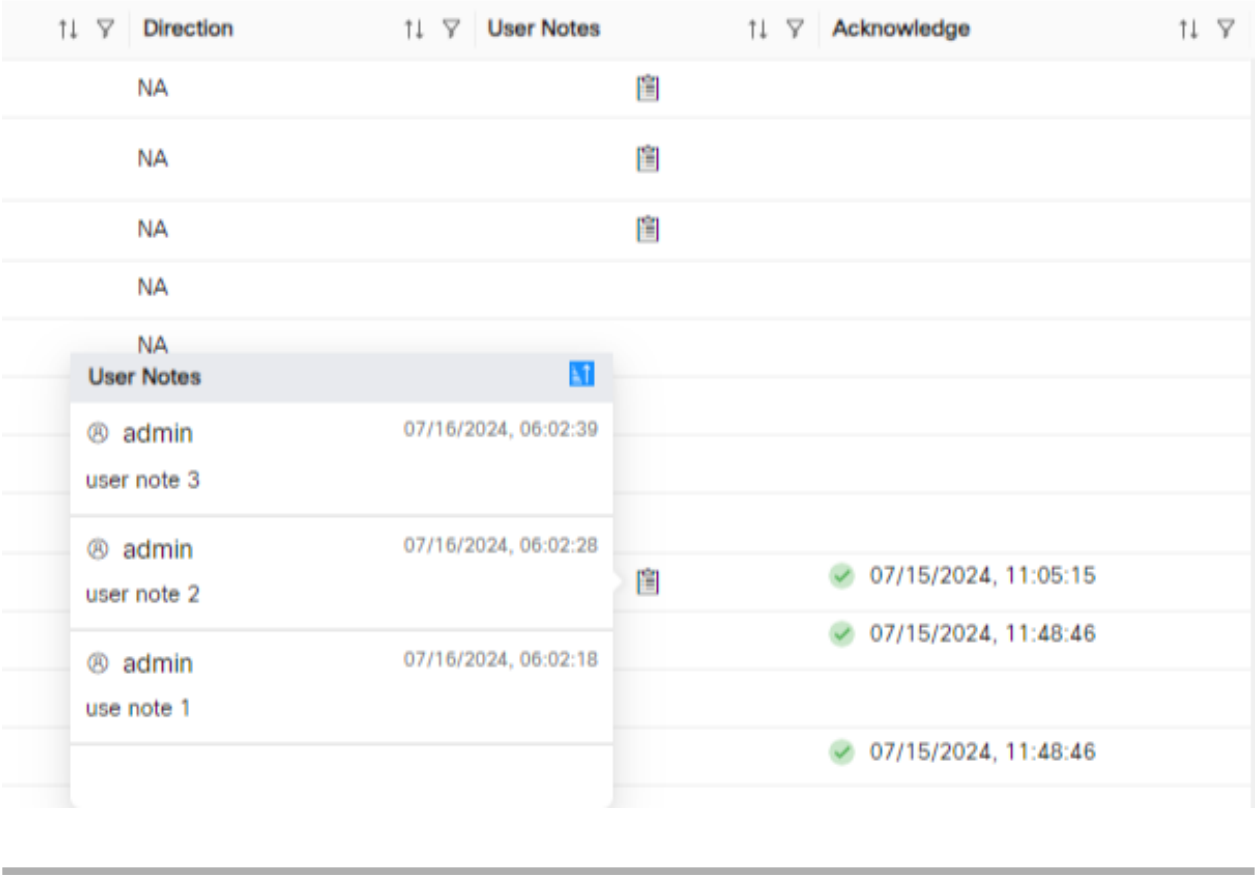
Step 12 Use the **Acknowledge** column in the table to view the acknowledged or unacknowledged alarms.

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

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

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

Figure 44: User Notes



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

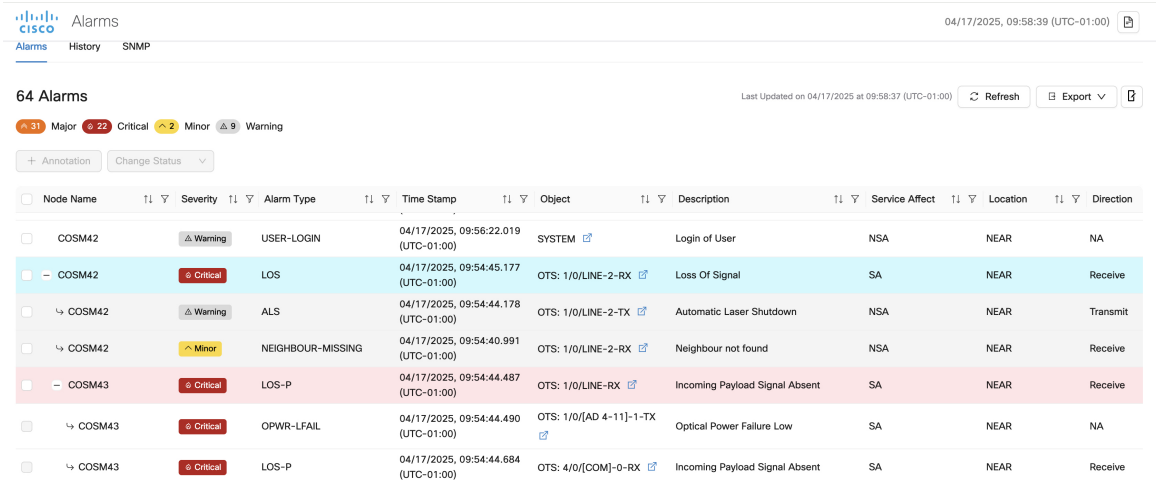
- The node or site level correlation is done by Cisco Optical Site Manager and the network level correlation is done by Cisco Optical Network Controller.
- From Cisco Optical Network Controller release 25.1.1, NLAC works over a a single OMS domain. Alarm correlation does not cover alarms across multiple 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 45: Alarms History



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 24: 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

Alarm	Object Type
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 46: Mute Acknowledged Alarms in Topology

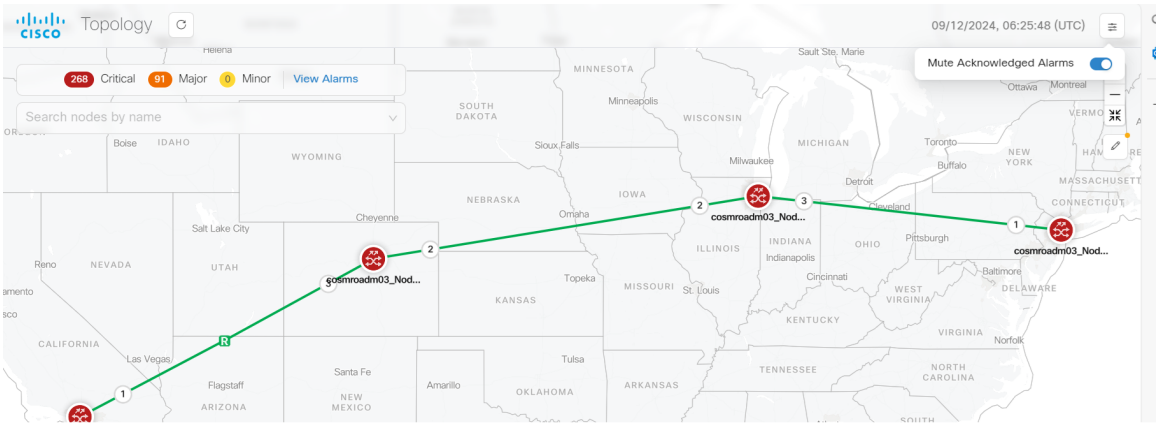
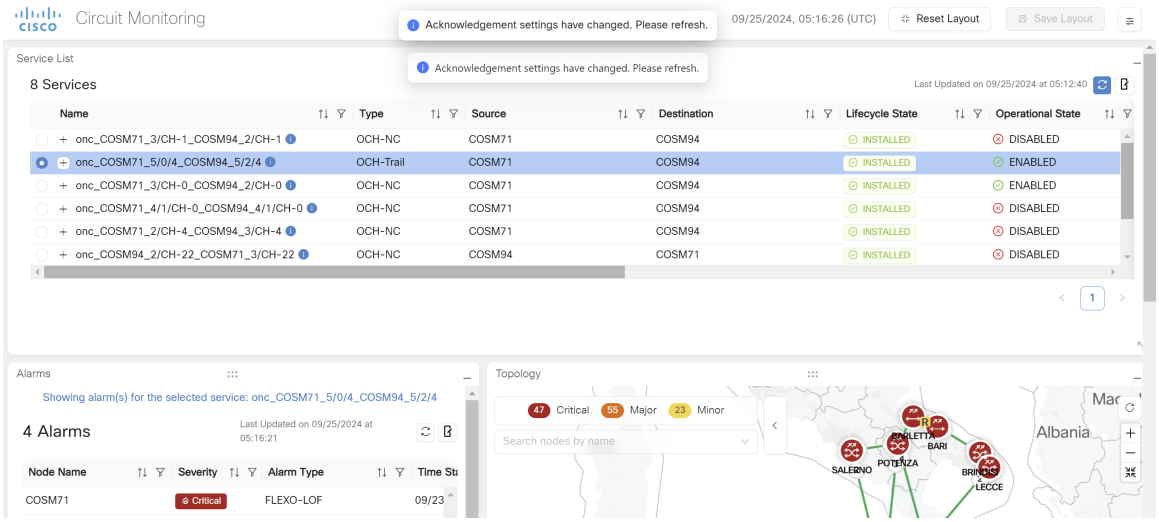
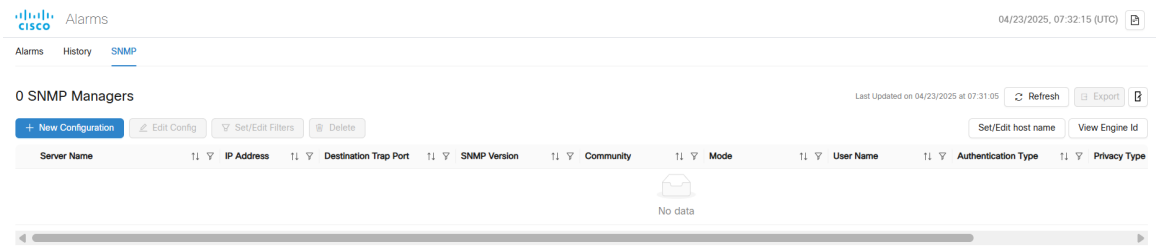


Figure 47: Mute Acknowledged Alarms in Circuit Monitoring



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 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**.

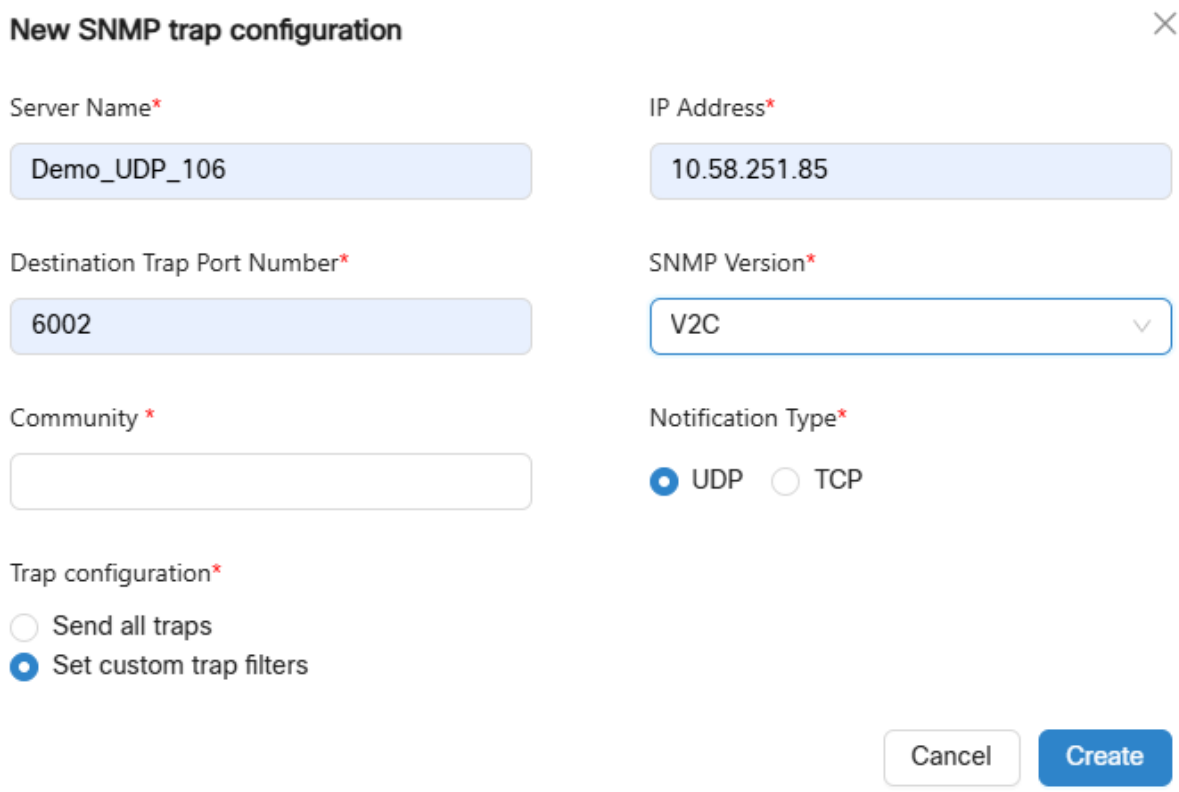
Step 2 Create a New SNMP Manager.

a) Enter the Server Name and IP Address.

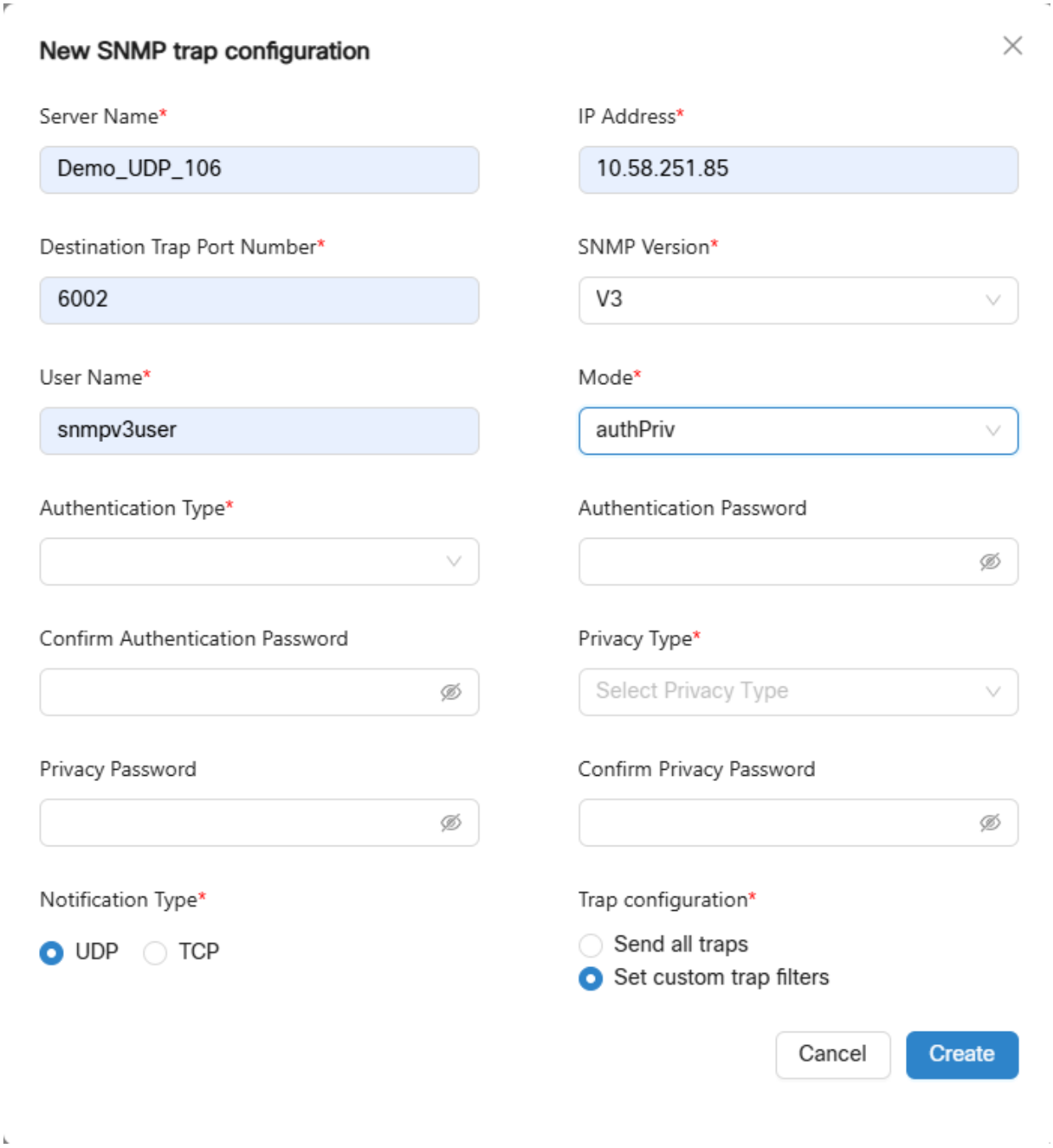
Cisco Optical Network Controller supports only IPv4.

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.



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**.



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

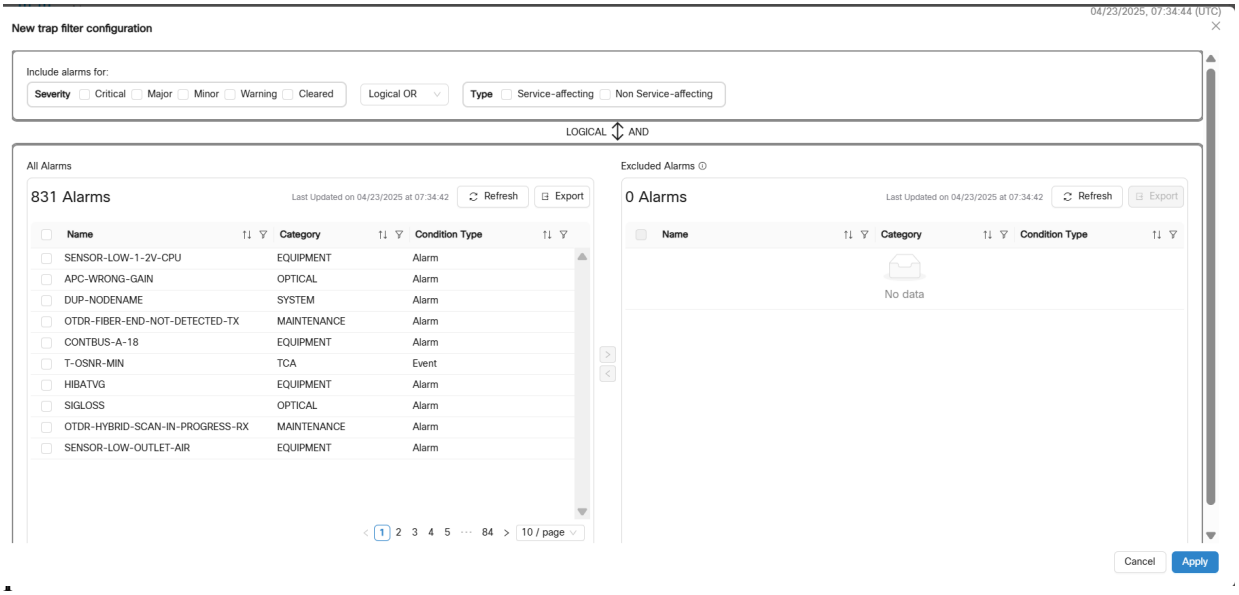
f) Choose the **Trap Configuration**, Send all traps or Set custom trap filters.
If you choose custom trap filters follow3.c, on page 87

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



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.

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.

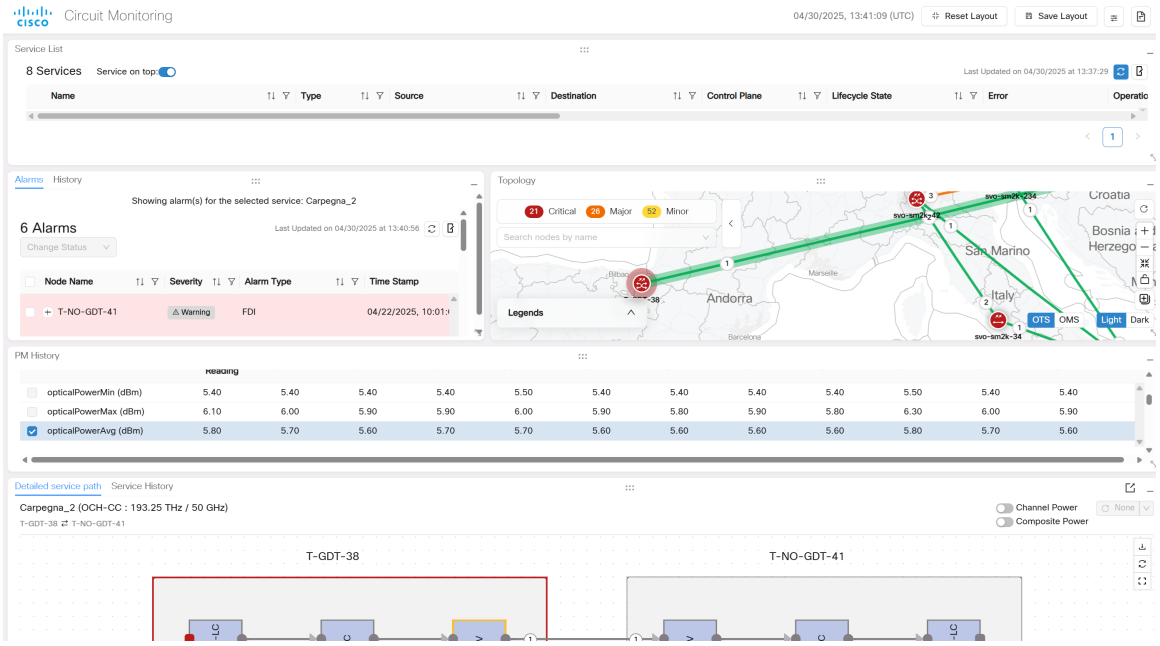
Step 5 Some of the other options that are available on these panels are mentioned below.

- 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.

Circuit Monitoring workspace

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

Figure 48: Circuit Monitoring

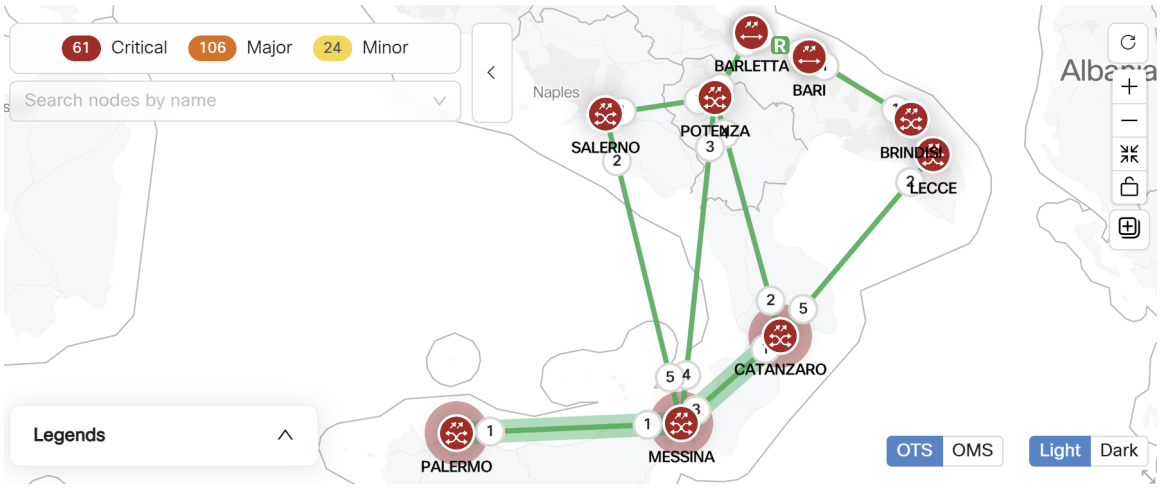


In **Circuit Monitoring**, the services list is primary. This list has these tabs

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

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

Figure 49: Service Summary



OTN circuit table

The OTN circuit table provides the OTN circuit parameter information.

Table 25: OTN circuit parameter description

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

SLTE ASE table

Table 26: STLE ASE table

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

Parameter	Description
Source Attenuation	Signal attenuation at source node
Destination Attenuation	Signal attenuation at destination node

Alarms table

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

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

Table 27: Alarms table parameters

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

Parameters	Description
Low Device Name	Low device name

History table

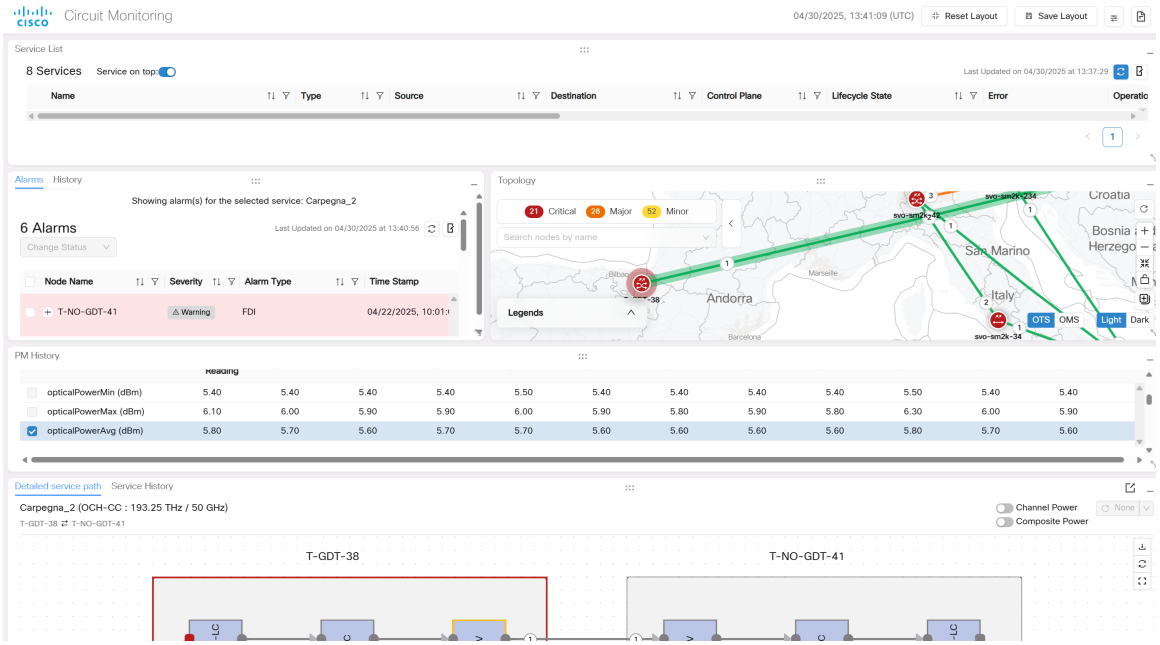
Use the **History** table in the **Alarms** pane to view the history of alarms in the network.

Table 28: Alarms history table parameters

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

Release-wise circuit workspace enhancements

Figure 50: Circuit Monitoring



- From release 24.3.1, **PM** tab is available in the **Circuit Monitoring** workspace application.
- From release 25.1.1, you can select multiple links or nodes in the topology.
  1. Click **Select node(s)/link(s)**in topology.
  2. Use the OTS/OMS/ 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.

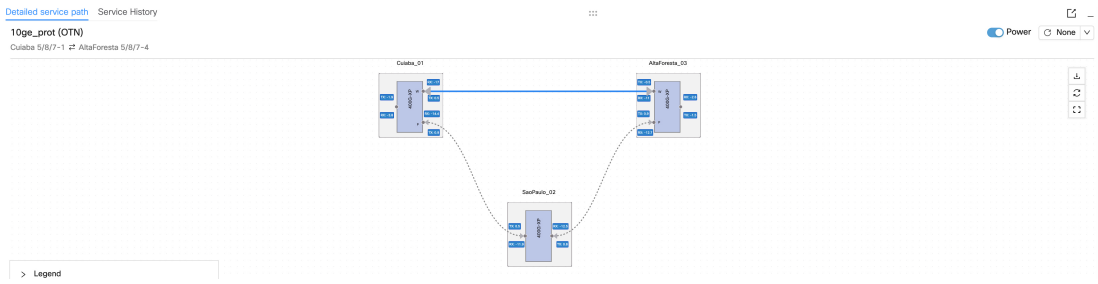
Detailed service path

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

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

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

  Figure 51: Power toggle switch

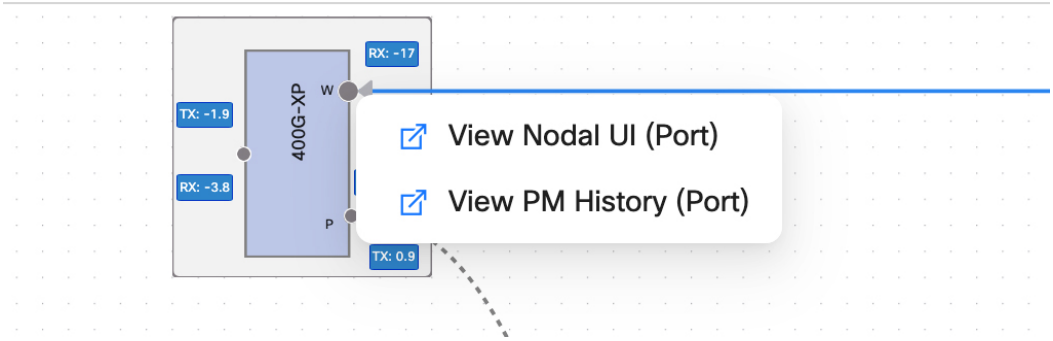


- Hover over a port or equipment in the detailed service path to view a tooltip. The tooltip displays W and P that specify the working and protected path for protected OTN service and source and destination ODU port information.

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

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

    Figure 52: Port pop-up options



The PM History in Circuit monitoring appears.

Figure 53: PM History in Circuit Monitoring

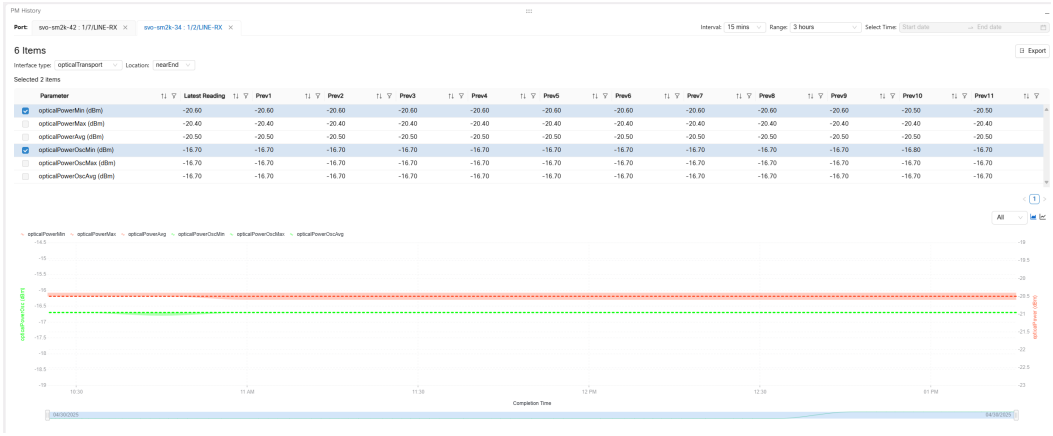
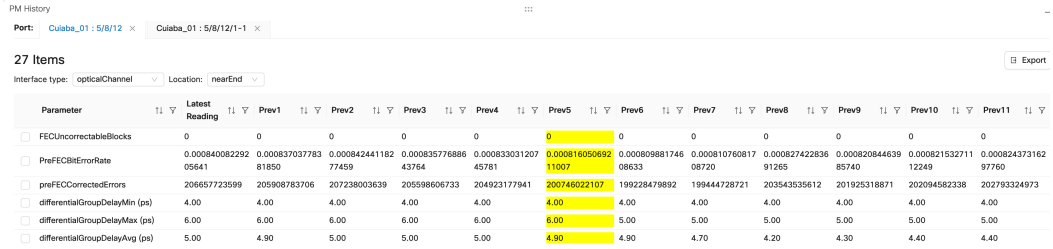


Figure 54: PM History in Circuit workspace

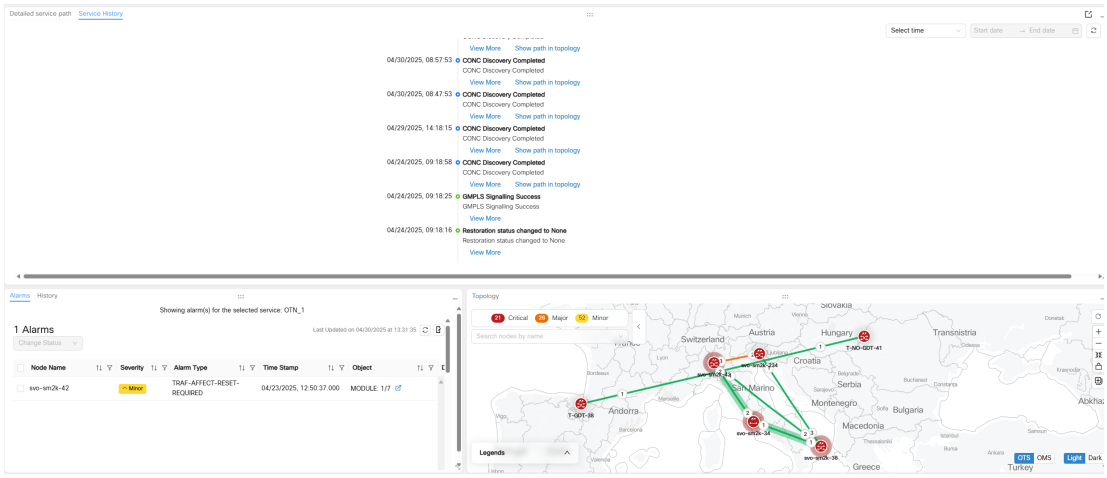


- **Interface type** drop-down list: By default, only one interface type is used to generate the report for the selected port. However, if the port has multiple interface types, you can choose the interface type from the drop-down.
- **Location** drop-down list: You can choose to view the PM history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

Service History

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

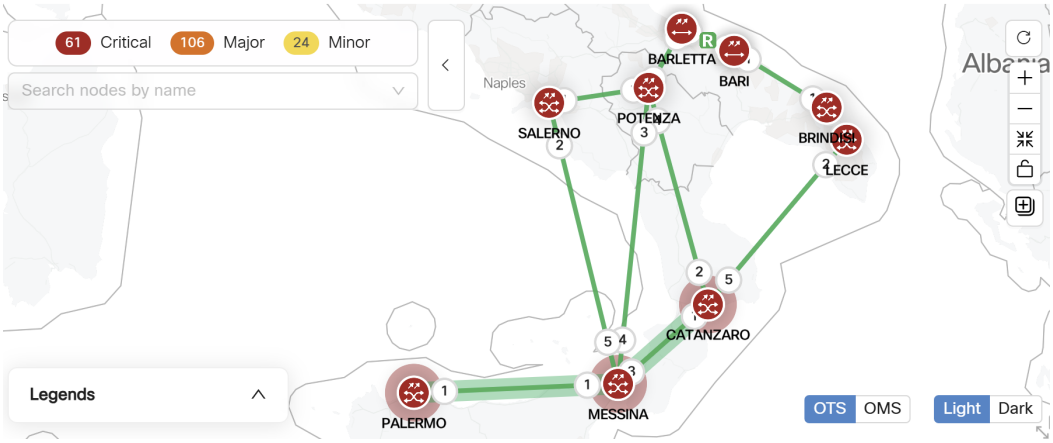
Figure 55: PM History in Circuit Monitoring



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

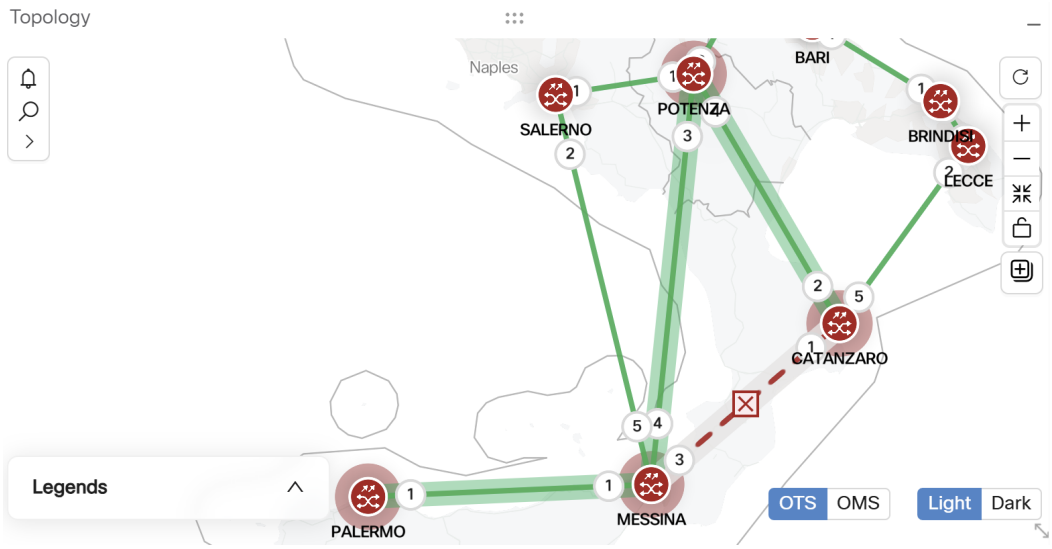
- **Visualize Circuit Restoration**
  - Select a Service from the Service List to highlight the circuit in the topology.

Figure 56: 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 57: 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.

Topology panel

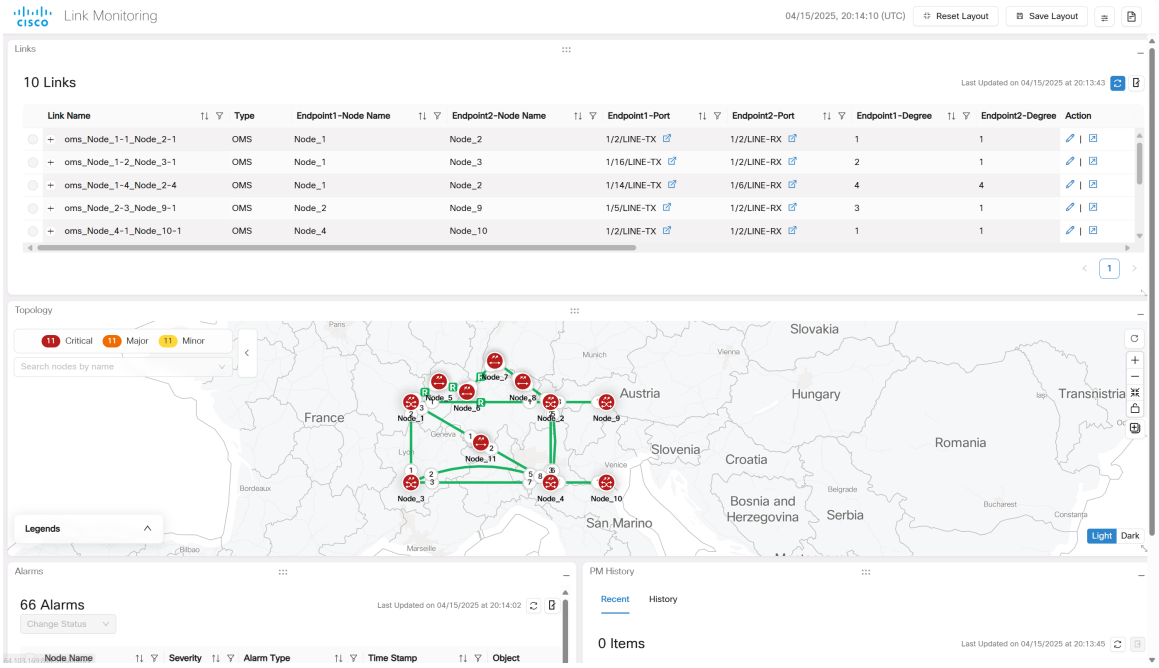
The **Topology** panel reflects the topology screen with a modified **Map View Options** icon.

Link Monitoring workspace

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

Links monitoring workspace functionalities

Figure 58: Link Monitoring workspace



- 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`.

  In Links monitoring workspace, a selection is bidirectional. For example, the link you select from the Links table list is highlighted in the topology. The nodes and links you select in topology are filtered in the links table list.
- In links table, click the pencil icon (**edit link**) in the action column to edit link details.
- You can cross launch circuit monitoring for circuits using a link by clicking **View in Circuit Monitoring** in the action column.
- In links table, you can select only forward/reverse OTS links.
- You can select multiple links or nodes in the topology.

  1. In **Topology**, click **Select links** icon.
  2. Select the nodes or links you want to modify.

     You can select up to 20 entities at a time. Multiple selection is available only for OTS links.
  3. Click **Select Links**.

     The links list shows the selected links.
  4. Click the **Refresh data and reset the hierarchy** icon in **Links** table to reset the table to show all links.

OMS Links tab

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

Table 29: OMS Links table parameters

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

Link Monitoring workspace options

These action icons and button improve your interaction with the table

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

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

OTN Links tab

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

Table 30: OMS Links table parameters

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

Alarms tab

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

Table 31: Alarms table parameters

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

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

Alarm history tab

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

Table 32: Alarms history table parameters

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

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

PM History pane

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

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

Table 33: PM history table parameters

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

Topology pane

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

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

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

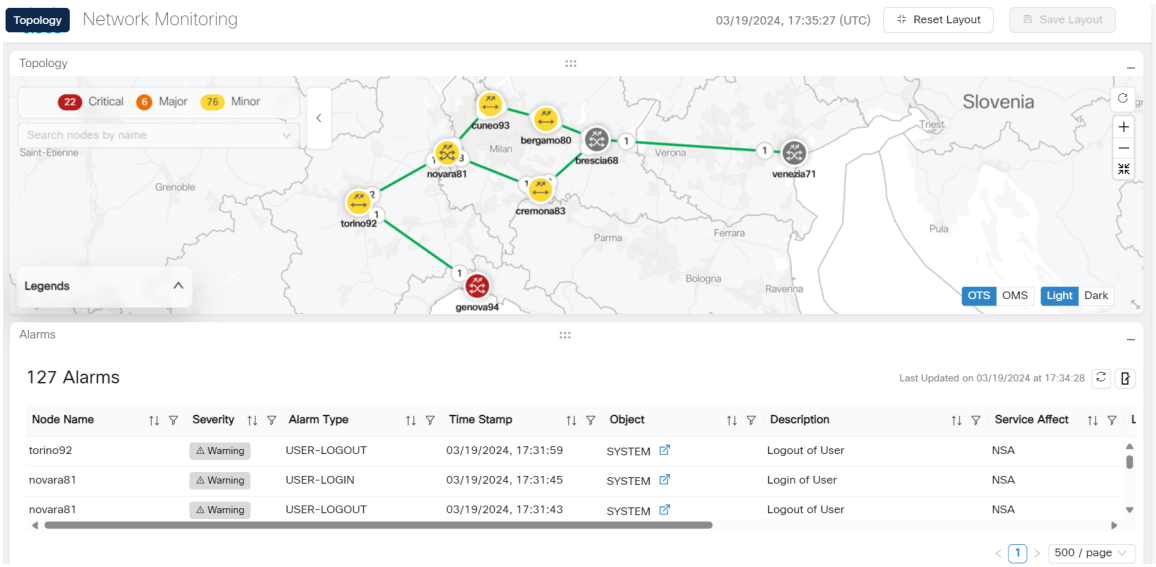
Table 34: PM history table parameters

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

Network Monitoring workspace

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

Figure 59: Network monitoring workspace screen



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

Software Image Management and Upgrade

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

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

Components of SWIMU

The SWIMU App is divided into these tabs:

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

Benefits of Using SWIMU

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

- **Centralized Management**: Provides a single interface for managing backups, restores, and upgrades.
- **Granular Control**: Allows detailed configuration of nodes used while scheduling a backup job on top of a node.
- **Manage Tasks**: It helps manage file storage, distribution, scheduling, and monitoring based tasks.
- **Efficiency**: The distribution and scheduling prevent network overload and ensure efficient operations.
- **Flexibility**: Supports ad hoc backups with detailed scheduling options.

- **Transparency**: Allows to track the progress with notifications to keep users informed of task statuses.
- **Long-term Storage**: Ensures backup files are stored for an extended period, with configurable storage options.



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

SFTP Servers

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

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

Types of Backup

There are two types of backup:

Table 35: 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 36: 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 37: 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.

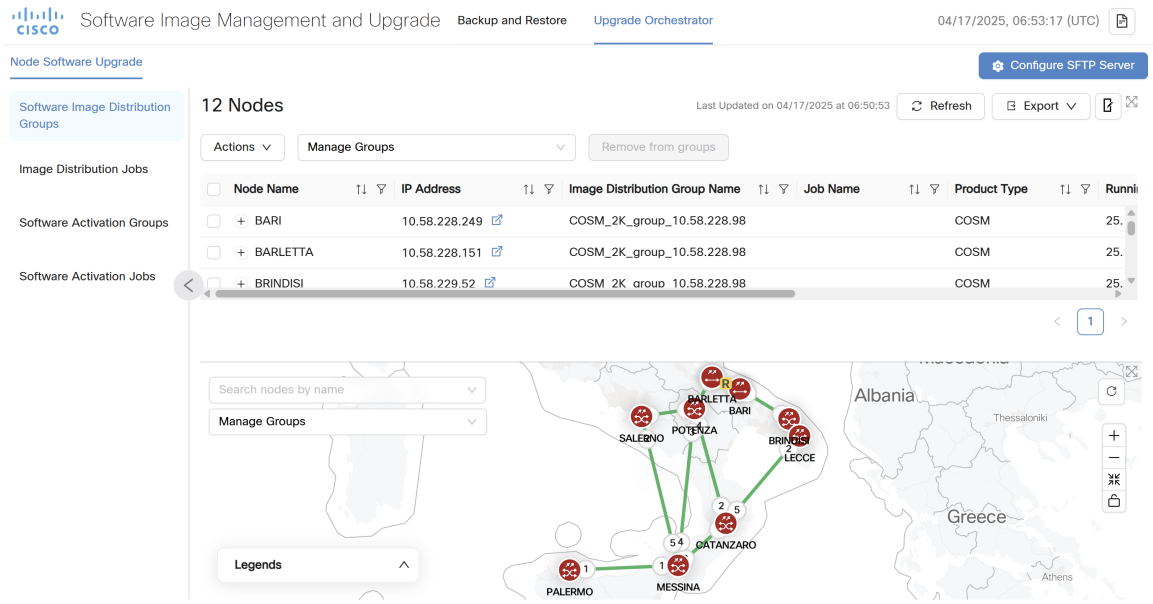
What to do next

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 60: Node Backup and Restore



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, on page 160 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

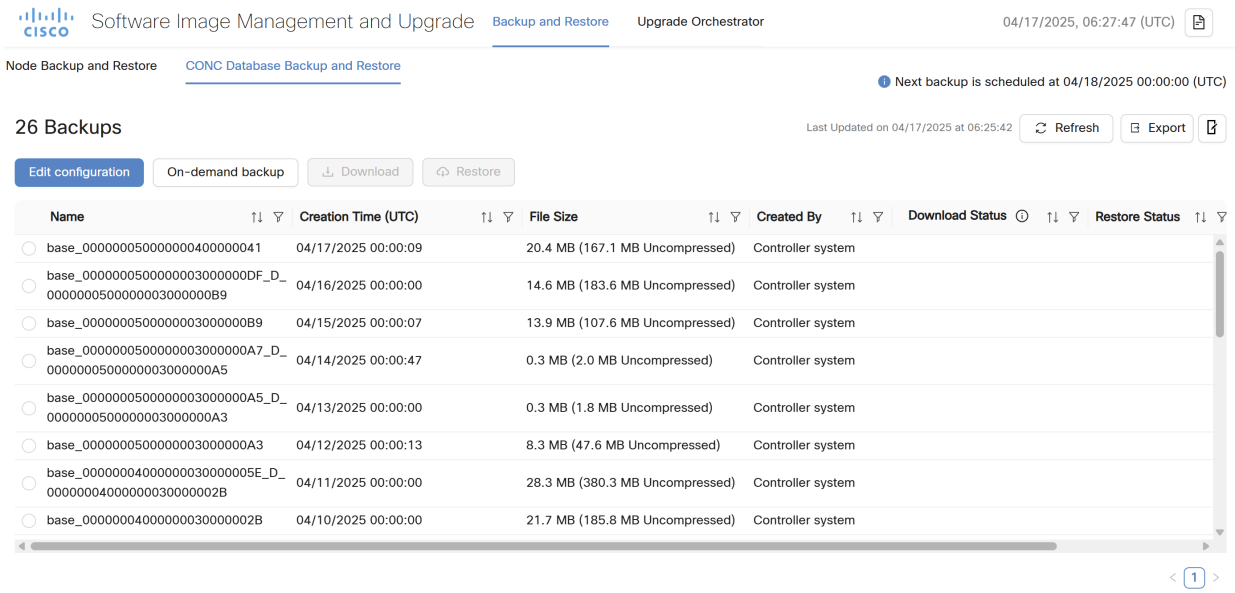
- The Cisco Optical Network Controller Database Backup and Restore feature relies on a properly configured SFTP server.
- Ensure that the SFTP server has sufficient storage space for the backups.
- If a backup fails, the BACKUP-FAILURE, on page 159 alarm is raised.
- If the upload of a backup to the SFTP server fails, the UPLOAD-FAILURE, on page 161 alarm is raised.

Procedure

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

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

Figure 61: Node Backup and Restore



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

Note
Cisco Optical Network Controller automatically validates the integrity of the selected backup before starting the restore process. Only backups that pass integrity validation are restored. If validation fails, the restore operation is aborted to prevent recovery from a corrupted or incomplete backup.

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>
```

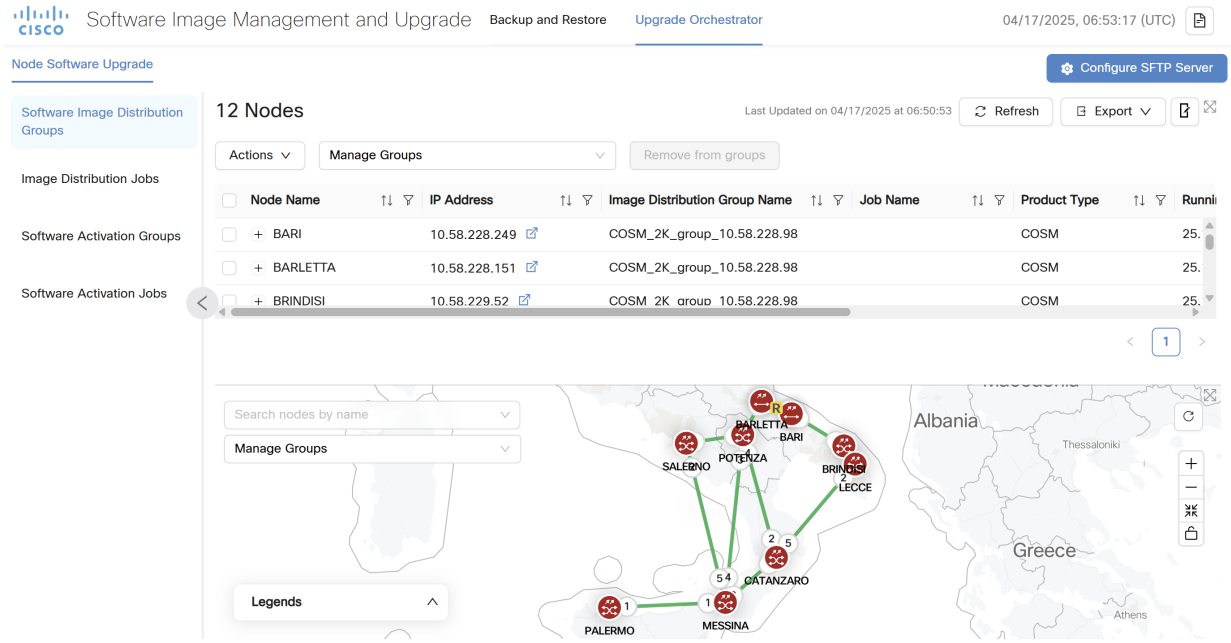
- `<file-name>`: The name of the file to delete.

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 62: Upgrade Orchestrator



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 autocreated by Cisco Optical Network Controller.

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

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

Step 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 drop-down list or give the details of the SFTP server.

e) Select the ISO image file to distribute.

f) Schedule the job to start immediately or later.
g) Click **Schedule** and choose a later time or schedule the job to run immediately.
h) Click the status for a device in the status column to view detailed status.
i) Select a job and click **Stop** to stop the job in the nodes in which the job has not started.

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

j) Select a job and click **Edit** to make changes to the job.

A job that is in progress cannot be edited.

k) Select a job and click **Delete** to delete a job that has completed or failed.

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

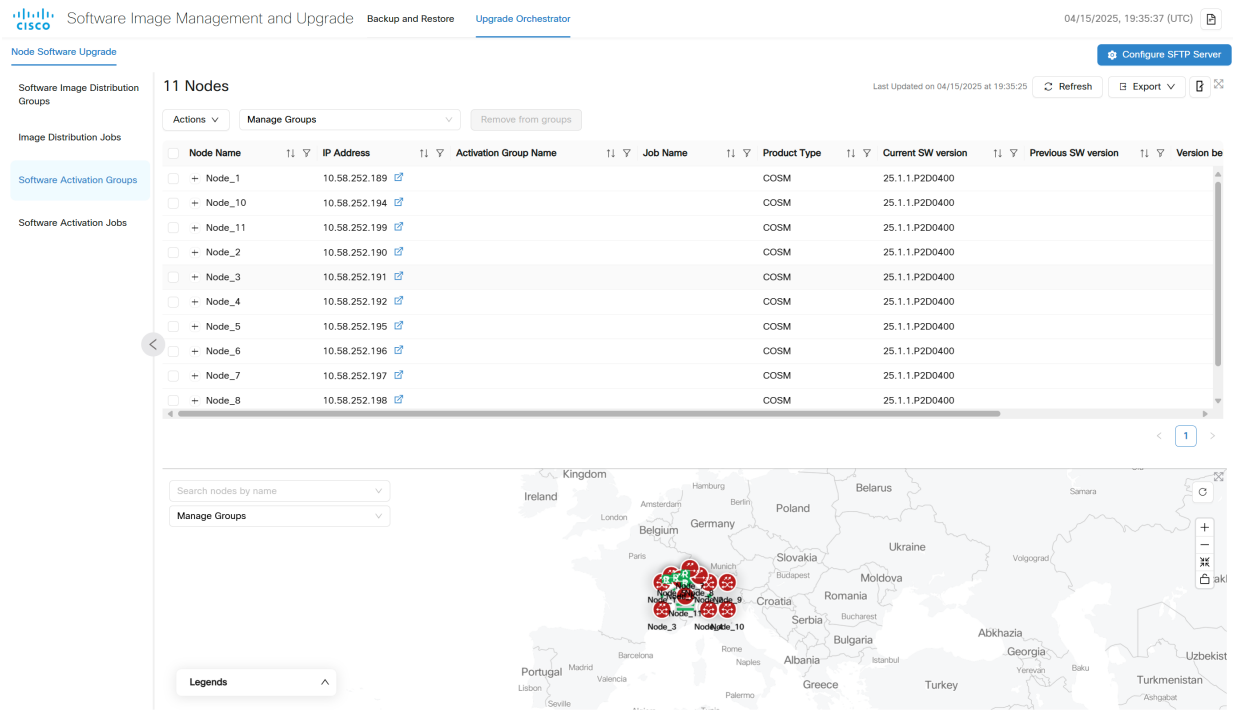
If a job status is **PARTIAL**, it means the job succeeded for some of the nodes, but failed for other nodes in the group of devices that the job was initiated for.

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

Step 4 Create Software Activation Groups.

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

Figure 63: Upgrade Orchestrator



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 autocreated by Cisco Optical Network Controller.

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

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

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

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

Step 6 Create a Software Activation Job.

Note
Software upgrade of a Cisco Optical Site Manager high-availability configuration from Cisco Optical Network Controller is not supported when the standby Cisco Optical Site Manager instance is either down or not present in a Cisco Optical Site Manager high-availability deployment. Configure or restore the active and standby peer status in Cisco Optical Site Manager before software activation. This prevents software-version misalignment between active and standby Cisco Optical Site Manager nodes.

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.

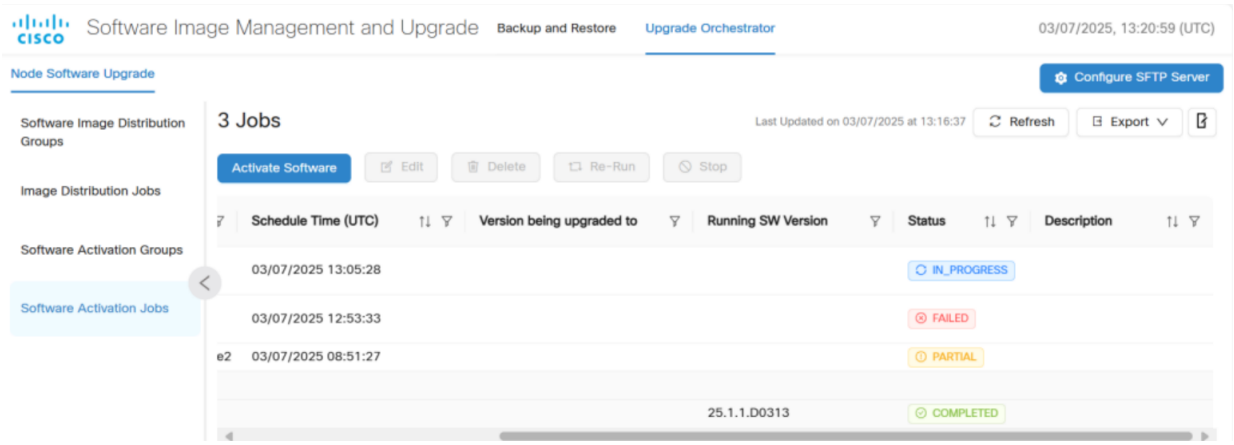
   The job continues on the nodes on which it was in progress.

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 64: Upgrade Orchestrator



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

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

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

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

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

PM History

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 38: 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.

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

Table 39: Time Range for Fetching Data

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

Port Details

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

Drop-down list	Description
Interface types	Type of interface on the ports. • opticalTransport • opticalChannel • otnOtu • otnOdu • ethernetCsmacd • zrPlus
Port Name	Port label
Location	Location of the node from where the PM is being collected. • near-end: The current node and current port. • far-end: The port to which the current port is connected to

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 40: 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.

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

Figure 65: 15-Minute Granularity PM Report

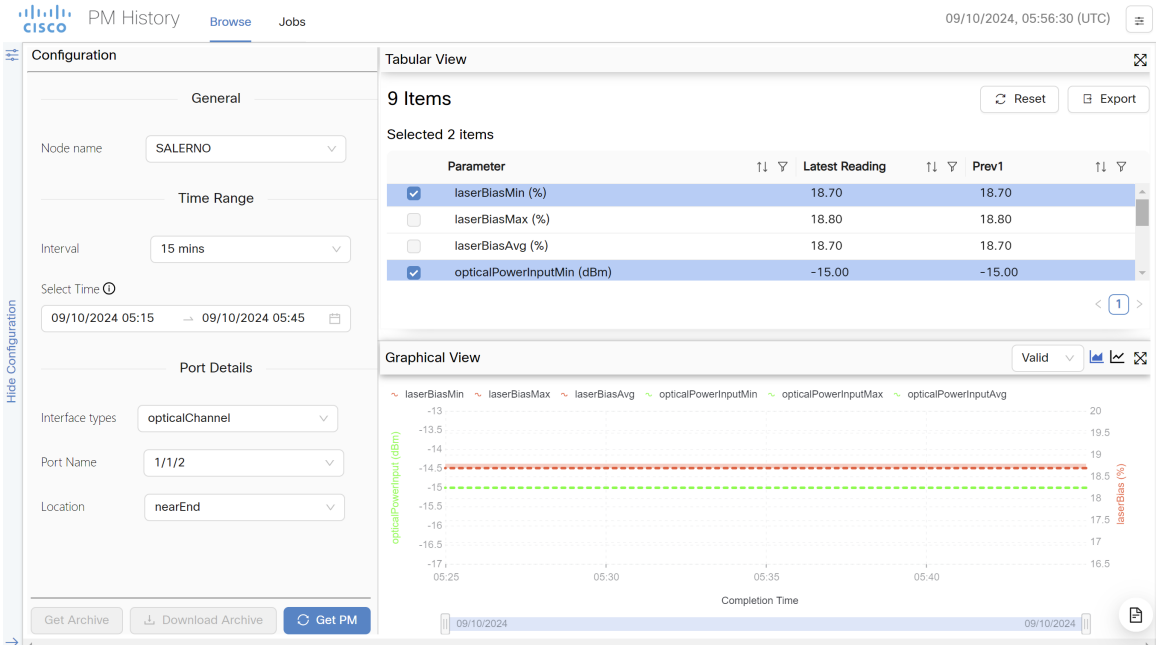
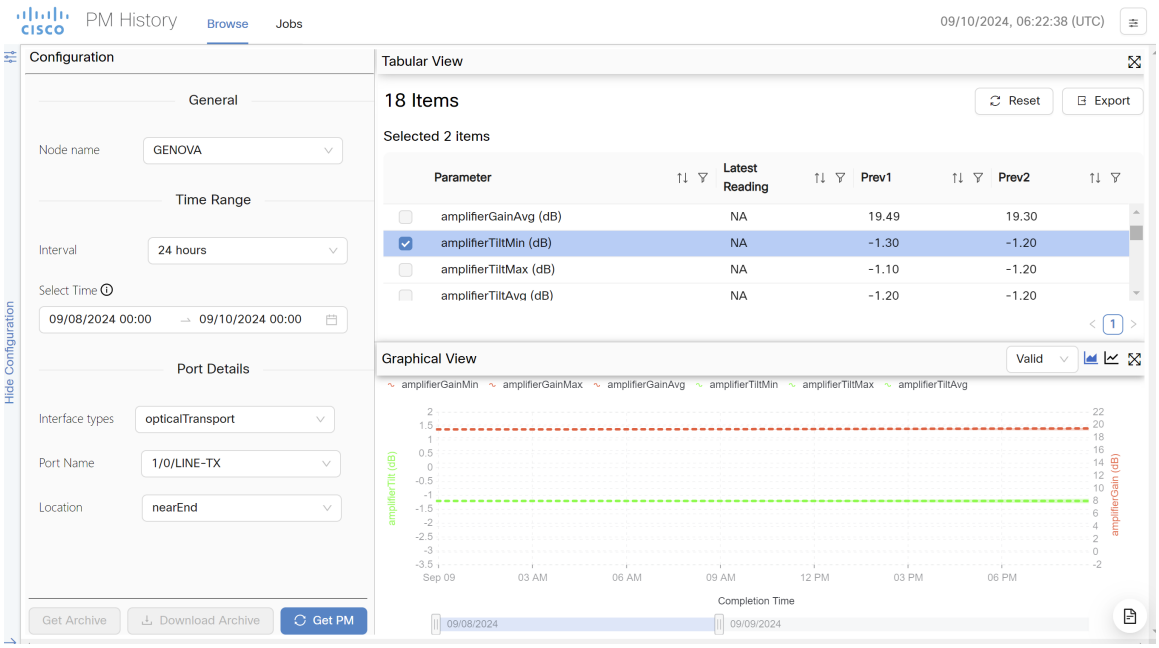


Figure 66: 24-Hour Granularity PM Report



Data Representation

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

PM Job Scheduler

The PM job scheduler manages the PM tasks as given:

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

Note

- **None**: one time applicable for both 15 minutes and 24 hours.
- **Daily**: is applicable only for 15 minutes.
- **Weekly** and **Monthly**: are applicable only for 24 hours.

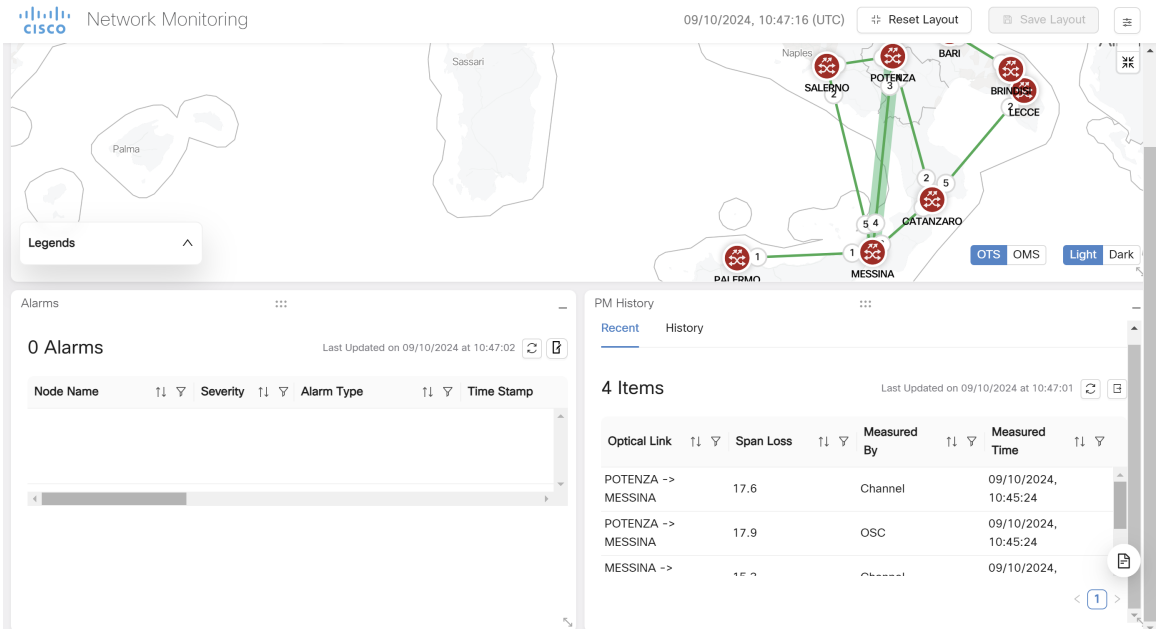
- Reports are sent through email which is configured through SMTP server and which are not password protected.

PM History in Network Monitoring

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

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

Figure 67: PM History in Network Monitoring



PM History in Topology

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

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

PM History in Circuit Monitoring

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

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

Note

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

Figure 68: PM History in Circuit Monitoring



Parameter	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:

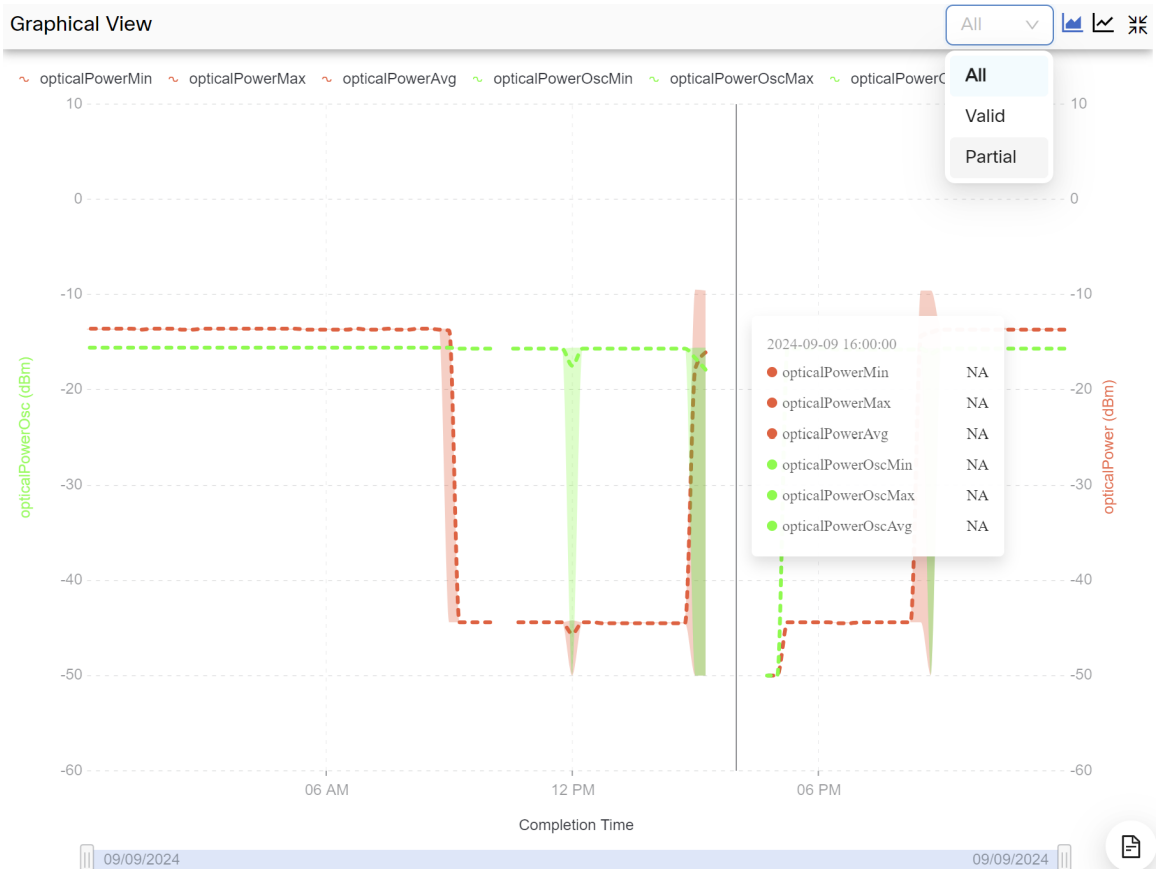
- Calculating and presenting total availability or outage time and percentage.
- Exporting to Excel and scheduling job options if available.

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 69: NA Values in Linear Graph



PM Data Retention

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

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

- **15 Mins (Max Range 31 days)**: PM data collected at 15-minute intervals.
  - **Days to retain active data:** The number of days the system keeps the most recent, high-granularity data.
  - **Days to retain archive data:** The number of days the system keeps historical data that has been moved to the archive.
- **24 hours (Max Range 180 days):** PM data collected at daily (24-hour) intervals.
  - **Days to retain active data:** The number of days the system keeps the daily aggregated active data.
  - **Days to retain archive data:** The number of days the system keeps the daily aggregated archive data.

Figure 70: PM Data Retention

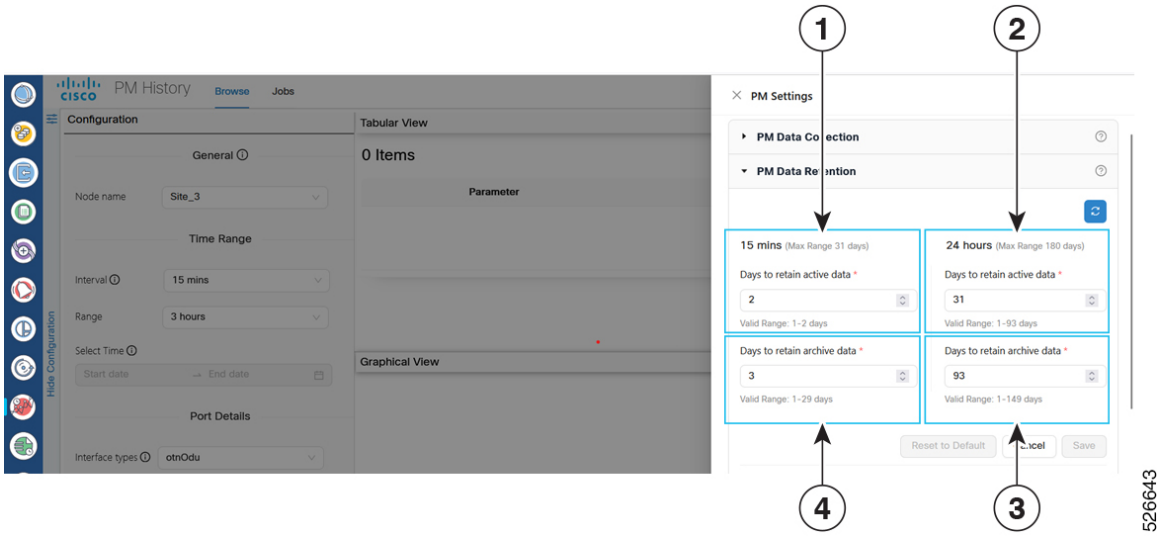


Table 41:

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

These are action buttons.

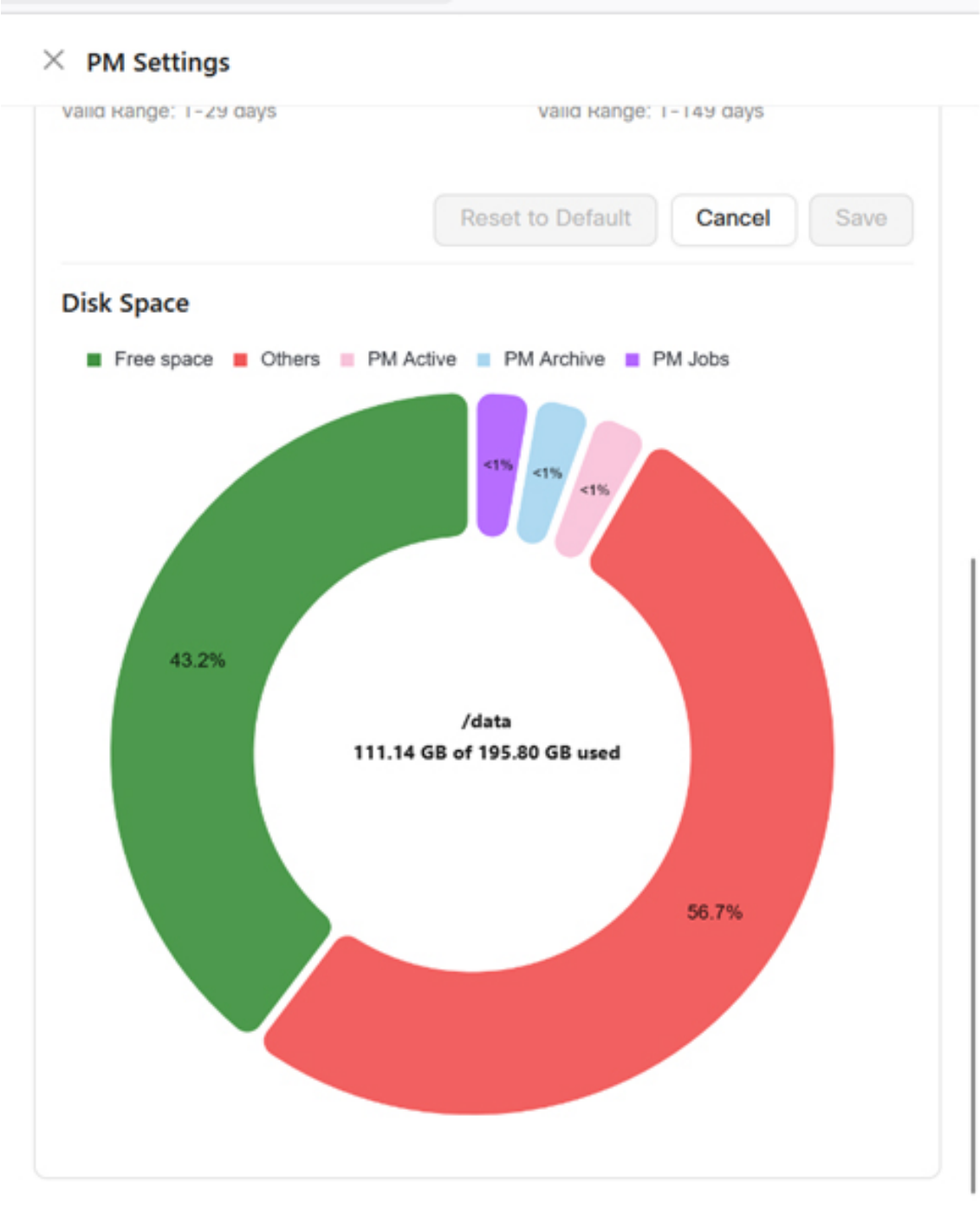
- **Reset to Default**: Restores data collection settings to their default state.
- **Cancel**: Discards any changes made to the PM data collection configuration.
- **Save**: Saves all configuration changes.

Disk Space

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

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

Figure 71: PM retention disk space



Charateresitics of PM data retention

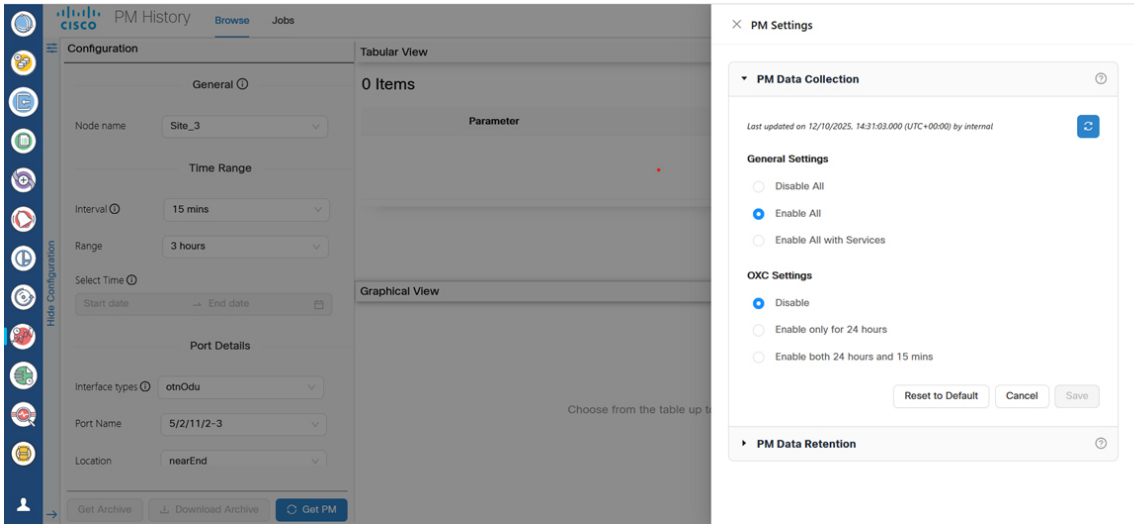
These are the characteristis of PM data retention.

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

PM Data Collection

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

Figure 72: PM History Data Collection



General Settings

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

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



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



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

OXC Settings

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



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



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

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

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

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

These are action buttons.

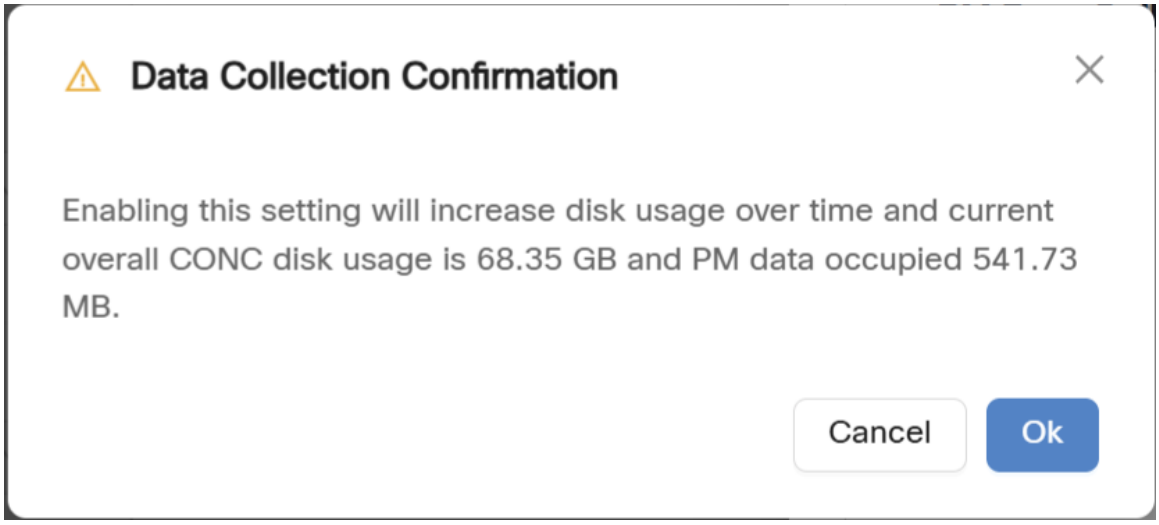
- **Reset to Default**: Restores data collection settings to their default state.
- **Cancel**: Discards any changes made to the PM data collection configuration.
- **Save**: Saves all configuration changes.



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

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

Figure 73: PM History Data Collection



Accessing PM History Report

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

Procedure

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

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

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

Note

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

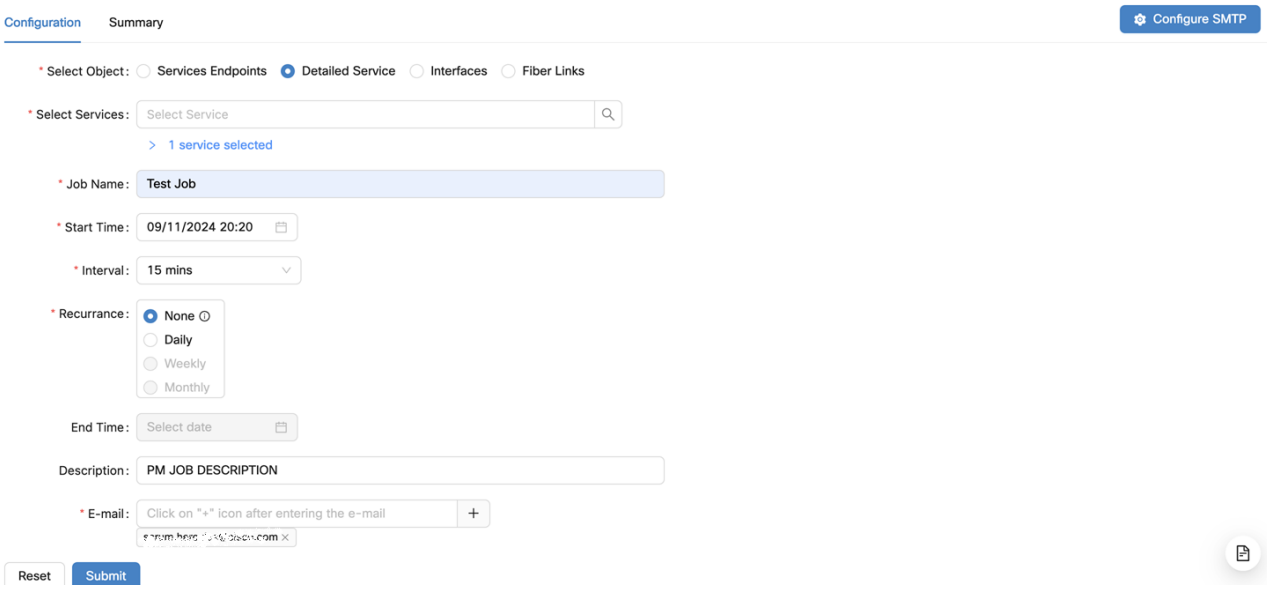
To browse or view the job scheduling details follow the steps given:

a) Click **Jobs** tab.

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

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

Figure 74: Configure SMTP



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

To schedule the jobs follow the steps given:

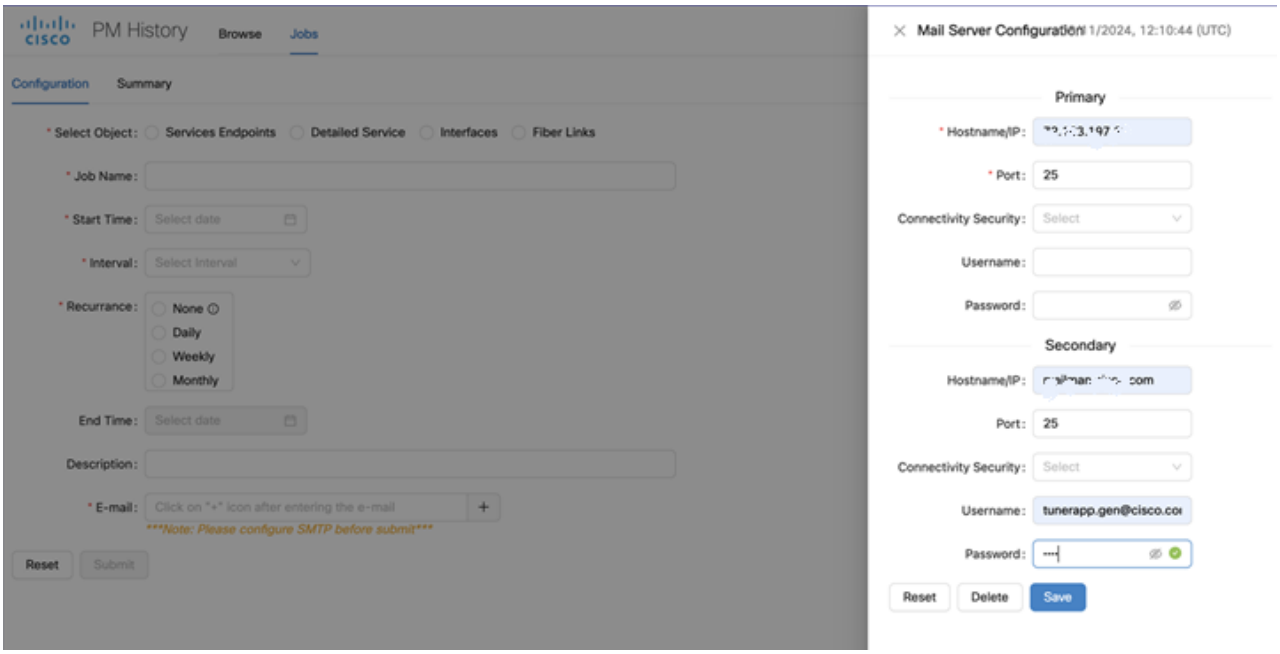
a) Use **Select Object** from **Services Endpoint** for OCH-Trail circuit or **Detailed Service** for OCH CC, OCH NC and OCH-Trail circuits or **Interfaces** to select site, equipments, shelves, cards, ports and layers or **Fiber Links**.

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 75: Jobs



Note

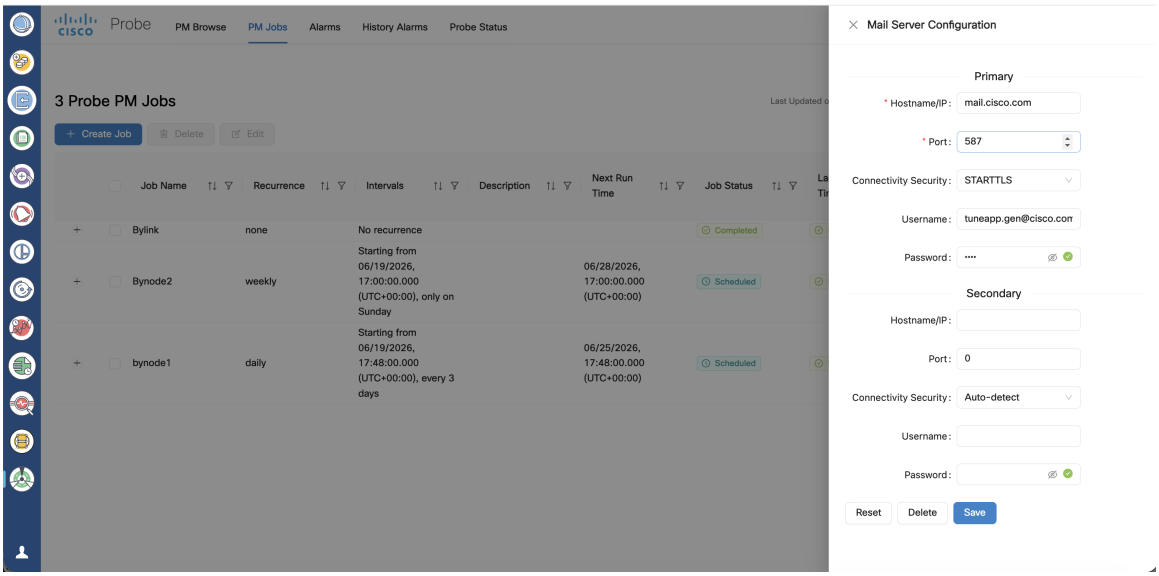
- To view the PM History values you must wait for a minimum of 15 minutes after onboarding.
- For 15 minutes interval, you must wait for 20 minutes post on-boarding.
- For 24 hours interval, you must wait for 15 mins past 12 A.M post on-boarding.

Configure the SMTP mail server

Configure the SMTP server that Cisco Optical Network Controller uses for email delivery from PM History jobs, Probe PM report jobs, and alarm email forwarding.

Cisco Optical Network Controller utilizes an SMTP mail server to send various email notifications, including performance monitoring reports and alarms. You can configure detailed server settings and optionally add a failover server.

Figure 76: Mail server configuration



Before you begin

- Obtain the SMTP server host name or IP address, port, connectivity security mode, and authentication details from the mail server provider.
- If the SMTP server requires authentication, obtain the SMTP account user name and the app password or server password required by the mail provider.

Follow these steps to configure the Cisco Optical Network Controller mail server:

Procedure

Step 1 Open the **PM History** application, then click the **PM Jobs** tab.

Step 2 Click **Configure SMTP**.

Step 3 In the **Mail Server Configuration** panel, enter the required **Primary** server fields.

Step 4 Select the **Connectivity Security** option that matches the primary SMTP server.

For details about the **Connectivity Security** field descriptions, see Connectivity security options, on page 133.

Step 5 If the primary SMTP server requires authentication, enter the **Username** and **Password**.

Step 6 Optional: In the **Secondary** section, enter the failover SMTP server details.

Step 7 Click **Save**.

Cisco Optical Network Controller saves the SMTP configuration and uses the configured mail server for email delivery. If a secondary server is configured and the primary server is unavailable, Cisco Optical Network Controller attempts to send email using the secondary server.

Mail server fields

The **Mail Server Configuration** panel contains separate **Primary** and **Secondary** sections. The primary server is the active SMTP server. The secondary server is optional and is used for failover.

Primary and Secondary server fields

Table 42: Primary server fields

Field	Description
Hostname/IP	Host name or IP address of the primary SMTP server. This field is mandatory.
Port	SMTP port for the primary server. This field is mandatory.
Connectivity Security	Security mode used when Cisco Optical Network Controller connects to the primary SMTP server.
Username	User name for SMTP authentication, if authentication is required by the server.
Password	Password or app password for SMTP authentication, if authentication is required by the server.

Configuration controls

Table 43: Configuration controls

Control	Description
Reset	Clears unsaved changes and restores the values shown when the panel was opened.
Delete	Deletes the saved mail server configuration when deletion is available.
Save	Saves the configured primary and secondary mail server details.

Connectivity security options

The **Connectivity Security** value and **Port** value must match the behavior expected by the SMTP server. Use the settings provided by the mail server provider for custom SMTP servers.

SMTP security options

Table 44: SMTP security options

Connectivity Security option	Standard port behavior
Auto-detect	Cisco Optical Network Controller selects the connectivity security mode based on the standard SMTP port and connectivity behavior.
None / Plain Text	Use for port `25` when the SMTP server expects no encryption.

Connectivity Security option	Standard port behavior
STARTTLS	Use for port `587` when the SMTP server expects an opportunistic TLS upgrade. The UI also lists port `2525` as a STARTTLS option.
SSL / TLS (implicit)	Use for port `465` when the SMTP server expects implicit TLS or SMTPS.

For a custom SMTP server or a nonstandard port, select the connectivity security mode that the server is configured to accept. For example, if a custom server uses a nonstandard port with STARTTLS, select **STARTTLS** instead of relying on the standard-port mapping.

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 45: 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
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.

Category Field	Description
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 77: Audit Logs

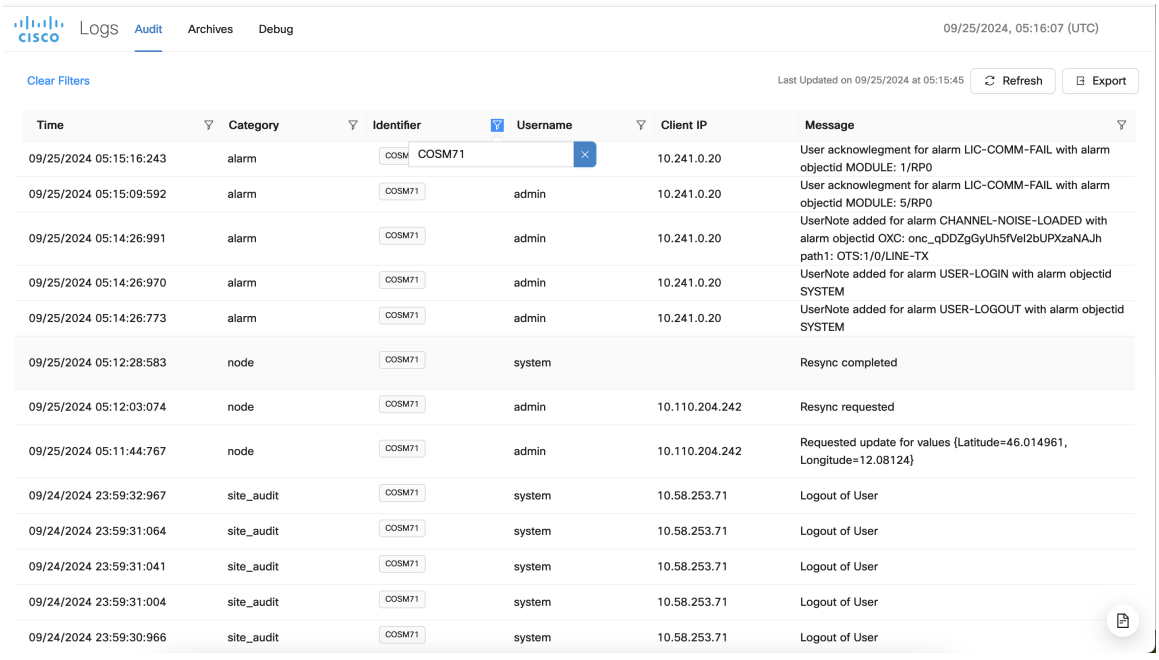


Figure 78: Archive Logs

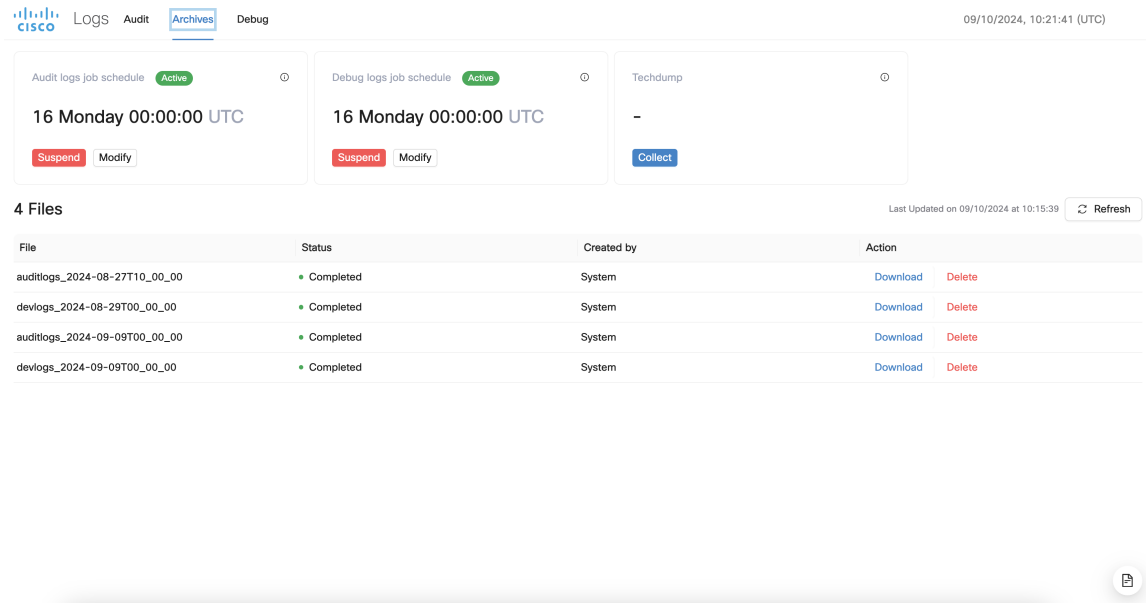


Figure 79: Scheduling Audit Logs Job

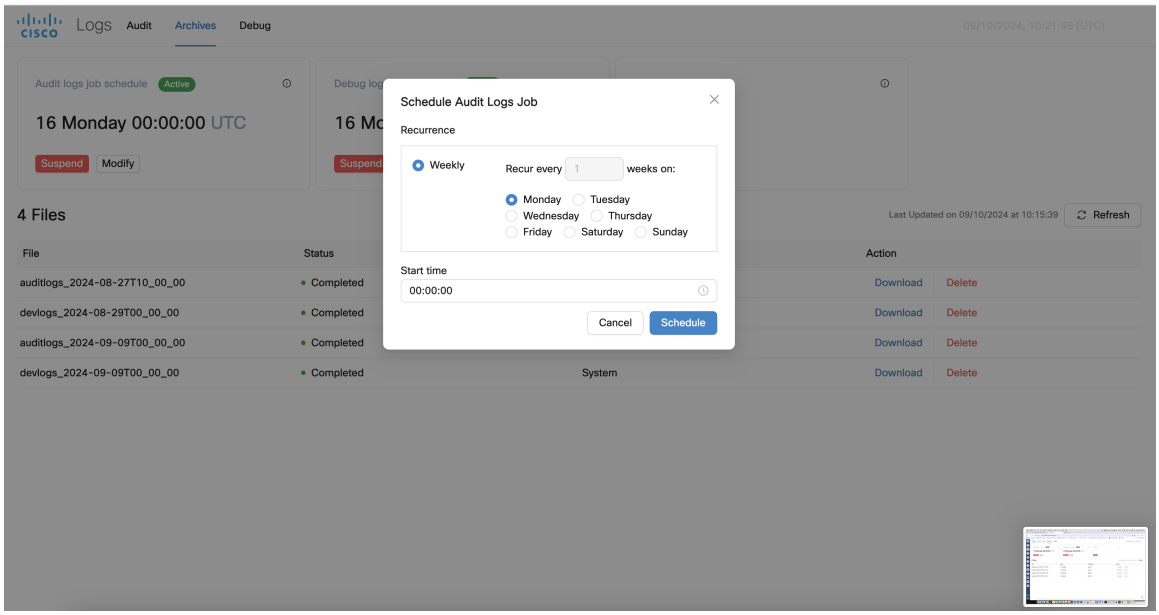
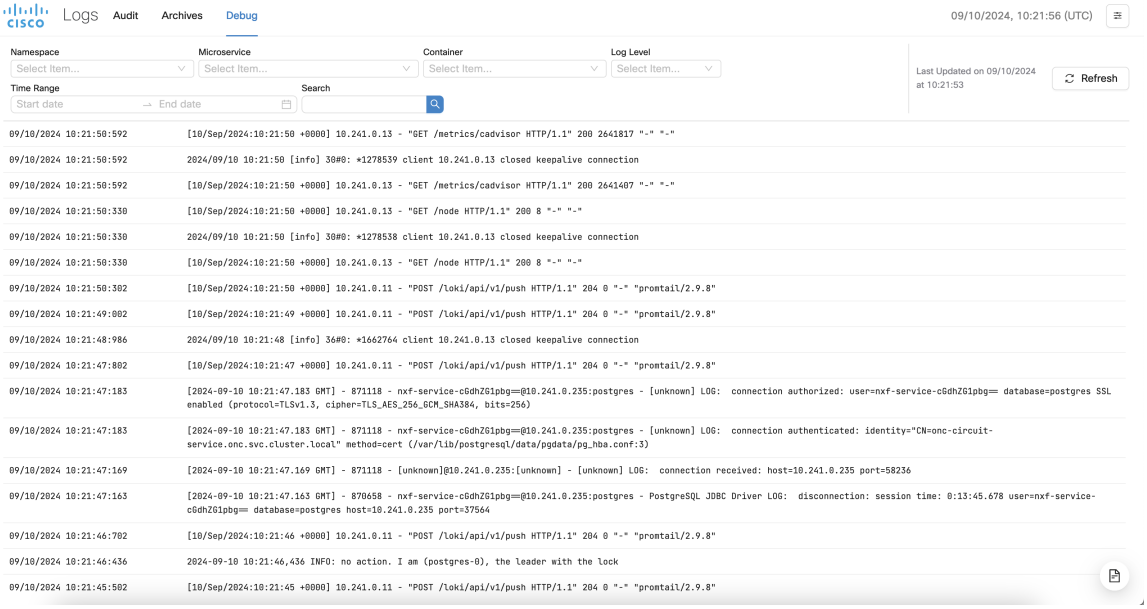


Figure 80: Debug Logs



Benefits of Logs Enhancement

Log enhancements help in:

Table 46: Benefit of Log Enhancements

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

Accessing Logs

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

Procedure

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

The **Logs** screen is displayed.

Step 2 Click **Audit** tab.

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

- **Time**: The time of audit log creation.
- **Category**: The category type of the audit log. It can be one of the following types based on your selection:
  - **System**
  - **Node**
  - **Inventory**
  - **Topology**
  - **Service**
  - **Alarm**
  - **Alien_Import**
  - **Site_Audit**
- **Identifier**: The names of unique Cisco Optical Network Controller identifiers like circuit names or device names, circuit tags or degree names which can be used to filter the **Audit** log table.
- **Username**: The user names based on type of user.
- **Client IP**: The IP address of the device or node. It can also have the Cisco Optical Network Controller IP address used for login or also appear as blank.
- **Message**: Messages are information pertaining to each log that are part of the **Audit**.

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

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

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

This will display the archives table along with the **Audit logs job scheduler**, **Debug logs job scheduler** and **Techdump** options.

For more information on each of these options you can click **i** the information icon, provided on top of each of these options.

Step 6 Click **Debug** tab to view the developer logs.

The **Debug** table has the following filter options which you can select:

- **Namespace**
- **Microservice**

- **Container**
- **Log Level**
- **Time Range**
- **Search**

There is also an **Enable Detailed Logs** option which allows you to fetch detailed log information from this table for debugging purpose. By default, this option is disabled and must be enabled only when required.

Generate and download tech dump logs

Tech dump logs on Cisco Optical Network Controller are diagnostic data bundles. They collect detailed system information, logs, and state files to help with troubleshooting and support.

From R26.1.1, you can collect, download, and delete tech dump logs from the **Tech Dump** tab of **Logs**.

When you generate a tech dump, Cisco Optical Network Controller compiles logs, configuration files, and operational data into a single archive file.

Before you begin

Ensure that there is sufficient space on the VM hosting the Cisco Optical Network Controller.

Follow these steps to generate and download the tech dump logs:

Procedure

Step 1 Click **Logs**.

Step 2 Click **Tech Dump** tab.

For details about the field descriptions on this tab, see Table 47: Tech dump tab field descriptions, on page 143.

Step 3 Click the **Collect** button to initiate the log collection.
A confirmation message appears, stating that starting a new log collection will delete the existing log file.

Step 4 Click the **Collect the DB dump** check box if you also want to collect information about CONC databases.

Note
Selecting this check box does not collect any sensitive information, including device credentials.

Step 5 Click **Collect** on the dialog box.

Collected log files remain local to the current active VM. If a switchover occurs, these files are not available on the new active VM.

Wait for the log collection to finish.

Step 6 Click **Download** to download the logs or **Delete** to remove them.

Warning

Do not log out during the download, as it can cause the file download to fail.

A file named in the *tech_dump_<timestamp>.tar.gz* format is downloaded.

The **Tech Dump** tab displays these fields:

Table 47: Tech dump tab field descriptions

Field	Description
File Name	Displays the name of the generated tech-dump file, including timestamp and timezone.
Status	Shows the current state of the tech-dump file generation. A green check mark indicates successful completion.
File Size	Indicates the size of the generated tech-dump archive in MB.
Triggered By	Shows the user ID that triggered the tech-dump collection.
Triggered On	Shows the exact timestamp (date and time with timezone) when the tech-dump creation started.
Action	Provides available operations for the generated file: • Download: Download the collected logs. • Delete: Delete the collected logs. **Note** These options are not displayed when the log collection is in progress.

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.

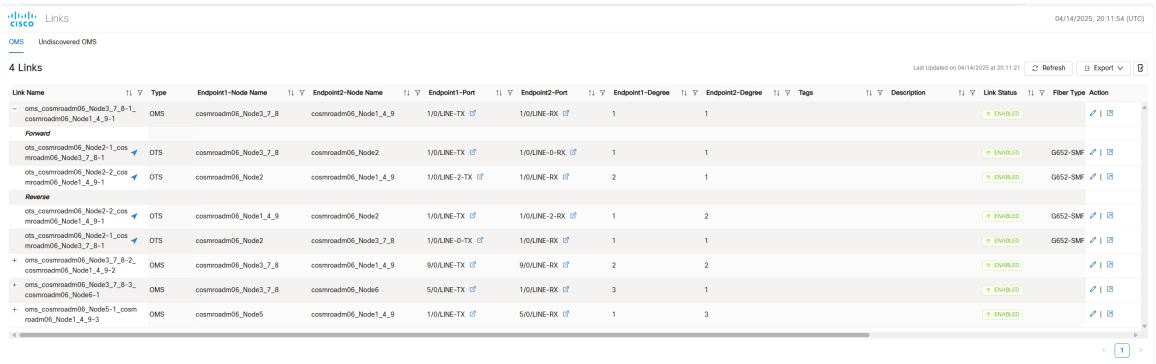
Procedure

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 81: Links App

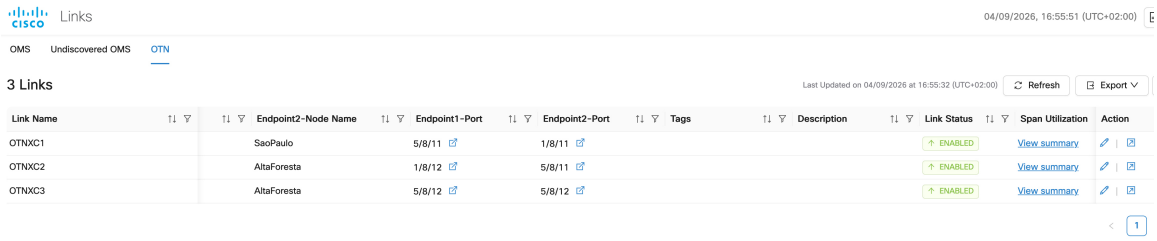


Key features of the Links app

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.

Figure 82: Links app



Click the **View summary** in **Span Utilization** to open the Span Utilization table.

Links table

The table includes these columns:

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

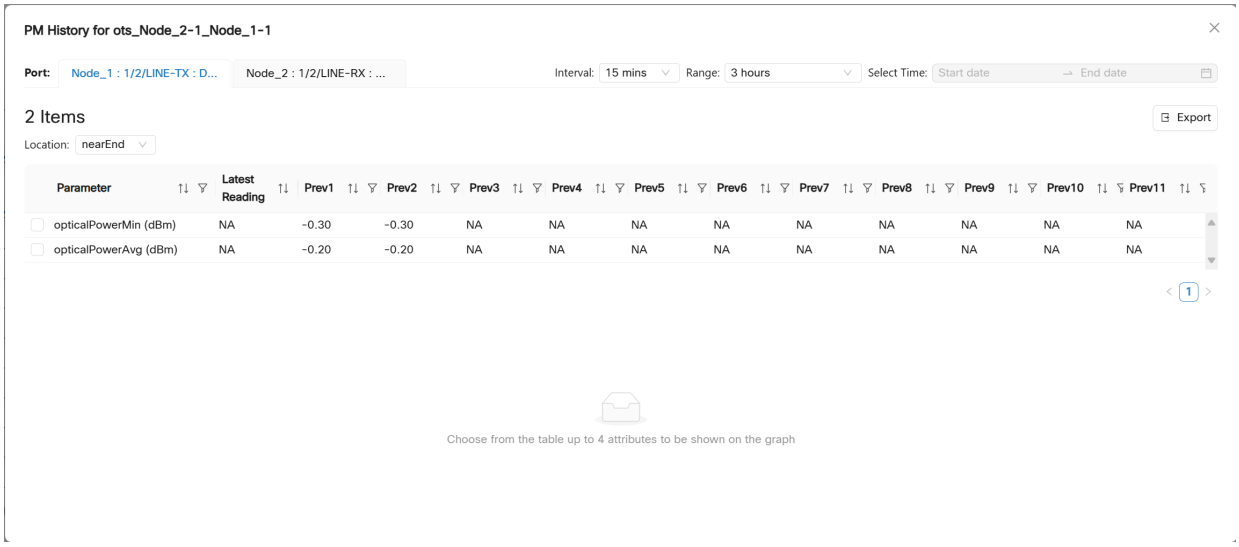
a) Select a link in the OMS or Undiscovered OMS tab.
b) Click the circuit monitoring icon in the Action column.

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 83: Links App



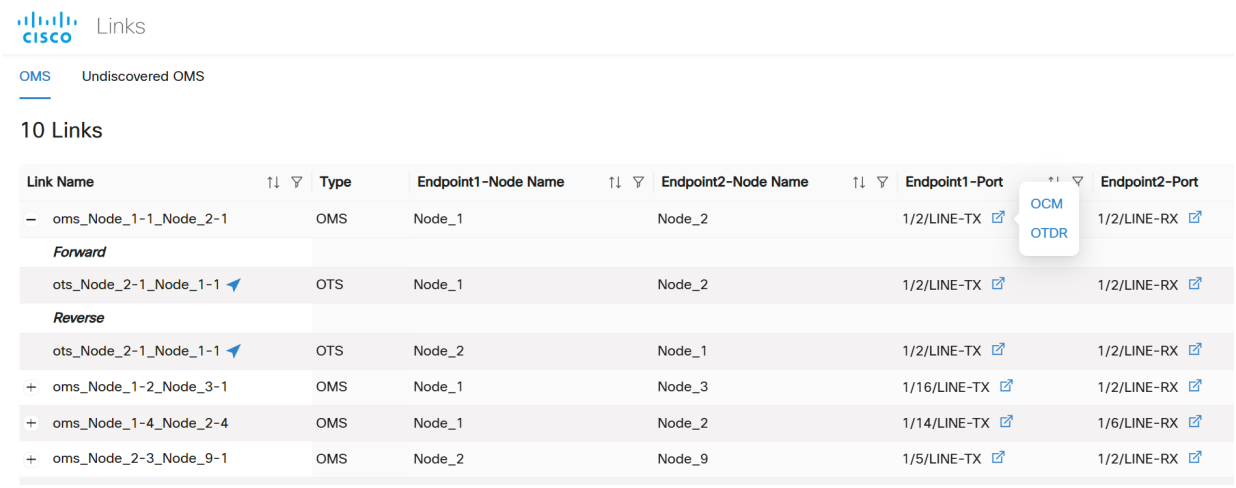
c) Select an interval and predefined time range or choose a custom range.
The PM history table is displayed.
d) Select up to 4 parameters to view on the graph.

Step 5 Cross-Launch to OCM/OTDR in Cisco Optical Site Manager.

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 84: Links App



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:

  ```
  sudo sedo diagnostics archive-logs /data
  ```

  Collect it along with the Grafana view.

Unmanaged Equipment Support

Unmanaged devices are third party devices that can be included in the Cisco Optical Network Controller circuit trails connected to transponders.

Cisco Optical Network Controller supports the unmanaged device MXD65-ADVA-FSP-3000-METRO-DCI-OLS in:

- **Topology**,
- **Service Assurance**,
- **Network Monitoring Workspace** and
- **Circuit Monitoring Workspace** applications.



Note

- The MXD65-ADVA-FSP-3000-METRO-DCI-OLS unmanaged device appears as 3LS in the circuit link.
- In case a degree between the ADVA devices is deleted and recreated, then a resync of the COSM nodes is mandatory.
- This is pre-provisioned equipment in COSM, the link status is not known since Cisco Optical Network Controller has no access to real HW.
- Alarms and PM are supported only for NCS 1014 and TXP cards.
- Power levels are reported only on the TXP card endpoint of the service, and not on the UME side.
- There is no support for automatic degree detection. The neighbouring nodes have to be configured manually through NETCONF RPC.

Figure 85: Unmanaged Equipment Support in Topology

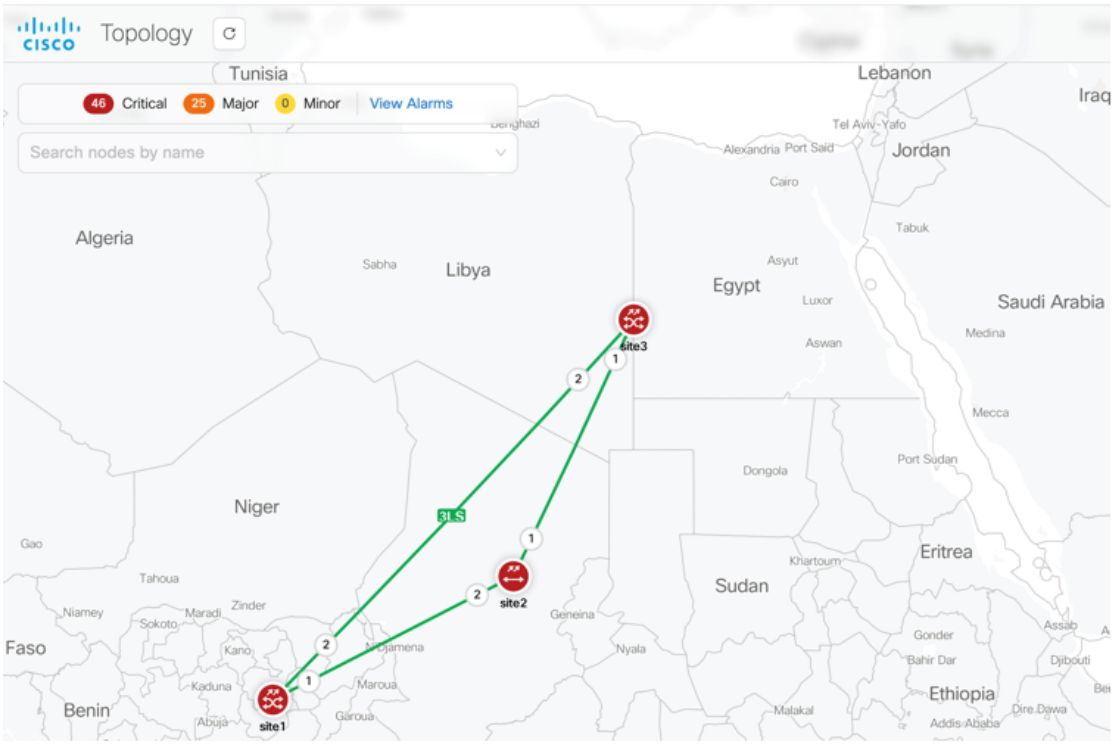
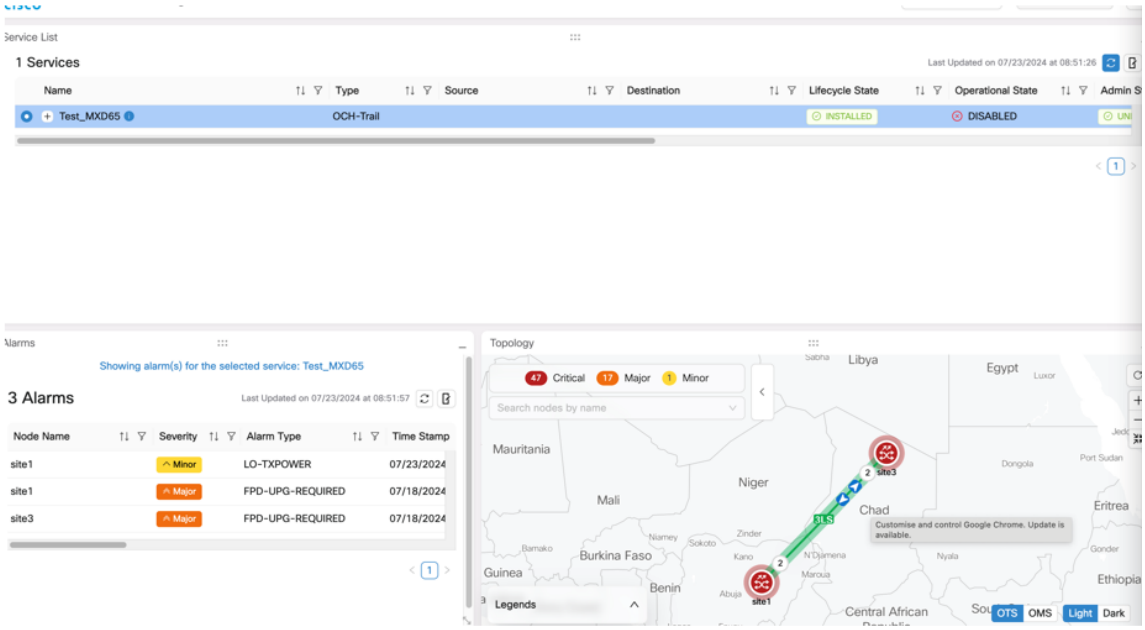


Figure 86: Unmanaged Equipment Support in Service Assurance



PSM OMS Protection

Protection Switching Module (PSM) is a Cisco Optical Network Controller feature that protects the Optical Multiplex Section (OMS) segment in the optical network. It ensures the continuity of signal transmission by automatically switching circuit paths in case of any fiber cut.

Note

- Cisco Optical Network Controller supports only brownfield network.
- Cisco Optical Network Controller does not support greenfield networks. From Cisco Optical Network Controller, you cannot create new PSM services.
- PSM module is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.
- NCS 1001 is supported only if it is managed by a COSM instance running over a NCS 1014 chassis.

Configuration in PSM Circuits

PSM supports two-way configurations and can be manually configured. Out of the two paths one will be active and the other will be a standby path. Whenever the active path fails due to fiber cut then the standby path is used for receiving the signal. This is because both the active and standby paths are always used in the TX direction for transmitting the signal, but only one of them can be used to receive the signal at a time.

Note PSM supports both automatic and manual path switching. Once you cross launch to COSM, there is also a manual switch option provided there for you to select any path and use it as the active path in the PSM circuit.

Benefits of PSM

The benefits of using PSM are:

- Enhanced network reliability and protection through PSM OMS protection.
- Improved network management and monitoring with clear visualization of active and standby paths in the circuits.
- Flexibility in network design with support for various connection scenarios for PSM.
- Comprehensive event logging and user-driven OAM for better operational control. See Configuration Guide for Cisco NCS 1001.
- Being multiplexer-agnostic ensures compatibility with various network components.

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

Protection switching in optical circuits with NCS 1010 ILA modules between NCS 1010 OLT nodes.

Additional PSM Functions

PSM generates alarms and performs automatic path switching with minimal data loss. PSM is integral to circuit creation and can be deployed in any network segment for protection. Additionally, it includes features for monitoring channel power and composite power.

PSM Circuit in Service Manager

In the Service Manager application, the PSM circuit is created like any other circuit using the Provision Circuit option. Once the PSM circuit is installed and it appears in the Services screen it can be visualized in the Service Assurance and the Workspace applications.

Limitations of PSM OMS protection

- Cisco Optical Network Controller does not support 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 NCS 1001 PSM must be set carefully based on the number of channels. If the number of channels is lower, a significant power drop from one channel going off may cause the PSM to switch, leading to traffic hits on other channels. See **Configuration Guide for Cisco NCS 1001**
- Cisco Optical Network Controller does not display the Reason for switchover.
- Cisco Optical Network Controller supports only configurations with amplifiers positioned after the PSM module. OMS protection is not supported.
- You must perform a resync if you onboard devices, add or modify IPCs, or add or remove degrees to the network after onboarding the PSM.
- If the same network is being managed by two separate active Cisco Optical Network Controller instances, the same connection service, either a discovered service in both instances, or a service provisioned in one and discovered in the other, must be deleted on both instances for all types of connection services.

PSM Circuit in Workspace Screen

To view the selected PSM circuit follow the steps:

Procedure

Step 1 Click **Workspace** option on the left panel.

Step 2 Click **Circuit Monitoring**.

Step 3 Select the PSM circuit.

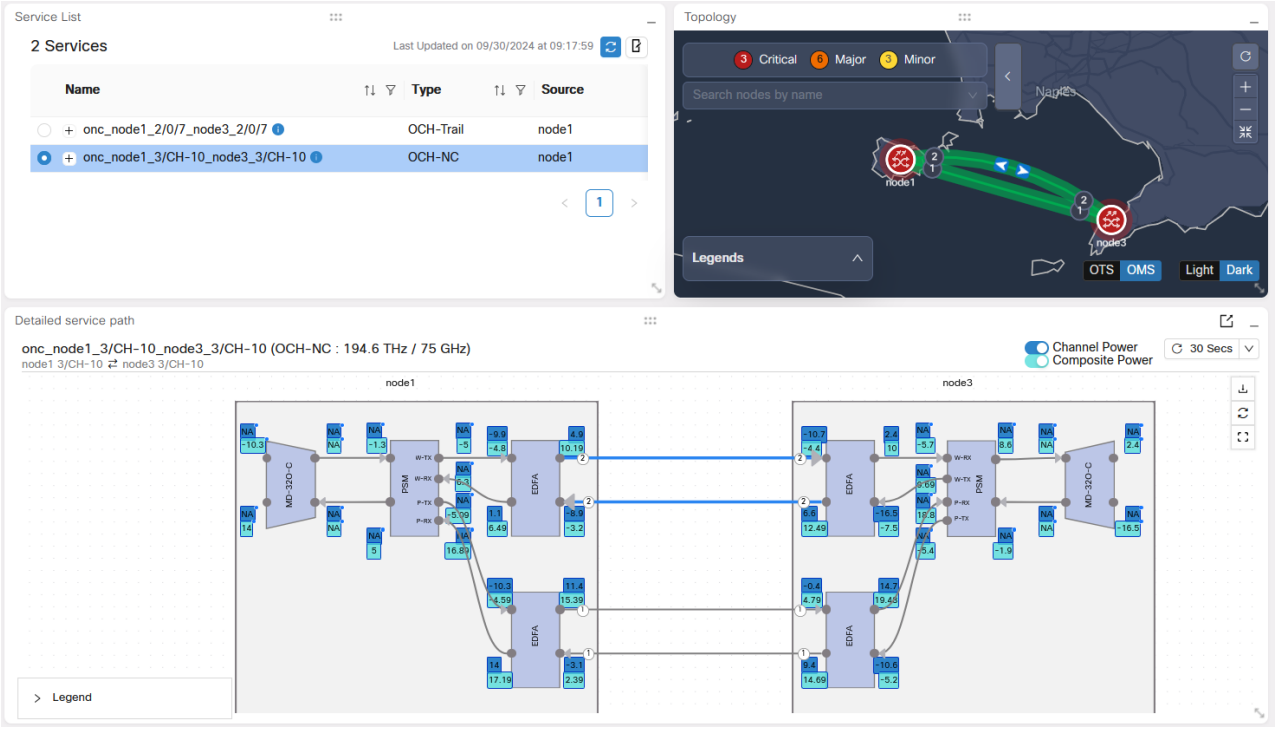
This will display the PSM circuit on the Topology screen where you can see the active PSM circuit path displayed with a blue colored arrow.

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 87: PSM Circuit in Workspace



- Unidirection service states are supported and displayed at channel level.
- If only one of the channel is discovered, work or protect, then the controller marks the service as PARTIAL. When that channel and carrier is INSTALLED, then the service moves to INSTALLED when other channel is discovered.
- If a path is standby in both directions, then it will show up as dotted line in topology in Circuit monitoring workspace.
- If different paths are active in different directions, then we will not see dotted line.

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>
```

Collect and download SEDO diagnostic files

This task provides instructions for interacting with the Torch Service API to trigger, monitor, and download system tech dump files that contains SEDO diagnostic logs.

Security Warning: **Security Warning:** The credentials provided in this guide (`username:password`) are for demonstration purposes. **Do not hardcode credentials in your scripts.** Use environment variables or a secure secret management system to handle your authentication tokens.

Note Only admin and supervisor users can use these APIs. Readonly user can not access these APIs.

Before you begin

Follow these base configurations.

- **Base URL:** `https://{CONC-HOST}:8443/onc-torch-service`
- **Authentication:** HTTP Basic Auth.
- **TLS:** The service uses self-signed certificates. Use the `-k` (insecure) flag in your requests to skip TLS certificate verification for self-signed certificates.

Procedure

Step 1 Trigger tech dump collection.

Example:

Endpoint

```
POST /v1/tech-dump/collection
```

Initiates a new tech dump collection. This request returns immediately with the current status.

Table 48: Query Parameters

Parameter	Type	Required	Description
triggeredBy	String	Yes	Identifier of the user who triggered the dump.

Parameter	Type	Required	Description
collectDbDump	Boolean	Optional	Set to `true` to include Postgres database snapshots. Defaults to `false`.

Example Request:

```
curl -sk -u <USERNAME>:<PASSWORD> \
  -X POST \

"https://{CONC-HOST}:8443/onc-torch-service/v1/tech-dump/collection?triggeredBy=admin&collectDbDump=true"
 \
  -H "Accept: application/json"
```

Example Response

```
{
      "filename": "tech_dump_2026-05-05T06_29_21_(UTC+0000).tar.gz",
      "status": "In progress",
      "completedPercentage": 0.0,
      "failureMsg": "",
      "triggeredBy": "admin",
      "triggeredOn": "05/05/2026, 06:29:21.840 (UTC+00:00)",
      "fileSize": 0,
      "downloadStatus": null
    }
```

Step 2 Monitor the status of the collection.

Example:

Endpoint

```
GET /v1/tech-dump/info
```

Initiates a new tech dump collection. This request returns immediately with the current status.

Query Parameters: No query parameters required.

Response Codes:

- `200 OK`: Returns the current status and completion percentage.
- `204 No Content`: No collection has been triggered yet.

```
# Example polling logic
for i in {1..30}; do
  resp=$(curl -sk -u <USERNAME>:<PASSWORD> \
    "https://{CONC-HOST}:8443/onc-torch-service/v1/tech-dump/info" \
    -H "Accept: application/json")

  st=$(echo "$resp" | python3 -c "import sys,json; d=json.load(sys.stdin); print(d.get('status',''))")

  echo "[$(date +%H:%M:%S)] Status: $st"

  if [[ "$st" == *"Completed"* ]] || [[ "$st" == *"failed"* ]]; then break; fi
  sleep 15
done
```

Example Response: Tech Dump Collection In Progress

```
{
      "filename": "tech_dump_2026-05-05T06_29_21_(UTC+0000).tar.gz",
```

```
    "status": "In progress",
    "completedPercentage": 63.32,
    "failureMsg": "",
    "triggeredBy": "admin",
    "triggeredOn": "05/05/2026, 06:29:21.840 (UTC+00:00)",
    "fileSize": 0,
    "downloadStatus": null
  }
```

Example Response: Tech Dump Collection Complete

```
{
    "filename": "tech_dump_2026-05-05T06_29_21_(UTC+0000).tar.gz",
    "status": "Completed",
    "completedPercentage": 100.0,
    "failureMsg": "",
    "triggeredBy": "admin",
    "triggeredOn": "05/05/2026, 06:29:21.840 (UTC+00:00)",
    "fileSize": <bytes>,
    "downloadStatus": null
  }
```

Step 3 Download the archive tech dump.

Example:

Endpoint

```
GET /v1/tech-dump/download
```

Retrieves the generated `.tar.gz` archive.

Table 49: Query Parameters

Parameter	Type	Required	Description
Range: bytes=<start>-<end>	String	Optional	Set `Range: bytes=0-1023` for resumable downloads.

Response Codes:

- `200 OK`: Full file stream.
- `206 Partial Content`: Returned when using the `Range` header.
- `409 Conflict`: File not ready (collection is still in progress).
- `416 Range Not Satisfiable`: Value entered is out of range.

No query parameters required:

Example Request: Full Download

```
curl -k -u <USERNAME>:<PASSWORD> \
  -X GET \
  "https://{CONC-HOST}:8443/onc-torch-service/v1/tech-dump/download" \
  -o tech_dump.tar.gz
```

You can use the `Range` header to resume interrupted downloads:

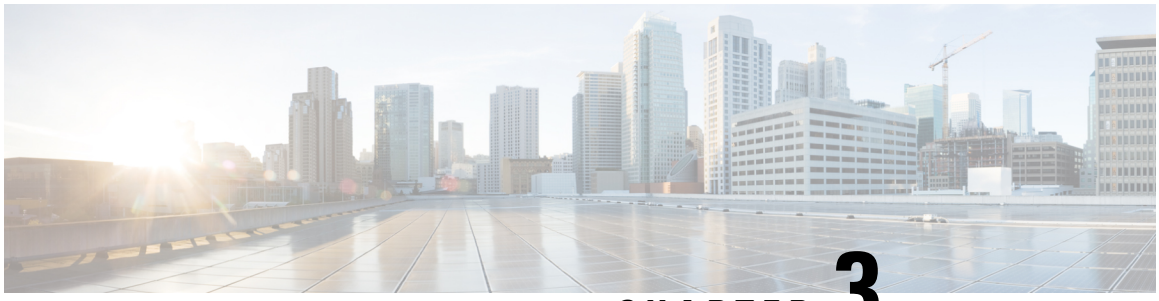
Example Request: Resumable Downloads

```
curl -k -u <USERNAME>:<PASSWORD> \
  -X GET \
  "https://{CONC-HOST}:8443/onc-torch-service/v1/tech-dump/download" \
```

```
-H "Range: bytes=102400-" \
-o tech_dump_resume.tar.gz
```

Note

- Only call /download after /info returns "Completed".
- The file is a `.tar.gz` archive containing logs, CONC service data, and DB dump.



CHAPTER 3

Alarm Troubleshooting

For information about alarms and clearing procedures, see the *Alarm Troubleshooting* chapter in the following guides:

- Troubleshooting Guide for Cisco NCS 1014
- Troubleshooting Guide for Cisco NCS 1010
- Troubleshooting Guide for Cisco NCS 1004
- Cisco NCS 2000 Series SVO Troubleshooting Guide

This chapter provides a description, severity, and troubleshooting procedure for each Cisco Optical Network Controller alarm and condition. To clear an alarm when it is raised, refer to its clearing procedure.

- BACKUP-FAILURE, on page 159
- NODE-BACKUP-FAILURE, on page 160
- NODE-DISCONNECT, on page 160
- UPLOAD-FAILURE, on page 161
- DISK THRESHOLD, on page 161
- SWITCHOVER, on page 163
- FAILOVER, on page 163

BACKUP-FAILURE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: Controller system-Database Backup

The BACKUP-FAILURE alarm is raised when Cisco Optical Network Controller system database backup file creation fails.

Clear the BACKUP-FAILURE Alarm

To clear this alarm:

Procedure

Step 1 Wait until the next succesful On-demand backup or scheduled backup, the backup failure alarm is cleared.

Step 2 If backup keeps failing, check the PostGRES database pod health using the **sedo system status | grep postgres** in the CLI interface by accessing the VM using SSH.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NODE-BACKUP-FAILURE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: Node-Database Backup

The NODE-BACKUP-FAILURE alarm is raised when Node backup file creation fails in Cisco Optical Site Manager.

Clear the NODE-BACKUP-FAILURE Alarm

To clear this alarm:

Procedure

Step 1 To clear this alarm:

Step 2 Wait until the next succesful On-demand backup or scheduled backup, the node backup failure alarm is cleared.

Step 3 If backup keeps failing, troubleshoot the backup creation in Cisco Optical Site Manager

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NODE-DISCONNECT

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: NODE: {Node-name}

The NODE-DISCONNECT alarm is raised when Cisco Optical Network Controller is unable to connect to a node.

Clear the NODE-DISCONNECT Alarm

To clear this alarm:

Procedure

Step 1 Check the connectivity to the node that got disconnected and fix any network issues.

Step 2 If the node went down, bring it back up.

Step 3 Check the node configuration, in the Nodes app and ensure the username and password are correct.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UPLOAD-FAILURE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: Controller system-Database Backup

The UPLOAD-FAILURE alarm is raised when Cisco Optical Network Controller system Database Backup File Upload to SFTP fails.

Clear the UPLOAD-FAILURE Alarm

To clear this alarm:

Procedure

Step 1 Wait until the next succesful upload, the upload failure alarm is cleared.

Step 2 If the uploads keep failing, check the network connectivity to the SFTP server and fix any connectivity issues.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DISK THRESHOLD

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: DISK: mount:/data

The DISK-THRESHOLD alarm is raised when Cisco Optical Network Controller disk usage exceeds the threshold. When free space is less than 30% this alarm is raised.

Note This alarm was introduced in Cisco Optical Network Controller Release 25.1.2.

Clear the DISK-THRESHOLD Alarm

To clear this alarm:

Procedure

Step 1 Pause PM Jobs from the CONC UI

a) Go to the PM History app.
b) In the Summary tab, select the desired job and click the Edit button.

Note
Only one job can be edited at a time.

A popup window appears.
c) Use the toggle button at the top-left corner to disable the job.
This action pauses the job and prevents further PM data collection.

Step 2 Remove user created files from the `/data` directory. Remove all additional files or directories under `/data` directory.

Only the following folders are expected in the `/data` directory.

```
drwx------  2 root        root            16384 Jun 30 12:35 lost+found
drwxr-xr-x 14 root        root             4096 Jun 30 12:35 containerd
drwxr-xr-x 34 root        root             4096 Jun 30 12:39 local-path-provisioner
drwxr-xr-x  3 kube-system kube-system      4096 Jul 25 05:36 etcd
drwxr-xr-x  2 kube-system kube-system      4096 Jul 30 08:05 promtail
```

Step 3 Delete ISO Files from Local SFTP.

a) SSH into the CONC VM.
b) Get the list of all ISO files on the VM.

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

c) Delete an iso file from the list using the following command.

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

Step 4 Download and Remove Archive Files from CONC UI

a) Go to the Logs app.
Under the Archives tab, there is the list of all available archive files.
b) Click **Download** in the **Action** column to save the file locally.
c) Click **Delete** in the **Action** column to delete an archive file.

Step 5 When the freespace is more than 30%, the alarm gets cleared within 5 minutes.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SWITCHOVER

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: CLUSTER

The SWITCHOVER alarm is raised when Cisco Optical Network Controller CLUSTER switchover has occurred.

Clear the SWITCHOVER Alarm

This alarm clears automatically once the switchover is complete and database replication is complete.

Procedure

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAILOVER

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: CLUSTER

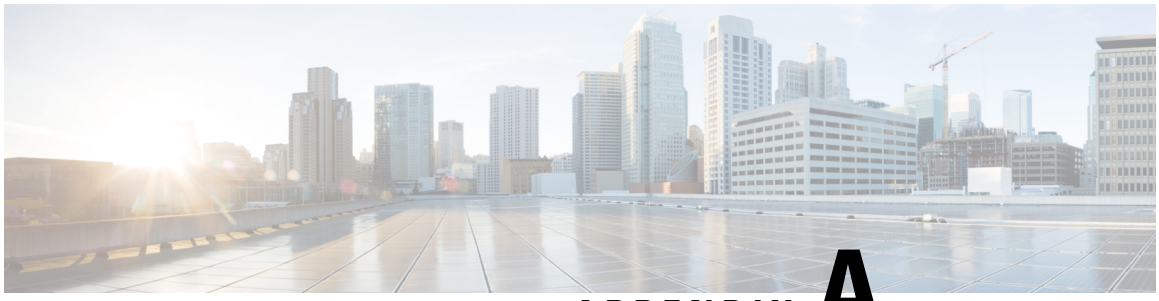
The FAILOVER alarm is raised when Cisco Optical Network Controller CLUSTER failover has occurred.

Clear the FAILOVER Alarm

This alarm clears automatically once the failover is complete and database replication is complete.

Procedure

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).



APPENDIX A

Alarm categories

Cisco Optical Network Controller classifies alarms under these categories:

- SYSTEM
- EQUIPMENT
- MAINTENANCE
- CONC_SYSTEM
- TRANSPORT
- PROTECTION
- TIMING
- SECURITY
- OPTICAL
- TCA

You may see the following alarm categories:

- **UNKNOWN**: When Cisco Optical Network Controller receives an alarm from Cisco Optical Site Manager that is not in the following list.
- **NA**: This category is displayed when Cisco Optical Network Controller has an internal issue and cannot get the category info

Severity and Impact abrevations

These abbreviations are used in the Severity and Impact columns of the alarms table in this chapter:

Severity

- NA – Not Alarmed
- CR – Critical
- MN – Minor
- MJ – Major

Impact

- SA – Service Affecting
- NSA – Not Service Affecting

SYSTEM alarm details

This table lists the alarm details for the SYSTEM category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AUD-ARCHIVE-FAIL	Archival of Audit Log Failed	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
AUD-LOG-LOSS	Audit Log 100 Percent Full - Oldest records will be lost	NA	NSA	Alarm	NE SYSTEM/NCS2K/SYSTEM
AUD-LOG-LOW	Audit Log 80 Percent Full	NR	NSA	Alarm	NE/NCS2K
BAD-DB-DETECTED	Bad Database Detected And Database Load Failed	CR	SA	Alarm	NE/NCS2K
BAND-PARTNER-NODE-UNPAIRED	Node is unpaired from band partner node	NA	NSA	Alarm	CARD/NCS1K
COMMIT-REPLACE-FAILED	Configuration commit replace failed	MJ	SA	Alarm	NE/NCS1K
CONFIG-INCONSISTENCY	Configuration is in inconsistent state	CR	SA	Alarm	NE/NCS1K
CP-UNVER-CLEARED	Control Plane Unverified Cleared Alarms Present	CR	SA	Alarm	NE/NCS2K
DATAFLT	Software Fault - Data Integrity Fault	MN	NSA	Alarm	NE/NCS2K
DBBACKUP-FAIL	Database Backup Failed	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
DBBACKUP-IN-PROGRESS	Database Backup In Progress	–	–	Alarm	SYSTEM/SYSTEM
DBOSYNC	Standby Database Out of Sync	MJ	SA	Alarm	NE/NCS2K
DBREST-IN-PROGRESS	Database Restore In Progress	no result	–	Alarm	SYSTEM/SYSTEM
DBRESTORE-FAIL	Database Restore Failed	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
DEGREE-MISMATCH	Degree Mismatch	–	–	Alarm	OPT/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
DISK-SPACE-FULL	No Space Left On Device	CR	SA	Alarm	SYSTEM/SYSTEM
DISK-SPACE-LOW	Low Disk Space Remaining On Device	CR	SA	Alarm	SYSTEM/SYSTEM
DR-UNAVAILABLE	Disaster recovery boot is currently unavailable due to a missing or corrupted chassis SSD. If an install transaction is in progress, this cannot be cleared until the transaction is completed	CR	SA	Alarm	SHELF/NCS1K
DUP-IPADDR	IP Address A1ready In Use Within The Same DCC Area	MN	NSA	Alarm	NE/NCS2K
DUP-NODENAME	Node name already in use within the same DCC Area	MN	NSA	Alarm	NE/NCS2K
DUP-SHELF-ID	Duplicated Shelf Identifier	MJ	SA	Alarm	SHELF/NCS2K
EVAL-LIC	Evaluation License Is In Use	MN	NSA	Alarm	CARD/NCS2K
EXT	Failure Detected External To The NE	MN	NSA	Alarm	ENVALRM/NCS2K
HELLO	OSPF Hello Fail	MN	NSA	Alarm	OPT OTUk OCn STMn ETH/NCS2K
INSTALL-IN-PROGRESS	SW Installation In Progress	NA	NSA	Alarm	CARD/NCS1K
INVALID-SYSDB	Invalid System DB	MN	NSA	Alarm	CARD/NCS2K
INVMACADR	Invalid MAC Address	MN	NSA	Alarm	BACKPLANE/NCS2K
LCMODE-CONFIG-CHANGED	LCMODE changed, delete the datapath config and reload line card	MJ	NSA	Alarm	CARD/NCS1K
LCMODE-CONFIG-INVALID	LC Mode Configuration Invalid	CR	SA	Alarm	CARD/NCS1K
LCMODE-NOT-CONFIG	LC Mode Configuration Not Applied	MJ	SA	Alarm	CARD/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LIC-COMM-FAIL	Communications Failure With Cisco Licensing Cloud	MJ	NSA	Alarm	CARD SHELF/NCS1K
LIC-EXPIRED	License Expired	CR	SA	Alarm	CARD/NCS2K
LIC-EXPIRING-SHORTLY	License Will Expire Within 24 Hours	MJ	SA	Alarm	CARD/NCS2K
LIC-EXPIRING-SOON	License Will Expire At Any Time After 1 Day But Before 14 Days	MJ	SA	Alarm	CARD/NCS2K
LIC-MISSING	License Is Missing	CR	SA	Alarm	CARD/NCS2K
LIC-OUT-OF-COMPL	One Or More Entitlements Are Out Of Compliance	MJ	–	Alarm	CARD SHELF/NCS1K
LIC-SIA-OF-COMPL-UPGRADE-BLOCKED	SW Upgrade will be blocked as SIA Grace Period has expired	MJ	SA	Alarm	CARD SHELF/NCS1K
LIC-SIA-OUT-OF-COMPL-GP-REM	SW Upgrade is still allowed as SIA Grace Period is remaining	MN	NSA	Alarm	CARD SHELF/NCS1K
LIC-UPGRADE-OF-COMPL-UPGRADE-BLOCKED	SW Upgrade will be blocked as Upgrade License Grace Period has expired	MJ	SA	Alarm	CARD SHELF/NCS1K
LIC-UPGRADE-OUT-OF-COMPL-GP-REM	SW Upgrade is still allowed as Upgrade License Grace Period is remaining	MJ	SA	Alarm	CARD SHELF/NCS1K
LINK-BROKEN	Ha link Broken	MJ	SA	Alarm	SYSTEM/SYSTEM
LOGIN-MISSING-GROUP	Missing Authorization Group Information	–	–	Event	SYSTEM/SYSTEM
NE-CONFIG-INCONSISTENT	Device has the Config Blocked due to an Inconsistency	–	–	Event	NE/SYSTEM
NE-DISCONNECTED	Connection To Managed NE Lost	MJ	SA	Alarm	NE/SYSTEM
NE-EVENT-DISCONNECTED	Event Channel To Managed NE Lost	MJ	SA	Alarm	NE/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
NE-NOT-AUTH-ACCESS	Not Authorised Access To Managed NE	MJ	–	Alarm	NE/SYSTEM
NE-VER-NOT-SUPP	Not Supported Version Of Managed NE	MJ	SA	Alarm	NE/SYSTEM
NEIGHBOUR-MISSING	Neighbour not found	MN	NSA	Alarm	OPT/NCS1K
NO-VALID-USB-DB	No Valid USB DB exists	MN	NSA	Alarm	USB_FLASH/NCS2K
NODE-FACTORY-MODE	Node in Factory Mode	CR	–	Alarm	NE/NCS2K
NODE-INCONSISTENCIES	Owner and/or partner packages on at least one node do not match the active RP	MJ	–	Alarm	NE/NCS1K
OTN-XP-DP-FPD-PKG-MISSING	OTN XP Data Plane FPD Package Missing	NA	NSA	Alarm	CARD/NCS1K
PATCH-ACTIVATION-FAILED	Patch Activation Failed	CR	SA	Alarm	CARD/NCS2K
PATCH-DOWNLOAD-FAILED	Patch Download Failed	CR	SA	Alarm	NE/NCS2K
PROV-FAILED	Provisioning Failed	–	–	Alarm	CARD OPT/NCS1K
PROV-INPROGRESS	Provisioning In Progress	–	–	Alarm	SHELF CARD PPM ODUk OCH OPT OTUk/NCS1K
RESOURCES-LOW	Running Low On Resources	–	–	Alarm	CARD/NCS2K
ROLE-SWITCH-ACTIVE	Role is Switched to active	–	–	Event	SYSTEM/SYSTEM
ROUTE-OVERFLOW	OSPF Routing Table Overflow	MN	NSA	Alarm	NE/NCS2K
SFTWDOWN	Software Download In Progress	MN	NSA	Alarm	NE/NCS2K
SFTWDOWN-FAIL	Software Download Failed	MN	NSA	Alarm	NE/NCS2K
SNTP-HOST	NTP/SNTP Host Failure	MN	NSA	Alarm	NE CARD SYSTEM/NCS2K/ NCS2K-SVO-K9/SYSTEM
SOFT-VERIF-FAIL	Software Signature Verification Failed	CR	SA	Alarm	NE/NCS2K
SW-MISMATCH	Software Mismatch	NA	NSA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SYSBOOT	System Reboot	MJ	SA	Alarm	NE SYSTEM/NCS2K/SYSTEM
TEMP-LIC	Temporary License Is In Use	MN	NSA	Alarm	CARD/NCS2K
UNTRUSTED-APPLICATION	Trust Not Established With CSLU/CSSM	CR	NSA	Alarm	SYSTEM/SYSTEM
USAGE-NOT-REPORTED	Licenses Usage Is Not Reported	MJ	NSA	Alarm	SYSTEM/SYSTEM
WRMRESTART	Warm Restart	–	–	Event	NE/NCS2K

EQUIPMENT alarm details

This table lists the alarm details for the EQUIPMENT category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ACT-SOFT-VERIF-FAIL	Active Volume Software Signature Verification Failed	CR	SA	Alarm	CARD/NCS2K
AUTORESET	Automatic System Reset	MN	NSA	Alarm	CARD/NCS2K
AVST-FAILURE	AVST Failure	MJ	NSA	Alarm	CARD/NCS1K
AWG-DEG	AWG Temperature Degrade	MN	NSA	Alarm	OPT/NCS2K
AWG-FAIL	AWG Temperature Failure	CR	SA	Alarm	OPT/NCS2K
AWG-OVERTEMP	AWG Over-Temperature	CR	SA	Alarm	OPT/NCS2K
AWG-WARM-UP	AWG Warm Up	NA	NSA	Alarm	OPT/NCS2K
BAT-FAIL	Battery Failure	MJ	SA	Alarm	PWR/NCS2K
BIOS-IMAGE-CORRUPTION	BIOS image corruption	MJ	NSA	Alarm	CARD/NCS1K
BKUPMEMP	Primary Non-Volatile Backup Memory Failure	CR	NSA	Alarm	CARD USB_FLASH/NCS2K
BP-FPGA-IMAGE-CORRUPTION	BP FPGA Image Corruption	MJ	NSA	Alarm	CARD/NCS1K
BP-FPGA-PCIE-ERROR	BP FPGA PCIE Error	MJ	SA	Alarm	CARD/NCS1K
BP-FPGA-XR-EP-FPGA-PCIE-ERROR	BP FPGA XR EP FPGA PCIe Error	MJ	NSA	Alarm	CARD/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
CARD-IS-SHUTDOWN	Card failed to come up after multiple recovery attempts	CR	SA	Alarm	CARD/NCS1K
CARD-UNREACHABLE	RemoteCard Not Reachable For Key Exchange. Retrying ...	CR	SA	Alarm	PORT/NCS2K
CASETEMP-DEG	Case Temperature Degrade	MN	NSA	Alarm	OPT/NCS2K
CLDRESTART	Cold Restart	NA	NSA	Alarm	CARD/NCS2K
COMM-FAIL	Plug-in Module Communication Failure	MN	NSA	Alarm	CARD/NCS2K/NCS1K
COMP-CARD-MISSING	Companion Card Missing	MN	NSA	Alarm	CARD/NCS2K
CONTBUS-A-18	Controller Card A To DCC A Processor Communication Failure	MJ	NSA	Alarm	CARD/NCS2K
CONTBUS-B-18	Controller Card B To DCC B Processor Communication Failure	MN	NSA	Alarm	CARD/NCS2K
CONTBUS-CLK-A	Clock Bus Failure - Shelf Controller A	MJ	NSA	Alarm	CARD/NCS2K
CONTBUS-CLK-B	Clock Bus Failure - Shelf Controller B	MJ	NSA	Alarm	CARD/NCS2K
CONTBUS-DISABLED	Slot Communication Disabled	CR	SA	Alarm	CARD/NCS2K
CONTBUS-IO-A	Peer To Peer Slot Communication Failure	MN	NSA	Alarm	CARD/NCS2K
CONTBUS-IO-B	Peer To Peer Slot Communication Failure	MN	NSA	Alarm	CARD/NCS2K
COOL-MISM	Cooling Profile Mismatch	NR	SA	Alarm	FAN_TRAY/NCS2K
CPP-INCAPABLE	Card/Ports Unable To Provide Protection	NA	NSA	Alarm	CARD/NCS2K
CPU-FPGA-PCIE-ERROR	CPU FPGA PCIe Error	MJ	NSA	Alarm	CARD/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
DSP-COMM-FAIL	DSP Communication Failure	MJ	SA	Alarm	OCH/NCS2K
DSP-FAIL	DSP Failure	MJ	SA	Alarm	OCH/NCS2K
EHIBATVG	Extreme High Volt	MJ	SA	Alarm	PWR/NCS2K
ELWBATVG	Extreme Low Volt	MJ	SA	Alarm	PWR/NCS2K
EPROM-SUDI-SN-MISMATCH	Card Serial Number and Certificate Serial Number Mismatch	MJ	NSA	Alarm	CARD/NCS2K
EQPT	Equipment Failure	CR	SA	Alarm	CARD ECU LCD_FLASH PPM/NCS2K
EQPT-DEGRADE	Equipment Degrade	MN	NSA	Alarm	CARD/NCS2K/NCS1K
EQPT-DIAG	Diagnostic Failure	CR	SA	Alarm	CARD/NCS2K
EQPT-FAIL	Board Failure	MJ	SA	Alarm	CARD PPM NE/NCS2K/NCS1K
EQPT-FPGA-IMAGE-AVAILABLE	Different FPGA Image Available	NR	NSA	Alarm	CARD/NCS2K
EQPT-MISS	Replaceable Equipment/Unit is Missing	CR	SA	Alarm	CARD FAN_TRAY ECU LCD_FLASH PWR/NCS2K
ETH-LINKLOSS	Rear Panel Ethernet Link Removed	NA	NSA	Alarm	NE/NCS2K
FAN	Fan Failure	CR	SA	Alarm	FAN_TRAY/NCS2K/NCS1K
FAN-OUT-OF-TOLERANCE	Fan Out of tolerance	MN	NSA	Alarm	FAN_TRAY FAN_ENV/NCS1K
FAN-POWER-ERROR	FAN tray Power Error	MJ	NSA	Alarm	FAN_TRAY/NCS1K
FAN-SENSOR-FAILED	Sensor in failed state	MJ	SA	Alarm	FAN_TRAY FAN_ENV/NCS1K
FANDEGRADE	Partial Fan Failure	MN	NSA	Alarm	FAN_TRAY/NCS2K/NCS1K
FEED-MISMATCH	Feed Not Available/Improper Connection	MN	NSA	Alarm	PWR/NCS2K
FIBERTEMP-DEG	Fiber Temperature Degrade	MN	NSA	Alarm	OPT/NCS2K
FIRMWARE-DOWNLOAD	Firmware Download In Progress	–	–	Event	CARD PPM/NCS2K
FIRMWARE-UPG	Firmware Upgrade In Progress	NA	NSA	Alarm	CARD PPM/NCS2K
FIRMWARE-UPG-COMPLETE	Firmware Upgrade Completed	–	–	Event	CARD PPM/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
FIRMWARE-UPG-FAIL	Firmware Upgrade Failed	MJ	SA	Alarm	CARD PPM/NCS2K
FLASH0-ERROR	CPU Flash 0 Error	MJ	NSA	Alarm	CARD/NCS1K
FLASH1-ERROR	CPU Flash 1 Error	MJ	NSA	Alarm	CARD/NCS1K
FPD-UPG-REQUIRED	Firmware upgrade required	MJ	NSA	Alarm	PPM CARD SHELF FAN_TRAY PWR/NCS2K/NCS1K
FPGA-ERROR	BP FPGA Error	MJ	NSA	Alarm	CARD/NCS1K
FPGA-SEU-UNCORR	BP FPGA SEU Uncorrected Error	CR	SA	Alarm	CARD/NCS1K
FPGA-UPGRADE-FAILED	FPGA Upgrade fail	CR	SA	Alarm	CARD/NCS2K/NCS1K
FTA-MISMATCH	FanTray Mismatch	NA	NSA	Alarm	CARD/NCS2K
HI-LASERBIAS	Equipment High Laser Bias	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
HI-LASERTEMP	Equipment High Laser Temp	MN	NSA	Alarm	OCH/NCS2K
HI-TXPOWER	Equipment High Tx power	MJ	SA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
HIBATVG	High Volt	CR	SA	Alarm	PWR/NCS2K
HIGH-VOLTAGE	high voltage alarm	CR	SA	Alarm	CHASSIS_ENV_VOLTAGE MODULE_ENV_VOLTAGE/NCS1K
HITEMP	High Temperature	CR	SA	Alarm	CARD/NCS2K
HITEMP	High Temperature	NA	NSA	Alarm	NE/NCS2K
I-HITEMP	Industrial High Temperature	NA	NSA	Alarm	NE/NCS2K
IMPROPRMVL	Improper Removal	MN	NSA	Alarm	CARD PPM PORT SHELF FAN_TRAY/NCS2K /NCS2K-SVO-K9/SYSTEM/NCS1K
IMPROPRMVL-FS	Improper removal of Fiber Shuffle	MJ	SA	Alarm	PASSIVE_SHELF/NCS2K
INVALID-CARD-SLOT	Invalid Card Slot	MJ	NSA	Alarm	CARD/NCS1K
INVALID-SENSOR-READ-ERR	Invalid sensor read error	MN	NSA	Alarm	CHASSIS_ENV_VOLTAGE MODULE_ENV_ VOLTAGE/NCS1K
LAN-POL-REV	Lan Connection Polarity Reversed	MJ	NSA	Alarm	NE/NCS2K
LASERBIAS-DEG	Laser Bias Degrade	MN	NSA	Alarm	OCH/NCS2K
LASERBIAS-FAIL	Laser Bias Failure	CR	SA	Alarm	OCH/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LASEREOL	Laser Approaching End of Life	MJ	NSA	Alarm	OCH/NCS2K
LASERTEMP-DEG	Laser Temperature Degrade	MJ	SA	Alarm	OCH/NCS2K
LC-BOOT-TIMEOUT	LC Boot Timeout	MJ	SA	Alarm	CARD/NCS1K
LC-CPU-IMAGE-CORRUPTION	LC CPU Image Corruption	NA	NSA	Alarm	CARD/NCS1K
LC-DP-IMAGE-CORRUPTION	LC Data Plane Image Corruption	NA	NSA	Alarm	CARD/NCS1K
LC-FPD-DEV-FAILURE	CPU_MOD_FW is corrupt, system booted with golden copy	NA	NSA	Alarm	CARD/NCS1K
LC-OFFLINE-ERROR	LC Offline Error	NA	NSA	Alarm	CARD/NCS1K
LO-LASERBIAS	Equipment Low Laser Bias	MN	NSA	Alarm	OCH/NCS2K
LO-LASERTEMP	Equipment Low Laser Temp	MN	NSA	Alarm	OCH/NCS2K
LO-TXPOWER	Equipment Low Tx power	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
LOW-VOLTAGE	low voltage alarm	CR	SA	Alarm	CHASSIS_ENV_VOLTAGE MODULE_ENV _VOLTAGE/NCS1K
LSC-NOT-PRESENT-MIC-IN-USE	LSC not present using MIC	MJ	NSA	Alarm	CARD/NCS2K
LWBATVG	Low Volt	MJ	SA	Alarm	PWR/NCS2K
MB-SSD-ATA-ERRORS	Motherboard SSD ATA Errors	CR	SA	Alarm	CARD/NCS1K
MEA	Mismatch Of Equipment And Attributes	CR	SA	Alarm	FAN_TRAY CARD PPM PASSIVE_UNIT/ NCS2K/NCS2K-SVO-K9/SYSTEM
MEA	Mismatch Of Equipment And Attributes	CR	SA	Alarm	SHELF NE PASSIVE_SHELF PORT/ NCS2K/NCS2K-SVO-K9/SYSTEM
MEM-GONE	Free Memory On Card Near Zero	MJ	SA	Alarm	CARD/NCS2K
MEM-LOW	Free Memory On Card Very Low	MN	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
MFGMEM	Manufacturing Data Memory (EEPROM) Failure	CR	SA	Alarm	FAN_TRAY ECU LCD_FLASH PWR BACKPLANE PPM/NCS2K
NODE-OBFL-ERROR	Node OBFL Error	MJ	NSA	Alarm	CARD/NCS1K
NON-CISCO-PPM	Non Cisco PPM Inserted	MN	NSA	Alarm	PPM PORT/NCS2K/NCS2K-SVO-K9
ONE-OR-MORE-FAN-TRAY-ABSENT	One or more Fan Trays missing	MJ	NSA	Alarm	SHELF/NCS1K
ONE-OR-MORE-LC-MISSING	One or more LCs missing, running fans at max speed	CR	SA	Alarm	SHELF/NCS1K
OPEN-SLOT	Open Slot(s)	MN	NSA	Alarm	CARD SHELF/NCS2K
OPT-MOD-ABSENT	One or more Optical Modules missing	CR	SA	Alarm	CARD/NCS1K
OVER-TEMP-UNIT-PROT	Over Temperature Unit Protected	CR	SA	Alarm	OCH/NCS2K
PEX-SWITCH-ACCESS-FAILURE	PEX Switch Access Failure	MJ	NSA	Alarm	CARD/NCS1K
PORT-COMM-FAIL	Module Communication Failure	CR	SA	Alarm	PORT/NCS2K
POWER-MODULE-FAN-OUT-OF-TOLERANCE	Power Module: fan out of tolerance	MN	NSA	Alarm	PWR/NCS1K
POWER-MODULE-FAN-OUT-OF-TOLERANCE-WARNING	Power Module Warning: fan out of tolerance	MN	NSA	Alarm	PWR/NCS1K
POWER-MODULE- OUTPUT-DISABLED	Power Module Output Disable	MJ	SA	Alarm	PWR/NCS1K
POWER-MODULE- REDUNDANCY-LOST	Power Module Redundancy lost	MJ	SA	Alarm	PWR SHELF/NCS1K
POWER-OFF	Card In Power Off Status	MJ	NSA	Alarm	CARD/NCS1K
POWER-ON-TIMEOUT	Card In Power On Timeout	MJ	NSA	Alarm	CARD/NCS1K
PPM-MISMATCH	Incompatible pluggable inserted in the port	CR	SA	Alarm	PPM/NCS1K
PROTNA	Protection Unit Not Available	MN	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
PROV-INCOMPATIBLE	Incompatible Provision	–	–	Alarm	CARD/NCS1K
PROV-MISMATCH	Provisioning Mismatch	MN	NSA	Alarm	PORT/NCS2K/ NCS2K-SVO-K9/SYSTEM/NCS1K
PROV-MISMATCH	Provisioning Mismatch	MN	NSA	Alarm	CARD PPM/NCS2K/ NCS2K-SVO-K9/SYSTEM/NCS1K
PWR	Power Failure at Connector	–	–	Alarm	PWR/NCS2K
PWR-CON-LMT	Power Consumption Limit Has Crossed	MN	NSA	Alarm	SHELF/NCS2K
PWR-ERROR	Power Module Error (PM_VIN_VOLT_OOR)	–	–	Alarm	SHELF/NCS1K
PWR-EXCEEDS	Power reservation exceeds configured power	–	–	Alarm	PWR/NCS1K
PWR-EXCEEDS-CAPACITY	Power reservation exceeds configured power capacity	–	–	Alarm	PWR/NCS1K
PWR-FAIL-A	Equipment power failure at connector A	MN	NSA	Alarm	PWR/NCS2K
PWR-FAIL-B	Equipment power failure at connector B	MN	NSA	Alarm	PWR/NCS2K
PWR-FAIL-RET-A	Equipment power failure at return connector A	MN	NSA	Alarm	PWR/NCS2K
PWR-FAIL-RET-B	Equipment power failure at return connector B	MN	NSA	Alarm	PWR/NCS2K
PWR-GRP-REDUNDANCY-LOST	Power Group Redundancy lost	MJ	SA	Alarm	SHELF/NCS1K
PWR-MISMATCH	PEM PID mismatch in the chassis	–	–	Alarm	SHELF/NCS1K
PWR-OUTPUT-DISABLED	Power Module Output Disabled	MJ	SA	Alarm	SHELF/NCS1K
PWRRESTART	Powerfail Restart	–	–	Alarm	NE/NCS2K
RACK-OBFL-ERROR	Obfl error	MJ	NSA	Alarm	SHELF/NCS1K
RESOURCE-ALLOC-FAIL	Resource Allocation Failed	MN	SA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
RESOURCES-GONE	No More Resources Available	MN	NSA	Alarm	CARD/NCS2K
RUNNING-FANS-AT-MAX-SPEED	FANs Running At Maximum Speed	CR	SA	Alarm	FAN_TRAY/NCS1K
SENSOR-HIGH-0-6V-CPU-A	0.6V-CPU-A sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-0-6V-CPU-B	0.6V-CPU-B sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-05V-CPU	1.05V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-0V	1.0V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-0V-PHY	1.0V-PHY sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-2V	1.2V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-2V-CPU	1.2V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-3V-CPU	1.3V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-5V-CPU	1.5V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-7V-CPU	1.7V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-82V-CPU	1.82V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-8V	1.8V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-2-5V	2.5V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-3-3V	3.3V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-3-3V-CPU	3.3V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-3-3V-STBY	3.3V-STBY sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-5-0V-STBY	5.0V-STBY sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-BP-48V	BP-48V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-CPU-TEMP	CPU-TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SENSOR-HIGH-DDR-CH0-TEMP	DDR-CH0- TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-DDR-CH1-TEMP	DDR-CH1- TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-ETHERNET -SWITCH-TEMP	ETHERNET-SWITCH-TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-HOTSPOT1	HOTSPOT1 sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-HOTSPOT2	HOTSPOT2 sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-INLET-AIR	INLET-AIR sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-OUTLET-AIR	OUTLET-AIR sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-0-6V-CPU-A	0.6V-CPU-A sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-0-6V-CPU-B	0.6V-CPU-B sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-05V-CPU	1.05V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-0V	1.0V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-0V-PHY	1.0V-PHY sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-2V	1.2V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-2V-CPU	1.2V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-3V-CPU	1.3V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-5V-CPU	1.5V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-7V-CPU	1.7V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-82V-CPU	1.82V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-8V	1.8V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-2-5V	2.5V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-3-3V	3.3V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-3-3V-CPU	3.3V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-3-3V-STBY	3.3V-STBY sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SENSOR-LOW-5-0V-STBY	5.0V-STBY sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-BP-48V	BP-48V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-CPU-TEMP	CPU-TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-DDR-CH0-TEMP	DDR-CH0- TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-DDR-CH1-TEMP	DDR-CH1- TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-ETHERNET-SWITCH-TEMP	ETHERNET-SWITCH-TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-HOTSPOT1	HOTSPOT1 sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-HOTSPOT2	HOTSPOT2 sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-INLET-AIR	INLET-AIR sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-OUTLET-AIR	OUTLET-AIR sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SHELF-COMM-FAIL	Shelf Communication Failure	MJ	SA	Alarm	SHELF/NCS2K
SSD-ATA-ERRORS	CPU SSD ATA Error	CR	SA	Alarm	CARD/NCS1K
SSD-HI-TEMP	CPU SSD High Temperature	MJ	NSA	Alarm	CARD/NCS1K
TEMP-MISM	Temperature Reading Mismatch Between SC Cards	NA	NSA	Alarm	NE/NCS2K
TEMPERATURE	Temperature out of working range	CR	SA	Alarm	CHASSIS_ENV_TEMPERATURE MODULE_ENV_TEMPERATURE PWR_ENV_TEMPERATURE/NCS1K
TRAF-AFFECT-RESET-REQUIRED	Traffic Affecting Reset Required	MN	NSA	Alarm	CARD/NCS2K
TRAF-AFFECT-SEC-UPG-REQUIRED	Traffic Affecting Security Upgrade Required	NR	NSA	Alarm	CARD/NCS2K
UNIT-HIGH-TEMP	Unit High Temperature	MN	NSA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
UNQUAL-PPM	Unqualified PPM Inserted	NR	NSA	Alarm	PPM PORT/NCS2K/ NCS2K-SVO-K9/NCS1K
USB-MOUNT-FAIL	USB Mount Failure	CR	SA	Alarm	USB_FLASH/NCS2K
USB-OC-1	USB 1 Over Current	MJ	NSA	Alarm	USB_FLASH/NCS1K
USB-OC-2	USB 2 Over Current	MJ	NSA	Alarm	USB_FLASH/NCS1K
USB-PORTS-DOWN	USB Ports in ECU are not functional	–	–	Event	ECU/NCS2K
USB-WRITE-FAIL	USB Write Failure	CR	SA	Alarm	USB_FLASH/NCS2K
USBSYNC	USB Sync in Progress	NA	NSA	Alarm	USB_FLASH/NCS2K
VOLT-MISM	Voltage Reading Mismatch Between SC Cards	NA	NSA	Alarm	PWR/NCS2K/NCS1K
XGE-EEPROM-ERROR	XGE EEPROM Error	MJ	SA	Alarm	CARD/NCS1K
XGE-FLASH-ERROR	XGE Flash Error	–	–	Alarm	CARD/NCS1K

MAINTENANCE alarm details

This table lists the alarm details for the MAINTENANCE category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AS-CMD	Alarms Suppressed By User Command	NA	NSA	Alarm	OCH ETH OCn STMn ODUk OTUk zrPlus OPT OXC CARD FC PASSIVE_SHELF PORT PPM RAMAN_AMPLIFIER SHELF/NCS2K
AS-MT	Alarms Suppressed For Maintenance	NA	NSA	Alarm	OCH ETH OCn STMn ODUk OTUk zrPlus OPT OXC CARD FC PASSIVE_SHELF PORT PPM RAMAN_AMPLIFIER SHELF/NCS2K/NCS1K
BP-LPBKFACILITY	Back-panel Facility Loopback	NA	NSA	Alarm	CARD/NCS2K
BP-LPBKTERMINAL	Back-panel Terminal Loopback	NA	–	Alarm	CARD/NCS2K
IPC-LASER-FAIL	Ipc Laser failure	MN	NSA	Alarm	CARD/NCS2K
IPC-LOOPBACK-MISS	Patchcords Verification Loopback Missing	MJ	NSA	Alarm	OPT OXC/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
IPC-VERIFICATION-DEGRADE	Patchcords Verification Degrade	NA	NSA	Alarm	SYSTEM/NCS2K
IPC-VERIFICATION-EXCESSIVE-LOSS	Measured Patchcord Loss above the Threshold	MJ	SA	Alarm	SYSTEM/NCS1K
IPC-VERIFICATION-FAIL	Patchcords Verification Failure	MJ	SA	Alarm	SYSTEM/NCS2K
IPC-VERIFICATION-RUNNING	Patchcords Verification Running	NA	NSA	Alarm	SYSTEM/NCS2K
LPBKFACILITY	Facility Loopback	NA	NSA	Alarm	OCn STMn ETH zrPlus OTUk ODUk OCH OPT/NCS2K/NCS1K
LPBKTERMINAL	Terminal Loopback	NA	NSA	Alarm	OCn STMn ETH zrPlus OTUk ODUk OCH OPT/NCS2K/NCS1K
MANRESET	Manual System Reset	NA	NSA	Alarm	CARD/NCS2K
OCHNC-MT	OCHNC Maintenance	MN	–	Alarm	OXC/NCS2K
OTDR-ABSOLUTE-A-EXCEEDED-RX	Attenuation Exceeded Absolute Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ABSOLUTE-A-EXCEEDED-TX	Attenuation Exceeded Absolute Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ABSOLUTE-R-EXCEEDED-RX	Reflectance Exceeded Absolute Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ABSOLUTE-R-EXCEEDED-TX	Reflectance Exceeded Absolute Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-BASELINE-A-EXCEEDED-RX	Attenuation Exceeded Baseline Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-BASELINE-A-EXCEEDED-TX	Attenuation Exceeded Baseline Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-BASELINE-R-EXCEEDED-RX	Reflectance Exceeded Baseline Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
OTDR-BASELINE-R-EXCEEDED-TX	Reflectance Exceeded Baseline Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-FAST-FAR-END-IN-PROGRESS	OTDR Fast Scan Is In Progress On Remote Side	MN	NSA	Alarm	OTDR/NCS2K
OTDR-FAST-SCAN-IN-PROGRESS-RX	OTDR Fast Scan Is In Progress - RX Direction	MN	NSA	Alarm	OPT/NCS2K
OTDR-FAST-SCAN-IN-PROGRESS-TX	OTDR Fast Scan Is In Progress - TX Direction	MN	NSA	Alarm	OPT/NCS2K
OTDR-FIBER-END-NOT-DETECTED-RX	Fiber End Not Detected - RX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-FIBER-END-NOT-DETECTED-TX	Fiber End Not Detected - TX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-HYBRID-FAR-END-IN-PROGRESS	OTDR Hybrid Scan Is In Progress On Remote Side	NA	NSA	Alarm	OTDR/NCS2K
OTDR-HYBRID-SCAN-IN-PROGRESS-RX	OTDR Hybrid Scan Is In Progress - RX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-HYBRID-SCAN- IN-PROGRESS-TX	OTDR Hybrid Scan Is In Progress - TX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-LOSS-THR-EXCEEDED	OTDR Loss Threshold Exceeded	CR	NSA	Alarm	OTDR/NCS2K
OTDR-ORL-THRESHOLD-EXCEEDED-RX	ORL Exceeded Threshold - RX Direction	MN	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ORL-THRESHOLD-EXCEEDED-TX	ORL Exceeded Threshold - TX Direction	MN	–	Alarm	OPT/NCS2K/NCS1K
OTDR-ORL-TRAINING-FAILED-RX	ORL Training Failed - RX Direction	MN	–	Alarm	OPT/NCS2K
OTDR-ORL-TRAINING-FAILED-TX	ORL Training Failed - TX Direction	MN	–	Alarm	OPT/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
OTDR-ORL-TRAINING-IN-PROGRESS-RX	ORL Training Is In Progress - RX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-ORL-TRAINING-IN-PROGRESS-TX	ORL Training Is In Progress - TX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-OTDR-TRAINING- FAILED-RX	OTDR Training Failed - RX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-OTDR-TRAINING- FAILED-TX	OTDR Training Failed - TX Direction	NA	NSA	Alarm	OPT/NCS2K
OTDR-SCAN-FAILED	OTDR Scan Failed	MJ	NSA	Alarm	OTDR/NCS2K
OTDR-SCAN-FAILED-RX	OTDR Scan Failed RX	MJ	NSA	Alarm	OPT/NCS1K
OTDR-SCAN-FAILED-TX	OTDR Scan Failed TX	MJ	NSA	Alarm	OPT/NCS1K
OTDR-SCAN-IN-PROGRESS	OTDR Scan Is In Progress	MN	NSA	Alarm	OTDR/NCS2K
OTDR-SCAN-IN-PROGRESS-RX	OTDR Scan In Progress RX	MN	NSA	Alarm	OPT/NCS1K
OTDR-SCAN-IN-PROGRESS-TX	OTDR Scan In Progress TX	MN	NSA	Alarm	OPT/NCS1K
OTDR-SCAN-NOT-COMPLETED	OTDR Scan Not Completed	MN	NSA	Alarm	OTDR/NCS2K
TD-FAILED	Tone Detection Failed	–	–	Event	OPT/NCS1K
TD-INPROGRESS	Tone Detection In Progress	MN	NSA	Alarm	OPT/NCS1K
TD-LASER-ON	Tone Detection Laser is ON	–	–	Event	OPT/NCS1K
TD-SUCCESS	Tone Detection Success	–	–	Event	OPT/NCS1K
TG-INPROGRESS	Tone Generation In Progress	MN	NSA	Alarm	OPT/NCS1K

CONC_SYSTEM alarms details

This table lists the alarm details for the CONC_SYSTEM category.

Table 50: CONC_SYSTEM alarms details

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
NODE-DISCONNECT	Controller system disconnected from node	MJ	NSA	Alarm	NODE/NA
BACKUP-FAILURE	Controller system Database Backup Creation is failed	MJ	NSA	Alarm	Controller system/NA
UPLOAD-FAILURE	Controller system Database Backup File Upload to SFTP is failed.	MJ	NSA	Alarm	Controller system/NA
NODE-BACKUP-FAILURE	Node Database Backup creation failed.	MJ	NSA	Alarm	Controller system/NA
DISK-THRESHOLD	Disk usage exceeded the threshold. Free space is now under 30%.	CR	NSA	Alarm	DISK: mount:/data/NA

TRANSPORT alarm details

This table lists the alarm details for the TRANSPORT category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AIS	Alarm Indication Signal	NR	NSA	Alarm	OCn/NCS2K
AIS-L	Alarm Indication Signal Line	NR	NSA	Alarm	OCn/NCS2K/NCS1K
APS-PROV-MISM	APS Protection Type Mismatch	MN	NSA	Alarm	ODUk/NCS2K
AUTH-EC	Payload Authentication Error Count	MJ	NSA	Alarm	ODUk/NCS2K
B-AUTH-EC	Backward Auth Error Count	MJ	NSA	Alarm	ODUk/NCS2K
BDI	Backward Defect Indication	NR	NSA	Alarm	OXC/NCS2K
BERT-ENBL	BERT Enabled	NR	NSA	Alarm	OCn STMn OTUk/NCS2K
DEG-SER	FEC Degraded Symbol Error Rate	–	–	Event	ETH/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ENC-CERT-EXP	MIC cert is expired switch to LSC	MN	NSA	Alarm	ODUk/NCS2K
EOC	SDCC Termination Failure	MJ	NSA	Alarm	OPT OCn/NCS2K
EOC-E	Ethernet OSC Termination Failure	MN	NSA	Alarm	ETH/NCS2K
EOC-L	Line DCC Termination Failure	MN	NSA	Alarm	OCn/NCS2K
FC-DE-NES	Fibre Channel Distance Extension Function Not Established	MJ	SA	Alarm	FC/NCS2K
FC-NO-CREDITS	Fibre Channel Distance Extension Credit Starvation	MJ	SA	Alarm	FC/NCS2K
FEC-MISM	FEC Mismatched	MJ	SA	Alarm	OTUk/NCS1K
FLEXO-GIDM	FlexO Group Identification Mismatch	CR	SA	Alarm	OTUk OCH/NCS1K
FLEXO-LOF	FlexO Loss of Frame	CR	SA	Alarm	OTUk OCH/NCS1K
FLEXO-LOM	FlexO Loss of MultiFrame	CR	SA	Alarm	OTUk OCH/NCS1K
FLEXO-MM	FlexO Map Mismatch	CR	SA	Alarm	OTUk OCH/NCS1K
FLEXO-RDI	FlexO Remote Defect Indicator	NR	SA	Alarm	OTUk OCH/NCS1K
FOIC-GIDM	FOIC Group ID mismatch defect	MJ	SA	Alarm	zrPlus/NCS2K
FOIC-LDI-LD	FOIC Link Degrade indicator - Local Degrade	MN	NSA	Alarm	zrPlus/NCS2K
FOIC-LDI-RD	FOIC Link Degrade indicator- Remote Degrade	MN	NSA	Alarm	zrPlus/NCS2K
FOIC-LOF-LOM	FOIC Loss of Frame loss of Multiframe	CR	SA	Alarm	zrPlus/NCS2K
FOIC-LOL	FOIC Loss of Lock Detect	CR	SA	Alarm	zrPlus/NCS2K
FOIC-LOM	FOIC Loss of Multiframe Indication	CR	SA	Alarm	zrPlus/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
FOIC-PMM	FOIC Phy Map mismatch Alarm	MN	SA	Alarm	zrPlus/NCS2K
FOIC-RPF	FOIC Remote Phy Fault Detect	MN	SA	Alarm	zrPlus/NCS2K
FOIC-TIM	FOIC Trail Trace Identifier Mismatch	CR	SA	Alarm	zrPlus/NCS2K
GCC-EOC	GCC Termination Failure	MN	NSA	Alarm	OTUk/NCS2K
GE-OOSYNC	GigaBit Ethernet Out of Sync	CR	SA	Alarm	ETH/NCS2K
GFP-CSF	GFP Client Signal Fail Detected	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-CSF-SIGLOSS	GFP Client Signal Fail Detected Due To Sigloss	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-CSF-SYNCLOSS	GFP Client Signal Fail Detected Due To Syncloss	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-DE-MISMATCH	GFP Fibre Channel Distance Extension Mismatch	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-EX-MISMATCH	GFP Extension Header Mismatch	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-LFD	GFP Loss of Frame Delineation	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-NO-BUFFERS	GFP Fibre Channel Distance Extension Buffer Starvation	MJ	SA	Alarm	GFP/NCS2K/NCS1K
GFP-UP-MISMATCH	GFP User Payload Mismatch	MJ	SA	Alarm	GFP/NCS2K/NCS1K
HI-BER	High Bit Error Rate	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
HI-SER	High Symbol Error Rate	CR	SA	Event	ETH/NCS1K
IDLE	Idle Signal Condition	CR	SA	Alarm	ETH/NCS2K
KEY-EX-FAIL	Primary Key Exchange Failed	NA	NSA	Alarm	ODUk/NCS2K
KEY-WRITE-FAIL	Key Program On FPGA Failed	MN	NSA	Alarm	ODUk/NCS2K
LOA	Loss of Alignment	CR	SA	Alarm	OCH/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LOCAL-DEG-SER	Local FEC Degraded Symbol Error Rate	–	–	Event	ETH/NCS1K
LOCAL-FAULT	Local Fault	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
LOF	Loss Of Frame	CR	SA	Alarm	OCn STMn/NCS2K/NCS1K
LOF	Loss Of Frame	CR	SA	Alarm	BITS/NCS2K/NCS1K
LOM	Loss of Multi-Frame	CR	SA	Alarm	OCn STMn BITS/NCS2K/NCS1K
MAX-AUTH-LIST	Reached Max Authentication List	MJ	SA	Alarm	ODUk/NCS2K
MS-AIS	AIS - Multiplex Section - Alarm Indication Signal	NR	NSA	Alarm	STMn/NCS2K/NCS1K
MS-DEG	Multiplex Section - Signal Degraded	NA	NSA	Alarm	STMn/NCS2K
MS-EOC	Multiplex Section DCC Termination Failure	MN	NSA	Alarm	STMn/NCS2K
MS-EXC	Multiplex Section - Excessive Errors	NA	NSA	Alarm	STMn/NCS2K
MS-RDI	RDI - Multiplex Section - Remote Defect/Alarm Indication	MJ	SA	Alarm	STMn/NCS2K/NCS1K
NO-SHARED-CIPHERS	Different Ciphers Used by Client and Server	MJ	SA	Alarm	ODUk/NCS2K
NOS	Not-Operational primitive Sequence	CR	SA	Alarm	FC/NCS1K
OCHNC-INC	Optical Channel Incomplete	MN	–	Alarm	OXC/NCS2K
OCHTERM-INC	Optical Termination Incomplete	NR	NSA	Alarm	OXC/NCS2K
ODUK-1-AIS-PM	ODUk1 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-2-AIS-PM	ODUk2 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-3-AIS-PM	ODUk3 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-4-AIS-PM	ODUk4 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-AIS-PM	ODUk: PM Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K/NCS1K
ODUK-AIS-TCM1	TCM1 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM2	TCM2 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM3	TCM3 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM4	TCM4 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM5	TCM5 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM6	TCM6 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-BDI-PM	ODUk: PM Backward Defect Indication	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-BDI-TCM1	TCM1 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM2	TCM2 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM3	TCM3 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM4	TCM4 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM5	TCM5 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM6	TCM6 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BIAE	Path Monitoring Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-BIAE-TCM1	TCM1 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-BIAE-TCM2	TCM2 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-BIAE-TCM3	TCM3 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-BIAE-TCM4	TCM4 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-BIAE-TCM5	TCM5 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-BIAE-TCM6	TCM6 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE	Path Monitoring Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE-TCM1	TCM1 Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE-TCM2	TCM2 Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE-TCM3	TCM3 Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE-TCM4	TCM4 Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE-TCM5	TCM5 Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-IAE-TCM6	TCM6 Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-LCK-PM	ODUk: Locked Defect - PM	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-LCK-TCM1	TCM1 Locked	–	–	Event	ODUk/NCS1K
ODUK-LCK-TCM2	TCM2 Locked	–	–	Event	ODUk/NCS1K
ODUK-LCK-TCM3	TCM3 Locked	–	–	Event	ODUk/NCS1K
ODUK-LCK-TCM4	TCM4 Locked	–	–	Event	ODUk/NCS1K
ODUK-LCK-TCM5	TCM5 Locked	–	–	Event	ODUk/NCS1K
ODUK-LCK-TCM6	TCM6 Locked	–	–	Event	ODUk/NCS1K
ODUK-LTC-TCM1	TCM1 Loss of Tandem Connection	–	–	Event	ODUk/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-LTC-TCM2	TCM2 Loss of Tandem Connection	–	–	Event	ODUk/NCS1K
ODUK-LTC-TCM3	TCM3 Loss of Tandem Connection	–	–	Event	ODUk/NCS1K
ODUK-LTC-TCM4	TCM4 Loss of Tandem Connection	–	–	Event	ODUk/NCS1K
ODUK-LTC-TCM5	TCM5 Loss of Tandem Connection	–	–	Event	ODUk/NCS1K
ODUK-LTC-TCM6	TCM6 Loss of Tandem Connection	–	–	Event	ODUk/NCS1K
ODUK-OCI-PM	ODUk: Open Connection Indication	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-OCI-TCM1	TCM1 Open Connection Indication	–	–	Event	ODUk/NCS1K
ODUK-OCI-TCM2	TCM2 Open Connection Indication	–	–	Event	ODUk/NCS1K
ODUK-OCI-TCM3	TCM3 Open Connection Indication	–	–	Event	ODUk/NCS1K
ODUK-OCI-TCM4	TCM4 Open Connection Indication	–	–	Event	ODUk/NCS1K
ODUK-OCI-TCM5	TCM5 Open Connection Indication	–	–	Event	ODUk/NCS1K
ODUK-OCI-TCM6	TCM6 Open Connection Indication	–	–	Event	ODUk/NCS1K
ODUK-SD-PM	ODUk: Signal Degrade	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-SD-TCM1	TCM1 Signal Degrade	–	–	Event	ODUk/NCS1K
ODUK-SD-TCM2	TCM2 Signal Degrade	–	–	Event	ODUk/NCS1K
ODUK-SD-TCM3	TCM3 Signal Degrade	–	–	Event	ODUk/NCS1K
ODUK-SD-TCM4	TCM4 Signal Degrade	–	–	Event	ODUk/NCS1K
ODUK-SD-TCM5	TCM5 Signal Degrade	–	–	Event	ODUk/NCS1K
ODUK-SD-TCM6	TCM6 Signal Degrade	–	–	Event	ODUk/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-SF-PM	ODUk: Signal Failure	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-SF-TCM1	TCM1 Signal Failure	–	–	Event	ODUk/NCS1K
ODUK-SF-TCM2	TCM2 Signal Failure	–	–	Event	ODUk/NCS1K
ODUK-SF-TCM3	TCM3 Signal Failure	–	–	Event	ODUk/NCS1K
ODUK-SF-TCM4	TCM4 Signal Failure	–	–	Event	ODUk/NCS1K
ODUK-SF-TCM5	TCM5 Signal Failure	–	–	Event	ODUk/NCS1K
ODUK-SF-TCM6	TCM6 Signal Failure	–	–	Event	ODUk/NCS1K
ODUK-TIM-PM	ODUk: Trail Trace Identifier Mismatch	MJ	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-TIM-TCM1	TCM1 Trail Trace Identifier Mismatch	–	–	Event	ODUk/NCS1K
ODUK-TIM-TCM2	TCM2 Trail Trace Identifier Mismatch	–	–	Event	ODUk/NCS1K
ODUK-TIM-TCM3	TCM3 Trail Trace Identifier Mismatch	–	–	Event	ODUk/NCS1K
ODUK-TIM-TCM4	TCM4 Trail Trace Identifier Mismatch	–	–	Event	ODUk/NCS1K
ODUK-TIM-TCM5	TCM5 Trail Trace Identifier Mismatch	–	–	Event	ODUk/NCS1K
ODUK-TIM-TCM6	TCM6 Trail Trace Identifier Mismatch	–	–	Event	ODUk/NCS1K
OPU-CSF	OPU Client Signal Fail	CR	SA	Alarm	ODUk/NCS2K/NCS1K
OSNR	Optical Signal-to-Noise Ratio	MN	NSA	Alarm	OCH/NCS1K
OTUK-AIS	OTUk: Alarm Indication Signal	NA	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-BDI	OTUk: SM Backward Defect Indication	NA	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-BIAE	OTUk: SM Backward Incoming Alignment Error	MN	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-IAE	OTUk: Incoming Alignment Error	MN	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-LOF	OTUk: Loss Of Frame	CR	SA	Alarm	OTUk/NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
OTUK-LOM	OTUK Loss Of MultiFrame	–	–	Event	OTUk/NCS1K
OTUK-SD	OTUk: Signal Degrade	NA	SA	Alarm	OTUk/NCS2K/NCS1K
OTUK-SF	OTUk: Signal Failure	NA	SA	Alarm	OTUk/NCS2K/NCS1K
OTUK-TIM	OTUk: Trail Trace Identifier Mismatch	CR	SA	Alarm	OTUk/NCS2K/NCS1K
PCS-ERROR	PCS Error/Invalid	–	–	Alarm	FC/NCS1K
PEER-CERT-VERIFICATION-FAILED	Peer card certificate verification failed	MJ	NSA	Alarm	ODUk/NCS2K
PEER-CSF	Peer Port Client Signal Fail Detected	MJ	SA	Alarm	ODUk/NCS2K
PRBS-ENABLED	PRBS Generation Enabled	NA	NSA	Alarm	ODUk/NCS2K
PROV-IN-PROG	Provisioning In Progress	–	–	Event	ODUk/NCS1K
PTIM	Payload Type Identifier Mismatch	MJ	SA	Alarm	ODUk/NCS2K/NCS1K
RDI-L	Remote Defect Indication Line	–	–	Alarm	OCn/NCS2K
REMOTE-CERT-FAIL	RemoteCard Certificate Validation Failed	–	–	Alarm	ODUk/NCS2K
REMOTE-DEG-SER	Remote FEC Degraded Symbol Error Rate	–	–	Event	ETH/NCS1K
REMOTE-FAULT	Remote Fault	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
RS-EOC	Regenerator Section - DCC Termination Failure	MN	NSA	Alarm	STMn/NCS2K
RS-TIM	Regenerator Section Trace Identifier Mismatch	CR	SA	Alarm	STMn/NCS2K/NCS1K
SD-L	BER Threshold Exceeded For Signal Degrade Line	NA	SA	Alarm	OCn/NCS2K
SIP	Startup In Progress	NA	NSA	Alarm	OXC/NCS2K/NCS1K
SQUELCHED	Equipment Squelched	NA	NSA	Alarm	OCH ODUk FC/NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
TIM-S	Section Trace Identifier Mismatch	CR	SA	Alarm	OCn/NCS2K
TRAIL-SIGNAL-FAIL	Trail Signal Fail	NA	NSA	Alarm	OPT OXC/NCS2K
TRUNK-ODU-AIS	Trunk ODU Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
TRUNK-OPU-CSF	Trunk OPU Client Signal Fail	NR	NSA	Alarm	ODUk/NCS2K
TRUNK-PAYLOAD-MISM	Trunk Payload Type Mismatch	MJ	SA	Alarm	ODUk/NCS2K
TX-POWER-PROV-MISMATCH	Provisioned Optics Transmit Power Not Supported	–	–	Event	ODUk/NCS1K
UNC-WORD	FEC Uncorrected Word	NA	NSA	Alarm	OCH OTUk/NCS2K/NCS1K

PROTECTION alarm details

This table lists the alarm details for the PROTECTION category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
APS-NO-RESPONSE	APS Signal Mismatch	MN	SA	Alarm	ODUk/NCS2K
FAILTOSW	Failure To Switch To Protection	NA	NSA	Alarm	OPT ODUk OTUk OCn STMn ETH zrPlus/NCS2K
FORCED-REQ	Forced Switch Request	NA	NSA	Alarm	CARD OPT ODUk/NCS2K
LOCKOUT-REQ	Lockout Switch Request	NA	NSA	Alarm	OCn STMn ETH OPT ODUk OTUk zrPlus/NCS2K
MAN-REQ	Manual Switch Request	NA	NSA	Alarm	CARD OPT ODUk/NCS2K
PROT-CONFIG-MISMATCH	Protection Card Configuration Mismatch	MN	NSA	Alarm	CARD/NCS2K
REROUTE-IN-PROG	Reroute In Progress	–	–	Alarm	OXC/NCS2K
RESTORE-IN-PROG	Restoration in Progress	–	–	Alarm	OXC/NCS2K
REVERT-IN-PROG	Revert In Progress	NA	NSA	Alarm	OXC/NCS2K
WKSWBK	Switched Back To Working	–	–	Event	OPT ODUk/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
WKSWPR	Switched To Protection	NA	NSA	Alarm	OPT OCn STMn ODUk OTUk ETH/NCS2K/NCS1K
WRK-PATH- RECOVERY-CHECK	Checking For Work Path Recovery	NA	NSA	Alarm	OPT/NCS2K
WTR	Wait To Restore	NA	NSA	Alarm	OPT OCn STMn ODUk OTUk ETH/NCS2K

TIMING alarm details

This table lists the alarm details for the TIMING category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
BERT-SYNC-FAIL	BERT Synchronization Status Failed	NR	NSA	Alarm	OCn STMn OTUk/NCS2K
FRCDSWTOINT	Forced Switch To Internal Clock	NA	NSA	Alarm	NE_SYNCHREF/NCS2K
FRCDSWTOPRI	Forced Switch To Primary Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
FRCDSWTOSEC	Forced Switch To Second Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
FRCDSWTOTHIRD	Forced Switch To Third Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
FRNGSYNC	Free Running Synchronization Mode	NA	NSA	Alarm	NE_SYNCHREF/NCS2K
HI-CCVOLT	Composite Clock High Line Voltage	MN	NSA	Alarm	BITS/NCS2K
HLDOVRSYNC	Holdover Synchronization Mode	CR	SA	Alarm	NE_SYNCHREF/NCS2K
MANSWTOINT	Manual Switch To Internal Clock	NA	NSA	Alarm	NE_SYNCHREF/NCS2K
MANSWTOPRI	Manual Switch To Primary Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
MANSWTOSEC	Manual Switch To Second Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
MANSWTOTHIRD	Manual Switch To Third Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SSM-DUS	Do Not Use For Synchronization	NA	NSA	Alarm	OCn STMn OTUk BITS/NCS2K
SSM-FAIL	Failed To Receive Synchronization Status Message	MN	NSA	Alarm	OCn STMn OTUk BITS/NCS2K
SSM-LNC	G812L - Local Node Clock traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-OFF	Synchronization Status Messages Are Disabled On This Interface	NA	NSA	Alarm	OCn STMn OTUk BITS/NCS2K
SSM-PRC	G811 - Primary Reference Clock traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-PRS	Stratum 1 Primary Reference Source Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-RES	Reserved For Network Synchronization Use	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-SDH-TN	G812T - Transit Node Clock traceable	NA	NSA	Alarm	STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-SETS	G813 - Synchronous Equipment Timing Source traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-SMC	SONET Minimum Clock Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST2	Stratum 2 Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST3	Stratum 3 Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST3E	Stratum 3E Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST4	Stratum 4 Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-STU	Synchronized - Traceability Unknown	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-TNC	Transit Node Clock Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SWTOPRI	Switch To Primary Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
SWTOSEC	Switch To Second Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
SWTOTHIRD	Switch To Third Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
SYNC-FREQ	Synchronization Reference Frequency Out Of Bounds	NA	NSA	Alarm	OTUk BITS OCn STMn/NCS2K
SYNCCLK	Synchronization Unit Failure	MJ	SA	Alarm	NE_SYNCHREF/NCS2K
SYNCLOSS	Synchronization Loss on Data Interface	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
SYNCPRI	Primary Synchronization Reference Failure	MN	NSA	Alarm	NE_SYNCHREF/NCS2K
SYNCPRI	Primary Synchronization Reference Failure	MJ	SA	Alarm	EXT_SYNCHREF/NCS2K
SYNCSEC	Secondary Synchronization Reference Failure	MN	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
SYNCTHIRD	Third Synchronization Reference Failure	MN	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K

SECURITY alarm details

This table lists the alarm details for the SECURITY category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADMIN-CONFIG-INCONSISTENCY	Admin Configuration is in inconsistent state	–	–	Alarm	NE/NCS1K
ADMIN-DISABLE	Disable Inactive User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-DISABLE-CLR	Disable Inactive Clear	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-LOCKOUT	Admin Lockout of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-LOCKOUT-CLR	Admin Lockout Clear	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-LOGOUT	Admin Logout of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADMIN-SUSPEND	Suspend User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-SUSPEND-CLR	Suspend User Clear	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
CRYPTO-HW-FAILURE	Cryptographic self-test failure	CR	SA	Alarm	SHELF/NCS1K
CRYPTO-INDEX-MISMATCH	Crypto Index Mismatch	MN	NSA	Alarm	CARD/NCS1K
CRYPTO-KEY-EXPIRED	Crypto key expired	CR	SA	Alarm	CARD/NCS1K
INTRUSION	Security: Invalid Login Username - See Audit Trail	MJ	NSA	Event	NE SYSTEM/NCS2K/SYSTEM
INTRUSION-PSWD	Security Intrusion Attempt Detected - See Audit Log	MN	NSA	Alarm	NE SYSTEM/NCS2K/SYSTEM
INTRUSION-USERID	Security Intrusion Attempt Detected - See Audit Log	CR	SA	Event	NE SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-CHAIN-VERIFICATION-FAILED	Local cert chain verification failed	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-EXPIRED	Local certificate expired	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-EXPIRING-WITHIN-30-DAYS	Local cert expiring within 30 days	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-ISSUED-FOR-FUTURE-DATE	Local cert issued for future date	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-SUDI-CERT-VERIFICATION-FAILED	Local sudi cert verification failed	MJ	NSA	Alarm	CARD/NCS2K/NCS1K
LOGIN-FAIL-LOCKOUT	Security: Invalid Login - Locked Out - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAIL-ONALRDY	Security: Invalid Login - Already Logged On - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAILURE-PSWD	Security: Invalid Login - Password - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAILURE-USER	Security: Invalid Login - Username - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LOGOUT-IDLE-USER	Automatic Logout of IdleUser	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
MASTERKEY-SUCCESS	MasterKey Exchange Success	–	–	Event	NE/NCS2K
NON-TRAF-AFFECT-SEC-UPG-REQUIRED	Non Traffic Affecting Security Upgrade Required	NR	NSA	Alarm	CARD/NCS2K
OTNSEC-LOCALLY-SECURED	OTNSEC Locally Secured	NA	NSA	Alarm	CARD/NCS1K
PROT-SOFT-VERIF-FAIL	Protect Volume Software Signature Verification Failed		–	Alarm	CARD/NCS2K
PSWD-CHG-REQUIRED	User Password Change Required	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
SESSION-TIME-LIMIT	Session Time Limit Expired	–	–	Event	NE/NCS2K
USER-LOCKOUT	User Locked Out	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
USER-LOGIN	Login of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
USER-LOGOUT	Logout of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM

OPTICAL alarm details

This table lists the alarm details for the OPTICAL category.

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADD-OPWR-HDEG	Port Add Power Degrade High	MN	NSA	Alarm	OPT/NCS2K
ADD-OPWR-HFAIL	Port Add Power Fail High	CR	SA	Alarm	OPT/NCS2K
ADD-OPWR-LDEG	Port Add Power Degrade Low	MN	NSA	Alarm	OPT/NCS2K
ADD-OPWR-LFAIL	Port Add Power Fail Low	CR	SA	Alarm	OPT/NCS2K
ALC-IN-PROGRESS	Automatic-link-calibration procedure is running	MN	NSA	Alarm	OPT/NCS1K
ALC-PROC-FAILED	Automatic-link-calibration procedure failed	CR	SA	Alarm	OPT/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ALS	Automatic Laser Shutdown	NA	NSA	Alarm	OPT OCH ETH/NCS2K/NCS1K
ALS-DISABLED	Auto Laser Shutdown Disabled	NA	NSA	Alarm	OPT OCH/NCS2K
AMPLI-INIT	Optical Amplifier Initialization	NA	NSA	Alarm	OPT/NCS2K
AMPLI-OSRI	Amplifier Optical Safety Remote Interlock	NA	NSA	Alarm	OPT/NCS1K
APC-BLOCKED	APC blocked	MN	NSA	Alarm	OPT/NCS1K
APC-BLOCKED-RX	APC blocked in RX direction	MN	NSA	Alarm	OPT/NCS1K
APC-BLOCKED-TX	APC blocked in TX direction	MN	NSA	Alarm	OPT/NCS1K
APC-CORR-SKIPPED	Automatic Power Control Correction Skipped	MN	NSA	Alarm	OPT/NCS2K
APC-DISABLED	Automatic Power Control Disabled	MN	NSA	Alarm	OPT CARD/NCS2K
APC-DISABLED	Automatic Power Control Disabled	MN	NSA	Alarm	NE/NCS2K
APC-END	Manual Requested Automatic Power Control run Completed	NA	NSA	Alarm	NE/NCS2K
APC-HW-FAIL	APC Hardware Failure	MJ	NSA	Alarm	OPT/NCS1K
APC-OUT-OF-RANGE	APC Cannot Set Value Due To Range Limits	MN	NSA	Alarm	OPT/NCS2K/NCS1K
APC-TARGET-PSD-NOT-MET-RX	APC Target PSD not met in RX direction	MN	NSA	Alarm	OPT/NCS1K
APC-TARGET-PSD-NOT-MET-TX	APC Target PSD not met in TX direction	MN	NSA	Alarm	OPT/NCS1K
APC-WRONG-GAIN	APC Wrong Gain Set Point	NA	NSA	Alarm	OPT/NCS2K
ASE-LOADING-DISABLED	ASE Loading is disabled	NA	NSA	Alarm	OPT OXC/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AUTO-AMPLI-DISABLED	Auto Ampli Control Disabled	MN	NSA	Alarm	OPT/NCS1K
AUTO-AMPLI-MISMATCH	Auto Ampli Control Mismatch	NA	NSA	Alarm	OPT/NCS1K
AUTO-AMPLI-RUNNINNG	Auto Ampli Control Running	NA	NSA	Alarm	OPT/NCS1K
AUTOWDMANS	Automatic WDM ANS Finished	–	–	Event	NE/NCS2K
CANNOT-BE-EQUALIZED	Incoming signal cannot be equalized	–	–	Alarm	OPT OXC/NCS2K
CARLOSS	Carrier Loss On The LAN	MJ	SA	Alarm	MS_ETH ETH/NCS2K/NCS1K
CD	Chromatic Dispersion	–	–	Alarm	OCH/NCS2K/NCS1K
CHAN-PWR-THRESHOLD-CHECK	Channel Power would fall below threshold value	MN	NSA	Alarm	OPT/NCS2K
CHANNEL-NOISE-LOADED	Channel is Loaded with Noise	MJ	NSA	Alarm	OPT OXC/NCS1K
CHANNEL-READY	Channel Presence is Detected and Ready	MN	NSA	Alarm	OPT OXC/NCS1K
DCU-LOSS-FAIL	DCU Loss Failure	MN	NSA	Alarm	OPT/NCS2K
DGD	Differential Group Delay	MN	NSA	Alarm	OCH/NCS1K
EMB-AMPLIFIER-SATURATED	Embedded amplifier saturated alarm	MN	NSA	Alarm	OPT/NCS2K
EXPECTED-POWER-FAIL	Channel Power Reading Exceeds the Expected Power Tolerance Limits	MN	NSA	Alarm	OPT OXC/NCS1K
FDI	Forward Defect Indication	NA	NSA	Alarm	OXC OCn/NCS2K
GAIN-HDEG	Optical Amplifier Gain Degrade High	MN	NSA	Alarm	OPT/NCS2K
GAIN-HFAIL	Optical Amplifier Gain Failure High	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
GAIN-LDEG	Optical Amplifier Gain Degrade Low	MN	NSA	Alarm	OPT/NCS2K
GAIN-LFAIL	Optical Amplifier Gain Failure Low	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
GAIN-NEAR-LIMIT	Amplifier Gain is near its limit	MN	NSA	Alarm	OPT/NCS2K
HI-RX-BR-PWR	Input High BR Power	MN	NSA	Alarm	RAMAN_AMPLIFIER/NCS1K
HI-RXPOWER	Facility High Rx power	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
HI-TX-BR-PWR	Output High BR Power	MN	NSA	Alarm	OPT/NCS1K
LASER-APR	Laser Auto Power Reduction	MN	NSA	Alarm	OPT/NCS2K/NCS1K
LO-RXPOWER	Facility Low Rx power	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
LOS	Loss Of Signal	CR	SA	Alarm	OCn STMn OPT/NCS2K/ NCS2K-SVO-K9/NCS1K
LOS	Loss Of Signal	CR	SA	Alarm	BITS PORT/NCS2K/ NCS2K-SVO-K9/NCS1K
LOS-D	Loss Of DFB Signal	CR	SA	Alarm	OPT/NCS2K
LOS-O	Incoming Overhead Signal Absent	MN	NSA	Alarm	OPT/NCS2K
LOS-P	Incoming Payload Signal Absent	CR	SA	Alarm	OPT OCH OXC/NCS2K/NCS1K
LOS-RAMAN	Loss Of Raman Signal	CR	SA	Alarm	OPT/NCS2K
MAN-LASER-RESTART	Manual Laser Restart	NA	NSA	Alarm	OPT OCH/NCS2K
OPWR-HDEG	Optical Power Degrade High	MN	NSA	Alarm	OPT OXC/NCS2K
OPWR-HFAIL	Optical Power Failure High	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
OPWR-LDEG	Optical Power Degrade Low	MN	NSA	Alarm	OPT OXC/NCS2K
OPWR-LFAIL	Optical Power Failure Low	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
OSRION	Optical Safety Remote Interlock On	NA	NSA	Alarm	OPT/NCS2K
PARAM-MISM	Plug-in Module Range Settings Mismatch	CR	SA	Alarm	OPT OXC/NCS2K
PARTIAL-TOPOLOGY	APC Partial topology	MN	NSA	Alarm	OPT/NCS1K
PMD-DEG	PMD Degrade	MJ	NSA	Alarm	OCH/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
PMI	Payload Missing Indication	NA	NSA	Alarm	OPT OXC/NCS2K
PSD-FAILED	Failure in Power Spectrum Distribution	–	–	Alarm	OPT OXC/NCS1K
PWR-PROT-ON	Raman Power Protection On	MJ	SA	Alarm	OPT/NCS2K
RAMAN-AMPLI-OSRI	Raman Amplifier Optical Safety Remote Interlock	CR	SA	Alarm	RAMAN_AMPLIFIER/NCS1K
RAMAN-CALIBRATION-FAILED	Raman Calibration Failed	MN	NSA	Alarm	RAMAN_AMPLIFIER/NCS2K/ SYSTEM/NCS1K
RAMAN-CALIBRATION-PENDING	Raman Calibration Pending	NA	NSA	Alarm	RAMAN_AMPLIFIER/NCS2K
RAMAN-CALIBRATION-RUNNING	Raman Calibration Running	CR	SA	Alarm	RAMAN_AMPLIFIER/ NCS2K/NCS1K
RAMAN-GAIN-NOT-REACHED	Raman Gain Not Reached	MJ	SA	Alarm	RAMAN_AMPLIFIER/ NCS2K/SYSTEM/NCS1K
RAMAN-TURNUP-FAIL	Raman Pumps Turnup Fail	MJ	SA	Alarm	RAMAN_AMPLIFIER/NCS1K
RFI	Remote Failure Indication	NR	NSA	Alarm	OPT/NCS2K
RLS	Raman Laser Shutdown	NA	NSA	Alarm	RAMAN_AMPLIFIER/NCS2K
RMON-ALARM	RMON Threshold Crossing Alarm	–	–	Event	ETH FC ODUk/NCS2K
RMON-RESET	RMON Histories And Alarms Reset Reboot	–	–	Event	ETH FC ODUk/NCS2K
RX-BELOW-MIN-PSD	Receive Channel Power Below Minimum Power Spectral Density	MJ	SA	Alarm	OPT/NCS1K
SD	Signal Degrade	NA	NSA	Alarm	OCn/NCS2K
SF	Signal Failure	NA	NSA	Alarm	OCn/NCS2K
SF-L	BER Threshold Exceeded For Signal Failure Line	NA	NSA	Alarm	OCn/NCS2K
SIGLOSS	Signal Loss on Data Interface	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SIGNAL-OSC-SPAN-LOSS-DIFF-OUT-OF-RANGE	Difference in Rx OSC span loss and Rx signal span loss exceeded threshold	MN	NSA	Alarm	OPT/NCS1K
SPAN-LOSS-BASELINE-DEVIATION-OUT-OF-RANGE	Rx span loss deviated from baseline	MN	NSA	Alarm	OPT/NCS1K
SPAN-LOSS-OUT-OF-RANGE	Span Loss Value Out Of Range	MN	NSA	Alarm	OPT/NCS2K/NCS1K
SPAN-NOT-MEASURED	Span Measurement Cannot Be Performed	MN	NSA	Alarm	OPT/NCS2K
SPAN-TOO-SHORT	OTS Span Too Short	MN	NSA	Alarm	OPT/NCS1K
SPECTRUM-VIOLATED	Spectrum is Violated	CR	SA	Alarm	OPT OXC/NCS1K
VOA-DISABLED	VOA Control Loop Disable Due To Excessive Counter-Propagation Light	CR	SA	Alarm	CARD/NCS2K
VOA-HDEG	Variable Optical Attenuator Degrade High	MN	NSA	Alarm	OPT OXC/NCS2K
VOA-HFAIL	Variable Optical Attenuator Failure High	CR	SA	Alarm	OPT OXC/NCS2K
VOA-LDEG	Variable Optical Attenuator Degrade Low	MN	NSA	Alarm	OPT OXC/NCS2K
VOA-LFAIL	Variable Optical Attenuator Failure Low	CR	SA	Alarm	OPT OXC/NCS2K
WVL-MISMATCH	Equipment Wavelength Mismatch	MJ	SA	Alarm	OCH/NCS2K
WVL-UNLOCKED	Wavelength Unlocked	MJ	SA	Alarm	OCH/NCS2K/NCS1K

TCA alarm details

This table lists the alarm details for the TCA category.

Condition Name	Description	Condition Type	Resource Type/Source
PM-TCA	Performance Monitor Threshold Crossing Alert	Event	CARD ETH FC OCH OCn ODUk OPT OTUk OXC PORT PPM STMn/NCS2K
T-BAD-SH	Threshold Crossing Alert	Event	FC/NA
T-BBE-PM	Threshold Crossing Alert	Event	ODUk/NA
T-BBE-SM	Threshold Crossing Alert	Event	OTUk/NA
T-BBE-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-BBE-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-BBEL	Threshold Crossing Alert	Event	OCn/NA
T-BBER-PM	Threshold Crossing Alert	Event	ODUk/NA
T-BBER-SM	Threshold Crossing Alert	Event	OTUk/NA
T-BBER-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-BBER-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-BBES	Threshold Crossing Alert	Event	OCn/NA
T-BIEC	Threshold Crossing Alert	Event	OTUk/NA
T-BIP	Threshold Crossing Alert	Event	FC/NA
T-BIT-EC	Threshold Crossing Alert	Event	OCH OTUk/NA
T-BYTE-EC	Threshold Crossing Alert	Event	OCH OTUk/NA
T-CDPM-AVG	Threshold Crossing Alert	Event	OCH/NA
T-CDPM-MAX	Threshold Crossing Alert	Event	OCH/NA
T-CDPM-MIN	Threshold Crossing Alert	Event	OCH/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-CHROM-DISP	Threshold Crossing Alert	Event	OCH/NA
T-CVL	Threshold Crossing Alert	Event	OCn/NA
T-CVS	Threshold Crossing Alert	Event	OCn/NA
T-DGD-MAX	Threshold Crossing Alert	Event	OCH/NA
T-DGD-MIN	Threshold Crossing Alert	Event	OCH/NA
T-EC-WORD	Threshold Crossing Alert	Event	ETH FC/NA
T-ES-PCS	Threshold Crossing Alert	Event	FC/NA
T-ES-PM	Threshold Crossing Alert	Event	ODUk/NA
T-ES-SM	Threshold Crossing Alert	Event	OTUk/NA
T-ES-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-ES-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-ESL	Threshold Crossing Alert	Event	OCn/NA
T-ESR-PM	Threshold Crossing Alert	Event	ODUk/NA
T-ESR-SM	Threshold Crossing Alert	Event	OTUk/NA
T-ESR-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-ESR-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-ESS	Threshold Crossing Alert	Event	OCn/NA
T-FC-L	Threshold Crossing Alert	Event	STMn/NA
T-FC-PM	Threshold Crossing Alert	Event	ODUk/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-FC-SM	Threshold Crossing Alert	Event	OTUk/NA
T-FC-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-FC-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-FRM-ERR	Threshold Crossing Alert	Event	FC/NA
T-GAIN-AVG	Threshold Crossing Alert	Event	OPT/NA
T-GAIN-MAX	Threshold Crossing Alert	Event	OPT/NA
T-GAIN-MIN	Threshold Crossing Alert	Event	OPT/NA
T-LASER-BIAS-MAX	Threshold Crossing Alert	Event	OCH/NA
T-LASER-BIAS-MIN	Threshold Crossing Alert	Event	OCH/NA
T-LASER-TEMP-MAX	Threshold Crossing Alert	Event	OCH/NA
T-LASER-TEMP-MIN	Threshold Crossing Alert	Event	OCH/NA
T-LOW-FREQ-OFF-AVG	Threshold Crossing Alert	Event	OCH/NA
T-LOW-FREQ-OFF-MAX	Threshold Crossing Alert	Event	OCH/NA
T-LOW-FREQ-OFF-MIN	Threshold Crossing Alert	Event	OCH/NA
T-MS-BBE	Threshold Crossing Alert	Event	STMn/NA
T-MS-BBER	Threshold Crossing Alert	Event	STMn/NA
T-MS-EB	Threshold Crossing Alert	Event	STMn/NA
T-MS-ES	Threshold Crossing Alert	Event	STMn/NA
T-MS-ESR	Threshold Crossing Alert	Event	STMn/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-MS-FC	Threshold Crossing Alert	Event	STMn/NA
T-MS-LOSS	Threshold Crossing Alert	Event	STMn/NA
T-MS-SES	Threshold Crossing Alert	Event	STMn/NA
T-MS-SESR	Threshold Crossing Alert	Event	STMn/NA
T-MS-UAS	Threshold Crossing Alert	Event	STMn/NA
T-OPBR-AVG	Threshold Crossing Alert	Event	OPT/NA
T-OPBR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-OPBR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OPBRR-AVG	Threshold Crossing Alert	Event	OPT/NA
T-OPBRR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-OPBRR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OPR-AVG	Threshold Crossing Alert	Event	OCH/NA
T-OPR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-OPR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-OPT-AVG	Threshold Crossing Alert	Event	OCH/NA
T-OPT-MAX	Threshold Crossing Alert	Event	OCH/NA
T-OPT-MIN	Threshold Crossing Alert	Event	OCH/NA
T-OPWR-AVG	Threshold Crossing Alert	Event	OPT/NA
T-OPWR-CL-MAX	Threshold Crossing Alert	Event	OPT/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-OPWR-CL-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OPWR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-OPWR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OSC-PWR-AVG	Threshold Crossing Alert	Event	OPT/NA
T-OSC-PWR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-OSC-PWR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OSNR-AVG	Threshold Crossing Alert	Event	OCH/NA
T-OSNR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-OSNR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PCR-AVG	Threshold Crossing Alert	Event	OCH/NA
T-PCR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-PCR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PDL-AVG	Threshold Crossing Alert	Event	OCH/NA
T-PDL-MAX	Threshold Crossing Alert	Event	OCH/NA
T-PDL-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PMD-AVG	Threshold Crossing Alert	Event	OCH/NA
T-PMD-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PN-MAX	Threshold Crossing Alert	Event	OCH/NA
T-PN-MIN	Threshold Crossing Alert	Event	OCH/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-POST-FEC-BER-MAX	Threshold Crossing Alert	Event	OTUk FC/NA
T-POST-FEC-BER-MIN	Threshold Crossing Alert	Event	OTUk FC/NA
T-PRE-FEC-BER-MAX	Threshold Crossing Alert	Event	OTUk FC/NA
T-PRE-FEC-BER-MIN	Threshold Crossing Alert	Event	OTUk FC/NA
T-PWR-AVG	Threshold Crossing Alert	Event	OPT/NA
T-PWR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-PWR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-Q-MARGIN-MAX	Threshold Crossing Alert	Event	OTUk FC/NA
T-Q-MARGIN-MIN	Threshold Crossing Alert	Event	OTUk FC/NA
T-Q-MARGIN_INST-MAX	Threshold Crossing Alert	Event	OTUk/NA
T-Q-MARGIN_INST-MIN	Threshold Crossing Alert	Event	OTUk/NA
T-Q-MAX	Threshold Crossing Alert	Event	OTUk FC/NA
T-Q-MIN	Threshold Crossing Alert	Event	OTUk FC/NA
T-RAMAN-BR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-RAMAN-BR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-RAMAN-BRR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-RAMAN-BRR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-RS-BBE	Threshold Crossing Alert	Event	STMn/NA
T-RS-BBER	Threshold Crossing Alert	Event	STMn/NA

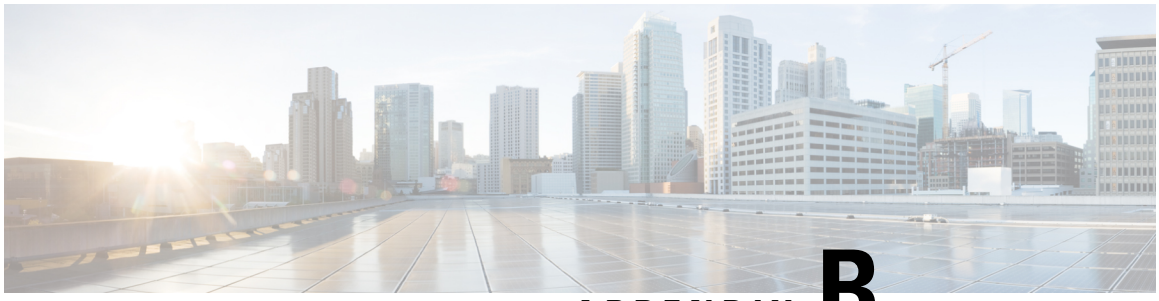
Condition Name	Description	Condition Type	Resource Type/Source
T-RS-EB	Threshold Crossing Alert	Event	STMn/NA
T-RS-ES	Threshold Crossing Alert	Event	STMn/NA
T-RS-ESR	Threshold Crossing Alert	Event	STMn/NA
T-RS-OFS	Threshold Crossing Alert	Event	STMn/NA
T-RS-SES	Threshold Crossing Alert	Event	STMn/NA
T-RS-SESR	Threshold Crossing Alert	Event	STMn/NA
T-RS-UAS	Threshold Crossing Alert	Event	STMn/NA
T-RX-PWR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-RX-PWR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-RX-SIG-POW-AVG	Threshold Crossing Alert	Event	OCH/NA
T-RX-SIG-POW-MAX	Threshold Crossing Alert	Event	OCH/NA
T-RX-SIG-POW-MIN	Threshold Crossing Alert	Event	OCH/NA
T-RX-TEMP-MAX	Threshold Crossing Alert	Event	OCH/NA
T-RX-TEMP-MIN	Threshold Crossing Alert	Event	OCH/NA
T-SEFS	Threshold Crossing Alert	Event	OCn/NA
T-SES-PCS	Threshold Crossing Alert	Event	FC/NA
T-SES-PM	Threshold Crossing Alert	Event	ODUk/NA
T-SES-SM	Threshold Crossing Alert	Event	OTUk/NA
T-SES-TCM1	Threshold Crossing Alert	Event	ODUk/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-SES-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-SESL	Threshold Crossing Alert	Event	OCn/NA
T-SESR-PM	Threshold Crossing Alert	Event	ODUk/NA
T-SESR-SM	Threshold Crossing Alert	Event	OTUk/NA
T-SESR-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-SESR-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-SESS	Threshold Crossing Alert	Event	OCn/NA
T-SIG-SPAN-LOSS-MAX	Threshold Crossing Alert	Event	OPT/NA
T-SIG-SPAN-LOSS-MIN	Threshold Crossing Alert	Event	OPT/NA
T-SOPMD-AVG	Threshold Crossing Alert	Event	OCH/NA
T-SOPMD-MAX	Threshold Crossing Alert	Event	OCH/NA
T-SOPMD-MIN	Threshold Crossing Alert	Event	OCH/NA
T-TILT-MAX	Threshold Crossing Alert	Event	OPT/NA
T-TILT-MIN	Threshold Crossing Alert	Event	OPT/NA
T-TOT-SPAN-LOSS-CL-MAX	Threshold Crossing Alert	Event	OPT/NA
T-TOT-SPAN-LOSS-CL-MIN	Threshold Crossing Alert	Event	OPT/NA
T-TOT-SPAN-LOSS-MAX	Threshold Crossing Alert	Event	OPT/NA
T-TOT-SPAN-LOSS-MIN	Threshold Crossing Alert	Event	OPT/NA
T-TX-PWR-MAX	Threshold Crossing Alert	Event	OCH/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-TX-PWR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-UAS-PCS	Threshold Crossing Alert	Event	FC/NA
T-UAS-PM	Threshold Crossing Alert	Event	ODUk/NA
T-UAS-SM	Threshold Crossing Alert	Event	OTUk/NA
T-UAS-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-UAS-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-UASL	Threshold Crossing Alert	Event	OCn/NA
T-UASS	Threshold Crossing Alert	Event	OCn/NA
T-UNC-WORDS	Threshold Crossing Alert	Event	OCH OTUk/NA
T-VOA-AVG	Threshold Crossing Alert	Event	OPT/NA
T-VOA-MAX	Threshold Crossing Alert	Event	OPT/NA
T-VOA-MIN	Threshold Crossing Alert	Event	OPT/NA
T-GFPSTATSROUNDTRIPLATENCYUSEC	Threshold Crossing Alert	Event	ETH/NA
T-RXCONTROLFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-RXPAUSEFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-RXPKTSDROPPED INTERNALCONGESTION	Threshold Crossing Alert	Event	ETH/NA
T-RXUNKNOWNOPCODEFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-TXPAUSEFRAMES	Threshold Crossing Alert	Event	ETH/NA

Condition Name	Description	Condition Type	Resource Type/Source
T-TXPKTSDROPPED INTERNALCONGESTION	Threshold Crossing Alert	Event	ETH/NA

Alarm categories



APPENDIX B

MIB Definition For Cisco Optical Network Controller

The MIB for Cisco Optical Network Controller traps includes a set of SNMP objects that represent various attributes of alarms and events generated by the system.

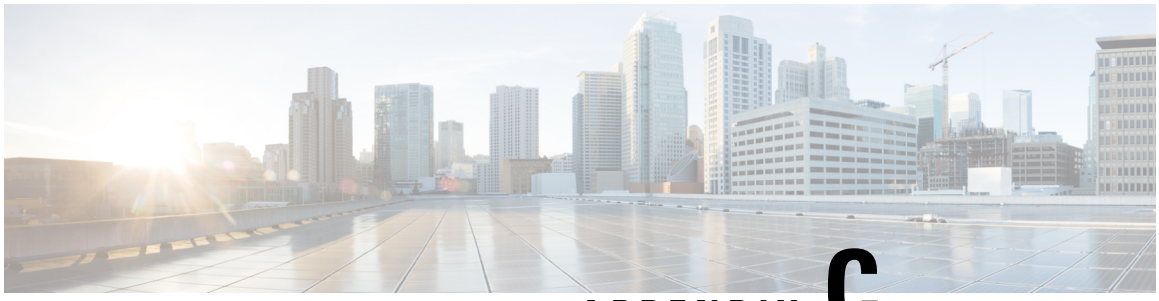
Note Each Cisco Optical Network Controller-generated trap is postfixed with an Event ID, which corresponds to the `cenAlarmIndex` in the MIB definition. This Event ID is a monotonically increasing signed 64-bit integer used solely for indexing attributes in the `ciscoEpmNotificationMIBObjects`. When the maximum value is reached, it wraps back to 1.

SNMPvarbind	Data Type	OID
cenAlarmVersion	SnmpAdminString	1.3.6.1.4.9.9
cenAlarmTimestamp	Timestamp	1.3.6.1.4.9.9
cenAlarmUpdatedTimestamp	Timestamp	.1.3.6.1.4.9.
cenAlarmInstanceID	SnmpAdminString	1.3.6.1.4.9.9
cenAlarmStatus	Integer	1.3.6.1.4.9.9
cenAlarmStatusDefinition	SnmpAdminString	1.3.6.1.4.9.9

SNMPvarbind	Data Type	OID
cenAlarmType	Integer	.1.3.6.1.4.9.9.31
cenAlarmCategory	Integer	.1.3.6.1.4.9.9.31
cenAlarmCategoryDefinition	SnmpAdminString	.1.3.6.1.4.9.9.31
cenAlarmServerAddressType	InetAddressType	.1.3.6.1.4.9.9.31
cenAlarmServerAddress	cenAlarmServerAddress	.1.3.6.1.4.9.9.31
cenAlarmManagedObjectClass	SnmpAdminString	.1.3.6.1.4.9.9.31
cenAlarmManagedObjectAddressType	InetAddressType	.1.3.6.1.4.9.9.31
cenAlarmManagedObjectAddress	InetAddress	.1.3.6.1.4.9.9.31
cenAlarmDescription	OctetString	.1.3.6.1.4.9.9.31
cenAlarmSeverity	Integer	.1.3.6.1.4.9.9.31
cenAlarmSeverityDefinition	SnmpAdminString	.1.3.6.1.4.9.9.31
cenAlarmTriageValue	Integer	.1.3.6.1.4.9.9.31

SNMPvarbind	Data Type	OID
cenEventIDList	OctetString	.1.3.6.1.4.9.
cenUserMessage1	SnmpAdminString	.1.3.6.1.4.9.
cenUserMessage2	SnmpAdminString	.1.3.6.1.4.9.
cenUserMessage3	SnmpAdminString	.1.3.6.1.4.9.
cenAlarmMode	Integer	.1.3.6.1.4.9.
cenPartitionNumber	Integer	.1.3.6.1.4.9.

SNMPvarbind	Data Type	OID
cenPartitionName	SnmpAdminString	.1.3.6.1.4.9.9.31
cenCustomerIdentification	SnmpAdminString	.1.3.6.1.4.9.9.31
cenCustomerRevision	SnmpAdminString	.1.3.6.1.4.9.9.31
cenAlertID	SnmpAdminString	.1.3.6.1.4.9.9.31



APPENDIX C

Platforms Software Compatibility Matrix

This table shows which software versions the Cisco Optical Network Controller supports on managed devices and indicates whether a device can act as a Cisco Optical Site Manager host.

CONC version	Platform (XR) Software Release	NCS 1010		NCS 1014		NCS 1004		NCS 1001		NCS 2000	
		Support	COSM Host	Support	COSM Host	Support	COSM Host	Support	COSM Host	Support	COSM Host
24.3.1 and 24.3.2	7.10.1	—	—	—	—	—	—	✓	—	—	—
	24.3.1	All C band cards and passives	✓	All cards except 1.2T	✓	All cards except 1.2T and QXP	—	—	—	—	—
25.1.1	7.10.1	—		—		—	—	✓	—	—	—
	24.3.1	All C band cards and passives	✓	All cards except 1.2T	✓	✓	—	—	—	—	—
	25.1.1	All C band cards and passives	✓	✓	✓	—	—	—	—	✓	✓
25.1.2	7.10.1	—		—		—	—	✓	—	—	—
	24.3.1	All C band cards and passives	✓	All cards except 1.2T	✓	✓	—	—	—	—	—
	25.1.1	All C band cards and passives	✓	✓	✓	—	—	—	—	✓	✓
	25.2.1	—	—	✓	✓	—	—	—	—	—	—

Note

- A ✓ in the COSM Host column means the platform can host COSM which can connect to and manage other devices.
- 1.2T refers to NCS1K4-1.2T-K9 line card.
- QXP refers to NCS1K4-QXP-K9 line card.