Cisco Optical Network Controller Configuration Guide, Releases 26.x.x

Cisco Optical Network Controller
Release: 26.x.x | Updated September 15, 2026

Topics included

1 Cisco Optical Network Controller Capabilities....6

Cisco Optical Network Controller functions....7
Log in to Cisco Optical Network Controller....8
User access in Cisco Optical Network Controller....9
Add local users to Cisco Optical Network Controller....12
Set up authentication using LDAP....15
Set up authentication using SAMLv2 SSO....17
Set up permission mapping....19
Manage certificates in Cisco Optical Network Controller....20
Cisco Optical Network Controller MCP server....22
Configure Cisco Optical Network Controller MCP server settings in an AI agent....23
Cisco Optical Network Controller MCP server tool descriptions....25

Part I: Cisco Optical Network Controller Applications....28

2 Topology....30

Cisco Optical Network Controller topology....31
Topology troubleshooting information....38
Use common controls in Cisco Optical Network Controller applications....38

3 Nodes....42

Cisco Optical Network Controller nodes....43
Reserved internal IP addresses and subnets....46
Add nodes on Cisco Optical Network Controller....47
Import multiple nodes into Cisco Optical Network Controller....51
Export nodes on Cisco Optical Network Controller....54
Edit nodes on Cisco Optical Network Controller....54
Delete nodes on Cisco Optical Network Controller....55
Rebuild a Cisco Optical Site Manager container....57
Node troubleshooting information....57
Test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node....58

4 Alien Import....60

Import and export alien device data....61

5 Inventory....64

View network inventory....65

6 Service Manager....68
Service Manager application....69
CPCE service endpoints and operations....75
GMPLS endpoints and operations....91

7 Alarms....112
Manage alarms....113
View events in the alarms application....115
Network level alarm correlation....116
Acknowledged alarm mute....120
SNMP traps and alarm filters....122
Alarm email forwarding....126
View and manage current alarms....131
Filter and review alarm details....134

8 Workspaces....140
Launch workspaces....141
Circuit Monitoring workspace....144
Link Monitoring workspace....153
Network Monitoring workspace....158
OTN circuits....159
OTN circuit types and topology representation....160
Discover OTN services for NCS2K-400G-XP-LC card in Service Manager....160
Monitor OTN circuits....161
Monitor OTN link utilization....162
View OTN service event history....164

9 Service Assurance....166
View Service Assurance details....167
View PSM circuits in Service Assurance....168
Unmanaged equipment....169
PSM OMS protection....171
View PSM circuits in the workspace....173
PSM wavelength protection....175

10 Software Image Management and Upgrade....178
Software image management and upgrade....179
Configure an SFTP server....181
Back up and restore nodes....183
Back up and restore the database....185
Orchestrate software upgrades....189

11 PM History....200
PM history reports....201
Access PM history report....209
Configure the SMTP mail server....212
PM data retention....214
PM retention disk space....215
PM data retention characteristics....216
PM data collection settings....217
Access PM history report....219
Configure the SMTP mail server....221
Mail server fields....222
Connectivity security options....223

12 Logs....226
Audit and debug logs....227
Access logs....233
Generate and download tech dump logs....235
Syslog forwarding configuration....236

13 Monitoring....240
Monitor logs....241
General troubleshooting information....241

14 Links....242
Cisco Optical Network Controller links....243
Use the links application....245
SLTE links and ASE services in Cisco Optical Network Controller....247

15 Alarm Troubleshooting and Categories....250
Alarm troubleshooting procedures....251
BACKUP-FAILURE alarm....251
NODE-BACKUP-FAILURE alarm....252
NODE-DISCONNECT alarm....252
UPLOAD-FAILURE alarm....253
DISK-THRESHOLD alarm....254
SWITCHOVER alarm....256
FAILOVER alarm....256
Alarm categories....257
SYSTEM alarms....258
SYSTEM events....262
EQUIPMENT alarms....263

EQUIPMENT events....273
MAINTENANCE alarms....273
MAINTENANCE events....277
CONC_SYSTEM alarms....277
TRANSPORT alarms....278
TRANSPORT events....283
PROTECTION alarms....287
PROTECTION events....288
TIMING alarms....289
SECURITY alarms....291
SECURITY events....292
OPTICAL alarms....294
OPTICAL events....299
TCA events....299

Appendix A: MIB definition for Cisco Optical Network Controller....310

1 Cisco Optical Network Controller Capabilities

Topics:

- Cisco Optical Network Controller functions
- Log in to Cisco Optical Network Controller
- User access in Cisco Optical Network Controller
- Add local users to Cisco Optical Network Controller
- Set up authentication using LDAP
- Set up authentication using SAMLv2 SSO
- Set up permission mapping
- Manage certificates in Cisco Optical Network Controller
- Cisco Optical Network Controller MCP server

Introduces Cisco Optical Network Controller capabilities, including controller functions, login, user access, authentication, high availability, certificate management, and MCP server configuration.

Cisco Optical Network Controller functions

This section explains Cisco Optical Network Controller functions, including optical domain control, path computation, model-based abstraction, and software support. Use it to understand core controller capabilities.

Cisco Optical Network Controller functions is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Cisco Optical Network Controller functions details

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

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

Optical SDN controller

Optical SDN controller is a specialized SDN controller that

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

Core functions of Cisco Optical Network Controller

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

Cisco Optical Network Controller supports several functions.

- Optical Domain Controller

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

- Path Compute Engine (PCE)

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

- Model Based Network Abstraction

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

Note

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

Note

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

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

Log in to Cisco Optical Network Controller

Use this procedure to log in to Cisco Optical Network Controller. The task helps you access the web UI before you perform configuration and monitoring tasks.

Use this procedure to log in to Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

Note

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

Follow these steps to log into Cisco Optical Network Controller:

Procedure

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

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

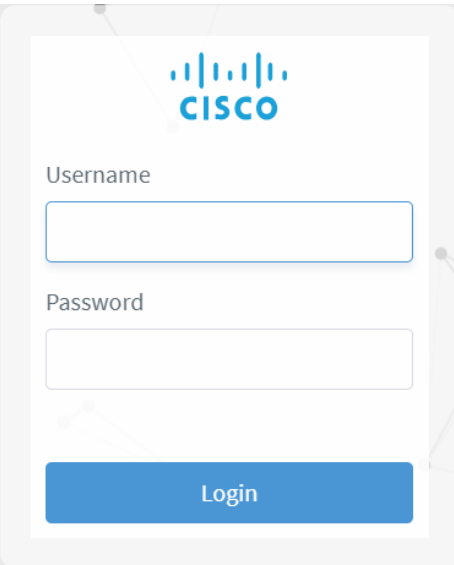
The browser displays the login page.

2. Enter the username and password.

   Username and password are provided by your system administrator.

3. Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



The log in to Cisco Optical Network Controller task is complete.

User access in Cisco Optical Network Controller

This section provides details about user access, including roles, permissions, access settings, system information, and security options. Use it to understand how Cisco Optical Network Controller manages authentication and authorization.

Use this reference to understand user access in Cisco Optical Network Controller.

Details about user access in Cisco Optical Network Controller.

Users, roles, and permissions

Users, roles, and permissions include:

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

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

Table 1: User roles and permissions

User role	Permission	Access level
Admin	permission/admin	has no restrictions
Supervisor	permission/supervisor	has similar permission as admin but with restrictions on user management and log checks
Read-only	permission/readonly	can check data, but cannot provision.
Internal	permission/internal	collects debug logs in case of any triage or troubleshooting.

Note

We recommend using it only under the supervision of the Cisco Technical Assistance Center (TAC).

Access settings

Access settings include:

- The settings button is available on the left navigation bar of Cisco Optical Network Controller.
- After clicking Settings you see the settings panel.

Figure 2: Settings

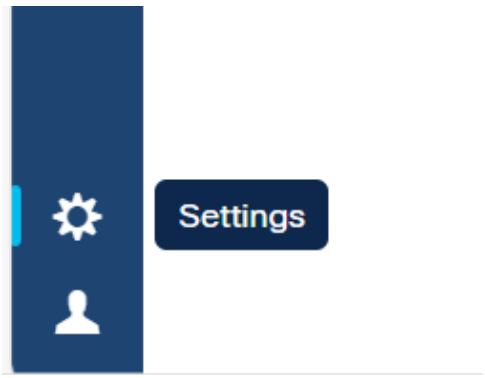
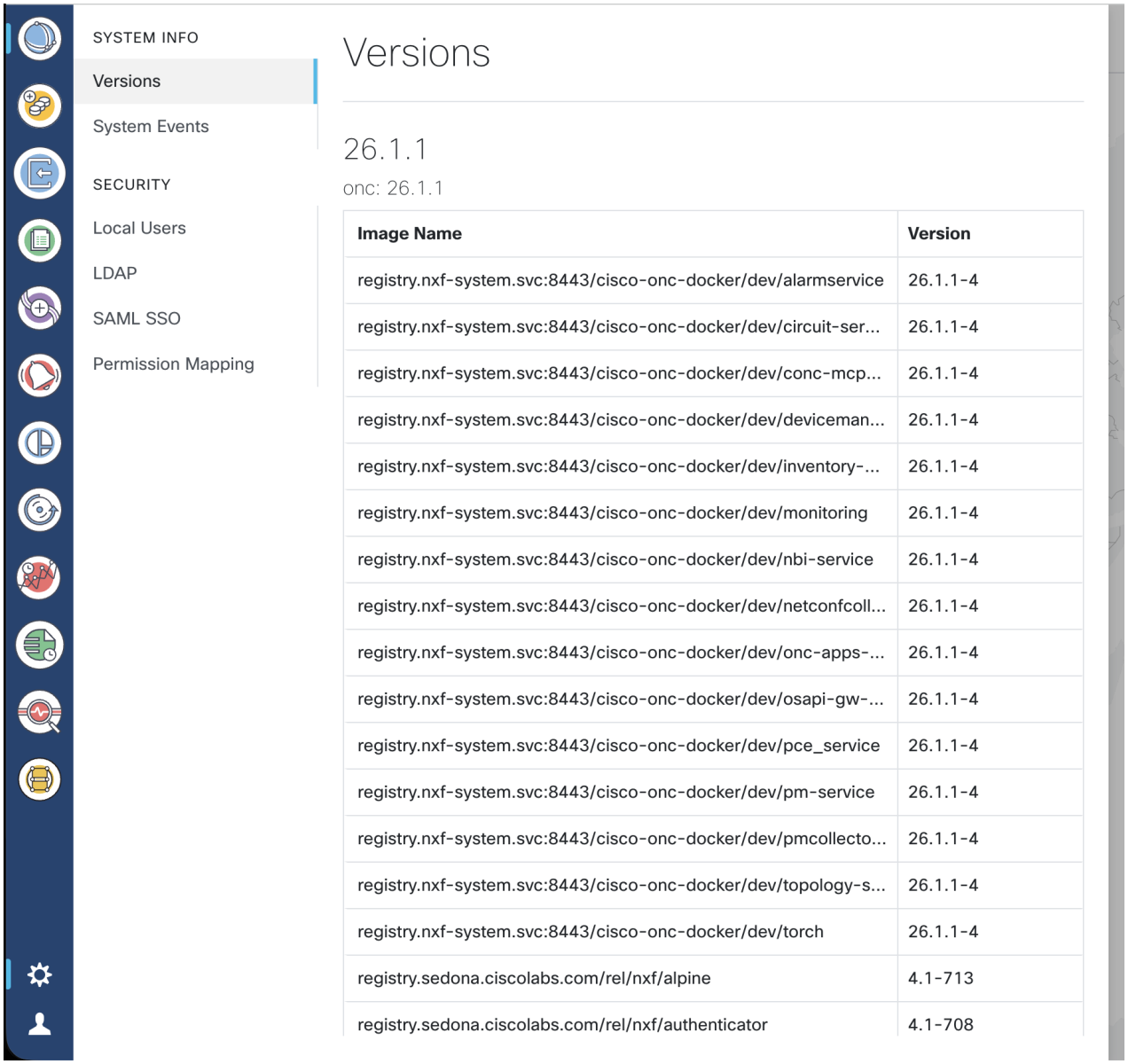


Figure 3: Settings Options



System info

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

Security

Security includes:

- 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.

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

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

Add local users to Cisco Optical Network Controller

Use this procedure to add local users to Cisco Optical Network Controller. Add local user accounts to Cisco Optical Network Controller by completing these steps.

Use this procedure to add local users to Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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.

Follow these steps to add local users to Cisco Optical Network Controller:

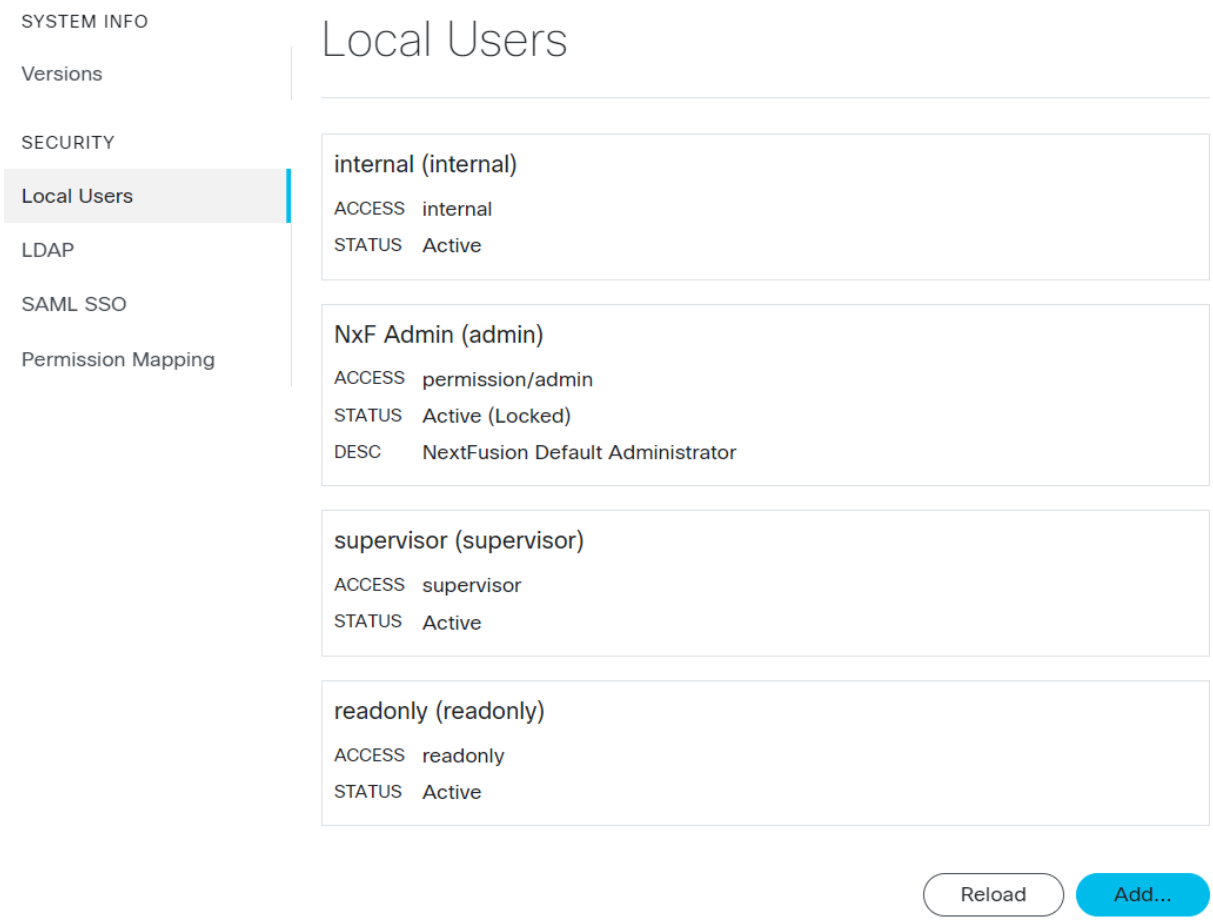
Procedure

1. From the Cisco Optical Network Controller home page click **Settings**.
2. From the panel list, select **Local Users** and click **Add**.
   The **Add User** screen appears.
3. In the **Add User** screen, fill these mandatory fields.
   a) Enter a username in **Username***.
   b) In **Password***, enter a password.
   c) In **Confirm Password***, re-enter the password to confirm the password.

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

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

Figure 4: Local Users

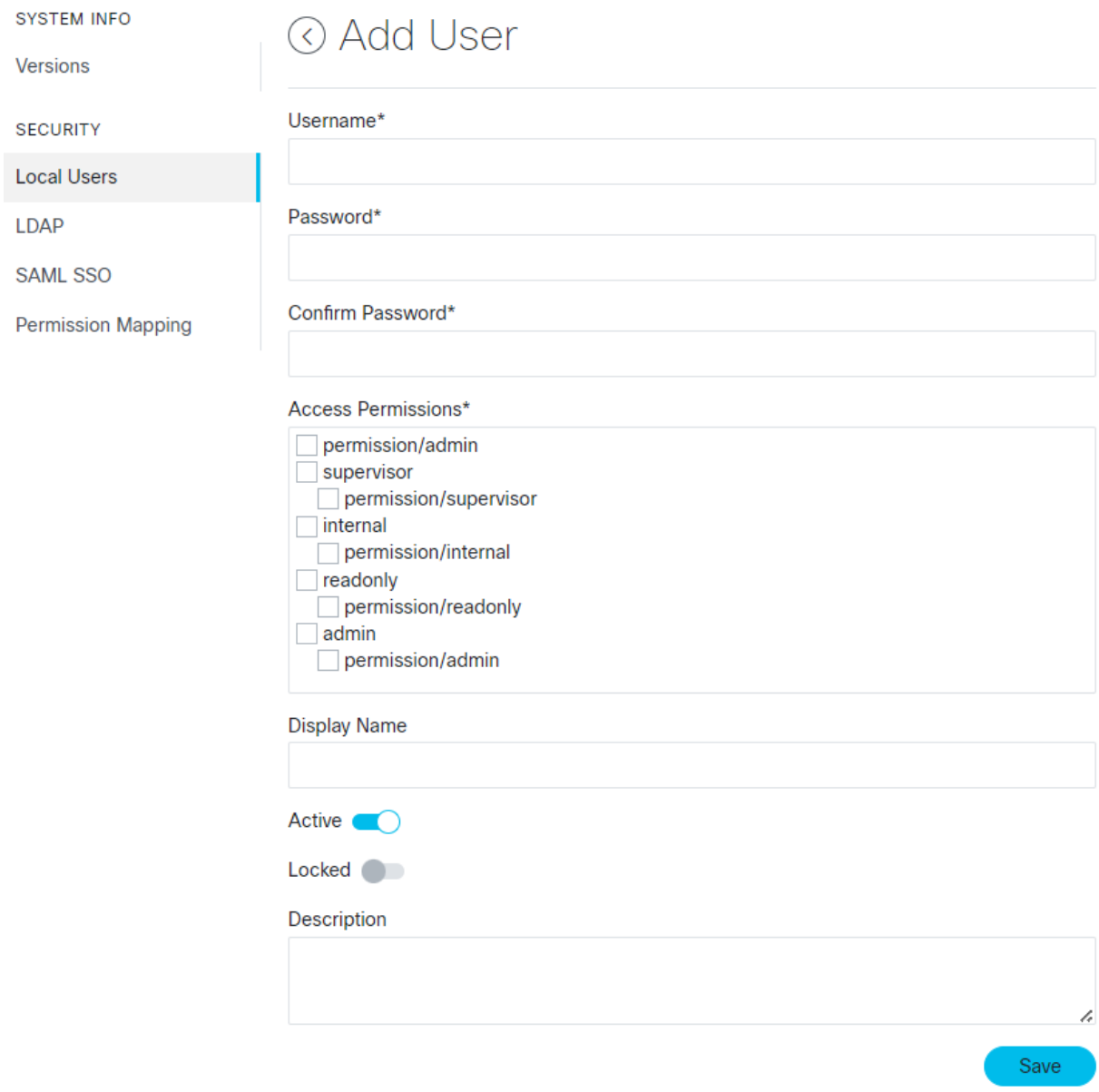


For example *permission/<admin>*

Note

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

Figure 5: Add User



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

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

- **Active enabled**: Allows the user to log into Cisco Optical Network Controller.
- **Active disabled**: Forbids the user from logging into Cisco Optical Network Controller.
- **Locked enabled**: Prevents deleting the user for auditing purposes or to retain historical data associated with that user.
- **Locked disabled**: Allows removal of the user

Table 2: Toggle combinations

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

6. Click **Save**.

Cisco Optical Network Controller successfully saves the new user.

Set up authentication using LDAP

Use this procedure to set up authentication using LDAP. The task helps you configure server details, bind credentials, and user search attributes for external authentication.

Use this procedure to set up authentication using LDAP in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

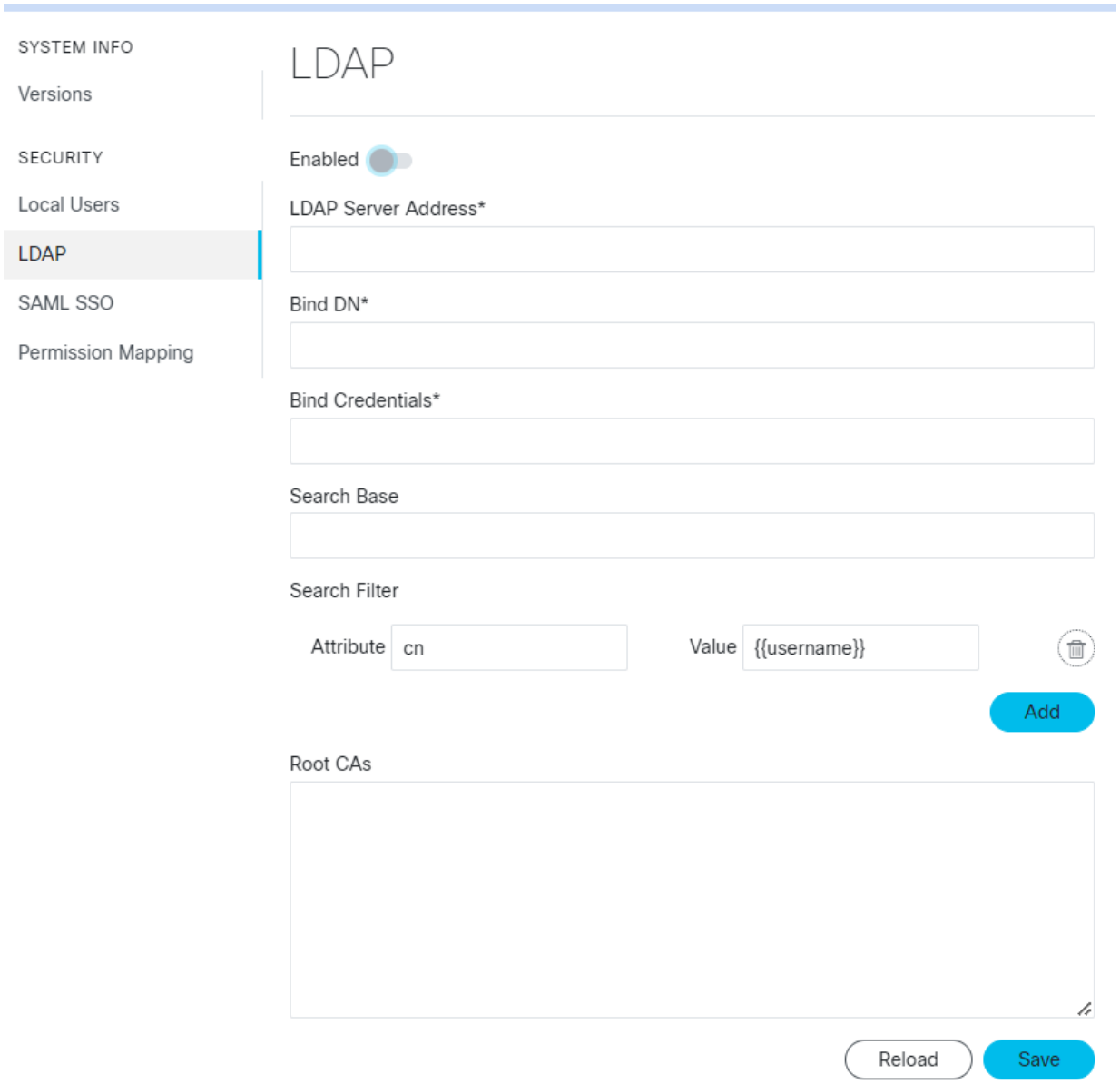
You need administrative user privileges to access Cisco Optical Network Controller.

Follow these steps to set up authentication using LDAP:

Procedure

1. From the Cisco Optical Network Controller home page click **Settings**.
2. Click **LDAP**.

Figure 6: LDAP



3. Enable **Enabled** toggle switch.
4. Fill in the mandatory fields marked with an asterisk.

Table 3: Madatory LDAP fields

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

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

5. Click **Save**.

You have successfully completed the LDAP authentication setup.

Set up authentication using SAMLv2 SSO

Use this procedure to 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.

Use this procedure to set up authentication using SAML SAMLv2 SSO in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Follow these instructions to set up SAML SSO authentication.

Before you begin

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

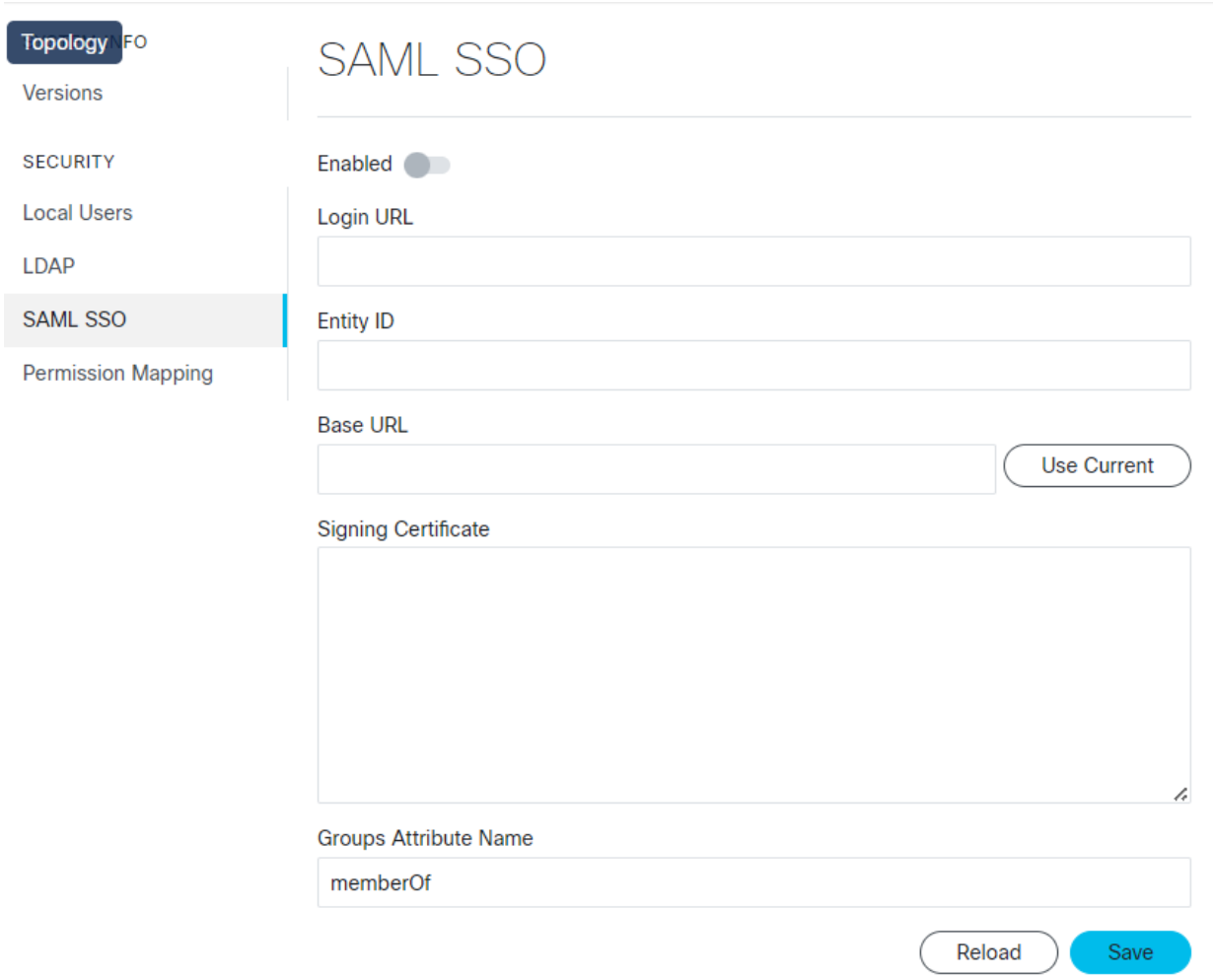
To set up authentication using SAMLv2 SSO, ensure your SSO server is installed and configured for the application.

Follow these steps to set up authentication using SAML SAMLv2 SSO:

Procedure

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

   Figure 7: SAML SSO



2. Enable **Enabled** toggle switch.
3. Fill in the fields.

Table 4: SAML SSO fields

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

4. Click **Save**.

You successfully completed the SAMLv2 SSO authentication setup.

Set up permission mapping

Use this procedure to set up permission mapping. The task helps you map roles and permissions so users receive the correct access in Cisco Optical Network Controller.

Use this procedure to set up permission mapping in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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.

Follow these steps to set up permission mapping:

Procedure

1. From the Cisco Optical Network Controller home page click **Settings**.
2. Select **Permission Mapping**.
3. Click **Add**.
4. In the **Add Permission Mapping** panel, choose one **Mapping Type** from the dropdown menu: **SAML User**, **SAML Group**, **LDAP User**, or **LDAP Group**.
5. Fill the **Match** field.

   For example, enter a specific username like 'jsmith' or a group name like 'network_admins' from your SAML/LDAP directory.
6. Select the appropriate **Access Permission**.
7. Click **Save**.

Figure 8: Permission Mapping

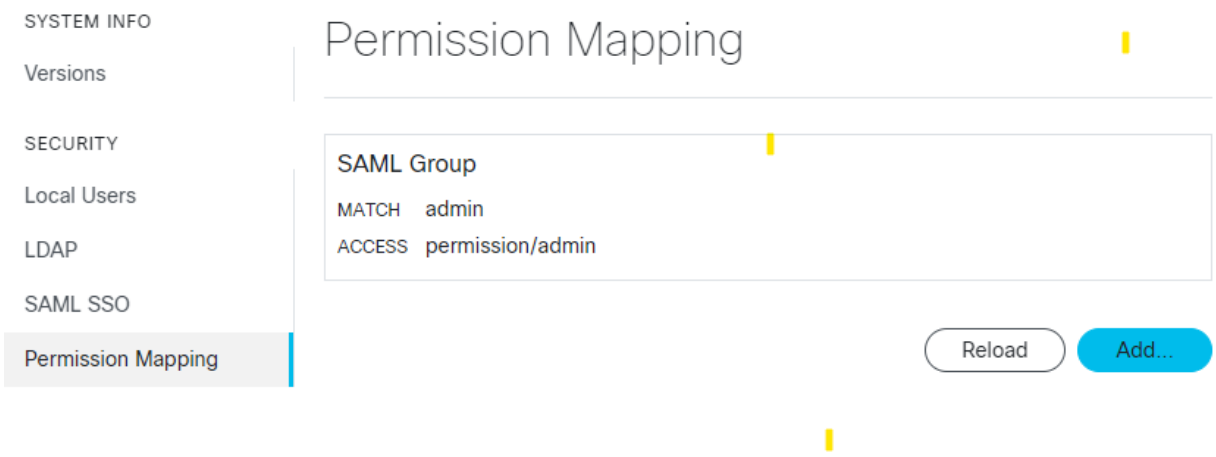
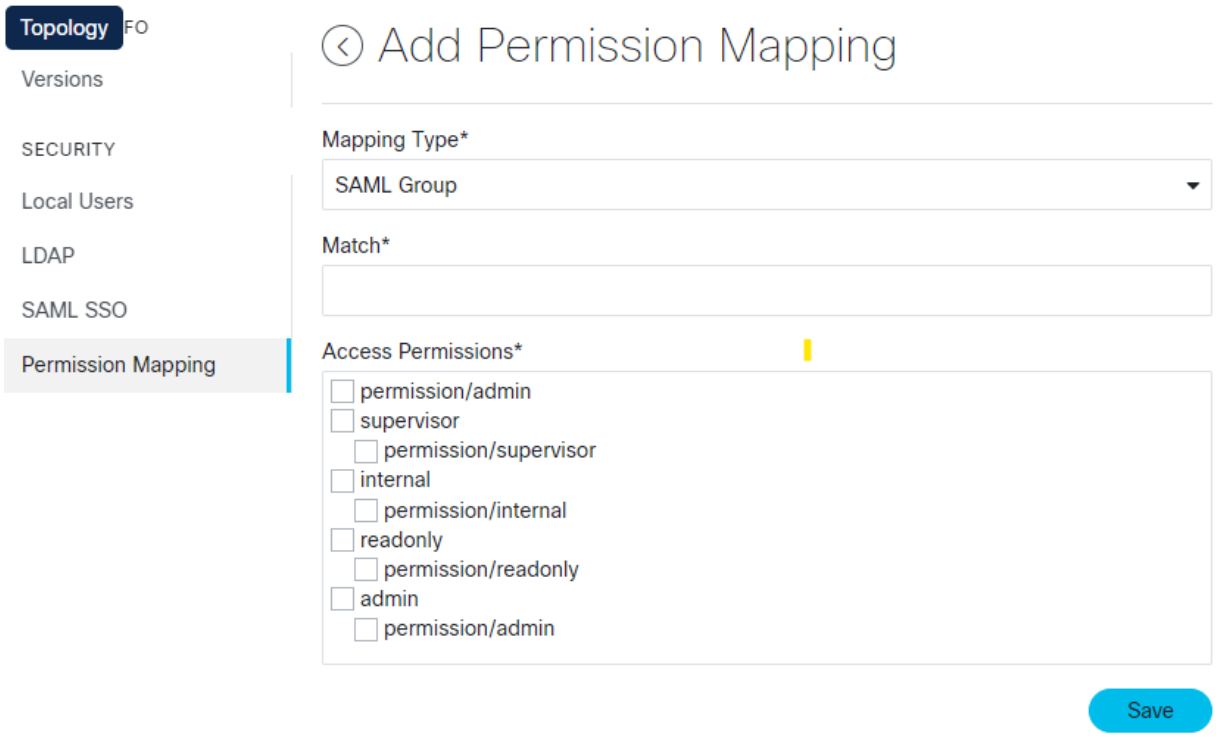


Figure 9: Add Permission Mapping



The set up permission mapping task is complete.

Manage certificates in Cisco Optical Network Controller

Use this procedure to 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.

Use this procedure to manage certificates in Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

Follow these steps to manage certificates in Cisco Optical Network Controller:

Procedure

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>
```

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

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

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.

4. Upload the prepared certificate chain to the system:

   Example

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

5. Verify the uploaded certificates:

   Example

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

```
144555732895016570685800348441338175498552228260 4 |
| 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 |         |
123259484163739452258161110198693132486685704514 3 |
```

```
sedo security certs delete ec
```

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

The manage certificates in Cisco Optical Network Controller task is complete.

Cisco Optical Network Controller MCP server

This section explains the Cisco Optical Network Controller MCP server, including AI-agent usage, enablement behavior, and hardware requirements. Use it to understand MCP server capabilities before configuration.

Cisco Optical Network Controller MCP server is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Cisco Optical Network Controller MCP server details

The Cisco Optical Network Controller MCP server is a Model Context Protocol (MCP) service that exposes supported Cisco Optical Network Controller APIs as tools for AI agents.

- Cisco Optical Network Controller MCP server is an optional component that requires an additional patch installation. If you want to deploy the MCP server, contact Cisco TAC for guidance and assistance with the installation process.
- AI agents connect to the server by using an MCP client configuration that includes the Cisco Optical Network Controller MCP endpoint and an `Authorization` header with Base64-encoded Cisco Optical Network Controller credentials.
- Installing a Cisco Optical Network Controller service pack disables the MCP Server. Contact Cisco TAC to enabled the MCP server again.

How AI agents use the Cisco Optical Network Controller MCP server

Use the Cisco Optical Network Controller MCP server when you want an MCP-compatible agent to query Cisco Optical Network Controller by calling supported tools instead of directly invoking individual REST APIs.

- The agent discovers the tools that the Cisco Optical Network Controller MCP server publishes and selects the required tool or tools based on the user request.
- The MCP server acts as an integration layer between the AI agent and Cisco Optical Network Controller and returns live data from the target system.
- If the Cisco Optical Network Controller deployment uses a self-signed HTTPS certificate, the MCP client must trust that certificate or use a client-specific workaround before it can connect successfully.

Additional hardware requirements

This table lists the minimum additional hardware requirements to run the Cisco Optical Network Controller MCP server. These CPU requirements are in addition to the vCPU requirements that are listed in the Minimum Hardware Requirements table in the Installation requirements section.

Table 5: MCP server additional hardware requirements

Sizing	CPUs
Extra Small (XS)	16 vCPU baseline + 2 additional vCPU
Small (S)	32 vCPU baseline + 2 additional vCPU
Medium (M)	48 vCPU baseline + 4 additional vCPU

Configure Cisco Optical Network Controller MCP server settings in an AI agent

Use this procedure to configure Cisco Optical Network Controller MCP server settings in an AI agent. The Cisco Optical Network Controller MCP server is a feature that is packaged with this release but disabled by default.

Use this procedure to configure Cisco Optical Network Controller MCP server settings in an AI agent in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

The Cisco Optical Network Controller MCP server is a feature that is packaged with this release but disabled by default. Cisco TAC or CX must enable the server before you start this procedure.

Before you begin

Before you begin, verify that you have these items:

- Access to a Cisco Optical Network Controller deployment where the Cisco Optical Network Controller MCP server is enabled
- A valid Cisco Optical Network Controller username and password
- An AI agent or MCP client that supports HTTP-based MCP server connections

Follow these steps to configure an MCP-compatible AI agent for the Cisco Optical Network Controller MCP server.

Procedure

1. Enable the Cisco Optical Network Controller MCP server.
   a) Contact Cisco TAC to enable the MCP server.

   > **Warning**
   >
   > Installing a Cisco Optical Network Controller service pack disables the MCP Server. Contact Cisco TAC to enabled the MCP server again.

   b) Reboot the VM.

   The Cisco Optical Network Controller MCP server is enabled and ready for client configuration.
2. Run this command in the operating system terminal to generate the Base64-encoded credentials for the *Authorization* header.

Example

```
printf '%s:%s' "<conc-username>" "<conc-password>" | base64
```

When you add the encoded value to the MCP configuration file, prefix it with `Basic` and a space.

Example

If your output is

aW50ZXJuXYw6Q2lZZ29ATMIz, your configuration entry should look like this:

```
"Authorization": "Basic aW50ZXJuXYw6Q2lZZ29ATMIz"
```

You have the encoded credential string that the AI agent uses in the MCP server configuration.

3. Open the MCP server configuration for your AI agent.

   The exact location and method depends on the AI agent.

4. Add the Cisco Optical Network Controller MCP server configuration.

   Replace `<conc-hostname-or-ip>` with the Cisco Optical Network Controller host name or IP address that the client can reach.

   Example

```
{
  "servers": {
    "conc-mcp-server": {
      "url": "https://10.0.10.1:8443/onc-mcp-server/mcp",
      "type": "http",
      "headers": {
        "Authorization": "Basic aW50ZXJuXYw6Q2lZZ29ATMIz"
      }
    }
  },
  "inputs": []
}
```

```
{
  "servers": {
    "conc-mcp-server": {
      "url": "https://<conc-hostname-or-ip>:8443/onc-mcp-server/mcp",
      "type": "http",
      "headers": {
        "Authorization": "Basic <base64-encoded-credentials>"
      }
    }
  },
  "inputs": []
}
```

5. CONC MCP server uses a self-signed certificate by default, which some agents may not support, in this case:

   - Use a CA signed certificate by raising a certificate signing request.

     For more details on creating a certificate signing request, see Manage Certificates in Cisco Optical Network Controller.

   - Use an agent that can handle self-signed certificate.

> **Note**
>
> If the deployment uses a CA-signed certificate, you do not need this workaround.

6. Enable **conc-mcp-server** in the AI agent and test the connection.

   Ask a question such as `What tools are available from the MCP server?`.

   The AI agent returns the list of tools that the Cisco Optical Network Controller MCP server publishes.

The AI agent is configured to use the Cisco Optical Network Controller MCP server and can query live Cisco Optical Network Controller data through the published MCP tools.

Cisco Optical Network Controller MCP server tool descriptions

This section lists Cisco Optical Network Controller MCP server tools and describes what each tool returns. Use it to understand which tool supports alarm, service, inventory, node, or network-summary queries.

Cisco Optical Network Controller MCP server tools provide access to specific controller data, such as alarms, services, inventory, node status, and network summary information.

Cisco Optical Network Controller MCP server provides these tools:

Table 6: Cisco Optical Network Controller MCP server tool descriptions

Tool name	Description
`get_conc_agent_guide`	Returns the Cisco Optical Network Controller MCP server agent instruction guide and tool-usage guidance. This is also available as resource for agents that support it.
`get_ns_timestamp_with_current_date`	Returns nanosecond timestamps and dates for a relative or custom time range.
`get_chassis_utilization`	Analyzes rack, shelf, and chassis utilization data across the network.
`get_conc_version`	Returns the current Cisco Optical Network Controller software version.
`get_top_n_issues`	Returns the top network issues or alarms, with optional service impact information.
`get_nodes_status`	Returns the current status of nodes in the network.
`analyze_alarms`	Analyzes one or more alarms and provides occurrence statistics and resolution guidance.
`get_network_summary`	Returns a summary dashboard of overall network status metrics.
`get_top_n_history_of_alarms`	Returns the top historical alarms for a selected time period.
`get_conc_services_mini_data`	Returns minimal service or circuit details for the network.

Tool name	Description
`get_services_by_site`	Returns the services for a specific site or node.
`get_services_by_ppm_and_card`	Returns the services that pass through a specific PPM or card.
`get_historical_flapping_alarms`	Returns historical flapping or fluctuating alarms.
`get_services_affected_count_by_top_alarms`	Returns the count of services that are affected by the top alarms.
`get_services_affected_details_by_top_alarms`	Returns detailed information about services that are affected by the top alarms.
`get_current_alarm_details`	Returns current alarm details with field selection and severity filtering.
`get_historical_alarm_details`	Returns historical alarm details and trends for a selected time range.
`get_services_data_details`	Returns detailed information about network services or circuits.
`quick_search`	Performs a unified search across network inventory tables.
`get_nodes_data`	Returns detailed node or site inventory data from the node inventory API.

Part I

Cisco Optical Network Controller Applications

Topics:

- Topology
- Nodes
- Alien Import
- Inventory
- Service Manager
- Alarms
- Workspaces
- Service Assurance
- Software Image Management and Upgrade
- PM History
- Logs
- Monitoring
- Links
- Alarm Troubleshooting and Categories

Summarizes Cisco Optical Network Controller applications, including topology, nodes, service management, alarms, logs, links, probe monitoring, and workflow-specific operational information.

This table lists the Cisco Optical Network Controller applications and the operational information they provide.

Table 7: Cisco Optical Network Controller applications

Application chapter	Description
Topology	Provides topology visualization, topology details, and topology troubleshooting information.
Nodes	Provides node restrictions, node onboarding, node updates, and node troubleshooting information.
Alien Import	Provides tasks for importing and exporting alien device data.
Inventory	Provides information about viewing network inventory and related operational details.
Service Manager	Provides information about CPCE services, GMPLS services, and service troubleshooting.
Alarms	Provides information about alarm management, event views, SNMP traps, and alarm email forwarding.
Workspaces	Provides information about launching workspaces and reviewing workspace-based service views.
Service Assurance	Provides information about service paths, PSM circuits, and unmanaged equipment.
Software Image Management and Upgrade	Provides information about SFTP, node backups, database backups, and software upgrades.
PM History	Provides information about PM reports, mail server configuration, and connectivity security options.
Logs	Provides information about audit logs, debug logs, tech dump logs, and syslog forwarding.
Monitoring	Provides information about log monitoring and general troubleshooting.
Links	Provides information about the Links application, SLTE links, and ASE services.

2 Topology

Topics:

- Cisco Optical Network Controller topology
- Use common controls in Cisco Optical Network Controller applications

Explains Cisco Optical Network Controller topology, including topology visualization, topology details, OTN and OTS views, topology troubleshooting, and related network views.

Cisco Optical Network Controller topology

This section explains Cisco Optical Network Controller topology, including topology views, node options, alarm severity indicators, OTS links, and OTN span utilization. Use it to interpret topology information.

Cisco Optical Network Controller topology is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Cisco Optical Network Controller topology details

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

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

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

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

Layer segment buttons

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

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

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

Map control icons

Last time refreshed

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

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

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

Configurations icon: This icon provides these toggle switches.

- **Mute Acknowledged Alarms**: Enable to mute the alarms.

- **Display Degree Descriptions**: Enable to display the first character of the degree description configured in COSM for every node degree. If the description is missing, the degree number will be shown. When you hover over the node, a pop up displays the full description of the degree. To add a degree description:
- Right-click the required node and select **View in Nodal UI** to cross-launch COSM.

  COSM opens.
- Select **Optical Setup** > **Optical Configurations** > **Optical Degrees**
- Click **Edit**, change description and click **Apply**.

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

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

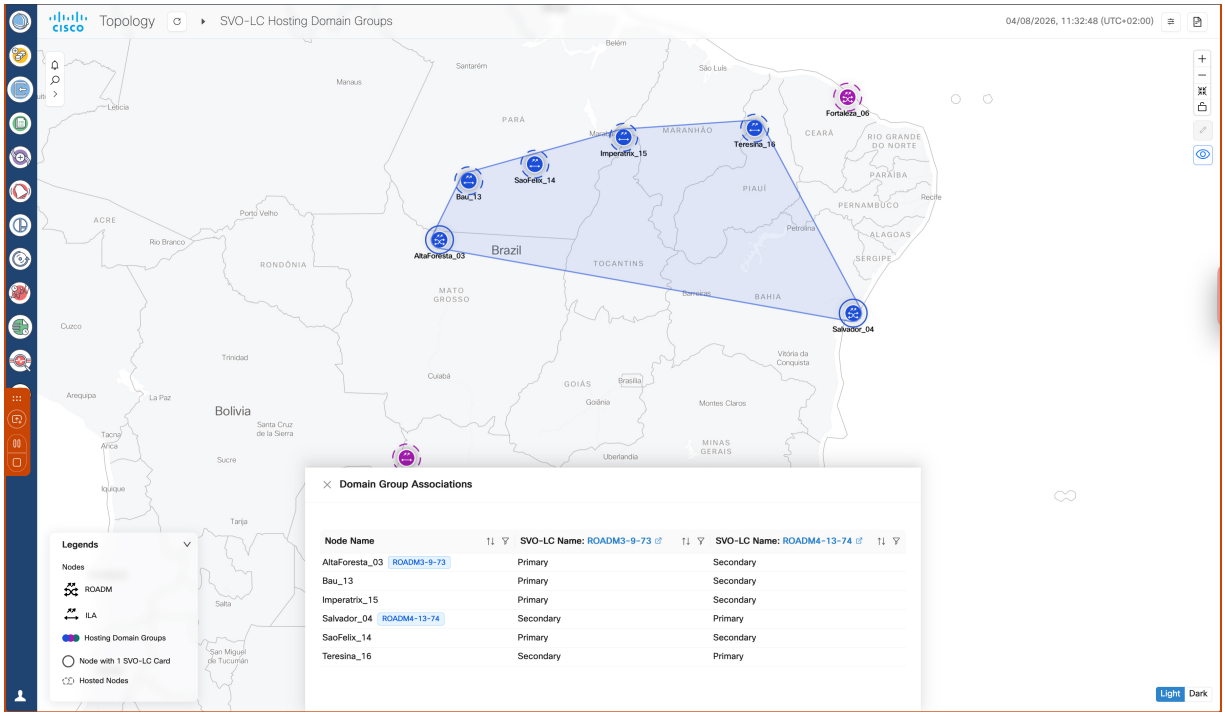
Documentation icon: Opens the Cisco Optical Network Controller configuration guide.

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

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

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

  Figure 10: Domain Group Associations



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

Alarm severity bar

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

Table 8: Alarm Severity

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

Note

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

Note

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

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

Individual node pop-up options

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

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

   The pop-up options appear.

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

Table 9: Topology Node Options

Options	Description
Resync	Resync starts the resync of the selected node.
View in Node UI	This option takes you to the COSM site from where you can view the node details.

Options	Description
View Alarms	This option opens the **Alarms** application in a new tab, from where you can view all the alarms details.

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

Figure 11: OTS view in Topology screen

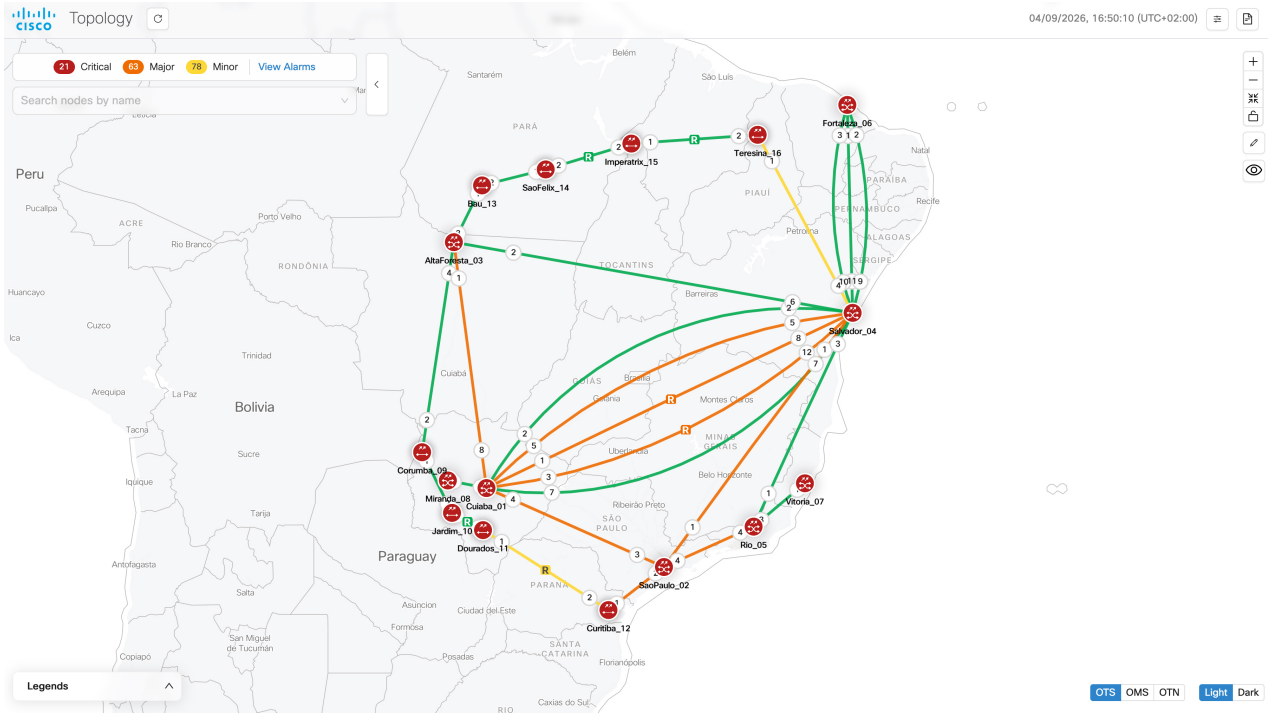
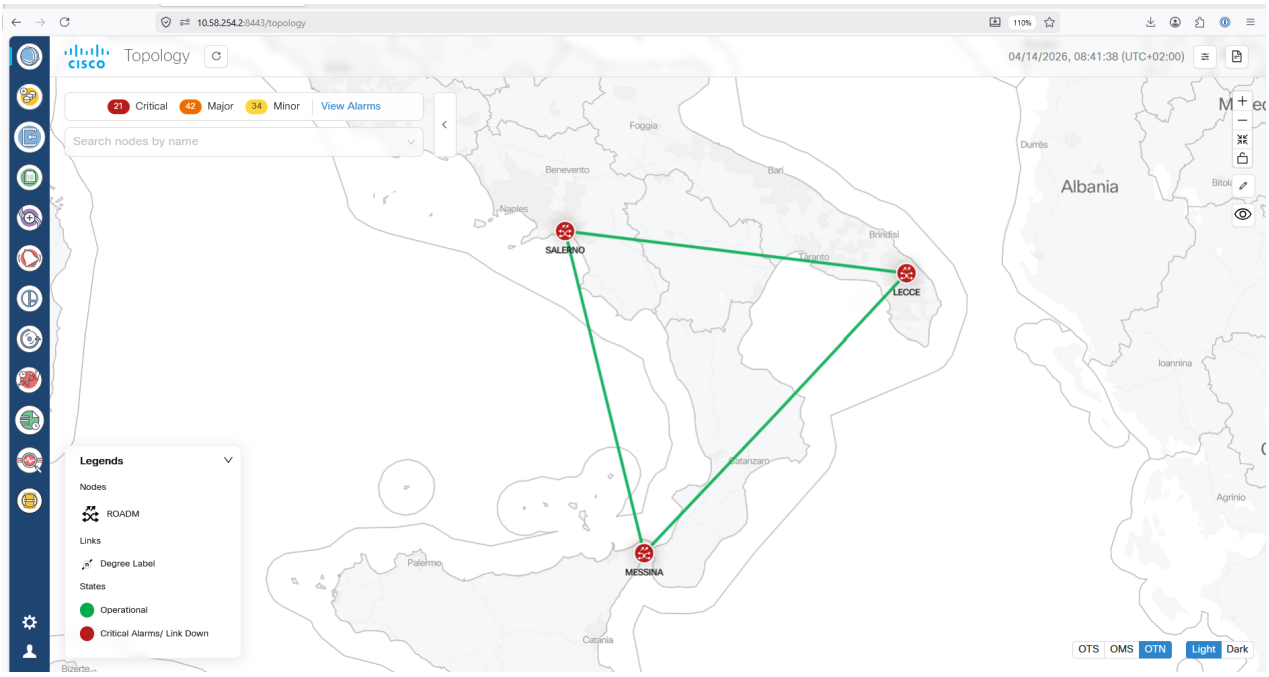


Figure 12: OTN view in Topology screen



Note

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

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

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

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

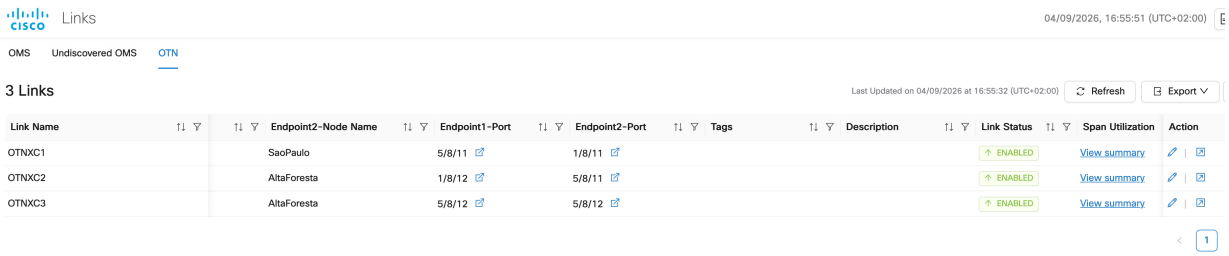
- **Fiber Type**: The type of fiber link.

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

Check span utilization summary for OTN links

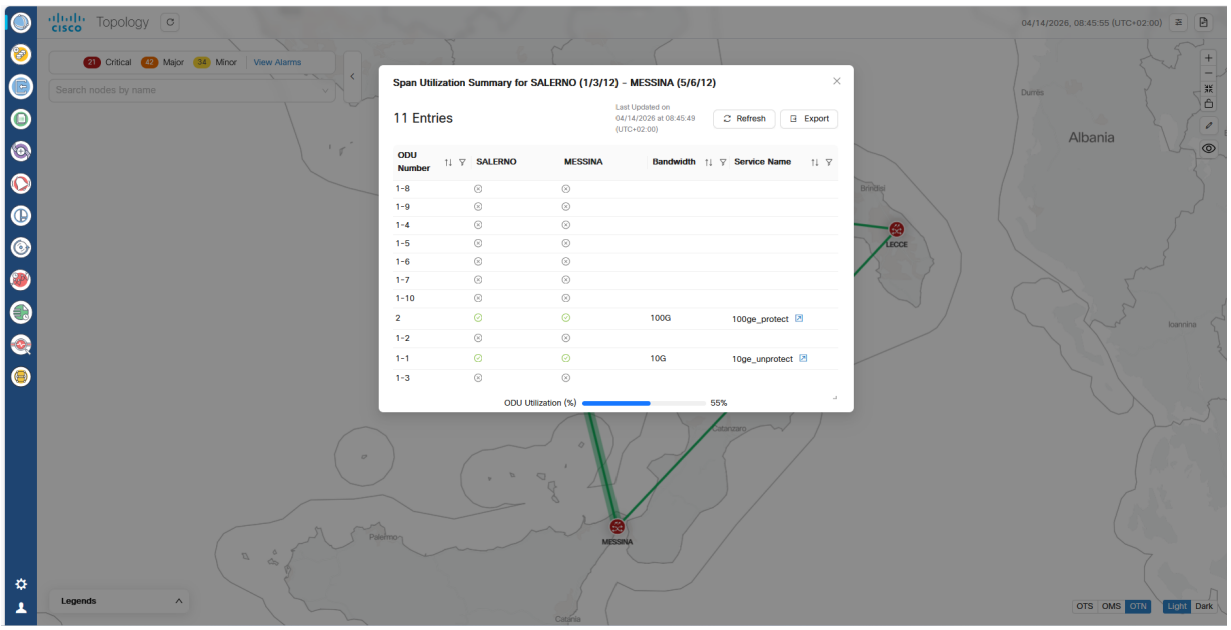
1. In the left panel, click the **Links** app.
2. Go to the **OTN** tab and click the required *OTN link*.

Figure 13: Links app



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

Figure 14: Span utilization summary in Topology screen



In this summary, these parameters appear:

Note

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

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

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

Note

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

Figure 15: Topology Live PM

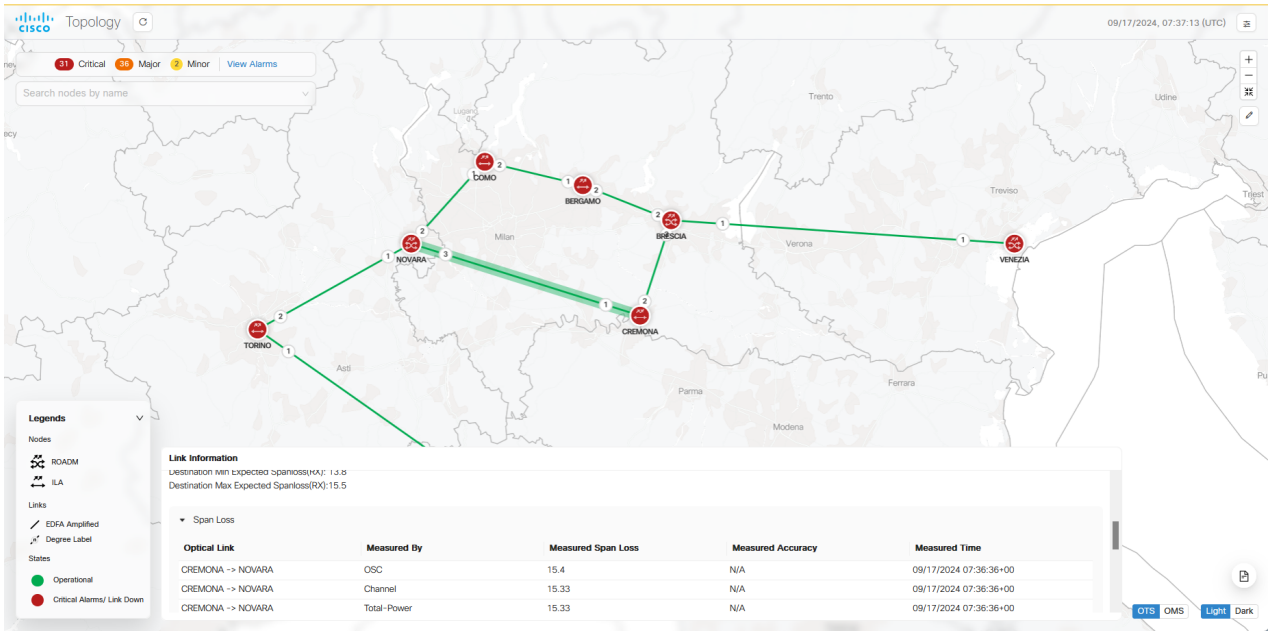
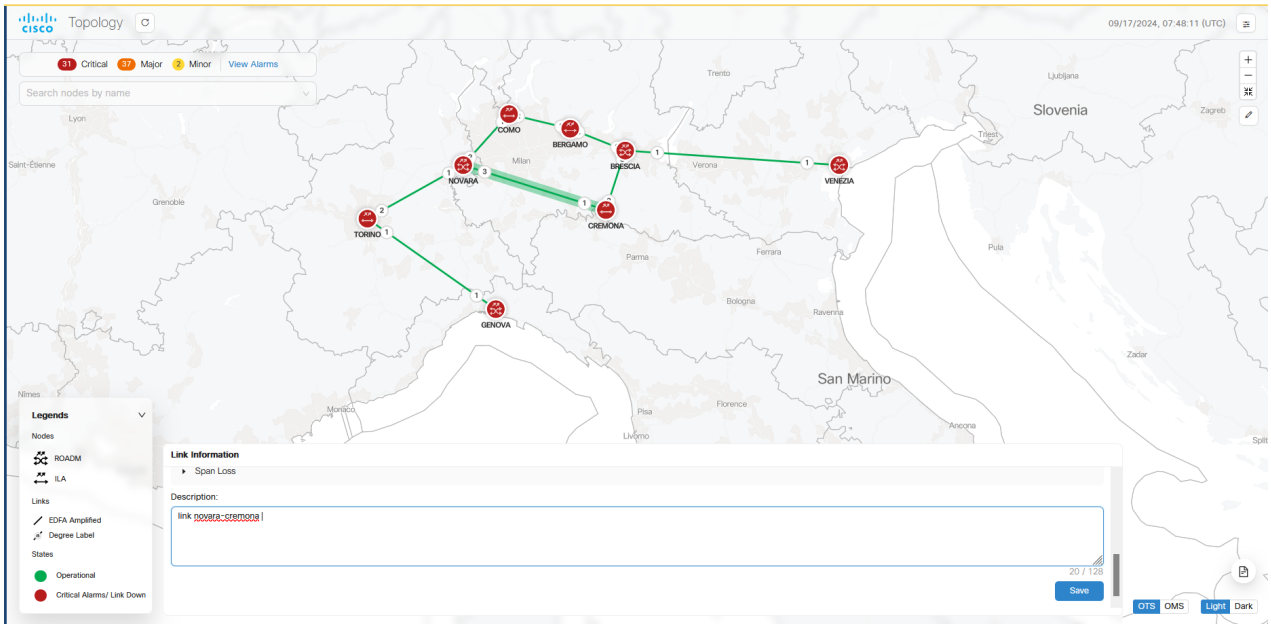


Figure 16: Tool Tip



Topology troubleshooting information

This section provides topology troubleshooting information, including reload prompts after node changes or geographic location updates. Use it to identify when the topology view needs refresh.

Use this reference to understand topology troubleshooting information.

Topology troubleshooting information includes:

- 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.

Use common controls in Cisco Optical Network Controller applications

Use this procedure to view timestamps, refresh data, manage table columns, resize columns, export table data, and sort or filter content in Cisco Optical Network Controller applications.

Use common controls in Cisco Optical Network Controller applications to manage table views, refresh data, export data, and sort or filter content.

Cisco Optical Network Controller applications share common controls for timestamps, refresh actions, column preferences, table export, sorting, and filtering. Use these controls to manage application views consistently across the web UI.

> **Note**
>
> Timezone configuration is supported from Release 25.1.2. Cisco Optical Network Controller web UI 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.

Before you begin

Log in to Cisco Optical Network Controller.

Follow these steps to use common controls in Cisco Optical Network Controller applications:

Procedure

1. View the timestamp.

   The timestamp appears in the header area of application screens. The current date appears with the time.

2. Click **Refresh** to refresh table content or topology status in an application screen.
3. Click the **Column Preferences** icon to display, hide, or reorder columns on an application page.
   a) Select or deselect the corresponding check box to display or hide a column from the table view.
   b) Use the drag handle next to the column name to move the column to a new position in the table.
   c) Click **Reset** to revert the view to its default settings.

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

4. Resize the columns.
   a) Hover over the boundary line between two column headers until the resize cursor appears.
   b) Click and drag left or right to adjust the column width as needed.
5. Export the current table.
   a) Click **Export** to export the details of any table from any application screen to a spreadsheet file.
   b) Choose a 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 columns in the table, not only the fields selected from the **Show or hide columns** drop-down list.

6. Export all data relevant to the current application.
   a) Click **Export** to export the details of any table from any application screen to a spreadsheet file.
   b) Choose **All items**.

> **Note**
>
> This label changes based on the app you are using. For example, All Nodes in the Nodes app, All Services in Service Manager, and so on.

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

7. Use the **Sort** option to sort the table values.
8. Use the **Filter** option to filter table content in each application screen.

You can use common application controls to manage table views, refresh content, export data, and sort or filter content in Cisco Optical Network Controller applications.

3 Nodes

Topics:

- Cisco Optical Network Controller nodes

Covers nodes in Cisco Optical Network Controller, including node restrictions, node onboarding, node updates, node deletion, connectivity testing, and node troubleshooting.

Cisco Optical Network Controller nodes

This section explains Cisco Optical Network Controller nodes, including node types, node details, geographic location values, and node state behavior. Use it to understand node information before onboarding or managing nodes.

Cisco Optical Network Controller nodes is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Cisco Optical Network Controller nodes details

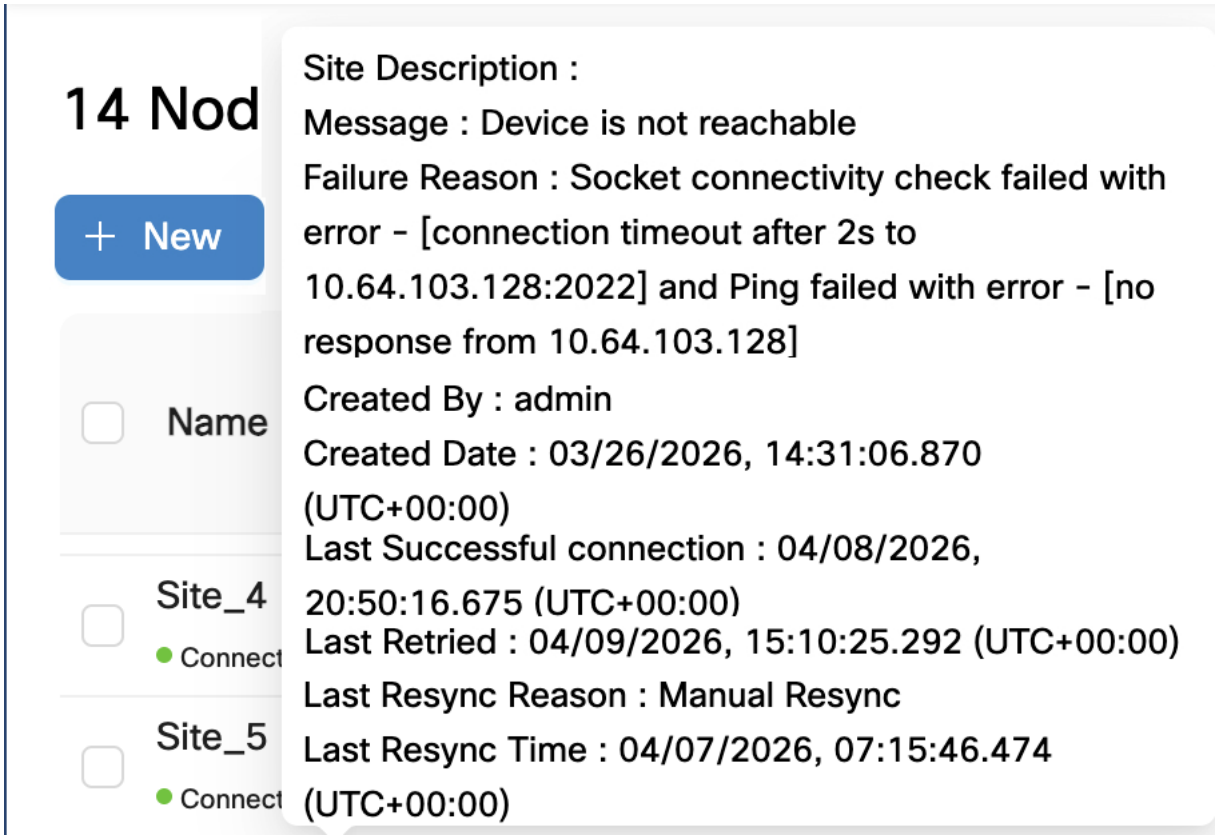
A node refers to a device in the network. You can add a single node or a set of nodes in the form of a batch at any given point in time.

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

- **Node Name**: The name of the node. The node name provided by you must match the original node name used in Cisco Optical Site Manager. In case of any mismatch or discrepancy issues, user given name is configured on Cisco Optical Site Manager.
- **Product Type**: The type of product the node belongs to. For example: Cisco Optical Site Manager.
- **IP: Port (NETCONF)**: The IP address of each node along with the port number.
- **Site Name**: The location of the site that each node belongs to. For example: ROADM_Site_Bengaluru_33
- **Geo Location**: The Geo location of each node in terms of the latitude and longitude values based on where exactly the node is situated in the world at any given time.
- **Status**: The status of each node within the network to know whether it is active or disconnected.
- **Number of Hosting Servers**: Define the number of SVO Line Cards present in the COSM NCS 2000 node.
- **Primary Hosting Server**: Displays the active SVO line card hyperlink. Click the hyperlink to open the COSM admin plane for the hosting server.
- **Secondary Hosting Server**: Displays the standby SVO line card hyperlink. Click the hyperlink to open the COSM admin plane for the hosting server.
- **Up Time**: Displays the duration the Cisco Optical Site Manager node is active.
- **Host Sync Error**: Displays the sync error details.

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

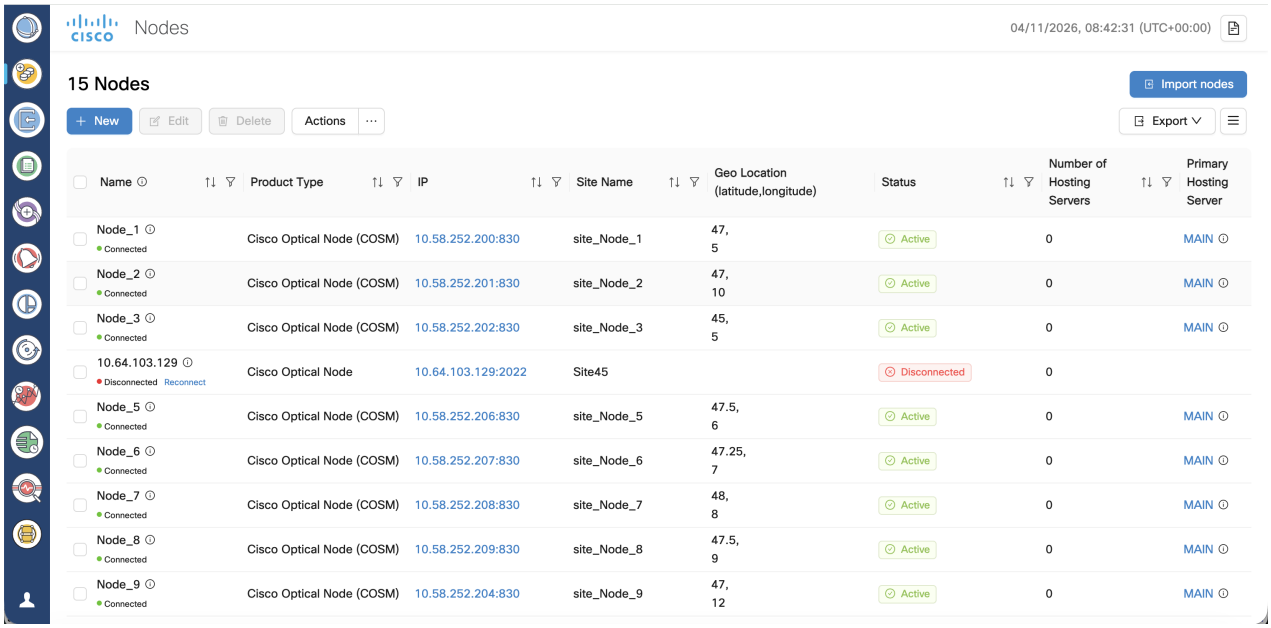
Figure 17: Additional details of a node



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

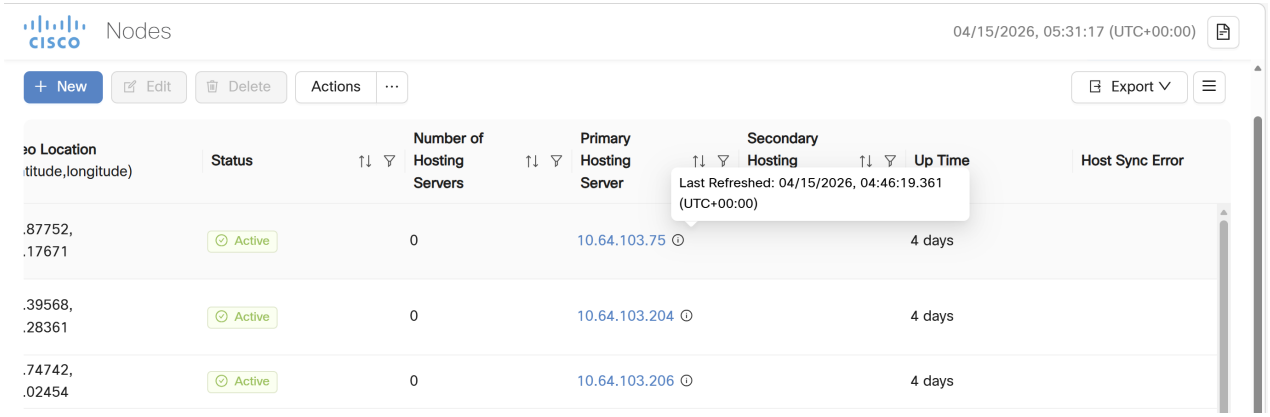
  Here are example values for the field:
- *Socket connectivity check failed with error - [dial tcp 10.20.30.40:2020: connect: connection refused] but Ping succeeded*
- *Socket connectivity check failed with error - [connection timeout after 2s to 10.20.30.40:22] and Ping failed with error - [no response from 10.20.30.40]*
- *Socket connectivity check failed with error - [dial tcp 10.20.30.40:22: connect: no route to host] but Ping succeeded*
- **Created by**: Displays the user id that added the node.
- **Created Date**: Shows the date and time when the node was added.
- **Modified Date**: Shows the date and time when the node details were last updated.
- **Last Successful connection**: Shows the date and time when the node last connected successfully.
- **Last Retried**: Shows the date and time when the last connection attempt was made for this node. This field is only visible when a node is in *Waiting_for_connection* state.
- **Last Resync Reason**: Shows the reason for the most recent resync of the node.
- **Last Resync Time**: Shows the date and time when the most recent resync of the node occurred.

Figure 18: Nodes



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

Figure 19: Last Refreshed information



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

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

- **ReSync**: Used for resyncing any selected node in the network.
- **ReSync All**: Used for resyncing all the nodes in the network.
- **Reconnect**: Used to reconnect any or all the nodes.
- **Configure Network Sync**: Used for **Daily Network Full Sync**. Enable or Disable this functionality.
- **Test Connection**: Used for sending pings to the far end node.
- **Resync Host Details**: Used for resyncing NCS 2000 node with SVO line cards.

Note

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

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

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

Reserved internal IP addresses and subnets

This section lists internal IP addresses and subnets that Cisco Optical Network Controller reserves for its internal network. Use it to prevent address overlap when you plan node IP assignments.

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

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

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

- 172.16.0.1/32

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

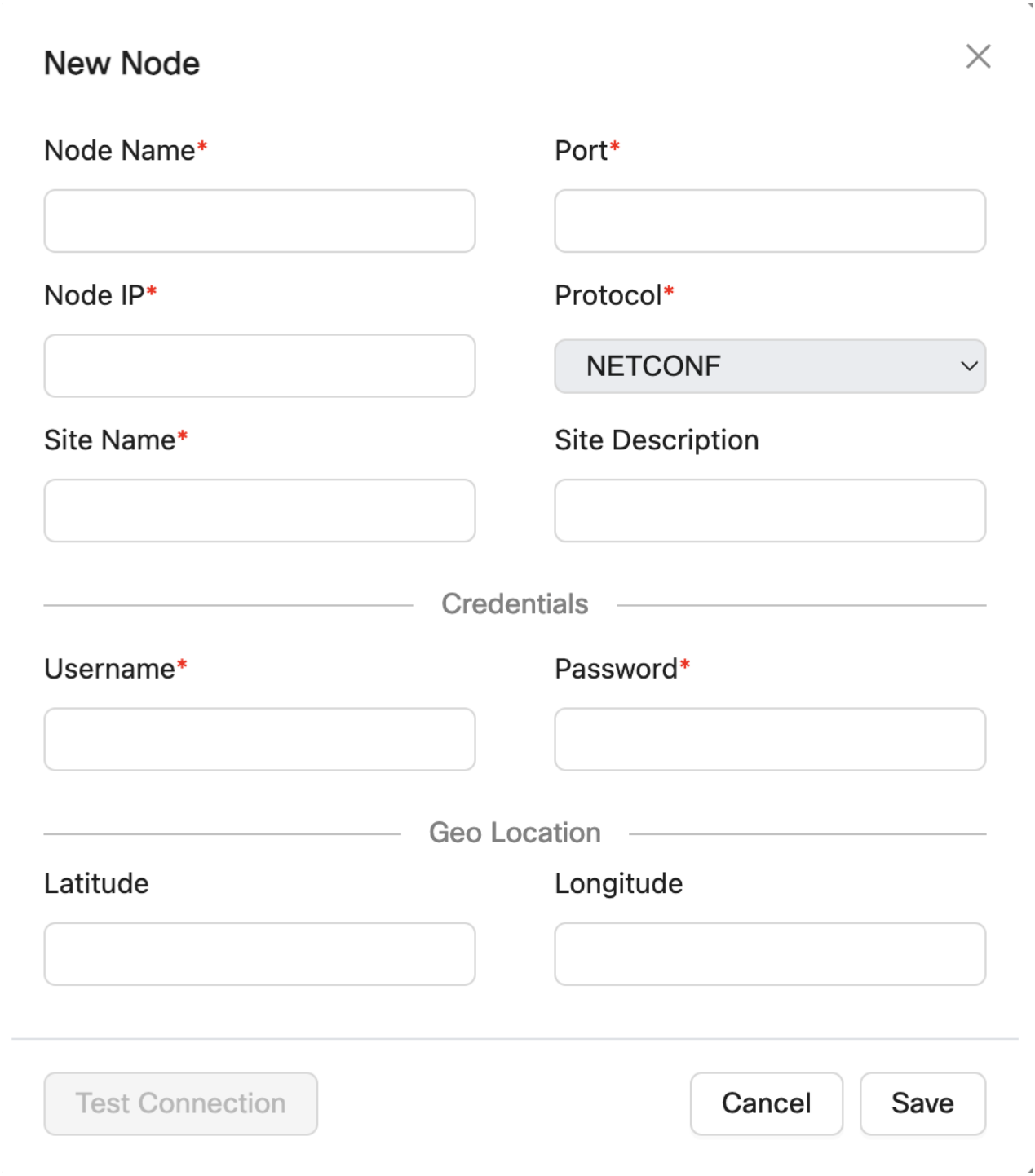
Add nodes on Cisco Optical Network Controller

Use this procedure to add nodes on Cisco Optical Network Controller. The task helps you onboard a single Cisco Optical Site Manager node with the required connection details.

Use this procedure to add nodes on Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Figure 20: Add New Node



Before you begin

Verify these before addding to Cisco Optical Network Controller:

- Verify the Cisco Optical Site Manager is reachable from Cisco Optical Network Controller server via DCN.
- NETCONF port is enabled on the Cisco Optical Site Manager. For more details, see Enable NETCONF over SSH.
- The COSM1K (NCS 1000 series) nodes must be added using port number 2022.
- All COSM2K (NCS 2000 series) nodes must be added using port number 830.

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

Follow these steps to add nodes on Cisco Optical Network Controller:

Procedure

1. Click **Nodes** in the left panel.
2. Click **New**.
3. In the **New Node** dialog box, enter the details necessary connect to the node.

   Ensure that you enter valid a username and password of the node to enable Cisco Optical Network Controller to connect to the node. For details about field descriptions, see the Table 10: Add new node field descriptions on page 50 table.

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

4. To test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node, perform these steps:
   a) (Optional) Click **Test Connection** to test the connectivity to the node.

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

      The **Test Connection** dialog opens for the selected node and shows the node name, node IP address, node port, connection status, and test duration..
   b) Click **Try Again** if you want to rerun the connection test.
   c) Click **Ping** if you want to verify node reachability from Cisco Optical Network Controller.

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

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

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

Table 10: Add new node field descriptions

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

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

Import multiple nodes into Cisco Optical Network Controller

Use this procedure to import multiple nodes into Cisco Optical Network Controller. Cisco Optical Network Controller onboards nodes in batches.

Use this procedure to import multiple nodes into Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

Cisco Optical Network Controller onboards nodes in batches:

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

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

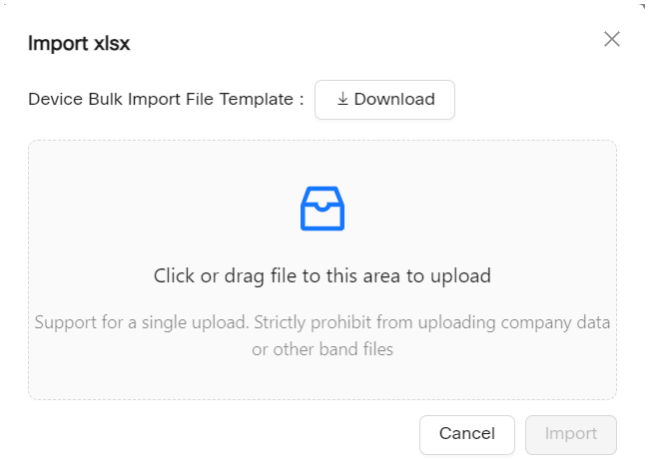
Before you begin

Follow these steps to import multiple nodes into Cisco Optical Network Controller:

Procedure

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

Figure 21: Import nodes



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

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

Table 11: Bulk Import File Template

Name	Description
Node Name	Name of the node Cisco Optical Site Manager node. **Note** This name replaces the already configured Cisco Optical Site Manager node name.
Node IP	The IP address of the node you are adding. **Note** Ensure that this IP does not overlap the Reserved internal IP addresses and subnets.
User Name	The username for accessing the new node. **Note** Use an administrator account to add and manage a Cisco Optical Site Manager node in Cisco Optical Network Controller. This account is required for onboarding and ongoing node operations, including performance monitoring collection, service provisioning and deletion, database backup and restore, and software download and activation. Other Cisco Optical Site Manager user roles are not supported for these operations.
Password	The password for accessing the new node.
Connectivity Type	The type of the protocol used for connecting the node. Default: NETCONF
Connectivity Port	The port number of the node. Port number 2022 for NCS 1000 series nodes. Port number 830 for NCS 2000 series nodes.
Site Name	The name of the site to which the new node belongs.
Site Description	The description of the site to which the new node belongs.

Name	Description
Product Type	Set it as *Cisco Optical Node*.
Latitude	Specify the latitude co-ordinate value you want to assign to the new node to set its location on the map.
Longitude	Specify the longitude co-ordinate value you want to assign for the new node to set its location on the map.

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

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

Export nodes on Cisco Optical Network Controller

Use this procedure to export nodes from Cisco Optical Network Controller. The task helps you download node data for review, backup, or offline updates.

Use this procedure to export nodes on Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

Use this task when you need to export nodes on Cisco Optical Network Controller.

Before you begin

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

Follow these steps to export nodes on Cisco Optical Network Controller:

Procedure

---

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

The export nodes on Cisco Optical Network Controller task is complete.

Edit nodes on Cisco Optical Network Controller

Use this procedure to edit nodes on Cisco Optical Network Controller. The task helps you update node properties, connection details, or related settings after onboarding.

Use this procedure to edit nodes on Cisco Optical Network Controller in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

Use this task when you need to edit nodes on Cisco Optical Network Controller.

Before you begin

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

Follow these steps to edit nodes on Cisco Optical Network Controller:

Procedure

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

The edit nodes on Cisco Optical Network Controller task is complete.

Delete nodes on Cisco Optical Network Controller

Use this procedure to delete nodes on Cisco Optical Network Controller. The task helps you remove one or more nodes and review service impact before deletion.

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

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

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

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

This table describes circuit behavior when a node is deleted:

Table 12: Circuit behavior after node deletion

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

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

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

Before you begin

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

Procedure

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

   The selected node is deleted from the table.

   Note

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

   A warning message is displayed.
4. Review the impacted services as described in the warning message.
5. In the **Delete Node** dialog box and click **Delete**.

The selected nodes are deleted from Cisco Optical Network Controller.

Rebuild a Cisco Optical Site Manager container

Use this procedure when maintenance requires you to delete and recreate a container through the Cisco Optical Site Manager admin plane.

The workflow preserves the Cisco Optical Network Controller database and restores management of the Cisco Optical Site Manager node after the container rebuild.

During the rebuild, Cisco Optical Network Controller must not communicate with the Cisco Optical Site Manager node while the container and its NCS 2000 device inventory are being restored. Temporarily disconnecting the node prevents automatic resynchronization before all devices return to the synchronized state.

Before you begin

- The Cisco Optical Site Manager node is onboarded in Cisco Optical Network Controller.
- You have administrator credentials for Cisco Optical Network Controller and the Cisco Optical Site Manager admin plane.

Procedure

1. Create an on-demand backup of the Cisco Optical Network Controller database.

   For more information, see Back up and restore the database.

2. Disconnect the Cisco Optical Site Manager node.
   a) In Cisco Optical Network Controller, click **Nodes**.
   b) Select the Cisco Optical Site Manager node and click **EDIT**.
   c) Temporarily change the node username or password and save the changes.
   d) Wait until the node status changes to **Disconnected**.
3. in Cisco Optical Site Manager admin plane, delete and recreate the container.
   a) Delete the local container
   b) Create a Cisco Optical Site Manager instance
4. Add all NCS 2000 devices to the recreated Cisco Optical Site Manager instance and wait until synchronization completes for every device.
5. In Cisco Optical Network Controller, edit the node and restore its original username and password.
   a) In Cisco Optical Network Controller, click **Nodes**.
   b) Select the Cisco Optical Site Manager node and click **EDIT**.
   c) Restore the original username or password and save the change.

      Cisco Optical Network Controller starts the Cisco Optical Site Manager node resynchronization automatically.

   d) On the **Nodes** page, verify that resynchronization completes, the node status changes to **Active**, and the connection state changes to **Connected**.

Cisco Optical Network Controller resumes management of the rebuilt Cisco Optical Site Manager container.

Node troubleshooting information

This section provides node troubleshooting information, including bulk import failures, node status values, connection states, and de-boarding failures. Use it to identify common node onboarding and deletion issues.

Use this reference to understand node troubleshooting information.

Node troubleshooting information includes:

- 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. 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 Details 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 Active All information has been collected from the device and it is ready for operations. It is recommended to wait for 60 secs once the device is turned to Discovery Completed Active state which ensures the device is ready for accepting requests.
- Nodes connection status Details Connection State Description User Action Connected Cisco ONC has successfully established the session with the COSM device provided user/password information. No action is needed. Disconnected Cisco ONC was unable to establish session with COSM. Attempt re-connect or resync. If the problem still persists contact Cisco TAC. Waiting for connection Cisco ONC is attempting to establish connection with COSM. No action is needed. Resync_needed Cisco ONC has gone out of sync with device and is scheduled for a resync. Either wait for scheduled resync or start the resync manually. Resync Failed Cisco ONC was unable to resync after multiple retries. Attempt Resync. If problem still persists contact Cisco TAC. Discovery Failed Cisco ONC was not able to collect information from the device as it might have timed out or failed. Attempt Resync. If problem still persists contact Cisco TAC. Errored Cisco ONC was not able to collect information from the device even after 3 retries. Attempt Resync. If problem still persists contact Cisco TAC.
- De-boarding of a node fails.
- Ensure no circuit is created involving this node.
- Retry deleting the node after sometime.
- In case the deletion fails even after you have retried it multiple times, contact Cisco TAC for further assistance.

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

Use this procedure to test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node. You can run these diagnostics while you add a node or after the node is onboarded.

Use this procedure to test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

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

Procedure

1. Open the connectivity test for the node.
   - To test connectivity during adding a new node, in the Node Node dialog box, click **Test Connection** after adding the node details.

     For detailed steps, see Add nodes on Cisco Optical Network Controller on page 47.
   - To test connectivity after onboarding, on the **Nodes** page, select the node, click **Actions**, and choose **Test Connection**.

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

2. Click **Try Again** if you want to rerun the connection test.
3. Click **Ping** if you want to verify node reachability from Cisco Optical Network Controller.

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

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

The test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node task is complete.

4 Alien Import

Topics:

- Import and export alien device data

Provides information about alien import in Cisco Optical Network Controller, including alien device data import, template export, and imported device review.

Import and export alien device data

Use this procedure to import and export alien device data. The task helps you download a template, add alien device details, import data, and export existing records.

Use this procedure to import and export alien device data in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

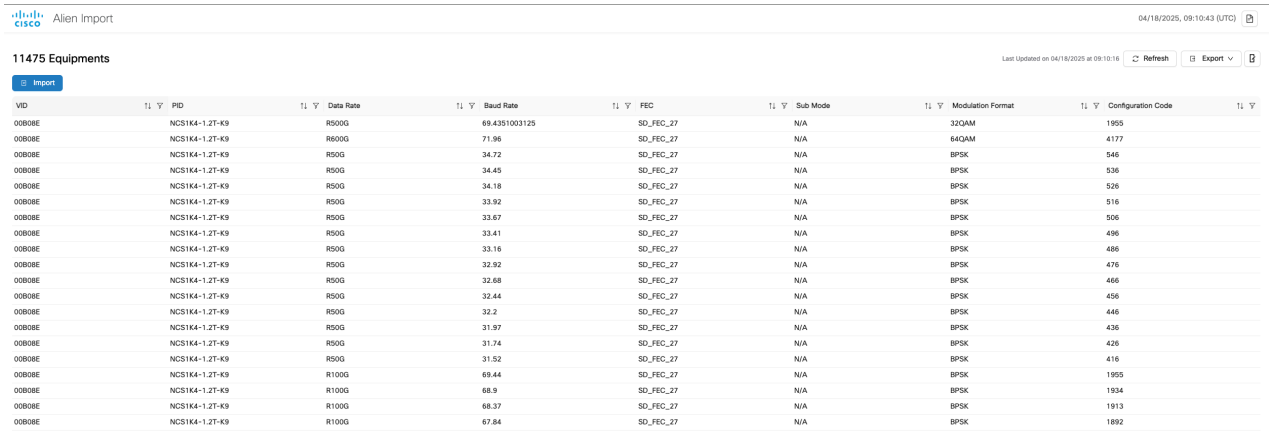
Use this task when you need to import and export alien device data.

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 22: Alien Import



VID	PID	Data Rate	Baud Rate	FEC	Sub Mode	Modulation Format	Configuration Code
00B08E	NCS1K4-1.2T-K9	R500G	69.4351003125	SD_FEC_27	N/A	32QAM	1955
00B08E	NCS1K4-1.2T-K9	R600G	71.96	SD_FEC_27	N/A	64QAM	4177
00B08E	NCS1K4-1.2T-K9	R50G	34.72	SD_FEC_27	N/A	BPSK	546
00B08E	NCS1K4-1.2T-K9	R50G	34.45	SD_FEC_27	N/A	BPSK	536
00B08E	NCS1K4-1.2T-K9	R50G	34.18	SD_FEC_27	N/A	BPSK	526
00B08E	NCS1K4-1.2T-K9	R50G	33.92	SD_FEC_27	N/A	BPSK	516
00B08E	NCS1K4-1.2T-K9	R50G	33.67	SD_FEC_27	N/A	BPSK	506
00B08E	NCS1K4-1.2T-K9	R50G	33.41	SD_FEC_27	N/A	BPSK	496
00B08E	NCS1K4-1.2T-K9	R50G	33.16	SD_FEC_27	N/A	BPSK	486
00B08E	NCS1K4-1.2T-K9	R50G	32.92	SD_FEC_27	N/A	BPSK	476
00B08E	NCS1K4-1.2T-K9	R50G	32.68	SD_FEC_27	N/A	BPSK	466
00B08E	NCS1K4-1.2T-K9	R50G	32.44	SD_FEC_27	N/A	BPSK	456
00B08E	NCS1K4-1.2T-K9	R50G	32.2	SD_FEC_27	N/A	BPSK	446
00B08E	NCS1K4-1.2T-K9	R50G	31.97	SD_FEC_27	N/A	BPSK	436
00B08E	NCS1K4-1.2T-K9	R50G	31.74	SD_FEC_27	N/A	BPSK	426
00B08E	NCS1K4-1.2T-K9	R50G	31.52	SD_FEC_27	N/A	BPSK	416
00B08E	NCS1K4-1.2T-K9	R100G	69.44	SD_FEC_27	N/A	BPSK	1955
00B08E	NCS1K4-1.2T-K9	R100G	68.9	SD_FEC_27	N/A	BPSK	1934
00B08E	NCS1K4-1.2T-K9	R100G	68.37	SD_FEC_27	N/A	BPSK	1913
00B08E	NCS1K4-1.2T-K9	R100G	67.84	SD_FEC_27	N/A	BPSK	1892

Follow these steps to import and export alien device data:

Procedure

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.

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.

3. Click the **Refresh** button to refresh the equipment status.
4. Click on the **Show or hide columns** icon to select any columns to be displayed or hidden from the table view anytime.
5. Use the page numbers and select the number of rows per page as required for the table display.
6. Use the sort or filter options to sort and filter values in the table.

The import and export alien device data task is complete.

5 Inventory

Topics:

- View network inventory

Summarizes inventory in Cisco Optical Network Controller, including network inventory views, node details, shelf data, card data, port details, and operational context.

View network inventory

Use this procedure to view network inventory. The task helps you review discovered racks, shelves, cards, ports, and related inventory details.

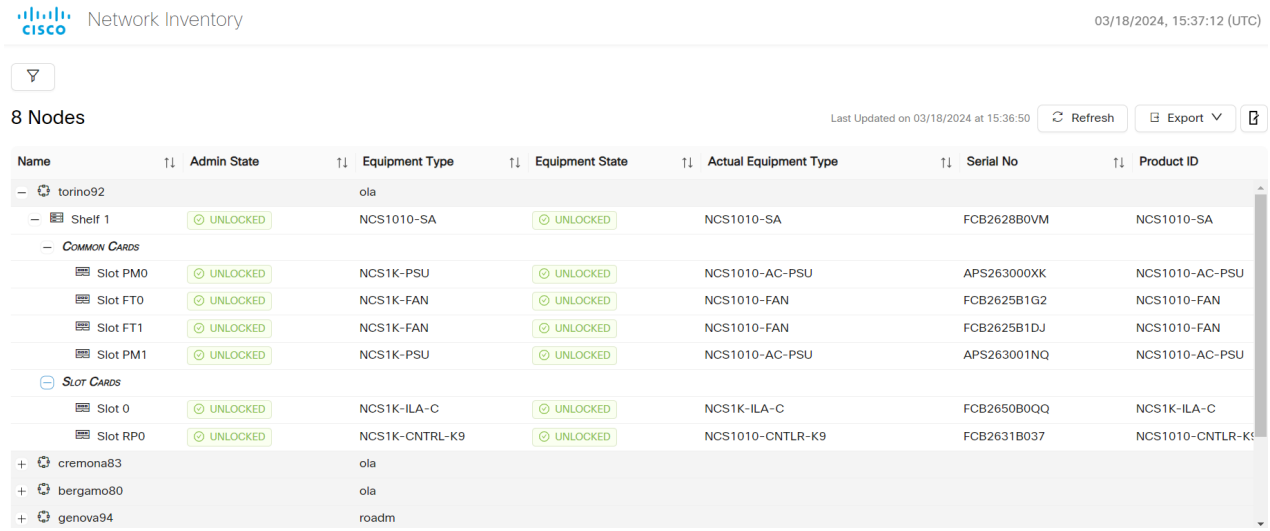
Use this procedure to view network inventory in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

Use this task when you need to view 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 23: Network Inventory



Follow these steps to view network inventory:

Procedure

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.

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.

3. (Optional) To export inventory data into an excel file, click **Export**.
4. Click the **Refresh** button to refresh the inventory status.
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.

The view network inventory task is complete.

6 Service Manager

Topics:

- Service Manager application

Explains Service Manager in Cisco Optical Network Controller, including CPCE services, GMPLS services, service creation, service management, and service troubleshooting.

Service Manager application

This section explains the Service Manager application, including supported circuit types, service creation, and service management options. Use it to understand service workflows before provisioning circuits.

Service manager application is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Service manager application details

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

Supported Circuit Types

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

GMPLS Support

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

Existing CPCE circuits

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

Resync services

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

  Figure 24: Select multiple toggle

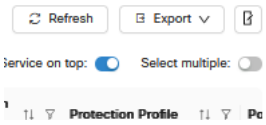
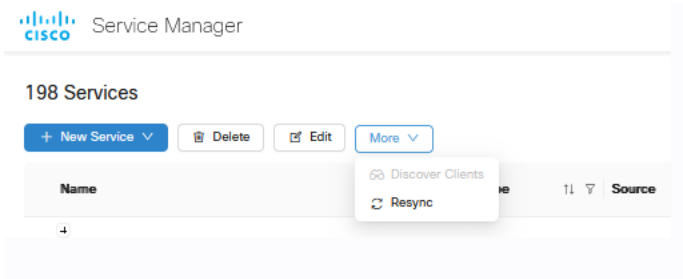


  Figure 25: Resync option for GMPLS circuits

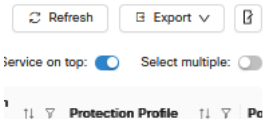


- Resyncing can resolve lifecycle state issues, for example, when the circuit is in PARTIAL, where clients are not discovered properly or are in an ambiguous state.
- When multiple services are selected, the **More** button is replaced with a **Resync** button.
- Resyncing a trail service also resyncs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

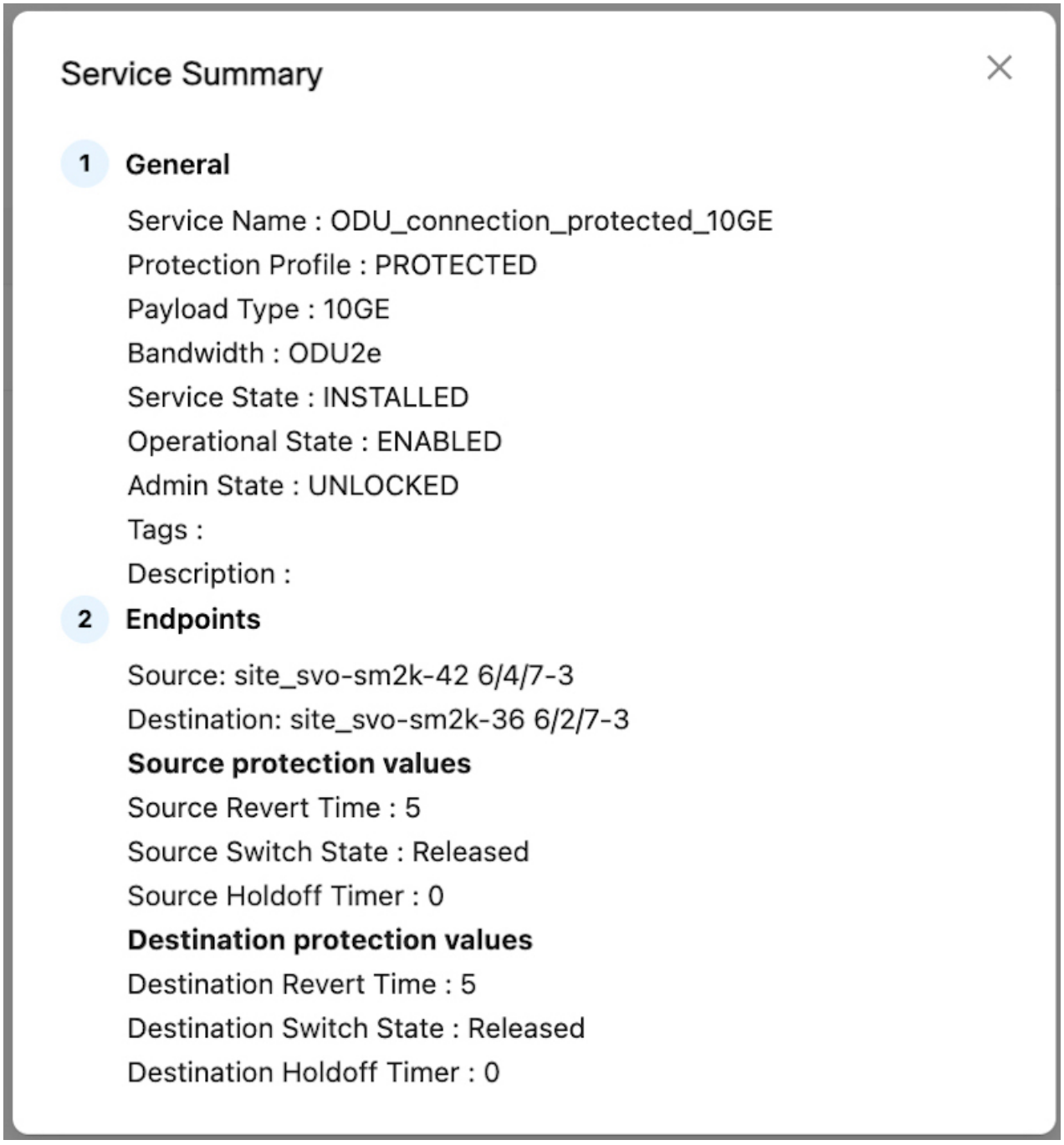
  Figure 26: Service on top and Select multiple toggles



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 27: Service summary in service manager



Service manager table fields
Table 13: Details

Column	Values	Description
Name		Name of the service
Type	OCH-NC	Type of the service
	OCH-Trail	
	OCH-CC	
Source	–	Source Node and Port

Column	Values	Description
Destination	–	Destination Node and Port
Control Plane	GMPLS	Control Plane Protocol
	CPCE	

Column	Values	Description
Lifecycle State	INSTALLED	The circuit is fully provisioned and active in the network.
	PLANNED	The circuit configuration is defined but not yet provisioned on the network.
	PENDING_REMOVAL	The circuit is marked for deletion but the deletion process is not yet complete.
	DELETION_IN_PROGRESS	The circuit deletion process is in progress.
	DELETION_FAILED	The circuit deletion process failed to complete successfully.
	PARTIAL	The circuit is in a partially provisioned state, possibly due to missing or undiscovered components.
	GMPLS_ACTIVE	GMPLS circuit is successfully working, cross corrections are created, and path is available.
	GMPLS_INACTIVE	There is no valid path for creating the circuits due to frequency not available, inconsistent constraints, optical validation failure, etc.
	GMPLS_HANDOVER	The circuit is configured to be upgraded from non-GMPLS to GMPLS or GMPLS to non-GMPLS.
	GMPLS_ACTIVATING	GMPLS circuit activation is in progress
	GMPLS_DEACTIVATING	GMPLS circuit deactivation is in progress.
	GMPLS_FAILED	GMPLS circuit failed (i.e. link down, node down).
	GMPLS_DEGRADED	Circuit trail failed (i.e. PSM working or protected is down or fail).
	GMPLS_RECOVERING	Temporary reboot status at circuit restart.
	GMPLS_REPAIRING	Circuit repair is in progress (i.e. node IP changed)
	GMPLS_RELEASING	A downgrade from GMPLS to non-GMPLS circuit has been requested and the action is running.
	GMPLS_REPAIR_NEEDED	

Column	Values	Description
		An IP address change is done on a node impacting the circuit, so the circuit must be repaired. **Note** Cisco Optical Network Controller does not support circuit repair in release 25.1.1.
	GMPLS_SYNC_IN_PROGRESS	GMPLS controller has acceptedthe configuration, Cisco Optical Network Controller is getting the updated data from the GMPLS controller. When a circuit is discovered in a node that is onboarded to CONC , the Lifecycle state continues in this state until CONC fetches the circuit information from the GMPLS controller.
Operational State	ENABLED	The circuit is active and functioning normally.
	DISABLED	The circuit is inactive and not functioning.
Admin State	UNLOCKED	The circuit is administratively enabled and available for use.
	LOCKED	The circuit is administratively disabled and unavailable for use.
Frequency (THz)		Optical carrier frequency at which the circuit will operate within the DWDM spectrum.
Bandwidth (GHz)		Bandwidth used by the circuit
Protection profile	PROTECTED	OTN service has both active and standby path.
	UNPROTECTED	For OTN service, only active path is present. For PSM circuit, the circuit is configured with PSM OMS protection.
	OCH-PSM	The circuit is configured with PSM wavelength protection to ensure service availability in case of failure.

Column	Values	Description
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.

CPCE service endpoints and operations

Use this reference to provision service endpoints, review supported options, and manage CPCE service lifecycle actions.

Provisioning CPCE services involves creating service endpoints, reviewing the conditions for circuit creation, and managing lifecycle operations such as resynchronizing nodes or updating card modes.

Conditions for Creating OCH-CC Circuits

Consider these conditions when creating OCH-CC circuits.

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

Provisioning requirements

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.

Completion state

The create and manage CPCE services task is complete.

Supported cards and provisioning options

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

Table 14: 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
NCS2K-1.2T-MXP	TXPMXP: 400G Trunk and 100GE, 400GE, and OTU4 clients

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

Table 15: Supported circuit provisioning options for 400G-XP-LC cards

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

CPCE service troubleshooting information

This section provides CPCE service troubleshooting information, including pending-removal scenarios and common Service Manager problems. Use it to identify probable causes and recovery actions.

Use this reference to understand CPCE service troubleshooting information.

CPCE service troubleshooting information includes:

- Some PCE error codes which you might encounter while provisioning the service are given below.
- [PCE-PR00003] - Failed for waves selector: [PCE-EXC00002] - Carrier 1 source wave (XXXXXXXX-XXXXX (XXXX.XX)) and Destination one (XXXXXXXX-XXXXX (XXXX.XX)) differs.
- [PCE-WAL00048] - Requested central frequency XXX,XXX is out of supported range.
- [PCE-WAL00026] - No free spectrum available to allocate MCH with central frequency XXX.XXX.
- [PCE-PR00001] - No routes available.
- [PCE-WAL00026] - No free spectrum available to allocate MCH with central frequency XXX.XXX.x.
- [PCE-PR00026] - Include constraint [Site uuid] not matched.

- [PCE-PR00018] - Optical validation failed: ZONE_RED worse than ZONE_GREEN.
- [PCE-PR00004] - Failed to evaluate optical path: [PCE-OV00016] - [Fiberspan UUID]: Invalid fiberType: [null value].

Table 16: Details

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

CPCE service troubleshooting information details

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

CPCE service troubleshooting information details

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

Create CPCE services

Use this procedure to create CPCE services. The task helps you enter service parameters, choose endpoints, review supported cards, and submit the service request.

Create a CPCE service by selecting endpoints and configuring circuit parameters.

Consider these conditions when creating OCH-CC circuits.

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

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

Before you begin

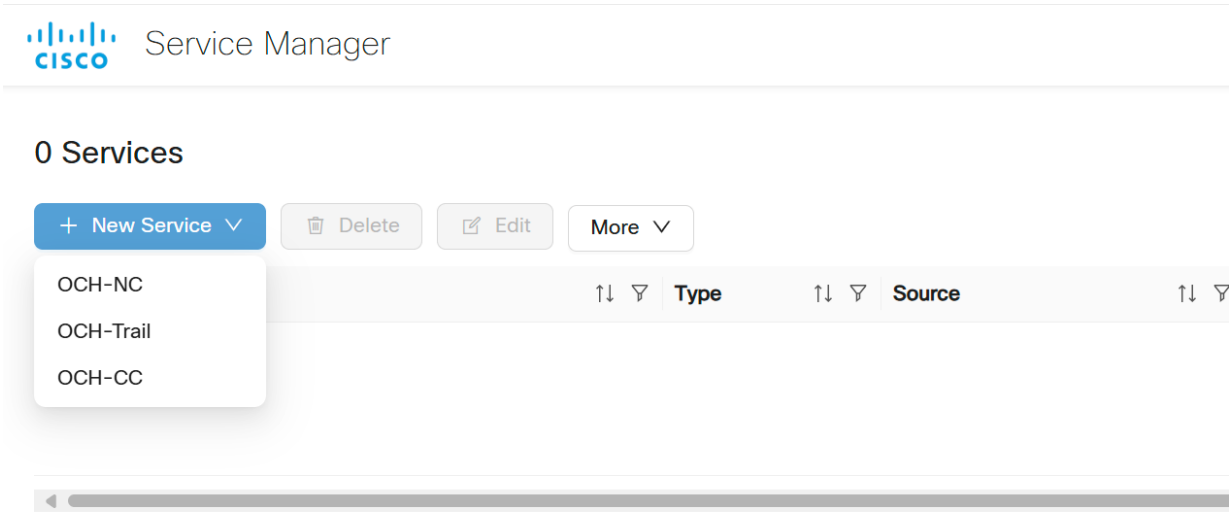
Note

- After changing the card mode for NCS1K4-1.2T-K9, resync the nodes from the Nodes page to ensure that the client ports are correctly displayed.
- If you do not see the ports on your target nodes during endpoint selection, we recommend you perform a resync of the nodes before creating a new service.
- If a new NCS 2000 chassis with a TXP present is added to a node already present in COSM, you must perform a resync of the node to see the endpoints during circuit provisioning.
- Do not configure optical validation for CPCE circuits that use QDD-400G-ZR-S or QDD-400G-ZRP-S interfaces with BRK24 or BRK16 passive filters. Out-of-band Optical Signal-to-Noise Ratio is not defined for these filter combinations, and PCE path computation may fail with the PCE-PR00018 error.

Follow these steps to create and manage CPCE services:

Procedure

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

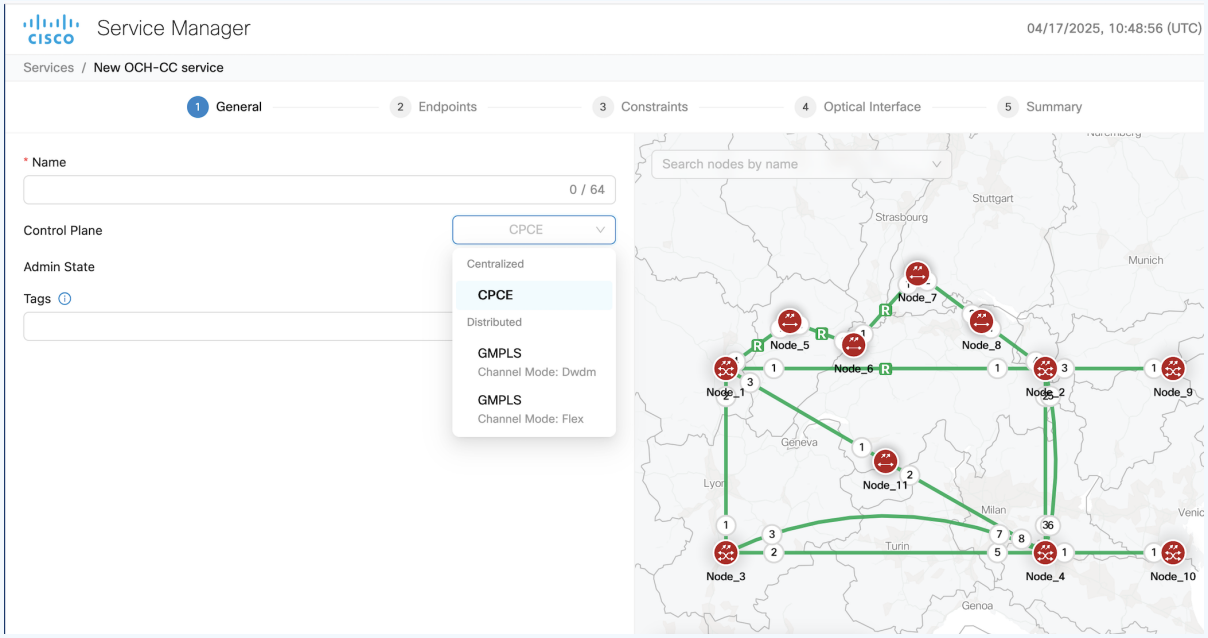


2. Select **OCH-NC**, **OCH-Trail**, or **OCH-CC**.

Note

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

Figure 28: Service Manager



Service Manager launches the new service wizard.

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

Figure 29: Service Manager

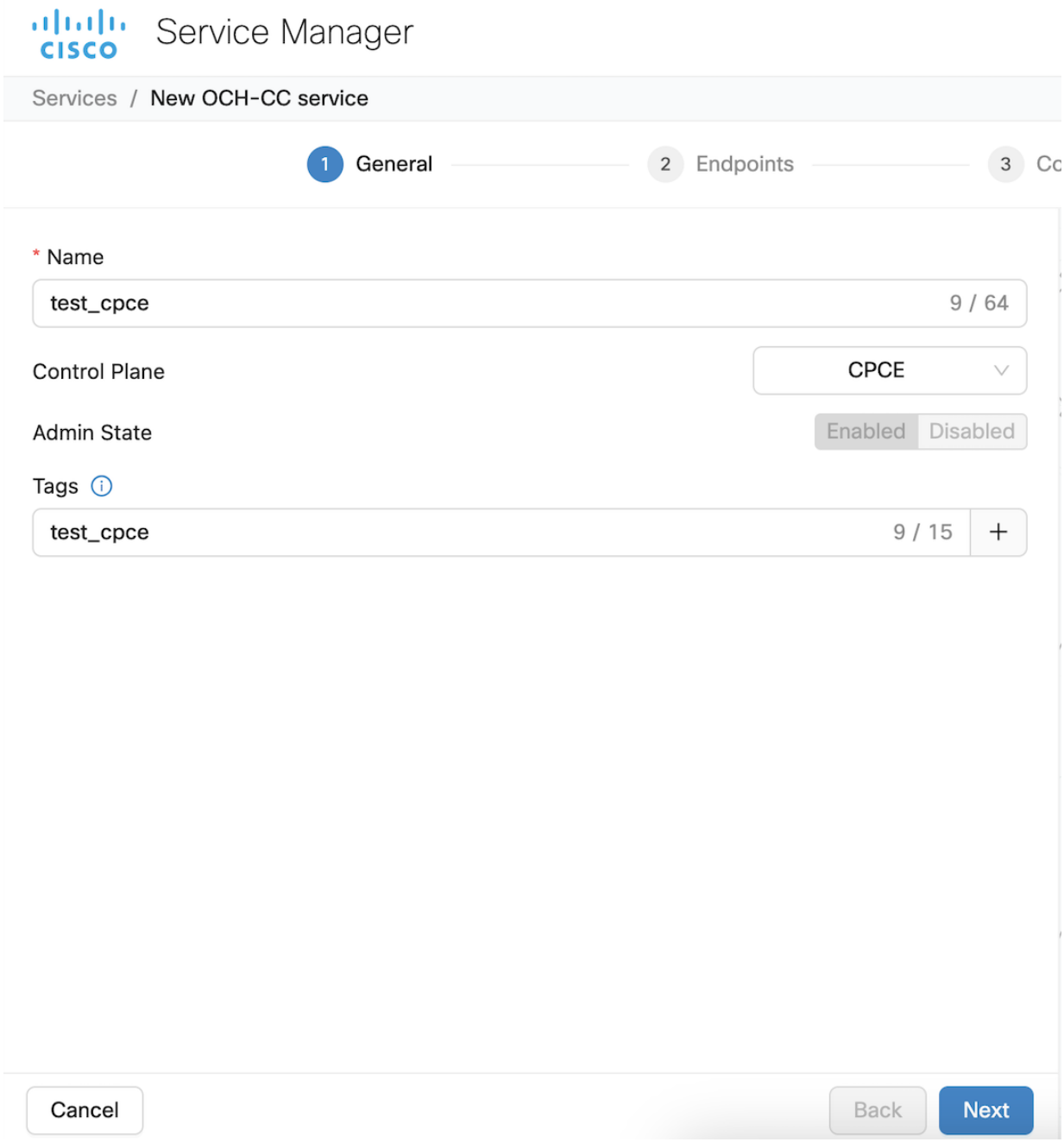


Table 17: General Parameters

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

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

Figure 30: Service Manager

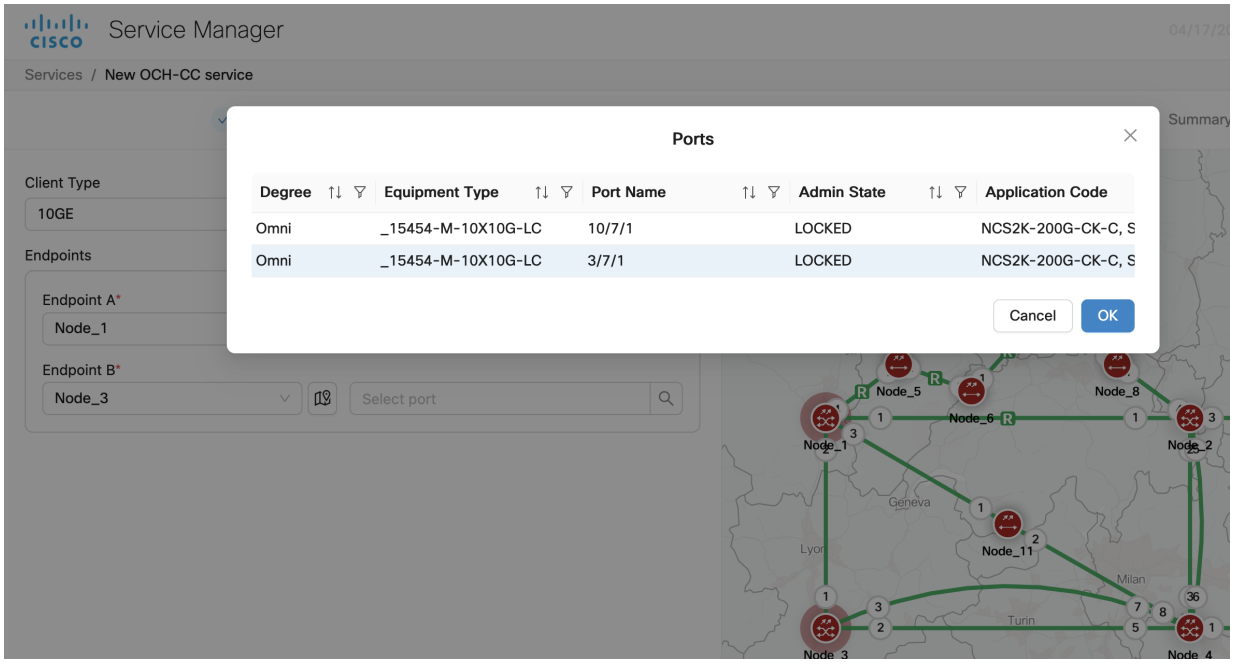


Table 18: Endpoints Parameters

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	–
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.

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

Figure 31: Service Manager

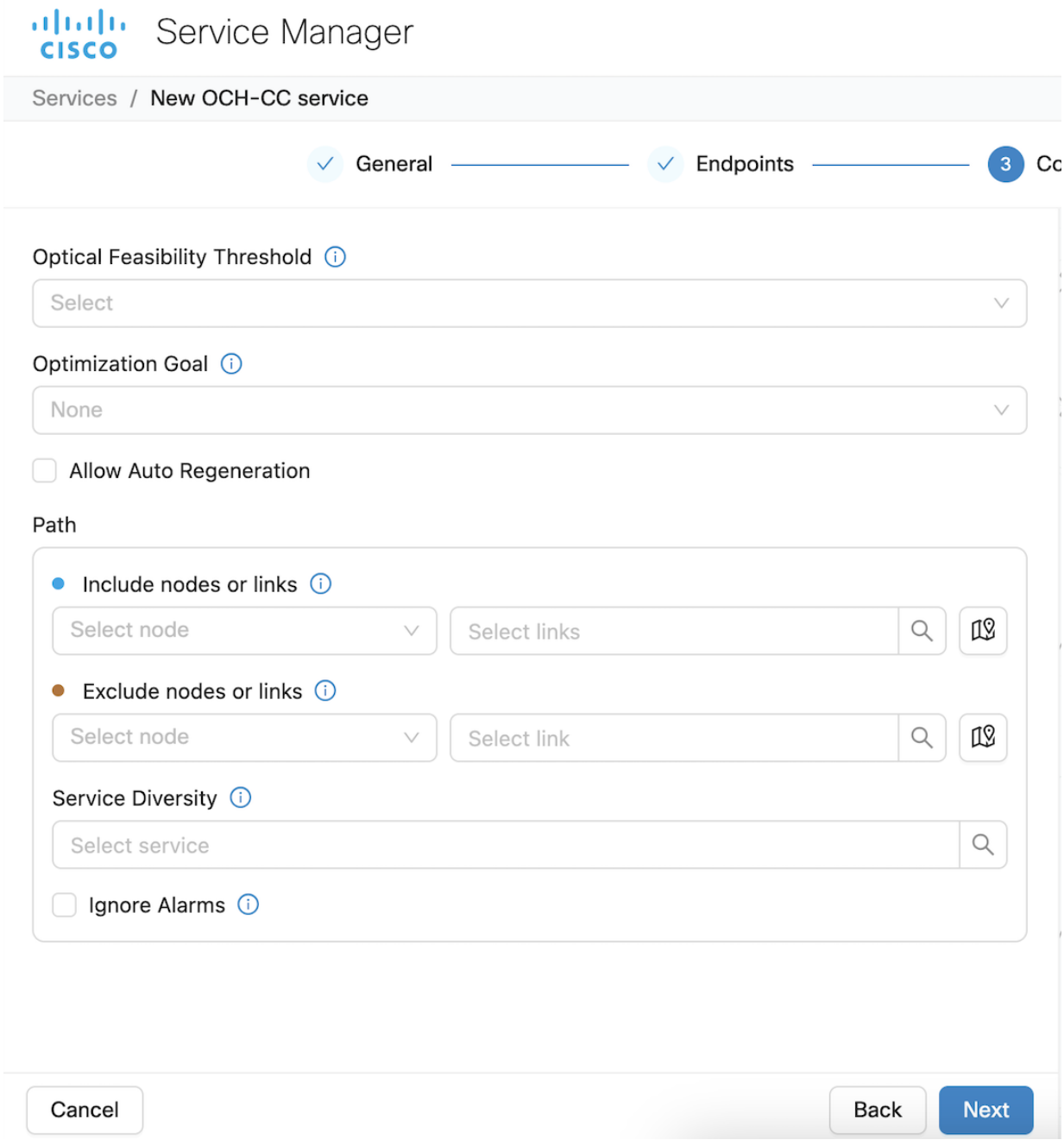


Table 19: Constraint parameters

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

Field	Description	Values/restrictions
Optimization Goal	Defines the mechanism for the control plane to compute optimum path depending on various criteria.	LENGTH (Max): Computation criteria based on minimizing the path LENGTH HOPS(Max): Computation criteria based on minimizing the number of HOPS OSNR(Min): Computation criteria based on maximizing the OSNR
Allow Auto Regeneration	Whether to allow auto regeneration	–
Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	–
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	–
Service Diversity	Select one or more existing services from the dropdownfor the control plane to exclude the resources that the services use during path computation.	–
Ignore Alarms	If true, Service manager ignores any alarms present on the path and continues to provision the service.	–

Note

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

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

Table 20: Optical interface parameters

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

Nyquist Spacing	Select **Yes** to allow channels to share spectral boundaries as long as the center frequency of one channel does not fall within the spectrum of another.
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

This option is only enabled if central frequency is specified.

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.

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

The create and manage CPCE services task is complete.

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

Table 21: Supported transponder cards and modes

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

Card	Modes Supported
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

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

Table 22: Supported circuit provisioning options for 400G-XP-LC cards

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

Manage CPCE services

Use this procedure to manage CPCE services. The task helps you view service details, change service state, and perform supported service actions.

Review existing CPCE services and perform supported lifecycle operations.

Consider these conditions when creating OCH-CC circuits.

- The OCH-Trail must be in installed state before an OCH-CC circuit can be created.
- When the corresponding trail is in planned state, no new OCH-CC circuits can be created.

- The number of OCH-CC circuits that you can have per trail depends on the card mode configuration of the transponder card.
- OCH-CC circuits inherit constraints from the parent trail.
- Creating an OCH-CC circuit creates the associated OCH-Trail circuit automatically.

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

Before you begin

Note

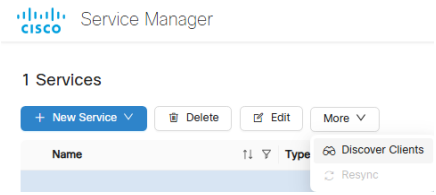
- After changing the card mode for NCS1K4-1.2T-K9, resync the nodes from the Nodes page to ensure that the client ports are correctly displayed.
- If you do not see the ports on your target nodes during endpoint selection, we recommend you perform a resync of the nodes before creating a new service.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

Follow these steps to create and manage CPCE services:

Procedure

1. Select a service and click **Edit** to edit the circuit.
   a) Update the name.
   b) Click **Save**.
2. Select an OCH-Trail circuit and click **More** > **Discover Clients** to discover its OCH-CC circuits.

   Figure 32: Service Manager



Note

Client discovery for an OCH-Trail circuit is supported only when the client ports at both endpoints are in slots with the same slot number. Client discovery is not supported when the client ports use different slot numbers.

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

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

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

4. 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.

The create and manage CPCE services task is complete.

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

Table 23: 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

Card	Modes Supported
NCS2K-200G-CK-C	TXP-100G: 100G trunk and client FEC Modes: HG_FEC_7, SD_FEC_20, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON
NCS2K-1.2T-MXP	TXPMXP: 400G Trunk and 100GE, 400GE, and OTU4 clients

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

Table 24: Supported circuit provisioning options for 400G-XP-LC cards

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

GMPLS endpoints and operations

Use this reference to provision service endpoints, review supported values, and manage GMPLS service lifecycle actions.

Provisioning GMPLS services involves selecting a supported circuit type, defining compatible endpoints, configuring path and restoration constraints, and validating optical feasibility before deployment.

Supported transponder cards and modes
Table 25: 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

Card	Modes Supported
NCS2K-400G-XP-LC	MXP: 400G trunk and 100g, 10G clients FEC Modes: SD_FEC_15_DE_OFF, SD_FEC_15_DE_ON, SD_FEC_25_DE_OFF, SD_FEC_25_DE_ON MXP with backplane connection to 15454-M-10X10G-LC with slice 2 configured as OPM-PEER-ODU2 or OPM-PEER-ODU2E REGEN: 100G and 200G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits
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 RGN-100G: 100G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits
15454-M-10X10G-LC	MXP 10x10G (with backplane connection to NCS2k-200G-CK-C/15454-M-100G-LC-C/15454-M-100G-ME-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients
15454-M-100G-LC-C and 15454-M-100G-ME-C	• 10x10G client card • 100GE TXP mode: 100G trunk and 100GE/OTU4 clients

Note

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

Note

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

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

Troubleshooting GMPLS provisioning errors

These are some common errors encountered during GMPLS circuit provisioning:

Table 26: Details

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.
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.

Additional supported provisioning options

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

Table 27: Supported circuit provisioning options for 100G-LC-C/100G-ME-C and 400G-XP-LC cards

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

Create GMPLS services

Use this procedure to create GMPLS services. The task helps you define service endpoints, enter parameters, review supported values, and submit the service request.

Create a GMPLS circuit by defining its endpoints and provisioning parameters.

Review the supported configurations and troubleshooting information before provisioning a GMPLS circuit.

Before you begin

Table 28: 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 MXP with backplane connection to 15454-M-10X10G-LC with slice 2 configured as OPM-PEER-ODU2 or OPM-PEER-ODU2E REGEN: 100G and 200G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits
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 RGN-100G: 100G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits
15454-M-10X10G-LC	MXP 10x10G (with backplane connection to NCS2k-200G-CK-C/15454-M-100G-LC-C/15454-M-100G-ME-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients
15454-M-100G-LC-C and 15454-M-100G-ME-C	• 10x10G client card • 100GE TXP mode: 100G trunk and 100GE/OTU4 clients

Note

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

Note

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

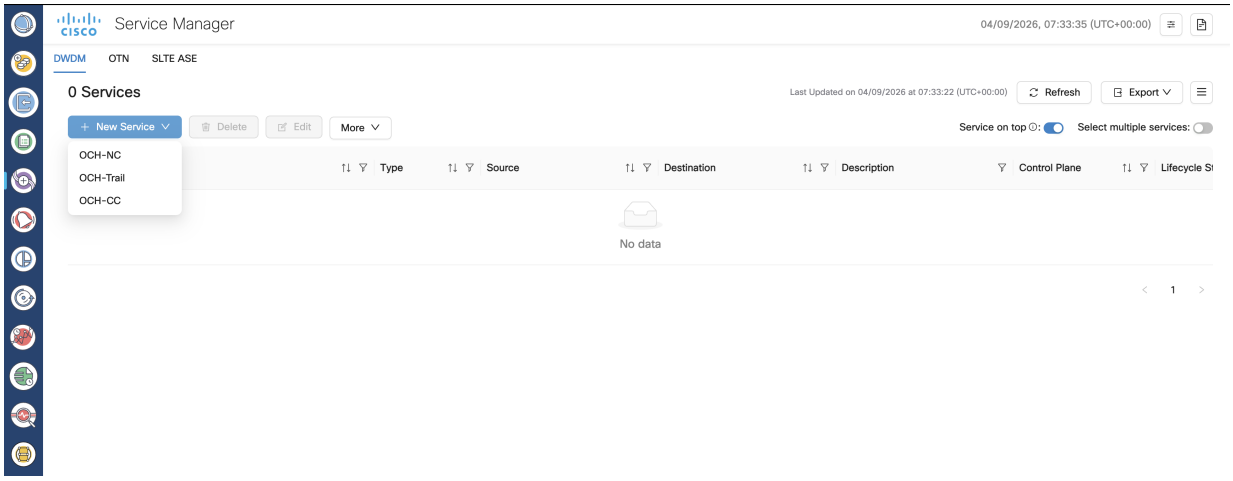
In release 26.1.1, OTN services are supported in the OTN-XC card mode of the NCS2K-400G-XP-LC line card only.

Follow these steps to create and manage GMPLS services:

Procedure

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

   Figure 33: Service Manager



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.

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

Figure 34: Service Manager > General

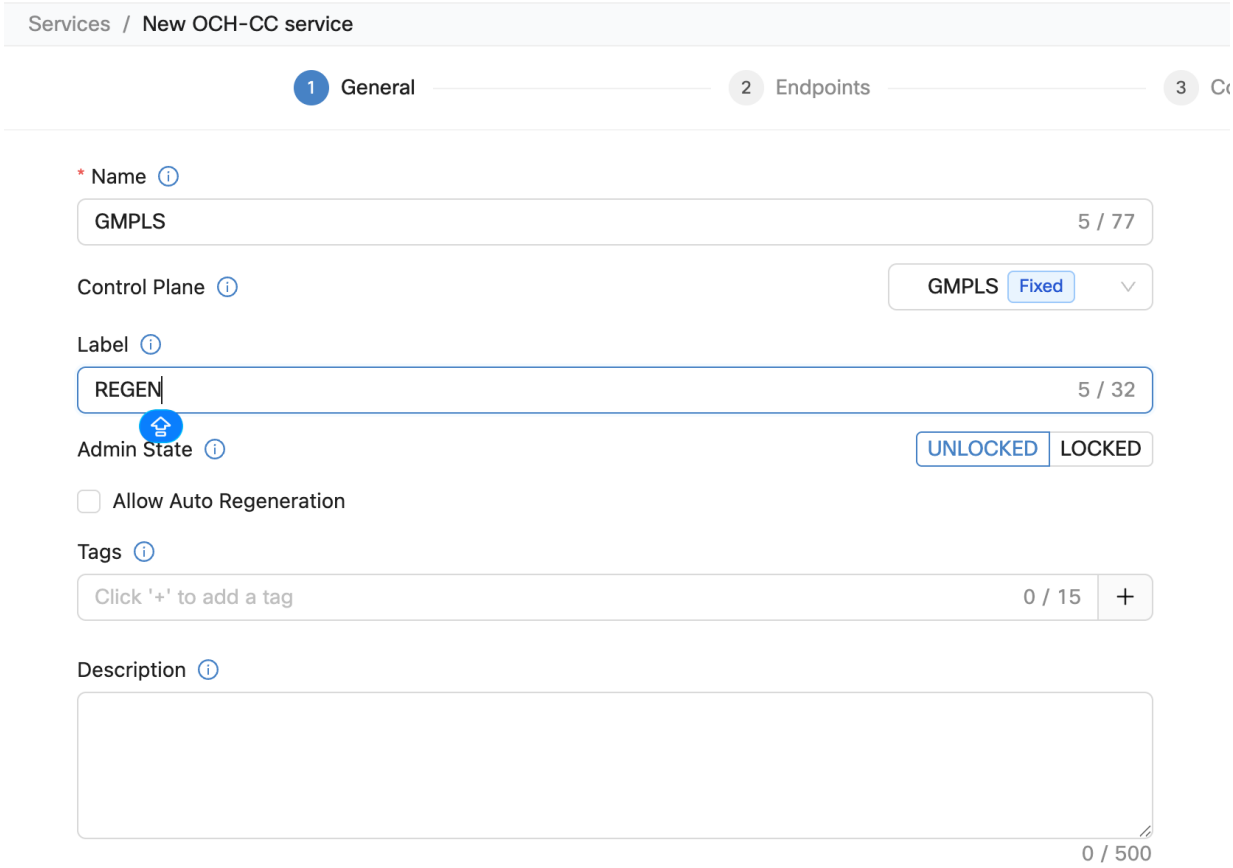


Table 29: General Parameters

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.

Field	Description	Values/restrictions
Admin State	The admin state of the service	UNLOCKED or LOCKED
Allow Auto Regeneration	Allows the control plane to find a regenerator deployed in the network when a single DWDM channel is not optically feasible end to end. **Note** This field is only displayed when GMPLS is selected in **Control Plane**.	Available for GMPLS OCH-Trail and OCH-CC circuits.
Tags	Tags can be attached to a service for better management, to group them together.	–
Description	Add a description about the service.	–

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

Figure 35: Service Manager > Endpoints

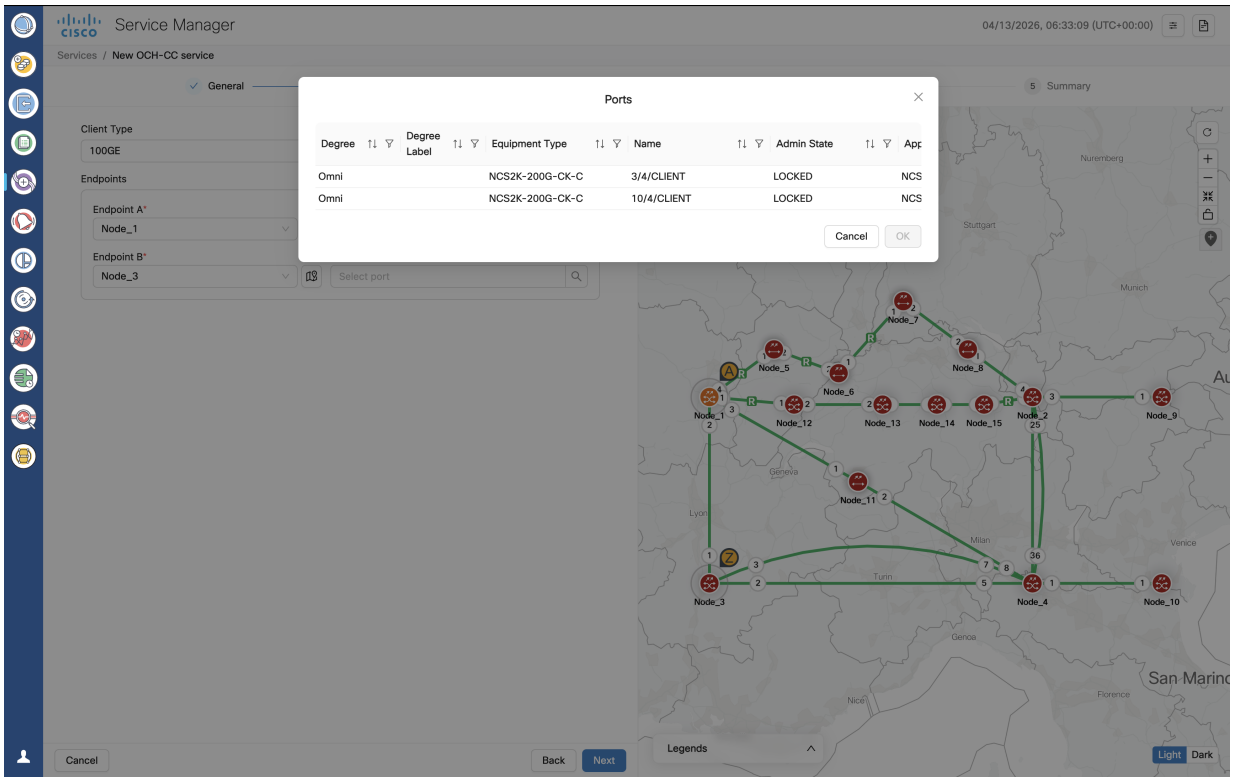


Table 30: Endpoints Parameters

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.

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

Figure 36: Service Manager > Constraints > General

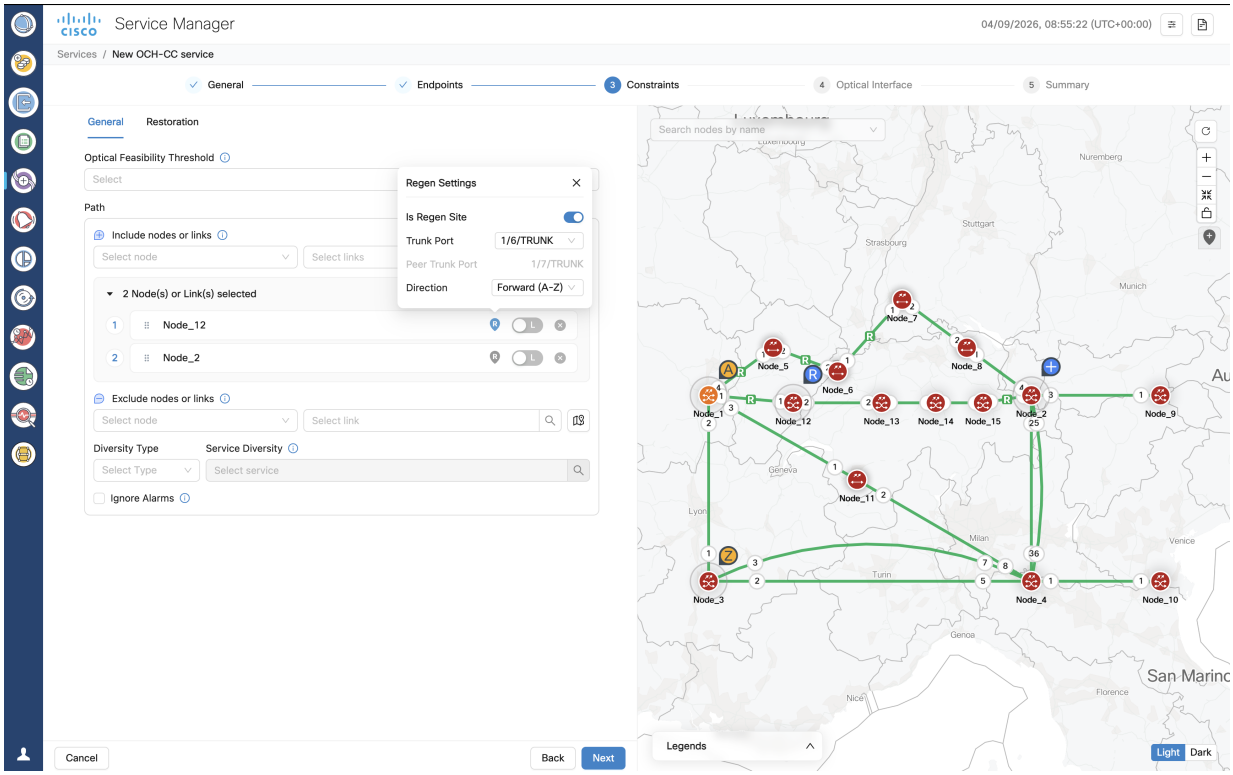


Table 31: General constraints field descriptions

Field	Description	Values/restrictions
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	Select RED, GREEN, YELLOW or ORANGE. GREEN = mean value YELLOW = +1 sigma ORANGE = +2 sigma RED = +3 sigma
Path		
Include nodes or links	select list of nodes & links that has to be included by the control plane during path computation.	–
Regen (R) settings icon	Allows the control plane to include a regen node present in network to create an end-to-end circuit.	–
Regen Settings	Includes the selected node as a mandatory regen site in the working circuit path.	Use the **R** icon to open this dialog. • **Include as regen:** Enable toggle button include node as regen. • **Trunk Port**: (Optional) Select the trunk port. • **Direction**: (Optional) Select the direction.
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	–
Diversity Type	Choose the type of service diversity	Node, link, or srlg
Service Diversity	Select one or more existing services from the dropdown for the control plane to exclude the resources that the services use during path computation.	–
Ignore Alarms	If true, Service manager ignores unverified alarms present on the path and continues to provision the service.	–

Note

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

a) For regenerated GMPLS OCH-Trail and OCH-CC circuits, add a node in the include constraint list and click the **R** icon

Alternatively, you can click the map icon or the blue inverted teardrop icon in the map and select a node from the map.

b) In the **Regen Settings** dialog, enable the **Is Regen Site** toggle button.
c) You can optionally select a **Trunk Port** and **Direction** for the regen site.

- If the node is selected as general regen node, it appears with a blue inverted teardrop **R** icon in the topology and **REGEN** icon in the **Detailed service path** tab of **Circuit Monitoring** application.
- If the node is a normal general node, it appears with a blue inverted teardrop **+** icon in the topology.
- For each regen node circuits, when you expand a service in the Service Manager table, segments are displayed and the **Regenerated** column shows **True**.

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

Figure 37: Service Manager > Constraints > Restoration

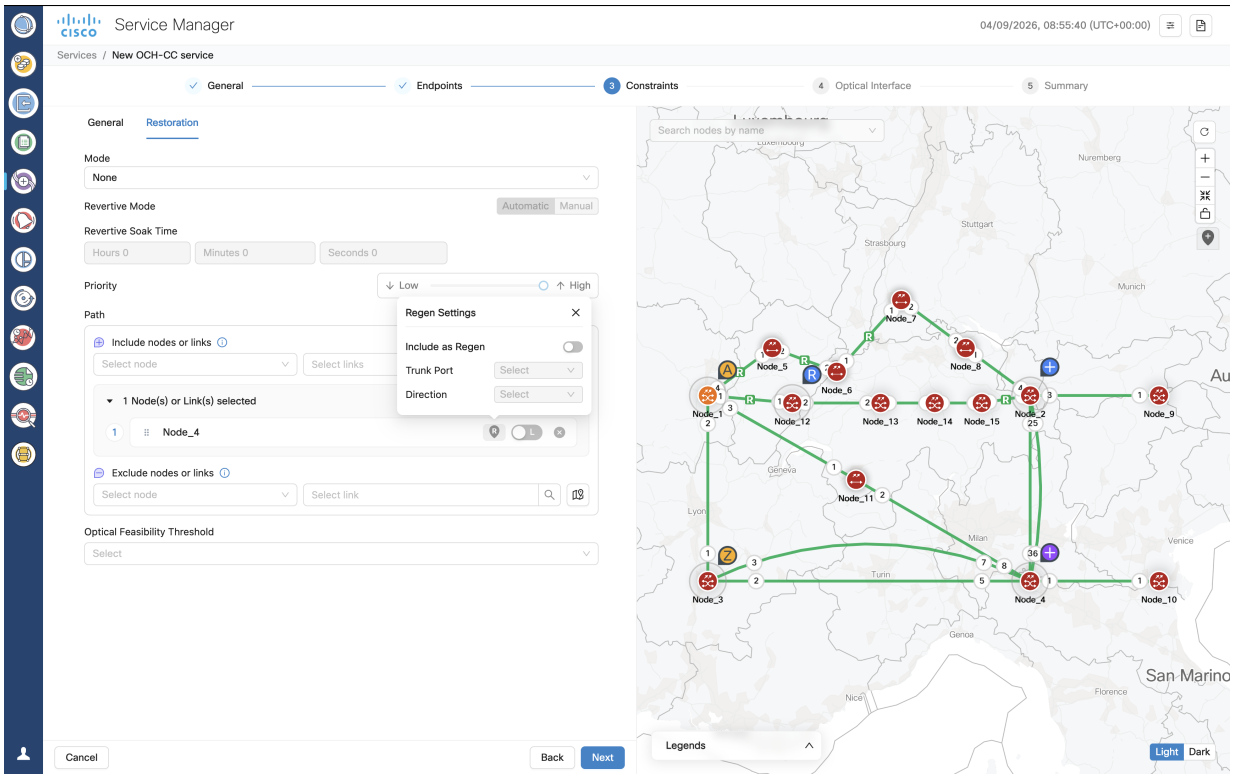


Table 32: Restoration constraints field descriptions

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

Field	Description	Values/restrictions
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.	
Regen (R) settings icon	Allows the control plane to include a regen node present in network to create an end-to-end circuit.	–
Regen Settings	Includes the selected node as a mandatory regen site in the working circuit path.	Click the **R** icon to open this dialog. • **Include as regen:** Enable toggle button include node as regen. • **Trunk Port**: (Optional) Select the trunk port. • **Direction**: (Optional) Select the direction.
Exclude nodes or links	select list of nodes & links that has to be excluded by the control plane during path computation.	
Optical Feasibility Threshold	Indicates the optical feasibility of the link to ensure that the link is operational after provisioning.	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.

a) For regenerated GMPLS OCH-Trail and OCH-CC circuits, add a node in the include constraint list and click the **R** icon

   Alternatively, you can click the map icon or the blue inverted teardrop icon in the map and select a node from the map.

b) In the **Regen Settings** dialog, enable the **Include as Regen** toggle button.
c) You can optionally select a **Trunk Port** and **Direction** for the regen site.

- If the node is selected as restoration regen node, it appears with a purple inverted teardrop **R** icon in the topology and **REGEN** icon in the **Detailed service path** tab of **Circuit Monitoring** application after regeneration is completed.
- If the node is a normal restoration node, it appears with a purple inverted teardrop **+** icon in the topology.
- For each regen node circuits, when you expand a service in the Service Manager table, segments are displayed and the **Regenerated** column shows **True**.

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

Table 33: Optical interface parameters

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

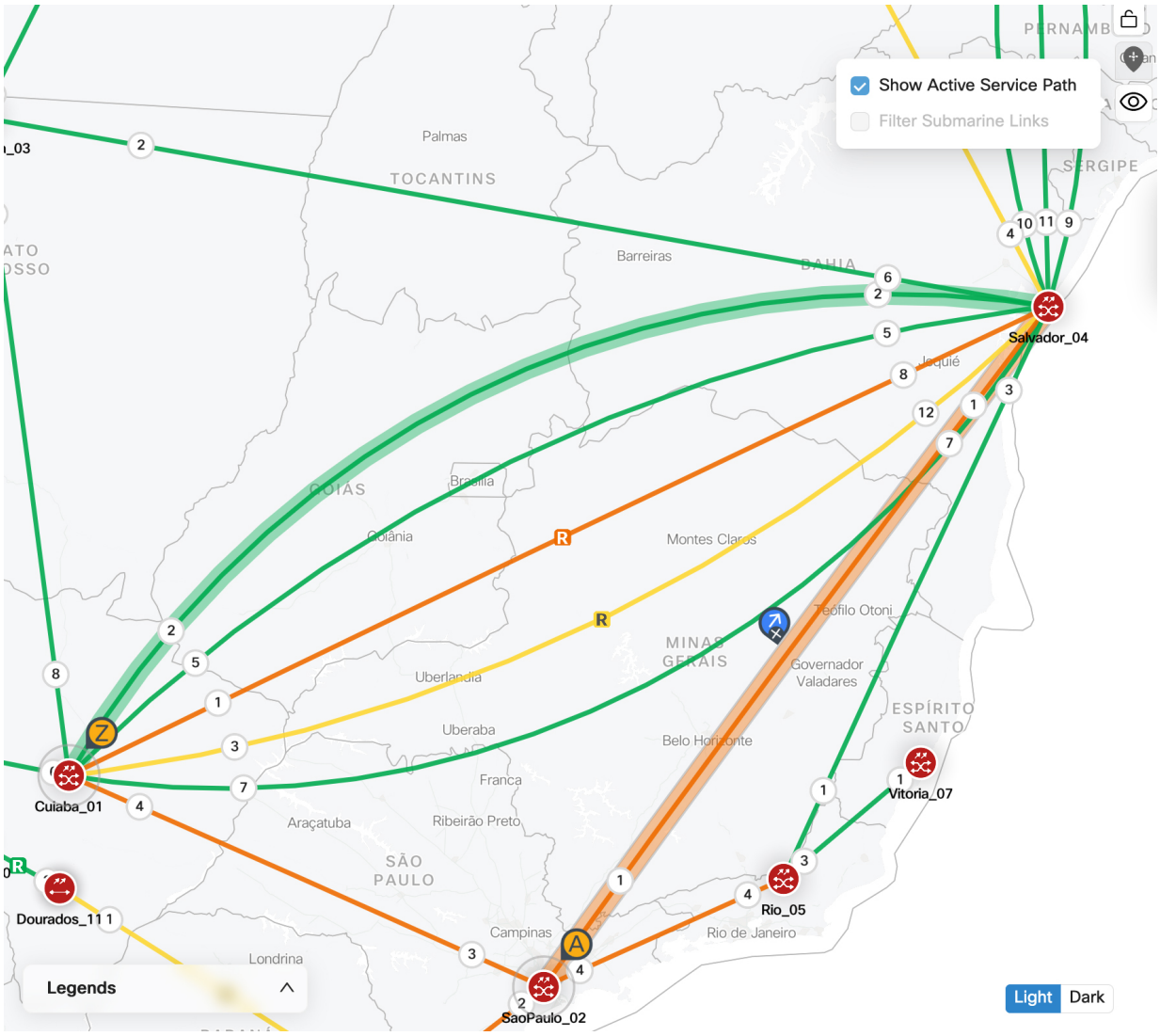
Note

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

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

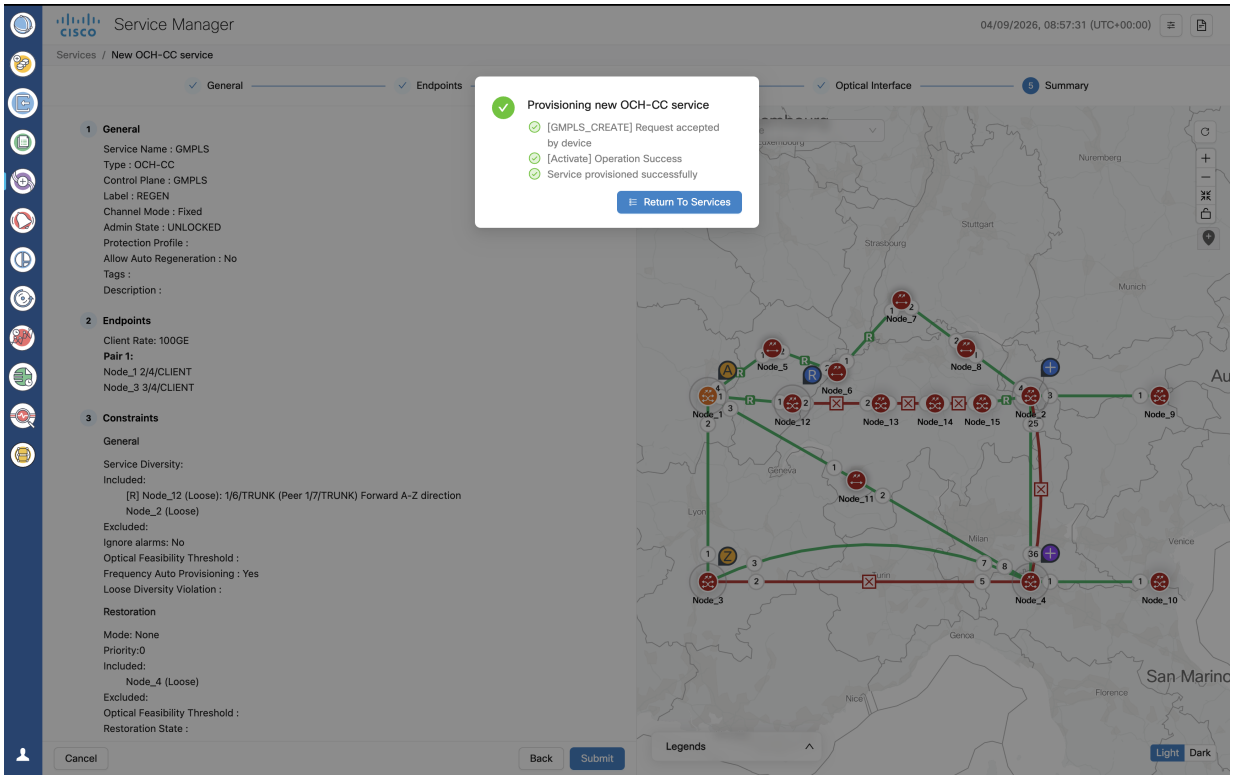
In Release 26.1.1, Topology view in Service Manager reflects the topology screen with a modified **Map View Options** eye icon. Click the eye icon and then **Show Active Service Path** to see the current active service path in the network like in Circuit monitoring screen.

Figure 38: Show Active Service Path



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

Figure 39: Service Manager > Summary



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

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

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

The create and manage GMPLS services task is complete.

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

Table 34: Details

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.
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.

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

Table 35: Supported circuit provisioning options for 100G-LC-C/100G-ME-C and 400G-XP-LC cards

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

Manage GMPLS services

Use this procedure to manage GMPLS services. The task helps you view service details, update supported settings, and perform service lifecycle actions.

Use this procedure to create and manage circuits.

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

Table 36: Details

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.
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.

Before you begin

Table 37: Supported transponder cards and modes

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

Card	Modes Supported
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 MXP with backplane connection to 15454-M-10X10G-LC with slice 2 configured as OPM-PEER-ODU2 or OPM-PEER-ODU2E REGEN: 100G and 200G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits
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 RGN-100G: 100G trunk regeneration for GMPLS OCH-Trail and OCH-CC circuits
15454-M-10X10G-LC	MXP 10x10G (with backplane connection to NCS2k-200G-CK-C/15454-M-100G-LC-C/15454-M-100G-ME-C) 100G trunk and 10G, OTU2, OTU2e, and OC192/STM64 clients
15454-M-100G-LC-C and 15454-M-100G-ME-C	• 10x10G client card • 100GE TXP mode: 100G trunk and 100GE/OTU4 clients

Note

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

Note

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

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

Follow these steps to create and manage GMPLS services:

Procedure

1. Select a service and click **Edit** to edit the circuit.
   a) Go to **Constraints** > **General** and update the constraints. Click **Reroute** after updating constraints to reroute the circuit.
   A status pop-up appears showing the progress of the reroute process.

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

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

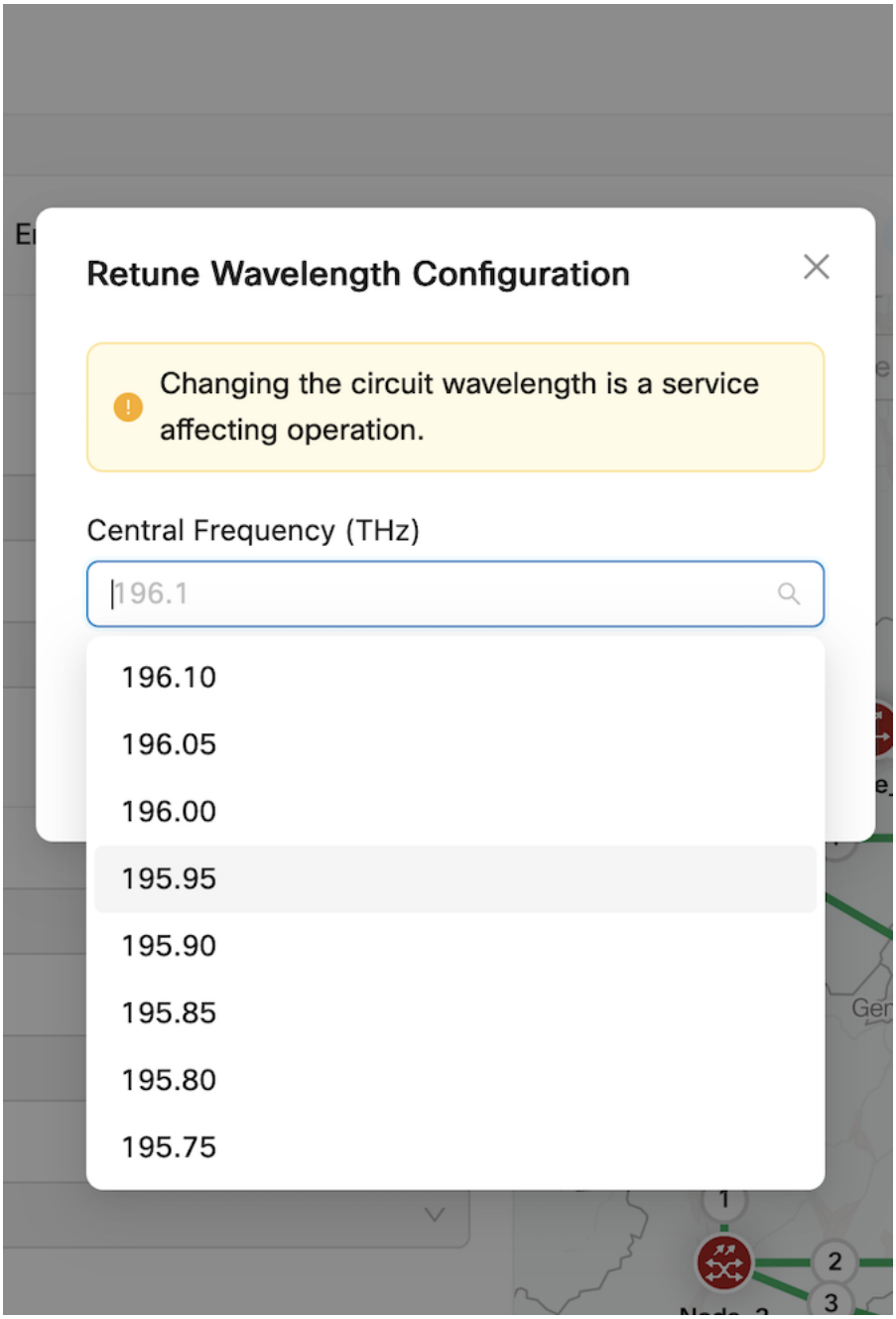
   You can update regen constraints for the restoration path of a regenerated circuit.

   c) Click **Upgrade Restored** to make a restored circuit path the main circuit path.
   d) Click **Revert Restored** to revert to the main path when **Revertive mode** is **Manual**.

   Clear unverified alarms from COSM before performing this step.

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

   Figure 40: Service Manager > Optical Interface > Retune



Note

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

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

2. 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 38: 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

3. 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.

The create and manage GMPLS services task is complete.

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

Table 39: Supported circuit provisioning options for 100G-LC-C/100G-ME-C and 400G-XP-LC cards

Configuration	OCH-CC	OCH-Trail	OCH-NC
NCS2000 100G-LC-C/100G-ME-C standalone	Yes	Yes	Yes
NCS2000 100G-LC-C/100G-ME-C with peered ONS 15454 10x10G-LC	Yes	Yes	Yes
NCS2000 400G-XP-LC with peered ONS 15454 10x10G-LC	Yes	Yes	Yes

Configuration	OCH-CC	OCH-Trail	OCH-NC
10X10G with MPO cable connected to 400G-XP-LC	No	Yes	Yes

7 Alarms

Topics:

- Manage alarms

Covers alarms in Cisco Optical Network Controller, including current alarms, alarm history, event views, SNMP traps, alarm filters, and email forwarding.

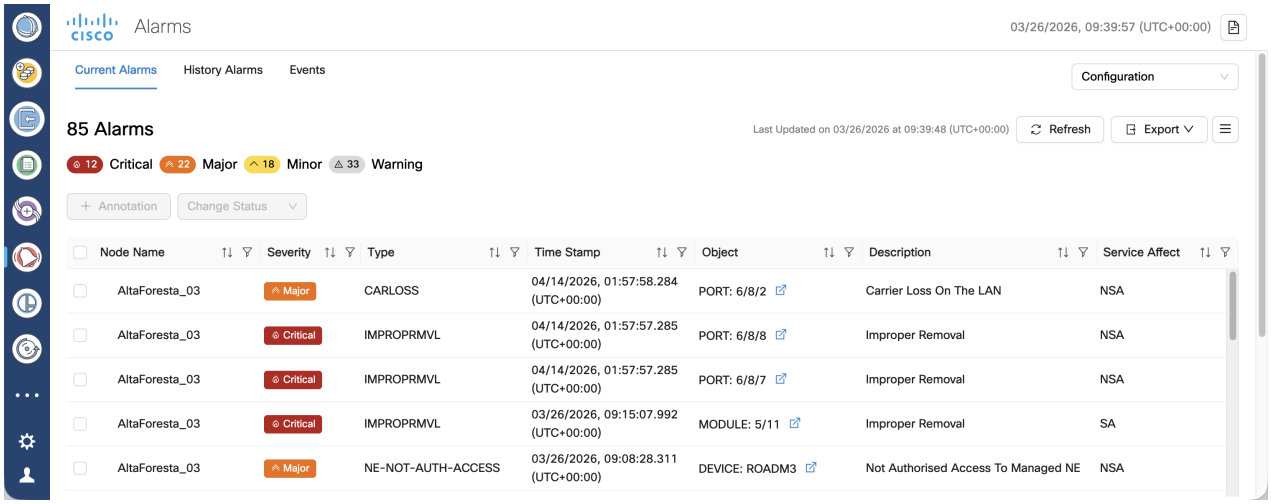
Manage alarms

Use this procedure to manage alarms. The Alarms screen displays all the alarm details for each node based on the severity level.

Use this procedure to manage alarms in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Figure 41: Alarms



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

Table 40: Alarm table field descriptions

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

Field Name	Description	Example/Values
User Tag	User-defined tags for categorizing and filtering alarms. **Note** • User tags propagate from parent to child components of a chassis by default. A user tag on a child component overrides the inherited tag from its parent. • User Tag information comes from Cisco Optical Site Manager. See User Tags. • User tags are not supported on system-level and device alarms. • User tags can apply CLLI (Common Language Location Identifier), a standardized 11-character code that uniquely identifies geographic locations and equipment for network sites, network support sites, and customer locations.	Custom tags/labels
User Notes	User-added notes or comments related to the alarm.	Free-form text
Acknowledge	Indicates whether the alarm has been acknowledged.	Acknowledged, Unacknowledged
UUID	Unique Universal Identifier for the alarm.	UUID string
Correlation Type	The type of correlation applied to the alarm.	Network Level, Node Level

Note

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

Before you begin

Follow these steps to manage alarms:

Procedure

1. Complete view and manage current alarms.

   View and manage current alarms

2. Complete filter and review alarm details.

Filter and review alarm details

The manage alarms task is complete.

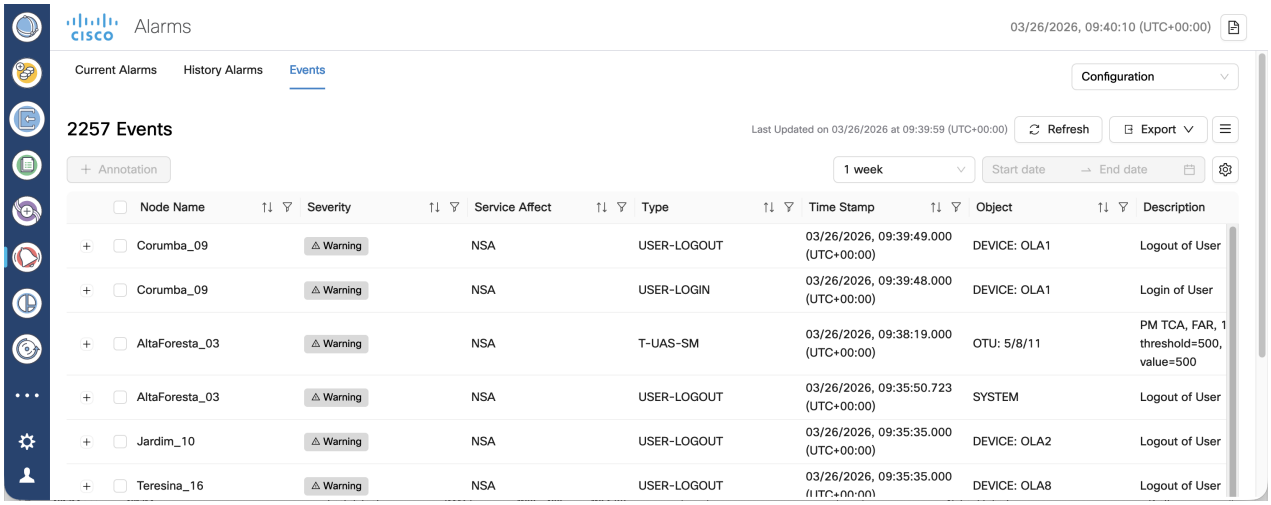
View events in the alarms application

Use this procedure to view events in the alarms application. The Events tab displays events tracked separately from current alarms, such as user login, logout activity, and performance monitoring notifications.

Use this procedure to view events in the alarms application in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

The **Events** tab displays events tracked separately from current alarms, such as user login, logout activity, and performance monitoring notifications. Unlike **Current Alarms**, events are informational entries and do not support acknowledge or unacknowledge actions.

Figure 42: Events tab in Alarms application



Before you begin

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

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

Procedure

1. Click **Alarms** in the left pane.
2. Click the **Events** tab.

   The table shows the latest event for each node. Event types include user login, user logout, and performance monitoring notifications. For details about the table fields, see Table 40: Alarm table field descriptions on page 113.

3. To filter events by timeframe:
   a) Select *Custom Date Range* and specify the start and end dates to filter the events for the selected period.

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

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

      Valid range: 1 week to 12 weeks

> **Note**
>
> Transient alarms are also displayed under the **Events** tab. During new device onboarding or resynchronization, the client receives updates only for transient alarm differences within the configured retention period. If the retention period is increased and device resynchronization is triggered, older historical transient alarms that fall within the expanded retention period but are not present in CONC may be sent as Raised notifications. This can cause an expected temporary increase in notifications.

4. To add user notes to events, complete these steps.
   a) Select an alarm or multiple alarms and click **Annotation**.
   b) In the **Add User Notes** dialog box, enter the note text and click **Add**.
5. Optional: Use the sort and filter controls in the column headers to find specific events.
6. Click the + icon next to an event entry to view the event history and the associated user notes.
   The expanded view shows the recorded event status entries for the selected node and any user notes that were added to that event.
7. Click the hamburger icon to show or hide columns.

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

Network level alarm correlation

This section explains network level alarm correlation, including correlation scenarios and alarms suppressed by LOS on line. Use it to understand how related alarms are grouped or suppressed.

Network level alarm correlation is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Network level alarm correlation details

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

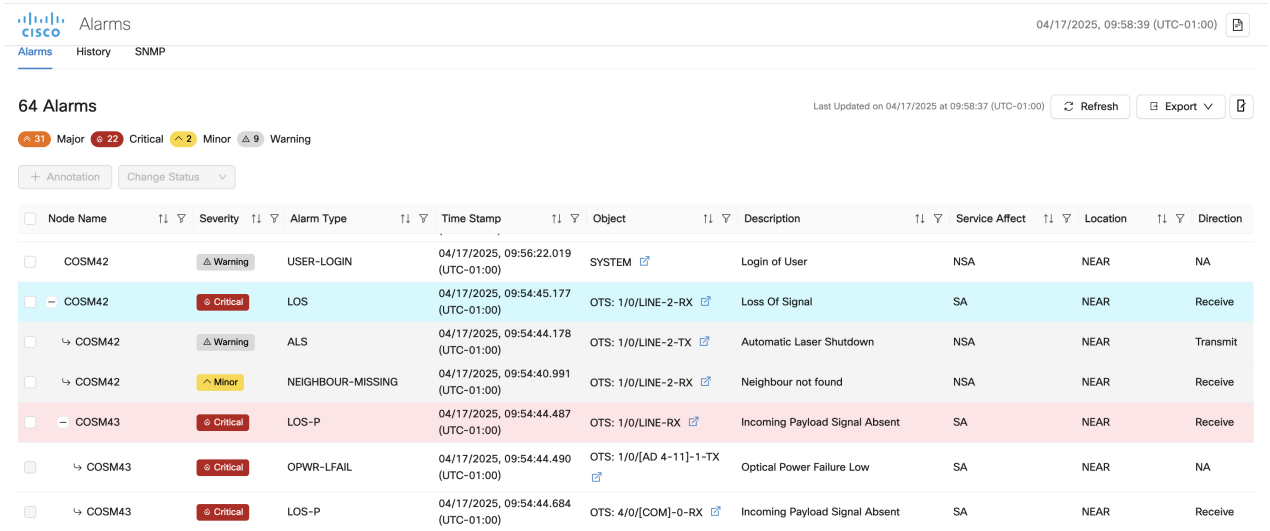
Note

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

Alarm Hierarchy Display

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

Figure 43: Alarms History



Alarm Correlation

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

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

Table 41: Alarms suppressed by LOS on line

Alarm	Object Type
LOS-P	LINE

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

Note

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

Purpose of Using NLAC

When a fiber cut occurs, it triggers a Loss of Continuity (LOC) alarm, which is then correlated with other Loss of Signal-Payload (LOS-P) alarms in the circuit. The root cause alarm, typically the LOC, suppresses other alarms, ensuring that subsequent LOS-P alarms depend on the LOC rather than the Automatic Laser Shutdown (ALS) alarms.

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.

Scenarios for Using NLAC

There are multiple scenarios which specify how NLAC is used, some of them are:

- **Unidirectional Fiber Cut**:
- **Correlation Mechanism: LOS to LOS-P**: Forward direction
- **Correlation Mechanism: ALS to LOS-P**: Reverse direction.

- **Multiple LOS in Forward Direction**: For multiple LOS scenarios both in upstream and downstream circuits.
- **Bidirectional Fiber Cut**:

> **Note**
>
> In the bidirectional scenario, we have LOS and LOS-P correlations in both the directions. In addition, we will also have ALS to LOS-P correlation up to the port where we have the LOS. In this situation, LOS will correlate to all LOS-P downstream.

- **Correlation Mechanism: LOS to LOS-P**: Forward and reverse direction.
- **Correlation Mechanism: ALS to LOS-P**: Reverse direction.
- **Multiple LOS in Forward or Reverse Direction**: For multiple LOS scenarios both in upstream and downstream circuits.
- **New LOS in Reverse direction**: For new loss in the downstream circuits.

NLAC LOC and LOS-P Alarms

These alarms can be viewed in the **Alarms** and **Workspaces** applications for each node.

Figure 44: LOS and LOS-P Correlation

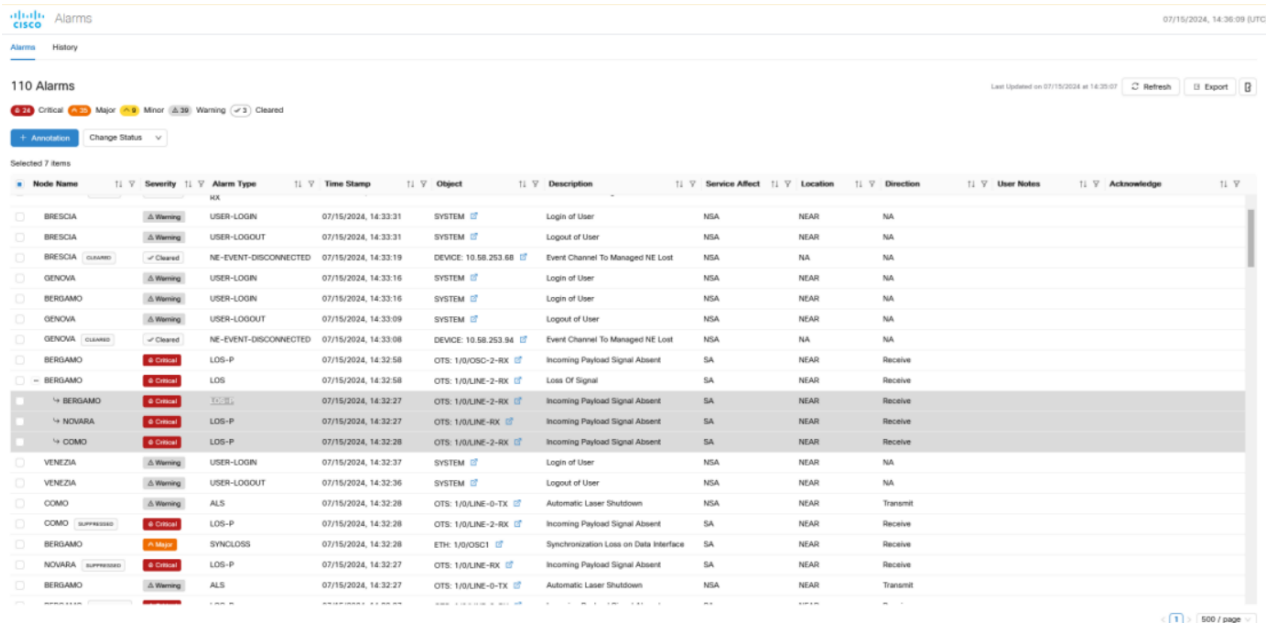
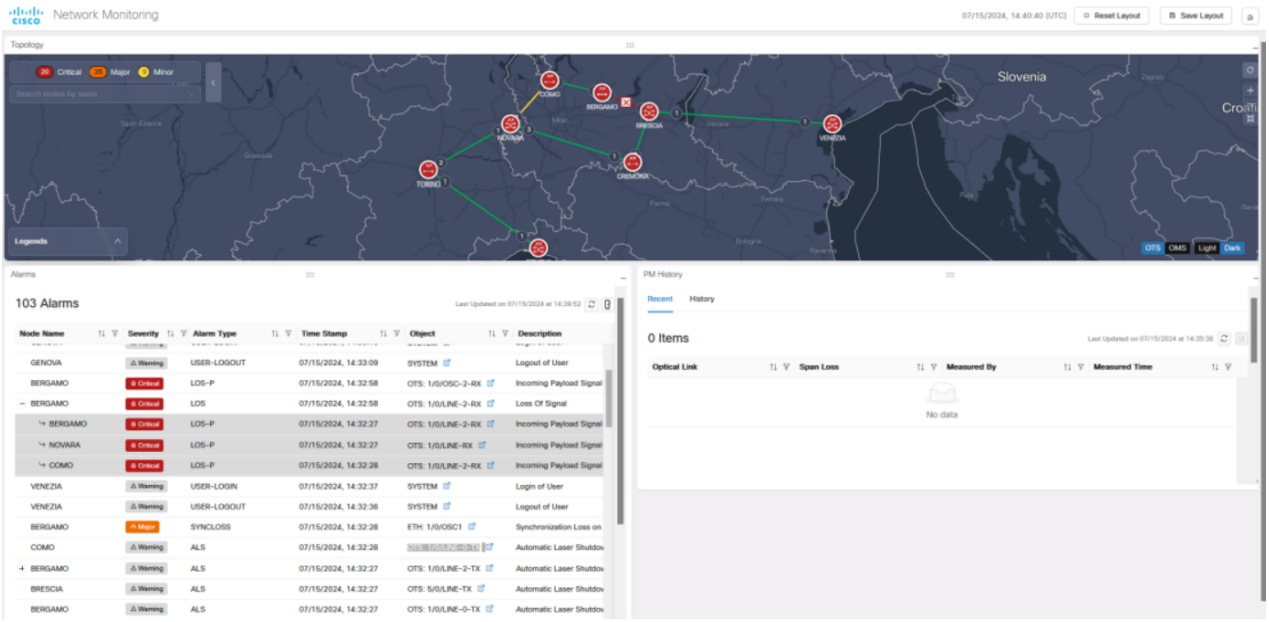


Figure 45: LOS and LOS-P Correlation in Network Monitoring



Acknowledged alarm mute

This section explains acknowledged alarm mute, including mute behavior and alarm display changes. Use it to understand how acknowledged alarms are handled in Cisco Optical Network Controller.

Acknowledged alarm mute is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Acknowledged alarm mute details

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

Purpose of Acknowledged Alarm Mute

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

Benefits of Using Acknowledged Alarm Mute Option

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

Muting the Acknowledged Alarms

To mute the alarms on the screen:

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

Note

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

Notifications for Acknowledged Alarm Mute

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

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

Note

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

Figure 46: Mute Acknowledged Alarms in Topology

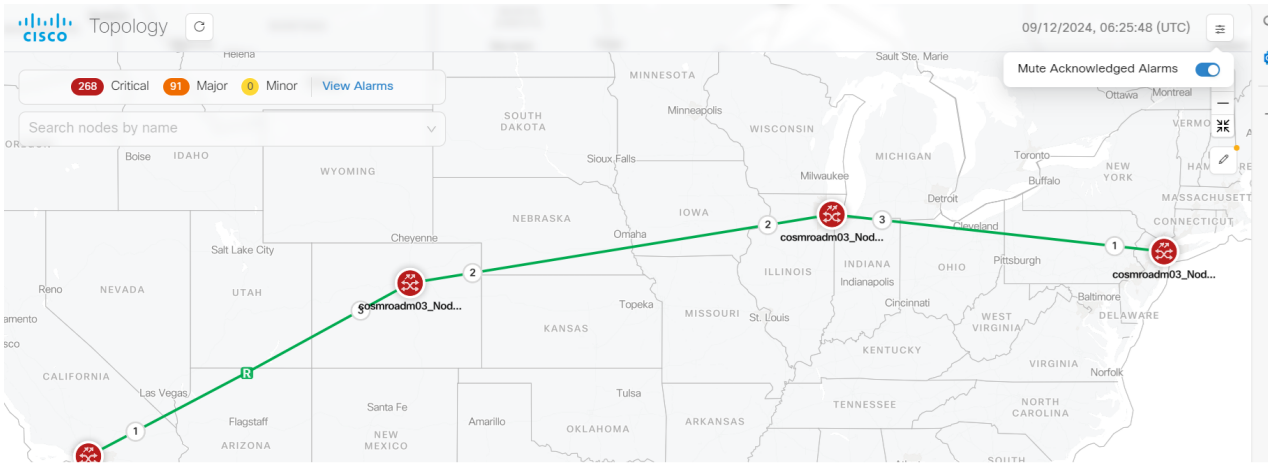
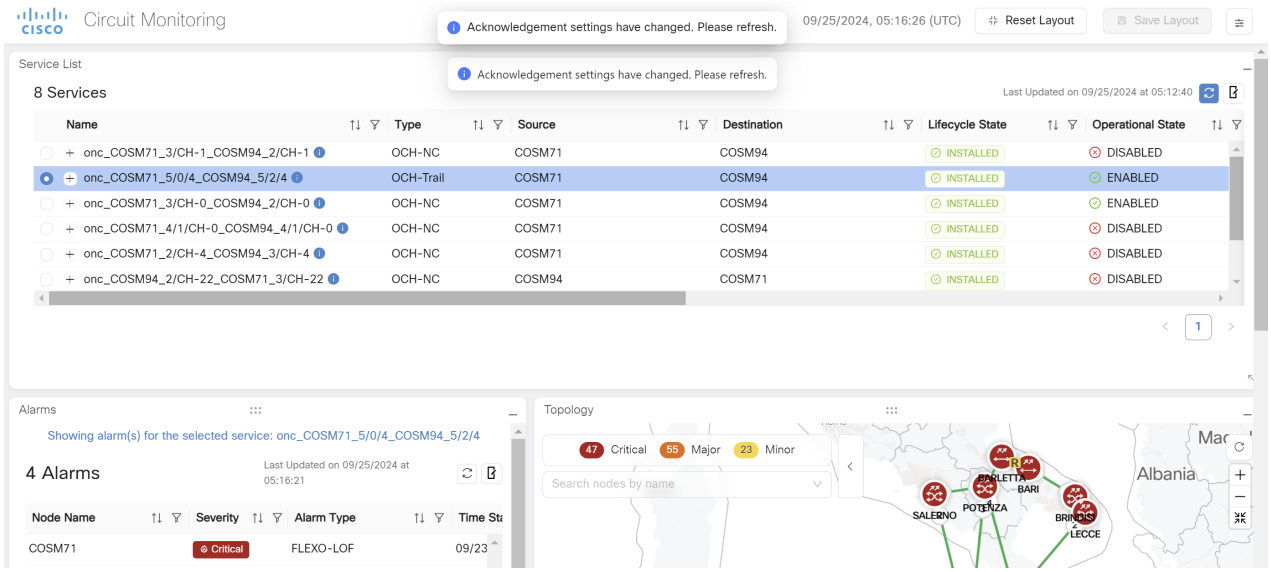


Figure 47: Mute Acknowledged Alarms in Circuit Monitoring



SNMP traps and alarm filters

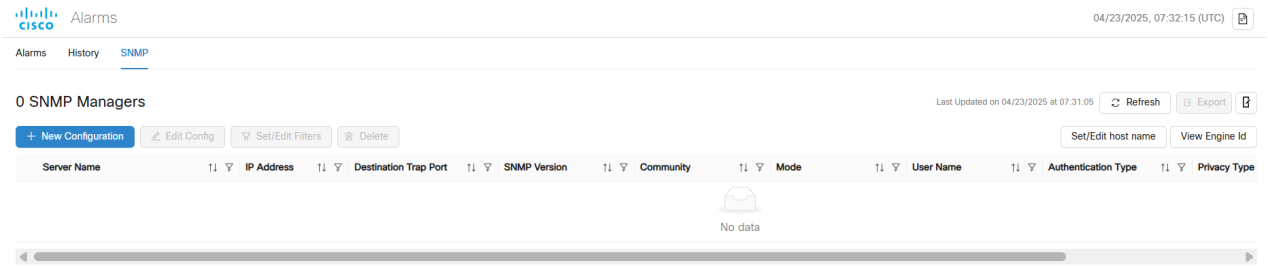
This section explains SNMP traps and alarm filters, including trap receiver settings and filter behavior. Use it to understand how Cisco Optical Network Controller sends alarm notifications.

SNMP traps and alarm filters is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

SNMP traps and alarm filters details

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 host name

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

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

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.

Follow these steps to set the host name:

Procedure

1. Click **Set/Edit Host Name**.
2. Enter the desired hostname.
3. Click Save.
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.

The set the host name task is complete.

Configure SNMP managers

Configure SNMP managers to forward filtered alarms and events as traps using CISCO-EPM-NOTIFICATION-MIB.

Add an SNMP manager and configure the alarm filters used to send traps.

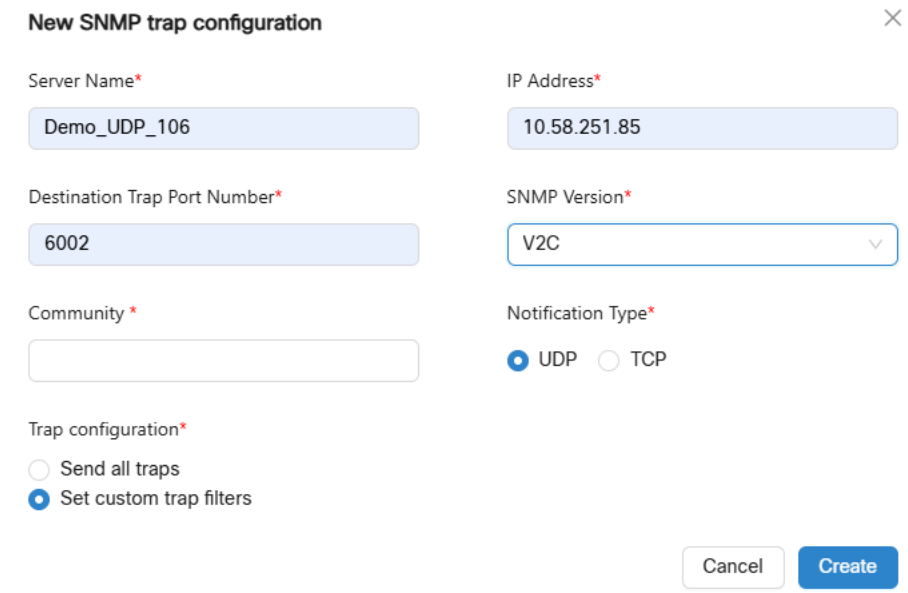
Cisco Optical Network Controller converts alarms and events that match the configured filters into traps and sends them to the SNMP manager using CISCO-EPM-NOTIFICATION-MIB. For more information, see MIB Definition For Cisco Optical Network Controller.

Procedure

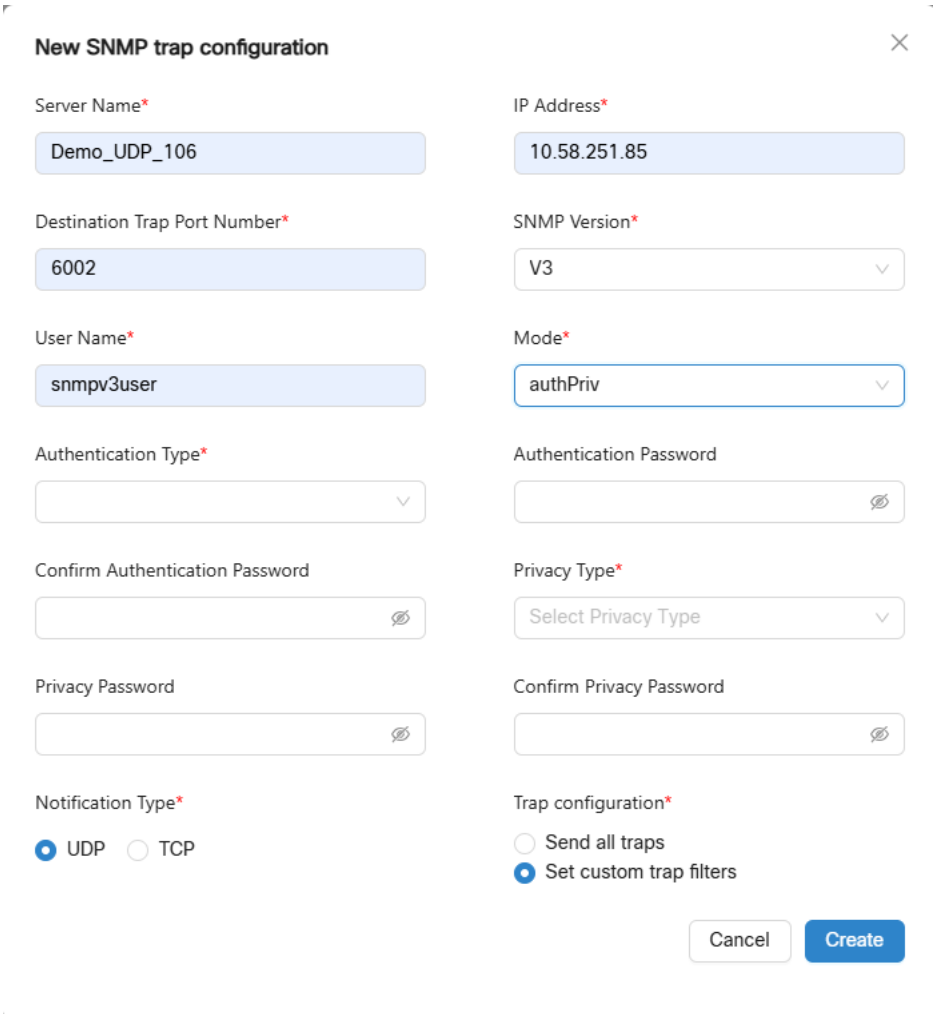
1. Navigate to **Alarms** > **SNMP**.
2. Create an SNMP manager.
   a) Enter the Server Name and IP Address.

      Cisco Optical Network Controller supports only IPv4.

   b) Enter the Port Number, and choose the SNMP Version.
   c) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.

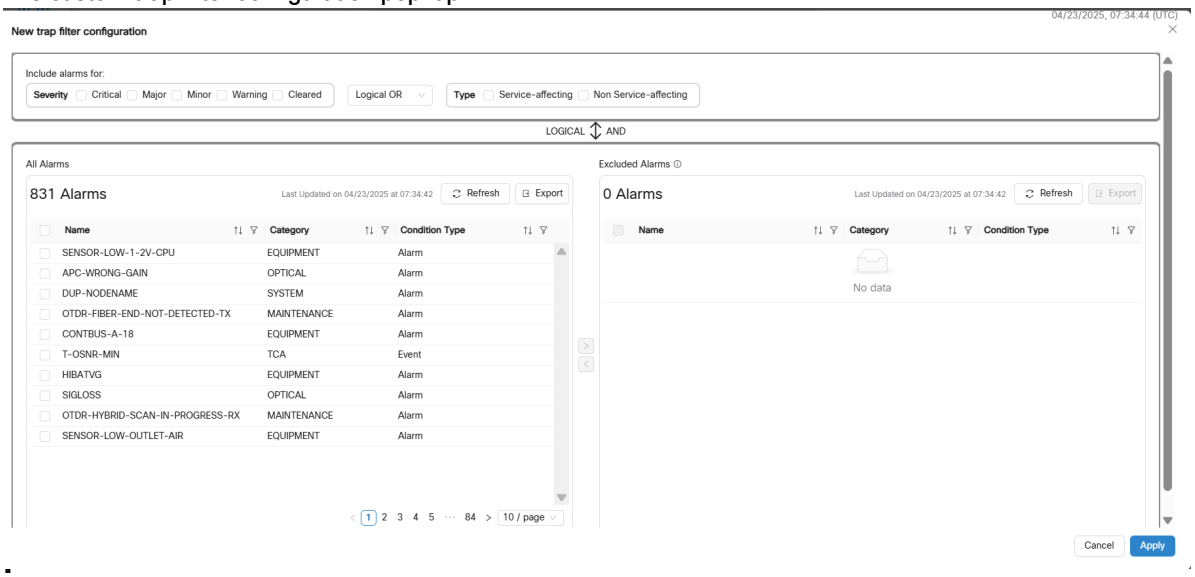


d) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth. Type**, **Auth. Password**, **Confirm Auth. Password**, **Privacy Type**, **Privacy Password**, and **Confirm Privacy Password**.



e) Choose the **Notification Type**, TCP or UDP.
f) Choose the **Trap Configuration**, Send all traps or Set custom trap filters.
If you choose custom trap filters, continue to Configure alarm filters.

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.

The configure SNMP managers task is complete.

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

Alarm email forwarding

This section explains alarm email forwarding, including SMTP server requirements, supported alarm types, subscriptions, and notification behavior. Use it to understand how alarm emails are generated.

Alarm email forwarding is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Alarm email forwarding details

A alarm email forwarding is a notification capability that

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

How alarm email forwarding works

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

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

  For example, if user 1 is configured in Subscription A and Subscription B, and the same alarm matches both subscriptions, use 1 receives only one email notification for that alarm.
- The sender email address is fixed and is not user-configurable.
- Read-only users cannot create, edit, or delete alarm subscriptions.
- All notification emails are sent from the fixed sender address *noreply-conc@cisco.com*. This address cannot be changed by users.

SMTP server requirement

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

- SMTP settings can be configured from the **Jobs** tab of the **PM History** application. For more details, see Access PM history report on page 209.
- You can specify both a primary SMTP server and, optionally, a secondary SMTP server for failover. If the primary server becomes unavailable, the system automatically attempts to send notifications using the secondary SMTP server.
- The email subscription page displays the current SMTP configuration status. If SMTP is not configured, a warning **SMTP Server is not configured** is displayed with a link to the PM Jobs configuration page.

Alarm types that trigger notifications

These alarm events trigger email notifications:

Table 42: Details

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

Alarm email forwarding subscription settings

This section provides details about alarm email forwarding subscription settings, including subscription names, alarm filters, severity options, and recipient addresses. Use it to understand subscription configuration fields.

Use this reference to understand alarm email forwarding subscription settings.

Details about alarm email forwarding subscription settings.

Subscription settings

The alarm email forwarding page uses these settings.

Table 43: Alarm email forwarding settings

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

Alarm email notification format

This section provides details about alarm email notification format, including subject lines, email body sections, summary fields, and sender details. Use it to interpret alarm notification messages.

Use this reference to understand alarm email notification format.

Details about alarm email notification format.

Alarm email subject line format

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

Table 44: Alarm email subject line format

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

Email body format

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

Table 45: Alarm email summary fields

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

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

Sender details

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

Table 46: Alarm email sender details

Field	Value
From Address	noreply-conc@cisco.com

Configure alarm email forwarding subscriptions

Use this procedure to configure alarm email forwarding subscriptions. The Alarms page shows the existing subscriptions and provides options to create, edit, filter, delete, refresh, and export subscription entries.

Use this procedure to configure alarm email forwarding subscriptions in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

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

Follow these steps to configure an alarm email forwarding subscription.

Before you begin

Follow these steps to configure alarm email forwarding subscriptions:

Procedure

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

   The subscription list opens.

2. Click **New Subscription**.

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

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

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

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

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

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

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

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

   To create filters, click **No filters set** and proceed with the steps outlined in the Configure SNMP managers on page 124 topic.

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

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

7. To manage the subscriptions, perform these optional steps:
   a) To edit a subscription, select an existing subscription and click **Edit Subscription**.

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

b) To edit the filters, click **Set/Edit Filters**.
c) To delete a subscription, select a subscription and click **Delete**.
d) To export all subscription details, click **Export**.
The report is downloaded in a *.xlsx* file.

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

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

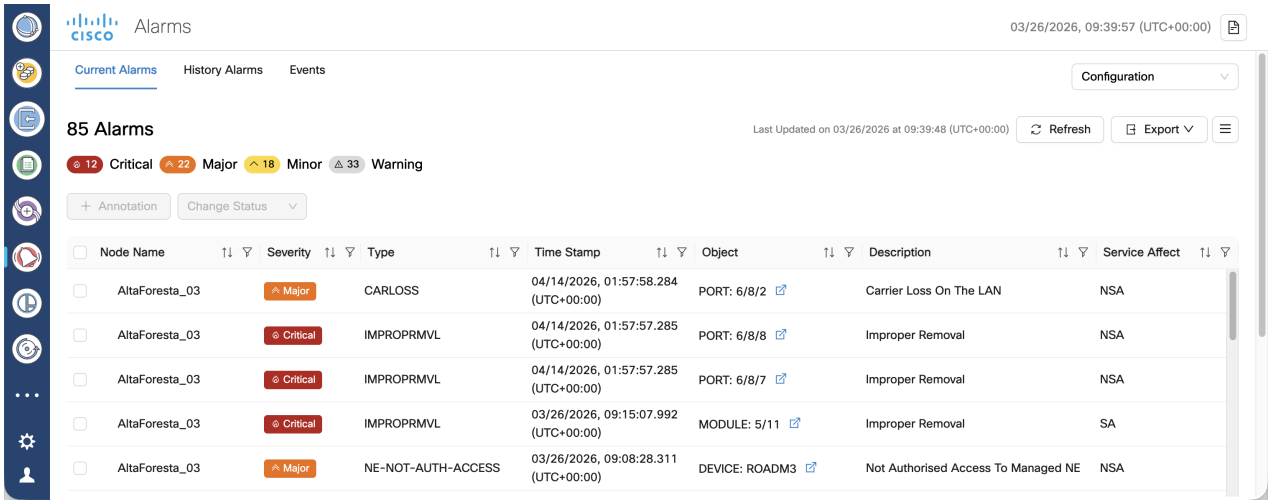
View and manage current alarms

Use this procedure to view and manage current alarms. The Alarms screen displays all the alarm details for each node based on the severity level.

Use this procedure to manage alarms in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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 48: Alarms



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

Table 47: Alarm table field descriptions

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

Field Name	Description	Example/Values
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.

Before you begin

Follow these steps to manage alarms:

Procedure

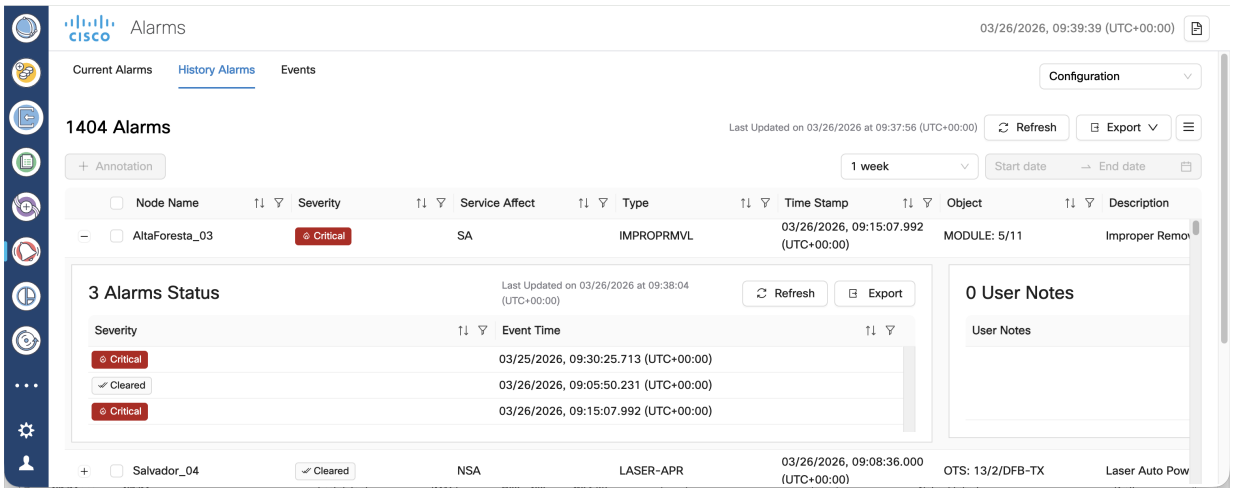
1. Click **Alarms** in the left panel.
2. Select the **AlarmsCurrent Alarms** tab to view the active alarms of each node.
3. Select an alarm or multiple alarms and click **Annotation** to add user notes to any alarm
   a) Enter the user notes and click **Add**.

   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.
4. Click **Change Status**and choose an option from the dropdown list to acknowledge or unacknowledge alarms.
5. Click **HistoryHistory Alarms** to view the inactive or previous alarms. The details of each alarm based on each node and alarm type are displayed in the form of a cascading list and tables. Use the **Custom Date Range** Custom Date Range drop down option to view the history alarms based on different dates or time periods.

Figure 49: Alarm History Expanded View



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

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

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

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.
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.

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.

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.

The manage alarms task is complete.

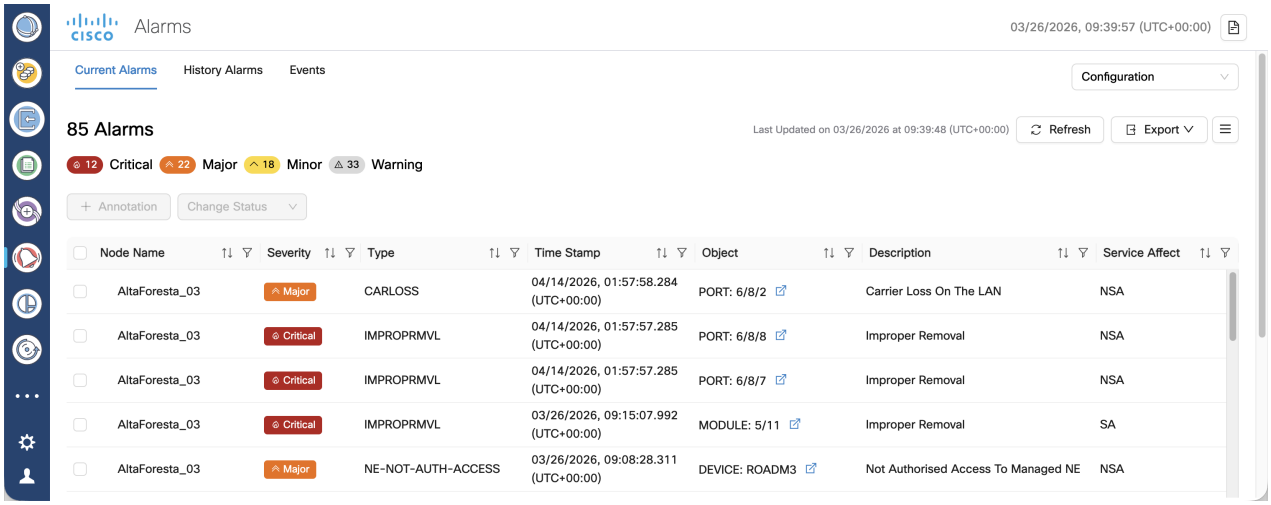
Filter and review alarm details

Use this procedure to filter and review alarm details. The Alarms screen displays all the alarm details for each node based on the severity level.

Use this procedure to manage alarms in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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 50: Alarms



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

Table 48: Alarm table field descriptions

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

Field Name	Description	Example/Values
User Tag	User-defined tags for categorizing and filtering alarms. **Note** • User tags propagate from parent to child components of a chassis by default. A user tag on a child component overrides the inherited tag from its parent. • User Tag information comes from Cisco Optical Site Manager. See User Tags. • User tags are not supported on system-level and device alarms. • User tags can apply CLLI (Common Language Location Identifier), a standardized 11-character code that uniquely identifies geographic locations and equipment for network sites, network support sites, and customer locations.	Custom tags/labels
User Notes	User-added notes or comments related to the alarm.	Free-form text
Acknowledge	Indicates whether the alarm has been acknowledged.	Acknowledged, Unacknowledged
UUID	Unique Universal Identifier for the alarm.	UUID string
Correlation Type	The type of correlation applied to the alarm.	Network Level, Node Level

Note

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

Before you begin

Follow these steps to manage alarms:

Procedure

1. 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.

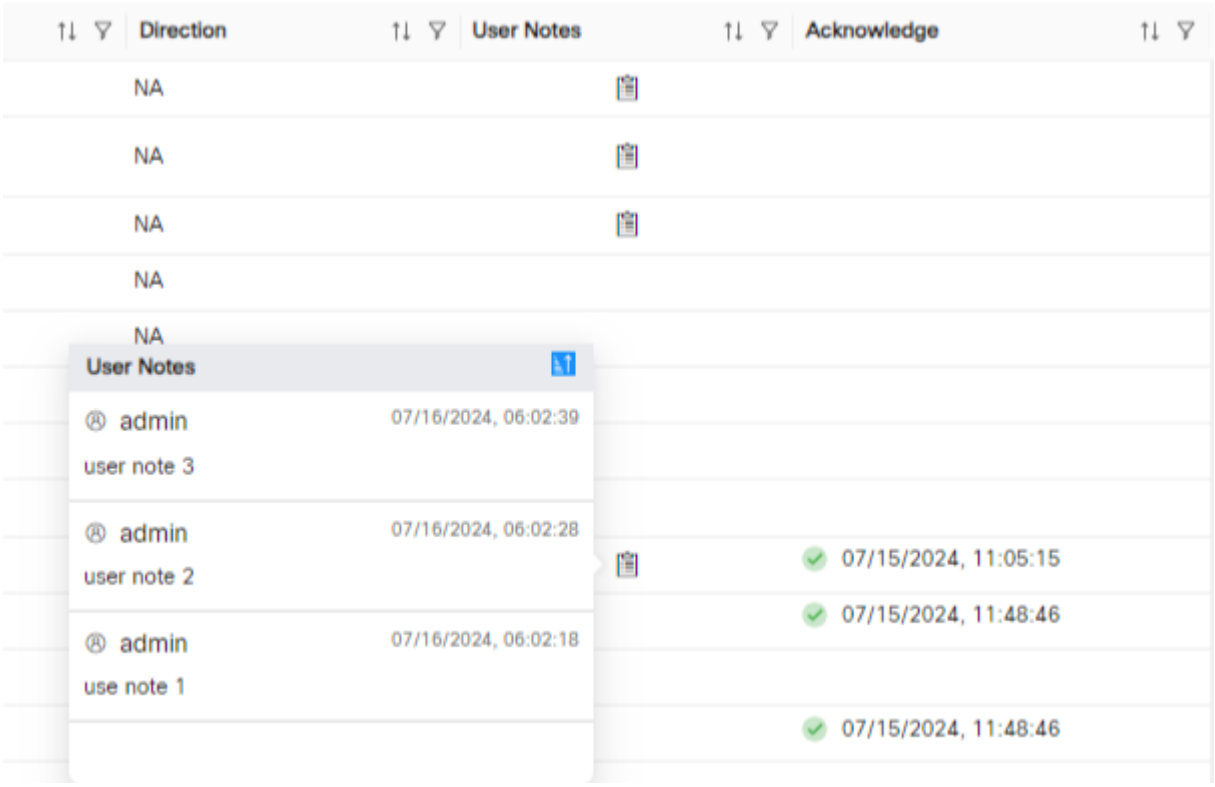
2. Click on **Critical**, **Major**, **Minor**, **Warning**, and **Cleared** alarm types to filter and display the alarms belonging to each type.
3. Use the **Acknowledge** column in the table to view the acknowledged or unacknowledged alarms.

> **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.

4. 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 51: User Notes



The manage alarms task is complete.

8 Workspaces

Topics:

- Launch workspaces
- Circuit Monitoring workspace
- Link Monitoring workspace
- Network Monitoring workspace
- OTN circuits

Covers workspaces in Cisco Optical Network Controller, including launching workspaces, Circuit Monitoring, Link Monitoring, Network Monitoring, OTN circuit discovery, and OTN monitoring workflows.

Covers workspaces in Cisco Optical Network Controller, including launching workspaces, Circuit Monitoring, Link Monitoring, Network Monitoring, OTN circuit discovery, and OTN monitoring workflows.

Covers workspaces in Cisco Optical Network Controller, including launching workspaces, Circuit Monitoring, Link Monitoring, Network Monitoring, OTN circuit discovery, and OTN monitoring workflows.

Launch workspaces

Use this procedure to launch workspaces. The task helps you open focused monitoring and management views for service, network, and operational workflows.

Use this procedure to view launch workspaces in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Note

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

Note

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

Before you begin

Workspaces option allows you to manage different workflows on a daily basis. The multiple standalone applications can interact with each other anytime and are displayed in multiple panels. The workflows available are **Network Monitoring, Link Monitoring,** and **Circuit Monitoring**.

Figure 52: Workspaces

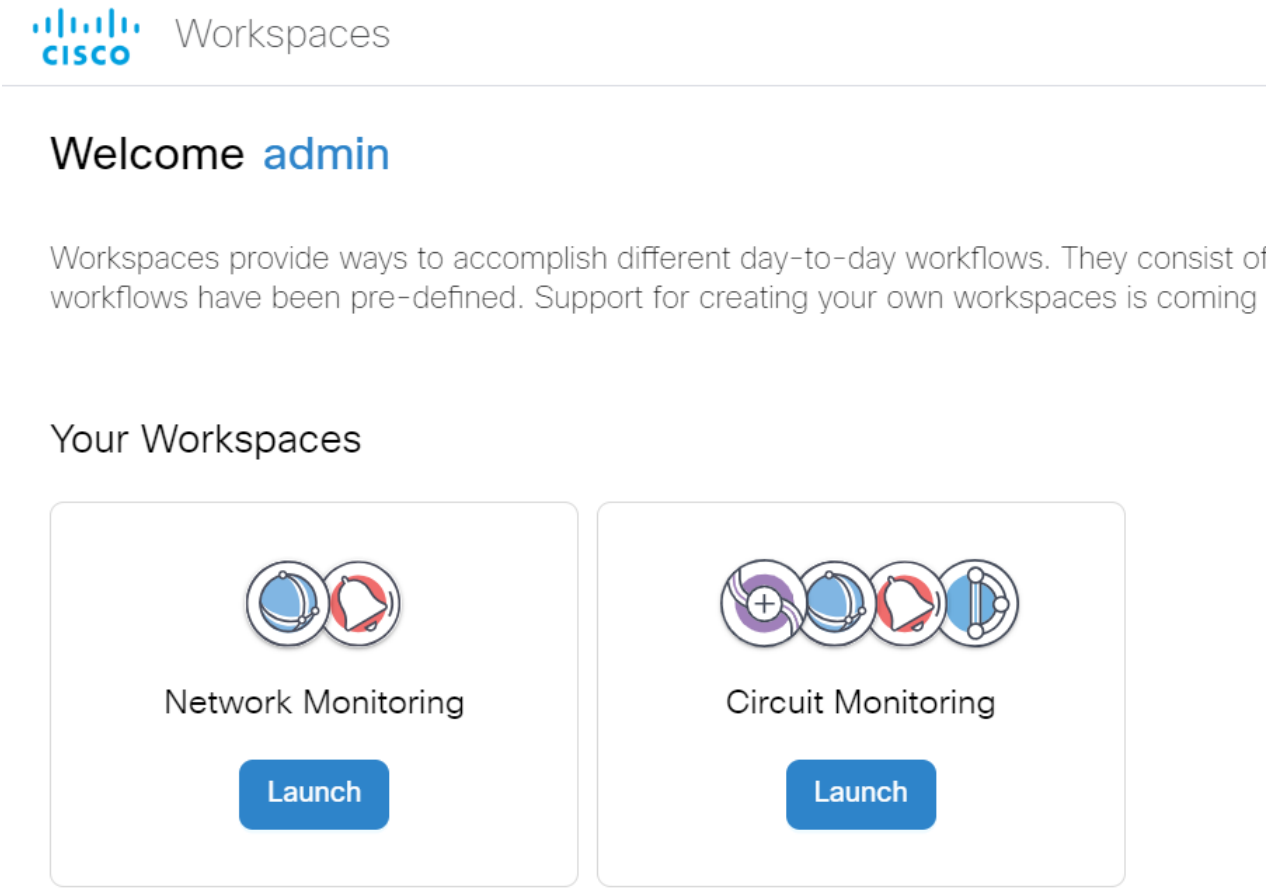
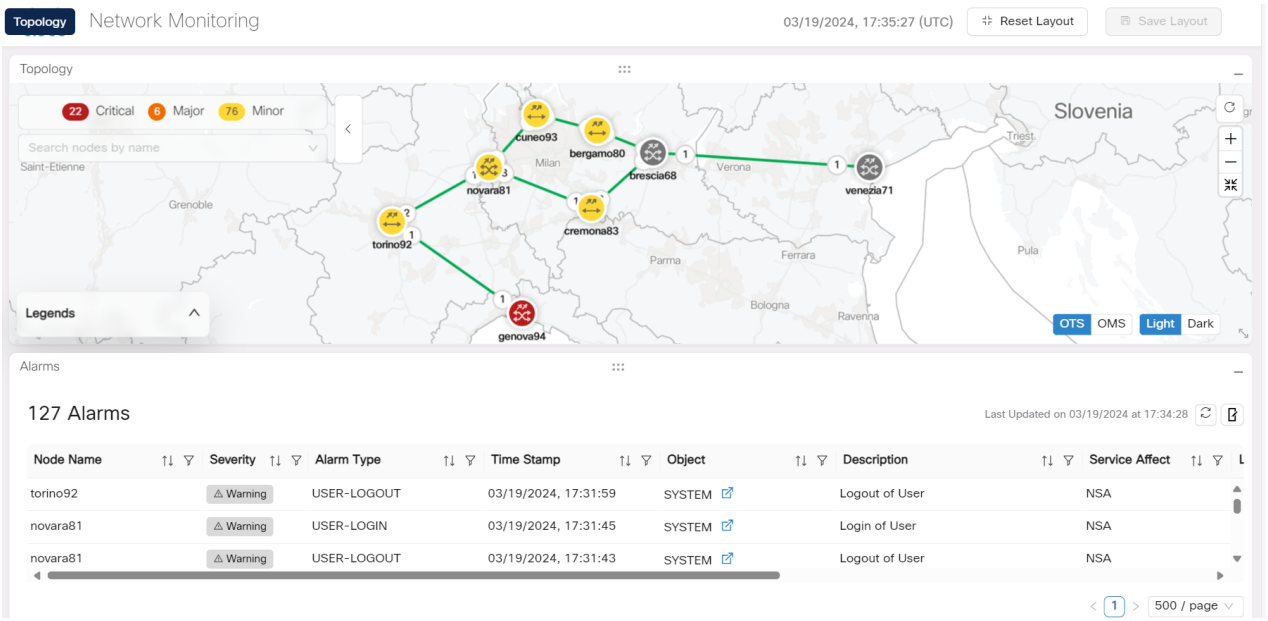


Figure 53: Workspaces Network Monitoring



Note

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

Figure 54: Workspaces Circuit Monitoring

Note

- In the **Topology** screen above, select any node or link and right click followed by **Show service(s)**. This will display all the services related to the selected node or link in the services layout.
- 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 24.3.1 release onwards, PM tab is available in the **Circuit Monitoring** workflow application.
- The IMPROPER-REMOVAL alarm is not displayed in the detailed service path or the alarms table when a circuit is selected.

There can be many such workflows that can be added to the workspace anytime. Also, the workspace panels are dynamic and interactive. By default, we can see the **Alarms**, **Service List**, **Topology** and **Detailed Service Path** panels. These individual panels can be dragged and dropped anywhere on the monitoring screen. They can also be minimized and maximized as necessary anytime.

Note

The alarms displayed here are applicable to the selected services only and not to the entire **Topology**. Also for multi carrier services, alarms are displayed for the selected carrier only.

Follow these steps to view launch workspaces:

Procedure

1. Click **Workspaces** in the left panel.
2. Select the workspace and click **Launch**.
3. Click **Save Layout** to save the layout at any given point in time.
4. Click **Reset Layout** to revert to the default layout.
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.

The view launch workspaces task is complete.

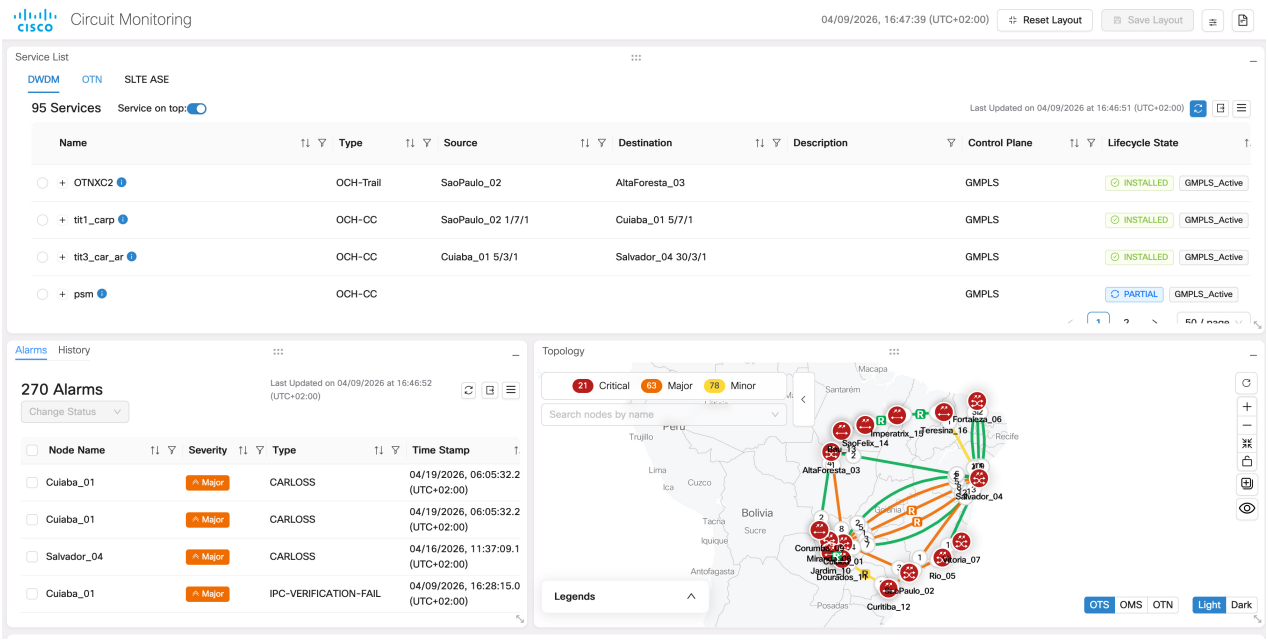
Circuit Monitoring workspace

Provides information about the Circuit Monitoring workspace, including service tabs, OTN circuit fields, SLTE ASE fields, service summaries, topology panels, performance history, and circuit monitoring actions.

Use this reference to understand how the Circuit Monitoring workspace displays circuit paths, associated alarms, performance history, service details, and topology panels.

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

Figure 55: Circuit Monitoring



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

- DWDM–DWDM circuit services

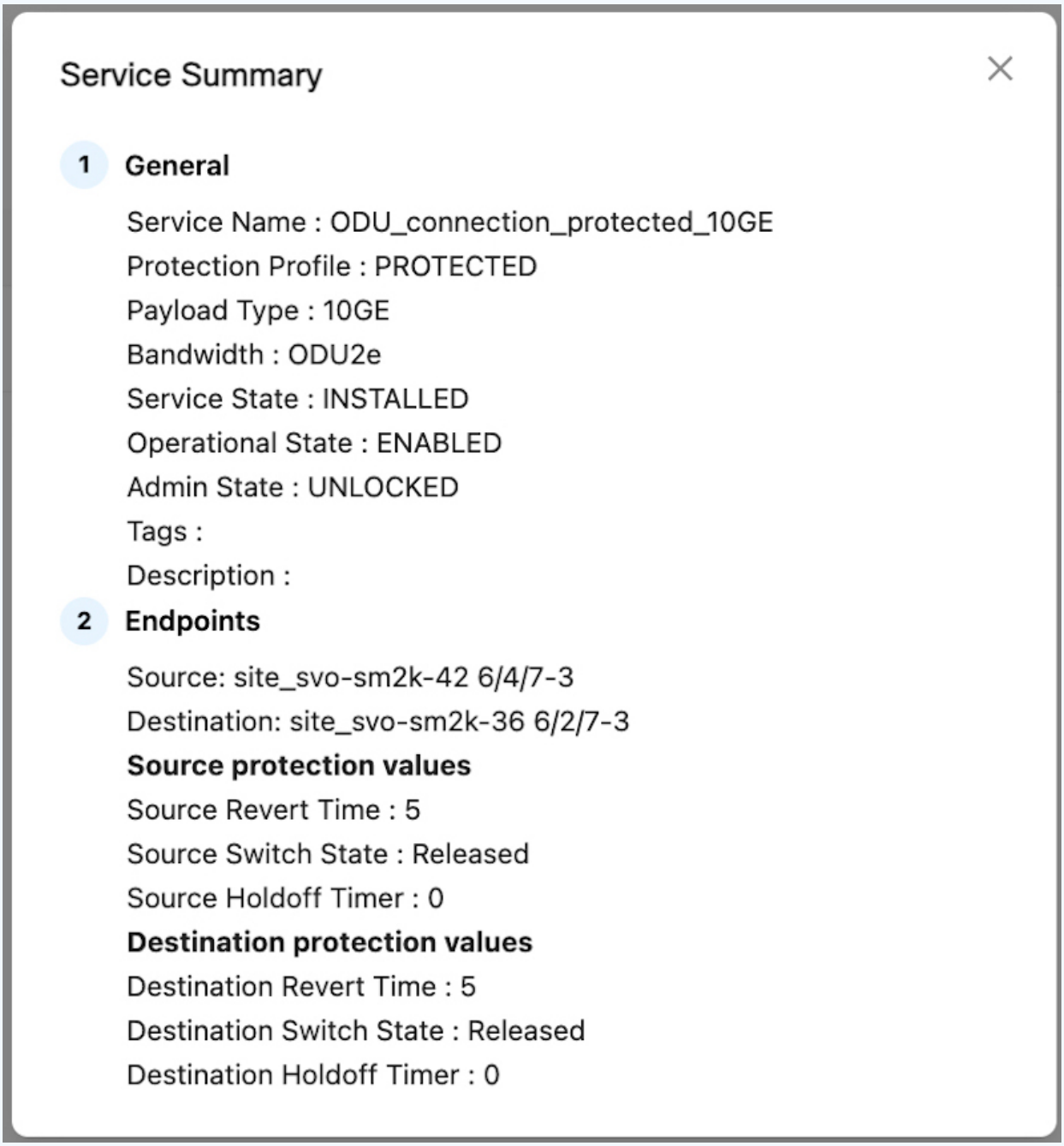
- OTN–OTN circuit services
- SLTE ASE–Submarine circuit services

Note

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

Figure 56: Service Summary

This image is an example of summary for OTN service.



OTN circuit table

The OTN circuit table provides the OTN circuit parameter information.

Table 49: OTN circuit parameter description

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

SLTE ASE table
Table 50: STLE ASE table

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

Alarms table

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

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

Table 51: Alarms table parameters

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

History table

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

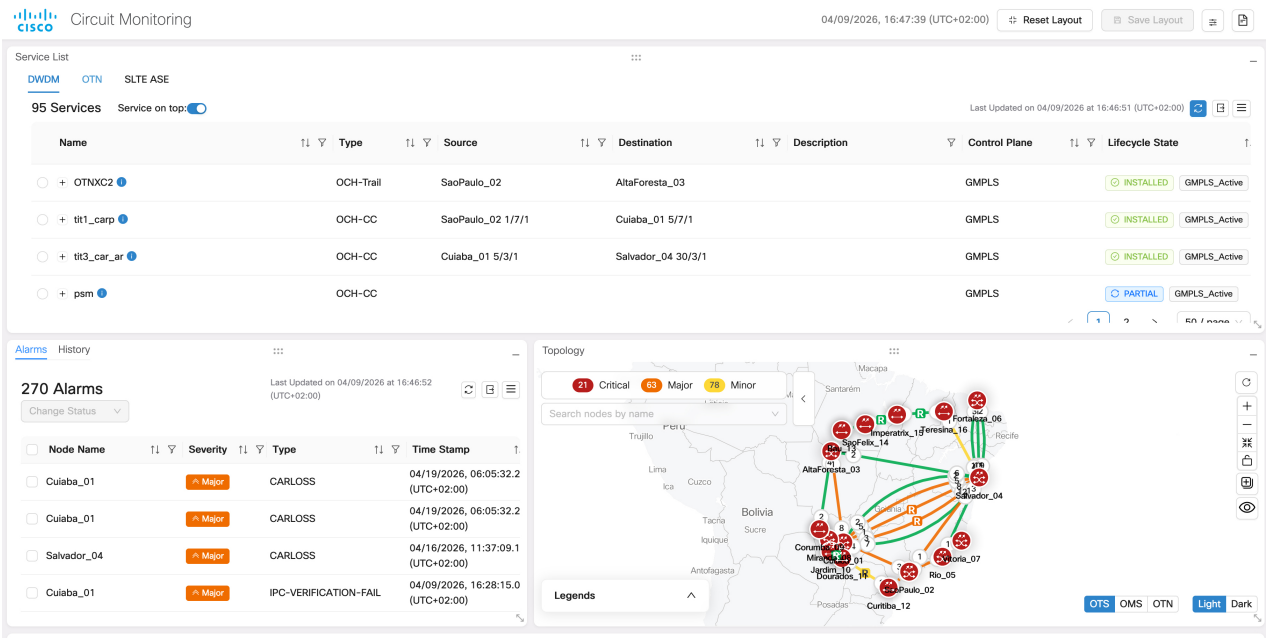
Table 52: Alarms history table parameters

Parameters	Description
Node Name	Name of the node the alarms was raised

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

Release-wise circuit workspace enhancements

Figure 57: Circuit Monitoring



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

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

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

     The history tab displays both cleared and active alarms for the selected circuit within the specified time range.
     - The maximum time period is 3 months. If you select a time range more than 3 months using custom date range, Cisco Optical Network Controller throws an error.
     - Alarm history queries are rate limited. You can query up to 5 alarms history every minute.
- From release 26.1.1, the **Circuit Monitoring** workspace has these enhancements related to OTN.
  - **OTN** tab–New tab in the Services List to check the protected and unprotected services.
  - **OTN** toggle button–New toggle button in Topology pane enables OTN links of the transponder cards.

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

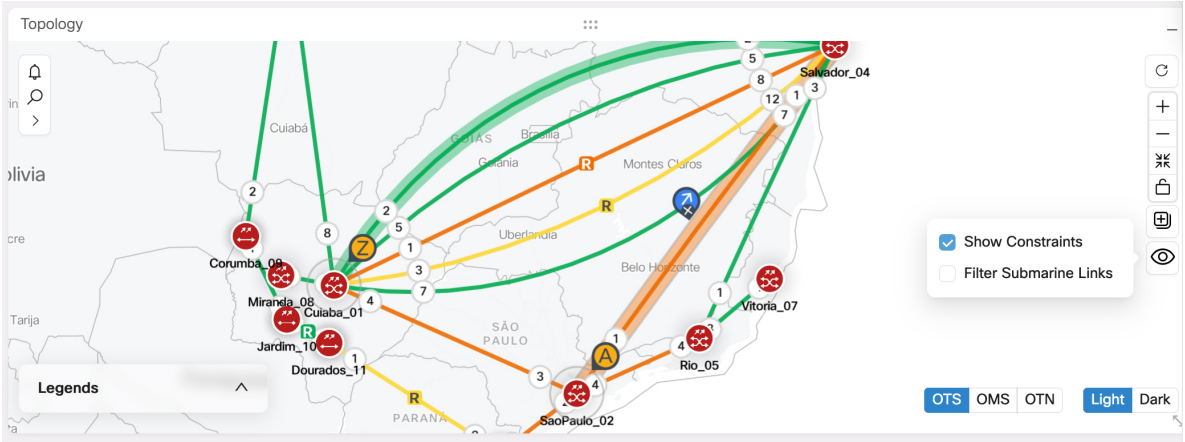
- The *Circuit Monitoring* workspace displays the detailed OTN service path including the OTN clients, OTN trunk, OTU links, and OTN-level alarms, for example, OTN interface alarms and service history specific to OTN service.

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

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

   The active circuit path with constraint is highlighted.

   Figure 58: Show Constraints



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

   Figure 59: Constraints Legends

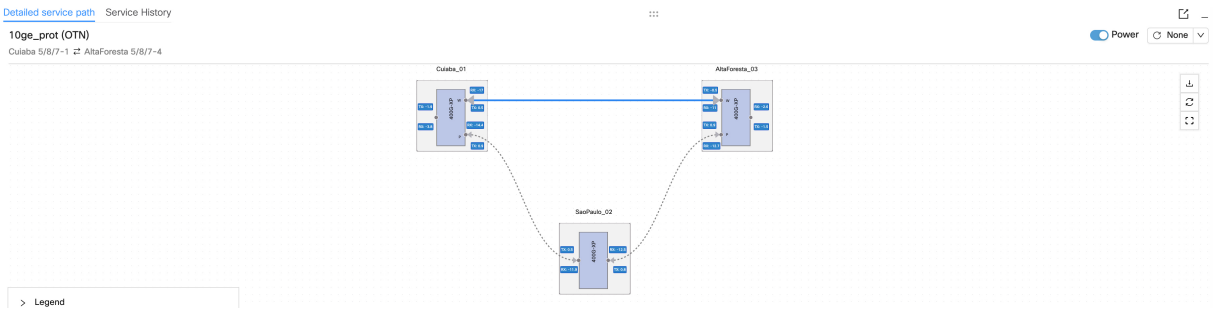
Detailed service path

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

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

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

  Figure 60: Power toggle switch

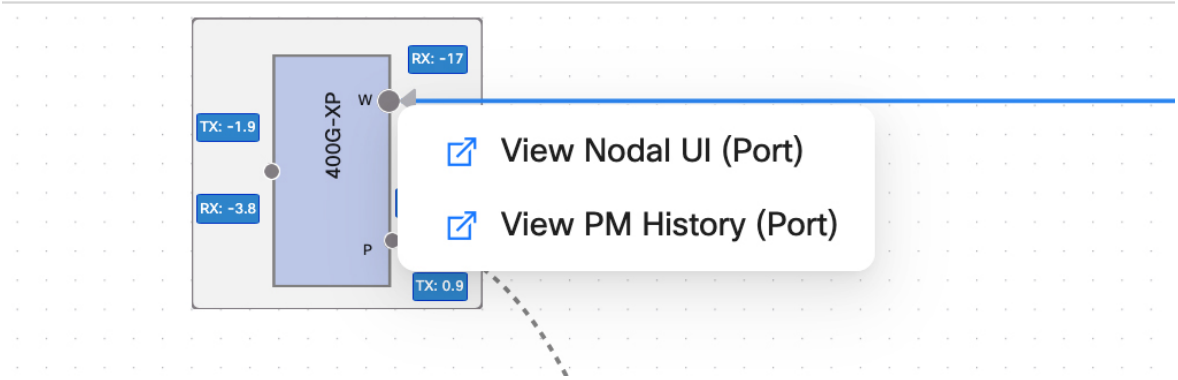


- Hover over a port or equipment in the detailed service path to view a tooltip. The tooltip displays W and P that specify the working and protected path for protected OTN service and source and destination ODU port information.

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

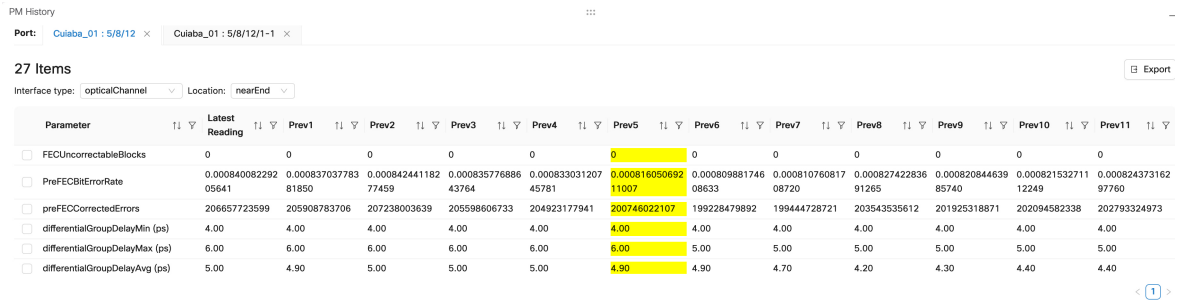
- PM history
  - Select a service from the service list.
  - From detailed service path, right click a port and choose View PM history.

    Figure 61: Port pop-up options



The PM History in Circuit monitoring appears.

Figure 62: PM History in Circuit workspace

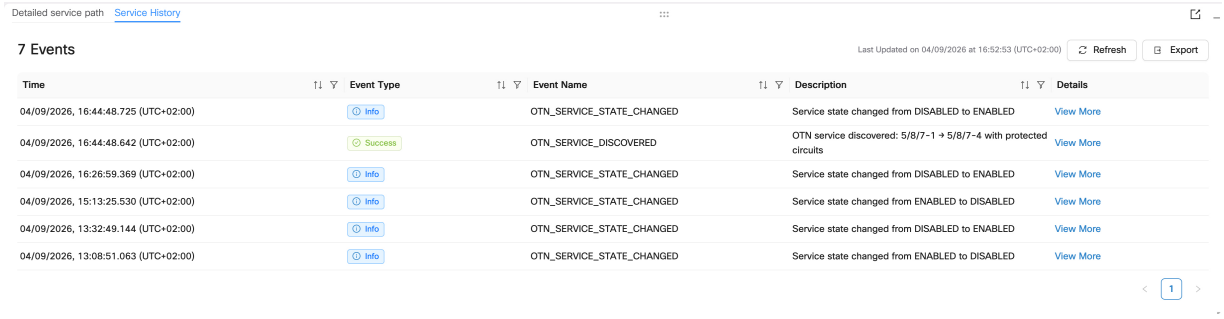


- **Interface type** drop-down list: By default, only one interface type is used to generate the report for the selected port. However, if the port has multiple interface types, you can choose the interface type from the drop-down.
- **Location** drop-down list: You can choose to view the PM history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

Service History

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

Figure 63: Service history table



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

Topology panel

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

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

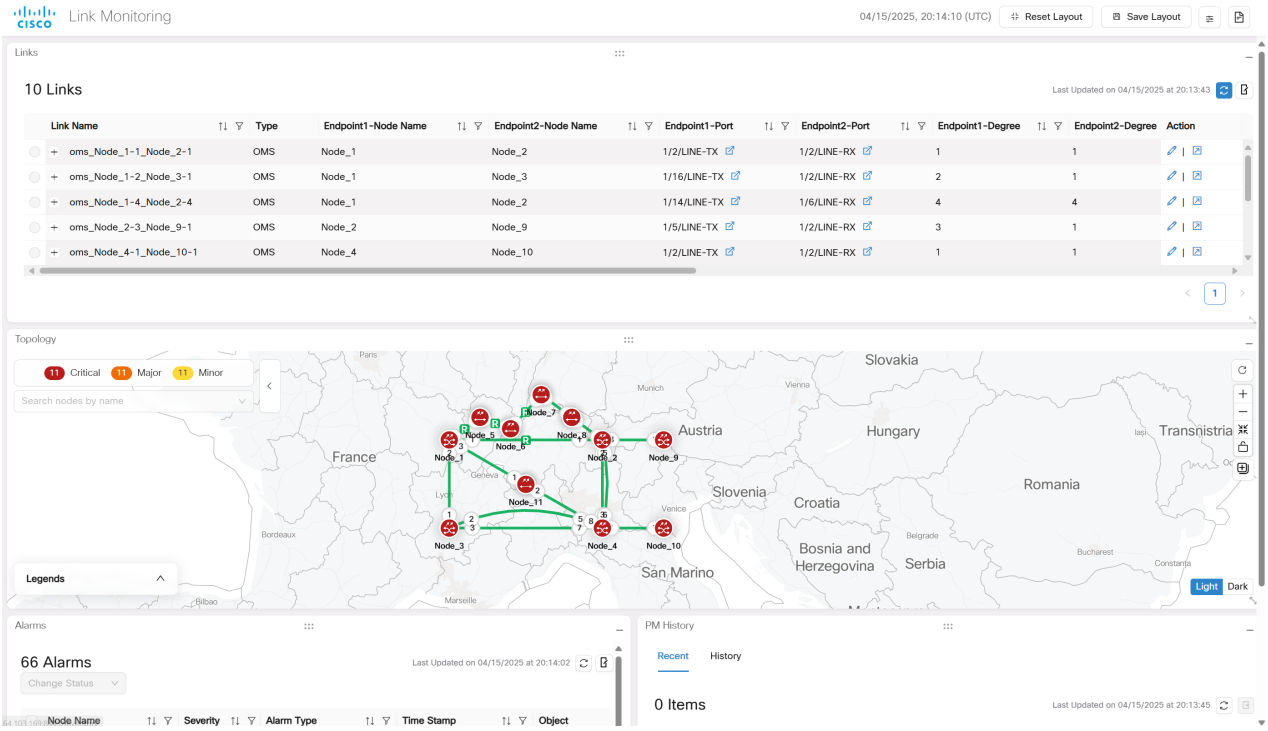
Link Monitoring workspace

Provides information about the Link Monitoring workspace, including link filtering, OMS and OTN link fields, link alarms, PM history, topology options, and circuit navigation.

Use this reference to understand how the Link Monitoring workspace displays link alarms, performance history, topology context, and associated circuits.

Links monitoring workspace functionalities

Figure 64: Link Monitoring workspace



The Link Monitoring workspace provides these functions:

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

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

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

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

OMS Links tab

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

Table 53: OMS Links table parameters

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

Link Monitoring workspace options

These action icons and button improve your interaction with the table

- **Collapse All** button–Collapses the expands tables.
- Refresh icon–Refreshes the table data.
- Export icon–Exports the table view and network report in excel.
- Column preferences icon–Enables display or removal of columns in the table.

OTN Links tab

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

Table 54: OMS Links table parameters

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

Alarms tab

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

Table 55: Alarms table parameters

Parameters	Description
Node Name	Name of the node on which the alarm is raised
Device Object Name	Name of the device object
Severity	Severity of the alarm
Type	Type of alarm
Time Stamp	Time stamp of the alarm
Object	Logical object of the alarm
Description	Description of the alarm
Category	Alarm category
Service Affect	Marks the alarm as service affecting or non service affecting
Location	Location of the node where the alarm is raised
Direction	Direction of the alarm
User Tag	User-defined tags

Parameters	Description
User Notes	User-defined notes
Acknowledge	Acknowledge or unacknowledged the alarms
UUID	Unique ID of the device
Transient	Transient or non-transient alarm
Correlation Type	Correlation type
Ru Position	Rack unit position of the device
Rack ID	Rack ID of the device
Low Device Name	Low device name

Alarm history tab

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

Table 56: Alarms history table parameters

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

PM History pane

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

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

Table 57: PM history table parameters

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

Topology pane

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

- Light/Dark toggle buttons–Allows switching between light and dark themes.
- Legends–Represents the Nodes, Links, States and Node Resync in a visual format
- Map view icons–Allows zoom in, zoom out, reset and lock default view functions
- Select links icon–Selects the discovered OMS links
- Map view options icon–Pops up **Filter Submarine Links** check box to display submarine links only in the map.

Table 58: PM history table parameters

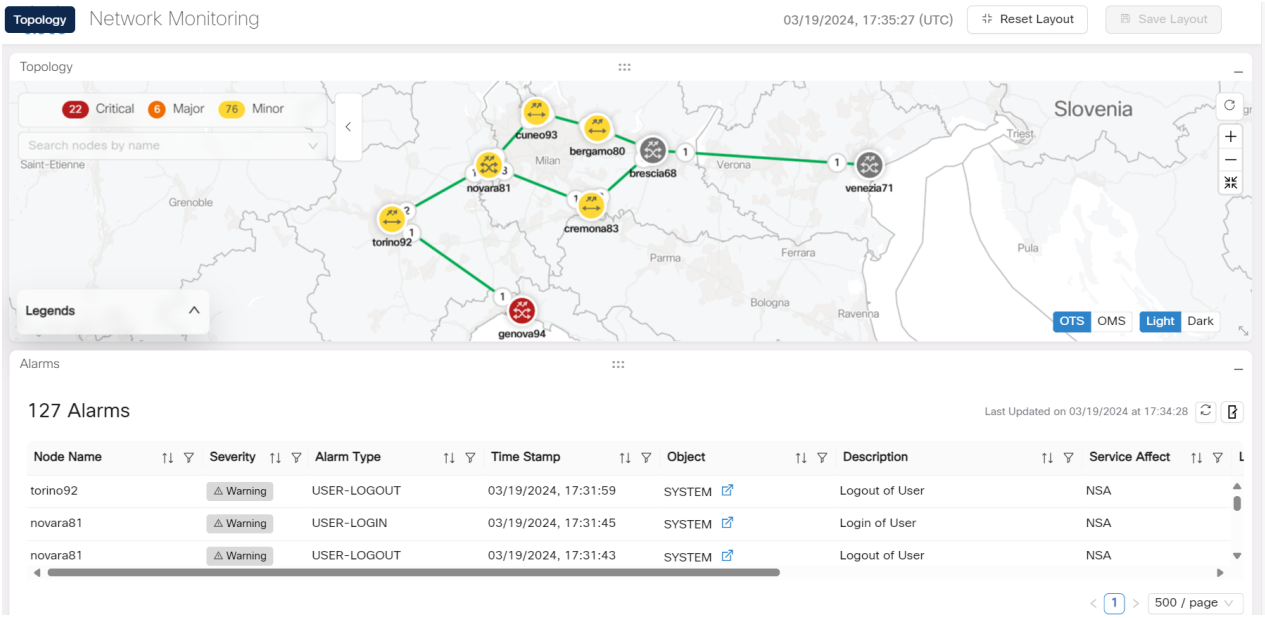
Parameters	Description
Optical Link	Name of the optical link
Span Loss	Link span loss between the source and destination node
Measured By	Entity measured for PM data
Measured Time	PM data reported time

Network Monitoring workspace

Provides information about the Network Monitoring workspace, including topology-based alarm details, node and link selection behavior, and Probe-enabled link monitoring.

Use this reference to understand how the Network Monitoring workspace displays topology-based alarms, node status, link status, and Probe-enabled link details.

Figure 65: Network monitoring workspace screen



Note

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

OTN circuits

Explains OTN circuit discovery and monitoring in Cisco Optical Network Controller, including protected and unprotected circuits, service discovery, link utilization, service history, and detailed service paths.

An OTN circuit is a logical transport connection that

- uses pre-existing GMPLS OCH trails that are created on an NCS2K-400G-XP-LC card in OTN-XC card mode,
- appears in Service Manager, topology views, and the Circuit Monitoring workspace, and
- supports protected circuits with a standby protection path and unprotected circuits with a single active path.

OTN circuit discovery scope

Cisco Optical Network Controller supports brownfield discovery of OTN circuits that are already provisioned on the network using CTC or other tools.

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

OTN circuit types and topology representation

Explains how Cisco Optical Network Controller represents protected and unprotected OTN circuits, including working paths, standby paths, and OTN and OTS topology layer visibility.

An OTN circuit is a logical transport connection that

- carries client traffic over an OTN layer that runs on GMPLS OCH trails,
- is discovered and displayed by Cisco Optical Network Controller as a protected or unprotected circuit, and
- shows the active working path, protection standby path, underlying OCH trail, and OTS physical route.

OTN topology layers and circuit path visualization

Cisco Optical Network Controller provides two topology layers for OTN visibility:

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

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

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

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

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

This table compares OTN and OTS topology layer visibility.

Table 59: OTN versus OTS topology layer comparison

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

Discover OTN services for NCS2K-400G-XP-LC card in Service Manager

Use this procedure to discover OTN services for an NCS2K-400G-XP-LC line card in Service Manager after configuring OTN-XC card mode and creating an OCH-Trail GMPLS circuit.

Discover OTN services for an NCS2K-400G-XP-LC line card in Service Manager.

In release 26.1.1, OTN services are supported in the OTN-XC card mode of the NCS2K-400G-XP-LC line card. Use this procedure to discover OTN services for the NCS2K-400G-XP-LC line card.

> **Note**
>
> Use this procedure if you have not created an OCH-Trail GMPLS circuit for the NCS2K-400G-XP-LC line card in CTC.

Follow these steps to discover OTN services for an NCS2K-400G-XP-LC line card:

Procedure

1. Configure the OTN-XC card mode on trunk ports 11 and 12 in the NCS2K-400G-XP-LC line card.

   In the **Nodes** screen, click the IP address of the node and provision the OTN-XC card mode in Cisco Optical Site Manager.

2. Create an OCH-Trail GMPLS circuit in Cisco Optical Network Controller or CTC.

OTN services for the NCS2K-400G-XP-LC line card are visible in the OTN tab.

Monitor OTN circuits

Use this procedure to monitor OTN circuit status, active routes, protection status, and alarms for protected and unprotected OTN circuits in the Circuit Monitoring workspace.

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

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

Before you begin

OTN circuits are provisioned using CTC or other tools and discovered and displayed in Cisco Optical Network Controller on the **OTN** tab in Service Manager.

Follow these steps to monitor OTN circuits:

Procedure

1. Open the Circuit Monitoring workspace.

   Go to **Workspaces** > **Circuit Monitoring** > **Launch**.

   The circuit monitoring workspace appears displaying trails and OTN circuits in the topology panel. Trails are shown in the OTN layer and serve as the underlying transport on which OTN circuits are built.

2. Click the **OTN** toggle button in the topology to display OTN circuits.

   The OTN topology shows the OTN links and circuits between endpoint nodes. You can switch between the OTS and OTN layers using the layer selector buttons in the topology panel.

3. Select an OTN circuit to open the detailed service panel.

For a protected circuit, the circuit detailed service panel shows:

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

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

4. Right-click a node or card in the Cisco Optical Network Controller topology and choose **View in Nodal UI** to open the component in Cisco Optical Site Manager.

   Cisco Optical Network Controller opens the Cisco Optical Site Manager interface at the specific card location. From Cisco Optical Site Manager, you can perform maintenance operations such as protection switching. Direct protection switching from the Cisco Optical Network Controller web UI is not available in Release 26.1.1.

5. Right-click a node or card in the Cisco Optical Network Controller topology and choose **View PM History (port)** to view performance monitoring graphs for a specific port.

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

   These PM data types are available on trunk ports:

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

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

Monitor OTN link utilization

Use this procedure to monitor OTN link utilization, review bandwidth consumption across OTN links, and export utilization data to Excel for offline analysis.

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

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

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

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

Follow these steps to monitor OTN link utilization:

Procedure

1. Open the link utilization view in the OTN link monitoring workspace or Links app.

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

   The Link Monitoring workspace displays all OMS links. Go to the **OTN Links** tab.

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

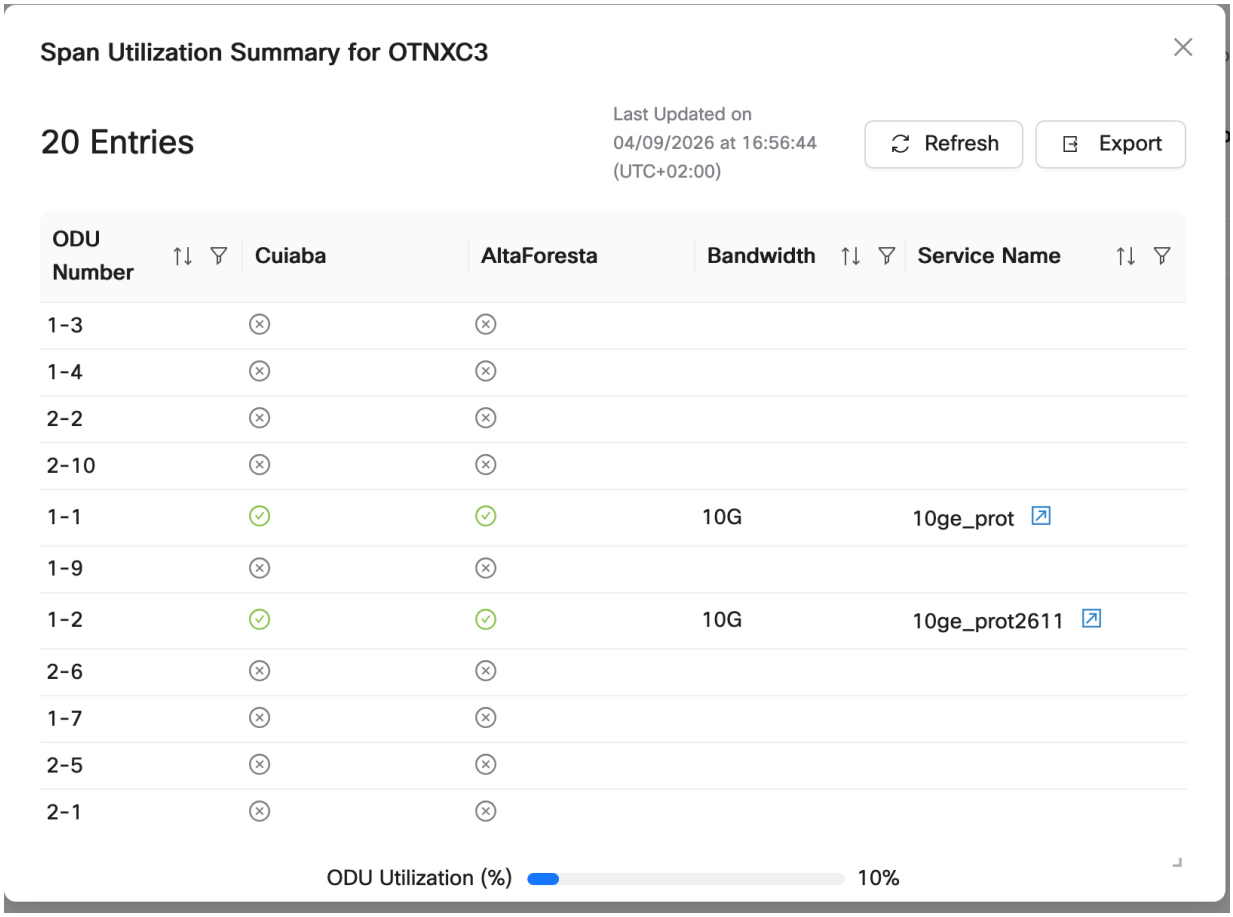
   The Links app opens and displays the OMS tab. Go to the **OTN** tab.

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

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

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

   Figure 66: Complete span utilization summary



3. Review the utilization percentage for each OTN link.

   The table displays these parameters for each link:

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

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

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

View OTN service event history

Use this procedure to view OTN service event history, review protection state changes and discovery events, and export the event log to Excel.

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

The service history for an OTN circuit displays a table of events associated with that circuit. Events are classified by event type, such as *success* or *info*. In Release 26.1.1, success events are generated only for initial discovery events, when the OTN service is first created. Protection switch events and state changes are reported as info events. The event table supports column resizing and export to Excel.

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

Follow these steps to view OTN service event history:

Procedure

---

1. In the circuit monitoring workspace, select an OTN circuit from the circuit list.

   The circuit detailed service list panel opens, showing topology, path information, and available tabs including service history.

2. Click the **Service History** tab to view the event log for the selected circuit.

   The event table displays these columns:

   - Timestamp: The date and time of the event (displayed in UTC)
   - Event name: A description of the event, such as protection state change or successful discovery
   - Event type: Classifies the event as success, info, or neutral
   - More details: A link to additional event details, if available

   You can resize columns by dragging the column header borders.

   The service event history table loads, showing all events recorded for the selected OTN circuit.

3. (Optional) Click the **Export** icon in the service history toolbar to export the event history.

   The event history is exported to an Excel file containing all event records currently visible in the table.

You can review the complete event history for the selected OTN circuit and export the log to Excel for offline analysis or audit purposes.

9 Service Assurance

Topics:

- View Service Assurance details
- View PSM circuits in Service Assurance
- Unmanaged equipment
- PSM OMS protection

Provides information about Service Assurance in Cisco Optical Network Controller, including service paths, PSM circuits, unmanaged equipment, and service monitoring details.

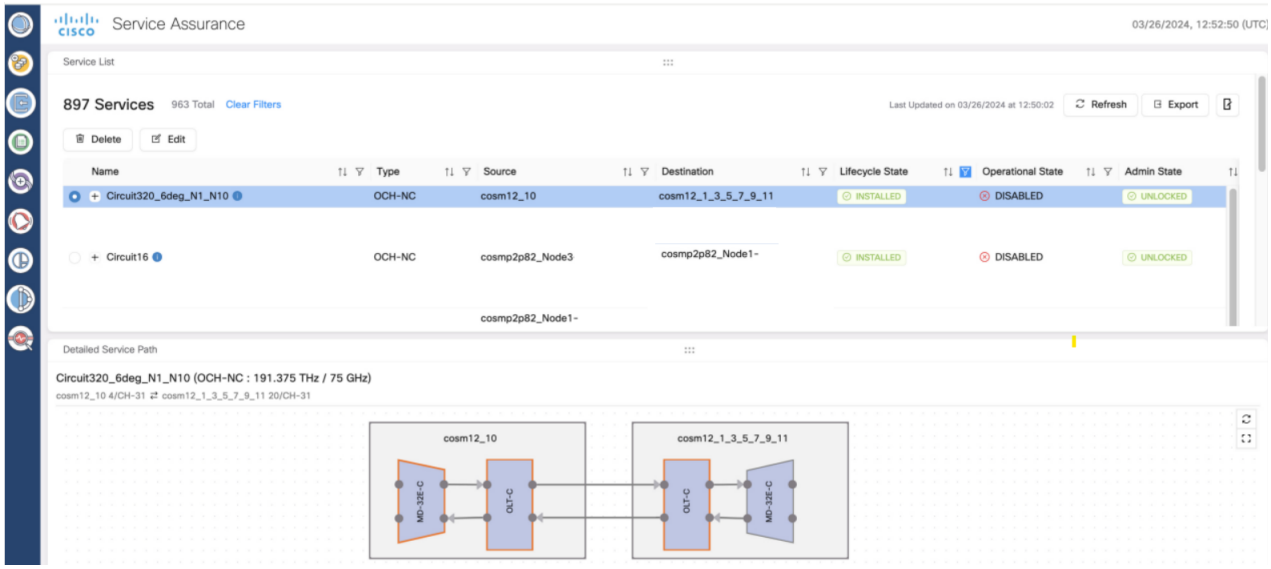
View Service Assurance details

Use this procedure to view Service Assurance details. The Service Assurance application visualizes circuits, related nodes, links, circuit paths, and live PM details for installed services.

Use this procedure to view service details, circuit paths, related nodes, links, and live PM information in the Service Assurance application.

The Service Assurance application visualizes circuits, related nodes, links, circuit paths, and live PM details for installed services.

Figure 67: Service Assurance



Before you begin

Follow these steps to view Service Assurance details:

Procedure

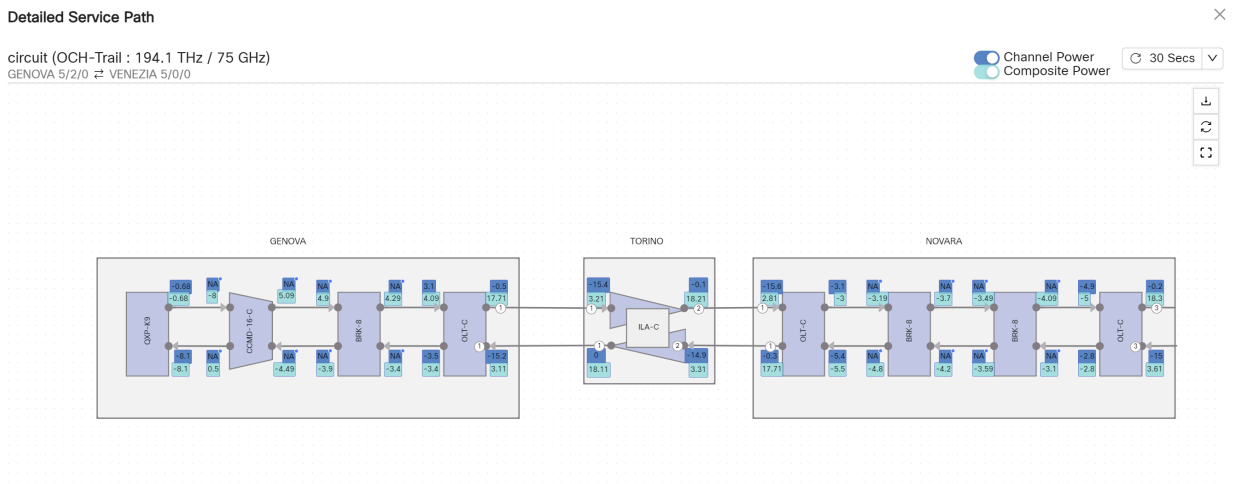
1. Click **Service Assurance** in the left panel.
2. Select the service from the **Service List**.
3. In the **Detailed Service Path** layout, you can view the service details by hovering over the visual circuit for each node, ports, links, and paths of any service at any given time. These details are available when the **Lifecycle State** is either **INSTALLED** or **DELETION FAILED**.

   From Cisco Optical Network Controller 24.3.1 release onwards:

   - Live PM information is enabled on the visual circuit. The tool tip is enabled to display these details when it is hovered over the nodes and internal ports visible in the **Detailed Service Path** circuits.
   - The new features include **Composite Power** and **Channel Power** values, which can be enabled using the toggle button options provided and refreshed at different time intervals as per requirement.
   - The tool tip for each port also displays the channel power, estimated channel power, composite power, and estimated composite power values.
   - Live PM values for greenfield and brownfield circuits are available.

4. Click **Export** to export the details of the table from the screen to a spreadsheet file.

Figure 68: Live PM Channel and Composite Power Values



Note

- You can use the fit to screen option provided in the **Detailed Service Path** screen.
- **NA** is displayed for not applicable ports on live PM.
- You can use the cursor to point to every port used by the circuit and view the service state, alarm summary, and the live power summary. It is also possible to cross-launch to COSM UI for any selected port.

5. Click **Refresh** to refresh live PM data at the required rate or interval.

The Service Assurance application displays the selected service path and related live PM details.

View PSM circuits in Service Assurance

Use this procedure to view PSM circuits in Service Assurance. You can view the selected PSM circuit path in the Detailed Service Path screen and cross-launch Cisco Optical Site Manager for target PSM equipment.

Use this procedure to view PSM circuit paths and cross-launch Cisco Optical Site Manager from the Service Assurance application for protection-switch operations.

You can view the selected PSM circuit path in the Detailed Service Path screen and cross-launch Cisco Optical Site Manager for target PSM equipment.

Before you begin

Follow these steps to view PSM circuits in Service Assurance:

Procedure

1. Select the PSM circuit you created from **Services**.
2. Click on the **Detailed Service Path** screen.

The PSM path is displayed in the circuit. You can also cross-launch Cisco Optical Site Manager from the selected equipment.

> **Note**
>
> You can cross-launch Cisco Optical Site Manager on target PSM equipment to run the Protection Switch command.

The Service Assurance application displays the selected PSM circuit path.

Unmanaged equipment

This section explains unmanaged equipment, including discovery behavior and equipment representation. Use it to understand how Cisco Optical Network Controller handles devices without full management context.

Unmanaged equipment is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Unmanaged equipment details

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

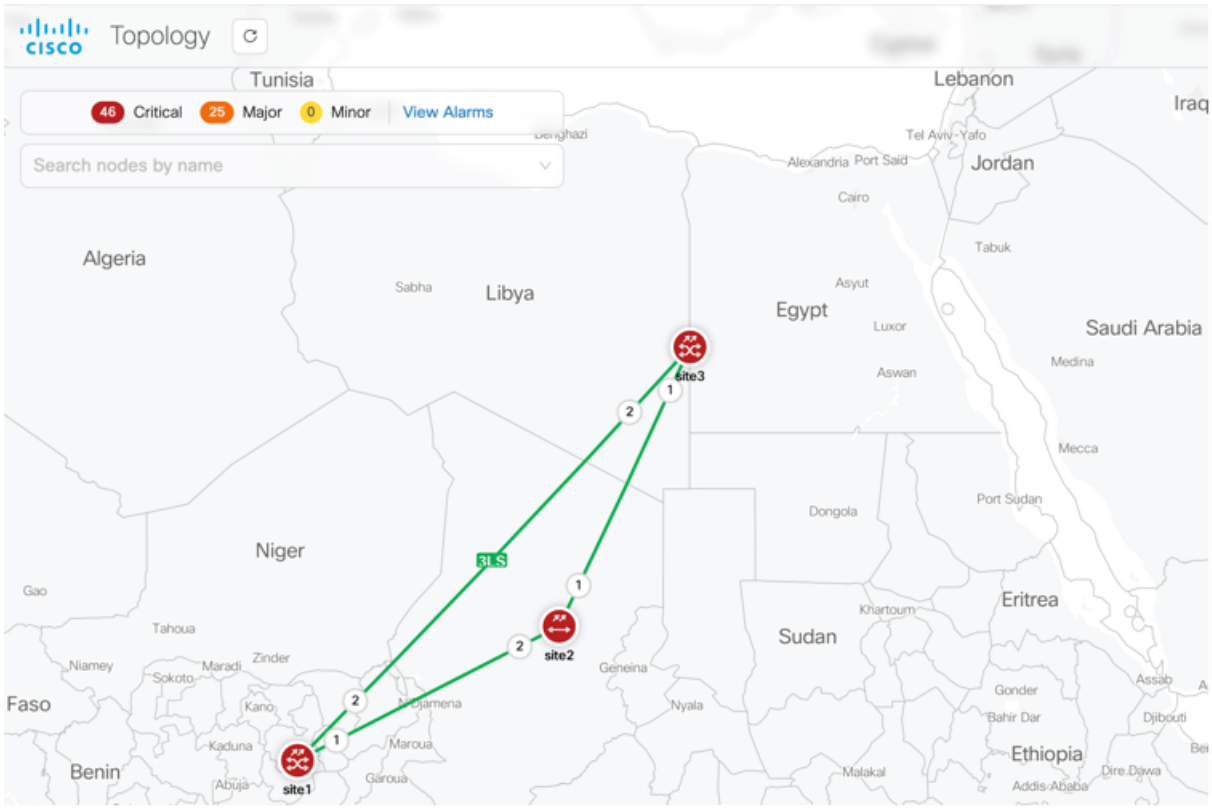
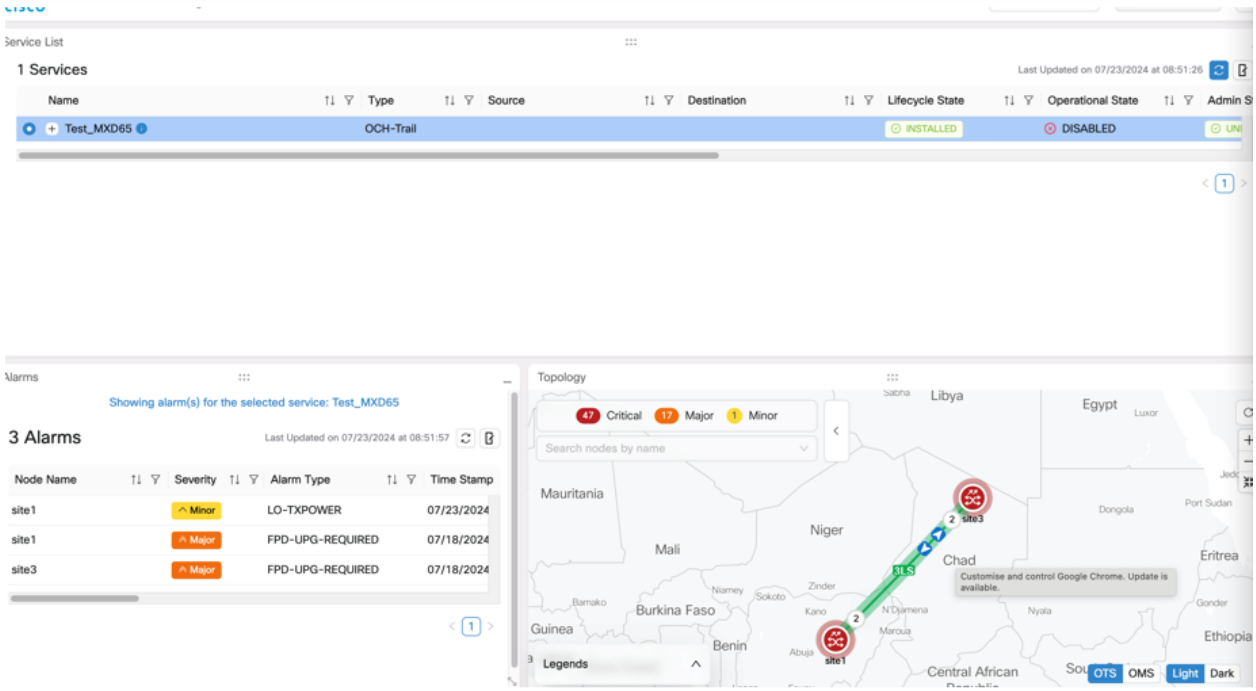


Figure 70: Unmanaged Equipment Support in Service Assurance



PSM OMS protection

This section explains PSM OMS protection, including protection behavior and supported topology conditions. Use it to understand how Cisco Optical Network Controller represents protected PSM fiber paths.

PSM OMS protection is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

PSM OMS protection details

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

Note

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

Configuration in PSM Circuits

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

Note

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

Benefits of PSM

The benefits of using PSM are:

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

Note

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

Additional PSM functions

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

PSM Circuit in Service Manager

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

Limitations of PSM OMS protection

- Cisco Optical Network Controller does not support 3-way PSM Protection switching.
- The W-RX and P-RX thresholds for the NCS 1001 PSM must be set carefully based on the number of channels. If the number of channels is lower, a significant power drop from one channel going off may cause the PSM to switch, leading to traffic hits on other channels. See **Configuration Guide for Cisco NCS 1001**
- Cisco Optical Network Controller does not display the Reason for switchover.
- Cisco Optical Network Controller supports only configurations with amplifiers positioned after the PSM module. OMS protection is not supported.

- You must perform a resync if you onboard devices, add or modify IPCs, or add or remove degrees to the network after onboarding the PSM.
- If the same network is being managed by two separate active Cisco Optical Network Controller instances, the same connection service, either a discovered service in both instances, or a service provisioned in one and discovered in the other, must be deleted on both instances for all types of connection services.

View PSM circuits in the workspace

Use this procedure to view PSM circuits in the workspace. The task helps you open selected PSM circuit details and review the related service path.

Use this procedure to view PSM circuits in the workspace in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

To view the selected PSM circuit follow the steps:

Before you begin

Follow these steps to view PSM circuits in the workspace:

Procedure

1. Click **Workspace** option on the left panel.
2. In **Circuit Monitoring**, click **Launch**.
3. Select the PSM circuit.

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

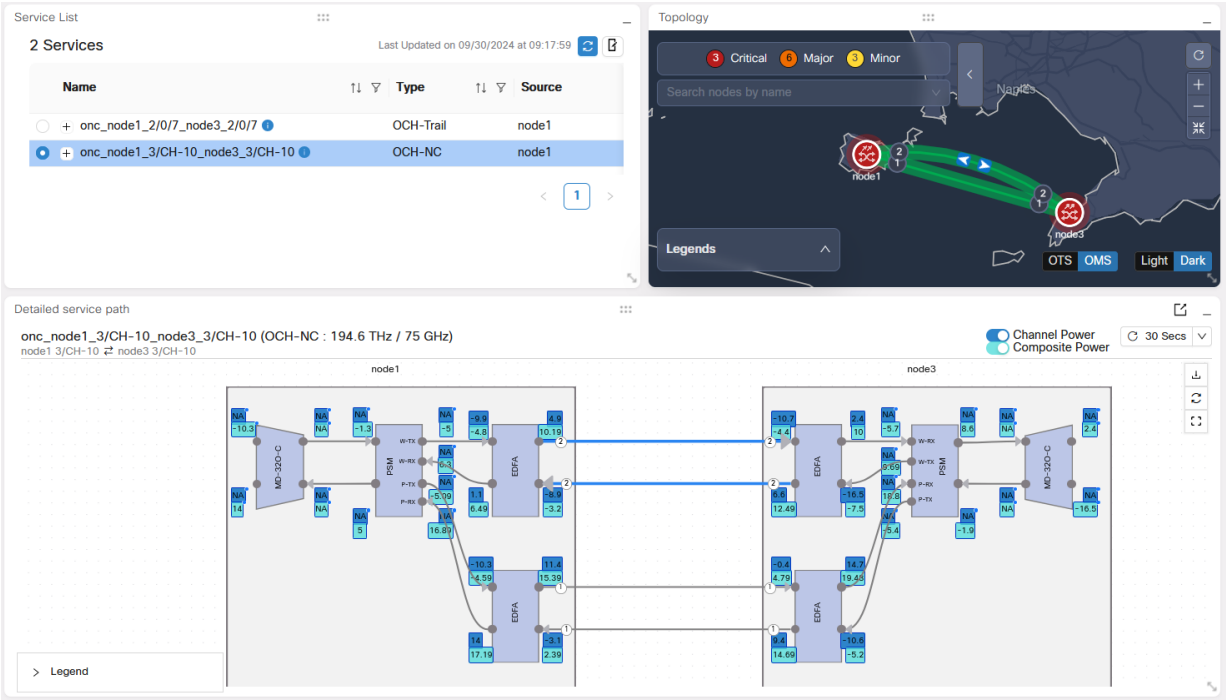
Note

- The **Detailed Service Path** displays all the equipments crossed by the circuit. The active path appears in blue and the standby path in grey color.
- The blue arrows indicate the RX direction of the light for a given PSM.

Note

- From Release 26.1.1, the NCS 1001 PSM Circuit Workspace has these UI enhancements.
- The **Detailed Service Path**.
- Highlights the active path between the NCS 1001 PSM nodes.
- Displays the equipment between the NCS 1010 OLT nodes as a cloud.
- From R26.1.1, service history is now enabled for PSM service to show discovery events, operation state changes, and switch events.
- In the **Service List** pane, the OCH-Trail services for NCS 1001 PSM cover the carrier (wavelength) information and add these new labels to each provisioned channel.
- Work–Channel passing through nominal Work port of PSM.
- Protect–Channel passing through nominal Protect port of PSM.
- Forward–Traffic flow from node A to Node Z ,where Node A is the Source Node.
- Reverse–Traffic flow from node Z to Node A ,where Node Z is the Source Node.
- Active–This label is added before the Forward/Reverse labels to indicate that the channel is carrying traffic in that Forward/Reverse direction.
- Standby–Channel that is not carrying any traffic

Figure 71: PSM Circuit in Workspace



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

The view PSM circuits in the workspace task is complete.

PSM wavelength protection

This section provides details about PSM wavelength protection, including protection characteristics, discovery behavior, and supported brownfield network conditions. Use it to understand how protected PSM links are represented.

Use this reference to understand PSM wavelength protection.

Details about PSM wavelength protection.

Table 60: Feature History

Feature Name	Release Information	Feature Description
Two-way PSM wavelength protection	Release 26.1.1	PSM wavelength protection is connecting the NCS 1001 PSM module COM port with the transponder trunk port. PSM wavelength protection supports two-way protection switching in optical circuits with NCS 1010 ILA modules between NCS 1010 OLT nodes. PSM wavelength protection does not support three-way and four-way switching. The Circuit Monitoring workspace UI is improved with for the PSM wavelength protection. • Only brownfield circuit discovery is supported. • In Services List pane, OCH-Trail services are added if an IPC between transponders and NCS 1001 PSM COM port is present. If IPC is not present, then PSM services are discovered as OCH-NC. • Onboard the node containing the PSM through Cisco Optical Network Controller to discover the circuit present in Cisco Optical Site Manager device. • In Services List pane, new labels are added to indicate the work and protect channels. The new labels are Work, Protect, Forward direction, Reverse direction, Active, Standby. • In Topology pane, the equipment connected between two NCS 1010 OLT nodes are represented as a cloud for a concise view. You can expand the cloud to check the equipment added between the two NCS 1010 OLT nodes.

PSM wavelength protection details

PSM wavelength protection is connecting the NCS 1001 PSM module COM port with the transponder trunk port.

Characteristics of PSM wavelength protection

Cisco Optical Network Controller supports only brownfield network. You can only discover the PSM wavelength protection services as OCH-NC and OCH-Trail. To discover or add nodes to the PSM wavelength protection services, see . Cisco Optical Network Controller does not support greenfield circuits, that is, circuit creation by selecting two endpoints in the circuit creation wizard in CONC service manager. From Cisco Optical Network Controller, you cannot create new PSM services. Create cross-connect between PSM COM port and LINE port using CLI and onboard them to COSM, then onboard all these nodes to CONC. Service discovery - Once your onboard all the COSM nodes with cross connects, then the CONC discovers the PSM services and displays in the service list. The listed services are tagged with Active, Standby, Protect, Work, Forward and Reverse. PSM switching is unidirectional and bidirectional, CONC will show both unidirectional and bidirectional services based on the Active and Standby labels. PSM switching supports only Centralized control plane circuits (CPCE) circuits. CPCE circuits are service-level circuits managed by Cisco Optical Network Controller using PCE for path computation and provisioning. In Circuit Monitoring workspace, you can check the service, detailed service path, and service history. PSM module is supported by Cisco Optical Network Controller only on the NCS 1001 chassis. NCS 1001 is supported only if it is managed by a COSM instance running over a NCS 1014 chassis.

Note

- Cisco Optical Network Controller supports only brownfield network. You can only discover the PSM wavelength protection services as OCH-NC and OCH-Trail. To discover or add nodes to the PSM wavelength protection services, see #unique_79/unique_79_Connect_42_section_gmh_pg2_y3c.
- Cisco Optical Network Controller does not support greenfield circuits, that is, circuit creation by selecting two endpoints in the circuit creation wizard in CONC service manager. From Cisco Optical Network Controller, you cannot create new PSM services.
- Create cross-connect between PSM COM port and LINE port using CLI and onboard them to COSM, then onboard all these nodes to CONC.
- Service discovery - Once your onboard all the COSM nodes with cross connects, then the CONC discovers the PSM services and displays in the service list.
- The listed services are tagged with Active, Standby, Protect, Work, Forward and Reverse.
- PSM switching is unidirectional and bidirectional, CONC will show both unidirectional and bidirectional services based on the Active and Standby labels.
- PSM switching supports only Centralized control plane circuits (CPCE) circuits. CPCE circuits are service-level circuits managed by Cisco Optical Network Controller using PCE for path computation and provisioning.
- In Circuit Monitoring workspace, you can check the service, detailed service path, and service history.
- PSM module is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.
- NCS 1001 is supported only if it is managed by a COSM instance running over a NCS 1014 chassis.

Discover the PSM wavelength protection

Discover the PSM wavelength protection includes:

- Before discovering the PSM wavelength circuits, do these actions.
- Create cross-connect between PSM COM port and LINE port of NCS 1010 or NCS1K-MD-32O/E-C patch panel mux/demux using CLI commands.
- Onboard the nodes to COSM, then onboard all these COSM nodes to CONC.

10 Software Image Management and Upgrade

Topics:

- Software image management and upgrade

Explains software image management and upgrade in Cisco Optical Network Controller, including SFTP setup, node backups, database backups, and software upgrade orchestration.

Software image management and upgrade

This section explains software image management and upgrade, including backup types, SFTP storage formulas, upgrade orchestration, and node software upgrades. Use it to understand software operation workflows.

Software image management and upgrade is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Software image management and upgrade details

Table 61: Feature history

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

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

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

Components of SWIMU

The SWIMU App is divided into these tabs:

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

- **Software Activation Groups:** Create and manage groups for software activation.
- **Software Activation Jobs:** Schedule and monitor software activation jobs to upgrade nodes and subtended devices .

Benefits of Using SWIMU

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

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

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

SFTP Servers

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

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

Types of Backup

There are two types of backup:

Table 62: 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 63: 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 64: Internal SFTP Server Storage Formula Parameters

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

Note

Minimum allowed job interval is hourly.

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

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

Cleanup of Storage

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

Configure an SFTP server

Use this procedure to configure an 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.

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.

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.

Follow these steps to configure SFTP server:

Procedure

1. Click the**Configure SFTP Server** in the SWIMU app.
   The SFTP Servers configuration screen is displayed.
2. On the SFTP Servers configuration screen, click **Add**.
   The Add SFTP Server screen is displayed.
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.
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.
5. Click **Save**.
6. Select the target SFTP server and click **Edit** to modify SFTP server details.
   a) Modify the details.
   b) Click **Check Connectivity Status**.
   c) Click **Save**.

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

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

The configure SFTP server task is complete.

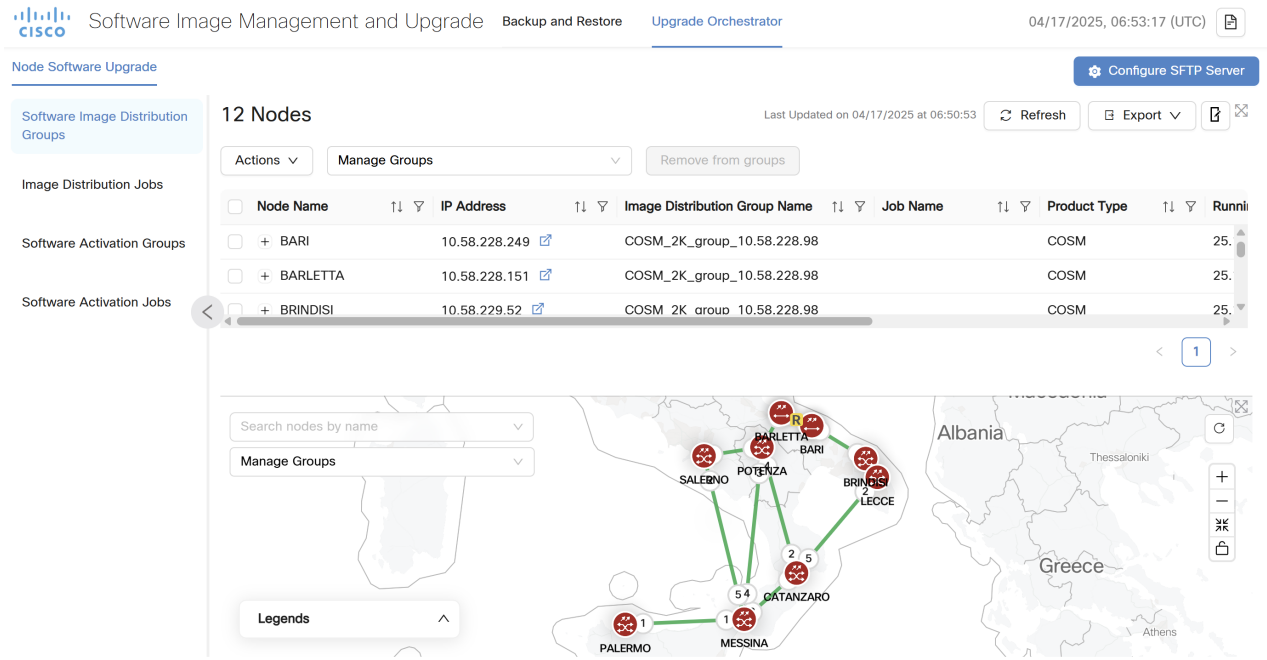
Back up and restore nodes

Use this procedure to back up and restore nodes. Node Backup and Restore enables administrators to create and manage backups of individual nodes in the network.

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.

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 72: 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 alarm on page 252 alarm is raised.

Follow these steps to back up and restore nodes:

Procedure

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

   Note

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

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.

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.

The back up and restore nodes task is complete.

Back up and restore the database

Use this procedure to back up and restore the database. CONC Database Backup and Restore enables administrators to create and manage backups of the Cisco Optical Network Controller 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.

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

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

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

- **Edit configuration:** Allows editing of backup settings or scheduling.
- **On-demand backup:** Manually triggers a new database backup.
- **Download:** Downloads a selected backup file to Cisco Optical Network Controller VM(disabled unless a backup is selected).
- **Restore:** Restores the Cisco Optical Network Controller database from a selected backup (disabled unless a backup is selected).
- **Scheduling Information:** Displays the next scheduled backup time.

Before you begin

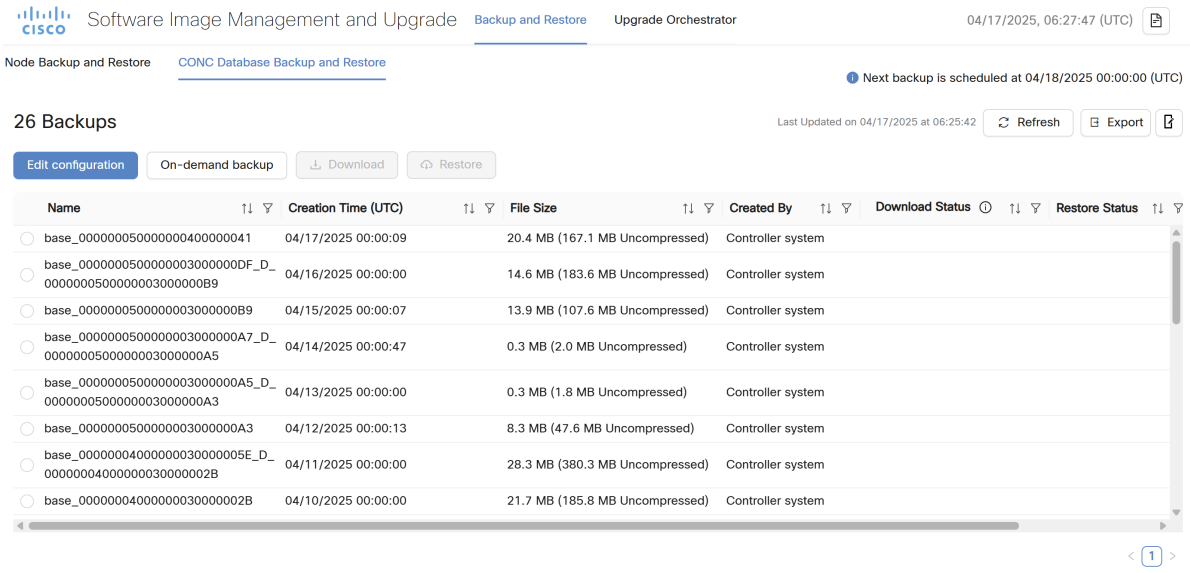
- The Cisco Optical Network Controller Database Backup and Restore feature relies on a properly configured SFTP server.
- Ensure that the SFTP server has sufficient storage space for the backups.
- If a backup fails, the BACKUP-FAILURE alarm on page 251 alarm is raised.
- If the upload of a backup to the SFTP server fails, the UPLOAD-FAILURE alarm on page 253 alarm is raised.

Follow these steps to back up and restore the database:

Procedure

1. Perform an **On-demand** backup.
   a) Navigate to **Backup and Restore** > **CONC Database Backup and Restore**.

   Figure 73: Node Backup and Restore



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

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

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

2. Download the database
   a) Navigate to **Backup and Restore** > **CONC Database Backup and Restore**.
   b) Select the backup you want to download from the table.
   c) Click **Download**.

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

   d) Enter a prefix string to be part of the downloaded file name and click **OK**.

      This prefix allows you to easily identify a backup file.

   e) Access Cisco Optical Network Controller VM CLI using SSH.
   f) Go to the path `/data/local-path-provisioner/pvc-*conc-database-backup*` to view the downloaded file.
3. Restore the database

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

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

   The Cisco Optical Network Controller database is restored from the selected backup.
4. Edit the backup configuration
   a) Click **Edit configuration**.
   b) Choose your **Preferred Backup Time (UTC)** and **Recurrence** preferences.
   c) Choose **Backup file retention time (weeks)** and set **Password to secure backup files**.

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

   d) Enable the check box if you want to **Copy the backup files to SFTP server** and enter the SFTP Server details.

- **SFTP Server Name:** A descriptive name for the SFTP server.
- **IP Address:** The IP address of the SFTP server.
- **Username:** The username for accessing the SFTP server.
- **Password:** The password for the specified username.
- **Remote Path:** The directory path on the SFTP server where software images and backups will be stored.
- **Disk memory space utilisation threshold for file overwrite(%):** The percentage of memory threshold allowed for each SFTP server. The minimum threshold value is 50. Anything exceeding the threshold will be cleaned up.

e) Click **Apply**.

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

Example

```
tar -zvxf <downloaded_file_name>
```

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

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

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

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

> **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.

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.

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.

e)

The back up and restore the database task is complete.

Orchestrate software upgrades

Use this procedure to orchestrate software upgrades. Use the upgrade Orchestrator to distribute images to the nodes and activate the images on the nodes.

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.

Follow these steps to orchestrate software upgrades:

Procedure

1. Upload ISO Images to the Local SFTP Server.

   Example

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

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

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

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

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

      - `<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:

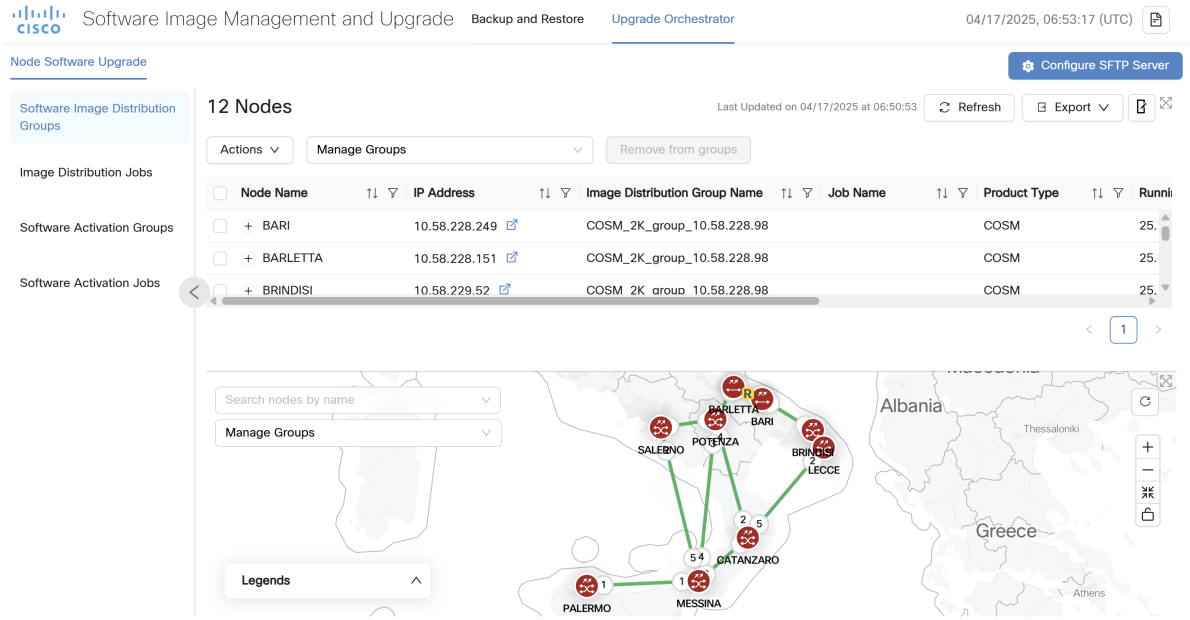
      - `<file-name>`: The name of the file to delete.

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

2. Create Image Distribution Groups.

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

Figure 74: Upgrade Orchestrator



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

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

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

d) Enter a Group Name and Description.

e) Select the nodes to include in the group and click **Manage Groups**.

f) Click the + icon next to a group name to add the nodes to the group.

g) Select a node and click **Remove from groups** to remove the node from the group it is a member of.

Note

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

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

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

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.

Figure 75: Upgrade Orchestrator

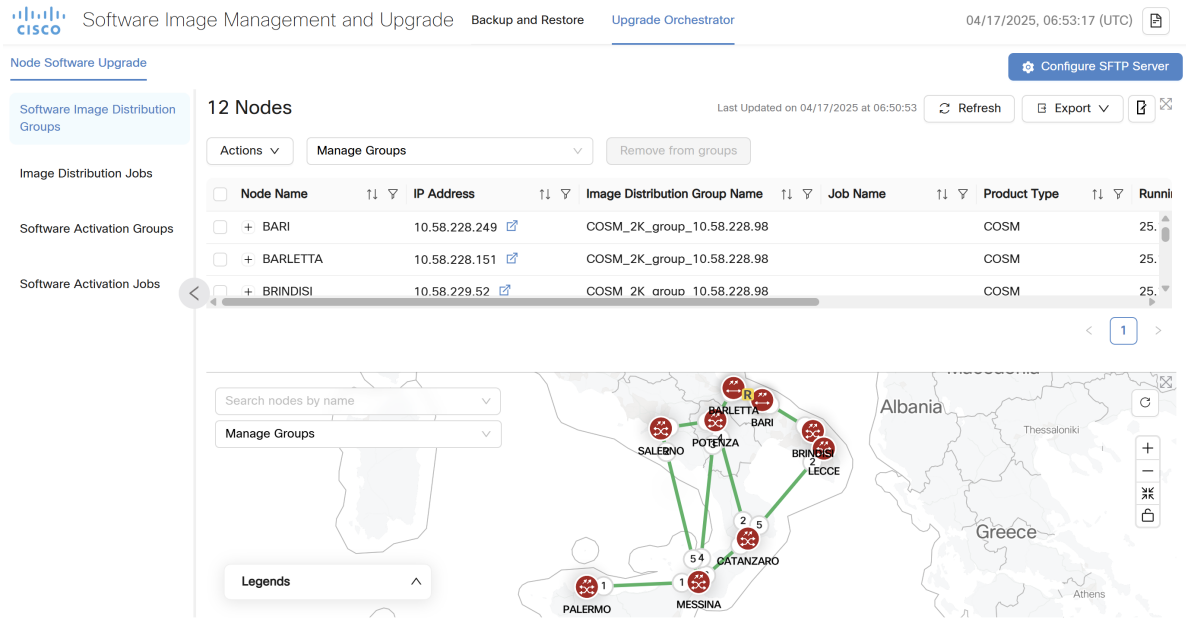


Table 65: Select node(s) or group(s) options

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

d) Select an SFTP server from the drop-down list or give the details of the SFTP server.
e) Select the ISO image file to distribute.
f) Schedule the job to start immediately or later.
g) Click **Schedule** and choose a later time or schedule the job to run immediately.
h) Click the status for a device in the status column to view detailed status.
i) Select a job and click **Stop** to stop the job in the nodes in which the job has not started.

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

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

A job that is in progress cannot be edited.

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

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

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

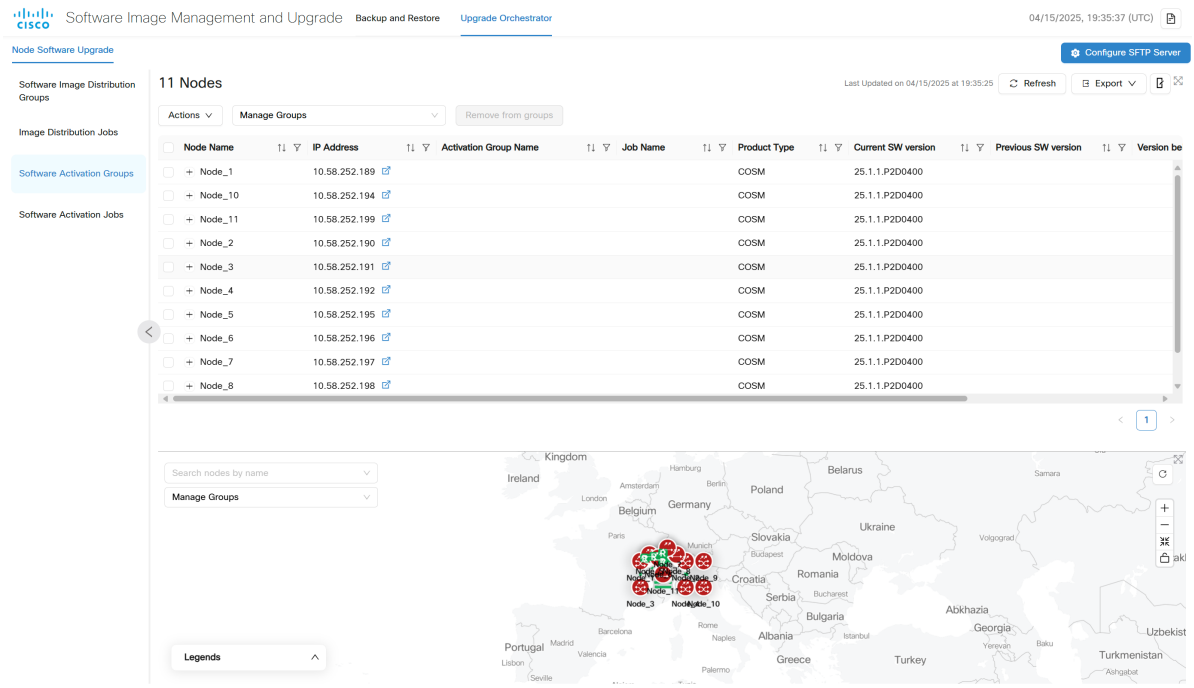
If a job status is **PARTIAL**, it means the job succeeded for some of the nodes, but failed for other nodes in the group of devices that the job was initiated for.

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

4. Create Software Activation Groups.

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

Figure 76: Upgrade Orchestrator



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

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

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

d) Enter a Group Name and Description.

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

> **Note**
>
> Groups for NCS 2000 nodes are autocreated by Cisco Optical Network Controller.
>
> You cannot delete the autocreated NCS 2000 groups. You can edit the name and description of the autocreated NCS 2000 groups.
>
> You cannot add the autocreated NCS 2000 nodes to NCS1000 groups or NCS1000 nodes to NCS 2000 autocreated groups.

5. Optional: Copy a group to **Software Activation Groups** from **Software Image Distribution Groups**.

> **Note**
>
> When managed devices are connected to the Cisco Optical Site Manager host in a daisy-chain configuration, image distribution through the Cisco Optical Network Controller SWIMU application might not complete on the first attempt. If the operation does not complete, try again.

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

6. Create a Software Activation Job.

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

a) Navigate to the Upgrade Orchestrator tab and select **Node Software Upgrade** > **Software Activation Jobs**
b) Click **Activate Software**.

> **Note**
>
> When managed devices are connected to the Cisco Optical Site Manager host in a daisy-chain configuration, image activation through the Cisco Optical Network Controller SWIMU application might not complete on the first attempt. If the operation does not complete, try again.

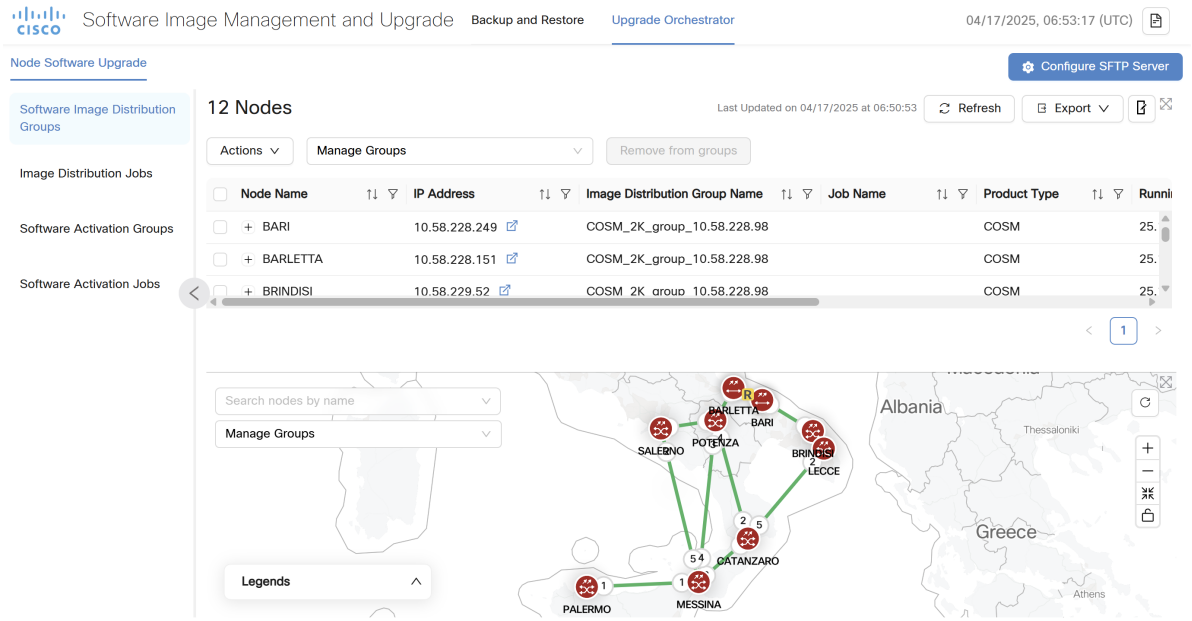
c) Select the target devices or groups.

Table 66: Select Groups or Nodes or Devices options

UI options	Actions
Activate only COSM radio button	Activates only Cisco Optical Site Manager **Note** COSM NCS 1000 Series: This activation job automatically performs an upgrade of hosting device(s) as well. COSM NCS 2000 Series: Only COSM is activated.
Activate both COSM and Device(s) radio button	Activates both Cisco Optical Site Manager and the selected subtended device(s). The activation job upgrades Cisco Optical Site Manager and selected subtended device(s). **Note** COSM NCS 1000 Series: The NCS 1000 hosting device(s) will be auto-selected if you have not selected the hosting device(s). COSM NCS 2000 Series: Activation of both Cisco Optical Site Manager and device(s) works based on the selected subtended device(s).
Activate only Device(s)	Activates only the selected subtended device(s). The activation job upgrades the subtended device(s) software version. **Note** COSM NCS 1000 Series: The NCS 1000 hosting device(s) will be auto-selected if you have not selected the hosting device(s). COSM NCS 2000 Series: Activation of device(s) works based on the selected subtended device(s). If COSM is not upgraded to the same, this option first upgrades the COSM and then proceed with the subtended device(s).
Group(s) or Node(s) or Device(s) search bar	Displays the list of nodes, devices and groups

UI options	Actions
Back	Goes back to the **Orchestrator Upgrade** tab.
Next	Moves to the next step.

Figure 77: Upgrade Orchestrator



Note

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

Figure 78: Upgrade Orchestrator

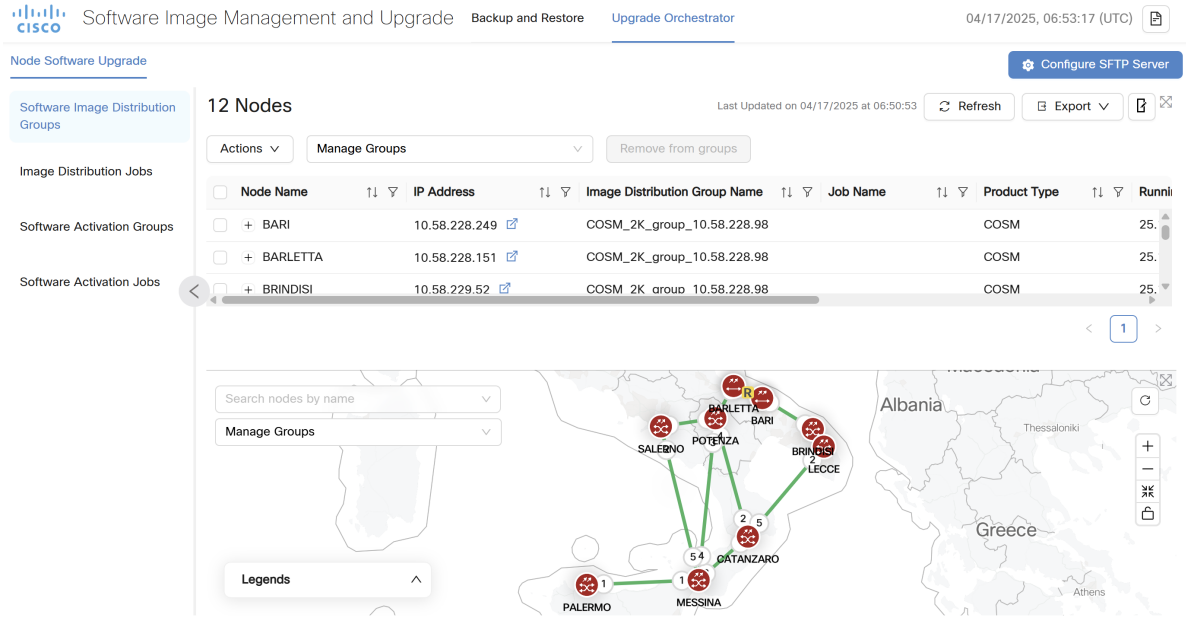


Figure 79: Upgrade Orchestrator

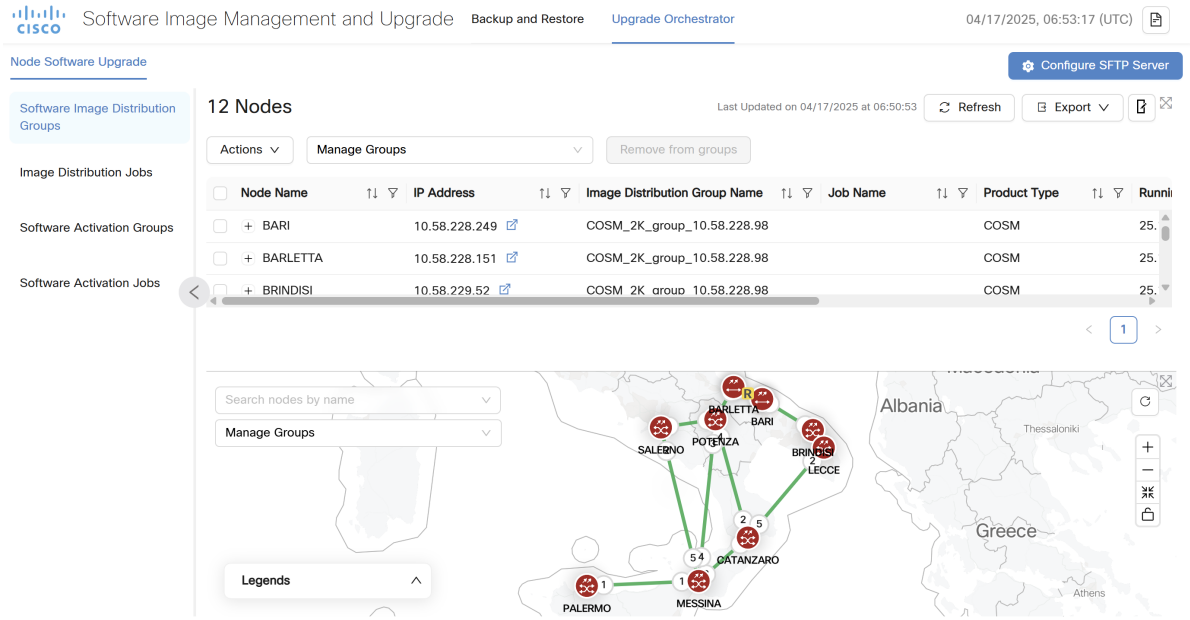
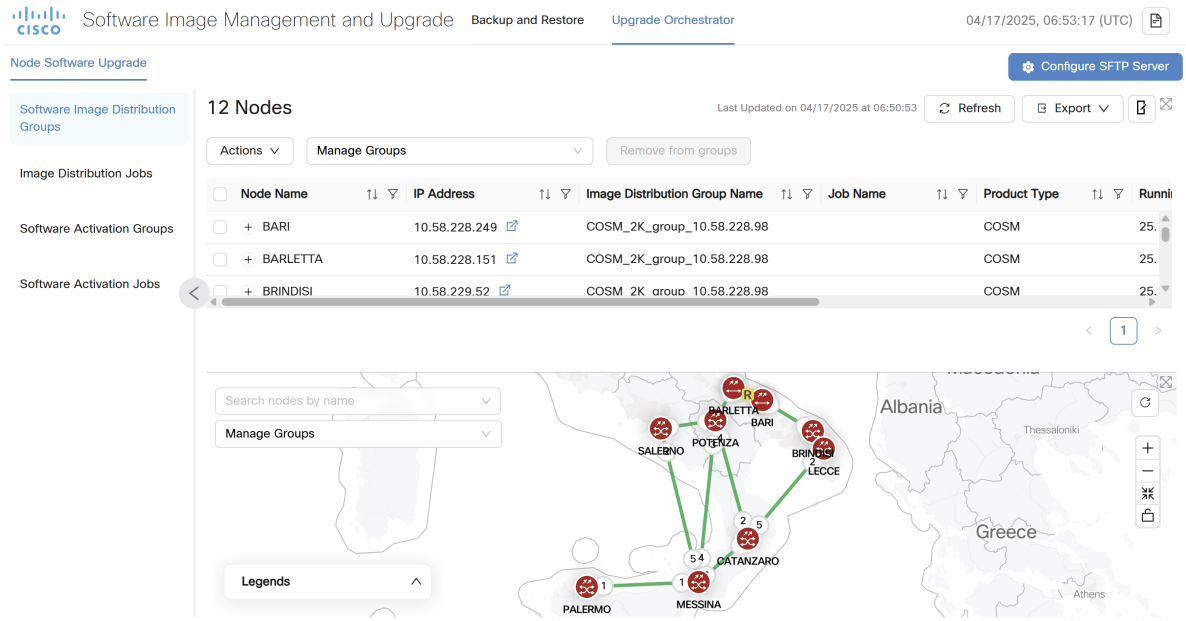


Figure 80: Upgrade Orchestrator



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

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

h) Select a job and click **Stop** to stop the job in the nodes in which the job has not started.

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

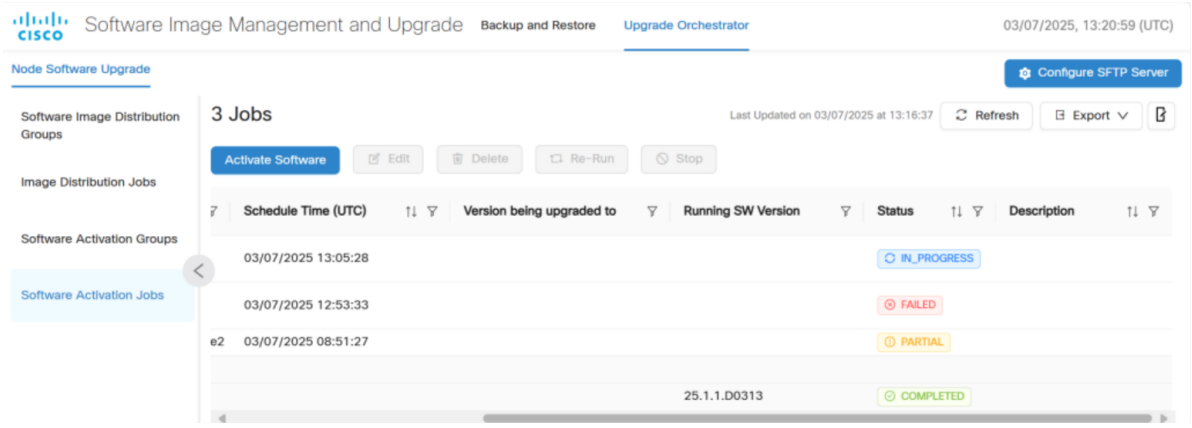
i) Select a job and click **Edit** to make changes to the job.

   A job that is in progress cannot be edited.

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

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

Figure 81: 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.**

The orchestrate software upgrades task is complete.

11 PM History

Topics:

- PM history reports
- PM data retention
- PM data collection settings
- Access PM history report
- Configure the SMTP mail server

Summarizes PM History in Cisco Optical Network Controller, including PM reports, dashboards, job scheduling, mail server configuration, and connectivity security options.

PM history reports

This section provides details about PM history reports, including report benefits, time ranges, port details, data storage, dashboards, and PM job scheduling. Use it to understand PM history data and reporting options.

Use this reference to understand PM history reports.

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.

Table 67: Feature history

Feature name	Release information	Feature description
PM history support for the AR-MXP cards	Release 26.1.1	PM history data collection is supported for the SONET and SDH interfaces type for the AR-MXP, AR-XP and AR-XPE cards. These UI enhancements are made to support the SONET and SDH interfaces of AR-MXP cards. • PM browse: Added *sonet* and *sdh* interfaces in the **Interface** type drop-down list. • PM jobs: To schedule PM jobs for AR cards, select **Interfaces** and enter *AR* in the **Equipment, Shelves, Cards, and Port** field.

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 68: 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.

Benefit	Description
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 69: Details

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

Table 70: Time Range for Fetching Data

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

Port details

Port details include:

- The Port Details area displays these drop-down lists.
- From R26.1.1, the PM browser supports the SDH and SONET interface types.

Table 71: Details

Drop-down list	Description
Interface types	Type of interface on the ports. • opticalTransport • opticalChannel • otnOtu • otnOdu • ethernetCsmacd • sonet • sdh • zrPlus

Drop-down list	Description
Port Name	Port label
Location	Location of the node from where the PM is being collected. • near-end: The current node and current port. • far-end: The port to which the current port is connected to

Data collection and storage

Data collection and storage includes:

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

Table 72: 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 - 32). Overall data is available for 32 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 31 days and for 24 hours granularity from 31 to 93 days.
- If the date range falls on archive data then you will receive a message to indicate the user has chosen a time range which coincides with the archived data time range.

Figure 82: 15-Minute Granularity PM Report

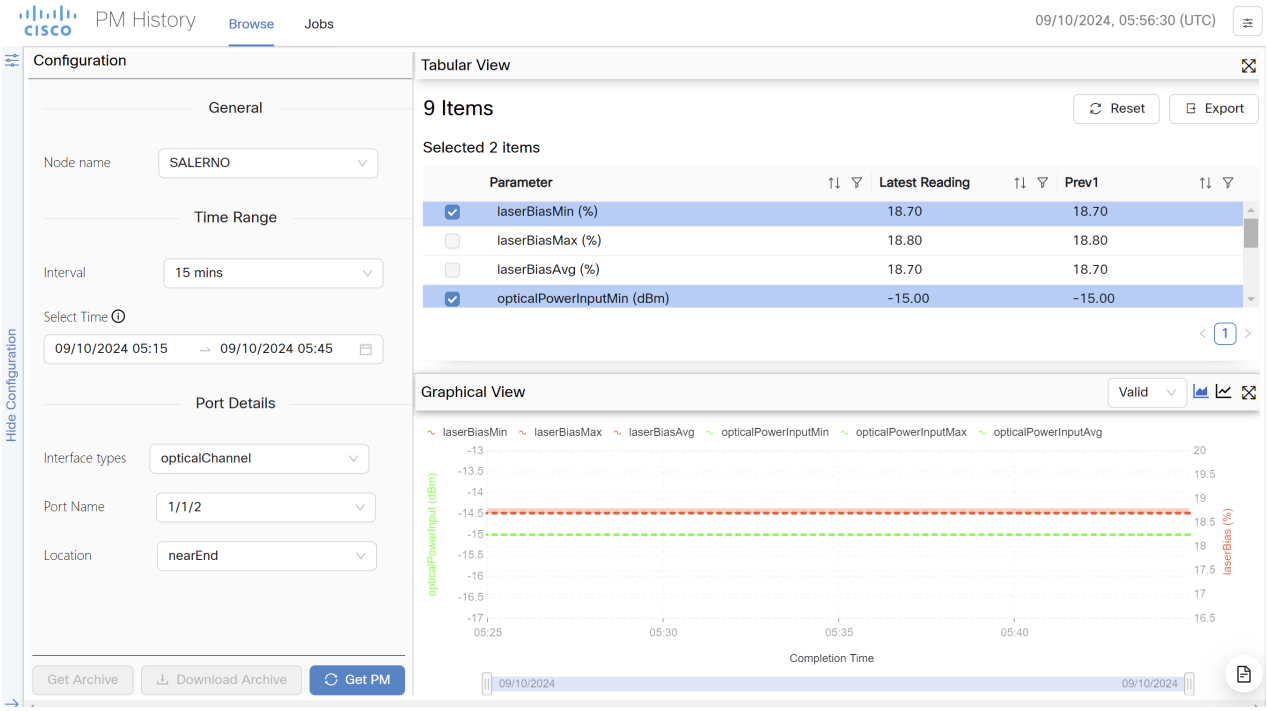
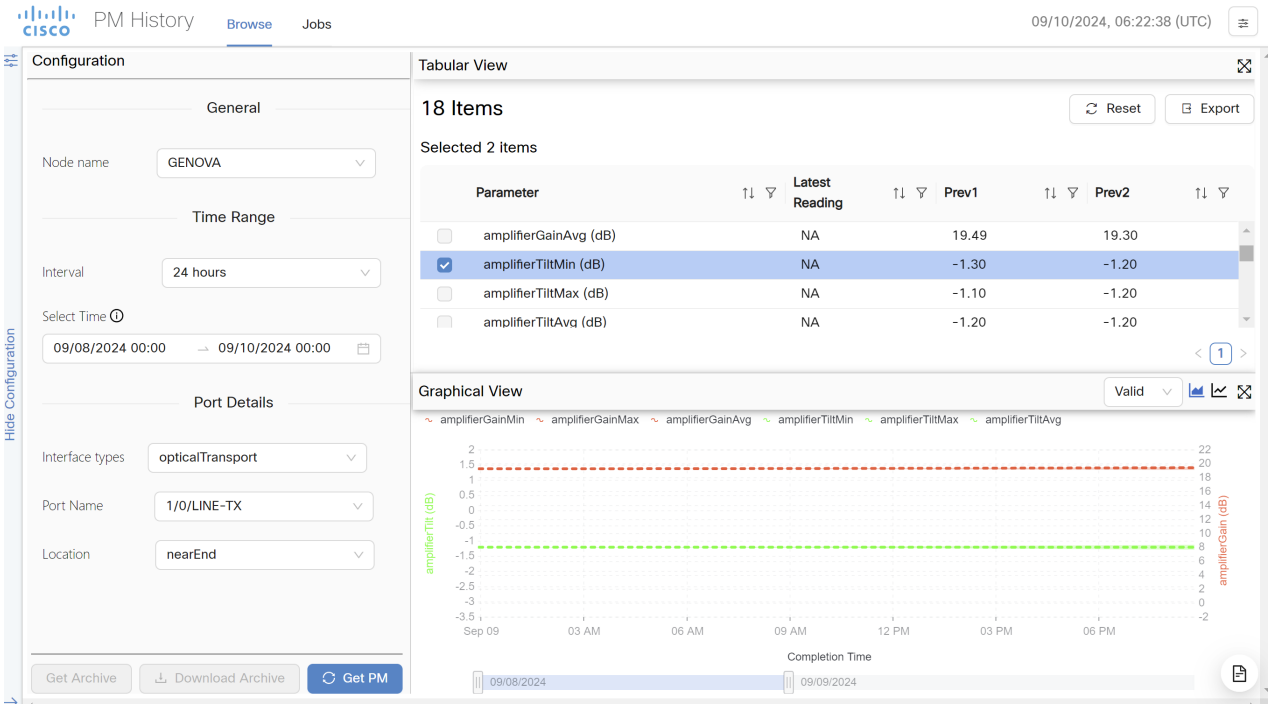


Figure 83: 24-Hour Granularity PM Report



Data representation

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

PM job scheduler

PM job scheduler includes:

- 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. 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

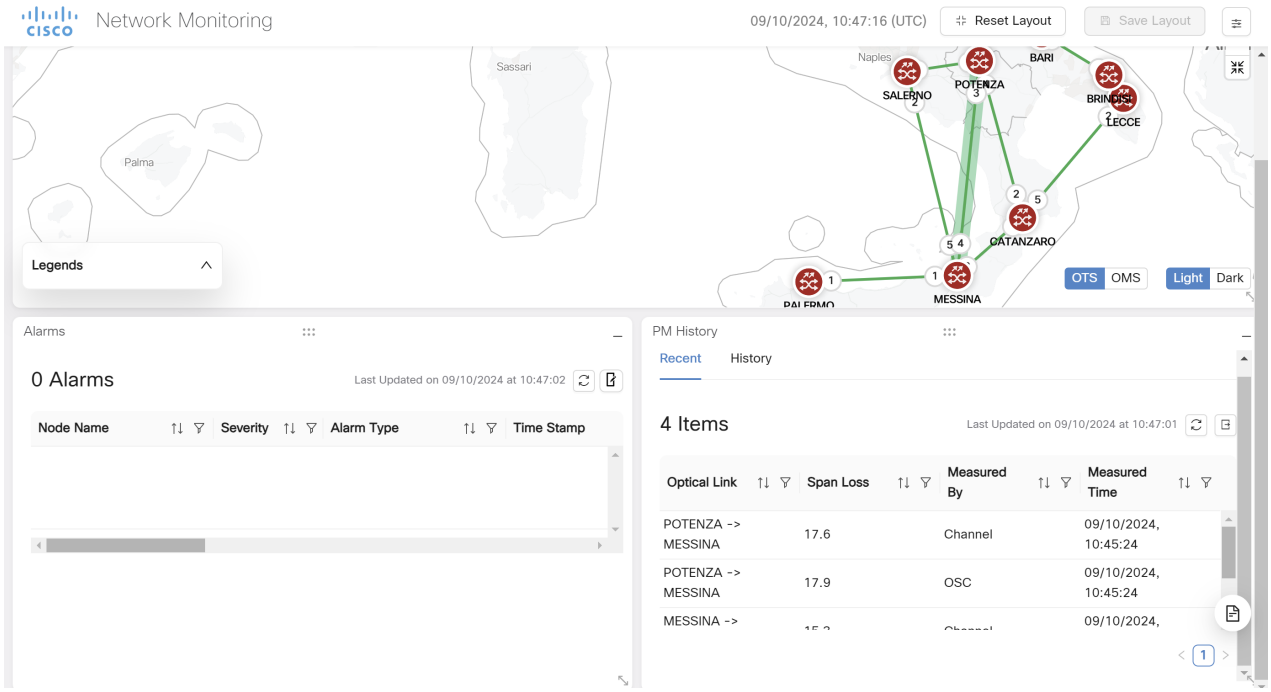
PM history in network monitoring includes:

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

Note

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

Figure 84: PM History in Network Monitoring



PM history in topology

PM history in topology includes:

- In the Topology application, the PM history tab:.
- Interacts with the Topology application and its components.
- Helps in viewing the span loss changes and information.

PM history in circuit monitoring

PM history in circuit monitoring includes:

- The Circuit Monitoring workspace will now feature a new dashboard in the detailed service path component, displaying PM History data. This new add-on dashboard has the Detailed Service Path component which displays the PM values based on selected port.
- The historical data for a particular port from the Detailed Service Path can be seen for 15 minutes and 24 hours interval. You can also select the start and end date. PM values for ports are displayed in the tabular and graphical formats.
- Right click on the port on Detailed Service Path and use the option to launch PM History for that port. Also you can choose up to two ports. PM and PM history is enabled only after circuits are created on a node. Using Interval and Select Time , select the data range for Circuit Monitoring PM history data, based on the retention days.

Note

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

Figure 85: PM History in Circuit Monitoring



Service endpoint PM history report

Service endpoint PM history report includes:

- The PM History application jobs dashboard report in service endpoint helps in:.
- Calculating and presenting total availability or outage time and percentage.
- Exporting to Excel and scheduling job options if available.

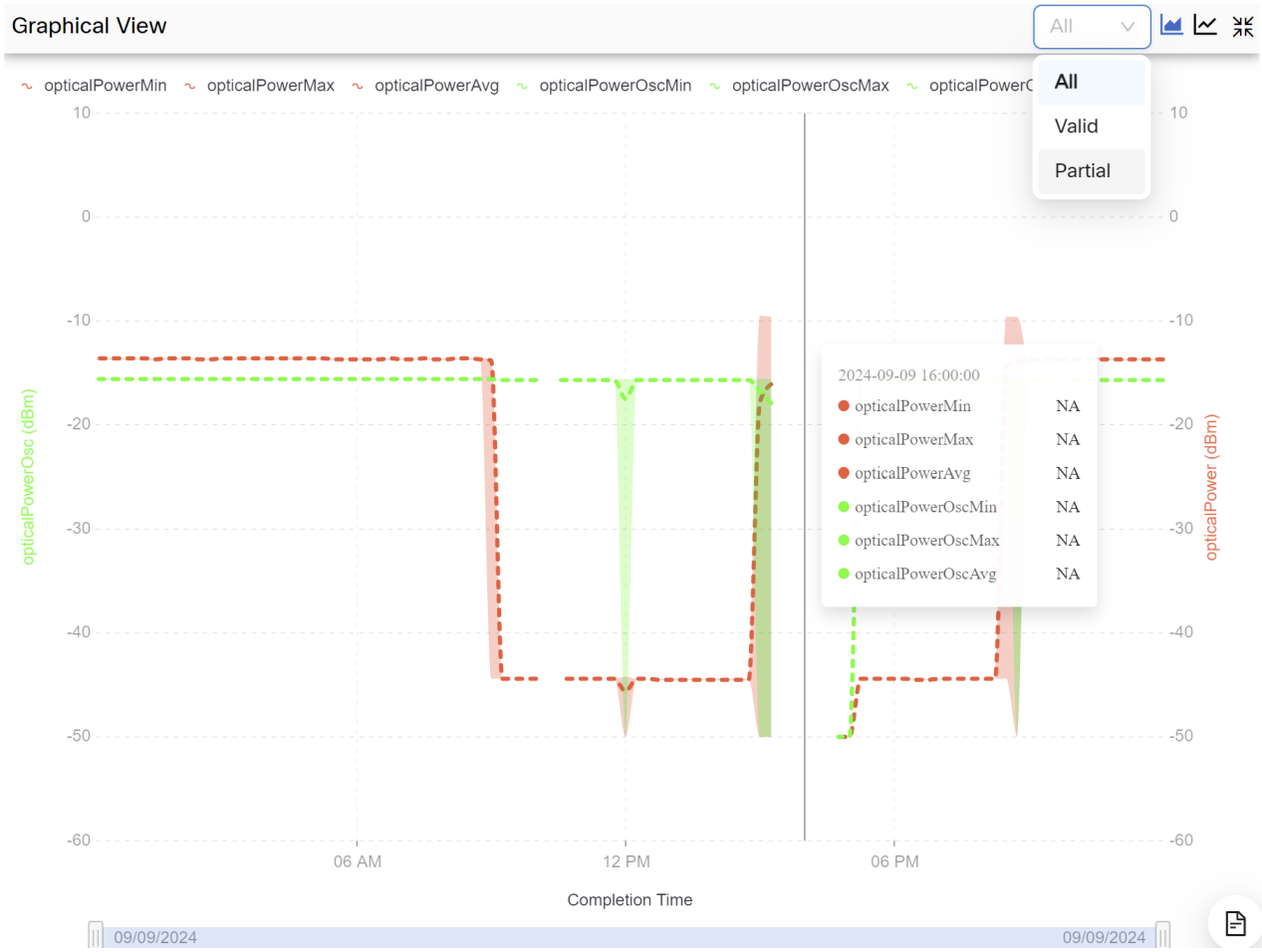
Graphical representation within PM history application

Graphical representation within PM history application includes:

- The linear graph displays ALL / VALID / PARTIAL PM values. Also, the NA values do not have any representation in the graph.
- Partial is represented in yellow.

> **Note**
>
> Partial is represented in yellow.

Figure 86: NA Values in Linear Graph



Access PM history report

Use this procedure to access the PM History report tab. The task helps you open PM History from the application launcher and review general reports or scheduled jobs.

Use this procedure to access PM history report in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

Follow these steps to access PM history report:

Procedure

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

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

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

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

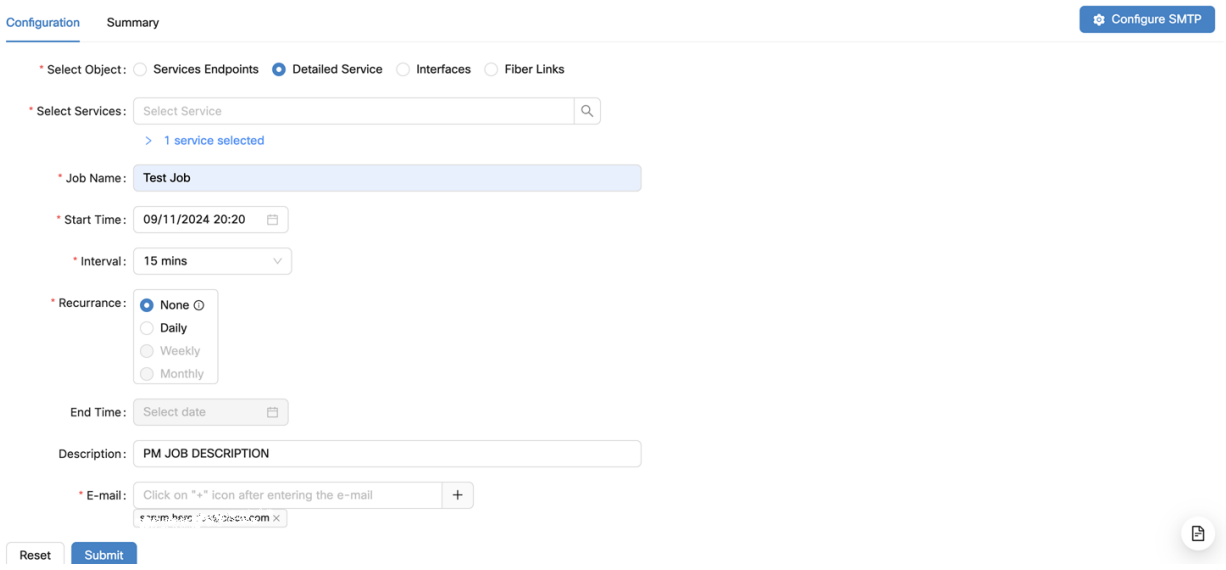
To browse or view the job scheduling details follow the steps given:

a) Click **Jobs** tab.

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

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

Figure 87: Configure SMTP



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.

Note

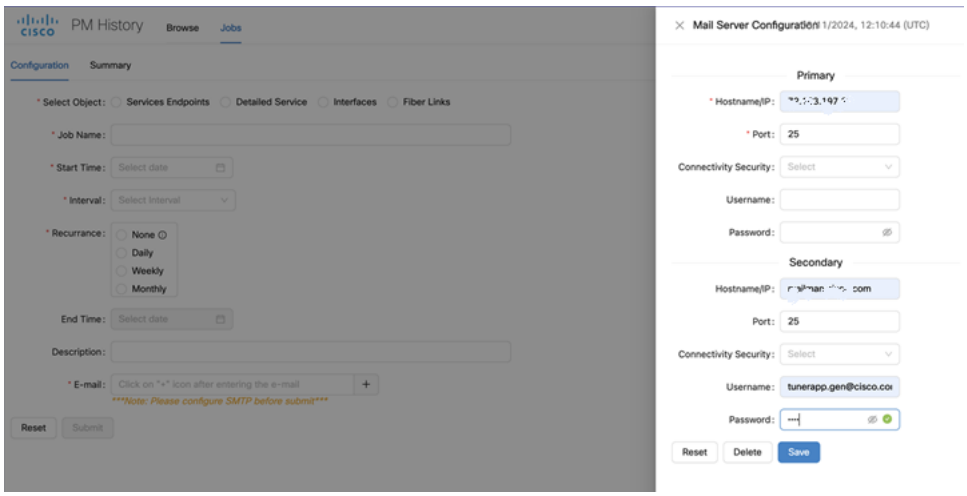
From release 26.1.1, you can schedule PM jobs for AR-MXP cards. Select **Interfaces** radio button and type **AR** in the **Equipments, Shelves, Cards, and Ports** field.

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 88: 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.

The access PM history report task is complete.

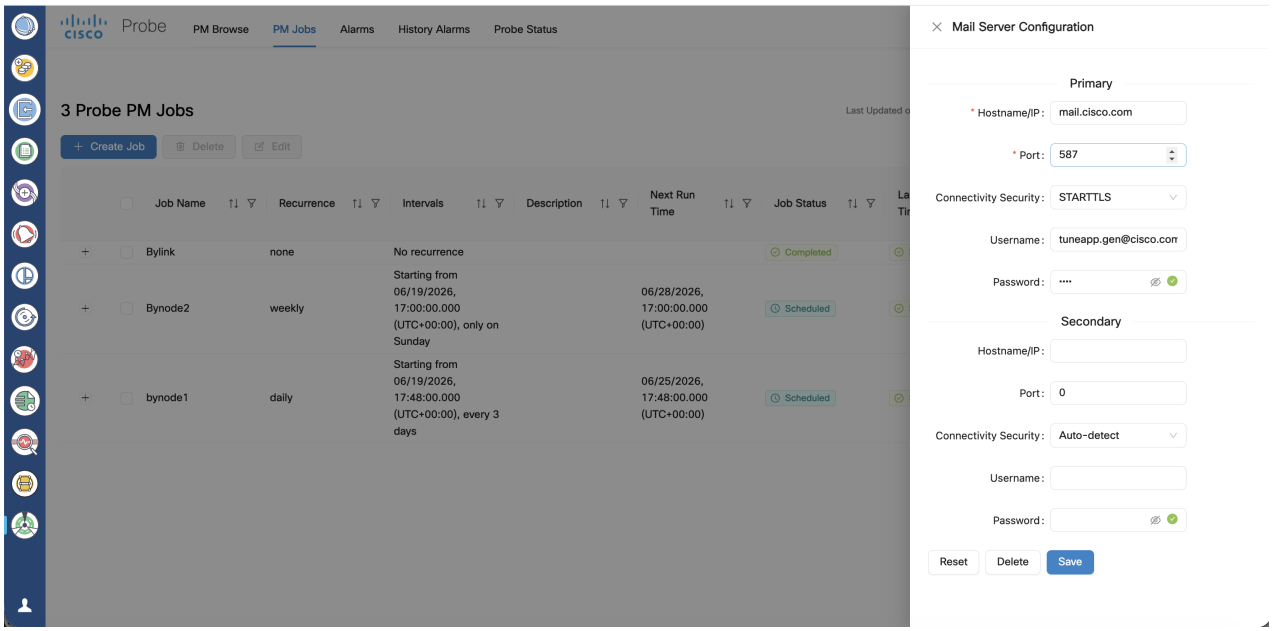
Configure the SMTP mail server

Use this procedure to configure the SMTP mail server. Cisco Optical Network Controller utilizes an SMTP mail server to send various email notifications, including performance monitoring reports and alarms.

Use this procedure to configure the SMTP mail server in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Figure 89: Mail server configuration



Before you begin

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

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

Procedure

1. Open the **PM History** application, then click the **PM Jobs** tab.
2. Click **Configure SMTP**.
3. In the **Mail Server Configuration** panel, enter the required **Primary** server fields.
4. Select the **Connectivity Security** option that matches the primary SMTP server.

   For details about the **Connectivity Security** field descriptions, see Connectivity security options on page 214.
5. If the primary SMTP server requires authentication, enter the **Username** and **Password**.
6. Optional: In the **Secondary** section, enter the failover SMTP server details.
7. Click **Save**.

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

Mail server fields

This section provides details about mail server fields, including primary and secondary server settings and configuration controls. Use it to understand required values before configuring email notifications.

Use this reference to understand mail server fields.

Primary and secondary server fields

This table descibes the primary and secondary server fields.

Table 73: Primary server fields

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

Configuration controls

This table describes the configuration controls.

Table 74: Configuration controls

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

Control	Description
Save	Saves the configured primary and secondary mail server details.

Connectivity security options

This section provides details about SMTP connectivity security options, including None, SSL, and STARTTLS modes. Use it to choose the correct mail server security setting.

Use this reference to understand connectivity security options.

Details about connectivity security options.

SMTP security options

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

Table 75: SMTP security options

Connectivity Security option	Standard port behavior
Auto-detect	Cisco Optical Network Controller selects the connectivity security mode based on the standard SMTP port and connectivity behavior.
None / Plain Text	Use for port `25` when the SMTP server expects no encryption.
STARTTLS	Use for port `587` when the SMTP server expects an opportunistic TLS upgrade. The UI also lists port `2525` as a STARTTLS option.
SSL / TLS (implicit)	Use for port `465` when the SMTP server expects implicit TLS or SMTPS.

PM data retention

Provides PM data retention settings, valid ranges, and controls for active and archived performance data collected at 15-minute and 24-hour intervals.

PM data retention settings control how long Cisco Optical Network Controller stores active and archived performance data.

The **PM Data Retention** pane provides these PM data buckets:

- **15 Mins (Max Range 31 days)**: PM data collected at 15-minute intervals.
- **24 hours (Max Range 180 days)**: PM data collected at daily intervals.

Retention settings

You can increase or decrease the retention values for active and archived data. These settings affect data availability across PM browse, jobs, and workspace history.

Figure 90: PM data retention



Table 76: PM data retention settings

Label	Setting category	Data type	Default value	Valid range
1	15-minute interval	Active data	2 days	1-2 days
2	24-hour interval	Active data	31 days	1-93 days
3	24-hour interval	Archive data	93 days	1-149 days
4	15-minute interval	Archive data	3 days	1-29 days

Retention controls

The PM data retention pane provides these controls:

- **Reset to Default**: Restores data retention settings to their default values.
- **Cancel**: Discards changes to the PM data retention configuration.
- **Save**: Saves the configuration changes.

PM retention disk space

Provides the disk-space categories used to show available capacity and storage consumed by active PM data, archived PM data, jobs, and other content.

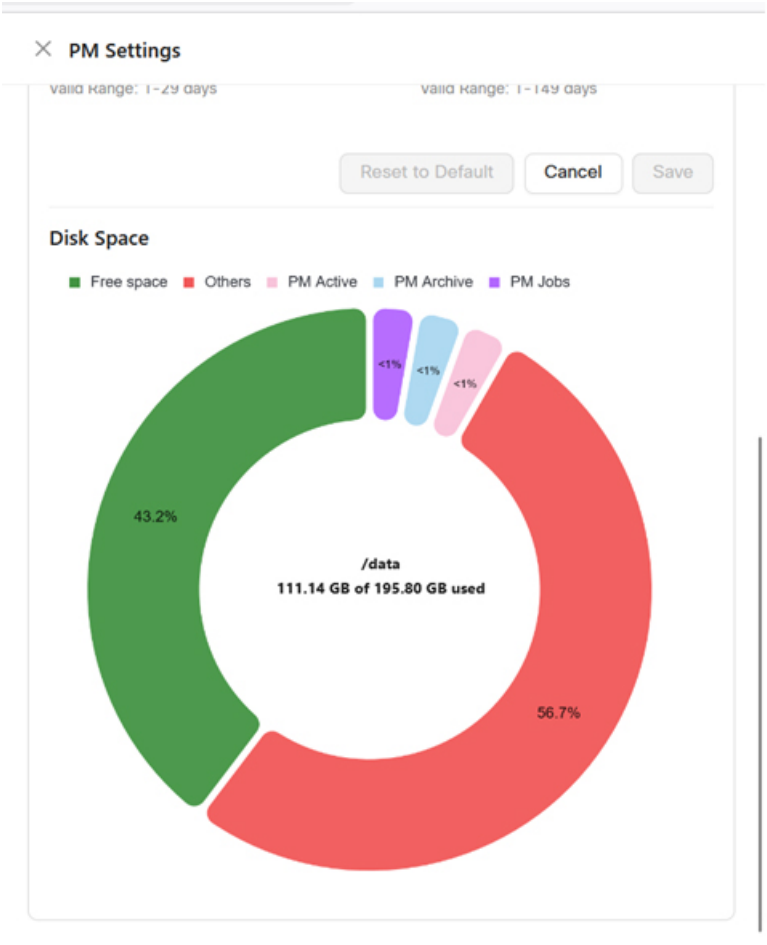
Disk-space information identifies how virtual machine storage is allocated to PM data, PM jobs, and other content.

The **Disk Space** pane displays virtual machine disk usage in a pie chart:

- **Free Space**: Displays unused space in the virtual machine.
- **Others**: Displays space used by files or data other than PM data.
- **PM Active**: Displays space used by recent active PM data in PostgreSQL.
- **PM Archive**: Displays space used by archived PM data in PostgreSQL.
- **PM Jobs**: Displays space used by PM job results and reports.

PM retention disk usage

Figure 91: PM retention disk space



PM data retention characteristics

Lists how PM data retention changes affect jobs, disk usage, browsing periods, workspace calendars, and notifications across concurrent user sessions.

PM data retention characteristics describe how retention changes affect stored data, system capacity, and PM workflows.

PM data retention has these characteristics:

- **Retention decrease:** Reducing the retention period can cause existing jobs to fail and move to the paused state.
- **Retention increase:** Increasing the retention period increases disk-space usage. For example, 55 nodes with 2 days of 15-minute data and 180 days of 24-hour data use 3.29 GB. Increasing 15-minute retention to 10 days raises the estimated usage to approximately 3.4 GB.
- **Threshold warning:** If virtual machine disk-space utilization exceeds 80%, you cannot increase PM data retention. Add storage or free disk space before increasing the retention period.
- **PM browse:** You can retrieve 15-minute PM data for up to 31 days and 24-hour PM data for up to 180 days.
- **PM jobs:** PM jobs update when retention settings change.
- **PM History workspace:** The calendar in circuit and link workspaces changes when retention settings change. Active history includes the configured number of active retention days plus the current day.

- **Multiple user sessions:** If one user updates retention values, other users in the same workspace receive a notification to refresh the page.

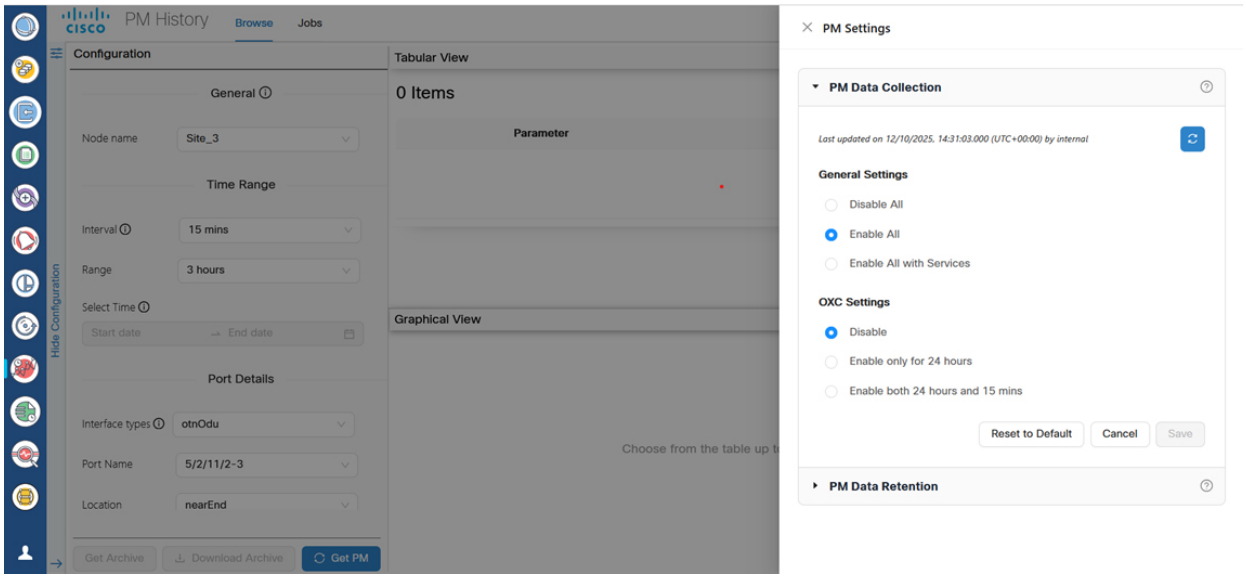
PM data collection settings

Provides PM data collection settings for general and Optical X Connection interfaces, including defaults, control behavior, interface availability, and disk-space constraints.

PM data collection settings control performance metric collection separately for general interfaces and Optical X Connection interfaces.

PM data collection provides separate settings for general interfaces and Optical X Connection (OXC) interfaces.

Figure 92: PM history data collection settings



General interface settings

General interface data collection provides these options:

- **Disable All**: Disables PM data collection for all general interfaces.
- **Enable All**: Enables PM data collection for all general interfaces.
- **Enable All with Services**: Enables data collection for all general interfaces except OXC interfaces and associated services. This option is selected by default.

> **Note**
>
> SONET and SDH PM data does not require circuits. To view SONET and SDH PM counters, select **Enable All**.

Optical X Connection settings

OXC interface data collection provides these options:

- **Disable**: Disables PM data collection for OXC interfaces. This option is selected by default.

- **Enable only for 24 hours**: Enables OXC data collection at 24-hour intervals.
- **Enable both 24 hours and 15 mins**: Enables OXC data collection at 24-hour and 15-minute intervals.

Table 77: Interface availability by collection setting

General setting	OXC setting	Available interface types
Disable	Disable	No interface types are available.
Enable	Enable	All interface types are available.
Enable	Disable	All interface types except OpticalXConnection are available.
Disable	Enable	All interface types except OpticalXConnection are available.

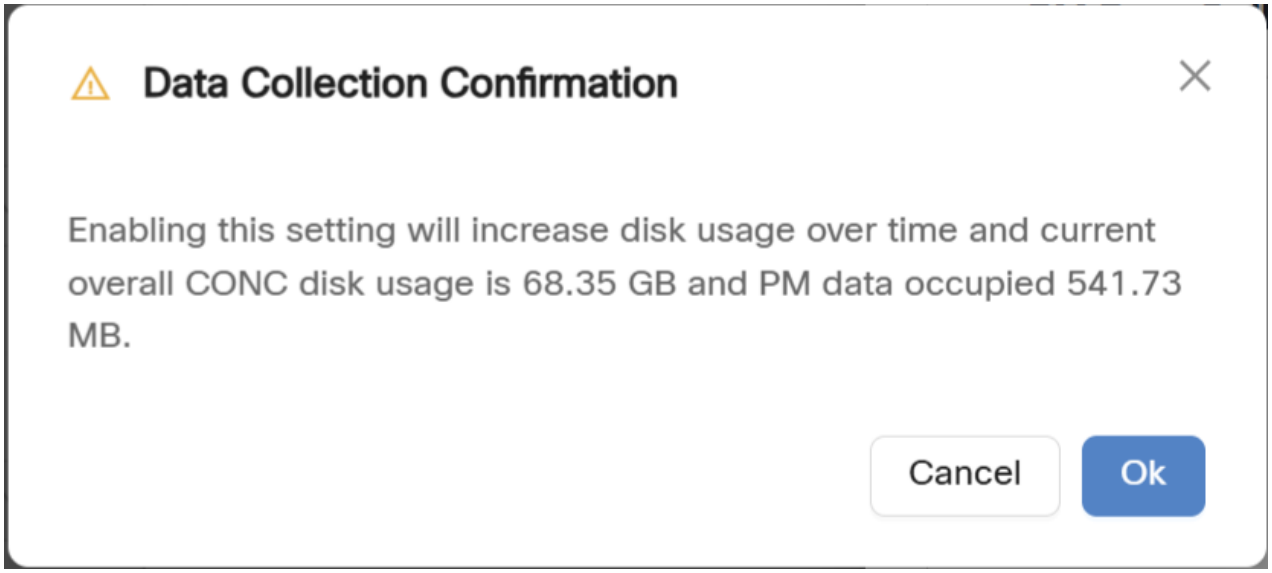
Data collection controls

PM data collection provides these controls:

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

> **Note**
>
> Selecting **Enable All** displays a confirmation message about disk-space usage. If virtual machine disk-space usage exceeds 80%, add storage or free disk space.

Figure 93: PM history data collection confirmation



Access PM history report

Use this procedure to access the PM History report tab. The task helps you open PM History from the application launcher and review general reports or scheduled jobs.

Use this procedure to access PM history report in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

Follow these steps to access PM history report:

Procedure

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

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

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

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

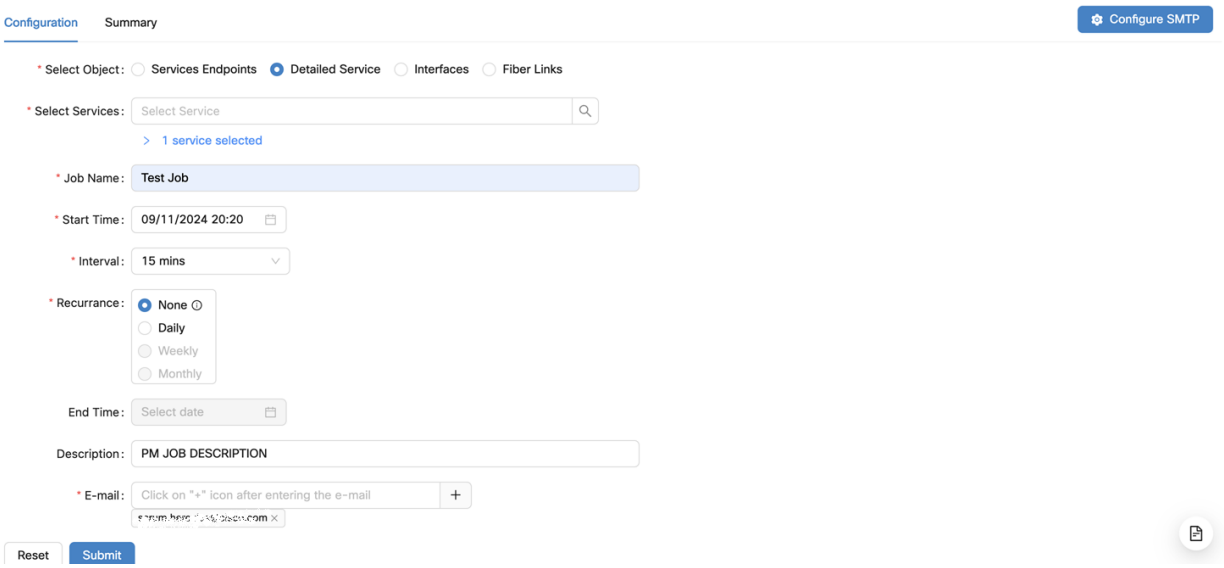
   To browse or view the job scheduling details follow the steps given:

   a) Click **Jobs** tab.

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

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

   Figure 94: Configure SMTP



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.

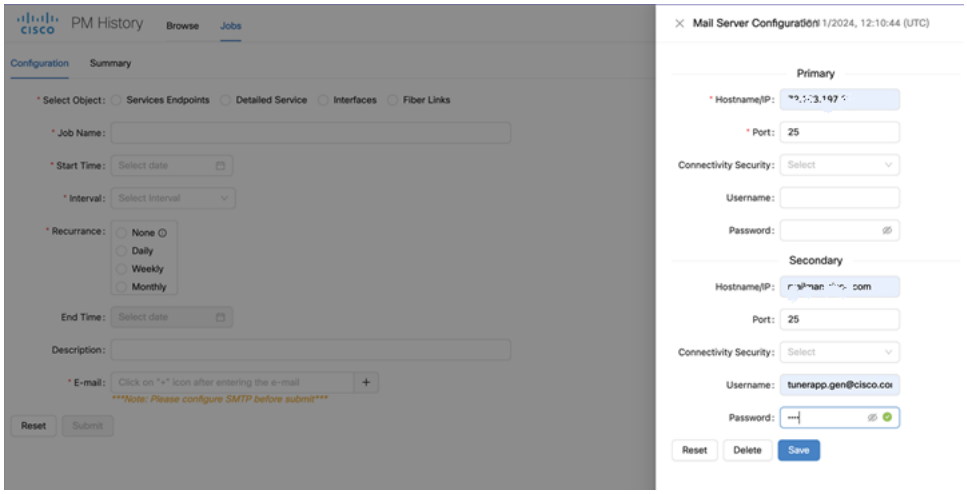
   > **Note**
   >
   > From release 26.1.1, you can schedule PM jobs for AR-MXP cards. Select **Interfaces** radio button and type **AR** in the **Equipments, Shelves, Cards, and Ports** field.

   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 95: 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.

The access PM history report task is complete.

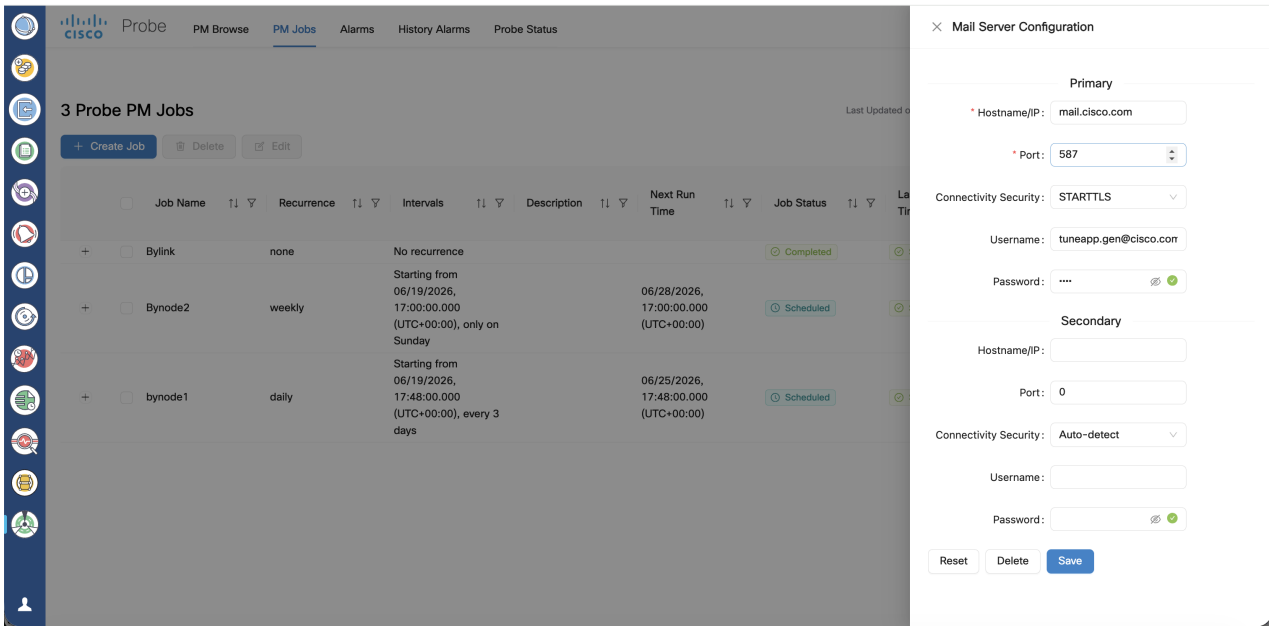
Configure the SMTP mail server

Use this procedure to configure the SMTP mail server. Cisco Optical Network Controller utilizes an SMTP mail server to send various email notifications, including performance monitoring reports and alarms.

Use this procedure to configure the SMTP mail server in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Figure 96: Mail server configuration



Before you begin

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

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

Procedure

1. Open the **PM History** application, then click the **PM Jobs** tab.
2. Click **Configure SMTP**.
3. In the **Mail Server Configuration** panel, enter the required **Primary** server fields.
4. Select the **Connectivity Security** option that matches the primary SMTP server.

   For details about the **Connectivity Security** field descriptions, see Connectivity security options on page 214.
5. If the primary SMTP server requires authentication, enter the **Username** and **Password**.
6. Optional: In the **Secondary** section, enter the failover SMTP server details.
7. Click **Save**.

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

Mail server fields

This section provides details about mail server fields, including primary and secondary server settings and configuration controls. Use it to understand required values before configuring email notifications.

Use this reference to understand mail server fields.

Primary and secondary server fields

This table descibes the primary and secondary server fields.

Table 78: Primary server fields

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

Configuration controls

This table describes the configuration controls.

Table 79: Configuration controls

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

Connectivity security options

This section provides details about SMTP connectivity security options, including None, SSL, and STARTTLS modes. Use it to choose the correct mail server security setting.

Use this reference to understand connectivity security options.

Details about connectivity security options.

SMTP security options

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

Table 80: SMTP security options

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

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

12 Logs

Topics:

- Audit and debug logs
- Syslog forwarding configuration

Covers logs in Cisco Optical Network Controller, including audit logs, debug logs, tech dump logs, syslog forwarding, access logs, and troubleshooting support.

Audit and debug logs

This section provides details about audit and debug logs, including log categories, display features, retention, archiving, and SEDO commands. Use it to understand log behavior and administration options.

Use this reference to understand audit and debug logs.

Audit and debug logs include:

- 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

Audit logs include:

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

Display features

Display features include:

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

Categorization of audit logs

Categorization of audit logs include:

- Audit logs are categorized into:.
- 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 .

Table 81: Audit Logs Category

Category Field	Description
System	The events that are part of this category are: • Login. • Logout. • Create user. • Delete user. • CONC database backup and restore
Inventory	The events that are part of this category are: • Card create/delete/state update. • Physical port and logical port create/delete/state update. • Interfaces create/delete/state update. • Chassis create/delete. • IPC add and delete. • Degree add and delete. • Passive unit add/delete • Port Frequency
Node	The events that are part of this category are: • Device add/delete/resync/reconnect. • Device state for discovered and disconnected status. • Connection loss or reconnect audit logs status.
Service	The events that are part of this category are: • Circuit add/delete/edit/update or state change. • Link up and down.
Topology	The events of this category include the OMS and OTS interfaces.
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

Category Field	Description
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

Debug logs include:

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

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

Retention and archiving and archive logs include:

- 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

Archive logs include:

- 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. Techdump : Refers to the on-demand collection of logs from the services which are displayed in the table. It collects the data base (DB) snapshots for all the services. You can collect or download and also delete these logs from the table.
- 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.

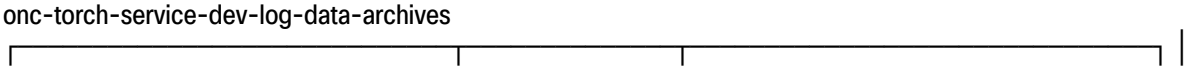
Note

- 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

SEDO commands include:

- 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:.
- 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 .
- Step 2: Use the scp command to copy nxfos-logs-xxxxxxxx.tar.gz file to the local system.
- Download of developer archive logs will time-out when logs are too huge, then it is recommended to use the sedo commands to download:.
- 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 │
└──────────────────────────┴──────────────┴──────────────────────────────┘.
```

- 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.
- Step 3: You can download the file to the local system.

Audit and debug logs details

Details about audit and debug logs details.

Figure 97: Audit Logs

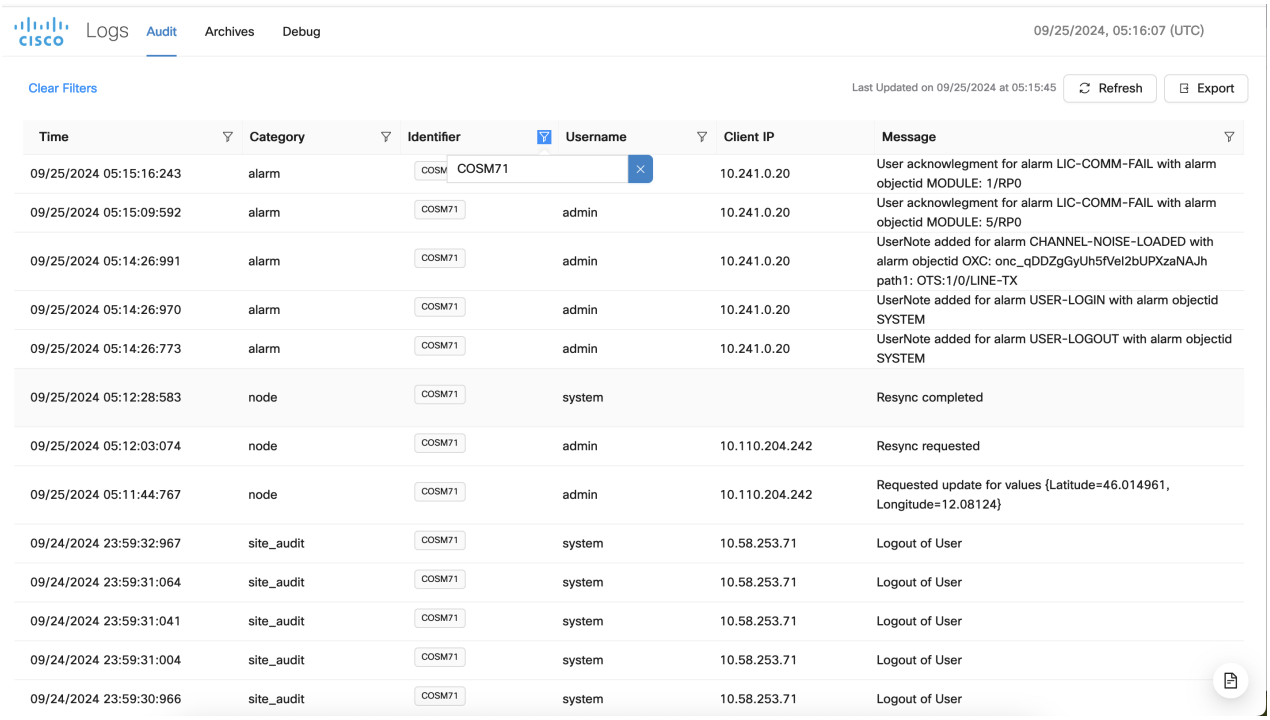


Figure 98: Archive Logs

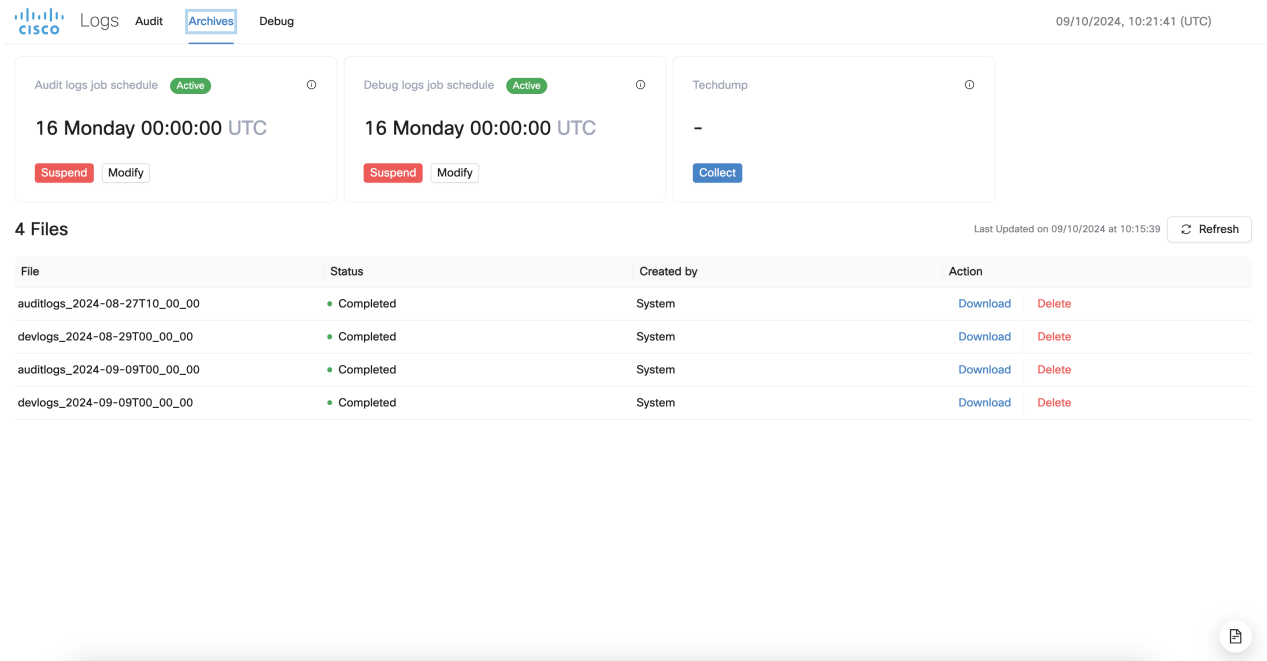


Figure 99: Scheduling Audit Logs Job

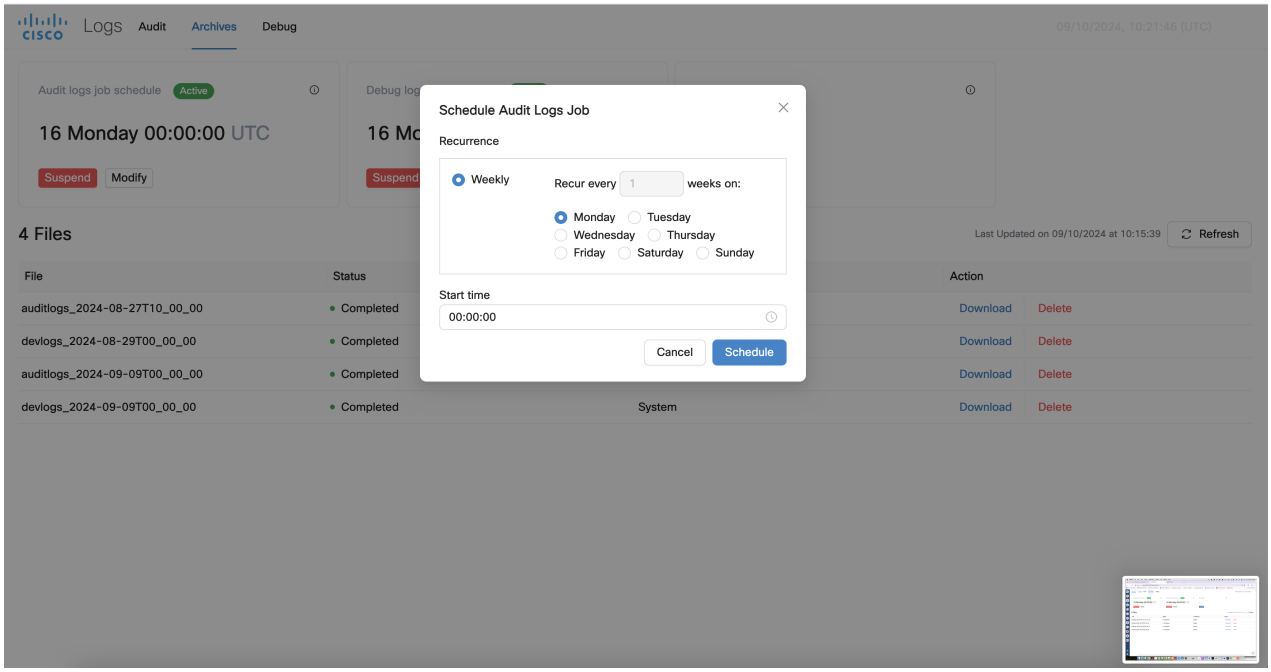
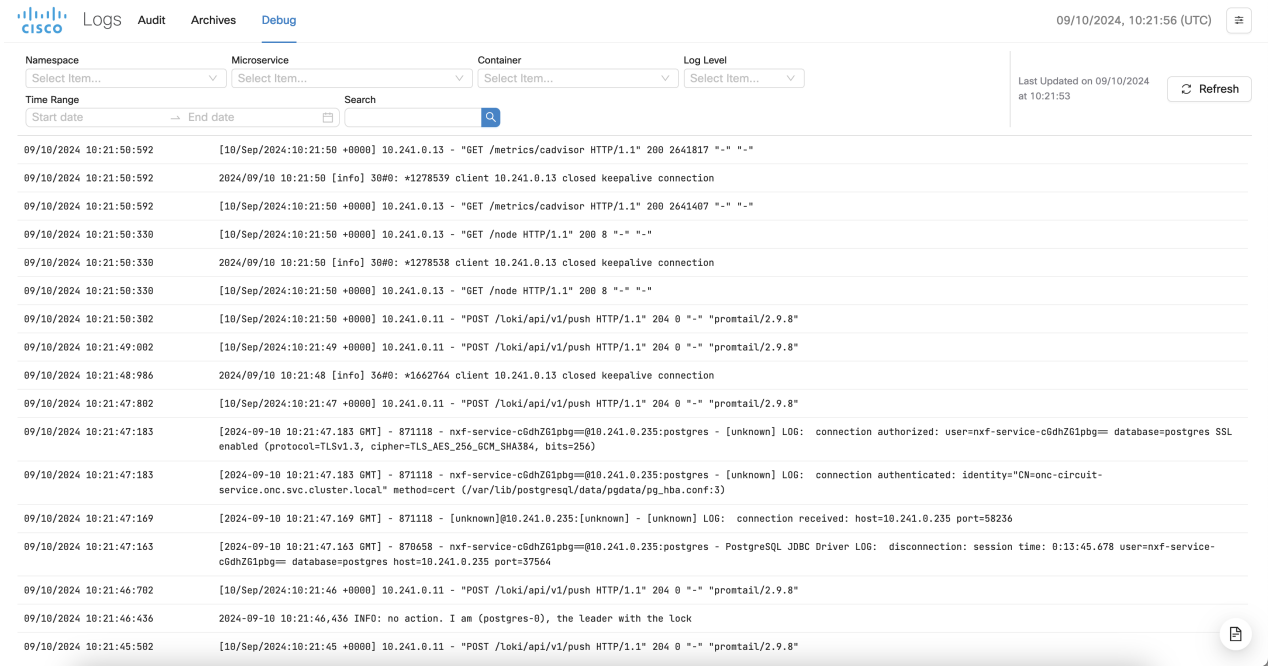


Figure 100: Debug Logs



Benefits of logs enhancement

Log enhancements help in:.

Table 82: 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.

Access logs

Use this procedure to access Cisco Optical Network Controller logs. The task helps you open the Logs application and review audit, debug, and archived log information.

Use this procedure to access logs in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

Follow these steps to access logs:

Procedure

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

   The **Logs** screen is displayed.

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**.

3. Click **Refresh** to refresh the **Audit** log table content anytime.
4. Click **Export** to export the entire **Audit** log table content to an **.xls* file.
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.

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.

The access logs task is complete.

Generate and download tech dump logs

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

Use this procedure to generate and download tech dump logs in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

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

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

Procedure

1. Click **Logs**.
2. Click **Tech Dump** tab.

   For details about the field descriptions on this tab, see Table 83: Tech dump tab field descriptions on page 236.
3. Click the **Collect** button to initiate the log collection.
   A confirmation message appears, stating that starting a new log collection will delete the existing log file.
4. Click the **Collect the DB dump** check box if you also want to collect information about CONC databases.

   Note

   Selecting this check box does not collect any sensitive information, including device credentials.
5. Click **Collect** on the dialog box.

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

   Wait for the log collection to finish.
6. Click **Download** to download the logs or **Delete** to remove them.

   Warning

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

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

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

Table 83: Tech dump tab field descriptions

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

Syslog forwarding configuration

This section provides details about syslog forwarding, including server and client installation commands. Use it to understand how Cisco Optical Network Controller forwards application logs to a syslog server.

Use this reference to understand syslog forwarding configuration.

Syslog forwarding configuration includes:

- 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

Install syslog on client includes:

- To install syslog server forwarding in client run the CLI commands in the example:.
- To create a syslog query to forward the apllication logs of a particular Cisco Optical Network Controller app:.
- The query inside single quotes is Grafana Loki's logQL, it can be tweaked according to user needs.
- To list all syslog queries:.
- To list all syslog servers:.
- To delete a syslog query:.
- To delete a syslog server:.

```
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)
```

```
 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

```
sedo syslog query list
```

```
sedo syslog server list
```

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

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

13 Monitoring

Topics:

- Monitor logs
- General troubleshooting information

Provides information about monitoring in Cisco Optical Network Controller, including log monitoring, general troubleshooting information, operational checks, and issue investigation.

Monitor logs

Use this procedure to monitor logs. The task helps you review log entries and confirm current operational status from Cisco Optical Network Controller.

Use this procedure to monitor logs in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

- **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.

Follow these steps to monitor logs:

Procedure

Click to view each option separately.

The monitor logs task is complete.

General troubleshooting information

This section provides general troubleshooting information for Cisco Optical Network Controller, including page refresh behavior after switchover. Use it to identify when a page reload is required.

Use this reference to understand general troubleshooting information.

General troubleshooting information includes:

- These are some generic troubleshooting points to consider which are common across the different applications within Cisco ONC.
- Switchover happens : Refresh the page.
- TAC case : In order to raise a TAC case, collect the sedo diagnostic logs with the command: sudo sedo diagnostics archive-logs /data Collect it along with the Grafana view.

14 Links

Topics:

- Cisco Optical Network Controller links

Explains links in Cisco Optical Network Controller, including the Links application, SLTE links, ASE services, link deployment changes, and user-channel conversion.

Cisco Optical Network Controller links

This section explains Cisco Optical Network Controller links, including link views, action options, and ASE service handling. Use it to understand link information before managing optical services.

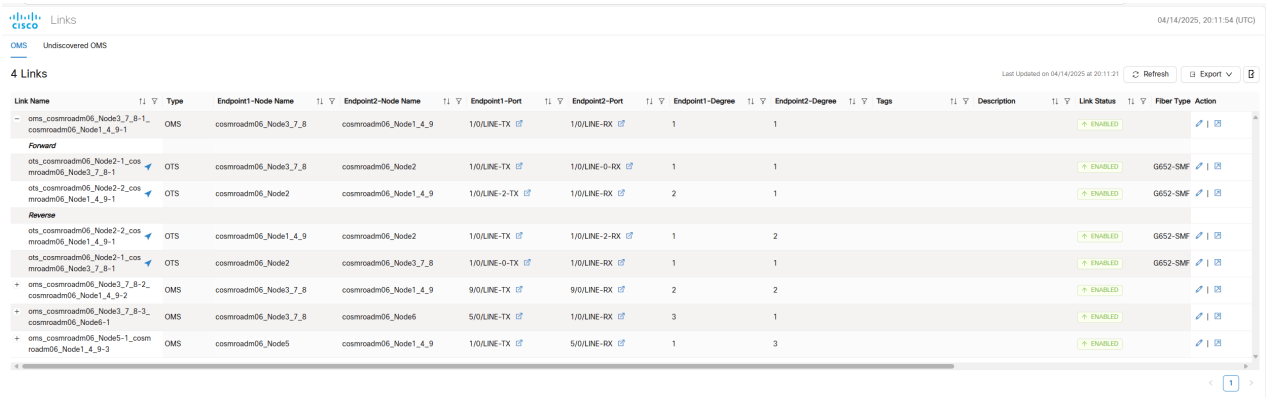
Cisco Optical Network Controller links is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

Cisco Optical Network Controller links details

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 101: Links App

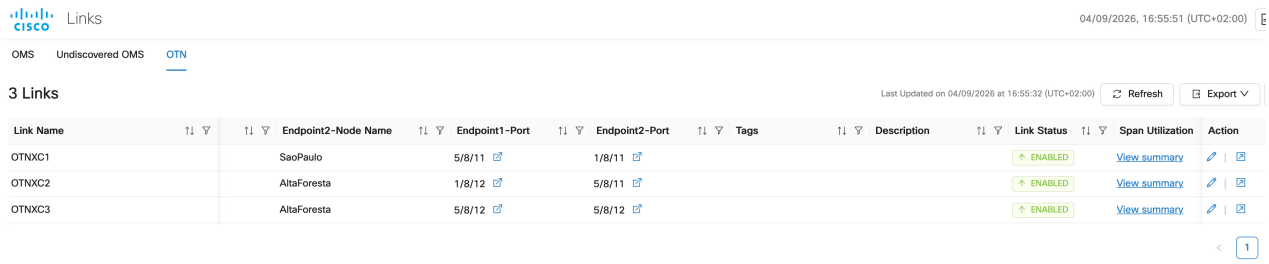


Key features of the Links app

The Links app has two tabs, OMS and Undiscovered OMS:

- **OMS tab:** Lists the discovered optical links in a hierarchical, tree-structured table. The parent row shows OMS links, which, when expanded, reveal the underlying OTS links in forward and reverse directions.
- **Undiscovered OMS tab:** Lists undiscovered OMS links, which are considered partial links. In this tab, the parent row is an OTS link.
- **OTN Links tab**: Lists the OTN links for the tranponsder networks.

Figure 102: Links app



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

Links table

The table includes these columns:

- Link Name
- Type (OMS or OTS or OTN)
- Endpoint information
- Endpoint 1 – Node Name
- Endpoint 2 – Node Name
- Endpoint 1 – Port
- Endpoint 2 – Port
- Endpoint 1 – Degree
- Endpoint 2 – Degree
- Tags
- Description
- Link Status
- Fiber Type
- OTS-specific information
- Fiber Length [km]
- Tx [dBm]
- Rx [dBm]
- Fiber Loss [dB]
- Action

The table contains these interactive options:

- **Action Column:** Provides the following actions:
- **Edit:** Allows users to edit the Link Name, Tags, and Description.
- **View Circuit Monitoring:** Cross-launches to the Circuit Monitoring page, filtering for circuits related to the selected link. This option is available only in the OMS tab and not in Undiscovered OMS tab.
- **PM History:** A small arrow icon for each OTS link provides access to PM history data.
- **OCM and OTDR Cross-Launch:** Each endpoint has a cross-launch icon to navigate to the relevant Cisco Optical Site Manager OCM (Optical Channel Monitoring) and OTDR (Optical Time Domain Reflectometer) measures. If OTDR is not supported, it navigates to alarms.

> **Note**
>
> From release 26.1.1, the Links Monitoring table supports the OTN links and features a new **Span Utilization** column that provides an overview of the ODU resource utilization summary and details.

Link monitoring workspace

Link monitoring in workspace integrates links table, topology, alarms and PM history, enabling cross-application interaction. You can select a link in the Topology App and highlight it in the Links App and vice versa.

Use the links application

Use this procedure to use the links application. This task describes the different actions that you can perform from the Links app.

This task describes the different actions that you can perform from the Links app.

This task describes the different actions that you can perform from the Links app.

Before you begin

Follow these steps to use the links application:

Procedure

1. Open the Links app from the sidebar.
2. Edit Link Attributes.
   a) Select a link in the OMS or Undiscovered OMS tab.

   > **Note**
   >
   > From release 26.1.1, for OTN networks, the Links application displays OMS Links and OTN Links attributes only.

   b) Click the edit (pencil) icon in the Action column.
   c) Modify the Link Name, Tags, or Description.
   d) Click Save to apply the changes.
3. View the Circuit Monitoring workspace for a link.
   a) Select a link in the OMS or Undiscovered OMS tab.

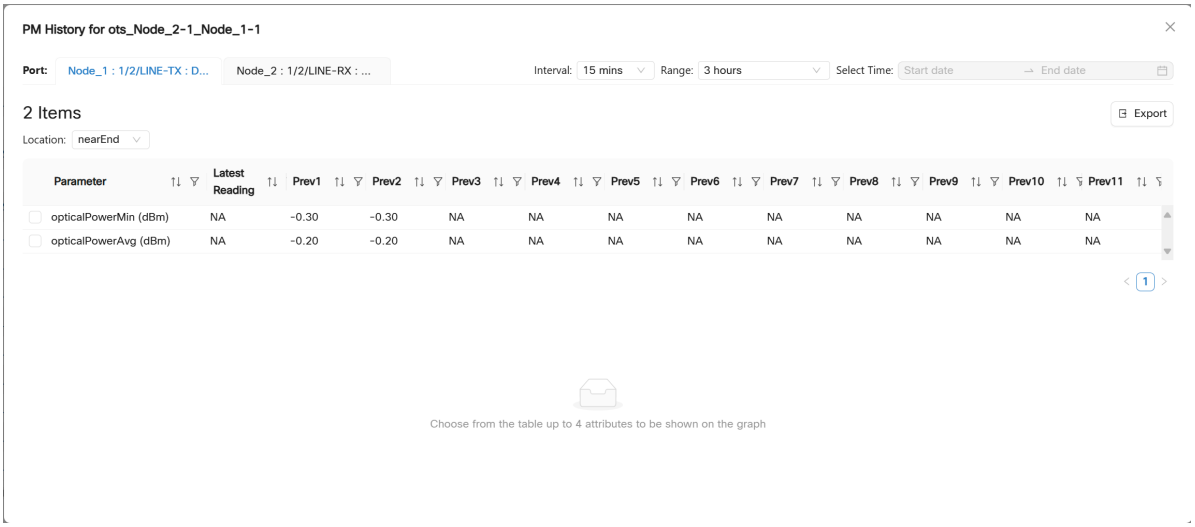
   > **Note**
   >
   > From release 26.1.1, for OTN networks, the Links application displays OMS Links and OTN Links attributes only.

   b) Click the circuit monitoring icon in the Action column.

The Circuit Monitoring page opens, filtered to display circuits related to the selected link.

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.

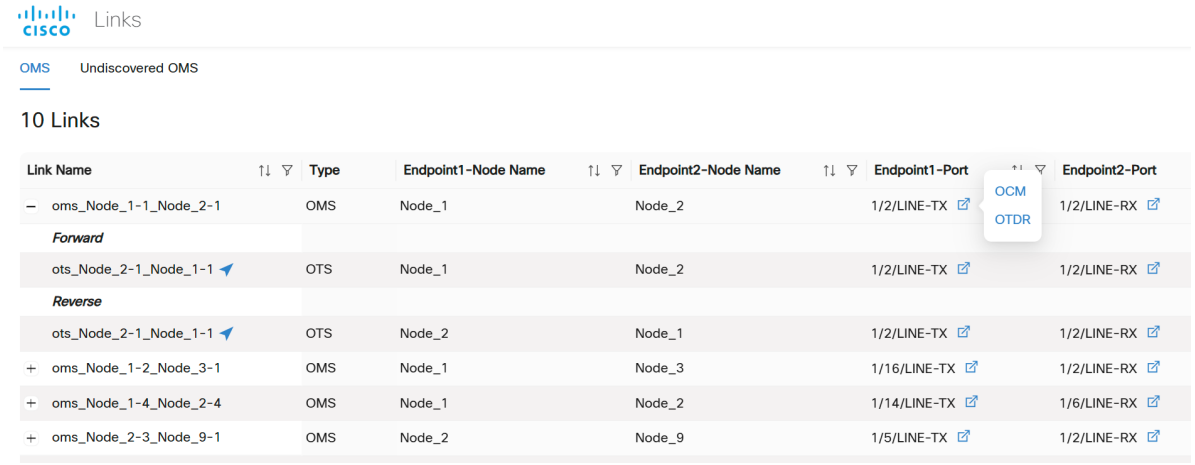
Figure 103: Links App



   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.

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 104: Links App



   c) Click **OCM** or **OTDR** to cross-launch the OCM or OTDR tab in Cisco Optical Site Manager for the selected endpoint.

   If OTDR is not supported, it navigates to alarms.

6. Export Links data.
   a) Click **Export**.
   b) Optional: Select **Table View** and click **Export** to export and download the data currently displayed in the table.

c) Select **Network Links**to export all network links.
d) Click **Generate**.
e) After the file is generated, click **Export** to download the XLS file.

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

The use the links application task is complete.

SLTE links and ASE services in Cisco Optical Network Controller

This section explains SLTE links and ASE services, including deployment behavior, ASE channel conversion, and user-channel handling. Use it to understand how Cisco Optical Network Controller manages SLTE links.

SLTE links and ASE services in Cisco Optical Network Controller is a Cisco Optical Network Controller capability that

- supports the related optical network management workflow,
- provides context for configuration, monitoring, or troubleshooting tasks, and
- helps operators understand how the feature behaves before they use it.

SLTE links and ASE services in Cisco Optical Network Controller details

An Submarine Line Terminal Equipment (SLTE) link is an optical link type that Cisco Optical Network Controller automaticlly discovers from Cisco Optical Site Manager configuration. This allows the different applications, such as Links, Topology, and Service Manager to distinguish submarine behavior from terrestrial behavior.

- Cisco Optical Network Controller shows SLTE links with the `Submarine` deployment type in **Links** app.
- Service Manager shows discovered ASE channels in a dedicated **SLTE ASE** tab.

For details

How Cisco Optical Network Controller handles SLTE links and ASE services

Use the SLTE link and ASE service views to verify discovery results and to manage the transition between discovered ASE channels and provisioned user channels.

- The submarine deployment type is discovered from Cisco Optical Site Manager and can be overridden in Cisco Optical Network Controller when the discovered topology needs correction for a custom deployment.
- The link override is applied at the OTS link level, even when the **Links** app groups the view under an OMS link.
- The **SLTE ASE** tab lists the ASE services with frequency, bandwidth, and endpoint information.
- Upgrading an ASE service converts the selected ASE channel into a user channel. Deleting that user channel adds the ASE channel back so that the spectrum remains filled.
- Cisco Optical Network Controller discovers an ASE service even when only one endpoint is available. If no matching OXC with the same frequency and bandwidth is present at the far end of the fiber, Cisco Optical Network Controller displays the ASE service as a partial discovery result with a single endpoint.

- When Cisco Optical Network Controller later discovers a matching endpoint with the same frequency and bandwidth at the other end of the fiber, it completes the ASE discovery and updates the service to show both endpoints.

Change the SLTE link deployment type

Use this procedure to change the SLTE link deployment type. Use this task in custom topologies where the submarine type is not correctly derived from link discovery.

Use this procedure to change the SLTE link deployment type in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

Use this task in custom topologies where the submarine type is not correctly derived from link discovery. Updating the deployment type aligns the Links app and topology views with the real-world link behavior.

Before you begin

- Configure the ASE channels on the submarine nodes by using XR CLI before onboarding the nodes in Cisco Optical Network Controller. For more details on configuring SLTE using XR CLI, see Sub-sea Configuration.
- Ensure that the SLTE nodes and their links are already discovered in Cisco Optical Network Controller.

Follow these steps to change an SLTE link deployment type.

Procedure

1. Click **Links** and then click the **OMS** tab.
2. Locate the required OMS link and expand the entry to show the underlying OTS links.

   The **Deployment Type** can be configured on the OTS link.
3. For the required OTS link, click **Edit** action.
4. In the **Edit Link** dialog box, select select **Submarine** or **Terrestrial** from the **Deployment Type** drop-down list.

   Select **Submarine** when the link is part of an SLTE deployment and the discovered type must be corrected.
5. Save the change.

   Cisco Optical Network Controller updates the OTS link deployment type.
6. Click **Refresh** and verify the updated deployment type in the link list.

- The selected OTS link uses the deployment type that you specified, and Cisco Optical Network Controller reflects the updated deployment type in the **Topology**.
- To filter submarine links in the **Topology** application, select **OTS** or **OMS** links, click the eye icon on the right side and select the **Filter Submarine Links** check box.

Convert SLTE ASE channel to user channel

Use this procedure to convert SLTE ASE channel to user channel. The SLTE ASE tab in Service Manager displays discovered ASE services with their endpoint, frequency, and bandwidth based on SLTE configuration.

Use this procedure to convert SLTE ASE channel to user channel in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

The **SLTE ASE** tab in **Service Manager** displays discovered ASE services with their endpoint, frequency, and bandwidth based on SLTE configuration.

During this upgrade, constraints used by other service types are not applicable to the SLTE ASE workflow.

- The configuration is rejected in these cases:
- The ASE channel central frequency and channel width exactly match the user-provided central frequency and channel width for the user channel. Remove the hardware module for the ASE channel and configure the end-to-end circuit from Cisco Optical Network Controller.
- The user channel extends beyond the ASE channel into empty spectrum. Remove the ASE channel and configure an end-to-end circuit from Cisco Optical Network Controller.
- The user channel has a narrower width than the ASE channel but uses the same central frequency. Remove the ASE channel and configure the end-to-end circuit from Cisco Optical Network Controller.
- Cisco Optical Network Controller provisions the required user circuit when a new user channel on the same add/drop port overlaps an existing user channel, provided that only frequency slices overlap and the payloads do not overlap.
- When a submarine channel is created, CPCE performs no optical validation except for central frequency and channel width.

Before you begin

Ensure that the SLTE nodes are onboarded and that the required ASE services are already discovered.

Before you convert an SLTE ASE channel to a user channel, configure ASE channels on the device through IOS XR CLI as day-1 configuration. On the LINE OTS-OCH controller, configure only egress-ase-attn and egress-channel-attn.

After Cisco Optical Network Controller converts the ASE channel to a signal channel, configure ingress-channel-attn on the COM-RX port from the Cisco Optical Site Manager OCM view.

If you configure the OTS-OCH controller through IOS XR CLI after the device is onboarded in Cisco Optical Site Manager, synchronize OXC data from the Cisco Optical Site Manager **Optical Cross Connections** tab. This synchronization updates Cisco Optical Site Manager and then Cisco Optical Network Controller.

Follow these steps to convert an SLTE ASE channel to a user channel.

Procedure

1. Click **Service Manager** and then click the **SLTE ASE** tab.

   The list of discovered ASE services is displayed.

2. Select the endpoint of the actual user channel service that you want to convert.

   Review the endpoint, frequency, and bandwidth columns to confirm that you selected the correct ASE channel.

3. Click **Upgrade** and select a service.
4. Complete the steps in the CPCE service endpoints and operations on page 75 task to finish converting the selected ASE channel to a user channel.

The selected ASE channel is converted to a user channel in Cisco Optical Network Controller, and the new user service is shown in Service Manager.

> **Note**
>
> Deleting the user channel restores the ASE channel, ensuring the spectrum is filled.

15 Alarm Troubleshooting and Categories

Topics:

- Alarm troubleshooting procedures
- Alarm categories

Summarizes alarm troubleshooting and categories in Cisco Optical Network Controller, including recovery procedures, alarm categories, severity abbreviations, and alarm impact details.

Alarm troubleshooting procedures

This section provides links to alarm troubleshooting guides for Cisco NCS 1014, Cisco NCS 1010, and Cisco NCS 1004. Use it to locate detailed alarm clearing procedures.

Use this reference to understand alarm troubleshooting information.

Alarm troubleshooting procedures include:

- 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 alarm

This section provides details about the BACKUP-FAILURE alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand bACKUP-FAILURE alarm.

Details about bACKUP-FAILURE alarm.

BACKUP-FAILURE alarm details

BACKUP-FAILURE alarm details include:

- 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

Use this procedure to clear the BACKUP-FAILURE alarm. Use the recovery steps to verify the condition and follow escalation guidance if the alarm persists.

Use this procedure to clear the BACKUP-FAILURE alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

To clear this alarm:

Before you begin

Follow these steps to clear the BACKUP-FAILURE alarm:

Procedure

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

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

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

The clear the BACKUP-FAILURE alarm task is complete.

NODE-BACKUP-FAILURE alarm

This section provides details about the NODE-BACKUP-FAILURE alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand nODE-BACKUP-FAILURE alarm.

Details about nODE-BACKUP-FAILURE alarm.

NODE-BACKUP-FAILURE alarm details

NODE-BACKUP-FAILURE alarm details include:

- 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

Use this procedure to clear the NODE-BACKUP-FAILURE alarm. Use the recovery steps to verify the condition and follow escalation guidance if the alarm persists.

Use this procedure to clear the NODE-BACKUP-FAILURE alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

To clear this alarm:

Before you begin

Follow these steps to clear the NODE-BACKUP-FAILURE alarm:

Procedure

---

1. To clear this alarm:
2. Wait until the next succesful On-demand backup or scheduled backup, the node backup failure alarm is cleared.
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).

The clear the NODE-BACKUP-FAILURE alarm task is complete.

NODE-DISCONNECT alarm

This section provides details about the NODE-DISCONNECT alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand nODE-DISCONNECT alarm.

Details about nODE-DISCONNECT alarm.

NODE-DISCONNECT alarm details

NODE-DISCONNECT alarm details include:

- 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

Use this procedure to clear the NODE-DISCONNECT alarm. Use the recovery steps to verify the condition and follow escalation guidance if the alarm persists.

Use this procedure to clear the NODE-DISCONNECT alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

To clear this alarm:

Before you begin

Follow these steps to clear the NODE-DISCONNECT alarm:

Procedure

1. Check the connectivity to the node that got disconnected and fix any network issues.
2. If the node went down, bring it back up.
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).

The clear the NODE-DISCONNECT alarm task is complete.

UPLOAD-FAILURE alarm

This section provides details about the UPLOAD-FAILURE alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand uPLOAD-FAILURE alarm.

Details about uPLOAD-FAILURE alarm.

UPLOAD-FAILURE alarm details

UPLOAD-FAILURE alarm details include:

- 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

Use this procedure to clear the UPLOAD-FAILURE alarm. Use the recovery steps to verify the condition and follow escalation guidance if the alarm persists.

Use this procedure to clear the UPLOAD-FAILURE alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

To clear this alarm:

Before you begin

Follow these steps to clear the UPLOAD-FAILURE alarm:

Procedure

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

The clear the UPLOAD-FAILURE alarm task is complete.

DISK-THRESHOLD alarm

This section provides details about the DISK-THRESHOLD alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand dISK-THRESHOLD alarm.

Details about dISK-THRESHOLD alarm.

DISK-THRESHOLD alarm details

DISK-THRESHOLD alarm details include:

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

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

Clear the DISK-THRESHOLD alarm

Use this procedure to clear the DISK-THRESHOLD alarm. Use the recovery steps to verify the condition and follow escalation guidance if the alarm persists.

Use this procedure to clear the DISK-THRESHOLD alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

To clear this alarm:

Before you begin

Follow these steps to clear the DISK-THRESHOLD alarm:

Procedure

1. Pause PM Jobs from the CONC UI
   a) Go to the PM History app.
   b) In the Summary tab, select the desired job and click the Edit button.

   > **Note**
   >
   > Only one job can be edited at a time.

   A popup window appears.
   c) Use the toggle button at the top-left corner to disable the job.
   This action pauses the job and prevents further PM data collection.
2. Remove user created files from the `/data` directory. Remove all additional files or directories under `/data` directory.

   Example

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

   Only the following folders are expected in the `/data` directory.
3. Delete ISO Files from Local SFTP.

   Example

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

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

   a) SSH into the CONC VM.
   b) Get the list of all ISO files on the VM.
   c) Delete an iso file from the list using the following command.
4. Download and Remove Archive Files from CONC UI
   a) Go to the Logs app.
   Under the Archives tab, there is the list of all available archive files.
   b) Click **Download** in the **Action** column to save the file locally.
   c) Click **Delete** in the **Action** column to delete an archive file.

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

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

The clear the DISK-THRESHOLD alarm task is complete.

SWITCHOVER alarm

This section provides details about the SWITCHOVER alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand sWITCHOVER alarm.

Details about sWITCHOVER alarm.

SWITCHOVER alarm details

SWITCHOVER alarm details include:

- 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

Use this procedure to clear the SWITCHOVER alarm. This alarm clears automatically once the switchover is complete and database replication is complete.

Use this procedure to clear the SWITCHOVER alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

Follow these steps to clear the SWITCHOVER alarm:

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).

The clear the SWITCHOVER alarm task is complete.

FAILOVER alarm

This section provides details about the FAILOVER alarm, including severity, logical object, trigger condition, and release information. Use it to understand when the alarm occurs before you follow the clearing procedure.

Use this reference to understand fAILOVER alarm.

Details about fAILOVER alarm.

FAILOVER alarm details

FAILOVER alarm details include:

- 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

Use this procedure to clear the FAILOVER alarm. This alarm clears automatically once the failover is complete and database replication is complete.

Use this procedure to clear the FAILOVER alarm in Cisco Optical Network Controller. Complete this task when you need to configure, verify, or manage the related network operation.

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

Before you begin

Follow these steps to clear the FAILOVER alarm:

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).

The clear the FAILOVER alarm task is complete.

Alarm categories

This section provides details about alarm categories, severity abbreviations, and alarm impact abbreviations. Use it to interpret alarm information in Cisco Optical Network Controller.

Use this reference to understand alarm categories and abbreviations used in alarm tables.

Cisco Optical Network Controller classifies alarms by category and condition type. Separate reference topics list the alarm and event tables for each category.

Alarm category names

Alarm categories details include:

- Cisco Optical Network Controller classifies alarms under these categories:.
- SYSTEM.
- EQUIPMENT.
- MAINTENANCE.
- CONC_SYSTEM.
- TRANSPORT.
- PROTECTION.
- TIMING.

- SECURITY.

Additional alarm category values

Alarm categories details details include:

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

Severity and impact abbreviations

Severity and impact abbreviations include:

- These abbreviations are used in the Severity and Impact columns of the alarms table in this chapter:.
- Severity.
- NA – Not Alarmed.
- CR – Critical.
- MN – Minor.
- MJ – Major.
- Impact.
- SA – Service Affecting.
- NSA – Not Service Affecting.

SYSTEM alarms

Lists the SYSTEM alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify SYSTEM alarms and their source information.

The SYSTEM alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

SYSTEM alarms

The SYSTEM alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 84: SYSTEM alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AUD-LOG-LOSS	Audit Log 100 Percent Full - Oldest records will be lost	NA	NSA	Alarm	NE SYSTEM/NCS2K/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AUD-LOG-LOW	Audit Log 80 Percent Full	NR	NSA	Alarm	NE/NCS2K
BAD-DB-DETECTED	Bad Database Detected And Database Load Failed	CR	SA	Alarm	NE/NCS2K
BAND-PARTNER-NODE-UNPAIRED	Node is unpaired from band partner node	NA	NSA	Alarm	CARD/NCS1K
COMMIT-REPLACE-FAILED	Configuration commit replace failed	MJ	SA	Alarm	NE/NCS1K
CONFIG-INCONSISTENCY	Configuration is in inconsistent state	CR	SA	Alarm	NE/NCS1K
CP-UNVER-CLEARED	Control Plane Unverified Cleared Alarms Present	CR	SA	Alarm	NE/NCS2K
DATAFLT	Software Fault - Data Integrity Fault	MN	NSA	Alarm	NE/NCS2K
DBBACKUP-IN-PROGRESS	Database Backup In Progress	-	-	Alarm	SYSTEM/SYSTEM
DBOSYNC	Standby Database Out of Sync	MJ	SA	Alarm	NE/NCS2K
DBREST-IN-PROGRESS	Database Restore In Progress	no result	-	Alarm	SYSTEM/SYSTEM
DEGREE-MISMATCH	Degree Mismatch	-	-	Alarm	OPT/SYSTEM
DISK-SPACE-FULL	No Space Left On Device	CR	SA	Alarm	SYSTEM/SYSTEM
DISK-SPACE-LOW	Low Disk Space Remaining On Device	CR	SA	Alarm	SYSTEM/SYSTEM
DR-UNAVAILABLE	Disaster recovery boot is currently unavailable due to a missing or corrupted chassis SSD. If an install transaction is in progress, this cannot be cleared until the transaction is completed	CR	SA	Alarm	SHELF/NCS1K
DUP-IPADDR	IP Address A1ready In Use Within The Same DCC Area	MN	NSA	Alarm	NE/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
DUP-NODENAME	Node name already in use within the same DCC Area	MN	NSA	Alarm	NE/NCS2K
DUP-SHELF-ID	Duplicated Shelf Identifier	MJ	SA	Alarm	SHELF/NCS2K
EVAL-LIC	Evaluation License Is In Use	MN	NSA	Alarm	CARD/NCS2K
EXT	Failure Detected External To The NE	MN	NSA	Alarm	ENVALRM/NCS2K
HELLO	OSPF Hello Fail	MN	NSA	Alarm	OPT OTUk OCn STMn ETH/NCS2K
INSTALL-IN-PROGRESS	SW Installation In Progress	NA	NSA	Alarm	CARD/NCS1K
INVALID-SYSDB	Invalid System DB	MN	NSA	Alarm	CARD/NCS2K
INVMACADR	Invalid MAC Address	MN	NSA	Alarm	BACKPLANE/NCS2K
LCMODE-CONFIG-CHANGED	LCMODE changed, delete the datapath config and reload line card	MJ	NSA	Alarm	CARD/NCS1K
LCMODE-CONFIG-INVALID	LC Mode Configuration Invalid	CR	SA	Alarm	CARD/NCS1K
LCMODE-NOT-CONFIG	LC Mode Configuration Not Applied	MJ	SA	Alarm	CARD/NCS1K
LIC-COMM-FAIL	Communications Failure With Cisco Licensing Cloud	MJ	NSA	Alarm	CARD SHELF/NCS1K
LIC-EXPIRED	License Expired	CR	SA	Alarm	CARD/NCS2K
LIC-EXPIRING-SHORTLY	License Will Expire Within 24 Hours	MJ	SA	Alarm	CARD/NCS2K
LIC-EXPIRING-SOON	License Will Expire At Any Time After 1 Day But Before 14 Days	MJ	SA	Alarm	CARD/NCS2K
LIC-MISSING	License Is Missing	CR	SA	Alarm	CARD/NCS2K
LIC-OUT-OF-COMPL	One Or More Entitlements Are Out Of Compliance	MJ	–	Alarm	CARD SHELF/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LIC-SIA-OF-COMPL-UPGRADE-BLOCKED	SW Upgrade will be blocked as SIA Grace Period has expired	MJ	SA	Alarm	CARD SHELF/NCS1K
LIC-SIA-OUT-OF-COMPL-GP-REM	SW Upgrade is still allowed as SIA Grace Period is remaining	MN	NSA	Alarm	CARD SHELF/NCS1K
LIC-UPGRADE-OF-COMPL-UPGRADE-BLOCKED	SW Upgrade will be blocked as Upgrade License Grace Period has expired	MJ	SA	Alarm	CARD SHELF/NCS1K
LIC-UPGRADE-OUT-OF-COMPL-GP-REM	SW Upgrade is still allowed as Upgrade License Grace Period is remaining	MJ	SA	Alarm	CARD SHELF/NCS1K
LINK-BROKEN	Ha link Broken	MJ	SA	Alarm	SYSTEM/SYSTEM
NE-DISCONNECTED	Connection To Managed NE Lost	MJ	SA	Alarm	NE/SYSTEM
NE-EVENT-DISCONNECTED	Event Channel To Managed NE Lost	MJ	SA	Alarm	NE/SYSTEM
NE-NOT-AUTH-ACCESS	Not Authorised Access To Managed NE	MJ	–	Alarm	NE/SYSTEM
NE-VER-NOT-SUPP	Not Supported Version Of Managed NE	MJ	SA	Alarm	NE/SYSTEM
NEIGHBOUR-MISSING	Neighbour not found	MN	NSA	Alarm	OPT/NCS1K
NO-VALID-USB-DB	No Valid USB DB exists	MN	NSA	Alarm	USB_FLASH/NCS2K
NODE-FACTORY-MODE	Node in Factory Mode	CR	–	Alarm	NE/NCS2K
NODE-INCONSISTENCIES	Owner and/or partner packages on at least one node do not match the active RP	MJ	–	Alarm	NE/NCS1K
OTN-XP-DP-FPD-PKG-MISSING	OTN XP Data Plane FPD Package Missing	NA	NSA	Alarm	CARD/NCS1K
PATCH-ACTIVATION-FAILED	Patch Activation Failed	CR	SA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
PATCH-DOWNLOAD-FAILED	Patch Download Failed	CR	SA	Alarm	NE/NCS2K
PROV-FAILED	Provisioning Failed	–	–	Alarm	CARD OPT/NCS1K
PROV-INPROGRESS	Provisioning In Progress	–	–	Alarm	SHELF CARD PPM ODUk OCH OPT OTUk/NCS1K
RESOURCES-LOW	Running Low On Resources	–	–	Alarm	CARD/NCS2K
ROUTE-OVERFLOW	OSPF Routing Table Overflow	MN	NSA	Alarm	NE/NCS2K
SFTWDOWN	Software Download In Progress	MN	NSA	Alarm	NE/NCS2K
SFTWDOWN-FAIL	Software Download Failed	MN	NSA	Alarm	NE/NCS2K
SNTP-HOST	NTP/SNTP Host Failure	MN	NSA	Alarm	NE CARD SYSTEM/NCS2K/ NCS2K-SVO-K9/SYSTEM
SOFT-VERIF-FAIL	Software Signature Verification Failed	CR	SA	Alarm	NE/NCS2K
SW-MISMATCH	Software Mismatch	NA	NSA	Alarm	CARD/NCS2K
SYSBOOT	System Reboot	MJ	SA	Alarm	NE SYSTEM/NCS2K/SYSTEM
TEMP-LIC	Temporary License Is In Use	MN	NSA	Alarm	CARD/NCS2K
UNTRUSTED-APPLICATION	Trust Not Established With CSLU/CSSM	CR	NSA	Alarm	SYSTEM/SYSTEM
USAGE-NOT-REPORTED	Licenses Usage Is Not Reported	MJ	NSA	Alarm	SYSTEM/SYSTEM

SYSTEM events

Lists the SYSTEM events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify SYSTEM events and their source information.

The SYSTEM events table lists descriptions, severity, impact, condition type, and resource type or source values.

SYSTEM events

The SYSTEM events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 85: SYSTEM events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AUD-ARCHIVE-FAIL	Archival of Audit Log Failed	-	-	Event	NE SYSTEM/NCS2K/SYSTEM
DBBACKUP-FAIL	Database Backup Failed	-	-	Event	NE SYSTEM/NCS2K/SYSTEM
DBRESTORE-FAIL	Database Restore Failed	-	-	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-MISSING-GROUP	Missing Authorization Group Information	-	-	Event	SYSTEM/SYSTEM
NE-CONFIG-INCONSISTENT	Device has the Config Blocked due to an Inconsistency	-	-	Event	NE/SYSTEM
ROLE-SWITCH-ACTIVE	Role is Switched to active	-	-	Event	SYSTEM/SYSTEM
WRMRESTART	Warm Restart	-	-	Event	NE/NCS2K

EQUIPMENT alarms

Lists the EQUIPMENT alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify EQUIPMENT alarms and their source information.

The EQUIPMENT alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

EQUIPMENT alarms

The EQUIPMENT alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 86: EQUIPMENT alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ACT-SOFT-VERIF-FAIL	Active Volume Software Signature Verification Failed	CR	SA	Alarm	CARD/NCS2K
AUTORESET	Automatic System Reset	MN	NSA	Alarm	CARD/NCS2K
AVST-FAILURE	AVST Failure	MJ	NSA	Alarm	CARD/NCS1K
AWG-DEG	AWG Temperature Degrade	MN	NSA	Alarm	OPT/NCS2K
AWG-FAIL	AWG Temperature Failure	CR	SA	Alarm	OPT/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AWG-OVERTEMP	AWG Over-Temperature	CR	SA	Alarm	OPT/NCS2K
AWG-WARM-UP	AWG Warm Up	NA	NSA	Alarm	OPT/NCS2K
BAT-FAIL	Battery Failure	MJ	SA	Alarm	PWR/NCS2K
BIOS-IMAGE-CORRUPTION	BIOS image corruption	MJ	NSA	Alarm	CARD/NCS1K
BKUPMEMP	Primary Non-Volatile Backup Memory Failure	CR	NSA	Alarm	CARD USB_FLASH/NCS2K
BP-FPGA-IMAGE-CORRUPTION	BP FPGA Image Corruption	MJ	NSA	Alarm	CARD/NCS1K
BP-FPGA-PCIE-ERROR	BP FPGA PCIE Error	MJ	SA	Alarm	CARD/NCS1K
BP-FPGA-XR-EP-FPGA-PCIE-ERROR	BP FPGA XR EP FPGA PCIe Error	MJ	NSA	Alarm	CARD/NCS1K
CARD-IS-SHUTDOWN	Card failed to come up after multiple recovery attempts	CR	SA	Alarm	CARD/NCS1K
CARD-UNREACHABLE	RemoteCard Not Reachable For Key Exchange. Retrying ...	CR	SA	Alarm	PORT/NCS2K
CASETEMP-DEG	Case Temperature Degrade	MN	NSA	Alarm	OPT/NCS2K
CLDRESTART	Cold Restart	NA	NSA	Alarm	CARD/NCS2K
COMM-FAIL	Plug-in Module Communication Failure	MN	NSA	Alarm	CARD/NCS2K/NCS1K
COMP-CARD-MISSING	Companion Card Missing	MN	NSA	Alarm	CARD/NCS2K
CONTBUS-A-18	Controller Card A To DCC A Processor Communication Failure	MJ	NSA	Alarm	CARD/NCS2K
CONTBUS-B-18	Controller Card B To DCC B Processor Communication Failure	MN	NSA	Alarm	CARD/NCS2K
CONTBUS-CLK-A	Clock Bus Failure - Shelf Controller A	MJ	NSA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
CONTBUS-CLK-B	Clock Bus Failure - Shelf Controller B	MJ	NSA	Alarm	CARD/NCS2K
CONTBUS-DISABLED	Slot Communication Disabled	CR	SA	Alarm	CARD/NCS2K
CONTBUS-IO-A	Peer To Peer Slot Communication Failure	MN	NSA	Alarm	CARD/NCS2K
CONTBUS-IO-B	Peer To Peer Slot Communication Failure	MN	NSA	Alarm	CARD/NCS2K
COOL-MISM	Cooling Profile Mismatch	NR	SA	Alarm	FAN_TRAY/NCS2K
CPP-INCAPABLE	Card/Ports Unable To Provide Protection	NA	NSA	Alarm	CARD/NCS2K
CPU-FPGA-PCIE-ERROR	CPU FPGA PCIe Error	MJ	NSA	Alarm	CARD/NCS1K
DSP-COMM-FAIL	DSP Communication Failure	MJ	SA	Alarm	OCH/NCS2K
DSP-FAIL	DSP Failure	MJ	SA	Alarm	OCH/NCS2K
EHIBATVG	Extreme High Volt	MJ	SA	Alarm	PWR/NCS2K
ELWBATVG	Extreme Low Volt	MJ	SA	Alarm	PWR/NCS2K
EPROM-SUDI-SN-MISMATCH	Card Serial Number and Certificate Serial Number Mismatch	MJ	NSA	Alarm	CARD/NCS2K
EQPT	Equipment Failure	CR	SA	Alarm	CARD ECU LCD_FLASH PPM/NCS2K
EQPT-DEGRADE	Equipment Degrade	MN	NSA	Alarm	CARD/NCS2K/NCS1K
EQPT-DIAG	Diagnostic Failure	CR	SA	Alarm	CARD/NCS2K
EQPT-FAIL	Board Failure	MJ	SA	Alarm	CARD PPM NE/NCS2K/NCS1K
EQPT-FPGA-IMAGE-AVAILABLE	Different FPGA Image Available	NR	NSA	Alarm	CARD/NCS2K
EQPT-MISS	Replaceable Equipment/Unit is Missing	CR	SA	Alarm	CARD FAN_TRAY ECU LCD_FLASH PWR/NCS2K
ETH-LINKLOSS	Rear Panel Ethernet Link Removed	NA	NSA	Alarm	NE/NCS2K
FAN	Fan Failure	CR	SA	Alarm	FAN_TRAY/NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
FAN-OUT-OF-TOLERANCE	Fan Out of tolerance	MN	NSA	Alarm	FAN_TRAY FAN_ENV/NCS1K
FAN-POWER-ERROR	FAN tray Power Error	MJ	NSA	Alarm	FAN_TRAY/NCS1K
FAN-SENSOR-FAILED	Sensor in failed state	MJ	SA	Alarm	FAN_TRAY FAN_ENV/NCS1K
FANDEGRADE	Partial Fan Failure	MN	NSA	Alarm	FAN_TRAY/NCS2K/NCS1K
FEED-MISMATCH	Feed Not Available/Improper Connection	MN	NSA	Alarm	PWR/NCS2K
FIBERTEMP-DEG	Fiber Temperature Degrade	MN	NSA	Alarm	OPT/NCS2K
FIRMWARE-UPG	Firmware Upgrade In Progress	NA	NSA	Alarm	CARD PPM/NCS2K
FIRMWARE-UPG-FAIL	Firmware Upgrade Failed	MJ	SA	Alarm	CARD PPM/NCS2K
FLASH0-ERROR	CPU Flash 0 Error	MJ	NSA	Alarm	CARD/NCS1K
FLASH1-ERROR	CPU Flash 1 Error	MJ	NSA	Alarm	CARD/NCS1K
FPD-UPG-REQUIRED	Firmware upgrade required	MJ	NSA	Alarm	PPM CARD SHELF FAN_TRAY PWR/NCS2K/NCS1K
FPGA-ERROR	BP FPGA Error	MJ	NSA	Alarm	CARD/NCS1K
FPGA-SEU-UNCORR	BP FPGA SEU Uncorrected Error	CR	SA	Alarm	CARD/NCS1K
FPGA-UPGRADE-FAILED	FPGA Upgrade fail	CR	SA	Alarm	CARD/NCS2K/NCS1K
FTA-MISMATCH	FanTray Mismatch	NA	NSA	Alarm	CARD/NCS2K
HI-LASERBIAS	Equipment High Laser Bias	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
HI-LASERTEMP	Equipment High Laser Temp	MN	NSA	Alarm	OCH/NCS2K
HI-TXPOWER	Equipment High Tx power	MJ	SA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
HIBATVG	High Volt	CR	SA	Alarm	PWR/NCS2K
HIGH-VOLTAGE	high voltage alarm	CR	SA	Alarm	CHASSIS_ENV_VOLTAGE MODULE_ENV_VOLTAGE/NCS1K
HITEMP	High Temperature	CR	SA	Alarm	CARD/NCS2K
HITEMP	High Temperature	NA	NSA	Alarm	NE/NCS2K
I-HITEMP	Industrial High Temperature	NA	NSA	Alarm	NE/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
IMPROPRMVL	Improper Removal	MN	NSA	Alarm	CARD PPM PORT SHELF FAN_TRAY/NCS2K /NCS2K-SVO-K9/SYSTEM/NCS1K
IMPROPRMVL-FS	Improper removal of Fiber Shuffle	MJ	SA	Alarm	PASSIVE_SHELF/NCS2K
INVALID-CARD-SLOT	Invalid Card Slot	MJ	NSA	Alarm	CARD/NCS1K
INVALID-SENSOR-READ-ERR	Invalid sensor read error	MN	NSA	Alarm	CHASSIS_ENV_VOLTAGE MODULE_ENV_ VOLTAGE/NCS1K
LAN-POL-REV	Lan Connection Polarity Reversed	MJ	NSA	Alarm	NE/NCS2K
LASERBIAS-DEG	Laser Bias Degrade	MN	NSA	Alarm	OCH/NCS2K
LASERBIAS-FAIL	Laser Bias Failure	CR	SA	Alarm	OCH/NCS2K
LASEREOL	Laser Approaching End of Life	MJ	NSA	Alarm	OCH/NCS2K
LASERTEMP-DEG	Laser Temperature Degrade	MJ	SA	Alarm	OCH/NCS2K
LC-BOOT-TIMEOUT	LC Boot Timeout	MJ	SA	Alarm	CARD/NCS1K
LC-CPU-IMAGE-CORRUPTION	LC CPU Image Corruption	NA	NSA	Alarm	CARD/NCS1K
LC-DP-IMAGE-CORRUPTION	LC Data Plane Image Corruption	NA	NSA	Alarm	CARD/NCS1K
LC-FPD-DEV-FAILURE	CPU_MOD_FW is corrupt, system booted with golden copy	NA	NSA	Alarm	CARD/NCS1K
LC-OFFLINE-ERROR	LC Offline Error	NA	NSA	Alarm	CARD/NCS1K
LO-LASERBIAS	Equipment Low Laser Bias	MN	NSA	Alarm	OCH/NCS2K
LO-LASERTEMP	Equipment Low Laser Temp	MN	NSA	Alarm	OCH/NCS2K
LO-TXPOWER	Equipment Low Tx power	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
LOW-VOLTAGE	low voltage alarm	CR	SA	Alarm	CHASSIS_ENV_VOLTAGE MODULE_ENV _VOLTAGE/NCS1K
LSC-NOT-PRESENT-MIC-IN-USE	LSC not present using MIC	MJ	NSA	Alarm	CARD/NCS2K
LWBATVG	Low Volt	MJ	SA	Alarm	PWR/NCS2K
MB-SSD-ATA-ERRORS	Motherboard SSD ATA Errors	CR	SA	Alarm	CARD/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
MEA	Mismatch Of Equipment And Attributes	CR	SA	Alarm	FAN_TRAY CARD PPM PASSIVE_UNIT/ NCS2K/NCS2K-SVO-K9/SYSTEM
MEA	Mismatch Of Equipment And Attributes	CR	SA	Alarm	SHELF NE PASSIVE_SHELF PORT/ NCS2K/NCS2K-SVO-K9/SYSTEM
MEM-GONE	Free Memory On Card Near Zero	MJ	SA	Alarm	CARD/NCS2K
MEM-LOW	Free Memory On Card Very Low	MN	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
MFGMEM	Manufacturing Data Memory (EEPROM) Failure	CR	SA	Alarm	FAN_TRAY ECU LCD_FLASH PWR BACKPLANE PPM/NCS2K
NODE-OBFL-ERROR	Node OBFL Error	MJ	NSA	Alarm	CARD/NCS1K
NON-CISCO-PPM	Non Cisco PPM Inserted	MN	NSA	Alarm	PPM PORT/NCS2K/NCS2K-SVO-K9
ONE-OR-MORE-FAN-TRAY-ABSENT	One or more Fan Trays missing	MJ	NSA	Alarm	SHELF/NCS1K
ONE-OR-MORE-LC-MISSING	One or more LCs missing, running fans at max speed	CR	SA	Alarm	SHELF/NCS1K
OPEN-SLOT	Open Slot(s)	MN	NSA	Alarm	CARD SHELF/NCS2K
OPT-MOD-ABSENT	One or more Optical Modules missing	CR	SA	Alarm	CARD/NCS1K
OVER-TEMP-UNIT-PROT	Over Temperature Unit Protected	CR	SA	Alarm	OCH/NCS2K
PEX-SWITCH-ACCESS-FAILURE	PEX Switch Access Failure	MJ	NSA	Alarm	CARD/NCS1K
PORT-COMM-FAIL	Module Communication Failure	CR	SA	Alarm	PORT/NCS2K
POWER-MODULE-FAN-OUT-OF-TOLERANCE	Power Module: fan out of tolerance	MN	NSA	Alarm	PWR/NCS1K
POWER-MODULE-FAN-OUT-OF-TOLERANCE-WARNING	Power Module Warning: fan out of tolerance	MN	NSA	Alarm	PWR/NCS1K
POWER-MODULE- OUTPUT-DISABLED	Power Module Output Disable	MJ	SA	Alarm	PWR/NCS1K
POWER-MODULE- REDUNDANCY-LOST	Power Module Redundancy lost	MJ	SA	Alarm	PWR SHELF/NCS1K
POWER-OFF	Card In Power Off Status	MJ	NSA	Alarm	CARD/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
POWER-ON-TIMEOUT	Card In Power On Timeout	MJ	NSA	Alarm	CARD/NCS1K
PPM-MISMATCH	Incompatible pluggable inserted in the port	CR	SA	Alarm	PPM/NCS1K
PROTNA	Protection Unit Not Available	MN	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
PROV-INCOMPATIBLE	Incompatible Provision	-	-	Alarm	CARD/NCS1K
PROV-MISMATCH	Provisioning Mismatch	MN	NSA	Alarm	PORT/NCS2K/ NCS2K-SVO-K9/SYSTEM/NCS1K
PROV-MISMATCH	Provisioning Mismatch	MN	NSA	Alarm	CARD PPM/NCS2K/ NCS2K-SVO-K9/SYSTEM/NCS1K
PWR	Power Failure at Connector	-	-	Alarm	PWR/NCS2K
PWR-CON-LMT	Power Consumption Limit Has Crossed	MN	NSA	Alarm	SHELF/NCS2K
PWR-ERROR	Power Module Error (PM_VIN_VOLT_OOR)	-	-	Alarm	SHELF/NCS1K
PWR-EXCEEDS	Power reservation exceeds configured power	-	-	Alarm	PWR/NCS1K
PWR-EXCEEDS-CAPACITY	Power reservation exceeds configured power capacity	-	-	Alarm	PWR/NCS1K
PWR-FAIL-A	Equipment power failure at connector A	MN	NSA	Alarm	PWR/NCS2K
PWR-FAIL-B	Equipment power failure at connector B	MN	NSA	Alarm	PWR/NCS2K
PWR-FAIL-RET-A	Equipment power failure at return connector A	MN	NSA	Alarm	PWR/NCS2K
PWR-FAIL-RET-B	Equipment power failure at return connector B	MN	NSA	Alarm	PWR/NCS2K
PWR-GRP-REDUNDANCY-LOST	Power Group Redundancy lost	MJ	SA	Alarm	SHELF/NCS1K
PWR-MISMATCH	PEM PID mismatch in the chassis	-	-	Alarm	SHELF/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
PWR-OUTPUT-DISABLED	Power Module Output Disabled	MJ	SA	Alarm	SHELF/NCS1K
PWRRESTART	Powerfail Restart	-	-	Alarm	NE/NCS2K
RACK-OBFL-ERROR	Obfl error	MJ	NSA	Alarm	SHELF/NCS1K
RESOURCE-ALLOC-FAIL	Resource Allocation Failed	MN	SA	Alarm	CARD/NCS2K
RESOURCES-GONE	No More Resources Available	MN	NSA	Alarm	CARD/NCS2K
RUNNING-FANS-AT-MAX-SPEED	FANs Running At Maximum Speed	CR	SA	Alarm	FAN_TRAY/NCS1K
SENSOR-HIGH-0-6V-CPU-A	0.6V-CPU-A sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-0-6V-CPU-B	0.6V-CPU-B sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-05V-CPU	1.05V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-0V	1.0V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-0V-PHY	1.0V-PHY sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-2V	1.2V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-2V-CPU	1.2V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-3V-CPU	1.3V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-5V-CPU	1.5V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-7V-CPU	1.7V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-82V-CPU	1.82V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-1-8V	1.8V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-2-5V	2.5V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-3-3V	3.3V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-3-3V-CPU	3.3V-CPU sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-3-3V-STBY	3.3V-STBY sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-5-0V-STBY	5.0V-STBY sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SENSOR-HIGH-BP-48V	BP-48V sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-CPU-TEMP	CPU-TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-DDR-CH0-TEMP	DDR-CH0- TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-DDR-CH1-TEMP	DDR-CH1- TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-ETHERNET -SWITCH-TEMP	ETHERNET-SWITCH-TEMP sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-HOTSPOT1	HOTSPOT1 sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-HOTSPOT2	HOTSPOT2 sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-INLET-AIR	INLET-AIR sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-HIGH-OUTLET-AIR	OUTLET-AIR sensor high	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-0-6V-CPU-A	0.6V-CPU-A sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-0-6V-CPU-B	0.6V-CPU-B sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-05V-CPU	1.05V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-0V	1.0V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-0V-PHY	1.0V-PHY sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-2V	1.2V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-2V-CPU	1.2V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-3V-CPU	1.3V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-5V-CPU	1.5V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-7V-CPU	1.7V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-82V-CPU	1.82V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-1-8V	1.8V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-2-5V	2.5V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SENSOR-LOW-3-3V	3.3V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-3-3V-CPU	3.3V-CPU sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-3-3V-STBY	3.3V-STBY sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-5-0V-STBY	5.0V-STBY sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-BP-48V	BP-48V sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-CPU-TEMP	CPU-TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-DDR-CH0-TEMP	DDR-CH0- TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-DDR-CH1-TEMP	DDR-CH1- TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-ETHERNET-SWITCH-TEMP	ETHERNET-SWITCH-TEMP sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-HOTSPOT1	HOTSPOT1 sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-HOTSPOT2	HOTSPOT2 sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-INLET-AIR	INLET-AIR sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SENSOR-LOW-OUTLET-AIR	OUTLET-AIR sensor low	MN	NSA	Alarm	CARD/NCS2K-SVO-K9
SHELF-COMM-FAIL	Shelf Communication Failure	MJ	SA	Alarm	SHELF/NCS2K
SSD-ATA-ERRORS	CPU SSD ATA Error	CR	SA	Alarm	CARD/NCS1K
SSD-HI-TEMP	CPU SSD High Temperature	MJ	NSA	Alarm	CARD/NCS1K
TEMP-MISM	Temperature Reading Mismatch Between SC Cards	NA	NSA	Alarm	NE/NCS2K
TEMPERATURE	Temperature out of working range	CR	SA	Alarm	CHASSIS_ENV_TEMPERATURE MODULE_ENV_TEMPERATURE PWR_ENV_TEMPERATURE/NCS1K
TRAF-AFFECT-RESET-REQUIRED	Traffic Affecting Reset Required	MN	NSA	Alarm	CARD/NCS2K
TRAF-AFFECT-SEC-UPG-REQUIRED	Traffic Affecting Security Upgrade Required	NR	NSA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
UNIT-HIGH-TEMP	Unit High Temperature	MN	NSA	Alarm	CARD/NCS2K
UNQUAL-PPM	Unqualified PPM Inserted	NR	NSA	Alarm	PPM PORT/NCS2K/ NCS2K-SVO-K9/NCS1K
USB-MOUNT-FAIL	USB Mount Failure	CR	SA	Alarm	USB_FLASH/NCS2K
USB-OC-1	USB 1 Over Current	MJ	NSA	Alarm	USB_FLASH/NCS1K
USB-OC-2	USB 2 Over Current	MJ	NSA	Alarm	USB_FLASH/NCS1K
USB-WRITE-FAIL	USB Write Failure	CR	SA	Alarm	USB_FLASH/NCS2K
USBSYNC	USB Sync in Progress	NA	NSA	Alarm	USB_FLASH/NCS2K
VOLT-MISM	Voltage Reading Mismatch Between SC Cards	NA	NSA	Alarm	PWR/NCS2K/NCS1K
XGE-EEPROM-ERROR	XGE EEPROM Error	MJ	SA	Alarm	CARD/NCS1K
XGE-FLASH-ERROR	XGE Flash Error	–	–	Alarm	CARD/NCS1K

EQUIPMENT events

Lists the EQUIPMENT events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify EQUIPMENT events and their source information.

The EQUIPMENT events table lists descriptions, severity, impact, condition type, and resource type or source values.

EQUIPMENT events

The EQUIPMENT events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 87: EQUIPMENT events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
FIRMWARE-DOWNLOAD	Firmware Download In Progress	–	–	Event	CARD PPM/NCS2K
FIRMWARE-UPG-COMPLETE	Firmware Upgrade Completed	–	–	Event	CARD PPM/NCS2K
USB-PORTS-DOWN	USB Ports in ECU are not functional	–	–	Event	ECU/NCS2K

MAINTENANCE alarms

Lists the MAINTENANCE alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify MAINTENANCE alarms and their source information.

The MAINTENANCE alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

MAINTENANCE alarms

The MAINTENANCE alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 88: MAINTENANCE alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AS-CMD	Alarms Suppressed By User Command	NA	NSA	Alarm	OCH ETH OCn STMn ODUk OTUk zrPlus OPT OXC CARD FC PASSIVE_SHELF PORT PPM RAMAN_AMPLIFIER SHELF/NCS2K
AS-MT	Alarms Suppressed For Maintenance	NA	NSA	Alarm	OCH ETH OCn STMn ODUk OTUk zrPlus OPT OXC CARD FC PASSIVE_SHELF PORT PPM RAMAN_AMPLIFIER SHELF/NCS2K/NCS1K
BP-LPBKFACILITY	Back-panel Facility Loopback	NA	NSA	Alarm	CARD/NCS2K
BP-LPBKTERMINAL	Back-panel Terminal Loopback	NA	-	Alarm	CARD/NCS2K
IPC-LASER-FAIL	Ipc Laser failure	MN	NSA	Alarm	CARD/NCS2K
IPC-LOOPBACK-MISS	Patchcords Verification Loopback Missing	MJ	NSA	Alarm	OPT OXC/NCS2K
IPC-VERIFICATION-DEGRADE	Patchcords Verification Degrade	NA	NSA	Alarm	SYSTEM/NCS2K
IPC-VERIFICATION-EXCESSIVE-LOSS	Measured Patchcord Loss above the Threshold	MJ	SA	Alarm	SYSTEM/NCS1K
IPC-VERIFICATION-FAIL	Patchcords Verification Failure	MJ	SA	Alarm	SYSTEM/NCS2K
IPC-VERIFICATION-RUNNING	Patchcords Verification Running	NA	NSA	Alarm	SYSTEM/NCS2K
LPBKFACILITY	Facility Loopback	NA	NSA	Alarm	OCn STMn ETH zrPlus OTUk ODUk OCH OPT/NCS2K/NCS1K
LPBKTERMINAL	Terminal Loopback	NA	NSA	Alarm	OCn STMn ETH zrPlus OTUk ODUk OCH OPT/NCS2K/NCS1K
MANRESET	Manual System Reset	NA	NSA	Alarm	CARD/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
OCHNC-MT	OCHNC Maintenance	MN	–	Alarm	OXC/NCS2K
OTDR-ABSOLUTE-A-EXCEEDED-RX	Attenuation Exceeded Absolute Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ABSOLUTE-A-EXCEEDED-TX	Attenuation Exceeded Absolute Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ABSOLUTE-R-EXCEEDED-RX	Reflectance Exceeded Absolute Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-ABSOLUTE-R-EXCEEDED-TX	Reflectance Exceeded Absolute Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K/NCS1K
OTDR-BASELINE-A-EXCEEDED-RX	Attenuation Exceeded Baseline Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-BASELINE-A-EXCEEDED-TX	Attenuation Exceeded Baseline Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-BASELINE-R-EXCEEDED-RX	Reflectance Exceeded Baseline Threshold - RX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-BASELINE-R-EXCEEDED-TX	Reflectance Exceeded Baseline Threshold - TX Direction	MJ	NSA	Alarm	OPT/NCS2K
OTDR-FAST-FAR-END-IN-PROGRESS	OTDR Fast Scan Is In Progress On Remote Side	MN	NSA	Alarm	OTDR/NCS2K
OTDR-FAST-SCAN-IN-PROGRESS-RX	OTDR Fast Scan Is In Progress - RX Direction	MN	NSA	Alarm	OPT/NCS2K
OTDR-FAST-SCAN-IN-PROGRESS-TX	OTDR Fast Scan Is In Progress - TX Direction	MN	NSA	Alarm	OPT/NCS2K
OTDR-FIBER-END-NOT-DETECTED-RX	Fiber End Not Detected - RX Direction	NA	NSA	Alarm	OPT/NCS2K

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

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
OTDR-SCAN-IN-PROGRESS-RX	OTDR Scan In Progress RX	MN	NSA	Alarm	OPT/NCS1K
OTDR-SCAN-IN-PROGRESS-TX	OTDR Scan In Progress TX	MN	NSA	Alarm	OPT/NCS1K
OTDR-SCAN-NOT-COMPLETED	OTDR Scan Not Completed	MN	NSA	Alarm	OTDR/NCS2K
TD-INPROGRESS	Tone Detection In Progress	MN	NSA	Alarm	OPT/NCS1K
TG-INPROGRESS	Tone Generation In Progress	MN	NSA	Alarm	OPT/NCS1K

MAINTENANCE events

Lists the MAINTENANCE events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify MAINTENANCE events and their source information.

The MAINTENANCE events table lists descriptions, severity, impact, condition type, and resource type or source values.

MAINTENANCE events

The MAINTENANCE events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 89: MAINTENANCE events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
TD-FAILED	Tone Detection Failed	-	-	Event	OPT/NCS1K
TD-LASER-ON	Tone Detection Laser is ON	-	-	Event	OPT/NCS1K
TD-SUCCESS	Tone Detection Success	-	-	Event	OPT/NCS1K

CONC_SYSTEM alarms

Lists the CONC_SYSTEM alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify CONC_SYSTEM alarms and their source information.

The CONC_SYSTEM alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

CONC_SYSTEM alarms

The CONC_SYSTEM alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 90: CONC_SYSTEM alarms

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

TRANSPORT alarms

Lists the TRANSPORT alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify TRANSPORT alarms and their source information.

The TRANSPORT alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

TRANSPORT alarms

The TRANSPORT alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 91: TRANSPORT alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AIS	Alarm Indication Signal	NR	NSA	Alarm	OCn/NCS2K
AIS-L	Alarm Indication Signal Line	NR	NSA	Alarm	OCn/NCS2K/NCS1K
APS-PROV-MISM	APS Protection Type Mismatch	MN	NSA	Alarm	ODUk/NCS2K
AUTH-EC	Payload Authentication Error Count	MJ	NSA	Alarm	ODUk/NCS2K

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

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

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LOA	Loss of Alignment	CR	SA	Alarm	OCH/NCS2K
LOCAL-FAULT	Local Fault	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
LOF	Loss Of Frame	CR	SA	Alarm	OCn STMn/NCS2K/NCS1K
LOF	Loss Of Frame	CR	SA	Alarm	BITS/NCS2K/NCS1K
LOM	Loss of Multi-Frame	CR	SA	Alarm	OCn STMn BITS/NCS2K/NCS1K
MAX-AUTH-LIST	Reached Max Authentication List	MJ	SA	Alarm	ODUk/NCS2K
MS-AIS	AIS - Multiplex Section - Alarm Indication Signal	NR	NSA	Alarm	STMn/NCS2K/NCS1K
MS-DEG	Multiplex Section - Signal Degraded	NA	NSA	Alarm	STMn/NCS2K
MS-EOC	Multiplex Section DCC Termination Failure	MN	NSA	Alarm	STMn/NCS2K
MS-EXC	Multiplex Section - Excessive Errors	NA	NSA	Alarm	STMn/NCS2K
MS-RDI	RDI - Multiplex Section - Remote Defect/Alarm Indication	MJ	SA	Alarm	STMn/NCS2K/NCS1K
NO-SHARED-CIPHERS	Different Ciphers Used by Client and Server	MJ	SA	Alarm	ODUk/NCS2K
NOS	Not-Operational primitive Sequence	CR	SA	Alarm	FC/NCS1K
OCHNC-INC	Optical Channel Incomplete	MN	–	Alarm	OXC/NCS2K
OCHTERM-INC	Optical Termination Incomplete	NR	NSA	Alarm	OXC/NCS2K
ODUK-1-AIS-PM	ODUk1 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-2-AIS-PM	ODUk2 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-3-AIS-PM	ODUk3 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-4-AIS-PM	ODUk4 Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
ODUK-AIS-PM	ODUk: PM Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-BDI-PM	ODUk: PM Backward Defect Indication	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-LCK-PM	ODUk: Locked Defect - PM	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-OCI-PM	ODUk: Open Connection Indication	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-SD-PM	ODUk: Signal Degrade	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-SF-PM	ODUk: Signal Failure	NA	SA	Alarm	ODUk/NCS2K/NCS1K
ODUK-TIM-PM	ODUk: Trail Trace Identifier Mismatch	MJ	SA	Alarm	ODUk/NCS2K/NCS1K
OPU-CSF	OPU Client Signal Fail	CR	SA	Alarm	ODUk/NCS2K/NCS1K
OSNR	Optical Signal-to-Noise Ratio	MN	NSA	Alarm	OCH/NCS1K
OTUK-AIS	OTUk: Alarm Indication Signal	NA	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-BDI	OTUk: SM Backward Defect Indication	NA	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-BIAE	OTUk: SM Backward Incoming Alignment Error	MN	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-IAE	OTUk: Incoming Alignment Error	MN	NSA	Alarm	OTUk/NCS2K/NCS1K
OTUK-LOF	OTUk: Loss Of Frame	CR	SA	Alarm	OTUk/NCS2K/NCS1K
OTUK-SD	OTUk: Signal Degrade	NA	SA	Alarm	OTUk/NCS2K/NCS1K
OTUK-SF	OTUk: Signal Failure	NA	SA	Alarm	OTUk/NCS2K/NCS1K
OTUK-TIM	OTUk: Trail Trace Identifier Mismatch	CR	SA	Alarm	OTUk/NCS2K/NCS1K
PCS-ERROR	PCS Error/Invalid	-	-	Alarm	FC/NCS1K
PEER-CERT-VERIFICATION-FAILED	Peer card certificate verification failed	MJ	NSA	Alarm	ODUk/NCS2K
PEER-CSF	Peer Port Client Signal Fail Detected	MJ	SA	Alarm	ODUk/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
PRBS-ENABLED	PRBS Generation Enabled	NA	NSA	Alarm	ODUk/NCS2K
PTIM	Payload Type Identifier Mismatch	MJ	SA	Alarm	ODUk/NCS2K/NCS1K
RDI-L	Remote Defect Indication Line	-	-	Alarm	OCn/NCS2K
REMOTE-CERT-FAIL	RemoteCard Certificate Validation Failed	-	-	Alarm	ODUk/NCS2K
REMOTE-FAULT	Remote Fault	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
RS-EOC	Regenerator Section - DCC Termination Failure	MN	NSA	Alarm	STMn/NCS2K
RS-TIM	Regenerator Section Trace Identifier Mismatch	CR	SA	Alarm	STMn/NCS2K/NCS1K
SD-L	BER Threshold Exceeded For Signal Degrade Line	NA	SA	Alarm	OCn/NCS2K
SIP	Startup In Progress	NA	NSA	Alarm	OXC/NCS2K/NCS1K
SQUELCHED	Equipment Squelched	NA	NSA	Alarm	OCH ODUk FC/NCS2K/NCS1K
TIM-S	Section Trace Identifier Mismatch	CR	SA	Alarm	OCn/NCS2K
TRAIL-SIGNAL-FAIL	Trail Signal Fail	NA	NSA	Alarm	OPT OXC/NCS2K
TRUNK-ODU-AIS	Trunk ODU Alarm Indication Signal	NR	NSA	Alarm	ODUk/NCS2K
TRUNK-OPU-CSF	Trunk OPU Client Signal Fail	NR	NSA	Alarm	ODUk/NCS2K
TRUNK-PAYLOAD-MISM	Trunk Payload Type Mismatch	MJ	SA	Alarm	ODUk/NCS2K
UNC-WORD	FEC Uncorrected Word	NA	NSA	Alarm	OCH OTUk/NCS2K/NCS1K

TRANSPORT events

Lists the TRANSPORT events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify TRANSPORT events and their source information.

The TRANSPORT events table lists descriptions, severity, impact, condition type, and resource type or source values.

TRANSPORT events

The TRANSPORT events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 92: TRANSPORT events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
DEG-SER	FEC Degraded Symbol Error Rate	–	–	Event	ETH/NCS1K
HI-SER	High Symbol Error Rate	CR	SA	Event	ETH/NCS1K
LOCAL-DEG-SER	Local FEC Degraded Symbol Error Rate	–	–	Event	ETH/NCS1K
ODUK-AIS-TCM1	TCM1 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM2	TCM2 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM3	TCM3 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM4	TCM4 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM5	TCM5 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-AIS-TCM6	TCM6 Alarm Indication Signal	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM1	TCM1 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM2	TCM2 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM3	TCM3 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM4	TCM4 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM5	TCM5 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BDI-TCM6	TCM6 Backward Defect Monitoring	–	–	Event	ODUk/NCS1K
ODUK-BIAE	Path Monitoring Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K
ODUK-BIAE-TCM1	TCM1 Backward Incoming Alignment Error	–	–	Event	ODUk/NCS1K

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

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-LTC-TCM3	TCM3 Loss of Tandem Connection	-	-	Event	ODUk/NCS1K
ODUK-LTC-TCM4	TCM4 Loss of Tandem Connection	-	-	Event	ODUk/NCS1K
ODUK-LTC-TCM5	TCM5 Loss of Tandem Connection	-	-	Event	ODUk/NCS1K
ODUK-LTC-TCM6	TCM6 Loss of Tandem Connection	-	-	Event	ODUk/NCS1K
ODUK-OCI-TCM1	TCM1 Open Connection Indication	-	-	Event	ODUk/NCS1K
ODUK-OCI-TCM2	TCM2 Open Connection Indication	-	-	Event	ODUk/NCS1K
ODUK-OCI-TCM3	TCM3 Open Connection Indication	-	-	Event	ODUk/NCS1K
ODUK-OCI-TCM4	TCM4 Open Connection Indication	-	-	Event	ODUk/NCS1K
ODUK-OCI-TCM5	TCM5 Open Connection Indication	-	-	Event	ODUk/NCS1K
ODUK-OCI-TCM6	TCM6 Open Connection Indication	-	-	Event	ODUk/NCS1K
ODUK-SD-TCM1	TCM1 Signal Degrade	-	-	Event	ODUk/NCS1K
ODUK-SD-TCM2	TCM2 Signal Degrade	-	-	Event	ODUk/NCS1K
ODUK-SD-TCM3	TCM3 Signal Degrade	-	-	Event	ODUk/NCS1K
ODUK-SD-TCM4	TCM4 Signal Degrade	-	-	Event	ODUk/NCS1K
ODUK-SD-TCM5	TCM5 Signal Degrade	-	-	Event	ODUk/NCS1K
ODUK-SD-TCM6	TCM6 Signal Degrade	-	-	Event	ODUk/NCS1K
ODUK-SF-TCM1	TCM1 Signal Failure	-	-	Event	ODUk/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ODUK-SF-TCM2	TCM2 Signal Failure	-	-	Event	ODUk/NCS1K
ODUK-SF-TCM3	TCM3 Signal Failure	-	-	Event	ODUk/NCS1K
ODUK-SF-TCM4	TCM4 Signal Failure	-	-	Event	ODUk/NCS1K
ODUK-SF-TCM5	TCM5 Signal Failure	-	-	Event	ODUk/NCS1K
ODUK-SF-TCM6	TCM6 Signal Failure	-	-	Event	ODUk/NCS1K
ODUK-TIM-TCM1	TCM1 Trail Trace Identifier Mismatch	-	-	Event	ODUk/NCS1K
ODUK-TIM-TCM2	TCM2 Trail Trace Identifier Mismatch	-	-	Event	ODUk/NCS1K
ODUK-TIM-TCM3	TCM3 Trail Trace Identifier Mismatch	-	-	Event	ODUk/NCS1K
ODUK-TIM-TCM4	TCM4 Trail Trace Identifier Mismatch	-	-	Event	ODUk/NCS1K
ODUK-TIM-TCM5	TCM5 Trail Trace Identifier Mismatch	-	-	Event	ODUk/NCS1K
ODUK-TIM-TCM6	TCM6 Trail Trace Identifier Mismatch	-	-	Event	ODUk/NCS1K
OTUK-LOM	OTUK Loss Of MultiFrame	-	-	Event	OTUk/NCS1K
PROV-IN-PROG	Provisioning In Progress	-	-	Event	ODUk/NCS1K
REMOTE-DEG-SER	Remote FEC Degraded Symbol Error Rate	-	-	Event	ETH/NCS1K
TX-POWER-PROV-MISMATCH	Provisioned Optics Transmit Power Not Supported	-	-	Event	ODUk/NCS1K

PROTECTION alarms

Lists the PROTECTION alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify PROTECTION alarms and their source information.

The PROTECTION alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

PROTECTION alarms

The PROTECTION alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 93: PROTECTION alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
APS-NO-RESPONSE	APS Signal Mismatch	MN	SA	Alarm	ODUk/NCS2K
FAILTOSW	Failure To Switch To Protection	NA	NSA	Alarm	OPT ODUk OTUk OCn STMn ETH zrPlus/NCS2K
FORCED-REQ	Forced Switch Request	NA	NSA	Alarm	CARD OPT ODUk/NCS2K
LOCKOUT-REQ	Lockout Switch Request	NA	NSA	Alarm	OCn STMn ETH OPT ODUk OTUk zrPlus/NCS2K
MAN-REQ	Manual Switch Request	NA	NSA	Alarm	CARD OPT ODUk/NCS2K
PROT-CONFIG-MISMATCH	Protection Card Configuration Mismatch	MN	NSA	Alarm	CARD/NCS2K
REROUTE-IN-PROG	Reroute In Progress	-	-	Alarm	OXC/NCS2K
RESTORE-IN-PROG	Restoration in Progress	-	-	Alarm	OXC/NCS2K
REVERT-IN-PROG	Revert In Progress	NA	NSA	Alarm	OXC/NCS2K
WKSWPR	Switched To Protection	NA	NSA	Alarm	OPT OCn STMn ODUk OTUk ETH/NCS2K/NCS1K
WRK-PATH- RECOVERY-CHECK	Checking For Work Path Recovery	NA	NSA	Alarm	OPT/NCS2K
WTR	Wait To Restore	NA	NSA	Alarm	OPT OCn STMn ODUk OTUk ETH/NCS2K

PROTECTION events

Lists the PROTECTION events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify PROTECTION events and their source information.

The PROTECTION events table lists descriptions, severity, impact, condition type, and resource type or source values.

PROTECTION events

The PROTECTION events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 94: PROTECTION events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
WKSWBK	Switched Back To Working	-	-	Event	OPT ODUk/NCS2K

TIMING alarms

Lists the TIMING alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify TIMING alarms and their source information.

The TIMING alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

TIMING alarms

The TIMING alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 95: TIMING alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
BERT-SYNC-FAIL	BERT Synchronization Status Failed	NR	NSA	Alarm	OCn STMn OTUk/NCS2K
FRCDSWTOINT	Forced Switch To Internal Clock	NA	NSA	Alarm	NE_SYNCHREF/NCS2K
FRCDSWTOPRI	Forced Switch To Primary Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
FRCDSWTOSEC	Forced Switch To Second Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
FRCDSWTOTHIRD	Forced Switch To Third Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
FRNGSYNC	Free Running Synchronization Mode	NA	NSA	Alarm	NE_SYNCHREF/NCS2K
HI-CCVOLT	Composite Clock High Line Voltage	MN	NSA	Alarm	BITS/NCS2K
HLDOVRSYNC	Holdover Synchronization Mode	CR	SA	Alarm	NE_SYNCHREF/NCS2K
MANSWTOINT	Manual Switch To Internal Clock	NA	NSA	Alarm	NE_SYNCHREF/NCS2K
MANSWTOPRI	Manual Switch To Primary Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
MANSWTOSEC	Manual Switch To Second Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
MANSWTOTHIRD	Manual Switch To Third Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
SSM-DUS	Do Not Use For Synchronization	NA	NSA	Alarm	OCn STMn OTUk BITS/NCS2K
SSM-FAIL	Failed To Receive Synchronization Status Message	MN	NSA	Alarm	OCn STMn OTUk BITS/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
SSM-LNC	G812L - Local Node Clock traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-OFF	Synchronization Status Messages Are Disabled On This Interface	NA	NSA	Alarm	OCn STMn OTUk BITS/NCS2K
SSM-PRC	G811 - Primary Reference Clock traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-PRS	Stratum 1 Primary Reference Source Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-RES	Reserved For Network Synchronization Use	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-SDH-TN	G812T - Transit Node Clock traceable	NA	NSA	Alarm	STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-SETS	G813 - Synchronous Equipment Timing Source traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-SMC	SONET Minimum Clock Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST2	Stratum 2 Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST3	Stratum 3 Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST3E	Stratum 3E Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-ST4	Stratum 4 Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-STU	Synchronized - Traceability Unknown	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SSM-TNC	Transit Node Clock Traceable	NA	NSA	Alarm	OCn STMn OTUk BITS NE_SYNCHREF/NCS2K
SWTOPRI	Switch To Primary Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K
SWTOSEC	Switch To Second Reference	NA	NSA	Alarm	EXT_SYNCHREF NE_SYNCHREF/NCS2K

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

SECURITY alarms

Lists the SECURITY alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify SECURITY alarms and their source information.

The SECURITY alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

SECURITY alarms

The SECURITY alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 96: SECURITY alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADMIN-CONFIG-INCONSISTENCY	Admin Configuration is in inconsistent state	-	-	Alarm	NE/NCS1K
CRYPTO-HW-FAILURE	Cryptographic self-test failure	CR	SA	Alarm	SHELF/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
CRYPTO-INDEX-MISMATCH	Crypto Index Mismatch	MN	NSA	Alarm	CARD/NCS1K
CRYPTO-KEY-EXPIRED	Crypto key expired	CR	SA	Alarm	CARD/NCS1K
INTRUSION-PSWD	Security Intrusion Attempt Detected - See Audit Log	MN	NSA	Alarm	NE SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-CHAIN-VERIFICATION-FAILED	Local cert chain verification failed	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-EXPIRED	Local certificate expired	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-EXPIRING-WITHIN-30-DAYS	Local cert expiring within 30 days	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-CERT-ISSUED-FOR-FUTURE-DATE	Local cert issued for future date	MJ	NSA	Alarm	CARD SYSTEM/NCS2K/SYSTEM
LOCAL-SUDI-CERT-VERIFICATION-FAILED	Local sudi cert verification failed	MJ	NSA	Alarm	CARD/NCS2K/NCS1K
NON-TRAF-AFFECT-SEC-UPG-REQUIRED	Non Traffic Affecting Security Upgrade Required	NR	NSA	Alarm	CARD/NCS2K
OTNSEC-LOCALLY-SECURED	OTNSEC Locally Secured	NA	NSA	Alarm	CARD/NCS1K
PROT-SOFT-VERIF-FAIL	Protect Volume Software Signature Verification Failed		-	Alarm	CARD/NCS2K

SECURITY events

Lists the SECURITY events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify SECURITY events and their source information.

The SECURITY events table lists descriptions, severity, impact, condition type, and resource type or source values.

SECURITY events

The SECURITY events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 97: SECURITY events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADMIN-DISABLE	Disable Inactive User	-	-	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-DISABLE-CLR	Disable Inactive Clear	-	-	Event	NE SYSTEM/NCS2K/SYSTEM

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADMIN-LOCKOUT	Admin Lockout of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-LOCKOUT-CLR	Admin Lockout Clear	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-LOGOUT	Admin Logout of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-SUSPEND	Suspend User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
ADMIN-SUSPEND-CLR	Suspend User Clear	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
INTRUSION	Security: Invalid Login Username - See Audit Trail	MJ	NSA	Event	NE SYSTEM/NCS2K/SYSTEM
INTRUSION-USERID	Security Intrusion Attempt Detected - See Audit Log	CR	SA	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAIL-LOCKOUT	Security: Invalid Login - Locked Out - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAIL-ONALRDY	Security: Invalid Login - Already Logged On - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAILURE-PSWD	Security: Invalid Login - Password - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGIN-FAILURE-USER	Security: Invalid Login - Username - See Audit Log	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
LOGOUT-IDLE-USER	Automatic Logout of IdleUser	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
MASTERKEY-SUCCESS	MasterKey Exchange Success	–	–	Event	NE/NCS2K
PSWD-CHG-REQUIRED	User Password Change Required	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
SESSION-TIME-LIMIT	Session Time Limit Expired	–	–	Event	NE/NCS2K
USER-LOCKOUT	User Locked Out	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
USER-LOGIN	Login of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM
USER-LOGOUT	Logout of User	–	–	Event	NE SYSTEM/NCS2K/SYSTEM

OPTICAL alarms

Lists the OPTICAL alarms in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify OPTICAL alarms and their source information.

The OPTICAL alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

OPTICAL alarms

The OPTICAL alarms table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 98: OPTICAL alarms

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
ADD-OPWR-HDEG	Port Add Power Degrade High	MN	NSA	Alarm	OPT/NCS2K
ADD-OPWR-HFAIL	Port Add Power Fail High	CR	SA	Alarm	OPT/NCS2K
ADD-OPWR-LDEG	Port Add Power Degrade Low	MN	NSA	Alarm	OPT/NCS2K
ADD-OPWR-LFAIL	Port Add Power Fail Low	CR	SA	Alarm	OPT/NCS2K
ALC-IN-PROGRESS	Automatic-link-calibration procedure is running	MN	NSA	Alarm	OPT/NCS1K
ALC-PROC-FAILED	Automatic-link-calibration procedure failed	CR	SA	Alarm	OPT/NCS1K
ALS	Automatic Laser Shutdown	NA	NSA	Alarm	OPT OCH ETH/NCS2K/NCS1K
ALS-DISABLED	Auto Laser Shutdown Disabled	NA	NSA	Alarm	OPT OCH/NCS2K
AMPLI-INIT	Optical Amplifier Initialization	NA	NSA	Alarm	OPT/NCS2K
AMPLI-OSRI	Amplifier Optical Safety Remote Interlock	NA	NSA	Alarm	OPT/NCS1K
APC-BLOCKED	APC blocked	MN	NSA	Alarm	OPT/NCS1K
APC-BLOCKED-RX	APC blocked in RX direction	MN	NSA	Alarm	OPT/NCS1K
APC-BLOCKED-TX	APC blocked in TX direction	MN	NSA	Alarm	OPT/NCS1K
APC-CORR-SKIPPED	Automatic Power Control Correction Skipped	MN	NSA	Alarm	OPT/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
APC-DISABLED	Automatic Power Control Disabled	MN	NSA	Alarm	OPT CARD/NCS2K
APC-DISABLED	Automatic Power Control Disabled	MN	NSA	Alarm	NE/NCS2K
APC-END	Manual Requested Automatic Power Control run Completed	NA	NSA	Alarm	NE/NCS2K
APC-HW-FAIL	APC Hardware Failure	MJ	NSA	Alarm	OPT/NCS1K
APC-OUT-OF-RANGE	APC Cannot Set Value Due To Range Limits	MN	NSA	Alarm	OPT/NCS2K/NCS1K
APC-TARGET-PSD-NOT-MET-RX	APC Target PSD not met in RX direction	MN	NSA	Alarm	OPT/NCS1K
APC-TARGET-PSD-NOT-MET-TX	APC Target PSD not met in TX direction	MN	NSA	Alarm	OPT/NCS1K
APC-WRONG-GAIN	APC Wrong Gain Set Point	NA	NSA	Alarm	OPT/NCS2K
ASE-LOADING-DISABLED	ASE Loading is disabled	NA	NSA	Alarm	OPT OXC/NCS1K
AUTO-AMPLI-DISABLED	Auto Ampli Control Disabled	MN	NSA	Alarm	OPT/NCS1K
AUTO-AMPLI-MISMATCH	Auto Ampli Control Mismatch	NA	NSA	Alarm	OPT/NCS1K
AUTO-AMPLI-RUNNINNG	Auto Ampli Control Running	NA	NSA	Alarm	OPT/NCS1K
CANNOT-BE-EQUALIZED	Incoming signal cannot be equalized	-	-	Alarm	OPT OXC/NCS2K
CARLOSS	Carrier Loss On The LAN	MJ	SA	Alarm	MS_ETH ETH/NCS2K/NCS1K
CD	Chromatic Dispersion	-	-	Alarm	OCH/NCS2K/NCS1K
CHAN-PWR-THRESHOLD-CHECK	Channel Power would fall below threshold value	MN	NSA	Alarm	OPT/NCS2K
CHANNEL-NOISE-LOADED	Channel is Loaded with Noise	MJ	NSA	Alarm	OPT OXC/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
CHANNEL-READY	Channel Presence is Detected and Ready	MN	NSA	Alarm	OPT OXC/NCS1K
DCU-LOSS-FAIL	DCU Loss Failure	MN	NSA	Alarm	OPT/NCS2K
DGD	Differential Group Delay	MN	NSA	Alarm	OCH/NCS1K
EMB-AMPLIFIER-SATURATED	Embedded amplifier saturated alarm	MN	NSA	Alarm	OPT/NCS2K
EXPECTED-POWER-FAIL	Channel Power Reading Exceeds the Expected Power Tolerance Limits	MN	NSA	Alarm	OPT OXC/NCS1K
FDI	Forward Defect Indication	NA	NSA	Alarm	OXC OCn/NCS2K
GAIN-HDEG	Optical Amplifier Gain Degrade High	MN	NSA	Alarm	OPT/NCS2K
GAIN-HFAIL	Optical Amplifier Gain Failure High	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
GAIN-LDEG	Optical Amplifier Gain Degrade Low	MN	NSA	Alarm	OPT/NCS2K
GAIN-LFAIL	Optical Amplifier Gain Failure Low	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
GAIN-NEAR-LIMIT	Amplifier Gain is near its limit	MN	NSA	Alarm	OPT/NCS2K
HI-RX-BR-PWR	Input High BR Power	MN	NSA	Alarm	RAMAN_AMPLIFIER/NCS1K
HI-RXPOWER	Facility High Rx power	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
HI-TX-BR-PWR	Output High BR Power	MN	NSA	Alarm	OPT/NCS1K
LASER-APR	Laser Auto Power Reduction	MN	NSA	Alarm	OPT/NCS2K/NCS1K
LO-RXPOWER	Facility Low Rx power	MN	NSA	Alarm	OCH PORT PPM/NCS2K/ NCS2K-SVO-K9/NCS1K
LOS	Loss Of Signal	CR	SA	Alarm	OCn STMn OPT/NCS2K/ NCS2K-SVO-K9/NCS1K
LOS	Loss Of Signal	CR	SA	Alarm	BITS PORT/NCS2K/ NCS2K-SVO-K9/NCS1K
LOS-D	Loss Of DFB Signal	CR	SA	Alarm	OPT/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
LOS-O	Incoming Overhead Signal Absent	MN	NSA	Alarm	OPT/NCS2K
LOS-P	Incoming Payload Signal Absent	CR	SA	Alarm	OPT OCH OXC/NCS2K/NCS1K
LOS-RAMAN	Loss Of Raman Signal	CR	SA	Alarm	OPT/NCS2K
MAN-LASER-RESTART	Manual Laser Restart	NA	NSA	Alarm	OPT OCH/NCS2K
OPWR-HDEG	Optical Power Degrade High	MN	NSA	Alarm	OPT OXC/NCS2K
OPWR-HFAIL	Optical Power Failure High	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
OPWR-LDEG	Optical Power Degrade Low	MN	NSA	Alarm	OPT OXC/NCS2K
OPWR-LFAIL	Optical Power Failure Low	CR	SA	Alarm	OPT OXC/NCS2K/NCS1K
OSRION	Optical Safety Remote Interlock On	NA	NSA	Alarm	OPT/NCS2K
PARAM-MISM	Plug-in Module Range Settings Mismatch	CR	SA	Alarm	OPT OXC/NCS2K
PARTIAL-TOPOLOGY	APC Partial topology	MN	NSA	Alarm	OPT/NCS1K
PMD-DEG	PMD Degrade	MJ	NSA	Alarm	OCH/NCS2K
PMI	Payload Missing Indication	NA	NSA	Alarm	OPT OXC/NCS2K
PSD-FAILED	Failure in Power Spectrum Distribution	-	-	Alarm	OPT OXC/NCS1K
PWR-PROT-ON	Raman Power Protection On	MJ	SA	Alarm	OPT/NCS2K
RAMAN-AMPLI-OSRI	Raman Amplifier Optical Safety Remote Interlock	CR	SA	Alarm	RAMAN_AMPLIFIER/NCS1K
RAMAN-CALIBRATION-FAILED	Raman Calibration Failed	MN	NSA	Alarm	RAMAN_AMPLIFIER/NCS2K/ SYSTEM/NCS1K
RAMAN-CALIBRATION-PENDING	Raman Calibration Pending	NA	NSA	Alarm	RAMAN_AMPLIFIER/NCS2K
RAMAN-CALIBRATION-RUNNING	Raman Calibration Running	CR	SA	Alarm	RAMAN_AMPLIFIER/ NCS2K/NCS1K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
RAMAN-GAIN-NOT-REACHED	Raman Gain Not Reached	MJ	SA	Alarm	RAMAN_AMPLIFIER/ NCS2K/SYSTEM/NCS1K
RAMAN-TURNUP-FAIL	Raman Pumps Turnup Fail	MJ	SA	Alarm	RAMAN_AMPLIFIER/NCS1K
RFI	Remote Failure Indication	NR	NSA	Alarm	OPT/NCS2K
RLS	Raman Laser Shutdown	NA	NSA	Alarm	RAMAN_AMPLIFIER/NCS2K
RX-BELOW-MIN-PSD	Receive Channel Power Below Minimum Power Spectral Density	MJ	SA	Alarm	OPT/NCS1K
SD	Signal Degrade	NA	NSA	Alarm	OCn/NCS2K
SF	Signal Failure	NA	NSA	Alarm	OCn/NCS2K
SF-L	BER Threshold Exceeded For Signal Failure Line	NA	NSA	Alarm	OCn/NCS2K
SIGLOSS	Signal Loss on Data Interface	MJ	SA	Alarm	ETH FC/NCS2K/NCS1K
SIGNAL-OSC-SPAN-LOSS-DIFF-OUT-OF-RANGE	Difference in Rx OSC span loss and Rx signal span loss exceeded threshold	MN	NSA	Alarm	OPT/NCS1K
SPAN-LOSS-BASELINE-DEVIATION-OUT-OF-RANGE	Rx span loss deviated from baseline	MN	NSA	Alarm	OPT/NCS1K
SPAN-LOSS-OUT-OF-RANGE	Span Loss Value Out Of Range	MN	NSA	Alarm	OPT/NCS2K/NCS1K
SPAN-NOT-MEASURED	Span Measurement Cannot Be Performed	MN	NSA	Alarm	OPT/NCS2K
SPAN-TOO-SHORT	OTS Span Too Short	MN	NSA	Alarm	OPT/NCS1K
SPECTRUM-VIOLATED	Spectrum is Violated	CR	SA	Alarm	OPT OXC/NCS1K
VOA-DISABLED	VOA Control Loop Disable Due To Excessive Counter-Propagation Light	CR	SA	Alarm	CARD/NCS2K
VOA-HDEG	Variable Optical Attenuator Degrade High	MN	NSA	Alarm	OPT OXC/NCS2K

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
VOA-HFAIL	Variable Optical Attenuator Failure High	CR	SA	Alarm	OPT OXC/NCS2K
VOA-LDEG	Variable Optical Attenuator Degrade Low	MN	NSA	Alarm	OPT OXC/NCS2K
VOA-LFAIL	Variable Optical Attenuator Failure Low	CR	SA	Alarm	OPT OXC/NCS2K
WVL-MISMATCH	Equipment Wavelength Mismatch	MJ	SA	Alarm	OCH/NCS2K
WVL-UNLOCKED	Wavelength Unlocked	MJ	SA	Alarm	OCH/NCS2K/NCS1K

OPTICAL events

Lists the OPTICAL events in Cisco Optical Network Controller, including descriptions, severity, impact, condition type, and resource type or source values.

Use this reference to identify OPTICAL events and their source information.

The OPTICAL events table lists descriptions, severity, impact, condition type, and resource type or source values.

OPTICAL events

The OPTICAL events table lists descriptions, severity, impact, condition type, and resource type or source values.

Table 99: OPTICAL events

Condition Name	Description	Severity	Impact	Condition Type	Resource Type/Source
AUTOWDMANS	Automatic WDM ANS Finished	-	-	Event	NE/NCS2K
RMON-ALARM	RMON Threshold Crossing Alarm	-	-	Event	ETH FC ODUk/NCS2K
RMON-RESET	RMON Histories And Alarms Reset Reboot	-	-	Event	ETH FC ODUk/NCS2K

TCA events

Lists the TCA events in Cisco Optical Network Controller, including descriptions, condition type, and resource type or source values.

Use this reference to identify TCA events and their source information.

The TCA events table lists descriptions, condition type, and resource type or source values.

TCA events

The TCA events table lists descriptions, condition type, and resource type or source values.

Table 100: TCA events

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

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

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

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

Condition Name	Description	Condition Type	Resource Type/Source
T-OPWR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OSC-PWR-AVG	Threshold Crossing Alert	Event	OPT/NA
T-OSC-PWR-MAX	Threshold Crossing Alert	Event	OPT/NA
T-OSC-PWR-MIN	Threshold Crossing Alert	Event	OPT/NA
T-OSNR-AVG	Threshold Crossing Alert	Event	OCH/NA
T-OSNR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-OSNR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PCR-AVG	Threshold Crossing Alert	Event	OCH/NA
T-PCR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-PCR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PDL-AVG	Threshold Crossing Alert	Event	OCH/NA
T-PDL-MAX	Threshold Crossing Alert	Event	OCH/NA
T-PDL-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PMD-AVG	Threshold Crossing Alert	Event	OCH/NA
T-PMD-MIN	Threshold Crossing Alert	Event	OCH/NA
T-PN-MAX	Threshold Crossing Alert	Event	OCH/NA
T-PN-MIN	Threshold Crossing Alert	Event	OCH/NA
T-POST-FEC-BER-MAX	Threshold Crossing Alert	Event	OTUk FC/NA
T-POST-FEC-BER-MIN	Threshold Crossing Alert	Event	OTUk FC/NA
T-PRE-FEC-BER-MAX	Threshold Crossing Alert	Event	OTUk FC/NA

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

Condition Name	Description	Condition Type	Resource Type/Source
T-RS-SES	Threshold Crossing Alert	Event	STMn/NA
T-RS-SESR	Threshold Crossing Alert	Event	STMn/NA
T-RS-UAS	Threshold Crossing Alert	Event	STMn/NA
T-RX-PWR-MAX	Threshold Crossing Alert	Event	OCH/NA
T-RX-PWR-MIN	Threshold Crossing Alert	Event	OCH/NA
T-RX-SIG-POW-AVG	Threshold Crossing Alert	Event	OCH/NA
T-RX-SIG-POW-MAX	Threshold Crossing Alert	Event	OCH/NA
T-RX-SIG-POW-MIN	Threshold Crossing Alert	Event	OCH/NA
T-RX-TEMP-MAX	Threshold Crossing Alert	Event	OCH/NA
T-RX-TEMP-MIN	Threshold Crossing Alert	Event	OCH/NA
T-SEFS	Threshold Crossing Alert	Event	OCn/NA
T-SES-PCS	Threshold Crossing Alert	Event	FC/NA
T-SES-PM	Threshold Crossing Alert	Event	ODUk/NA
T-SES-SM	Threshold Crossing Alert	Event	OTUk/NA
T-SES-TCM1	Threshold Crossing Alert	Event	ODUk/NA
T-SES-TCM2	Threshold Crossing Alert	Event	ODUk/NA
T-SESL	Threshold Crossing Alert	Event	OCn/NA
T-SESR-PM	Threshold Crossing Alert	Event	ODUk/NA
T-SESR-SM	Threshold Crossing Alert	Event	OTUk/NA
T-SESR-TCM1	Threshold Crossing Alert	Event	ODUk/NA

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

Condition Name	Description	Condition Type	Resource Type/Source
T-UASL	Threshold Crossing Alert	Event	OCn/NA
T-UASS	Threshold Crossing Alert	Event	OCn/NA
T-UNC-WORDS	Threshold Crossing Alert	Event	OCH OTUk/NA
T-VOA-AVG	Threshold Crossing Alert	Event	OPT/NA
T-VOA-MAX	Threshold Crossing Alert	Event	OPT/NA
T-VOA-MIN	Threshold Crossing Alert	Event	OPT/NA
T-GFPSTATSROUNDTRIPLATENCYUSEC	Threshold Crossing Alert	Event	ETH/NA
T-RXCONTROLFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-RXPAUSEFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-RXPKTSDROPPED INTERNALCONGESTION	Threshold Crossing Alert	Event	ETH/NA
T-RXUNKNOWNOPCODEFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-TXPAUSEFRAMES	Threshold Crossing Alert	Event	ETH/NA
T-TXPKTSDROPPED INTERNALCONGESTION	Threshold Crossing Alert	Event	ETH/NA

A MIB definition for Cisco Optical Network Controller

This section provides details about the Cisco EPM notification MIB, including supported objects and notification descriptions. Use it to understand management-system integrations for Cisco Optical Network Controller.

Use this reference to understand MIB definition for Cisco Optical Network Controller.

Details about MIB definition for Cisco Optical Network Controller.

MIB definition for Cisco Optical Network Controller details

MIB definition for Cisco Optical Network Controller details include:

- 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.
- 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.

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.

Table 101: Details

SNMPvarbind	Data Type
cenAlarmVersion	SnmpAdminString
cenAlarmTimestamp	Timestamp
cenAlarmUpdatedTimestamp	Timestamp
cenAlarmInstanceID	SnmpAdminString

SNMPvarbind	Data Type
cenAlarmStatus	Integer
cenAlarmStatusDefinition	SnmpAdminString
cenAlarmType	Integer
cenAlarmCategory	Integer
cenAlarmCategoryDefinition	SnmpAdminString
cenAlarmServerAddressType	InetAddressType
cenAlarmServerAddress	cenAlarmServerAddress
cenAlarmManagedObjectClass	SnmpAdminString
cenAlarmManagedObjectAddressType	InetAddressType
cenAlarmManagedObjectAddress	InetAddress
cenAlarmDescription	OctetString
cenAlarmSeverity	Integer
cenAlarmSeverityDefinition	SnmpAdminString

SNMPvarbind	Data Type
cenAlarmTriageValue	Integer
cenEventIDList	OctetString
cenUserMessage1	SnmpAdminString
cenUserMessage2	SnmpAdminString
cenUserMessage3	SnmpAdminString
cenAlarmMode	Integer
cenPartitionNumber	Integer

SNMPvarbind	Data Type
cenPartitionName	SnmpAdminString
cenCustomerIdentification	SnmpAdminString
cenCustomerRevision	SnmpAdminString
cenAlertID	SnmpAdminString