



Cisco Optical Network Controller 25.1.x Configuration Guide

First Published: 2025-04-28

Americas Headquarters

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



CONTENTS

CHAPTER 1

Overview of Cisco Optical Network Controller	1
Cisco Optical Network Controller Overview	1
Log in to Cisco Optical Network Controller	2
User access in Cisco Optical Network Controller	3
Add local users to Cisco Optical Network Controller	6
Set up authentication using LDAP	9
Set up authentication using SAMLv2 SSO	11
Set up Permission Mapping	13
Manage Certificates in Cisco Optical Network Controller	14

CHAPTER 2

Use Cisco Optical Network Controller	17
Topology	19
Troubleshooting in Topology	22
Nodes	23
Add Nodes on Cisco Optical Network Controller	25
Import Nodes on Cisco Optical Network Controller	28
Export Nodes on Cisco Optical Network Controller	30
Edit Nodes on Cisco Optical Network Controller	30
Delete Nodes on Cisco Optical Network Controller	30
Troubleshooting in Nodes	31
Alien Import	33
Network Inventory	34
Service Manager	35
Provision CPCE services	41
Troubleshoot CPCE Services	50
Provision GMPLS services	51

Alarms	62
Network Level Alarm Correlation	66
Acknowledged Alarm Mute	68
SNMP Traps and Alarm Filters	71
Set the Edit Host Name	72
Configure SNMP managers	72
Workspaces	75
Software Image Management and Upgrade	82
Configure SFTP server	85
Backup and Restore Nodes	86
Backup and Restore Database	88
Orchestrate Upgrades	91
PM History	96
Accessing PM History Report	101
Logs	104
Accessing Logs	111
Monitoring	112
Links	113
Use the Links Application	114
General Troubleshooting	116
Unmanaged Equipment Support	117
PSM Fiber Protection	119
PSM Circuit in Workspace Screen	120
Forwarding Syslogs	121

CHAPTER 3

Alarm Troubleshooting	123
BACKUP-FAILURE	123
Clear the BACKUP-FAILURE Alarm	123
NODE-BACKUP-FAILURE	124
Clear the NODE-BACKUP-FAILURE Alarm	124
NODE-DISCONNECT	124
Clear the NODE-DISCONNECT Alarm	125
UPLOAD-FAILURE	125
Clear the UPLOAD-FAILURE Alarm	125

DISK THRESHOLD	125
Clear the DISK-THRESHOLD Alarm	126
SWITCHOVER	126
Clear the SWITCHOVER Alarm	126
FAILOVER	126
Clear the FAILOVER Alarm	127

APPENDIX A	Alarm Categories	129
------------	------------------	-----

APPENDIX B	MIB Definition For Cisco Optical Network Controller	163
------------	---	-----



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 2](#)
- [User access in Cisco Optical Network Controller, on page 3](#)
- [Add local users to Cisco Optical Network Controller, on page 6](#)
- [Set up authentication using LDAP, on page 9](#)
- [Set up authentication using SAMLv2 SSO, on page 11](#)
- [Set up Permission Mapping, on page 13](#)
- [Manage Certificates in Cisco Optical Network Controller, on page 14](#)

Cisco Optical Network Controller Overview

Cisco Optical Network Controller (Cisco ONC) is an SDN Domain 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 and topology 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.

Cisco Optical Network Controller functions

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. Cisco Optical Network Controller has a North Bound Interface (NBI) based on the TAPI 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.

- 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](#).
- TAPI is disabled by default. 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.

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
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/`
The browser displays the login page.
- Step 2** Enter the username and password.
- Step 3** Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



User access in Cisco Optical Network Controller

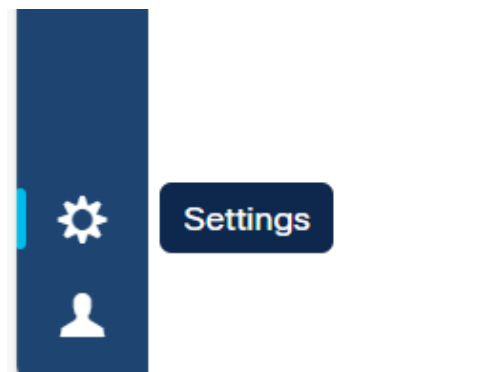
Users, Roles, and Permissions

Cisco Optical Network Controller allows you to manage user access and permissions. It adds an additional layer of security and works as a Single Authentication Agent, thus sharing local, Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML) users.

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.

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	Versions
Versions	
Audit Logs	
Monitoring	
SECURITY	
Local Users	
LDAP	
SAML SSO	
Permission Mapping	

Versions	
25.1.2	
Image Name	Version
docker.io/library/alpine	3.20.3
docker.io/rancher/local-path-provisioner	v0.0.30
quay.io/coreos/etcd	v3.5.15
registry.k8s.io/pause	3.10
registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmserv...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-s...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-s...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicem...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/monitoring	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-servi...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfc...	25.1.2-9
registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-app...	25.1.2-9

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.

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** .
- Step 3** In the **Add User** screen, enter **Username*** .
- Step 4** Enter and confirm the password.
- Step 5** Select the access permissions from the list **Access Permissions**.

For example *permission/<admin>*

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

Figure 4: Local Users

The screenshot shows the 'Local Users' configuration page in the Cisco Optical Network Controller. On the left is a navigation menu with the following items: SYSTEM INFO, Versions, SECURITY, Local Users (highlighted), LDAP, SAML SSO, and Permission Mapping. The main content area is titled 'Local Users' and displays a list of four local users, each in a separate box. At the bottom right of the main area are two buttons: 'Reload' and 'Add...'. The users listed are:

User Name	Access	Status	Description
internal (internal)	internal	Active	
NxF Admin (admin)	permission/admin	Active (Locked)	NextFusion Default Administrator
supervisor (supervisor)	supervisor	Active	
readonly (readonly)	readonly	Active	

Figure 5: Add User

SYSTEM INFO

Versions

SECURITY

Local Users

LDAP

SAML SSO

Permission Mapping

◀ Add User

Username*

Password*

Confirm Password*

Access Permissions*

- ☐ permission/admin
- ☐ supervisor
- ☐ permission/supervisor
- ☐ internal
- ☐ permission/internal
- ☐ readonly
- ☐ permission/readonly
- ☐ admin
- ☐ permission/admin

Display Name

Active ☒

Locked ☐

Description

Save

Step 6 Set the user status using radio buttons. The radio buttons 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.
- **Locked disabled:** Allows removal of the user

Step 7 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

SYSTEM INFO

Versions

SECURITY

Local Users

LDAP

SAML SSO

Permission Mapping

LDAP

Enabled ☒

LDAP Server Address*

Bind DN*

Bind Credentials*

Search Base

Search Filter

Attribute: cn Value: {{username}}

Add

Root CAs

Reload Save

Step 3 Click **Enabled** radio button.

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

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. Only local users can authenticate using SSO user credentials.

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

SAML SSO

Enabled ☐

Login URL

Entity ID

Base URL Use Current

Signing Certificate

Groups Attribute Name

Reload Save

Step 2 Click the **Enabled** radio button.

Step 3 Fill in the fields.

The fields are **Login URL**, **Entity ID**, **Base URL**, **Signing Certificate**, and **Groups Attribute Name**.

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.
- Step 6** Select the appropriate **Access Permission**.
- Step 7** Click **Save**.

Figure 8: Permission Mapping

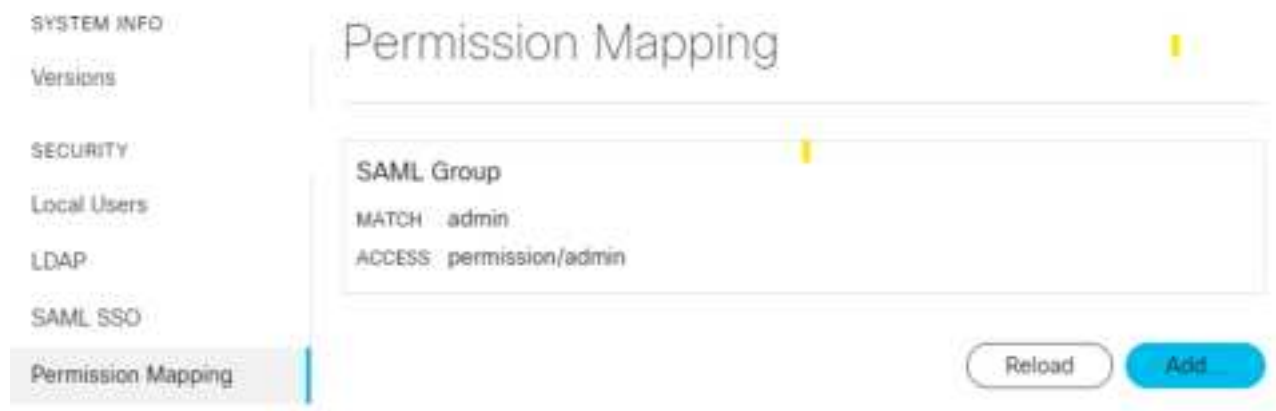


Figure 9: Add Permission Mapping

Note

Cisco Optical Network Controller offers different levels of permissions to map.

- **Admin:** No restrictions.
- **Supervisor:** Supervisors are similar to admin, but have restrictions on user management and log checks.
- **Readonly:** Users can check data, but they cannot provision.
- **Internal:** To be used in case of any triage or troubleshooting to collect debug logs. We recommend using it only under supervision of the Cisco Technical Assistance Center (TAC).

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. 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 CLI administration tool.

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).

Submit the generated CSR to a Certificate Authority 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	EXPIRES	ISSUER	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.

```
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 applications.

Before you begin

[Log in to Cisco Optical Network Controller, on page 2](#)

Procedure

-
- Step 1** View the timestamp.
- The timestamp appears on the top right corner of the screen in all the screens. It follows the UTC time zone. The current date is displayed along with the time.
- Step 2** Click the **Refresh** button to refresh the status of the table content or topology in each of the application screens anytime.
- Step 3** Click **Show or hide columns** icon to select any columns to be displayed or hidden from the table view anytime.
- Step 4** Export the current table.
- Click **Export** to export the details of any table from any application screen to a spreadsheet file.
 - Choose table view and click **Export** to download the current table with the filters enabled as an excel spreadsheet.
- Note**
When you export a table, the resulting spreadsheet contains all the columns of the table, not just the fields that you have selected from **Show or hide columns** dropdown.
- Step 5** Export all data relevant to the current application.
- Click **Export** to export the details of any table from any application screen to a spreadsheet file.
 - Choose **All items**.
- Note**
This label changes based on the app you are using. For example, All Nodes in the Nodes app, All Services in Service Manager, and so on.
- Click **Generate** to initiate file generation.
- Step 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 19](#)
- [Nodes, on page 23](#)
- [Alien Import, on page 33](#)
- [Network Inventory, on page 34](#)
- [Service Manager, on page 35](#)
- [Alarms, on page 62](#)
- [Workspaces, on page 75](#)
- [Software Image Management and Upgrade, on page 82](#)
- [PM History, on page 96](#)
- [Logs, on page 104](#)
- [Monitoring, on page 112](#)
- [Links, on page 113](#)
- [General Troubleshooting, on page 116](#)
- [Unmanaged Equipment Support, on page 117](#)
- [PSM Fiber Protection, on page 119](#)
- [Forwarding Syslogs , on page 121](#)

Topology

Topology displays the network along with the nodes and the associated network links on a map. You can toggle between the **Light** and **Dark** modes to view this screen. You can zoom in zoom out the entire screen to view the network and its components. You can select the **OTS** or **OMS** layers as options in the display. The OTS option is used to show all fiber span between all type of nodes, OLT or ILA. The OMS option is used to display only the ROADMs and the links between the ROADMs in the given network.

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

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

On the top of this screen, there is a panel for displaying the different alarm types and the count of each type of alarm that are part of the network. The alarm types are color coded based on the types of severity as seen in the table below.

Table 2: Alarm Severity

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



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



Note

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

You can get the node name along with the COSM site name it belongs to and its current state by hovering over each node in the **Topology** map anytime. Right click on any node in the map to select **Resync**, **View in Node UI** and **View Alarms** options.

Table 3: Topology Node Options

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

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

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

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

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

Figure 10: Topology Application



**Note**

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

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

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

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

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

**Note**

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

The screenshot shows a Google Maps interface with a route from London to Paris. The map displays a green line connecting several points. A sidebar on the left shows the 'Layers' panel with 'Traffic' selected. A table at the bottom provides details about the route, including the estimated time and distance.

Estimated Time	Estimated Distance	Estimated Speed	Estimated Fuel
1h 15m	100 km	80 km/h	10.0 L
1h 30m	120 km	80 km/h	12.0 L
1h 45m	140 km	80 km/h	14.0 L

Troubleshooting in Topology

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

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

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

Nodes

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

Use the **Nodes** screen to view the details of each node that is part of a service at any given point in time. The **Nodes** table displays the following details for each node:

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



Note

- If the geo location values that are coming from Cisco Optical Site Manager in a pre-filled format has more than four digits, then the length of the 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 operations, Cisco Optical Network Controller pushes the current node name to the node, ensuring consistency even if changes were missed while the device was offline.

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

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

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

- Modified Date

Figure 13: Nodes

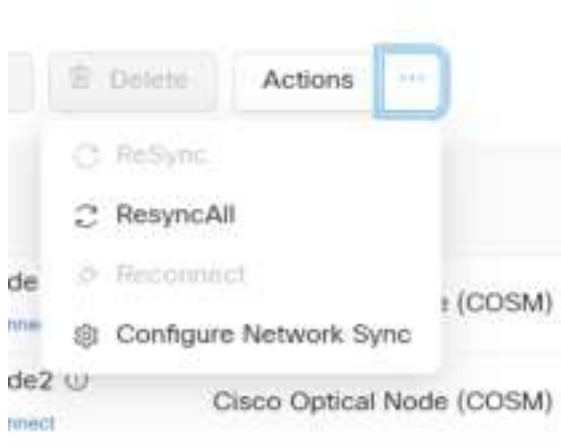
Node Name	Product Type	Model ID	Slot Name	Slot Location	Status
Node_1_1	Cisco Optical Node (COSM)	11-01-01-100-000	Slot_1	1	Connected
Node_2_1	Cisco Optical Node (COSM)	11-02-01-100-000	Slot_2	2	Connected
Node_3_1	Cisco Optical Node (COSM)	11-03-01-100-000	Slot_3	3	Connected
Node_4_1	Cisco Optical Node (COSM)	11-04-01-100-000	Slot_4	4	Connected

Use the sort or filter options to sort and filter values in the table. You can also cross launch to other supported pages using the links provided in this table.

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

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

Figure 14: Actions



**Note**

- Latitude and longitude values can be set in both Cisco Optical Site Manager and Cisco Optical Network Controller. The following scenarios are possible:
 - **Geo location is set in both Cisco Optical Site Manager and Cisco Optical Network Controller:** Cisco Optical Network Controller geo location is used.
 - **Geo location is set only in Cisco Optical Site Manager:** Cisco Optical Site Manager geo location is used .
 - **Geo location is set only in Cisco Optical Network Controller:** Cisco Optical Network Controller geo location is used.
 - **Geo location is not set in either Cisco Optical Network Controller or Cisco Optical Site Manager:** You will be prompted to add the node in **Topology** with the edit button.

For all the cases mentioned above, Cisco Optical Network Controller latitude and longitude value has a higher priority over the Cisco Optical Site Manager latitude and longitude values during the onboarding process. In case the Cisco Optical Network Controller latitude and longitude values are not provided, only then the Cisco Optical Site Manager latitude and longitude values are used.
- Even if the user updates the geo location in Cisco Optical Network Controller, it does not get updated in the Cisco Optical Site Manager device.
- If the geo location values coming from Cisco Optical Site Manager have more than four digits, they are shortened to up to four digits only and displayed.

Add Nodes on Cisco Optical Network Controller

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

Figure 15: Add New Node

New Node ✕

Name*

Port*

IP*

Protocol* NETCONF ▼

Site Name*

Site Description

Credentials

Username*

Password*

Geo Location

Latitude

Longitude

Cancel Save

Before you begin

To add nodes to Cisco Optical Network Controller:

- Cisco Optical Site Manager must be installed on the node.
- All COSM1K (NCS 1000 series) nodes must be added using port number 2022.
- All COSM2K (NCS 2000 series) nodes must be added using port number 830.

- You must create add only fully configured nodes. All passives and patchcords must already be created before you add a node.

Procedure

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

Step 2 Click **New**.

Step 3 Enter the device details necessary connect to the device as given in the table below.

Table 4: Add new node

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

Note

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

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

Import Nodes on Cisco Optical Network Controller

Before you begin

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

Procedure

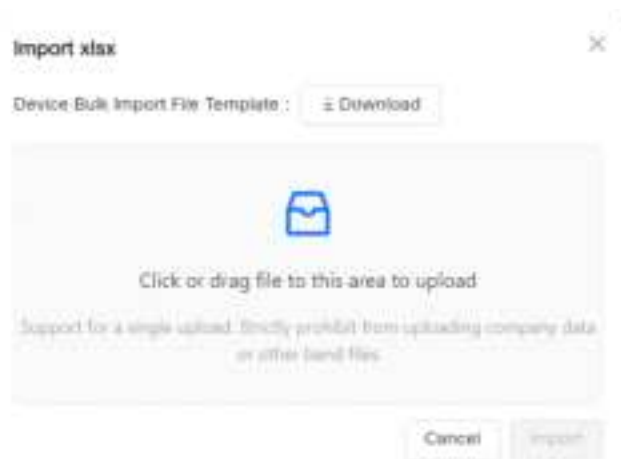
- Step 1** Click **Nodes** in the left panel.
- Step 2** Click **Import** to import the table details from external files.
- Step 3** Select the spreadsheet which has all the node details and click **Open**. The new nodes are onboarded and added to the **Nodes** table.

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

Note

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

Figure 16: 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	30.00.00.99			NETCONF	2022	sampleSite_1	sample site description test	Cisco Optical Node		
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											

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

Table 5: Bulk Import File Template

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

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

Export Nodes on Cisco Optical Network Controller

Before you begin

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

Procedure

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

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

Edit Nodes on Cisco Optical Network Controller

Before you begin

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

Procedure

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

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

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

Delete Nodes on Cisco Optical Network Controller

Before you begin

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

Procedure

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

Step 2 Select the node or nodes to be deleted.

Step 3 Click **DELETE**.

This will delete the selected node from the table.

Note

- We recommend to wait at least two minutes after device discovery completes before deleting the device.
- You cannot delete more than 5 nodes at a time.
- If the circuits are active and flowing over the nodes or if the resync is in progress, then deletion of the node fails. In this case you will receive an error message for the **Node Deletion Failure** when the circuit is spanning through the node.
For example: <Device A> cannot be deleted because circuit spanning across the device.
- Do not perform delete operations and Geo-Redundancy Switchover simultaneously. Make sure there is no switchover taking place before you perform delete operations.

Troubleshooting in Nodes

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

- **Bulk import failure**

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



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

- **Nodes possible status**

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

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

• **Nodes connection status**

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

• **De-boarding of a node fails**

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

Alien Import

Before you begin

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



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

Figure 17: Alien Import

ID	Name	Description	Location	Status	Imported	Exported	Deleted
1	ALIEN-01-01	ALIEN-01-01	ALIEN-01-01	ALIEN-01-01	ALIEN-01-01	ALIEN-01-01	ALIEN-01-01
2	ALIEN-02-01	ALIEN-02-01	ALIEN-02-01	ALIEN-02-01	ALIEN-02-01	ALIEN-02-01	ALIEN-02-01
3	ALIEN-03-01	ALIEN-03-01	ALIEN-03-01	ALIEN-03-01	ALIEN-03-01	ALIEN-03-01	ALIEN-03-01
4	ALIEN-04-01	ALIEN-04-01	ALIEN-04-01	ALIEN-04-01	ALIEN-04-01	ALIEN-04-01	ALIEN-04-01
5	ALIEN-05-01	ALIEN-05-01	ALIEN-05-01	ALIEN-05-01	ALIEN-05-01	ALIEN-05-01	ALIEN-05-01
6	ALIEN-06-01	ALIEN-06-01	ALIEN-06-01	ALIEN-06-01	ALIEN-06-01	ALIEN-06-01	ALIEN-06-01
7	ALIEN-07-01	ALIEN-07-01	ALIEN-07-01	ALIEN-07-01	ALIEN-07-01	ALIEN-07-01	ALIEN-07-01
8	ALIEN-08-01	ALIEN-08-01	ALIEN-08-01	ALIEN-08-01	ALIEN-08-01	ALIEN-08-01	ALIEN-08-01
9	ALIEN-09-01	ALIEN-09-01	ALIEN-09-01	ALIEN-09-01	ALIEN-09-01	ALIEN-09-01	ALIEN-09-01
10	ALIEN-10-01	ALIEN-10-01	ALIEN-10-01	ALIEN-10-01	ALIEN-10-01	ALIEN-10-01	ALIEN-10-01
11	ALIEN-11-01	ALIEN-11-01	ALIEN-11-01	ALIEN-11-01	ALIEN-11-01	ALIEN-11-01	ALIEN-11-01
12	ALIEN-12-01	ALIEN-12-01	ALIEN-12-01	ALIEN-12-01	ALIEN-12-01	ALIEN-12-01	ALIEN-12-01
13	ALIEN-13-01	ALIEN-13-01	ALIEN-13-01	ALIEN-13-01	ALIEN-13-01	ALIEN-13-01	ALIEN-13-01
14	ALIEN-14-01	ALIEN-14-01	ALIEN-14-01	ALIEN-14-01	ALIEN-14-01	ALIEN-14-01	ALIEN-14-01
15	ALIEN-15-01	ALIEN-15-01	ALIEN-15-01	ALIEN-15-01	ALIEN-15-01	ALIEN-15-01	ALIEN-15-01
16	ALIEN-16-01	ALIEN-16-01	ALIEN-16-01	ALIEN-16-01	ALIEN-16-01	ALIEN-16-01	ALIEN-16-01
17	ALIEN-17-01	ALIEN-17-01	ALIEN-17-01	ALIEN-17-01	ALIEN-17-01	ALIEN-17-01	ALIEN-17-01
18	ALIEN-18-01	ALIEN-18-01	ALIEN-18-01	ALIEN-18-01	ALIEN-18-01	ALIEN-18-01	ALIEN-18-01
19	ALIEN-19-01	ALIEN-19-01	ALIEN-19-01	ALIEN-19-01	ALIEN-19-01	ALIEN-19-01	ALIEN-19-01
20	ALIEN-20-01	ALIEN-20-01	ALIEN-20-01	ALIEN-20-01	ALIEN-20-01	ALIEN-20-01	ALIEN-20-01

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 18: Network Inventory

Name	Admin State	Equipment Type	Equipment State	Actual Equipment Type	Serial No.	Product ID
Core-1	Up	N7010-64	Up	N7010-64	F000000000	N7010-64
Core-2	Up	N7010-64	Up	N7010-64	F000000001	N7010-64
Core-3	Up	N7010-64	Up	N7010-64	F000000002	N7010-64
Core-4	Up	N7010-64	Up	N7010-64	F000000003	N7010-64
Core-5	Up	N7010-64	Up	N7010-64	F000000004	N7010-64
Core-6	Up	N7010-64	Up	N7010-64	F000000005	N7010-64
Core-7	Up	N7010-64	Up	N7010-64	F000000006	N7010-64
Core-8	Up	N7010-64	Up	N7010-64	F000000007	N7010-64
Core-9	Up	N7010-64	Up	N7010-64	F000000008	N7010-64
Core-10	Up	N7010-64	Up	N7010-64	F000000009	N7010-64
Core-11	Up	N7010-64	Up	N7010-64	F000000010	N7010-64
Core-12	Up	N7010-64	Up	N7010-64	F000000011	N7010-64
Core-13	Up	N7010-64	Up	N7010-64	F000000012	N7010-64
Core-14	Up	N7010-64	Up	N7010-64	F000000013	N7010-64
Core-15	Up	N7010-64	Up	N7010-64	F000000014	N7010-64
Core-16	Up	N7010-64	Up	N7010-64	F000000015	N7010-64
Core-17	Up	N7010-64	Up	N7010-64	F000000016	N7010-64
Core-18	Up	N7010-64	Up	N7010-64	F000000017	N7010-64
Core-19	Up	N7010-64	Up	N7010-64	F000000018	N7010-64
Core-20	Up	N7010-64	Up	N7010-64	F000000019	N7010-64
Core-21	Up	N7010-64	Up	N7010-64	F000000020	N7010-64
Core-22	Up	N7010-64	Up	N7010-64	F000000021	N7010-64
Core-23	Up	N7010-64	Up	N7010-64	F000000022	N7010-64
Core-24	Up	N7010-64	Up	N7010-64	F000000023	N7010-64
Core-25	Up	N7010-64	Up	N7010-64	F000000024	N7010-64
Core-26	Up	N7010-64	Up	N7010-64	F000000025	N7010-64
Core-27	Up	N7010-64	Up	N7010-64	F000000026	N7010-64
Core-28	Up	N7010-64	Up	N7010-64	F000000027	N7010-64
Core-29	Up	N7010-64	Up	N7010-64	F000000028	N7010-64
Core-30	Up	N7010-64	Up	N7010-64	F000000029	N7010-64
Core-31	Up	N7010-64	Up	N7010-64	F000000030	N7010-64
Core-32	Up	N7010-64	Up	N7010-64	F000000031	N7010-64
Core-33	Up	N7010-64	Up	N7010-64	F000000032	N7010-64
Core-34	Up	N7010-64	Up	N7010-64	F000000033	N7010-64
Core-35	Up	N7010-64	Up	N7010-64	F000000034	N7010-64
Core-36	Up	N7010-64	Up	N7010-64	F000000035	N7010-64
Core-37	Up	N7010-64	Up	N7010-64	F000000036	N7010-64
Core-38	Up	N7010-64	Up	N7010-64	F000000037	N7010-64
Core-39	Up	N7010-64	Up	N7010-64	F000000038	N7010-64
Core-40	Up	N7010-64	Up	N7010-64	F000000039	N7010-64
Core-41	Up	N7010-64	Up	N7010-64	F000000040	N7010-64
Core-42	Up	N7010-64	Up	N7010-64	F000000041	N7010-64
Core-43	Up	N7010-64	Up	N7010-64	F000000042	N7010-64
Core-44	Up	N7010-64	Up	N7010-64	F000000043	N7010-64
Core-45	Up	N7010-64	Up	N7010-64	F000000044	N7010-64
Core-46	Up	N7010-64	Up	N7010-64	F000000045	N7010-64
Core-47	Up	N7010-64	Up	N7010-64	F000000046	N7010-64
Core-48	Up	N7010-64	Up	N7010-64	F000000047	N7010-64
Core-49	Up	N7010-64	Up	N7010-64	F000000048	N7010-64
Core-50	Up	N7010-64	Up	N7010-64	F000000049	N7010-64
Core-51	Up	N7010-64	Up	N7010-64	F000000050	N7010-64
Core-52	Up	N7010-64	Up	N7010-64	F000000051	N7010-64
Core-53	Up	N7010-64	Up	N7010-64	F000000052	N7010-64
Core-54	Up	N7010-64	Up	N7010-64	F000000053	N7010-64
Core-55	Up	N7010-64	Up	N7010-64	F000000054	N7010-64
Core-56	Up	N7010-64	Up	N7010-64	F000000055	N7010-64
Core-57	Up	N7010-64	Up	N7010-64	F000000056	N7010-64
Core-58	Up	N7010-64	Up	N7010-64	F000000057	N7010-64
Core-59	Up	N7010-64	Up	N7010-64	F000000058	N7010-64
Core-60	Up	N7010-64	Up	N7010-64	F000000059	N7010-64
Core-61	Up	N7010-64	Up	N7010-64	F000000060	N7010-64
Core-62	Up	N7010-64	Up	N7010-64	F000000061	N7010-64
Core-63	Up	N7010-64	Up	N7010-64	F000000062	N7010-64
Core-64	Up	N7010-64	Up	N7010-64	F000000063	N7010-64
Core-65	Up	N7010-64	Up	N7010-64	F000000064	N7010-64
Core-66	Up	N7010-64	Up	N7010-64	F000000065	N7010-64
Core-67	Up	N7010-64	Up	N7010-64	F000000066	N7010-64
Core-68	Up	N7010-64	Up	N7010-64	F000000067	N7010-64
Core-69	Up	N7010-64	Up	N7010-64	F000000068	N7010-64
Core-70	Up	N7010-64	Up	N7010-64	F000000069	N7010-64
Core-71	Up	N7010-64	Up	N7010-64	F000000070	N7010-64
Core-72	Up	N7010-64	Up	N7010-64	F000000071	N7010-64
Core-73	Up	N7010-64	Up	N7010-64	F000000072	N7010-64
Core-74	Up	N7010-64	Up	N7010-64	F000000073	N7010-64
Core-75	Up	N7010-64	Up	N7010-64	F000000074	N7010-64
Core-76	Up	N7010-64	Up	N7010-64	F000000075	N7010-64
Core-77	Up	N7010-64	Up	N7010-64	F000000076	N7010-64
Core-78	Up	N7010-64	Up	N7010-64	F000000077	N7010-64
Core-79	Up	N7010-64	Up	N7010-64	F000000078	N7010-64
Core-80	Up	N7010-64	Up	N7010-64	F000000079	N7010-64
Core-81	Up	N7010-64	Up	N7010-64	F000000080	N7010-64
Core-82	Up	N7010-64	Up	N7010-64	F000000081	N7010-64
Core-83	Up	N7010-64	Up	N7010-64	F000000082	N7010-64
Core-84	Up	N7010-64	Up	N7010-64	F000000083	N7010-64
Core-85	Up	N7010-64	Up	N7010-64	F000000084	N7010-64
Core-86	Up	N7010-64	Up	N7010-64	F000000085	N7010-64
Core-87	Up	N7010-64	Up	N7010-64	F000000086	N7010-64
Core-88	Up	N7010-64	Up	N7010-64	F000000087	N7010-64
Core-89	Up	N7010-64	Up	N7010-64	F000000088	N7010-64
Core-90	Up	N7010-64	Up	N7010-64	F000000089	N7010-64
Core-91	Up	N7010-64	Up	N7010-64	F000000090	N7010-64
Core-92	Up	N7010-64	Up	N7010-64	F000000091	N7010-64
Core-93	Up	N7010-64	Up	N7010-64	F000000092	N7010-64
Core-94	Up	N7010-64	Up	N7010-64	F000000093	N7010-64
Core-95	Up	N7010-64	Up	N7010-64	F000000094	N7010-64
Core-96	Up	N7010-64	Up	N7010-64	F000000095	N7010-64
Core-97	Up	N7010-64	Up	N7010-64	F000000096	N7010-64
Core-98	Up	N7010-64	Up	N7010-64	F000000097	N7010-64
Core-99	Up	N7010-64	Up	N7010-64	F000000098	N7010-64
Core-100	Up	N7010-64	Up	N7010-64	F000000099	N7010-64

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 19: Select multiple toggle

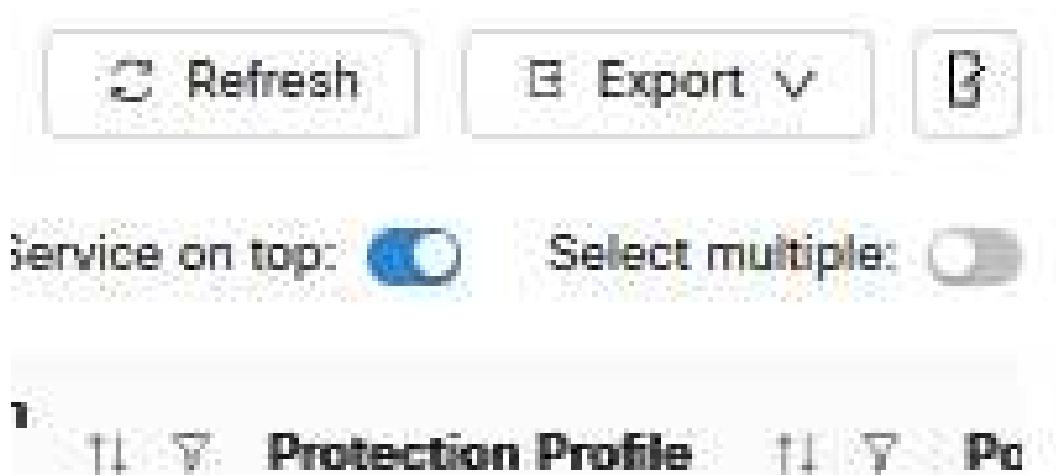
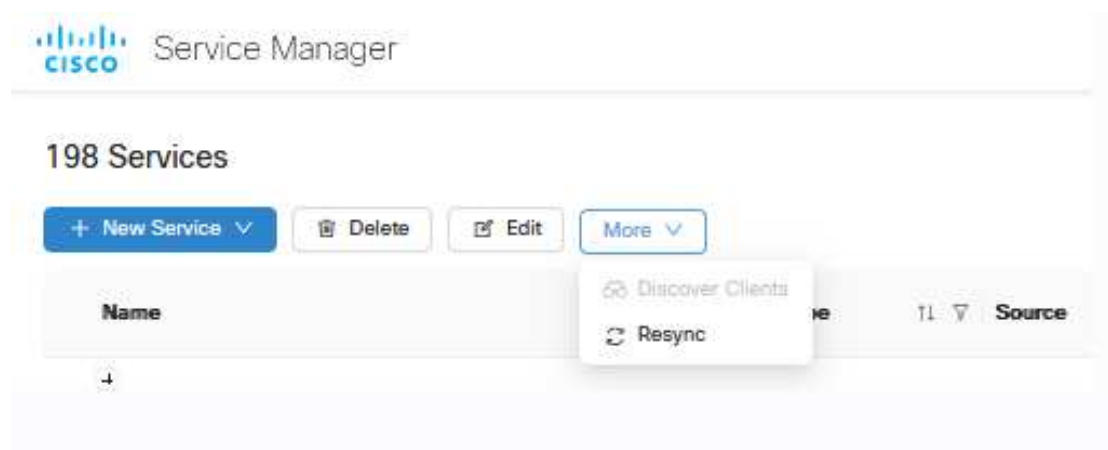


Figure 20: Resync option for GMPLS circuits

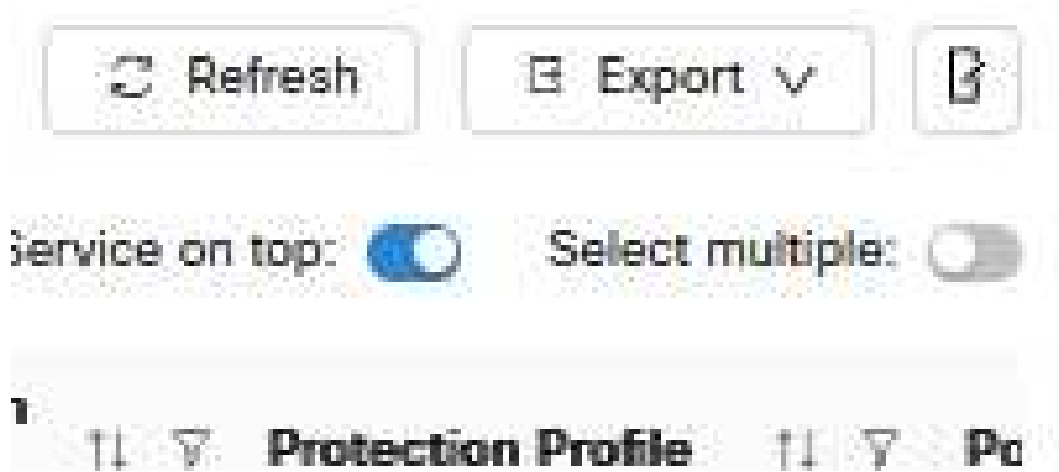


- Resyncing can resolve lifecycle state issues, for example, when the circuit is in PARTIAL, where clients are not discovered properly or are in an ambiguous state.
- When multiple services are selected, the **More** button is replaced with a **Resync** button.
- Resyncing a trail service also resyncs 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 21: 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 22: Service Manager



Service manager table fields

Column	Values	Description
Name		Name of the service

Column	Values	Description
Type	OCH-NC	Type of the service
	OCH-Trail	
	OCH-CC	
Source	—	Source Node and Port
Destination	—	Destination Node and Port
Control Plane	GMPLS	Control Plane Protocol
	CPCE	

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

Column	Values	Description
Admin State	UNLOCKED	The circuit is administratively enabled and available for use.
	LOCKED	The circuit is administratively disabled and unavailable for use.
Frequency (THz)		Optical carrier frequency at which the circuit will operate within the DWDM spectrum.
Bandwidth (GHz)		Bandwidth used by the circuit
Protection profile	PROTECTED	The circuit is configured with PSM protection to ensure service availability in case of failure.
	UNPROTECTED	The circuit is not configured with any protection mechanism, and may be subject to service disruption in case of failure.
Port Rate	10GE	Data rate
	40GE	
	100GE	
	400GE	
	OTU2	
	OTU2E	
	OTU4	
	OC192/ STM-64	
	FC16	
	FC32	
Discovery Date	—	Service discovery date
Restoration Type	None	No restoration is configured for the circuit.
	Enabled	Restoration is enabled for the circuit, and the network will automatically attempt to restore the circuit upon failure by calculating restoration path based on restoration constraints.
	Restorable Alternate	Restoration is enabled for the circuit, and the network will automatically attempt to restore the circuit upon failure by calculating restoration path based on restoration constraints and main path constraints alternatively.
	Enabled and Revertive(Automatic)	Restoration is enabled, and the circuit will automatically revert to the original (home) path after the failure is resolved and unverified alarms are manually cleared from COSM.
	Enabled and Revertive(Manual)	Restoration is enabled, and manual intervention is required to revert the circuit to the original (home) path after the failure is resolved.
Tags	—	Tags attached to the Service during circuit provisioning.

Provision CPCE services

Use the following procedure to create and manage circuits.

- The OCH-Traffic 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-Traffic circuit automatically.

Before you begin

Table 6: Supported transponder cards and modes

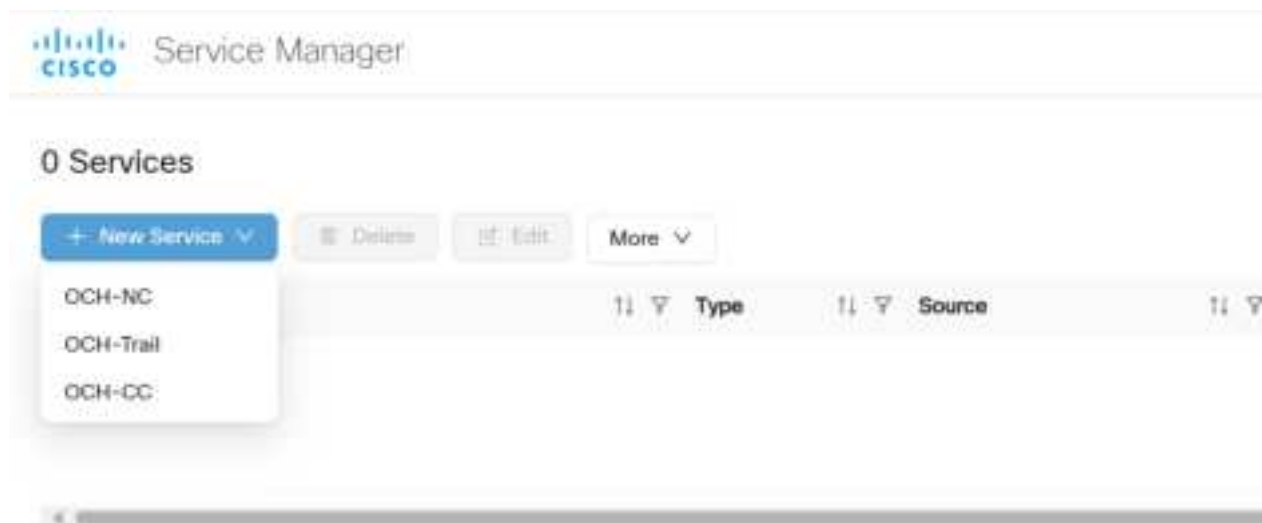
Card	Modes Supported
NCS1K4-2-QDD-C-K9	MXP-SLICE: 200G, 300G, 400G trunk and 100G and OTU4 client
NCS1K4-QXP-K9	MXP-SLICE: 400G trunk with 400G and 100G client
NCS1K4-OTN-XP	MXP: 4x100G TXP: 400G 400G trunk with 100G, 10G and OTU2 clients
NCS1K14-2.4T-X-K9	MXP-SLICE: 400G, 600G, 800G, 1T, 1.2T trunk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

**Note**

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

Procedure

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

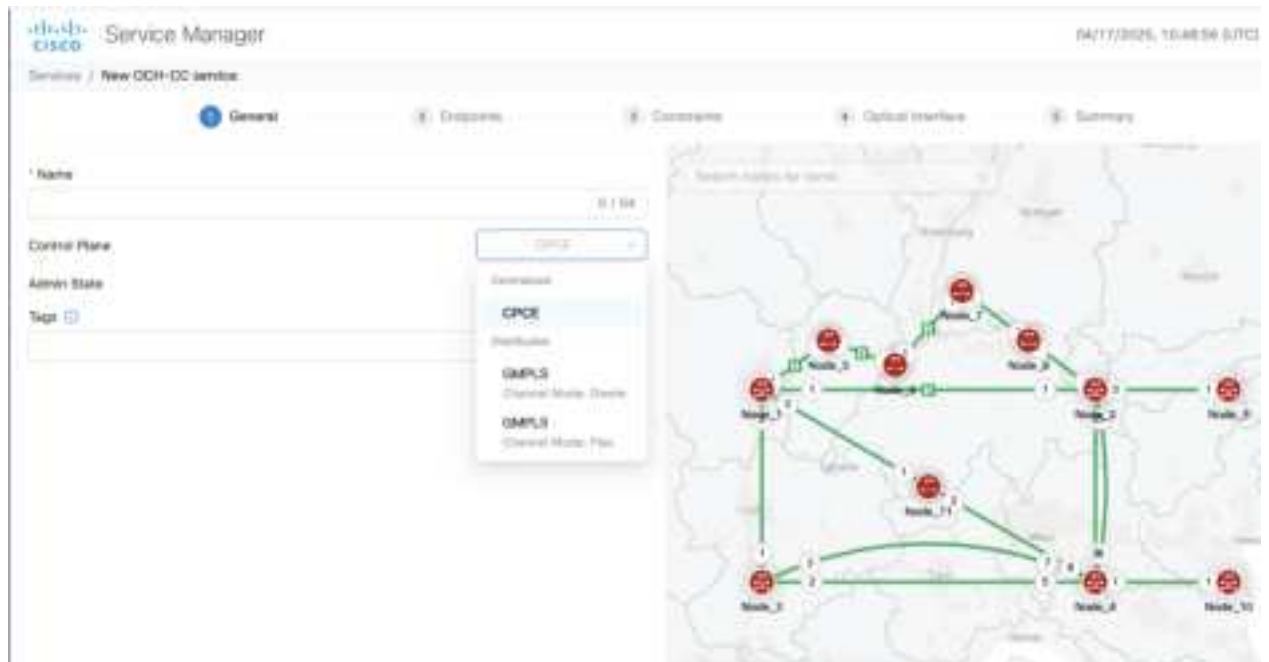


Step 2 Select **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

Note

- **OCH-NC:** An OCH-NC is a circuit established between add/drop ports on terminal OLTs (Optical Line Terminals) or ROADMs (Reconfigurable Optical Add-Drop Multiplexers). This type of circuit typically connects end-user equipment to the optical network.
- **OCH-Trail:** An OCH-Trail is a circuit established between trunk ports of transponders or muxponders. This type of circuit typically transports aggregated traffic across the optical core network.
- **OCH-CC:** An OCH-CC is a circuit established between cards within optical devices, such as transponders, muxponders, or ROADMs. This type of circuit facilitates internal cross-connections within the optical equipment.

Figure 23: Service Manager



Service Manager launches the new service wizard.

Step 3

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

Figure 24: Service Manager

The screenshot shows the Cisco Service Manager interface for creating a new OCH-CC service. The breadcrumb trail is 'Services / New OCH-CC service'. The 'General' tab is active, showing the following configuration details:

- Name:** test_cpce (9 / 64 characters)
- Control Plane:** CPCE (dropdown menu)
- Admin State:** Enabled (radio buttons for Enabled/Disabled)
- Tags:** test_cpce (9 / 15 characters, with a '+' button to add more)

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

Table 7: 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 25: Service Manager

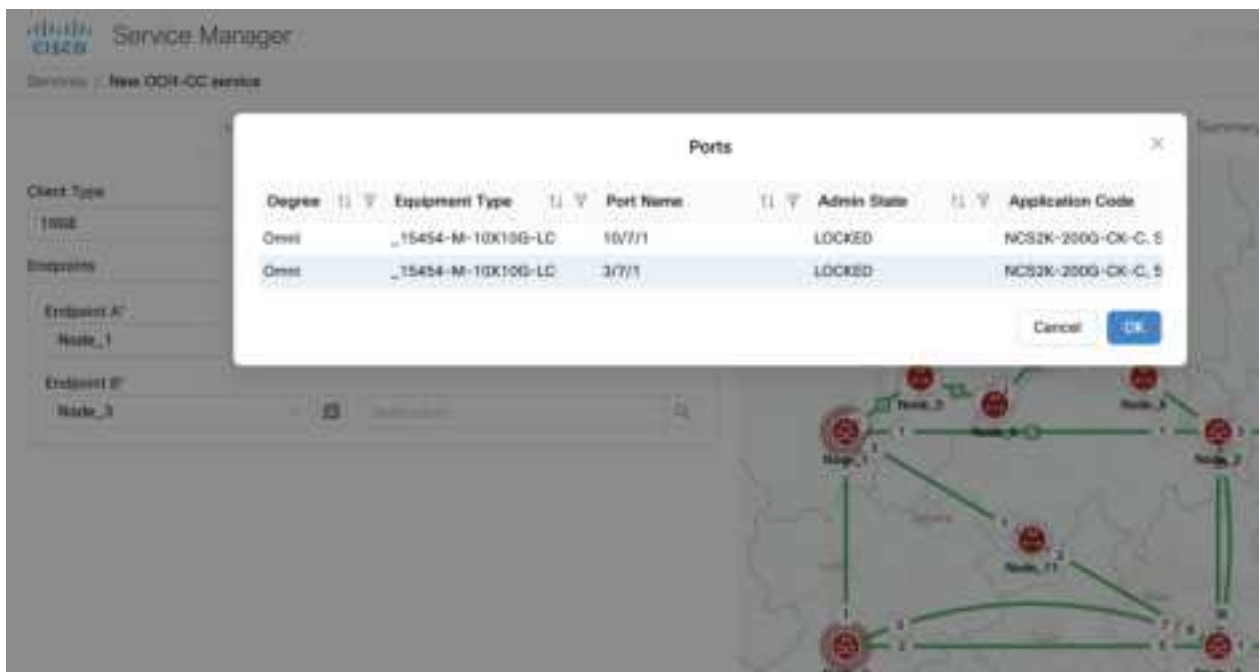


Table 8: Endpoints Parameters

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 26: Service Manager

Service Manager

Services / New OCH-CC service

General Endpoints 3 Co

Optical Feasibility Threshold ⓘ

Select

Optimization Goal ⓘ

None

☐ Allow Auto Regeneration

Path

☒ Include nodes or links ⓘ

Select node Select links

☐ Exclude nodes or links ⓘ

Select node Select link

Service Diversity ⓘ

Select service

☐ Ignore Alarms ⓘ

Cancel Back Next

Table 9: Constraint parameters

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

Note

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

Step 6

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

Table 10: 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 preview the circuit in the topology before it is created.

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

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

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

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

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

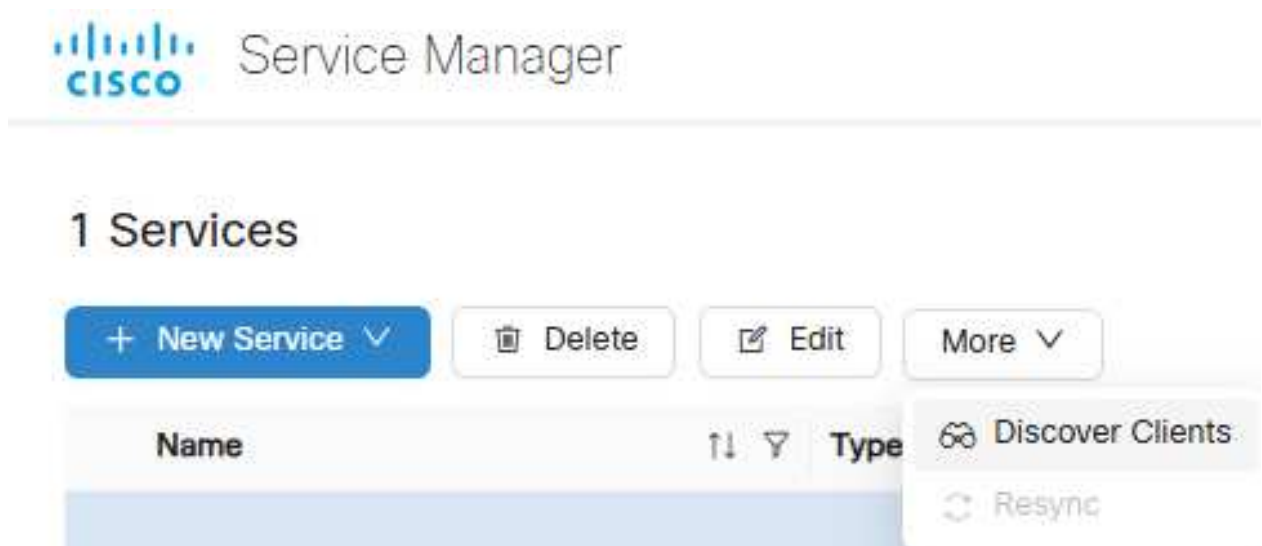
Step 11 Click **Delete** option to delete a selected service from the table.

Note

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

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

Figure 27: Service Manager



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

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

Step 14

Troubleshoot CPCE Services

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

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

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

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

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

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

Provision GMPLS services

Use the following procedure to create and manage circuits.

Before you begin

Table 11: Supported transponder cards and modes

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

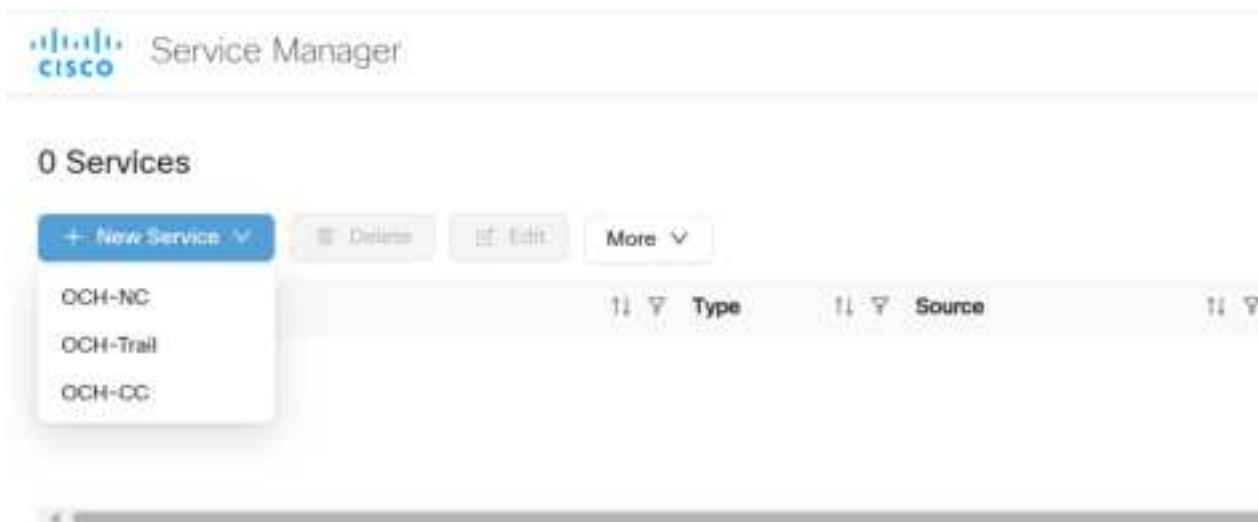
Card	Modes Supported
NCS1K4-1.2T-K9	MXP: 100G, 200G, 300G, 400G trunk with 100G and OTU4 client MXP-SLICE: 2 trunks with 100G, 200G, 300G, 400G bandwidth and 100G and OTU4 client Supports SD-FEC-27 and SD-FEC-15
NCS2K-400G-XP-LC	MXP: 400G trunk and 100g, 10G clients FEC Modes: SD_FEC_15_DE_OFF, SD_FEC_15_DE_ON, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON
NCS2K-200G-CK-C	TXP-100G: 100G trunk and client FEC Modes: HG_FEC_7, SD_FEC_20, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON
15454-M-10X10G-LC=	MXP 10x10G (with backplane connection to NCS2K-200G-CK-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients



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

Procedure

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



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

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

Note

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

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

Service Manager launches the new service wizard.

Step 3 Enter the details in the General tab and click **Next**.**Figure 28: Service Manager**

The screenshot shows the 'General' tab of the Service Manager configuration wizard. It includes the following fields and controls:

- Name:** A text input field containing 'GMPLS-2341' with a character count of 10 / 64.
- Control Plane:** A dropdown menu currently set to 'GMPLS', with 'Dwdm' also visible as an option.
- Label:** A text input field containing 'video' with a character count of 5 / 32.
- Admin State:** Two radio buttons, 'Enabled' (selected) and 'Disabled'.
- Tags:** A section with a plus icon, a text input field containing 'core', and a character count of 0 / 15.

Table 12: General Parameters

Field	Description	Values/restrictions
Name	The unique user defined name of the link.	(Allowed characters are a-z, A-Z, 0-9 and _ . <Space not allowed>).
Control Plane	GMPLS Dwdm OR GMPLS Flex	—
Label	This label is assigned to the NCS 2000 cross-connects.	A label is autogenerated if the field is left blank.
Admin State	The admin state of the service	Enabled or Disabled

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

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

Figure 29: Service Manager

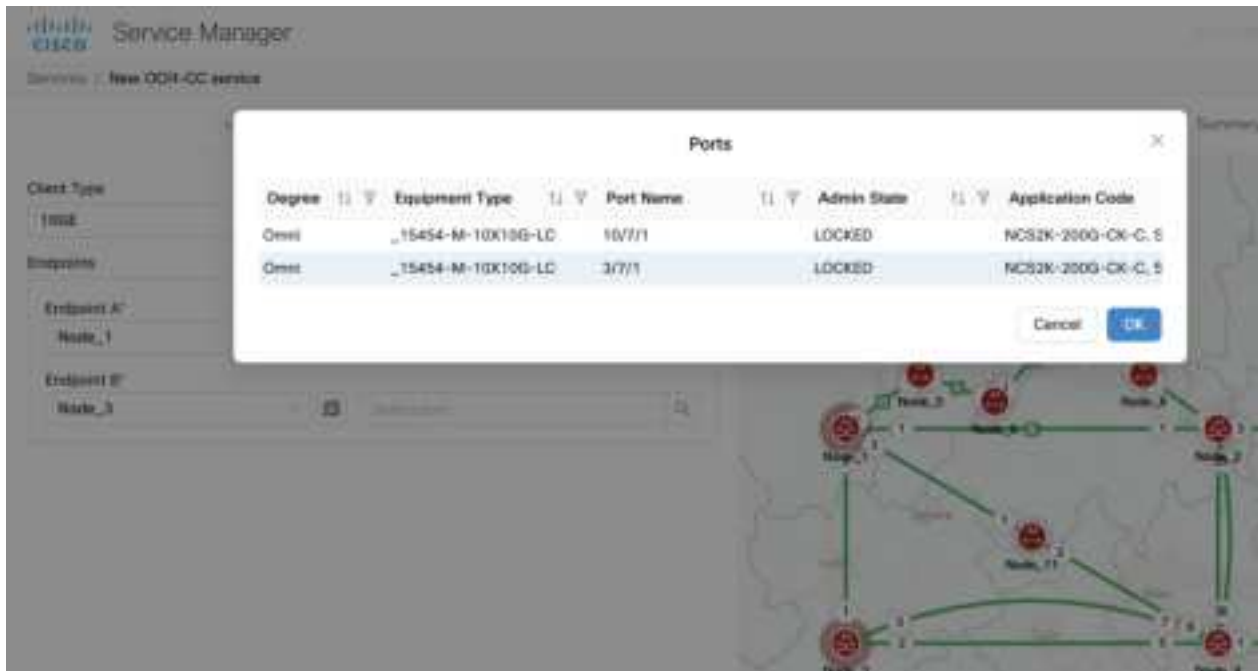


Table 13: Endpoints Parameters

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 30: Service Manager

The screenshot shows the Cisco Service Manager interface for editing the TRAIL-test_flex service. The breadcrumb trail is "Services / Editing TRAIL-test_flex service". At the top, there are three tabs: "General" (selected), "Endpoints", and "C". Below the tabs, there are two sub-tabs: "General" (selected) and "Restoration". A dropdown menu is set to "Select". Under the "Path" section, there are two main options: "Include nodes or links" (selected) and "Exclude nodes or links". Each option has a "Select node" dropdown and a "Select links" search field. Below the "Include nodes or links" section, it shows "1 Node(s) or Link(s) selected". Below the "Exclude nodes or links" section, it shows "1 Service(s) selected". Under the "Diversity Type" section, there is a "Select Type" dropdown. Under the "Service Diversity" section, there is a "Select service" search field. Below the "Service Diversity" section, it shows "1 Service(s) selected" with a list item "NODE TRAIL-test" and a toggle switch. At the bottom, there is a checkbox for "Ignore Alarms". Navigation buttons "Cancel", "Back", and "Next" are at the bottom right.

Service Manager

Services / Editing TRAIL-test_flex service

✓ General ———— ✓ Endpoints ———— ✓ C

General Restoration

Select

Path

- Include nodes or links ⓘ
Select node Select links 🔍 ⓘ
▶ 1 Node(s) or Link(s) selected
- Exclude nodes or links ⓘ
Select node Select link 🔍 ⓘ
▼ 1 Service(s) selected
NODE TRAIL-test 🔍

Diversity Type Service Diversity ⓘ
Select Type Select service 🔍

▼ 1 Service(s) selected

Ignore Alarms ⓘ

Cancel Back Next

Table 14: General constraints

Field	Description	Values/restrictions
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	Select RED, GREEN, YELLOW or ORANGE. GREEN = mean value YELLOW = +1 sigma ORANGE = +2 sigma RED = +3 sigma
Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	—
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	—
Diversity Type	Choose the type of service diversity	Node, link, or srlg
Service Diversity	Select one or more existing services from the 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.

Step 6

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

Figure 31: Service Manager

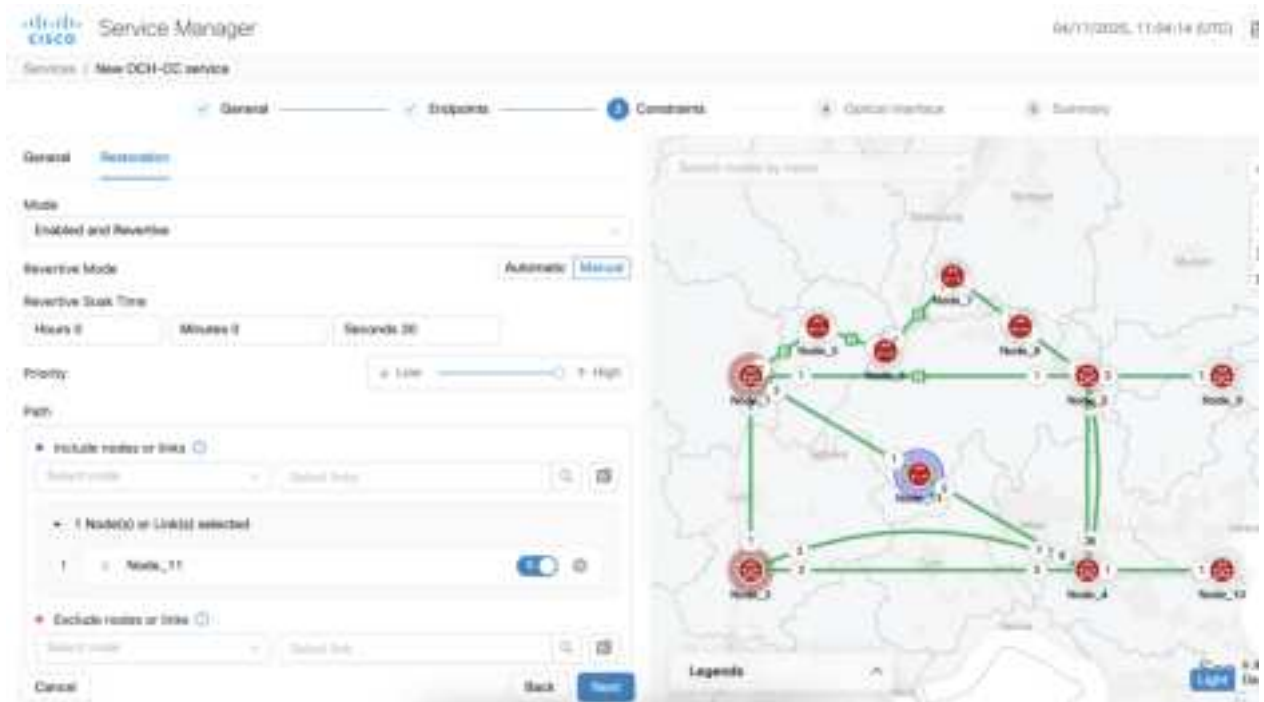


Table 15: Restoration constraints

Field	Description	Values/restrictions
Mode	—	None, Enabled, Restorable Alternate, Enabled and Revertive
Revertive Mode	Specifies if the revert to main path after it up after a 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.

Step 7

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

Table 16: 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

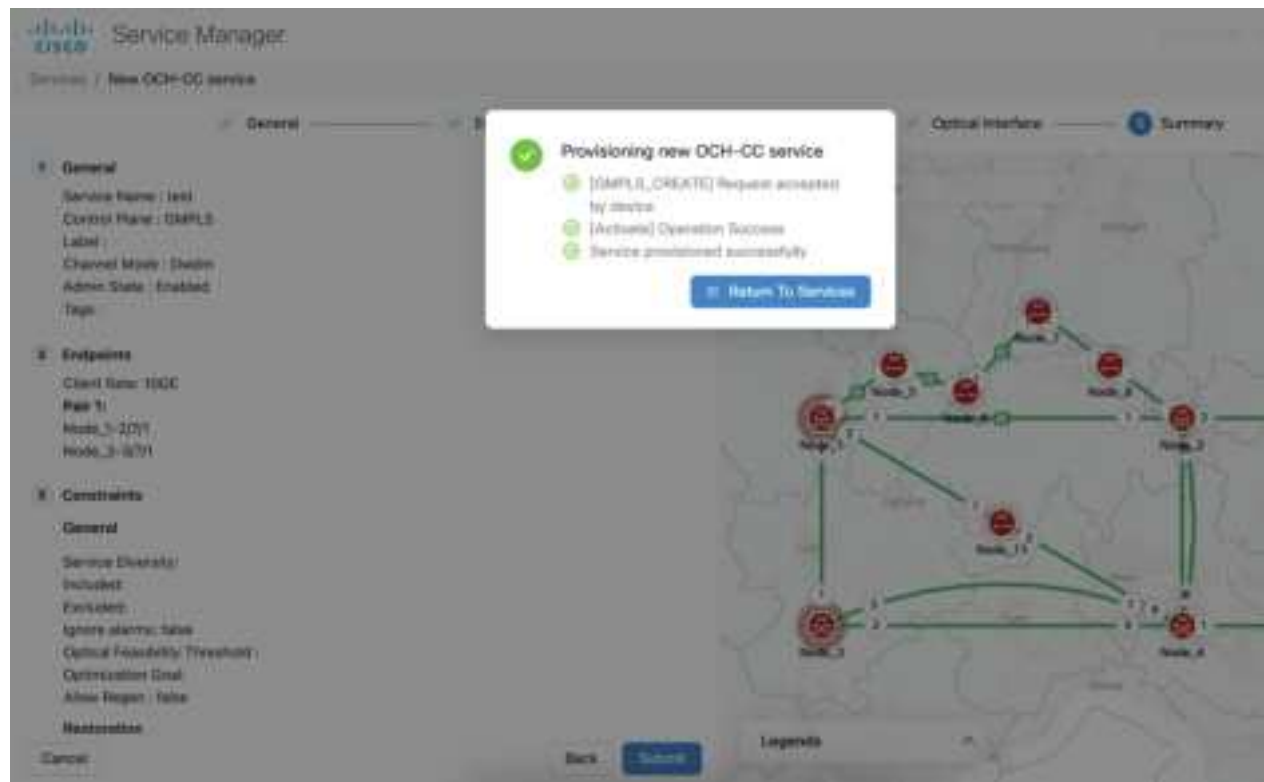
- For OCH-trail, Optical Interface fields are auto populated and non-editable.

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

Step 8

Click **Finish** to create the circuit.

Figure 32: 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 33: Service Manager

Note

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

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

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

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

Note

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

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

Table 17: Deletion failure scenarios

Reason	Troubleshooting
Cross connect was deleted outside Cisco Optical Network Controller	• Retry deleting the service • Use the resync option in Service Manager and try again • Perform an full network resync and try again • Try deleting the service from Cisco Transport Controller
Node busy	Wait for any operations on the node to complete and retry
Node disconnected	Reestablish connectivity to the node
COSM lost connection to the subtended device	Reestablish COSM connectivity to the device and try again

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

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

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

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

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

Alarms

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

Figure 34: Alarms

Node Name	Severity	Alarm Type	Time Stamp	Object	Description	Service Affect
example1	Critical	OTS-P	03/05/2024, 10:01:00	OTS-105/AD-4-11-1-40	Receiving Platform Single Record	SA
example2	Warning	USER-LOGIN	03/05/2024, 10:01:00	SYSTEM	Login of User	SA
example3	Major	NO-CONNECTED	03/05/2024, 14:01:00	DEVICE-1000-2000	Connection To Managed Node Lost	SA
example4	Warning	USER-LOGOUT	03/05/2024, 14:01:00	SYSTEM	Logout of User	SA
example5	Warning	USER-LOGIN	03/05/2024, 10:01:00	SYSTEM	Login of User	SA
example6	Major	SAV-UPGRADE-NO-ALLOWED	03/05/2024, 14:01:00	MODULE-1000	SAV Upgrade is not allowed on SA-Group	SA
example7	Warning	PM-TLS-Sys	03/05/2024, 09:00:00	OTLS-1000	PM-TLS-Sys-1000s Sys-1000s-1000	SA

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

Figure 35: Alarms History

Node Name	Severity	Service Affect	Alarm Type	Time Stamp	Object	Description
example2p_x20_Nodes	Critical	SA	OPAW-LINK	03/05/2024, 09:10:00	OTLS-1000	OTLS-1000-2000
example2p_x20_Nodes	Critical	SA	OPAW-LINK	03/05/2024, 09:10:00	OTLS-1000	OTLS-1000-2000
example2p_x20_Nodes	Major	NSA	PM-UPD-REQUIRED	03/05/2024, 10:00:00	MODULE-1000	PM-UPD-REQUIRED
example2p_x20_Nodes	Critical	SA	OPAW-LINK	03/05/2024, 09:10:00	OTLS-1000	OTLS-1000-2000

Table 18: Alarm Table Fields

Field Name	Description	Example/Values
Node Name	The name of the node where the alarm originated.	Node identifier/name (e.g., NODE-001)
Severity	The severity level of the alarm.	Critical, Major, Minor, Warning, Cleared
Alarm Type	The type of alarm.	LOSP, NODE-DISCONNECT
Time Stamp	The date and time when the alarm was raised.	YYYY-MM-DD HH:MM:SS.SSS
Object	The object associated with the alarm.	NODE: Node_1, SYSTEM, CHASSIS: 5
Description	A detailed description of the alarm.	Text describing alarm details
Alarm Category	The category of the alarm. See Alarm Categories , on page 129.	CONC_SYSTEM, SECURITY, EQUIPMENT
Service Affect	Indicates whether the alarm is service affecting or non-service affecting.	NSA, SA
Location	The physical location of the affected equipment.	
Direction	The direction of the alarm.	Receive,
User Tag	User-defined tags for categorizing and filtering alarms. Note • User tags propagate from parent to child components of a chassis by default. A user tag on a child component overrides the inherited tag from its parent. • User Tag information comes from Cisco Optical Site Manager. See User Tags. • User tags are not supported on system-level and device alarms. • User tags can apply CLI (Common Language Location Identifier), a standardized 11-character code that uniquely identifies geographic locations and equipment for network sites, network support sites, and customer locations.	Custom tags/labels
User Notes	User-added notes or comments related to the alarm.	Free-form text

Field Name	Description	Example/Values
Acknowledge	Indicates whether the alarm has been acknowledged.	Acknowledged, Unacknowledged
UUID	Unique Universal Identifier for the alarm.	UUID string
Correlation Type	The type of correlation applied to the alarm.	Network Level, Node Level



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

Procedure

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

Step 2 Select the **Alarms** tab to view the active alarms of each node.

Step 3 Select an alarm or multiple alarms and click **Annotation** to add user notes to any alarm

a) Enter the user notes and click **Add**.

Note

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

This will send a notification for the alarm.

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

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

Figure 36: 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

- The maximum time period is 3 months. If you select a time range more than 3 months using custom date range, Cisco Optical Network Controller throws an error.
- Alarm history queries are rate limited. You can query up to 5 alarms history in a minute.

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

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

Note

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

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

Note

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

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

Note

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

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

Note

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

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

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

Note

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

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

Note

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

Figure 37: User Notes

Direction	User Notes	Acknowledge
NA		
NA		
NA		
NA		
NA		
NA	User Notes admin 07/16/2024, 06:02:39 user note 3 admin 07/16/2024, 06:02:28 user note 2 admin 07/16/2024, 06:02:18 use note 1	
		 07/15/2024, 11:05:15
		 07/15/2024, 11:48:46
		 07/15/2024, 11:48:46

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.



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

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

Figure 38: Alarms History

64 Alarms

Major: 3 Critical: 0 Minor: 0 Warning: 61

Node Name	Severity	Alarm Type	Time Stamp	Object	Description	Service Affect	Location	Status
00000001	Warning	LOP-LOP	06/11/2025, 09:00:00.000	00000001	Loss of Power	000	0000	Yes
00000002	Critical	LOS	06/11/2025, 09:00:00.000	00000002	Loss of Signal	000	0000	Yes
00000003	Warning	ALD	06/11/2025, 09:00:00.000	00000003	Automatic Load Shedding	000	0000	Yes
00000004	Minor	NEF-NEF	06/11/2025, 09:00:00.000	00000004	Neighbour Node Fault	000	0000	Yes
00000005	Critical	LOS-P	06/11/2025, 09:00:00.000	00000005	Security/Physical Signal Received	000	0000	Yes
00000006	Critical	LOP-LOP	06/11/2025, 09:00:00.000	00000006	Optical Power Failure Loss	000	0000	Yes
00000007	Critical	LOS-P	06/11/2025, 09:00:00.000	00000007	Security/Physical Signal Received	000	0000	Yes

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 19: Alarms suppressed by LOS on line

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

**Note**

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

Benefits of Using NLAC

The benefits of using NLAC are:

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

Acknowledged Alarm Mute

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

Purpose of Acknowledged Alarm Mute

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

Benefits of Using Acknowledged Alarm Mute Option

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

Muting the Acknowledged Alarms

To mute the alarms on the screen:

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



Note

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

Notifications for Acknowledged Alarm Mute

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

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

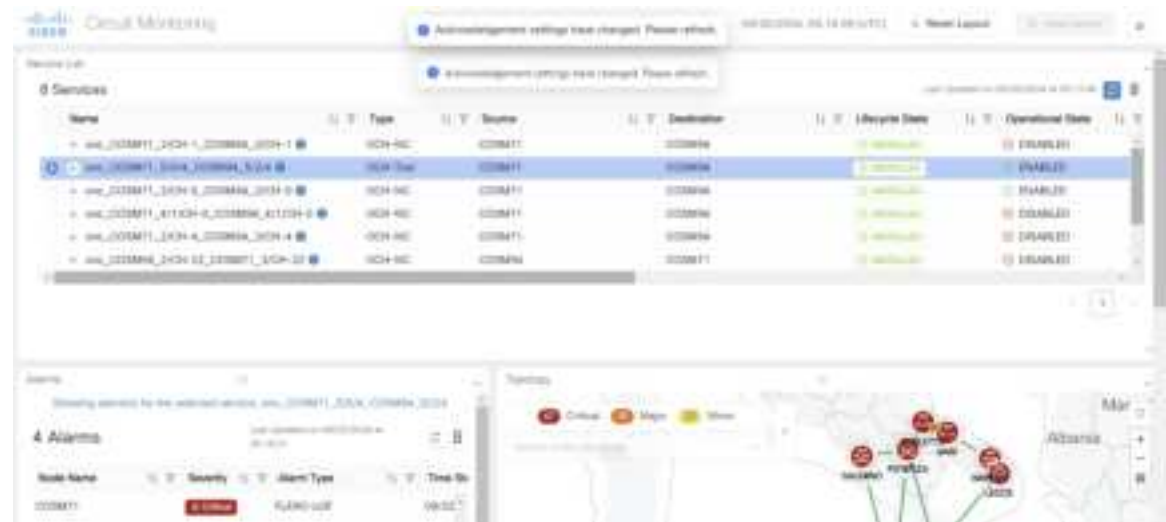
**Note**

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

Figure 39: Mute Acknowledged Alarms in Topology



Figure 40: 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, on page 163](#).

Procedure

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

Step 2 Create a New SNMP Manager.

a) Enter the Server Name and IP Address.

Cisco Optical Network Controller supports only IPv4.

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

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

New SNMP trap configuration

Server Name*

Demo_UDP_106

IP Address*

10.58.251.85

Destination Trap Port Number*

6002

SNMP Version*

V2C

Community*

Notification Type*



UDP



TCP

Trap configuration*



Send all traps



Set custom trap filters

Cancel

Create

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

New SNMP trap configuration

Server Name*
Demo_UDP_106

IP Address*
10.58.251.85

Destination Trap Port Number*
6002

SNMP Version*
V3

User Name*
snmpv3user

Mode*
authPriv

Authentication Type*
[Empty]

Authentication Password
[Empty]

Confirm Authentication Password
[Empty]

Privacy Type*
Select Privacy Type

Privacy Password
[Empty]

Confirm Privacy Password
[Empty]

Notification Type*
☒ UDP
 ☐ TCP

Trap configuration*
☐ Send all traps
☒ Set custom trap filters

Cancel Create

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

Step 3 Configure alarm filters.

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

The custom trap filter configuration pop-up



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

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

Workspaces

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

Types of Workspaces

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

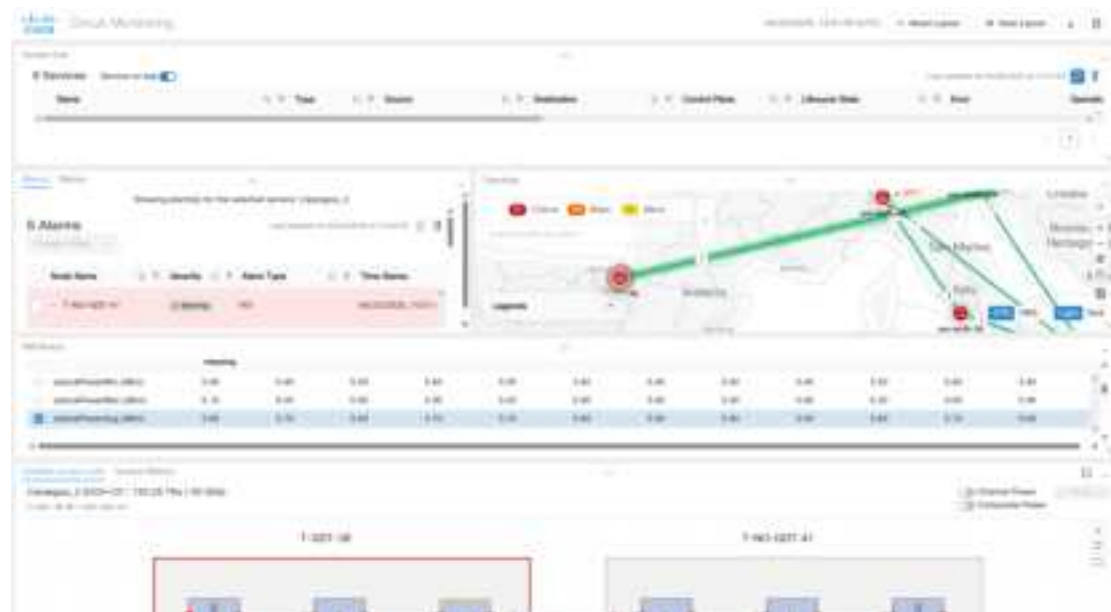
Figure 41: Workspaces Network Monitoring



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

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

Figure 42: Circuit Monitoring





Note

-
- In the **Alarms** screen above, select any alarm and right click followed by **Show Affected service(s)**. This will display all the services related to the selected alarm in the services layout.
 - From release 24.3.1, PM tab is available in the **Circuit Monitoring** workflow application.
 - From release 25.1.1, you can select multiple links or nodes in the topology.
 1. Click **Select node(s)/link(s)** in topology.
 2. Use the OTS/OMS toggle to select the segment type.
 3. Click the nodes or links you want to select.

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

The service list shows affected services for the selected nodes and links. The list shows the services that are with paths through all the selected nodes and links.
 5. Click **Refresh data and reset the layout** in **Service List** to reset the table to show all services.
 - From release 25.1.1, alarms history can be viewed for each circuit.
 1. Select a service from the service list.
 2. Click **History** in the **Alarms** tab.
 3. Choose a time period for which you want to view the alarm history from the **Select Time period** drop down list, or choose a custom date range.

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

 - The maximum time period is 3 months. If you select a time range more than 3 months using custom date range, Cisco Optical Network Controller throws an error.
 - Alarm history queries are rate limited. You can query up to 5 alarms history every minute.
 - **Detailed service path**
 - Select a service from the service list to view its detailed service path.
 - Use the **Channel Power** and **Composite Power** toggles to enable and disable the power display for all ports in the detailed service path.
 - Hover over a port or equipment in the detailed service path to view a tooltip with additional information.
 - PM history
 - Select a service from the service list.

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

Figure 43: PM History in Circuit Monitoring



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

• Service History

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

Figure 44: PM History in Circuit Monitoring



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

- **Visualise Circuit Restoration**

- Select a Service from the Service List to highlight the circuit in the topology.

Figure 45: Topology in circuit monitoring workspace



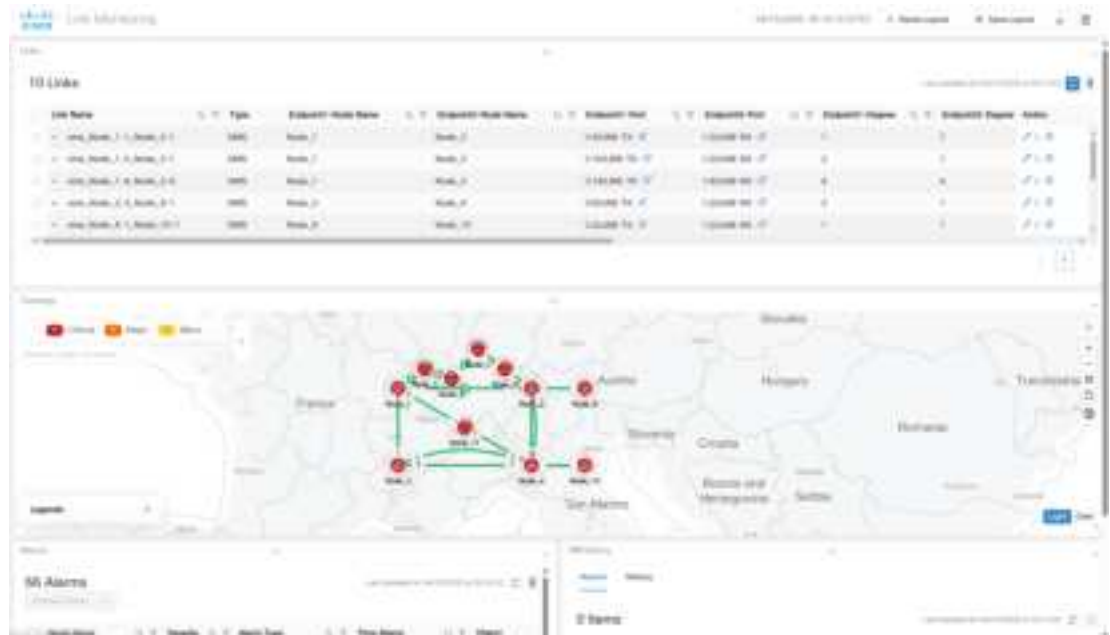
- If the circuit has undergone restoration due to a fiber cut, topology shows the new path and the main path. The main path is represented by dotted lines.

Figure 46: Topology in circuit monitoring workspace



- You can also see the service restoration and related events in Service History.
 - Restoration State column in the Service list also displays the restoration state of the service.
-
- **Link Monitoring Workspace:** Focuses on individual links, displaying their alarms, performance history, topology, and associated circuits.

Figure 47: 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.

Your selection is bidirectional. The link you select from the Links list is highlighted in topology. The nodes and links you select in topology are filtered in the links list.

- In links table, click **edit link** in the action column to edit link details.
- You can cross launch circuit monitoring for circuits using a link by clicking **View Circuit Monitoring** in the action column.
- In links table only forward/reverse ots can be selected.
- You can select multiple links or nodes in the topology.
 1. Click **Select node(s)/link(s)** in topology.
 2. Use the OTS/OMS toggle to select the segment type.
 3. Click the nodes or links you want to select.

You can select up to 20 entities at a time. Multiple selection is available only for ots links.

4. Click **Show services**.

The service list shows affected services for the selected nodes and links. The list shows the services that are with paths through all the selected nodes and links.

5. Click **Refresh data and reset the layout** in **Service List** to reset the table to show all services.



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

Procedure

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

Software Image Management and Upgrade

The Software Image Management and Upgrade (SWIMU) is a Cisco Optical Network Controller 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 20: 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 21: 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 22: 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.

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

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.

- Modify the details.
- Click **Check Connectivity Status**.
- 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 48: 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 124 alarm is raised.

Procedure

Step 1

Create a nodes group

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

Note

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

Step 2

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

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

- 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 123](#) alarm is raised.
- If the upload of a backup to the SFTP server fails, the [UPLOAD-FAILURE, on page 125](#) alarm is raised.

Procedure

Step 1

Perform an **On-demand** backup.

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

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

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

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

Step 5

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

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

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

Note

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

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

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

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

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

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

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

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

Replace the placeholders with actual file names and key.

This command generates the decrypted backup file.

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

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

- e)

Orchestrate Upgrades

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

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

Before you begin

- For the backend upload to proceed you must configure the router static settings for each node separately. See [Configure Static Route on Peer Devices](#) for more details on how to configure the static routes of a node.
- The Cisco Optical Network Controller time must be the same as the device time.
- You must download the golden ISO from software.cisco.com 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 50: 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 Manage groups from the topology view in the **Upgrade Orchestrator**.

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

Note

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

You cannot edit NCS 2000 groups.

You cannot add NCS 2000 nodes to NCS 1000 groups.

Step 3 Create an Image Distribution Job.

- a) Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade > Image Distribution Jobs**
- b) Click **Distribute Image**.
- c) Select the nodes or groups you want to distribute the images to.
- d) Select an SFTP server from the dropdown list or give the details of the SFTP server.
- e) Select the ISO image file to distribute.
- f) Schedule the job to start immediately or later.
- g) Click **Schedule** and choose a later time or schedule the job to run immediately.
- h) Click the status for a device in the status column to view detailed status.
- i) Select a job and click **Stop** to stop the job in the nodes in which the job has not started.

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

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

A job that is in progress cannot be edited.

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

Note

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

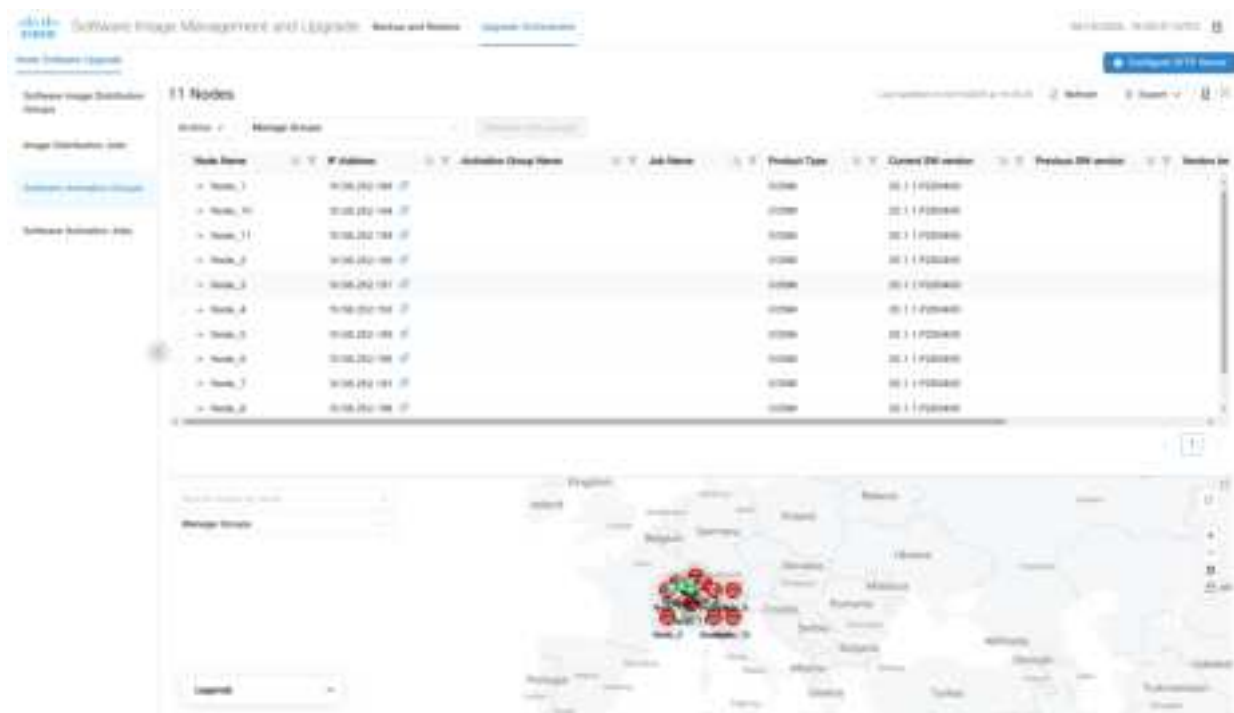
If a job status is **PARTIAL**, it means the job succeeded for some of the nodes, but failed for other nodes in the group of devices that the job was initiated for.

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

Step 4 Create Software Activation Groups.

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

Figure 51: Upgrade Orchestrator



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

- Click **Actions** and select **Expand all** to expand nodes in the table to view the individual devices.
- Click **Manage Groups** and select **New Group**.
- Enter a Group Name and Description.
- Select the nodes or individual devices to include in the group and click **Manage Groups**.
- Click the + icon next to a group name to add the nodes to the group.
- Select a node and click **Remove from groups** to remove the node from the group it is a member of.

Note

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

You cannot edit NCS 2000 groups.

You cannot add NCS 2000 nodes to NCS 1000 groups.

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

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

Step 6 Create a Software Activation Job.

- Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade > Software Activation Jobs**
- Click **Activate Software**.
- Select the target devices or groups.
- Choose the software package from the drop-down.
- Schedule the job to start immediately or later.
- Click **Schedule** and choose a later time or schedule the job to run immediately.
- 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.

- 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.

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

A job that is in progress cannot be edited.

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

Figure 52: 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 23: Benefits of PM History

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

Time Range for Fetching Data

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

Table 24: Time Range for Fetching Data

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

Data Collection and Storage

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

Types of PM History Reports

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

Table 25: Types of PM History Report

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



Note

- For both 15-Minute or 24-Hour granularity PM report, you can use the horizontal scroll bar to adjust the dates as per your need. For 15-Minute granularity archive data is available for download from 3 to 5 days and for 24 hours granularity from 31 to 93 days.
- If the date range falls on archive data then you will receive a message to indicate the user has chosen a time range which coincides with the archived data time range.

Figure 53: 15-Minute Granularity PM Report

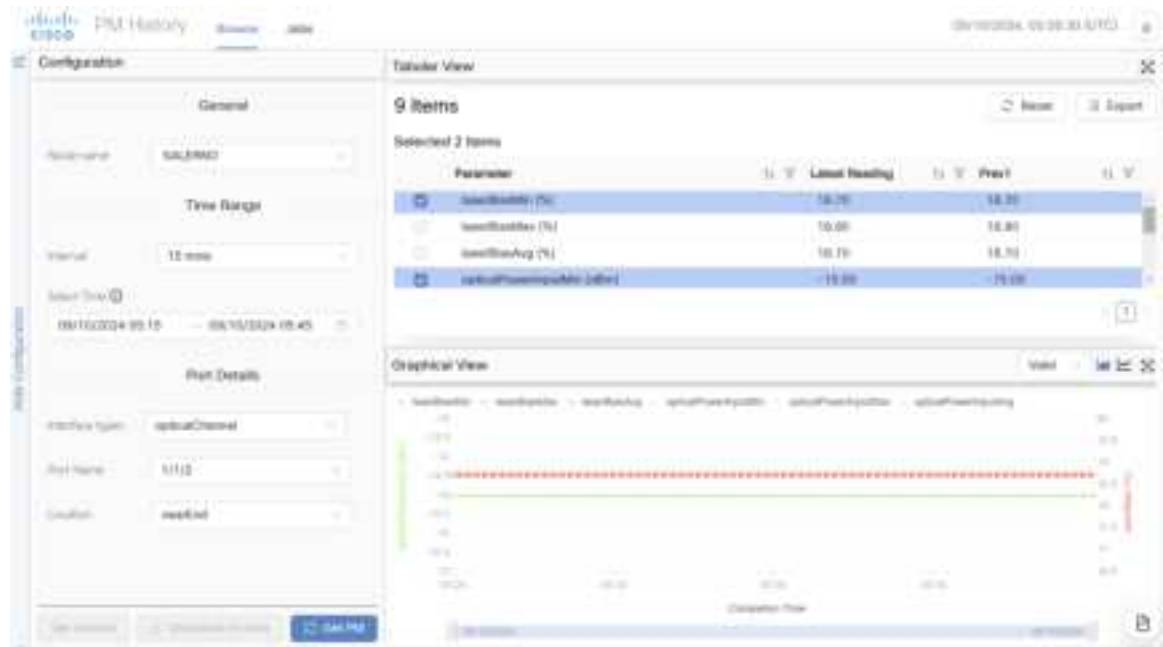
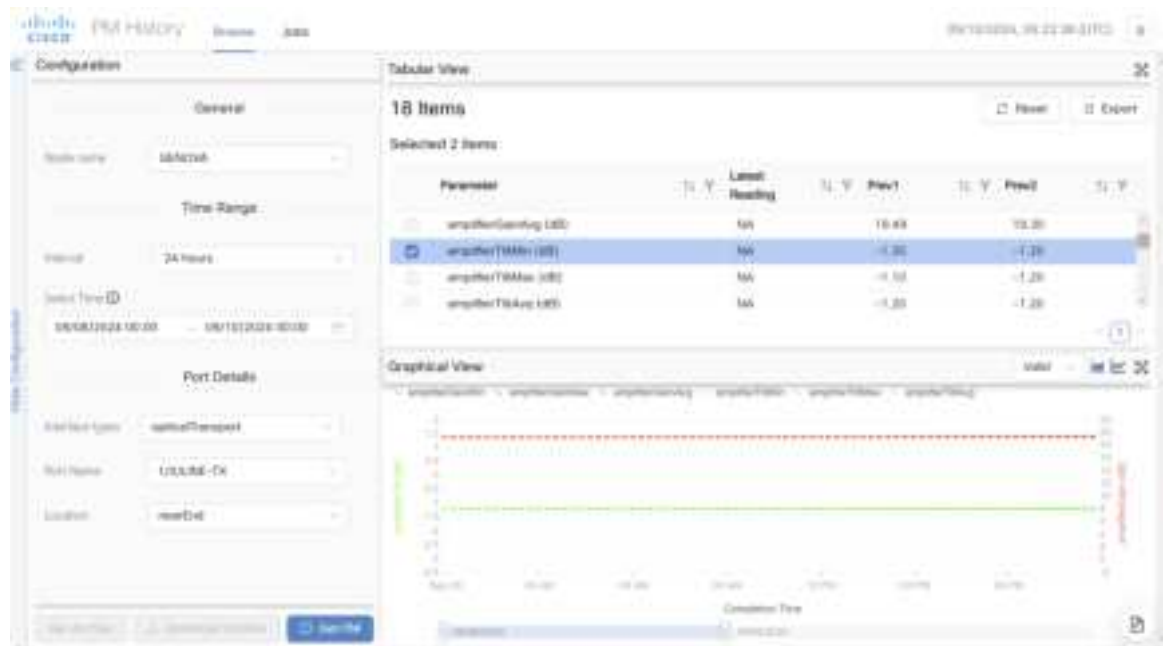


Figure 54: 24-Hour Granularity PM Report



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.

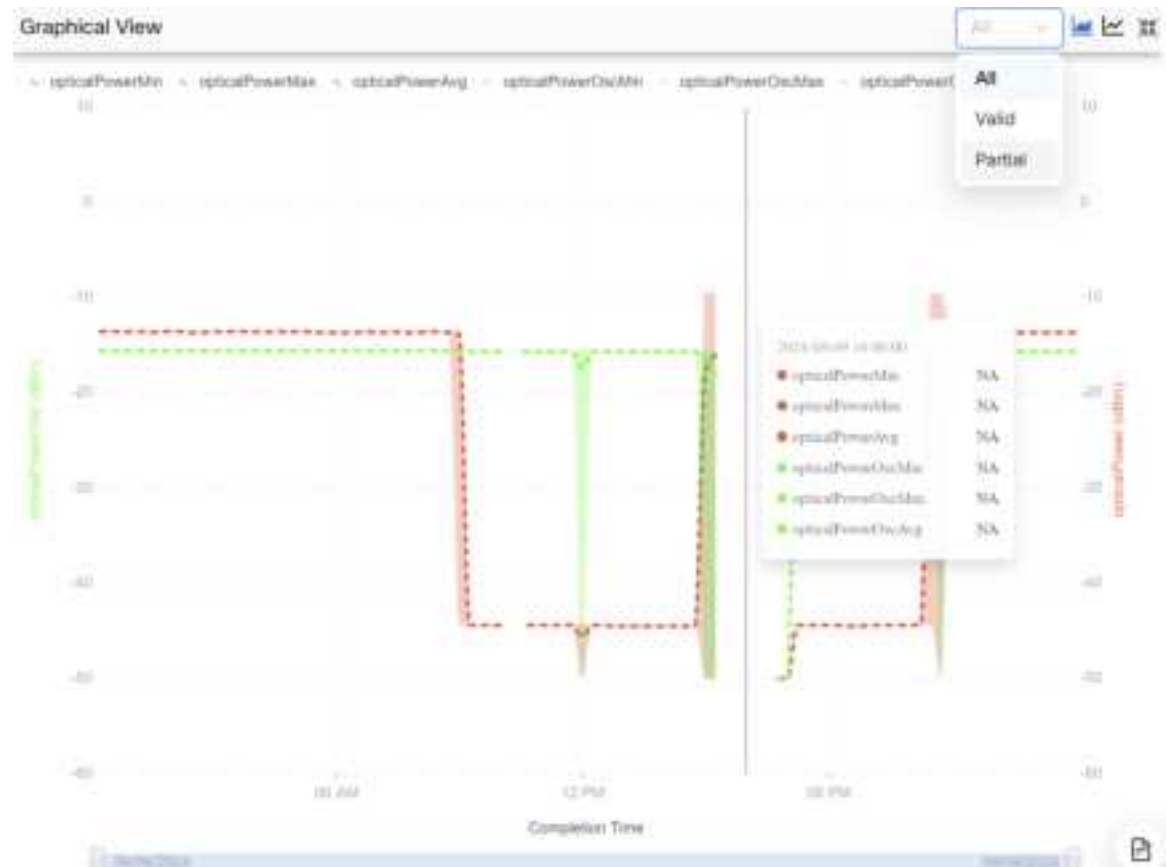
Figure 55: PM History in Network Monitoring





Note Partial is represented in yellow.

Figure 57: NA Values in Linear Graph



Accessing PM History Report

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

Procedure

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

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

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

Note

- Figure 58: PM History Data Collection**



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 60: 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

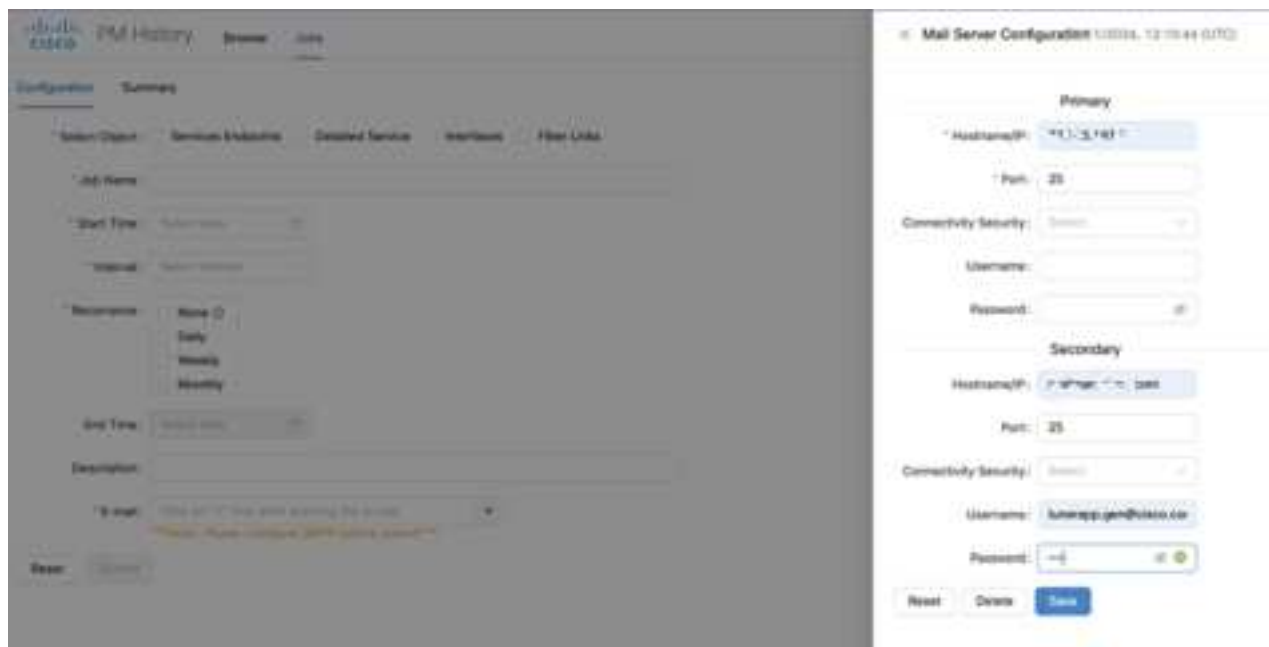
With **Services Endpoint** report, you can choose one or more than one services but with **Detailed Service** report, you can choose only one service.

- 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 61: Jobs

**Note**

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

Logs

Cisco Optical Network Controller supports two sets of logs:

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

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

Audit Logs

The **Audit** logs option helps in:

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

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



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

Display Features

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

Categorization of Audit Logs

Audit logs are categorized into:

Table 26: Audit Logs Category

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

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

**Note**

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

Debug Logs

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



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

Retention and Archiving and Archive Logs

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

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

Archive Logs

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

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



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

**Note**

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

Sedo Commands

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

The sedo commands are as given:

1. Step 1:

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

2. Step 2:

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

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

1. Step 1:

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

For example:

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

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

2. Step 2:

Use the command **sedo object-store get onc-torch-service-dev-log-data-archives/devlogs_2024-09-20T12_40_00** to download from the current directory. *devlogs_2024-09-20T12_40_00* is the file name list taken from the Step 1 output.

3. Step 3:

You can download the file to the local system.

Home	Logs	Alerts	Settings		
View More					
Date	Category	Month	Username	Client IP	Message
09/25/2024 09:10:10Z	alarm	[icon] 2024-11	[icon]	10.241.0.20	User acknowledgment for alarm LIC-COMM-FAL with alarm objectid MODULE_109F0
09/25/2024 09:13:06.992	alarm	[icon]	admin	10.241.0.20	User acknowledgment for alarm LIC-COMM-FAL with alarm objectid MODULE_5B9F0
09/25/2024 09:14:29.991	alarm	[icon]	admin	10.241.0.20	Userfence added for alarm CHANNEL_HOUSE_LOADED with alarm-objectid CMC_cmc_uoddygubumfwvcaupaumaaj-jad-i CPS_VISURE-TX
09/25/2024 09:14:29.979	alarm	[icon]	admin	10.241.0.20	Userfence added for alarm USER_LOGIN with alarm-objectid SYSTEM
09/25/2024 09:16:26.772	alarm	[icon]	admin	10.241.0.20	Userfence added for alarm USER_LOGOUT with alarm-objectid SYSTEM
09/25/2024 09:12:28.980	routd	[icon]	jythem		Request completed.
09/25/2024 09:12:03.974	routd	[icon]	admim	10.7.15.204.242	Response requested.
09/25/2024 09:11:44.747	routd	[icon]	admin	10.7.15.204.242	Requerrest system for value Latitude=46.014991, Longitude=12.081246)
09/24/2024 23:58:52.947	sms_auth	[icon]	system	10.58.203.71	Loginof User
09/24/2024 23:58:51.964	sms_auth	[icon]	system	10.58.203.71	Loginof User
09/24/2024 23:58:51.947	sms_auth	[icon]	system	10.58.203.71	Loginof User
09/24/2024 23:58:51.934	sms_auth	[icon]	system	10.58.203.71	Loginof User
09/24/2024 23:58:50.968	sms_auth	[icon]	system	10.58.203.71	Loginof User

Cisco Logs Audit Archive Debug

09/10/2024, 10:21:41 [UTC]

Audit logs job schedule Active

16 Monday 00:00:00 UTC

Suspend Modify

Debug logs job schedule Active

16 Monday 00:00:00 UTC

Suspend Modify

Techdump

=

Collect

4 Files Last updated on 09/10/2024 at 10:15:39 Refresh

File	Status	Created by	Action
autilsgs_2024-09-27T18_00_00	Completed	System	Download Delete
devlogs_2024-09-29T00_00_00	Completed	System	Download Delete
autilsgs_2024-09-29T00_00_00	Completed	System	Download Delete
devlogs_2024-09-29T00_00_00	Completed	System	Download Delete

Figure 64: Scheduling Audit Logs Job

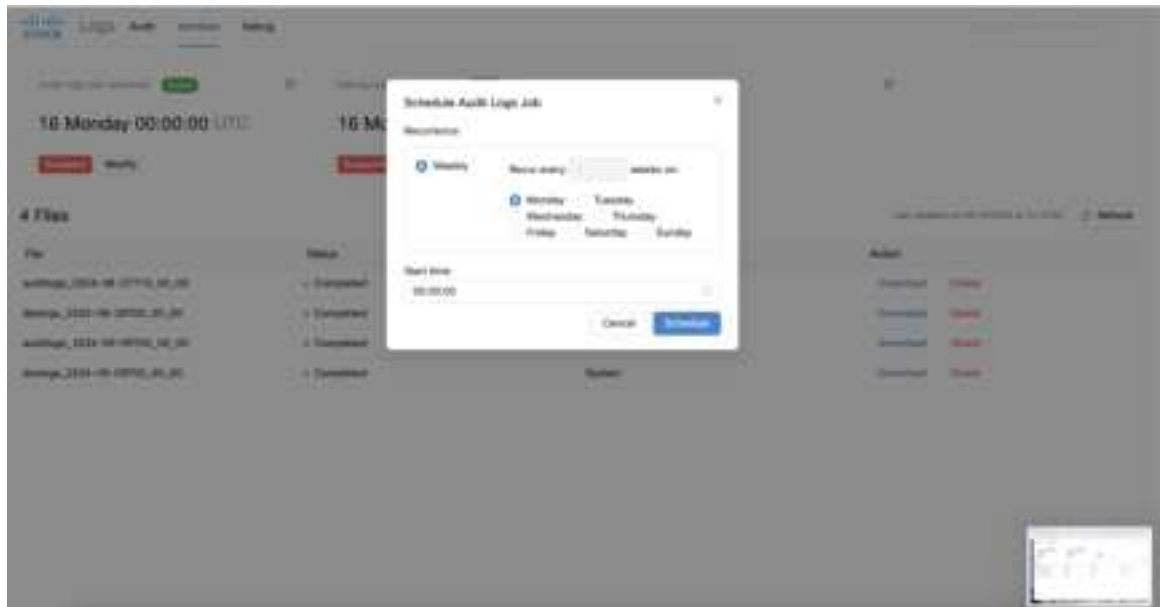
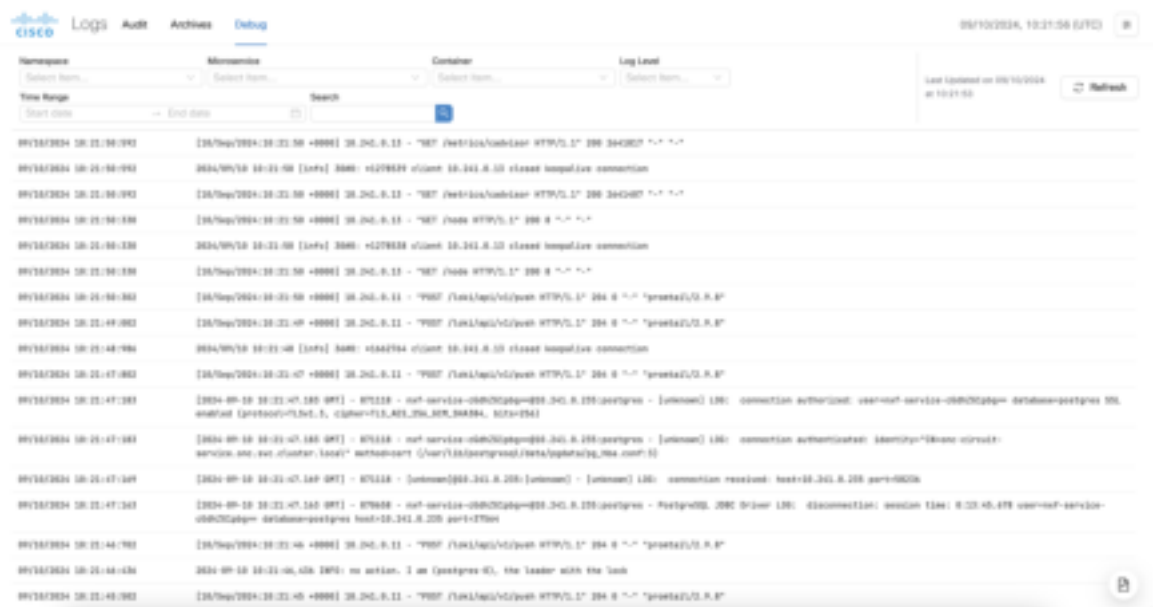


Figure 65: Debug Logs



Benefits of Logs Enhancement

Log enhancements help in:

Table 27: Benefit of Log Enhancements

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

Accessing Logs

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

Procedure

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

The **Logs** screen is displayed.

Step 2 Click **Audit** tab.

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

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

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

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

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

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

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

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

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

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

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

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

Monitoring

- **Detailed Node Resources:** You can monitor the CPU, memory or disk consumption of the host.
- **Pod Monitoring:** You can monitor the CPU, memory or disk consumption of the microservices within the kubernetes cluster.

Before you begin

Use this app to view the log messages and other related details.

Click to view each option separately.

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 66: Links App

[illegible]

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.

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 67: Links App

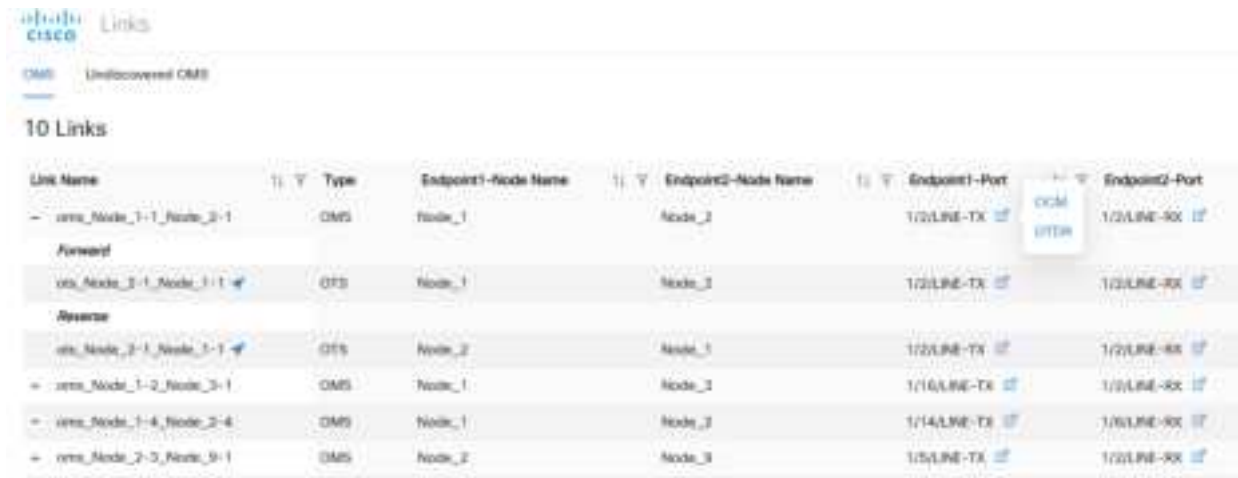


- c) Select an interval and predefined time range or choose a custom range. The PM history table is displayed.
- d) Select up to 4 parameters to view on the graph.

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 68: Links App



Link Name	Type	Endpoint1-Node Name	Endpoint2-Node Name	Endpoint1-Port	Endpoint2-Port
zms_Node_1-1_Node_2-1	OMS	Node_1	Node_2	1/2/LINE-TX	1/2/LINE-RX
<i>Forward</i>					
zms_Node_1-1_Node_2-1	OTS	Node_1	Node_2	1/2/LINE-TX	1/2/LINE-RX
<i>Reverse</i>					
zms_Node_2-1_Node_1-1	OTS	Node_2	Node_1	1/2/LINE-TX	1/2/LINE-RX
zms_Node_1-2_Node_2-1	OMS	Node_1	Node_2	1/16/LINE-TX	1/16/LINE-RX
zms_Node_1-4_Node_2-4	OMS	Node_1	Node_2	1/14/LINE-TX	1/14/LINE-RX
zms_Node_2-3_Node_1-1	OMS	Node_2	Node_1	1/5/LINE-TX	1/5/LINE-RX

- c) Click **OCM** or **OTDR** to cross-launch the OCM or OTDR tab in Cisco Optical Site Manager for the selected endpoint. If OTDR is not supported, it navigates to alarms.

Step 6 Export Links data.

- Click **Export**.
- (Optional) Select **Table View** and click **Export** to export and download the data currently displayed in the table.
- Select **Network Links** to export all network links.
- Click **Generate**.
- After the file is generated, click **Export** to download the XLS file.

Note

After expanding links, wait for up to 60 seconds for the **Total Transmit Power Tx(dBm)** and **Total Receiver Power Rx(dBm)** values to be fetched. If you export or Generate a full report before all the values are fetched, the report contains only the power values for the links for which the values were fetched.

General Troubleshooting

These are some generic troubleshooting points to consider which are common across the different applications within Cisco ONC.

- **TAC case:** In order to raise a TAC case, collect the sedo diagnostic logs with the command:

```
sedo diagnostics archive-logs
```

Collect it along with the Grafana view.

Unmanaged Equipment Support

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

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

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



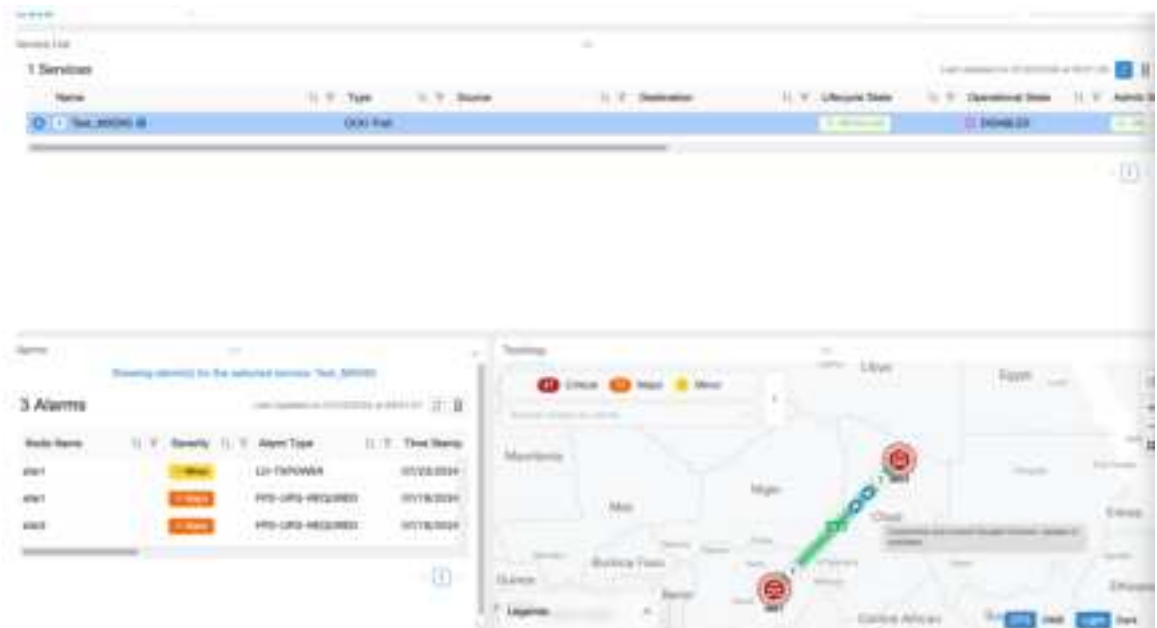
Note

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

Figure 69: Unmanaged Equipment Support in Topology



Figure 70: Unmanaged Equipment Support in Service Assurance



PSM Fiber Protection

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

**Note**

- PSM module is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.
- NCS 1001 is supported only if it is managed by a COSM instance running over a NCS 1014 chassis.

Configuration in PSM Circuits

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

**Note**

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

Benefits of PSM

The benefits of using PSM are:

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

**Note**

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

Additional PSM Functions

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

PSM Circuit in Service Manager

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

Limitations of PSM Fiber Protection

- Cisco Optical Network Controller does not support PSM Protection switching in optical circuits with NCS 1010 ILA modules between NCS 1010 OLT nodes.
- Cisco Optical Network Controller does not support 3-way PSM Protection switching.
- The W-RX and P-RX thresholds for the 1001 PSM must be set carefully based on the number of channels. If the number of channels is lower, a significant power drop from one channel going off may cause the PSM to switch, leading to traffic hits on other channels. See [Configuration Guide for Cisco NCS 1001](#)
- Cisco Optical Network Controller does not display the Reason for switchover.
- Cisco Optical Network Controller supports only configurations with amplifiers positioned after the PSM module. Fiber protection is not supported.
- You must perform a resync if you onboard devices, add or modify IPCs, or add or remove degrees to the 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**.

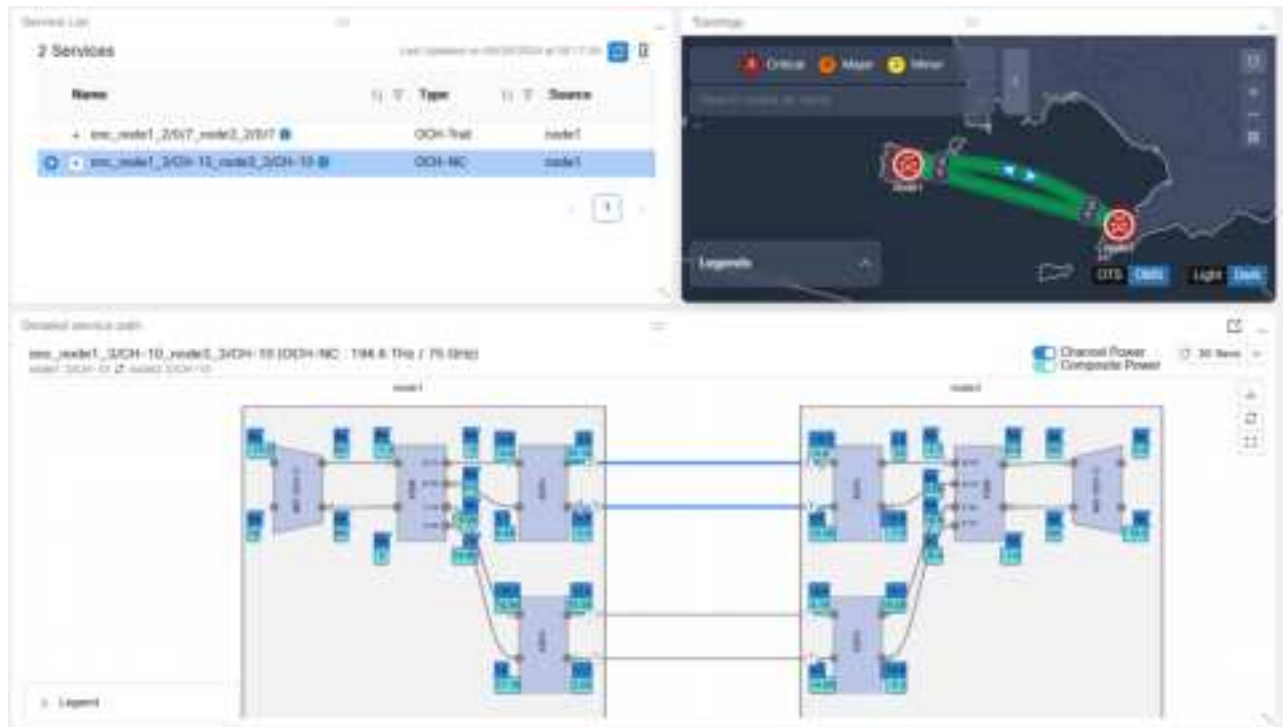
Step 3 Select the PSM circuit.

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 71: PSM Circuit in Workspace



Forwarding Syslogs

The syslog forwarding feature help in:

- Storing logs from the client VMs in the server VM.
- Allowing multiple client VMs to send logs to the same server VM.
- Server installation is done only once.
- The server's database stores all logs.

You need to run the commands from the client VMs to configure the server using the script provided.

Install Syslog on Server

To install syslog feature on the server run the CLI commands given in the example:

Create the rsyslog server using steps provided in below website
<https://www.makeuseof.com/set-up-linux-remote-logging-using-rsyslog/>

To create the folder structure

AUDIT logs here → /var/log/<host-ip>/audit.log

ONC service logs here → /var/log/<host-ip>/service_logs/

Add the below lines in the rsyslog.conf file

```

$ModLoad imudp
$UDPServerRun 514

Input (type="imudp" port="514" ruleset="rs1")

template (name="ServLogLoc" type="string"
string="/var/log/%FROMHOST-IP%/service_logs/%syslogtag%.log")
template (name="AuditLogLoc" type="string" string="/var/log/%FROMHOST-IP%/audit.log")

Ruleset (name="rs1") {
:msg, contains, "audit" ?AuditLogLoc
*.* ?ServLogLoc
}

Restart syslog server using command,
systemctl restart rsyslog

Check if rsyslog service is active and running using command,
systemctl status rsyslog

```

Install Syslog on Client

To install syslog server forwarding in client run the CLI commands in the example:

```

sedo syslog server create <IP> <PROTOCOL> <IP> <PORT>
    IP is the address of the syslog server.
    Protocol to be used - udp or tcp.
    Port on which syslog server is listening to (default is 514)

```

To create a syslog query to forward the application logs of a particular Cisco Optical Network Controller app:

```

sedo syslog query create '{namespace="onc", app="<app_name>", container="app"}' LOG_INFO
LOG_USER <app_name> <IP>

```



Note The query inside single quotes is Grafana Loki's logQL, it can be tweaked according to user needs

To list all syslog queries:

```
sedo syslog query list
```

To list all syslog servers:

```
sedo syslog server list
```

To delete a syslog query:

```
sedo syslog query delete <QUERY_ID>
```

To delete a syslog server:

```
sedo syslog server delete <IP>
```




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 123](#)
- [NODE-BACKUP-FAILURE, on page 124](#)
- [NODE-DISCONNECT, on page 124](#)
- [UPLOAD-FAILURE, on page 125](#)
- [DISK THRESHOLD, on page 125](#)
- [SWITCHOVER, on page 126](#)
- [FAILOVER, on page 126](#)

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 successful 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 `kubectl get pods -n nx-system | 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 successful 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 successful 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** Remove files from the /data folder in the Cisco Optical Network Controller VM.
If you have a geo-redundant deployment, remove files from the /data folder in the active VM.
Delete sedo diagnostics results and archived logs.
- Step 2** 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

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.

Condition Name	Description	Condition Type	Alarm Category
ACT-SOFT-VERIF-FAIL	Active Volume Software Signature Verification Failed	Alarm	EQUIPMENT
ADD-OPWR-HDEG	Port Add Power Degrade High	Alarm	OPTICAL
ADD-OPWR-HFAIL	Port Add Power Fail High	Alarm	OPTICAL
ADD-OPWR-LDEG	Port Add Power Degrade Low	Alarm	OPTICAL
ADD-OPWR-LFAIL	Port Add Power Fail Low	Alarm	OPTICAL
ADMIN-CONFIG-INCONSISTENCY	Admin Configuration is in inconsistent state	Alarm	SECURITY

Condition Name	Description	Condition Type	Alarm Category
ADMIN-DISABLE	Disable Inactive User	Event	SECURITY
ADMIN-DISABLE-CLR	Disable Inactive Clear	Event	SECURITY
ADMIN-LOCKOUT	Admin Lockout of User	Event	SECURITY
ADMIN-LOCKOUT-CLR	Admin Lockout Clear	Event	SECURITY
ADMIN-LOGOUT	Admin Logout of User	Event	SECURITY
ADMIN-SUSPEND	Suspend User	Event	SECURITY
ADMIN-SUSPEND-CLR	Suspend User Clear	Event	SECURITY
AIS	Alarm Indication Signal	Alarm	TRANSPORT
AIS-L	Alarm Indication Signal Line	Alarm	TRANSPORT
ALC-IN-PROGRESS	Automatic-link-calibration procedure is running	Alarm	OPTICAL
ALC-PROC-FAILED	Automatic-link-calibration procedure failed	Alarm	OPTICAL
ALS	Automatic Laser Shutdown	Alarm	OPTICAL
ALS-DISABLED	Auto Laser Shutdown Disabled	Alarm	OPTICAL
AMPLI-INIT	Optical Amplifier Initialization	Alarm	OPTICAL
AMPLI-OSRI	Amplifier Optical Safety Remote Interlock	Alarm	OPTICAL
APC-BLOCKED	APC blocked	Alarm	OPTICAL
APC-BLOCKED-RX	APC blocked in RX direction	Alarm	OPTICAL
APC-BLOCKED-TX	APC blocked in TX direction	Alarm	OPTICAL
APC-CORR-SKIPPED	Automatic Power Control Correction Skipped	Alarm	OPTICAL
APC-DISABLED	Automatic Power Control Disabled	Alarm	OPTICAL
APC-DISABLED	Automatic Power Control Disabled	Alarm	OPTICAL
APC-END	Manual Requested Automatic Power Control run Completed	Alarm	OPTICAL
APC-HW-FAIL	APC Hardware Failure	Alarm	OPTICAL
APC-OUT-OF-RANGE	APC Cannot Set Value Due To Range Limits	Alarm	OPTICAL
APC-TARGET-PSD-NOT-MET-RX	APC Target PSD not met in RX direction	Alarm	OPTICAL
APC-TARGET-PSD-NOT-MET-TX	APC Target PSD not met in TX direction	Alarm	OPTICAL
APC-WRONG-GAIN	APC Wrong Gain Set Point	Alarm	OPTICAL

Condition Name	Description	Condition Type	Alarm Category
APS-NO-RESPONSE	APS Signal Mismatch	Alarm	PROTECTION
APS-PROV-MISM	APS Protection Type Mismatch	Alarm	TRANSPORT
AS-CMD	Alarms Suppressed By User Command	Alarm	MAINTENANCE
AS-MT	Alarms Suppressed For Maintenance	Alarm	MAINTENANCE
ASE-LOADING-DISABLED	ASE Loading is disabled	Alarm	OPTICAL
AUD-ARCHIVE-FAIL	Archival of Audit Log Failed	Event	SYSTEM
AUD-LOG-LOSS	Audit Log 100 Percent Full - Oldest records will be lost	Alarm	SYSTEM
AUD-LOG-LOW	Audit Log 80 Percent Full	Alarm	SYSTEM
AUTH-EC	Payload Authentication Error Count	Alarm	TRANSPORT
AUTO-AMPLI-DISABLED	Auto Ampli Control Disabled	Alarm	OPTICAL
AUTO-AMPLI-MISMATCH	Auto Ampli Control Mismatch	Alarm	OPTICAL
AUTO-AMPLI-RUNNING	Auto Ampli Control Running	Alarm	OPTICAL
AUTORESET	Automatic System Reset	Alarm	EQUIPMENT
AUTOWDMANS	Automatic WDM ANS Finished	Event	OPTICAL
AVST-FAILURE	AVST Failure	Alarm	EQUIPMENT
AWG-DEG	AWG Temperature Degrade	Alarm	EQUIPMENT
AWG-FAIL	AWG Temperature Failure	Alarm	EQUIPMENT
AWG-OVERTEMP	AWG Over-Temperature	Alarm	EQUIPMENT
AWG-WARM-UP	AWG Warm Up	Alarm	EQUIPMENT
B-AUTH-EC	Backward Auth Error Count	Alarm	TRANSPORT
BAD-DB-DETECTED	Bad Database Detected And Database Load Failed	Alarm	SYSTEM
BAND-PARTNER-NODE-UNPAIRED	Node is unpaired from band partner node	Alarm	SYSTEM
BAT-FAIL	Battery Failure	Alarm	EQUIPMENT
BDI	Backward Defect Indication	Alarm	TRANSPORT
BERT-ENBL	BERT Enabled	Alarm	TRANSPORT
BERT-SYNC-FAIL	BERT Synchronization Status Failed	Alarm	TIMING

Condition Name	Description	Condition Type	Alarm Category
BIOS-IMAGE-CORRUPTION	BIOS image corruption	Alarm	EQUIPMENT
BKUPMEMP	Primary Non-Volatile Backup Memory Failure	Alarm	EQUIPMENT
BP-FPGA-IMAGE-CORRUPTION	BP FPGA Image Corruption	Alarm	EQUIPMENT
BP-FPGA-PCIE-ERROR	BP FPGA PCIE Error	Alarm	EQUIPMENT
BP-FPGA-XR-EP-FPGA-PCIE-ERROR	BP FPGA XR EP FPGA PCIE Error	Alarm	EQUIPMENT
BP-LPBKFACILITY	Back-panel Facility Loopback	Alarm	MAINTENANCE
BP-LPBKTERMINAL	Back-panel Terminal Loopback	Alarm	MAINTENANCE
CANNOT-BE-EQUALIZED	Incoming signal cannot be equalized	Alarm	OPTICAL
CARD-IS-SHUTDOWN	Card failed to come up after multiple recovery attempts	Alarm	EQUIPMENT
CARD-UNREACHABLE	RemoteCard Not Reachable For Key Exchange. Retrying ...	Alarm	EQUIPMENT
CARLOSS	Carrier Loss On The LAN	Alarm	OPTICAL
CASETEMP-DEG	Case Temperature Degrade	Alarm	EQUIPMENT
CD	Chromatic Dispersion	Alarm	OPTICAL
CHAN-PWR-THRESHOLD-CHECK	Channel Power would fall below threshold value	Alarm	OPTICAL
CHANNEL-NOISE-LOADED	Channel is Loaded with Noise	Alarm	OPTICAL
CHANNEL-READY	Channel Presence is Detected and Ready	Alarm	OPTICAL
CLDRESTART	Cold Restart	Alarm	EQUIPMENT
COMM-FAIL	Plug-in Module Communication Failure	Alarm	EQUIPMENT
COMMIT-REPLACE-FAILED	Configuration commit replace failed	Alarm	SYSTEM
COMP-CARD-MISSING	Companion Card Missing	Alarm	EQUIPMENT
CONFIG-INCONSISTENCY	Configuration is in inconsistent state	Alarm	SYSTEM
CONTBUS-A-18	Controller Card A To DCC A Processor Communication Failure	Alarm	EQUIPMENT
CONTBUS-B-18	Controller Card B To DCC B Processor Communication Failure	Alarm	EQUIPMENT
CONTBUS-CLK-A	Clock Bus Failure - Shelf Controller A	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
CONTBUS-CLK-B	Clock Bus Failure - Shelf Controller B	Alarm	EQUIPMENT
CONTBUS-DISABLED	Slot Communication Disabled	Alarm	EQUIPMENT
CONTBUS-IO-A	Peer To Peer Slot Communication Failure	Alarm	EQUIPMENT
CONTBUS-IO-B	Peer To Peer Slot Communication Failure	Alarm	EQUIPMENT
COOL-MISM	Cooling Profile Mismatch	Alarm	EQUIPMENT
CP-UNVER-CLEARED	Control Plane Unverified Cleared Alarms Present	Alarm	SYSTEM
CPP-INCAPABLE	Card/Ports Unable To Provide Protection	Alarm	EQUIPMENT
CPU-FPGA-PCIE-ERROR	CPU FPGA PCIe Error	Alarm	EQUIPMENT
CRYPTO-HW-FAILURE	Cryptographic self-test failure	Alarm	SECURITY
CRYPTO-INDEX-MISMATCH	Crypto Index Mismatch	Alarm	SECURITY
CRYPTO-KEY-EXPIRED	Crypto key expired	Alarm	SECURITY
DATAFLT	Software Fault - Data Integrity Fault	Alarm	SYSTEM
DBBACKUP-FAIL	Database Backup Failed	Event	SYSTEM
DBBACKUP-IN-PROGRESS	Database Backup In Progress	Alarm	SYSTEM
DBOSYNC	Standby Database Out of Sync	Alarm	SYSTEM
DBREST-IN-PROGRESS	Database Restore In Progress	Alarm	SYSTEM
DBRESTORE-FAIL	Database Restore Failed	Event	SYSTEM
DCU-LOSS-FAIL	DCU Loss Failure	Alarm	OPTICAL
DEG-SER	FEC Degraded Symbol Error Rate	Event	TRANSPORT
DEGREE-MISMATCH	Degree Mismatch	Alarm	SYSTEM
DGD	Differential Group Delay	Alarm	OPTICAL
DISK-SPACE-FULL	No Space Left On Device	Alarm	SYSTEM
DISK-SPACE-LOW	Low Disk Space Remaining On Device	Alarm	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	Alarm	SYSTEM
DSP-COMM-FAIL	DSP Communication Failure	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
DSP-FAIL	DSP Failure	Alarm	EQUIPMENT
DUP-IPADDR	IP Address Already In Use Within The Same DCC Area	Alarm	SYSTEM
DUP-NODENAME	Node name already in use within the same DCC Area	Alarm	SYSTEM
DUP-SHELF-ID	Duplicated Shelf Identifier	Alarm	SYSTEM
EHIBATVG	Extreme High Volt	Alarm	EQUIPMENT
ELWBATVG	Extreme Low Volt	Alarm	EQUIPMENT
EMB-AMPLIFIER-SATURATED	Embedded amplifier saturated alarm	Alarm	OPTICAL
ENC-CERT-EXP	MIC cert is expired switch to LSC	Alarm	TRANSPORT
EOC	SDCC Termination Failure	Alarm	TRANSPORT
EOC-E	Ethernet OSC Termination Failure	Alarm	TRANSPORT
EOC-L	Line DCC Termination Failure	Alarm	TRANSPORT
EPROM-SUDI-SN-MISMATCH	Card Serial Number and Certificate Serial Number Mismatch	Alarm	EQUIPMENT
EQPT	Equipment Failure	Alarm	EQUIPMENT
EQPT-DEGRADE	Equipment Degrade	Alarm	EQUIPMENT
EQPT-DIAG	Diagnostic Failure	Alarm	EQUIPMENT
EQPT-FAIL	Board Failure	Alarm	EQUIPMENT
EQPT-FPGA-IMAGE-AVAILABLE	Different FPGA Image Available	Alarm	EQUIPMENT
EQPT-MISS	Replaceable Equipment/Unit is Missing	Alarm	EQUIPMENT
ETH-LINKLOSS	Rear Panel Ethernet Link Removed	Alarm	EQUIPMENT
EVAL-LIC	Evaluation License Is In Use	Alarm	SYSTEM
EXPECTED-POWER-FAIL	Channel Power Reading Exceeds the Expected Power Tolerance Limits	Alarm	OPTICAL
EXT	Failure Detected External To The NE	Alarm	SYSTEM
FAILTOSW	Failure To Switch To Protection	Alarm	PROTECTION
FAN	Fan Failure	Alarm	EQUIPMENT
FAN-OUT-OF-TOLERANCE	Fan Out of tolerance	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
FAN-POWER-ERROR	FAN tray Power Error	Alarm	EQUIPMENT
FAN-SENSOR-FAILED	Sensor in failed state	Alarm	EQUIPMENT
FANDEGRADE	Partial Fan Failure	Alarm	EQUIPMENT
FC-DE-NES	Fibre Channel Distance Extension Function Not Established	Alarm	TRANSPORT
FC-NO-CREDITS	Fibre Channel Distance Extension Credit Starvation	Alarm	TRANSPORT
FDI	Forward Defect Indication	Alarm	OPTICAL
FEC-MISM	FEC Mismatched	Alarm	TRANSPORT
FEED-MISMATCH	Feed Not Available/Improper Connection	Alarm	EQUIPMENT
FIBERTEMP-DEG	Fiber Temperature Degrade	Alarm	EQUIPMENT
FIRMWARE-DOWNLOAD	Firmware Download In Progress	Event	EQUIPMENT
FIRMWARE-UPG	Firmware Upgrade In Progress	Alarm	EQUIPMENT
FIRMWARE-UPG-COMPLETE	Firmware Upgrade Completed	Event	EQUIPMENT
FIRMWARE-UPG-FAIL	Firmware Upgrade Failed	Alarm	EQUIPMENT
FLASH0-ERROR	CPU Flash 0 Error	Alarm	EQUIPMENT
FLASH1-ERROR	CPU Flash 1 Error	Alarm	EQUIPMENT
FLEXO-GIDM	FlexO Group Identification Mismatch	Alarm	TRANSPORT
FLEXO-LOF	FlexO Loss of Frame	Alarm	TRANSPORT
FLEXO-LOM	FlexO Loss of MultiFrame	Alarm	TRANSPORT
FLEXO-MM	FlexO Map Mismatch	Alarm	TRANSPORT
FLEXO-RDI	FlexO Remote Defect Indicator	Alarm	TRANSPORT
FOIC-GIDM	FOIC Group ID mismatch defect	Alarm	TRANSPORT
FOIC-LDI-LD	FOIC Link Degrade indicator - Local Degrade	Alarm	TRANSPORT
FOIC-LDI-RD	FOIC Link Degrade indicator- Remote Degrade	Alarm	TRANSPORT
FOIC-LOF-LOM	FOIC Loss of Frame loss of Multiframe	Alarm	TRANSPORT
FOIC-LOL	FOIC Loss of Lock Detect	Alarm	TRANSPORT
FOIC-LOM	FOIC Loss of Multiframe Indication	Alarm	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
FOIC-PMM	FOIC Phy Map mismatch Alarm	Alarm	TRANSPORT
FOIC-RPF	FOIC Remote Phy Fault Detect	Alarm	TRANSPORT
FOIC-TIM	FOIC Trail Trace Identifier Mismatch	Alarm	TRANSPORT
FORCED-REQ	Forced Switch Request	Alarm	PROTECTION
FPD-UPG-REQUIRED	Firmware upgrade required	Alarm	EQUIPMENT
FPGA-ERROR	BP FPGA Error	Alarm	EQUIPMENT
FPGA-SEU-UNCORR	BP FPGA SEU Uncorrected Error	Alarm	EQUIPMENT
FPGA-UPGRADE-FAILED	FPGA Upgrade fail	Alarm	EQUIPMENT
FRCDSWTOINT	Forced Switch To Internal Clock	Alarm	TIMING
FRCDSWTOPRI	Forced Switch To Primary Reference	Alarm	TIMING
FRCDSWTOSEC	Forced Switch To Second Reference	Alarm	TIMING
FRCDSWTOTHIRD	Forced Switch To Third Reference	Alarm	TIMING
FRNGSYNC	Free Running Synchronization Mode	Alarm	TIMING
FTA-MISMATCH	FanTray Mismatch	Alarm	EQUIPMENT
GAIN-HDEG	Optical Amplifier Gain Degrade High	Alarm	OPTICAL
GAIN-HFAIL	Optical Amplifier Gain Failure High	Alarm	OPTICAL
GAIN-LDEG	Optical Amplifier Gain Degrade Low	Alarm	OPTICAL
GAIN-LFAIL	Optical Amplifier Gain Failure Low	Alarm	OPTICAL
GAIN-NEAR-LIMIT	Amplifier Gain is near its limit	Alarm	OPTICAL
GCC-EOC	GCC Termination Failure	Alarm	TRANSPORT
GE-OOSYNC	GigaBit Ethernet Out of Sync	Alarm	TRANSPORT
GFP-CSF	GFP Client Signal Fail Detected	Alarm	TRANSPORT
GFP-CSF-SIGLOSS	GFP Client Signal Fail Detected Due To Sigloss	Alarm	TRANSPORT
GFP-CSF-SYNCLOSS	GFP Client Signal Fail Detected Due To Syncloss	Alarm	TRANSPORT
GFP-DE-MISMATCH	GFP Fibre Channel Distance Extension Mismatch	Alarm	TRANSPORT
GFP-EX-MISMATCH	GFP Extension Header Mismatch	Alarm	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
GFP-LFD	GFP Loss of Frame Delineation	Alarm	TRANSPORT
GFP-NO-BUFFERS	GFP Fibre Channel Distance Extension Buffer Starvation	Alarm	TRANSPORT
GFP-UP-MISMATCH	GFP User Payload Mismatch	Alarm	TRANSPORT
HELLO	OSPF Hello Fail	Alarm	SYSTEM
HI-BER	High Bit Error Rate	Alarm	TRANSPORT
HI-CCVOLT	Composite Clock High Line Voltage	Alarm	TIMING
HI-LASERBIAS	Equipment High Laser Bias	Alarm	EQUIPMENT
HI-LASERTEMP	Equipment High Laser Temp	Alarm	EQUIPMENT
HI-RX-BR-PWR	Input High BR Power	Alarm	OPTICAL
HI-RXPOWER	Facility High Rx power	Alarm	OPTICAL
HI-SER	High Symbol Error Rate	Event	TRANSPORT
HI-TX-BR-PWR	Otput High BR Power	Alarm	OPTICAL
HI-TXPOWER	Equipment High Tx power	Alarm	EQUIPMENT
HIBATVG	High Volt	Alarm	EQUIPMENT
HIGH-VOLTAGE	high voltage alarm	Alarm	EQUIPMENT
HITEMP	High Temperature	Alarm	EQUIPMENT
HITEMP	High Temperature	Alarm	EQUIPMENT
HLDOVRSYNC	Holdover Synchronization Mode	Alarm	TIMING
I-HITEMP	Industrial High Temperature	Alarm	EQUIPMENT
IDLE	Idle Signal Condition	Alarm	TRANSPORT
IMPROPRMVL	Improper Removal	Alarm	EQUIPMENT
IMPROPRMVL-FS	Improper removal of Fiber Shuffle	Alarm	EQUIPMENT
INSTALL-IN-PROGRESS	SW Installation In Progress	Alarm	SYSTEM
INTRUSION	Security: Invalid Login Username - See Audit Trail	Event	SECURITY
INTRUSION-PSWD	Security Intrusion Attempt Detected - See Audit Log	Alarm	SECURITY

Condition Name	Description	Condition Type	Alarm Category
INTRUSION-USERID	Security Intrusion Attempt Detected - See Audit Log	Event	SECURITY
INVALID-CARD-SLOT	Invalid Card Slot	Alarm	EQUIPMENT
INVALID-SENSOR-READ-ERR	Invalid sensor read error	Alarm	EQUIPMENT
INVALID-SYSDB	Invalid System DB	Alarm	SYSTEM
INVMACADR	Invalid MAC Address	Alarm	SYSTEM
IPC-LASER-FAIL	Ipc Laser failure	Alarm	MAINTENANCE
IPC-LOOPBACK-MISS	Patchcords Verification Loopback Missing	Alarm	MAINTENANCE
IPC-VERIFICATION-DEGRADE	Patchcords Verification Degrade	Alarm	MAINTENANCE
IPC-VERIFICATION-EXCESSIVE-LOSS	Measured Patchcord Loss above the Threshold	Alarm	MAINTENANCE
IPC-VERIFICATION-FAIL	Patchcords Verification Failure	Alarm	MAINTENANCE
IPC-VERIFICATION-RUNNING	Patchcords Verification Running	Alarm	MAINTENANCE
KEY-EX-FAIL	Primary Key Exchange Failed	Alarm	TRANSPORT
KEY-WRITE-FAIL	Key Program On FPGA Failed	Alarm	TRANSPORT
LAN-POL-REV	Lan Connection Polarity Reversed	Alarm	EQUIPMENT
LASER-APR	Laser Auto Power Reduction	Alarm	OPTICAL
LASERBIAS-DEG	Laser Bias Degrade	Alarm	EQUIPMENT
LASERBIAS-FAIL	Laser Bias Failure	Alarm	EQUIPMENT
LASEREOL	Laser Approaching End of Life	Alarm	EQUIPMENT
LASERTEMP-DEG	Laser Temperature Degrade	Alarm	EQUIPMENT
LC-BOOT-TIMEOUT	LC Boot Timeout	Alarm	EQUIPMENT
LC-CPU-IMAGE-CORRUPTION	LC CPU Image Corruption	Alarm	EQUIPMENT
LC-DP-IMAGE-CORRUPTION	LC Data Plane Image Corruption	Alarm	EQUIPMENT
LC-FPD-DEV-FAILURE	CPU_MOD_FW is corrupt, system booted with golden copy	Alarm	EQUIPMENT
LC-OFFLINE-ERROR	LC Offline Error	Alarm	EQUIPMENT
LCMODE-CONFIG-CHANGED	LCMODE changed, delete the datapath config and reload line card	Alarm	SYSTEM
LCMODE-CONFIG-INVALID	LC Mode Configuration Invalid	Alarm	SYSTEM

Condition Name	Description	Condition Type	Alarm Category
LCMODE-NOT-CONFIG	LC Mode Configuration Not Applied	Alarm	SYSTEM
LIC-COMM-FAIL	Communications Failure With Cisco Licensing Cloud	Alarm	SYSTEM
LIC-EXPIRED	License Expired	Alarm	SYSTEM
LIC-EXPIRING-SHORTLY	License Will Expire Within 24 Hours	Alarm	SYSTEM
LIC-EXPIRING-SOON	License Will Expire At Any Time After 1 Day But Before 14 Days	Alarm	SYSTEM
LIC-MISSING	License Is Missing	Alarm	SYSTEM
LIC-OUT-OF-COMPL	One Or More Entitlements Are Out Of Compliance	Alarm	SYSTEM
LICSIA-OF-COMPL-UPGRADE-BLOCKED	SW Upgrade will be blocked as SIA Grace Period has expired	Alarm	SYSTEM
LIC-SIA-OUT-OF-COMPL-GP-REM	SW Upgrade is still allowed as SIA Grace Period is remaining	Alarm	SYSTEM
LICUPGRADE-OF-COMPL-UPGRADE-BLOCKED	SW Upgrade will be blocked as Upgrade License Grace Period has expired	Alarm	SYSTEM
LICUPGRADE-OUT-OF-COMPL-GP-REM	SW Upgrade is still allowed as Upgrade License Grace Period is remaining	Alarm	SYSTEM
LINK-BROKEN	Ha link Broken	Alarm	SYSTEM
LO-LASERBIAS	Equipment Low Laser Bias	Alarm	EQUIPMENT
LO-LASERTEMP	Equipment Low Laser Temp	Alarm	EQUIPMENT
LO-RXPOWER	Facility Low Rx power	Alarm	OPTICAL
LO-TXPOWER	Equipment Low Tx power	Alarm	EQUIPMENT
LOA	Loss of Alignment	Alarm	TRANSPORT
LOCAL-CERT-CHAIN-VERIFICATION-FAILED	Local cert chain verification failed	Alarm	SECURITY
LOCAL-CERT-EXPIRED	Local certificate expired	Alarm	SECURITY
LOCAL-CERT-EXPIRING-WITHIN-30-DAYS	Local cert expiring within 30 days	Alarm	SECURITY
LOCAL-CERT-ISSUED-FOR-FUTURE-DATE	Local cert issued for future date	Alarm	SECURITY
LOCAL-DEG-SER	Local FEC Degraded Symbol Error Rate	Event	TRANSPORT
LOCAL-FAULT	Local Fault	Alarm	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
LOCALSUDICERT-VERIFICATION-FAILED	Local sudi cert verification failed	Alarm	SECURITY
LOCKOUT-REQ	Lockout Switch Request	Alarm	PROTECTION
LOF	Loss Of Frame	Alarm	TRANSPORT
LOF	Loss Of Frame	Alarm	TRANSPORT
LOGIN-FAIL-LOCKOUT	Security: Invalid Login - Locked Out - See Audit Log	Event	SECURITY
LOGIN-FAIL-ONALRDY	Security: Invalid Login - Already Logged On - See Audit Log	Event	SECURITY
LOGIN-FAILURE-PSWD	Security: Invalid Login - Password - See Audit Log	Event	SECURITY
LOGIN-FAILURE-USER	Security: Invalid Login - Username - See Audit Log	Event	SECURITY
LOGIN-MISSING-GROUP	Missing Authorization Group Information	Event	SYSTEM
LOGOUT-IDLE-USER	Automatic Logout of IdleUser	Event	SECURITY
LOM	Loss of Multi-Frame	Alarm	TRANSPORT
LOS	Loss Of Signal	Alarm	OPTICAL
LOS	Loss Of Signal	Alarm	OPTICAL
LOS-D	Loss Of DFB Signal	Alarm	OPTICAL
LOS-O	Incoming Overhead Signal Absent	Alarm	OPTICAL
LOS-P	Incoming Payload Signal Absent	Alarm	OPTICAL
LOS-RAMAN	Loss Of Raman Signal	Alarm	OPTICAL
LOW-VOLTAGE	low voltage alarm	Alarm	EQUIPMENT
LPBKFACILITY	Facility Loopback	Alarm	MAINTENANCE
LPBKTERMINAL	Terminal Loopback	Alarm	MAINTENANCE
LSC-NOT-PRESENT-MIC-IN-USE	LSC not present using MIC	Alarm	EQUIPMENT
LWBATVG	Low Volt	Alarm	EQUIPMENT
MAN-LASER-RESTART	Manual Laser Restart	Alarm	OPTICAL
MAN-REQ	Manual Switch Request	Alarm	PROTECTION
MANRESET	Manual System Reset	Alarm	MAINTENANCE

Condition Name	Description	Condition Type	Alarm Category
MANSWTOINT	Manual Switch To Internal Clock	Alarm	TIMING
MANSWTOPRI	Manual Switch To Primary Reference	Alarm	TIMING
MANSWTOSEC	Manual Switch To Second Reference	Alarm	TIMING
MANSWTOTHIRD	Manual Switch To Third Reference	Alarm	TIMING
MASTERKEY-SUCCESS	MasterKey Exchange Success	Event	SECURITY
MAX-AUTH-LIST	Reached Max Authentication List	Alarm	TRANSPORT
MB-SSD-ATA-ERRORS	Motherboard SSD ATA Errors	Alarm	EQUIPMENT
MEA	Mismatch Of Equipment And Attributes	Alarm	EQUIPMENT
MEA	Mismatch Of Equipment And Attributes	Alarm	EQUIPMENT
MEM-GONE	Free Memory On Card Near Zero	Alarm	EQUIPMENT
MEM-LOW	Free Memory On Card Very Low	Alarm	EQUIPMENT
MFGMEM	Manufacturing Data Memory (EEPROM) Failure	Alarm	EQUIPMENT
MS-AIS	AIS - Multiplex Section - Alarm Indication Signal	Alarm	TRANSPORT
MS-DEG	Multiplex Section - Signal Degraded	Alarm	TRANSPORT
MS-EOC	Multiplex Section DCC Termination Failure	Alarm	TRANSPORT
MS-EXC	Multiplex Section - Excessive Errors	Alarm	TRANSPORT
MS-RDI	RDI - Multiplex Section - Remote Defect/Alarm Indication	Alarm	TRANSPORT
NE-CONFIG-INCONSISTENT	Device has the Config Blocked due to an Inconsistency	Event	SYSTEM
NE-DISCONNECTED	Connection To Managed NE Lost	Alarm	SYSTEM
NE-EVENT-DISCONNECTED	Event Channel To Managed NE Lost	Alarm	SYSTEM
NE-NOT-AUTH-ACCESS	Not Authorised Access To Managed NE	Alarm	SYSTEM
NE-VER-NOT-SUPP	Not Supported Version Of Managed NE	Alarm	SYSTEM
NEIGHBOUR-MISSING	Neighbour not found	Alarm	SYSTEM
NO-SHARED-CIPHERS	Different Ciphers Used by Client and Server	Alarm	TRANSPORT
NO-VALID-USB-DB	No Valid USB DB exists	Alarm	SYSTEM

Condition Name	Description	Condition Type	Alarm Category
NODE-FACTORY-MODE	Node in Factory Mode	Alarm	SYSTEM
NODE-INCONSISTENCIES	Owner and/or partner packages on at least one node do not match the active RP	Alarm	SYSTEM
NODE-OBFL-ERROR	Node OBFL Error	Alarm	EQUIPMENT
NON-CISCO-PPM	Non Cisco PPM Inserted	Alarm	EQUIPMENT
NON-TRAFFIC-AFFECTING-SECURITY-UPGRADE-REQUIRED	Non Traffic Affecting Security Upgrade Required	Alarm	SECURITY
NOS	Not-Operational primitive Sequence	Alarm	TRANSPORT
OCHNC-INC	Optical Channel Incomplete	Alarm	TRANSPORT
OCHNC-MT	OCHNC Maintenance	Alarm	MAINTENANCE
OCHTERM-INC	Optical Termination Incomplete	Alarm	TRANSPORT
ODUK-1-AIS-PM	ODUk1 Alarm Indication Signal	Alarm	TRANSPORT
ODUK-2-AIS-PM	ODUk2 Alarm Indication Signal	Alarm	TRANSPORT
ODUK-3-AIS-PM	ODUk3 Alarm Indication Signal	Alarm	TRANSPORT
ODUK-4-AIS-PM	ODUk4 Alarm Indication Signal	Alarm	TRANSPORT
ODUK-AIS-PM	ODUk: PM Alarm Indication Signal	Alarm	TRANSPORT
ODUK-AIS-TCM1	TCM1 Alarm Indication Signal	Event	TRANSPORT
ODUK-AIS-TCM2	TCM2 Alarm Indication Signal	Event	TRANSPORT
ODUK-AIS-TCM3	TCM3 Alarm Indication Signal	Event	TRANSPORT
ODUK-AIS-TCM4	TCM4 Alarm Indication Signal	Event	TRANSPORT
ODUK-AIS-TCM5	TCM5 Alarm Indication Signal	Event	TRANSPORT
ODUK-AIS-TCM6	TCM6 Alarm Indication Signal	Event	TRANSPORT
ODUK-BDI-PM	ODUk: PM Backward Defect Indication	Alarm	TRANSPORT
ODUK-BDI-TCM1	TCM1 Backward Defect Monitoring	Event	TRANSPORT
ODUK-BDI-TCM2	TCM2 Backward Defect Monitoring	Event	TRANSPORT
ODUK-BDI-TCM3	TCM3 Backward Defect Monitoring	Event	TRANSPORT
ODUK-BDI-TCM4	TCM4 Backward Defect Monitoring	Event	TRANSPORT
ODUK-BDI-TCM5	TCM5 Backward Defect Monitoring	Event	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
ODUK-BDI-TCM6	TCM6 Backward Defect Monitoring	Event	TRANSPORT
ODUK-BIAE	Path Monitoring Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-BIAE-TCM1	TCM1 Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-BIAE-TCM2	TCM2 Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-BIAE-TCM3	TCM3 Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-BIAE-TCM4	TCM4 Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-BIAE-TCM5	TCM5 Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-BIAE-TCM6	TCM6 Backward Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE	Path Monitoring Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE-TCM1	TCM1 Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE-TCM2	TCM2 Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE-TCM3	TCM3 Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE-TCM4	TCM4 Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE-TCM5	TCM5 Incoming Alignment Error	Event	TRANSPORT
ODUK-IAE-TCM6	TCM6 Incoming Alignment Error	Event	TRANSPORT
ODUK-LCK-PM	ODUk: Locked Defect - PM	Alarm	TRANSPORT
ODUK-LCK-TCM1	TCM1 Locked	Event	TRANSPORT
ODUK-LCK-TCM2	TCM2 Locked	Event	TRANSPORT
ODUK-LCK-TCM3	TCM3 Locked	Event	TRANSPORT
ODUK-LCK-TCM4	TCM4 Locked	Event	TRANSPORT
ODUK-LCK-TCM5	TCM5 Locked	Event	TRANSPORT
ODUK-LCK-TCM6	TCM6 Locked	Event	TRANSPORT
ODUK-LTC-TCM1	TCM1 Loss of Tandem Connection	Event	TRANSPORT
ODUK-LTC-TCM2	TCM2 Loss of Tandem Connection	Event	TRANSPORT
ODUK-LTC-TCM3	TCM3 Loss of Tandem Connection	Event	TRANSPORT
ODUK-LTC-TCM4	TCM4 Loss of Tandem Connection	Event	TRANSPORT
ODUK-LTC-TCM5	TCM5 Loss of Tandem Connection	Event	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
ODUK-LTC-TCM6	TCM6 Loss of Tandem Connection	Event	TRANSPORT
ODUK-OCI-PM	ODUk: Open Connection Indication	Alarm	TRANSPORT
ODUK-OCI-TCM1	TCM1 Open Connection Indication	Event	TRANSPORT
ODUK-OCI-TCM2	TCM2 Open Connection Indication	Event	TRANSPORT
ODUK-OCI-TCM3	TCM3 Open Connection Indication	Event	TRANSPORT
ODUK-OCI-TCM4	TCM4 Open Connection Indication	Event	TRANSPORT
ODUK-OCI-TCM5	TCM5 Open Connection Indication	Event	TRANSPORT
ODUK-OCI-TCM6	TCM6 Open Connection Indication	Event	TRANSPORT
ODUK-SD-PM	ODUk: Signal Degrade	Alarm	TRANSPORT
ODUK-SD-TCM1	TCM1 Signal Degrade	Event	TRANSPORT
ODUK-SD-TCM2	TCM2 Signal Degrade	Event	TRANSPORT
ODUK-SD-TCM3	TCM3 Signal Degrade	Event	TRANSPORT
ODUK-SD-TCM4	TCM4 Signal Degrade	Event	TRANSPORT
ODUK-SD-TCM5	TCM5 Signal Degrade	Event	TRANSPORT
ODUK-SD-TCM6	TCM6 Signal Degrade	Event	TRANSPORT
ODUK-SF-PM	ODUk: Signal Failure	Alarm	TRANSPORT
ODUK-SF-TCM1	TCM1 Signal Failure	Event	TRANSPORT
ODUK-SF-TCM2	TCM2 Signal Failure	Event	TRANSPORT
ODUK-SF-TCM3	TCM3 Signal Failure	Event	TRANSPORT
ODUK-SF-TCM4	TCM4 Signal Failure	Event	TRANSPORT
ODUK-SF-TCM5	TCM5 Signal Failure	Event	TRANSPORT
ODUK-SF-TCM6	TCM6 Signal Failure	Event	TRANSPORT
ODUK-TIM-PM	ODUk: Trail Trace Identifier Mismatch	Alarm	TRANSPORT
ODUK-TIM-TCM1	TCM1 Trail Trace Identifier Mismatch	Event	TRANSPORT
ODUK-TIM-TCM2	TCM2 Trail Trace Identifier Mismatch	Event	TRANSPORT
ODUK-TIM-TCM3	TCM3 Trail Trace Identifier Mismatch	Event	TRANSPORT
ODUK-TIM-TCM4	TCM4 Trail Trace Identifier Mismatch	Event	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
ODUK-TIM-TCM5	TCM5 Trail Trace Identifier Mismatch	Event	TRANSPORT
ODUK-TIM-TCM6	TCM6 Trail Trace Identifier Mismatch	Event	TRANSPORT
ONE-OR-MORE-FAN-TRAY-ABSENT	One or more Fan Trays missing	Alarm	EQUIPMENT
ONE-OR-MORE-LC-MISSING	One or more LCs missing, running fans at max speed One or more LCs missing, running fans at max speed	Alarm	EQUIPMENT
OPEN-SLOT	Open Slot(s)	Alarm	EQUIPMENT
OPT-MOD-ABSENT	One or more Optical Modules missing	Alarm	EQUIPMENT
OPU-CSF	OPU Client Signal Fail	Alarm	TRANSPORT
OPWR-HDEG	Optical Power Degrade High	Alarm	OPTICAL
OPWR-HFAIL	Optical Power Failure High	Alarm	OPTICAL
OPWR-LDEG	Optical Power Degrade Low	Alarm	OPTICAL
OPWR-LFAIL	Optical Power Failure Low	Alarm	OPTICAL
OSNR	Optical Signal-to-Noise Ratio	Alarm	TRANSPORT
OSRION	Optical Safety Remote Interlock On	Alarm	OPTICAL
OTDR-ABSOLUTE-A-EXCEEDED-RX	Attenuation Exceeded Absolute Threshold - RX Direction	Alarm	MAINTENANCE
OTDR-ABSOLUTE-A-EXCEEDED-TX	Attenuation Exceeded Absolute Threshold - TX Direction	Alarm	MAINTENANCE
OTDR-ABSOLUTE-R-EXCEEDED-RX	Reflectance Exceeded Absolute Threshold - RX Direction	Alarm	MAINTENANCE
OTDR-ABSOLUTE-R-EXCEEDED-TX	Reflectance Exceeded Absolute Threshold - TX Direction	Alarm	MAINTENANCE
OTDR-BASELINE-A-EXCEEDED-RX	Attenuation Exceeded Baseline Threshold - RX Direction	Alarm	MAINTENANCE
OTDR-BASELINE-A-EXCEEDED-TX	Attenuation Exceeded Baseline Threshold - TX Direction	Alarm	MAINTENANCE
OTDR-BASELINE-R-EXCEEDED-RX	Reflectance Exceeded Baseline Threshold - RX Direction	Alarm	MAINTENANCE
OTDR-BASELINE-R-EXCEEDED-TX	Reflectance Exceeded Baseline Threshold - TX Direction	Alarm	MAINTENANCE
OTDR-FAST-FAR-END-IN-PROGRESS	OTDR Fast Scan Is In Progress On Remote Side	Alarm	MAINTENANCE

Condition Name	Description	Condition Type	Alarm Category
OTDR-FAST-SCAN-IN-PROGRESS-RX	OTDR Fast Scan Is In Progress - RX Direction	Alarm	MAINTENANCE
OTDR-FAST-SCAN-IN-PROGRESS-TX	OTDR Fast Scan Is In Progress - TX Direction	Alarm	MAINTENANCE
OTDR-FIBER-END-NOT-DETECTED-RX	Fiber End Not Detected - RX Direction	Alarm	MAINTENANCE
OTDR-FIBER-END-NOT-DETECTED-TX	Fiber End Not Detected - TX Direction	Alarm	MAINTENANCE
OTDR-HYBRID-SCAN-IN-PROGRESS	OTDR Hybrid Scan Is In Progress On Remote Side	Alarm	MAINTENANCE
OTDR-HYBRID-SCAN-IN-PROGRESS-RX	OTDR Hybrid Scan Is In Progress - RX Direction	Alarm	MAINTENANCE
OTDR-HYBRID-SCAN-IN-PROGRESS-TX	OTDR Hybrid Scan Is In Progress - TX Direction	Alarm	MAINTENANCE
OTDR-LOSS-THR-EXCEEDED	OTDR Loss Threshold Exceeded	Alarm	MAINTENANCE
OTDR-ORL-THRESHOLD-EXCEEDED-RX	ORL Exceeded Threshold - RX Direction	Alarm	MAINTENANCE
OTDR-ORL-THRESHOLD-EXCEEDED-TX	ORL Exceeded Threshold - TX Direction	Alarm	MAINTENANCE
OTDR-ORL-TRAINING-FAILED-RX	ORL Training Failed - RX Direction	Alarm	MAINTENANCE
OTDR-ORL-TRAINING-FAILED-TX	ORL Training Failed - TX Direction	Alarm	MAINTENANCE
OTDR-ORL-TRAINING-IN-PROGRESS-RX	ORL Training Is In Progress - RX Direction	Alarm	MAINTENANCE
OTDR-ORL-TRAINING-IN-PROGRESS-TX	ORL Training Is In Progress - TX Direction	Alarm	MAINTENANCE
OTDR-OTDR-TRAINING-FAILED-RX	OTDR Training Failed - RX Direction	Alarm	MAINTENANCE
OTDR-OTDR-TRAINING-FAILED-TX	OTDR Training Failed - TX Direction	Alarm	MAINTENANCE
OTDR-SCAN-FAILED	OTDR Scan Failed	Alarm	MAINTENANCE
OTDR-SCAN-FAILED-RX	OTDR Scan Failed RX	Alarm	MAINTENANCE
OTDR-SCAN-FAILED-TX	OTDR Scan Failed TX	Alarm	MAINTENANCE
OTDR-SCAN-IN-PROGRESS	OTDR Scan Is In Progress	Alarm	MAINTENANCE
OTDR-SCAN-IN-PROGRESS-RX	OTDR Scan In Progress RX	Alarm	MAINTENANCE
OTDR-SCAN-IN-PROGRESS-TX	OTDR Scan In Progress TX	Alarm	MAINTENANCE
OTDR-SCAN-NOT-COMPLETED	OTDR Scan Not Completed	Alarm	MAINTENANCE
OTN-XP-DP-FPD-PKG-MISSING	OTN XP Data Plane FPD Package Missing	Alarm	SYSTEM
OTNSEC-LOCALLY-SECURED	OTNSEC Locally Secured	Alarm	SECURITY
OTUK-AIS	OTUk: Alarm Indication Signal	Alarm	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
OTUK-BDI	OTUk: SM Backward Defect Indication	Alarm	TRANSPORT
OTUK-BIAE	OTUk: SM Backward Incoming Alignment Error	Alarm	TRANSPORT
OTUK-IAE	OTUk: Incoming Alignment Error	Alarm	TRANSPORT
OTUK-LOF	OTUk: Loss Of Frame	Alarm	TRANSPORT
OTUK-LOM	OTUk Loss Of MultiFrame	Event	TRANSPORT
OTUK-SD	OTUk: Signal Degrade	Alarm	TRANSPORT
OTUK-SF	OTUk: Signal Failure	Alarm	TRANSPORT
OTUK-TIM	OTUk: Trail Trace Identifier Mismatch	Alarm	TRANSPORT
OVER-TEMP-UNIT-PROT	Over Temperature Unit Protected	Alarm	EQUIPMENT
PARAM-MISM	Plug-in Module Range Settings Mismatch	Alarm	OPTICAL
PARTIAL-TOPOLOGY	APC Partial topology	Alarm	OPTICAL
PATCH-ACTIVATION-FAILED	Patch Activation Failed	Alarm	SYSTEM
PATCH-DOWNLOAD-FAILED	Patch Download Failed	Alarm	SYSTEM
PCS-ERROR	PCS Error/Invalid	Alarm	TRANSPORT
PEER-CERT-VERIFICATION-FAILED	Peer card certificate verification failed	Alarm	TRANSPORT
PEER-CSF	Peer Port Client Signal Fail Detected	Alarm	TRANSPORT
PEX-SWITCH-ACCESS-FAILURE	PEX Switch Access Failure	Alarm	EQUIPMENT
PM-TCA	Performance Monitor Threshold Crossing Alert	Event	TCA
PMD-DEG	PMD Degrade	Alarm	OPTICAL
PMI	Payload Missing Indication	Alarm	OPTICAL
PORT-COMM-FAIL	Module Communication Failure	Alarm	EQUIPMENT
POWERMODULEFANOUTOFTOLERANCE	Power Module: fan out of tolerance	Alarm	EQUIPMENT
POWERMODULEFANTOLERANCEWARNING	Power Module Warning: fan out of tolerance	Alarm	EQUIPMENT
POWERMODULEOUTPUT-DISABLED	Power Module Output Disable	Alarm	EQUIPMENT
POWERMODULEREDUNDANCYLOST	Power Module Redundancy lost	Alarm	EQUIPMENT
POWER-OFF	Card In Power Off Status	Alarm	EQUIPMENT
POWER-ON-TIMEOUT	Card In Power On Timeout	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
PPM-MISMATCH	Incompatible pluggable inserted in the port	Alarm	EQUIPMENT
PRBS-ENABLED	PRBS Generation Enabled	Alarm	TRANSPORT
PROT-CONFIG-MISMATCH	Protection Card Configuration Mismatch	Alarm	PROTECTION
PROT-SOFT-VERIF-FAIL	Protect Volume Software Signature Verification Failed	Alarm	SECURITY
PROTNA	Protection Unit Not Available	Alarm	EQUIPMENT
PROV-FAILED	Provisioning Failed	Alarm	SYSTEM
PROV-IN-PROG	Provisioning In Progress	Event	TRANSPORT
PROV-INCOMPATIBLE	Incompatible Provision	Alarm	EQUIPMENT
PROV-INPROGRESS	Provisioning In Progress	Alarm	SYSTEM
PROV-MISMATCH	Provisioning Mismatch	Alarm	EQUIPMENT
PROV-MISMATCH	Provisioning Mismatch	Alarm	EQUIPMENT
PSD-FAILED	Failure in Power Spectrum Distribution	Alarm	OPTICAL
PSWD-CHG-REQUIRED	User Password Change Required	Event	SECURITY
PTIM	Payload Type Identifier Mismatch	Alarm	TRANSPORT
PWR	Power Failure at Connector	Alarm	EQUIPMENT
PWR-CON-LMT	Power Consumption Limit Has Crossed	Alarm	EQUIPMENT
PWR-ERROR	Power Module Error (PM_VIN_VOLT_OOR)	Alarm	EQUIPMENT
PWR-EXCEEDS	Power reservation exceeds configured power	Alarm	EQUIPMENT
PWR-EXCEEDS-CAPACITY	Power reservation exceeds configured power capacity	Alarm	EQUIPMENT
PWR-FAIL-A	Equipment power failure at connector A	Alarm	EQUIPMENT
PWR-FAIL-B	Equipment power failure at connector B	Alarm	EQUIPMENT
PWR-FAIL-RET-A	Equipment power failure at return connector A	Alarm	EQUIPMENT
PWR-FAIL-RET-B	Equipment power failure at return connector B	Alarm	EQUIPMENT
PWR-GRP-REDUNDANCY-LOST	Power Group Redundancy lost	Alarm	EQUIPMENT
PWR-MISMATCH	PEM PID mismatch in the chassis	Alarm	EQUIPMENT
PWR-OUTPUT-DISABLED	Power Module Output Disabled (PM_OUTPUT_DISABLED)	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
PWR-PROT-ON	Raman Power Protection On	Alarm	OPTICAL
PWRRESTART	Powerfail Restart	Alarm	EQUIPMENT
RACK-OBFL-ERROR	Obfl error	Alarm	EQUIPMENT
RAMAN-AMPLI-OSRI	Raman Amplifier Optical Safety Remote Interlock	Alarm	OPTICAL
RAMAN-CALIBRATION-FAILED	Raman Calibration Failed	Alarm	OPTICAL
RAMAN-CALIBRATION-PENDING	Raman Calibration Pending	Alarm	OPTICAL
RAMAN-CALIBRATION-RUNNING	Raman Calibration Running	Alarm	OPTICAL
RAMAN-GAIN-NOT-REACHED	Raman Gain Not Reached	Alarm	OPTICAL
RAMAN-TURNUP-FAIL	Raman Pumps Turnup Fail	Alarm	OPTICAL
RDI-L	Remote Defect Indication Line	Alarm	TRANSPORT
REMOTE-CERT-FAIL	RemoteCard Certificate Validation Failed	Alarm	TRANSPORT
REMOTE-DEG-SER	Remote FEC Degraded Symbol Error Rate	Event	TRANSPORT
REMOTE-FAULT	Remote Fault	Alarm	TRANSPORT
REROUTE-IN-PROG	Reroute In Progress	Alarm	PROTECTION
RESOURCE-ALLOC-FAIL	Resource Allocation Failed	Alarm	EQUIPMENT
RESOURCES-GONE	No More Resources Available	Alarm	EQUIPMENT
RESOURCES-LOW	Running Low On Resources	Alarm	SYSTEM
RESTORE-IN-PROG	Restoration in Progress	Alarm	PROTECTION
REVERT-IN-PROG	Revert In Progress	Alarm	PROTECTION
RFI	Remote Failure Indication	Alarm	OPTICAL
RLS	Raman Laser Shutdown	Alarm	OPTICAL
RMON-ALARM	RMON Threshold Crossing Alarm	Event	OPTICAL
RMON-RESET	RMON Histories And Alarms Reset Reboot	Event	OPTICAL
ROLE-SWITCH-ACTIVE	Role is Switched to active	Event	SYSTEM
ROUTE-OVERFLOW	OSPF Routing Table Overflow	Alarm	SYSTEM
RS-EOC	Regenerator Section - DCC Termination Failure	Alarm	TRANSPORT
RS-TIM	Regenerator Section Trace Identifier Mismatch	Alarm	TRANSPORT

Condition Name	Description	Condition Type	Alarm Category
RUNNING-FANS-AT-MAX-SPEED	FANs Running At Maximum Speed	Alarm	EQUIPMENT
RX-BELOW-MIN-PSD	Receive Channel Power Below Minimum Power Spectral Density	Alarm	OPTICAL
SD	Signal Degrade	Alarm	OPTICAL
SD-L	BER Threshold Exceeded For Signal Degrade Line	Alarm	TRANSPORT
SENSOR-HIGH-0-6V-CPU-A	0.6V-CPU-A sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-0-6V-CPU-B	0.6V-CPU-B sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-05V-CPU	1.05V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-0V	1.0V sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-0V-PHY	1.0V-PHY sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-2V	1.2V sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-2V-CPU	1.2V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-3V-CPU	1.3V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-5V-CPU	1.5V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-7V-CPU	1.7V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-82V-CPU	1.82V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-1-8V	1.8V sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-2-5V	2.5V sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-3-3V	3.3V sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-3-3V-CPU	3.3V-CPU sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-3-3V-STBY	3.3V-STBY sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-5-0V-STBY	5.0V-STBY sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-BP-48V	BP-48V sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-CPU-TEMP	CPU-TEMP sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-DDR-CH0-TEMP	DDR-CH0-TEMP sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-DDR-CH1-TEMP	DDR-CH1-TEMP sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-ETHERNET-SWITCH-TEMP	ETHERNET-SWITCH-TEMP sensor high	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
SENSOR-HIGH-HOTSPOT1	HOTSPOT1 sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-HOTSPOT2	HOTSPOT2 sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-INLET-AIR	INLET-AIR sensor high	Alarm	EQUIPMENT
SENSOR-HIGH-OUTLET-AIR	OUTLET-AIR sensor high	Alarm	EQUIPMENT
SENSOR-LOW-0-6V-CPU-A	0.6V-CPU-A sensor low	Alarm	EQUIPMENT
SENSOR-LOW-0-6V-CPU-B	0.6V-CPU-B sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-05V-CPU	1.05V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-0V	1.0V sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-0V-PHY	1.0V-PHY sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-2V	1.2V sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-2V-CPU	1.2V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-3V-CPU	1.3V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-5V-CPU	1.5V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-7V-CPU	1.7V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-82V-CPU	1.82V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-1-8V	1.8V sensor low	Alarm	EQUIPMENT
SENSOR-LOW-2-5V	2.5V sensor low	Alarm	EQUIPMENT
SENSOR-LOW-3-3V	3.3V sensor low	Alarm	EQUIPMENT
SENSOR-LOW-3-3V-CPU	3.3V-CPU sensor low	Alarm	EQUIPMENT
SENSOR-LOW-3-3V-STBY	3.3V-STBY sensor low	Alarm	EQUIPMENT
SENSOR-LOW-5-0V-STBY	5.0V-STBY sensor low	Alarm	EQUIPMENT
SENSOR-LOW-BP-48V	BP-48V sensor low	Alarm	EQUIPMENT
SENSOR-LOW-CPU-TEMP	CPU-TEMP sensor low	Alarm	EQUIPMENT
SENSOR-LOW-DDR-CH0-TEMP	DDR-CH0-TEMP sensor low	Alarm	EQUIPMENT
SENSOR-LOW-DDR-CH1-TEMP	DDR-CH1-TEMP sensor low	Alarm	EQUIPMENT
SENSOR-LOW-ETHERNET-SWITCH-TEMP	ETHERNET-SWITCH-TEMP sensor low	Alarm	EQUIPMENT
SENSOR-LOW-HOTSPOT1	HOTSPOT1 sensor low	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
SENSOR-LOW-HOTSPOT2	HOTSPOT2 sensor low	Alarm	EQUIPMENT
SENSOR-LOW-INLET-AIR	INLET-AIR sensor low	Alarm	EQUIPMENT
SENSOR-LOW-OUTLET-AIR	OUTLET-AIR sensor low	Alarm	EQUIPMENT
SESSION-TIME-LIMIT	Session Time Limit Expired	Event	SECURITY
SF	Signal Failure	Alarm	OPTICAL
SF-L	BER Threshold Exceeded For Signal Failure Line	Alarm	OPTICAL
SFTWDOWN	Software Download In Progress	Alarm	SYSTEM
SFTWDOWN-FAIL	Software Download Failed	Alarm	SYSTEM
SHELF-COMM-FAIL	Shelf Communication Failure	Alarm	EQUIPMENT
SIGLOSS	Signal Loss on Data Interface	Alarm	OPTICAL
SIGNALLOSS SPANLOSSDIFFOUTOF RANGE	Difference in Rx OSC span loss and Rx signal span loss exceeded threshold	Alarm	OPTICAL
SIP	Startup In Progress	Alarm	TRANSPORT
SNTP-HOST	NTP/SNTP Host Failure	Alarm	SYSTEM
SOFT-VERIF-FAIL	Software Signature Verification Failed	Alarm	SYSTEM
SPANLOSSBASELINEDEVIATIONOUTOF RANGE	Rx span loss deviated from baselin	Alarm	OPTICAL
SPAN-LOSS-OUT-OF-RANGE	Span Loss Value Out Of Range	Alarm	OPTICAL
SPAN-NOT-MEASURED	Span Measurement Cannot Be Performed	Alarm	OPTICAL
SPAN-TOO-SHORT	OTS Span Too Short	Alarm	OPTICAL
SPECTRUM-VIOLATED	Spectrum is Violated	Alarm	OPTICAL
SQUELCHED	Equipment Squelched	Alarm	TRANSPORT
SSD-ATA-ERRORS	CPU SSD ATA Error	Alarm	EQUIPMENT
SSD-HI-TEMP	CPU SSD High Temperature	Alarm	EQUIPMENT
SSM-DUS	Do Not Use For Synchronization	Alarm	TIMING
SSM-FAIL	Failed To Receive Synchronization Status Message	Alarm	TIMING
SSM-LNC	G812L - Local Node Clock traceable	Alarm	TIMING

Condition Name	Description	Condition Type	Alarm Category
SSM-OFF	Synchronization Status Messages Are Disabled On This Interface	Alarm	TIMING
SSM-PRC	G811 - Primary Reference Clock traceable	Alarm	TIMING
SSM-PRS	Stratum 1 Primary Reference Source Traceable	Alarm	TIMING
SSM-RES	Reserved For Network Synchronization Use	Alarm	TIMING
SSM-SDH-TN	G812T - Transit Node Clock traceable	Alarm	TIMING
SSM-SETS	G813 - Synchronous Equipment Timing Source traceable	Alarm	TIMING
SSM-SMC	SONET Minimum Clock Traceable	Alarm	TIMING
SSM-ST2	Stratum 2 Traceable	Alarm	TIMING
SSM-ST3	Stratum 3 Traceable	Alarm	TIMING
SSM-ST3E	Stratum 3E Traceable	Alarm	TIMING
SSM-ST4	Stratum 4 Traceable	Alarm	TIMING
SSM-STU	Synchronized - Traceability Unknown	Alarm	TIMING
SSM-TNC	Transit Node Clock Traceable	Alarm	TIMING
SW-MISMATCH	Software Mismatch	Alarm	SYSTEM
SWTOPRI	Switch To Primary Reference	Alarm	TIMING
SWTOSEC	Switch To Second Reference	Alarm	TIMING
SWTOTHIRD	Switch To Third Reference	Alarm	TIMING
SYNC-FREQ	Synchronization Reference Frequency Out Of Bounds	Alarm	TIMING
SYNCCLK	Synchronization Unit Failure	Alarm	TIMING
SYNCLOSS	Synchronization Loss on Data Interface	Alarm	TIMING
SYNCPRI	Primary Synchronization Reference Failure	Alarm	TIMING
SYNCPRI	Primary Synchronization Reference Failure	Alarm	TIMING
SYNCSEC	Secondary Synchronization Reference Failure	Alarm	TIMING
SYNCTHIRD	Third Synchronization Reference Failure	Alarm	TIMING
SYSBOOT	System Reboot	Alarm	SYSTEM
TD-FAILED	Tone Detection Failed	Event	MAINTENANCE

Condition Name	Description	Condition Type	Alarm Category
TD-INPROGRESS	Tone Detection In Progress	Alarm	MAINTENANCE
TD-LASER-ON	Tone Detection Laser is ON	Event	MAINTENANCE
TD-SUCCESS	Tone Detection Success	Event	MAINTENANCE
TEMP-LIC	Temporary License Is In Use	Alarm	SYSTEM
TEMP-MISM	Temperature Reading Mismatch Between SC Cards	Alarm	EQUIPMENT
TEMPERATURE	Temperature out of working range	Alarm	EQUIPMENT
TG-INPROGRESS	Tone Generation In Progress	Alarm	MAINTENANCE
TIM-S	Section Trace Identifier Mismatch	Alarm	TRANSPORT
TRAF-AFFECT-RESET-REQUIRED	Traffic Affecting Reset Required	Alarm	EQUIPMENT
TRAF-AFFECT-SEC-UPG-REQUIRED	Traffic Affecting Security Upgrade Required	Alarm	EQUIPMENT
TRAIL-SIGNAL-FAIL	Trail Signal Fail	Alarm	TRANSPORT
TRUNK-ODU-AIS	Trunk ODU Alarm Indication Signal	Alarm	TRANSPORT
TRUNK-OPU-CSF	Trunk OPU Client Signal Fail	Alarm	TRANSPORT
TRUNK-PAYLOAD-MISM	Trunk Payload Type Mismatch	Alarm	TRANSPORT
TX-POWER-PROV-MISMATCH	Provisioned Optics Transmit Power Not Supported	Event	TRANSPORT
UNC-WORD	FEC Uncorrected Word	Alarm	TRANSPORT
UNIT-HIGH-TEMP	Unit High Temperature	Alarm	EQUIPMENT
UNQUAL-PPM	Unqualified PPM Inserted	Alarm	EQUIPMENT
UNTRUSTED-APPLICATION	Trust Not Established With CSLU/CSSM	Alarm	SYSTEM
USAGE-NOT-REPORTED	Licenses Usage Is Not Reported	Alarm	SYSTEM
USB-MOUNT-FAIL	USB Mount Failure	Alarm	EQUIPMENT
USB-OC-1	USB 1 Over Current	Alarm	EQUIPMENT
USB-OC-2	USB 2 Over Current	Alarm	EQUIPMENT
USB-PORTS-DOWN	USB Ports in ECU are not functional	Event	EQUIPMENT
USB-WRITE-FAIL	USB Write Failure	Alarm	EQUIPMENT
USBSYNC	USB Sync in Progress	Alarm	EQUIPMENT

Condition Name	Description	Condition Type	Alarm Category
USER-LOCKOUT	User Locked Out	Event	SECURITY
USER-LOGIN	Login of User	Event	SECURITY
USER-LOGOUT	Logout of User	Event	SECURITY
VOA-DISABLED	VOA Control Loop Disable Due To Excessive Counter-Propagation Light	Alarm	OPTICAL
VOA-HDEG	Variable Optical Attenuator Degrade High	Alarm	OPTICAL
VOA-HFAIL	Variable Optical Attenuator Failure High	Alarm	OPTICAL
VOA-LDEG	Variable Optical Attenuator Degrade Low	Alarm	OPTICAL
VOA-LFAIL	Variable Optical Attenuator Failure Low	Alarm	OPTICAL
VOLT-MISM	Voltage Reading Mismatch Between SC Cards	Alarm	EQUIPMENT
WKSWBK	Switched Back To Working	Event	PROTECTION
WKSWPR	Switched To Protection	Alarm	PROTECTION
WRK-PATH-RECOVERY-CHECK	Checking For Work Path Recovery	Alarm	PROTECTION
WRMRESTART	Warm Restart	Event	SYSTEM
WTR	Wait To Restore	Alarm	PROTECTION
WVL-MISMATCH	Equipment Wavelength Mismatch	Alarm	OPTICAL
WVL-UNLOCKED	Wavelength Unlocked	Alarm	OPTICAL
XGE-EEPROM-ERROR	XGE EEPROM Error	Alarm	EQUIPMENT
XGE-FLASH-ERROR	XGE Flash Error	Alarm	EQUIPMENT
T-BAD-SH	Threshold Crossing Alert	Event	TCA
T-BBE-PM	Threshold Crossing Alert	Event	TCA
T-BBE-SM	Threshold Crossing Alert	Event	TCA
T-BBE-TCM1	Threshold Crossing Alert	Event	TCA
T-BBE-TCM2	Threshold Crossing Alert	Event	TCA
T-BBEL	Threshold Crossing Alert	Event	TCA
T-BBER-PM	Threshold Crossing Alert	Event	TCA
T-BBER-SM	Threshold Crossing Alert	Event	TCA
T-BBER-TCM1	Threshold Crossing Alert	Event	TCA

Condition Name	Description	Condition Type	Alarm Category
T-BBER-TCM2	Threshold Crossing Alert	Event	TCA
T-BBES	Threshold Crossing Alert	Event	TCA
T-BIEC	Threshold Crossing Alert	Event	TCA
T-BIP	Threshold Crossing Alert	Event	TCA
T-BIT-EC	Threshold Crossing Alert	Event	TCA
T-BYTE-EC	Threshold Crossing Alert	Event	TCA
T-CDPM-AVG	Threshold Crossing Alert	Event	TCA
T-CDPM-MAX	Threshold Crossing Alert	Event	TCA
T-CDPM-MIN	Threshold Crossing Alert	Event	TCA
T-CHROM-DISP	Threshold Crossing Alert	Event	TCA
T-CVL	Threshold Crossing Alert	Event	TCA
T-CVS	Threshold Crossing Alert	Event	TCA
T-DGD-MAX	Threshold Crossing Alert	Event	TCA
T-DGD-MIN	Threshold Crossing Alert	Event	TCA
T-EC-WORD	Threshold Crossing Alert	Event	TCA
T-ES-PCS	Threshold Crossing Alert	Event	TCA
T-ES-PM	Threshold Crossing Alert	Event	TCA
T-ES-SM	Threshold Crossing Alert	Event	TCA
T-ES-TCM1	Threshold Crossing Alert	Event	TCA
T-ES-TCM2	Threshold Crossing Alert	Event	TCA
T-ESL	Threshold Crossing Alert	Event	TCA
T-ESR-PM	Threshold Crossing Alert	Event	TCA
T-ESR-SM	Threshold Crossing Alert	Event	TCA
T-ESR-TCM1	Threshold Crossing Alert	Event	TCA
T-ESR-TCM2	Threshold Crossing Alert	Event	TCA
T-ESS	Threshold Crossing Alert	Event	TCA
T-FC-L	Threshold Crossing Alert	Event	TCA

Condition Name	Description	Condition Type	Alarm Category
T-FC-PM	Threshold Crossing Alert	Event	TCA
T-FC-SM	Threshold Crossing Alert	Event	TCA
T-FC-TCM1	Threshold Crossing Alert	Event	TCA
T-FC-TCM2	Threshold Crossing Alert	Event	TCA
T-FRM-ERR	Threshold Crossing Alert	Event	TCA
T-GAIN-AVG	Threshold Crossing Alert	Event	TCA
T-GAIN-MAX	Threshold Crossing Alert	Event	TCA
T-GAIN-MIN	Threshold Crossing Alert	Event	TCA
T-LASER-BIAS-MAX	Threshold Crossing Alert	Event	TCA
T-LASER-BIAS-MIN	Threshold Crossing Alert	Event	TCA
T-LASER-TEMP-MAX	Threshold Crossing Alert	Event	TCA
T-LASER-TEMP-MIN	Threshold Crossing Alert	Event	TCA
T-LOW-FREQ-OFF-AVG	Threshold Crossing Alert	Event	TCA
T-LOW-FREQ-OFF-MAX	Threshold Crossing Alert	Event	TCA
T-LOW-FREQ-OFF-MIN	Threshold Crossing Alert	Event	TCA
T-MS-BBE	Threshold Crossing Alert	Event	TCA
T-MS-BBER	Threshold Crossing Alert	Event	TCA
T-MS-EB	Threshold Crossing Alert	Event	TCA
T-MS-ES	Threshold Crossing Alert	Event	TCA
T-MS-ESR	Threshold Crossing Alert	Event	TCA
T-MS-FC	Threshold Crossing Alert	Event	TCA
T-MS-LOSS	Threshold Crossing Alert	Event	TCA
T-MS-SES	Threshold Crossing Alert	Event	TCA
T-MS-SESR	Threshold Crossing Alert	Event	TCA
T-MS-UAS	Threshold Crossing Alert	Event	TCA
T-OPBR-AVG	Threshold Crossing Alert	Event	TCA
T-OPBR-MAX	Threshold Crossing Alert	Event	TCA

Condition Name	Description	Condition Type	Alarm Category
T-OPBR-MIN	Threshold Crossing Alert	Event	TCA
T-OPBRR-AVG	Threshold Crossing Alert	Event	TCA
T-OPBRR-MAX	Threshold Crossing Alert	Event	TCA
T-OPBRR-MIN	Threshold Crossing Alert	Event	TCA
T-OPR-AVG	Threshold Crossing Alert	Event	TCA
T-OPR-MAX	Threshold Crossing Alert	Event	TCA
T-OPR-MIN	Threshold Crossing Alert	Event	TCA
T-OPT-AVG	Threshold Crossing Alert	Event	TCA
T-OPT-MAX	Threshold Crossing Alert	Event	TCA
T-OPT-MIN	Threshold Crossing Alert	Event	TCA
T-OPWR-AVG	Threshold Crossing Alert	Event	TCA
T-OPWR-CL-MAX	Threshold Crossing Alert	Event	TCA
T-OPWR-CL-MIN	Threshold Crossing Alert	Event	TCA
T-OPWR-MAX	Threshold Crossing Alert	Event	TCA
T-OPWR-MIN	Threshold Crossing Alert	Event	TCA
T-OSC-PWR-AVG	Threshold Crossing Alert	Event	TCA
T-OSC-PWR-MAX	Threshold Crossing Alert	Event	TCA
T-OSC-PWR-MIN	Threshold Crossing Alert	Event	TCA
T-OSNR-AVG	Threshold Crossing Alert	Event	TCA
T-OSNR-MAX	Threshold Crossing Alert	Event	TCA
T-OSNR-MIN	Threshold Crossing Alert	Event	TCA
T-PCR-AVG	Threshold Crossing Alert	Event	TCA
T-PCR-MAX	Threshold Crossing Alert	Event	TCA
T-PCR-MIN	Threshold Crossing Alert	Event	TCA
T-PDL-AVG	Threshold Crossing Alert	Event	TCA
T-PDL-MAX	Threshold Crossing Alert	Event	TCA
T-PDL-MIN	Threshold Crossing Alert	Event	TCA

Condition Name	Description	Condition Type	Alarm Category
T-PMD-AVG	Threshold Crossing Alert	Event	TCA
T-PMD-MIN	Threshold Crossing Alert	Event	TCA
T-PN-MAX	Threshold Crossing Alert	Event	TCA
T-PN-MIN	Threshold Crossing Alert	Event	TCA
T-POST-FEC-BER-MAX	Threshold Crossing Alert	Event	TCA
T-POST-FEC-BER-MIN	Threshold Crossing Alert	Event	TCA
T-PRE-FEC-BER-MAX	Threshold Crossing Alert	Event	TCA
T-PRE-FEC-BER-MIN	Threshold Crossing Alert	Event	TCA
T-PWR-AVG	Threshold Crossing Alert	Event	TCA
T-PWR-MAX	Threshold Crossing Alert	Event	TCA
T-PWR-MIN	Threshold Crossing Alert	Event	TCA
T-Q-MARGIN-MAX	Threshold Crossing Alert	Event	TCA
T-Q-MARGIN-MIN	Threshold Crossing Alert	Event	TCA
T-Q-MARGIN_INST-MAX	Threshold Crossing Alert	Event	TCA
T-Q-MARGIN_INST-MIN	Threshold Crossing Alert	Event	TCA
T-Q-MAX	Threshold Crossing Alert	Event	TCA
T-Q-MIN	Threshold Crossing Alert	Event	TCA
T-RAMAN-BR-MAX	Threshold Crossing Alert	Event	TCA
T-RAMAN-BR-MIN	Threshold Crossing Alert	Event	TCA
T-RAMAN-BRR-MAX	Threshold Crossing Alert	Event	TCA
T-RAMAN-BRR-MIN	Threshold Crossing Alert	Event	TCA
T-RS-BBE	Threshold Crossing Alert	Event	TCA
T-RS-BBER	Threshold Crossing Alert	Event	TCA
T-RS-EB	Threshold Crossing Alert	Event	TCA
T-RS-ES	Threshold Crossing Alert	Event	TCA
T-RS-ESR	Threshold Crossing Alert	Event	TCA
T-RS-OFS	Threshold Crossing Alert	Event	TCA

Condition Name	Description	Condition Type	Alarm Category
T-RS-SES	Threshold Crossing Alert	Event	TCA
T-RS-SESR	Threshold Crossing Alert	Event	TCA
T-RS-UAS	Threshold Crossing Alert	Event	TCA
T-RX-PWR-MAX	Threshold Crossing Alert	Event	TCA
T-RX-PWR-MIN	Threshold Crossing Alert	Event	TCA
T-RX-SIG-POW-AVG	Threshold Crossing Alert	Event	TCA
T-RX-SIG-POW-MAX	Threshold Crossing Alert	Event	TCA
T-RX-SIG-POW-MIN	Threshold Crossing Alert	Event	TCA
T-RX-TEMP-MAX	Threshold Crossing Alert	Event	TCA
T-RX-TEMP-MIN	Threshold Crossing Alert	Event	TCA
T-SEFS	Threshold Crossing Alert	Event	TCA
T-SES-PCS	Threshold Crossing Alert	Event	TCA
T-SES-PM	Threshold Crossing Alert	Event	TCA
T-SES-SM	Threshold Crossing Alert	Event	TCA
T-SES-TCM1	Threshold Crossing Alert	Event	TCA
T-SES-TCM2	Threshold Crossing Alert	Event	TCA
T-SESL	Threshold Crossing Alert	Event	TCA
T-SESR-PM	Threshold Crossing Alert	Event	TCA
T-SESR-SM	Threshold Crossing Alert	Event	TCA
T-SESR-TCM1	Threshold Crossing Alert	Event	TCA
T-SESR-TCM2	Threshold Crossing Alert	Event	TCA
T-SESS	Threshold Crossing Alert	Event	TCA
T-SIG-SPAN-LOSS-MAX	Threshold Crossing Alert	Event	TCA
T-SIG-SPAN-LOSS-MIN	Threshold Crossing Alert	Event	TCA
T-SOPMD-AVG	Threshold Crossing Alert	Event	TCA
T-SOPMD-MAX	Threshold Crossing Alert	Event	TCA
T-SOPMD-MIN	Threshold Crossing Alert	Event	TCA

Condition Name	Description	Condition Type	Alarm Category
T-TILT-MAX	Threshold Crossing Alert	Event	TCA
T-TILT-MIN	Threshold Crossing Alert	Event	TCA
T-TOT-SPAN-LOSS-CL-MAX	Threshold Crossing Alert	Event	TCA
T-TOT-SPAN-LOSS-CL-MIN	Threshold Crossing Alert	Event	TCA
T-TOT-SPAN-LOSS-MAX	Threshold Crossing Alert	Event	TCA
T-TOT-SPAN-LOSS-MIN	Threshold Crossing Alert	Event	TCA
T-TX-PWR-MAX	Threshold Crossing Alert	Event	TCA
T-TX-PWR-MIN	Threshold Crossing Alert	Event	TCA
T-UAS-PCS	Threshold Crossing Alert	Event	TCA
T-UAS-PM	Threshold Crossing Alert	Event	TCA
T-UAS-SM	Threshold Crossing Alert	Event	TCA
T-UAS-TCM1	Threshold Crossing Alert	Event	TCA
T-UAS-TCM2	Threshold Crossing Alert	Event	TCA
T-UASL	Threshold Crossing Alert	Event	TCA
T-UASS	Threshold Crossing Alert	Event	TCA
T-UNC-WORDS	Threshold Crossing Alert	Event	TCA
T-VOA-AVG	Threshold Crossing Alert	Event	TCA
T-VOA-MAX	Threshold Crossing Alert	Event	TCA
T-VOA-MIN	Threshold Crossing Alert	Event	TCA
T-GFPSTATSROUNDTRIPLATENCYUSEC	Threshold Crossing Alert	Event	TCA
T-RXCONTROLFRAMES	Threshold Crossing Alert	Event	TCA
T-RXPAUSEFRAMES	Threshold Crossing Alert	Event	TCA
T-RXKISDROPPEDINTERNALCONGESTION	Threshold Crossing Alert	Event	TCA
T-RXUNKNOWNOPCODEFRAMES	Threshold Crossing Alert	Event	TCA
T-TXPAUSEFRAMES	Threshold Crossing Alert	Event	TCA
T-TXKISDROPPEDINTERNALCONGESTION	Threshold Crossing Alert	Event	TCA
NODE-DISCONNECT	Controller system disconnected from node	Alarm	CONCISEM

Condition Name	Description	Condition Type	Alarm Category
BACKUP-FAILURE	Controller system Database Backup Creation is failed	Alarm	CONCSYSTEM
UPLOAD-FAILURE	Controller system Database Backup File Upload to SFTP is failed	Alarm	CONCSYSTEM
NODE-BACKUP-FAILURE	Node Database Backup creation failed	Alarm	CONCSYSTEM
DISK-THRESHOLD	Disk usage exceeded the threshold.Free space is now under 30%	Alarm	CONCSYSTEM



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	.1.3.6.1.4.9.9
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