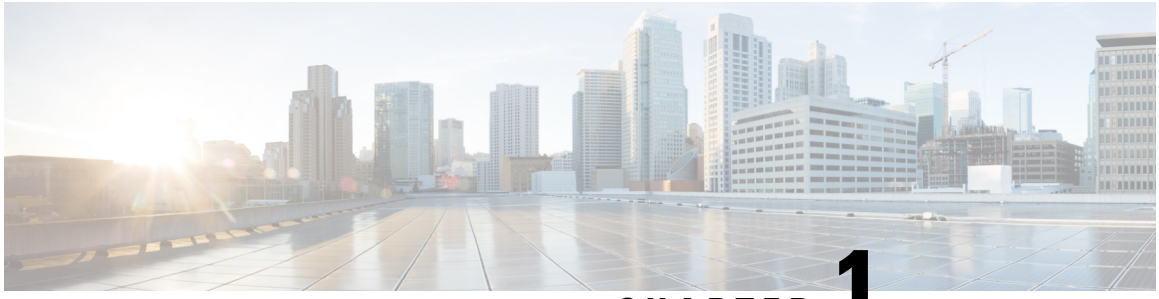
Cisco Optical Network Controller 24.3.1 Configuration Guide

First Published: 2024-10-03

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

CONTENTS



CHAPTER 1

Overview of Cisco Optical Network Controller

Overview of Cisco Optical Network Controller

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

- Collects information about the inventory and topology of the managed network.
- Monitors the physical or virtual topology of the network.
- Notifies of changes in topology and service changes.
- Supports optical path creation and deletion.

Cisco Optical Network Controller collects relevant data needed for optical applications. This data is also used to provide abstract network information to higher layer controllers, thus enabling a centralized control of optical network.

Some of the functions supported by Cisco Optical Network Controller are given below.

- Optical Domain Controller

  Cisco Optical Network Controller behaves as a domain controller for Cisco optical products. The domain controller feeds data into hierarchical controllers. Optical Network Controller has a North Bound Interface (NBI) based on the TAPI standard which enables it to connect to any hierarchical controller which has a TAPI compliant South Bound Interface (SBI) and provide its functions to the controller.

- Path Compute Engine (PCE)

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

- Model Based Network Abstraction

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

Note

- For more details on Cisco Optical Site Manager (COSM), see COSM Configuration Guide.
- For more details on Cisco Optical Network Planner (CONP), see CONP Configuration Guide.
- For further details about Cisco Optical Network Controller, see the data sheet .
- TAPI is disabled by default and it must be enabled before onboarding of devices.
- You must not enable TAPI after device on-boarding 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.

Log into Cisco Optical Network Controller

Before you begin

Use the following steps to log into Cisco Optical Network Controller:

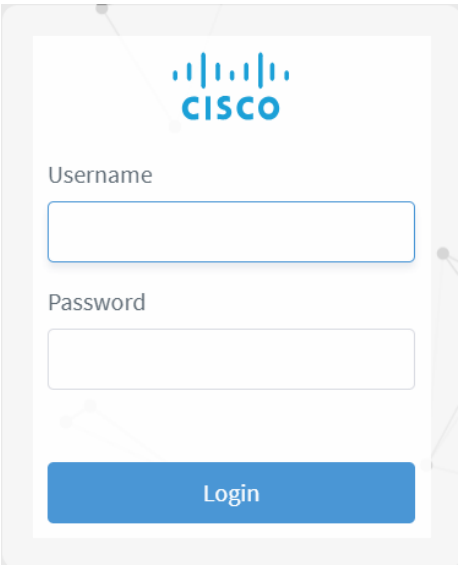
Step 1 In the browser URL field, enter **https://<virtual-ip>:8443/**

Login page is displayed.

Step 2 Enter the username and password.

Step 3 Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



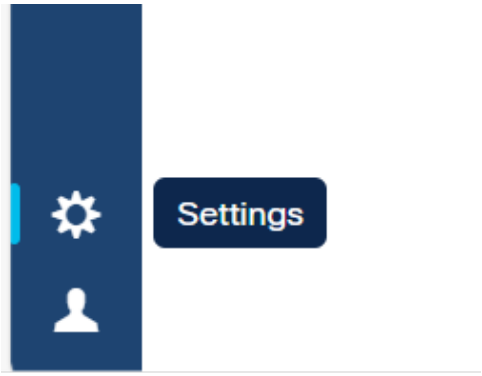
User Access in Cisco Optical Network Controller 24.3.1

You can manage the user access and permissions through Cisco ONC. It adds an additional layer of security and works as a Single Authentication Agent, thus sharing local, LDAP and SAML users.

Users, Roles, and Permissions

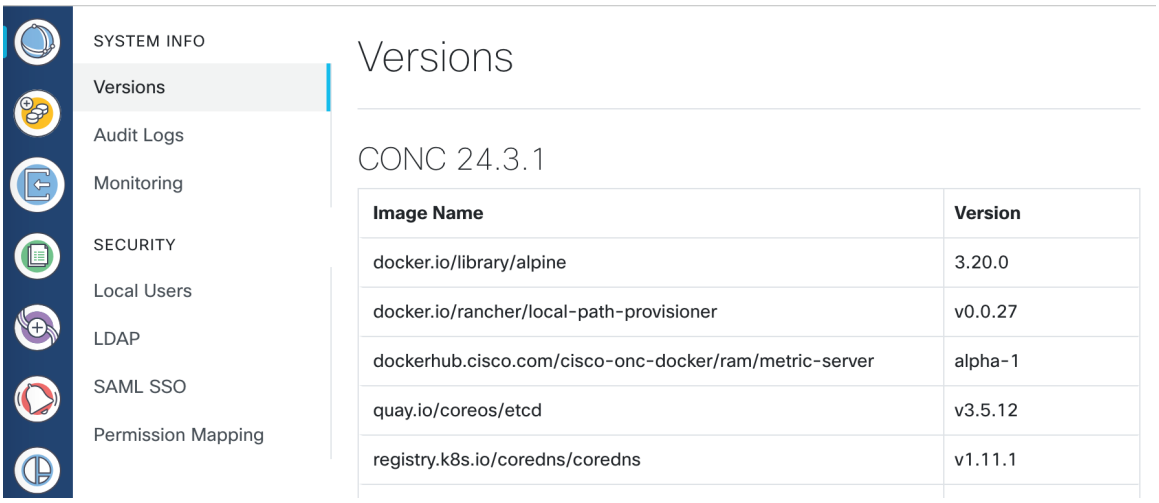
User can have have different permission levels. See *Set up Permission Mapping*. To allow access to Cisco ONC to a larger group of regular users, set the user authentication through LDAP or SAML SSO protocols. You can use both at the same time as well, depending on your environment.

Figure 2: Settings



Once you click **Settings** you will see the panel as given below.

Figure 3: Settings Options



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

The **Security** section is for access management and consists of the following options.

- **Local Users**: Here you can display, create and edit local users through the UI.
- **LDAP**: Here you can set LDAP settings for user authentication.
- **SAML SSO**: Here you can set SAML Single-Sign-On settings for user authentication
- **Permission Mapping**: Here you can handle permission management through the Cisco Policy Management Tool.

Add Local Users to Cisco Optical Network Controller 24.3.1

Before you begin

You will need access to Cisco Optical Network Controller 24.3.1 with admin user privileges.

Use the following steps to add local user accounts to Cisco Optical Network Controller 24.3.1.

Step 1 From the Cisco Optical Network Controller 24.3.1 home page click **Settings** .

Step 2 From the panel list, select **Local Users** tab and click **Add** .

Step 3 In the **Add User** screen, enter **Username*** .

Step 4 After entering the user name, enter **Password*** .

Step 5 Next confirm the password using **Confirm Password*** .

Step 6 Next enter the access permissions in the form of a comma separated list using **Access Permissions** and enter permission/admin as shown in the example below.

For example *permission/<admin>*

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

Figure 4: Local Users

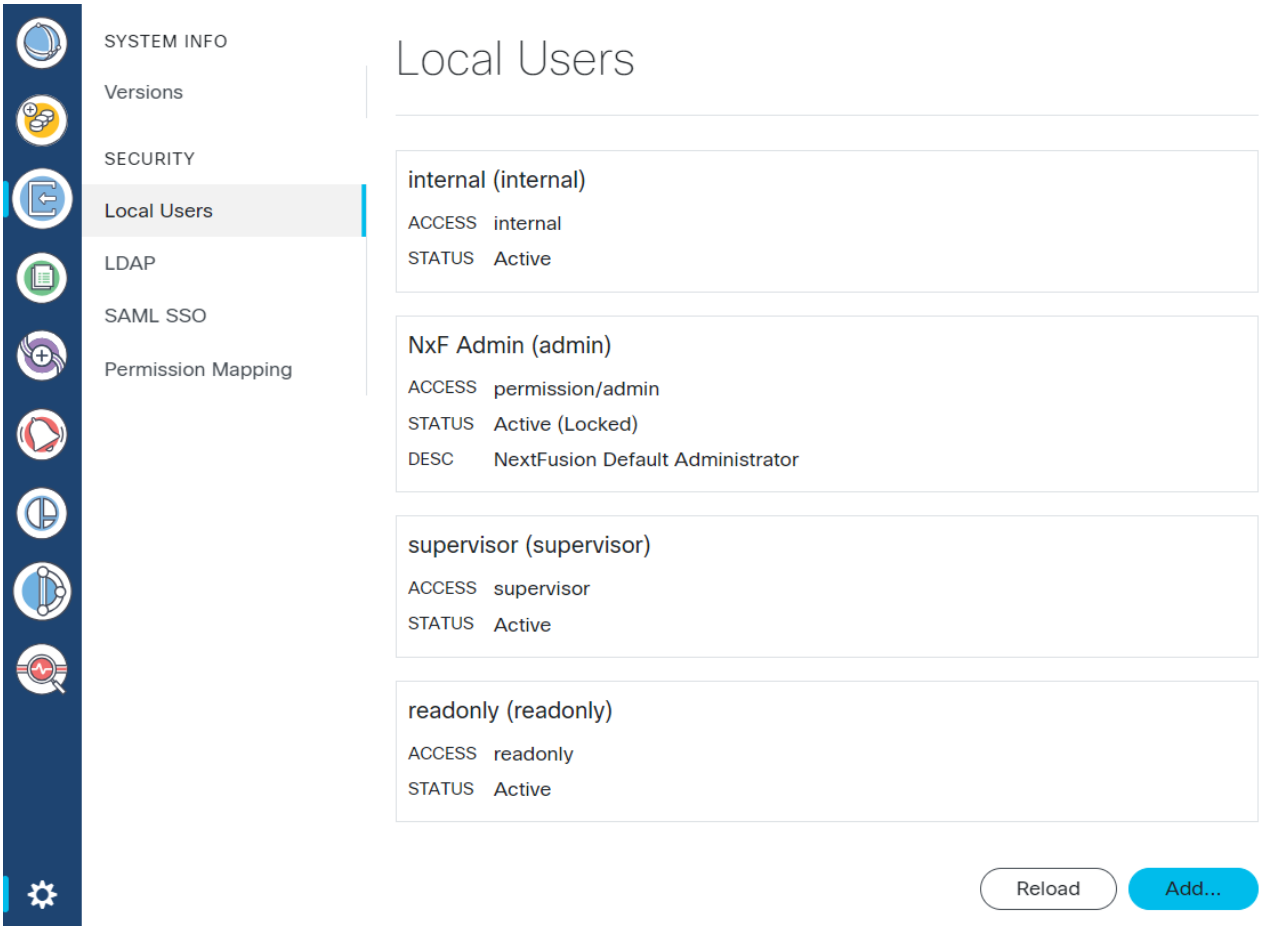
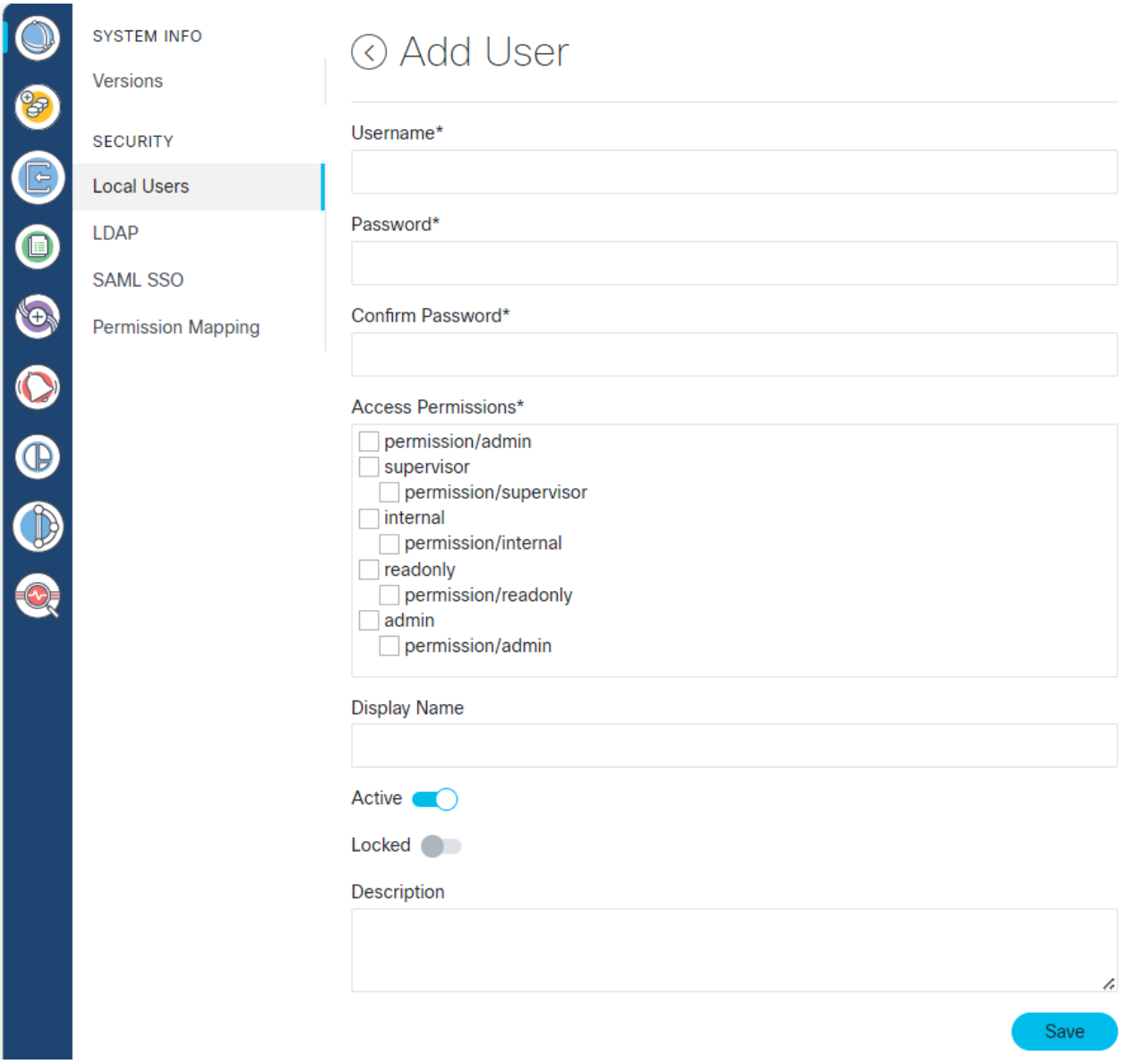


Figure 5: Add User



Step 7 Use radio buttons to set the user status. You can make both radio buttons disabled or enabled at the same time

- **Active enabled**: Allows the user to log in to Cisco ONC.
- **Active disabled**: Forbids the user to log in Cisco ONC.
- **Locked enabled**: Prevents deleting the user.
- **Locked disabled**: Allows removal of the user

Step 8 Click **Save**.

Set up Authentication through LDAP

Authentication can be done using Lightweight Directory Access Protocol (LDAP) protocol.

Step 1 From the Cisco Optical Network Controller 24.3.1 home page click **Settings**.

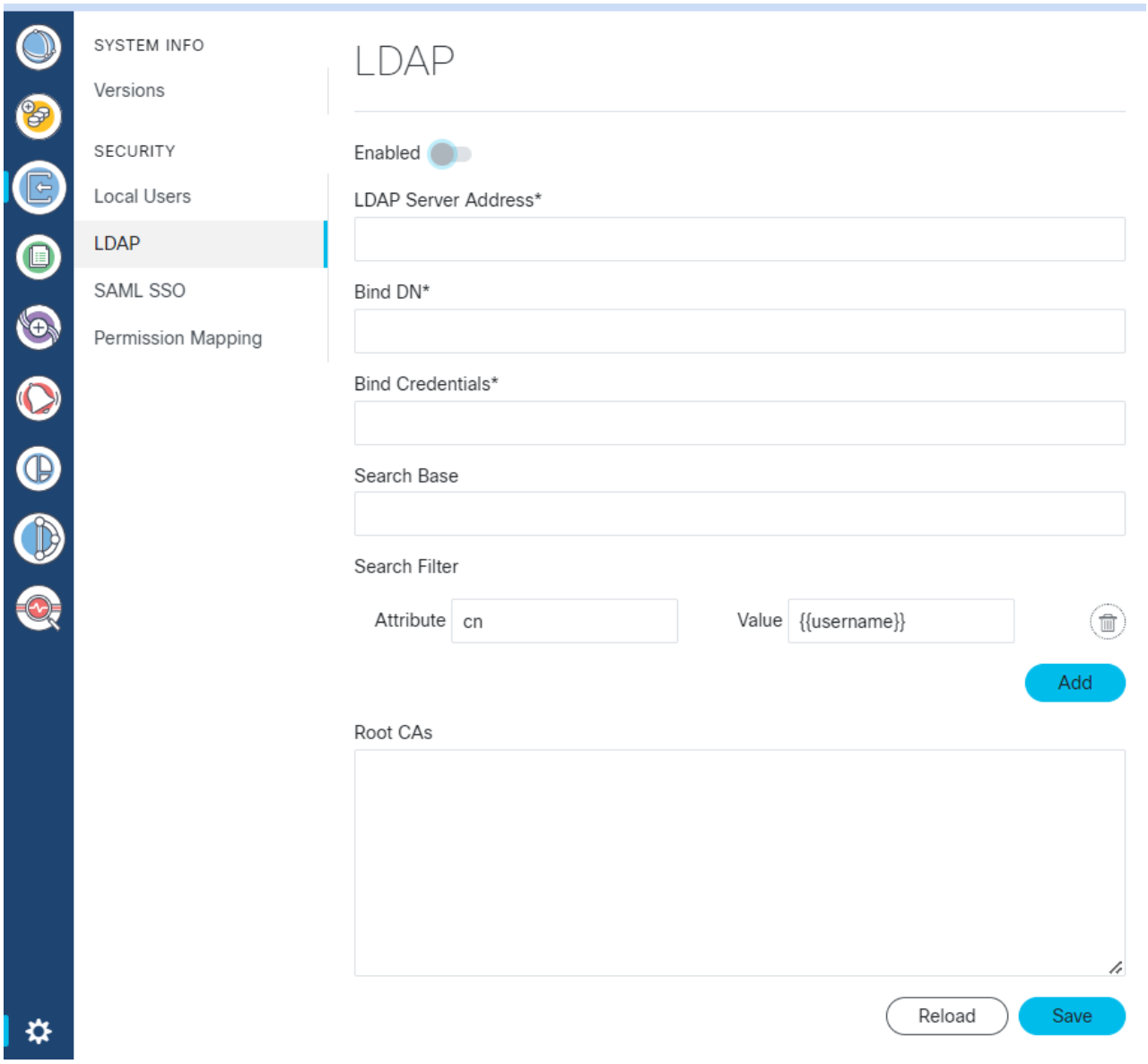
Step 2 Click **LDAP**.

Step 3 Click the **Enabled** radio button.

Step 4 Fill in the mandatory fields that are marked with an asterisk (*): **LDAP Server Address**, **Bind DN** and **Bind Credentials**. The **Search Filter**, **Search Base** and **Root CAs** are optional.

Step 5 Click **Save**.

Figure 6: LDAP



Set up Authentication through SAMLv2 SSO

The Security Assertion Markup Language (SAML) SSO feature allows you to gain single sign-on access based on the SAMLv2 protocol. Also, SSO user credential authentication works only for local users.

Step 1 In the CWM, go to the outermost navigation menu on the left

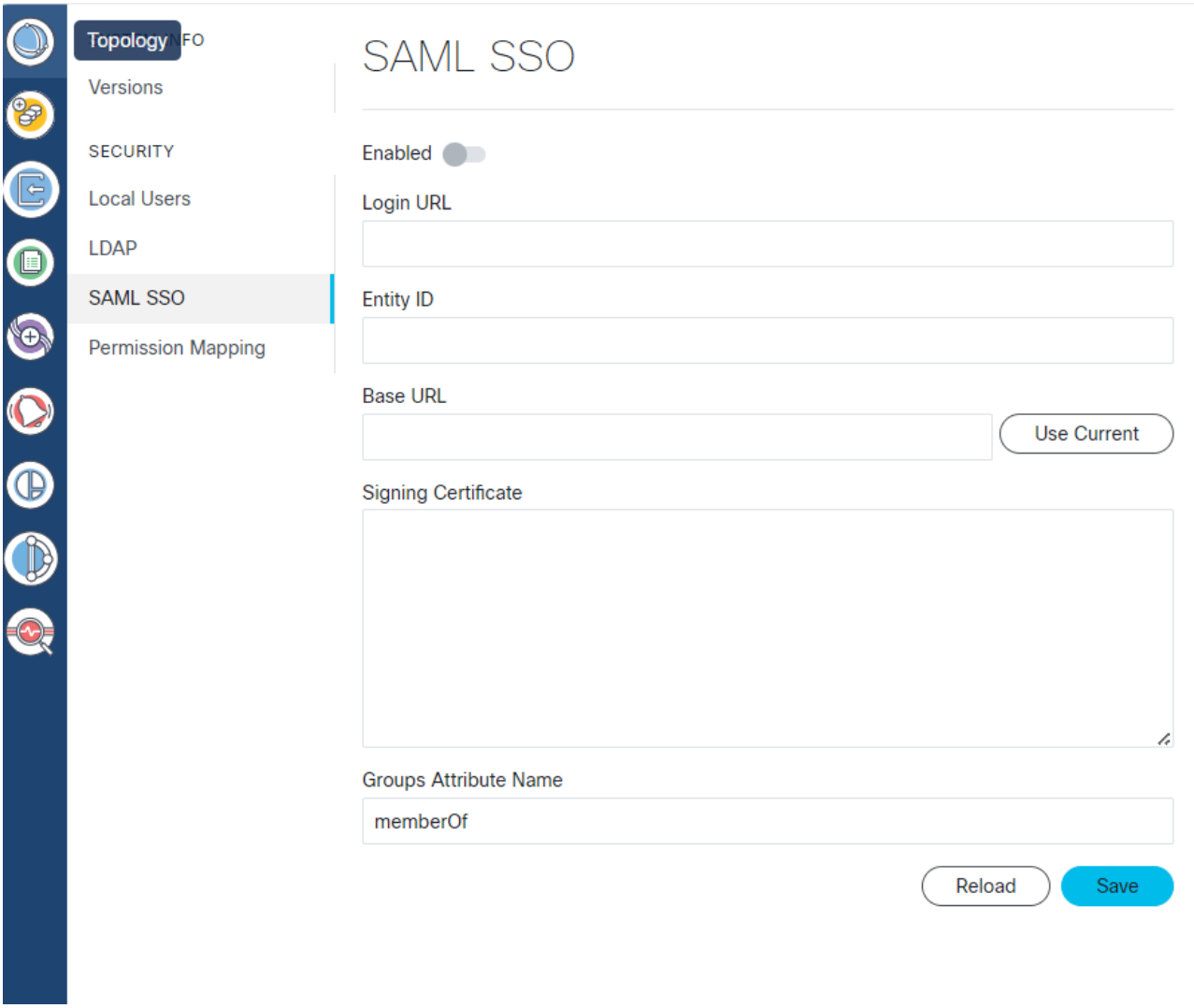
Step 2 From the Cisco Optical Network Controller 24.3.1 home page click **Settings** and navigate to **SAML SSO** tab.

Step 3 Click the **Enabled** radio button.

Step 4 Fill in the fields: **Login URL**, **Entity ID**, **Base URL**, **Signing Certificate** and **Groups Attribute Name**.

Step 5 Click **Save**.

Figure 7: SAML SSO



Set up Permission Mapping

You can give specific permissions to a group of users using this option.

Step 1 From the Cisco Optical Network Controller 24.3.1 home page click **Settings**.

Step 2 Navigate to **Permission Mapping**.

Step 3 Click **Add**.

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

Step 5 Fill in the **Match** field.

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

Step 7 Click **Save**.

Figure 8: Permission Mapping

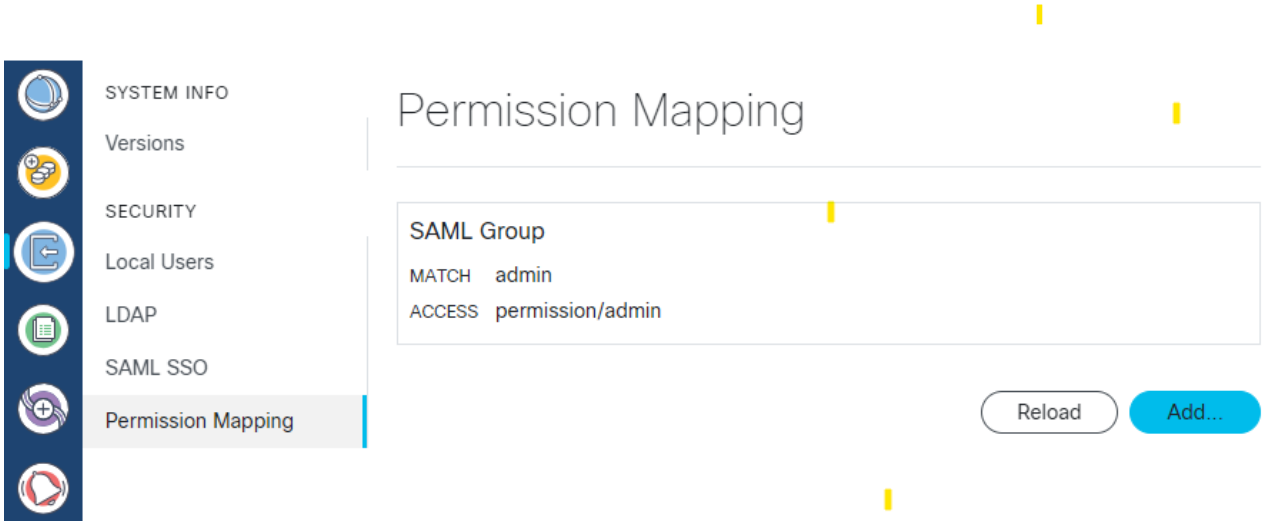
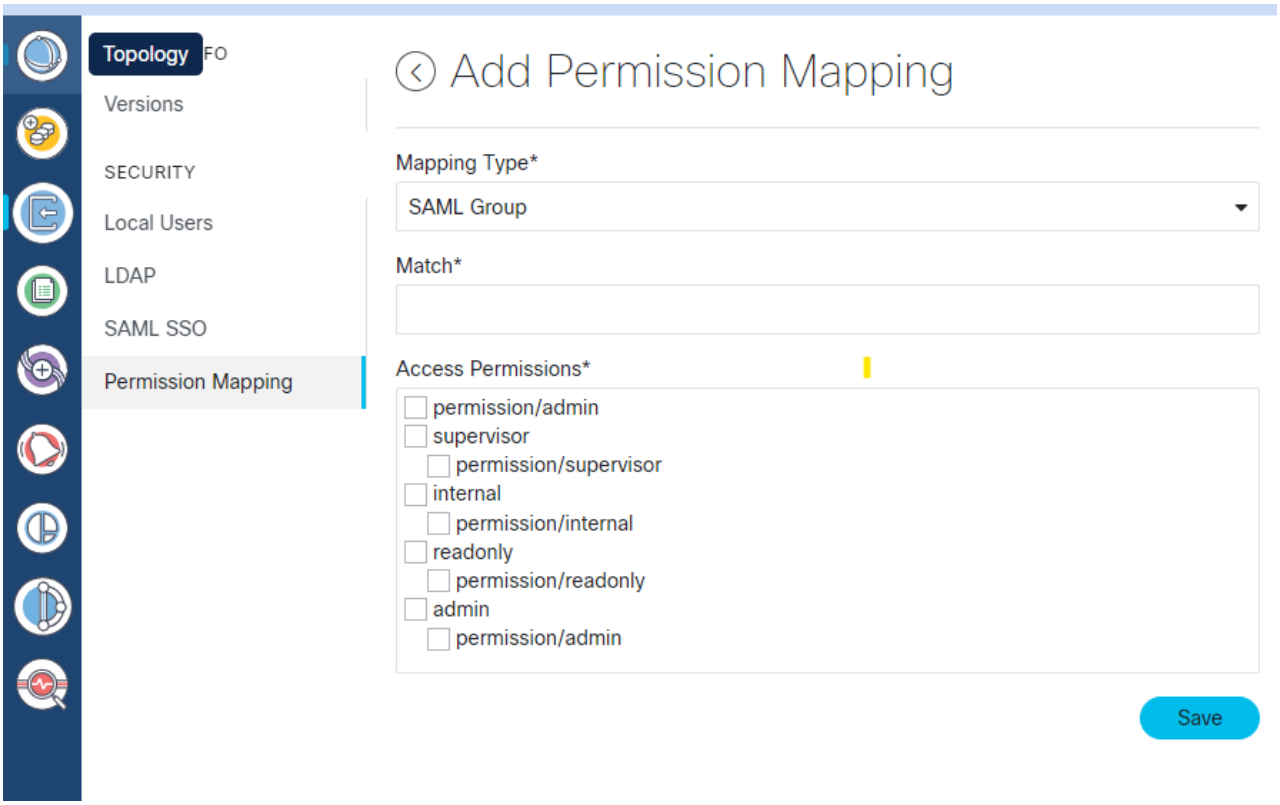
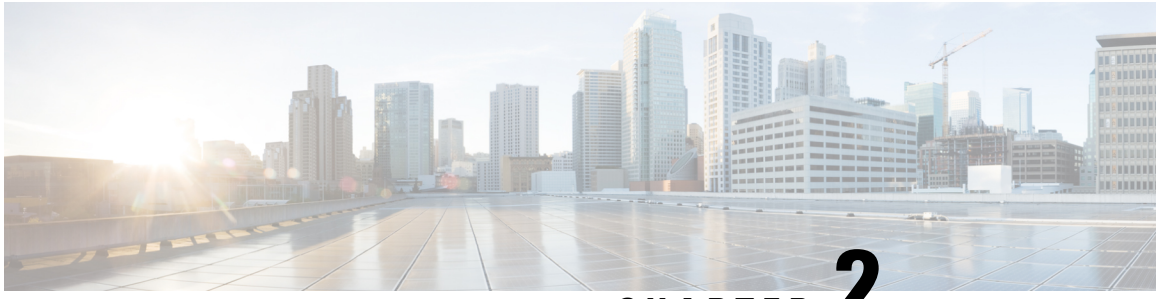


Figure 9: Add Permission Mapping



Note User can have different levels of permission mapping.

- **Admin**: No restrictions.
- **Supervisor**: Similar to admin but with restrictions on user management and log checks.
- **Readonly**: Can only check but provisioning is not allowed.
- **Internal**: To be used in case of any triage or troubleshooting to collect commands. It is recommended to use it only under supervision of Cisco Technical Assistance Center (TAC).



CHAPTER 2

Use Cisco Optical Network Controller

Before you begin

Log into Cisco Optical Network Controller, on page 2

Once you login, the **Topology** screen is displayed by default. The menu options are displayed on the left panel. You can click on the options and navigate to any specific screen. The options available are given below.

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

Note The following options can be used commonly across multiple application screens.

- The timestamp appears on the top right corner of the screen in all the screens. It follows the UTC time zone. The current date is displayed along with the time.
- Click **Refresh** button to refresh the status of the table content in each of the application screens anytime.
- Click **Show or hide columns** icon to select any columns to be displayed or hidden from the table view anytime.
- Click **Export** to export the details of any table from any application screen to a spreadsheet file.
- Use the **Sort** option to sort the table values and use the **Filter** option to filter the table content as per requirement in each application screen.

Topology

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

The OTS option is used to show all fiber span between all type of nodes, OLT or ILA. The OMS option is used to display only the ROADMs and the links between the ROADMs in the given network.

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

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

Table 1: Alarm Severity

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

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

Note

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

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

Table 2: Topology Node Options

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

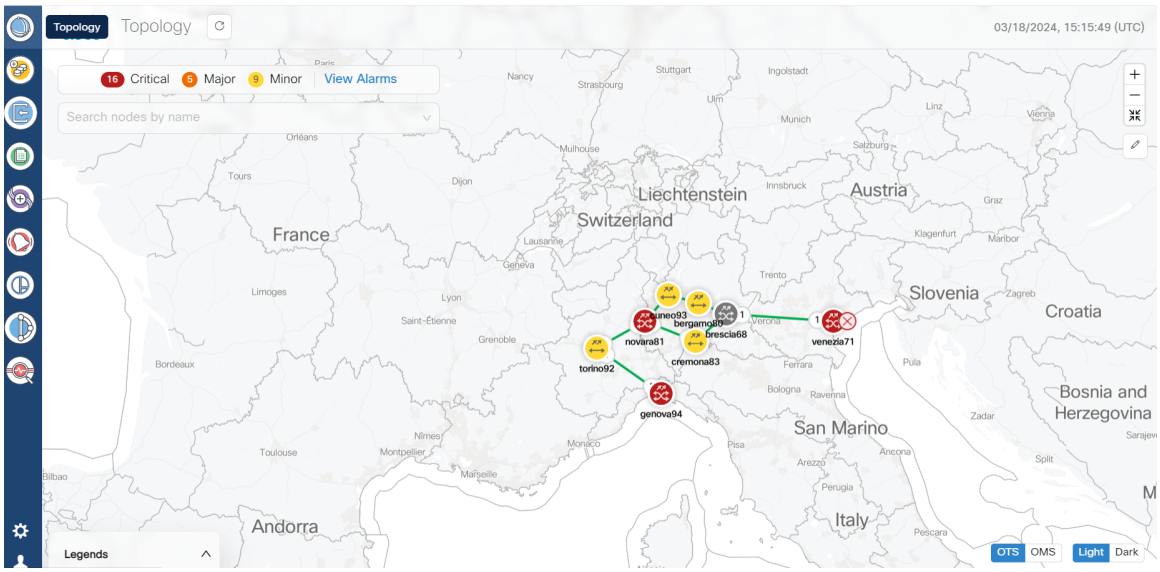
You can also view the information related to the different nodes, links, and the states of each node in the network at any point in time by clicking the **Legends** option. To select any node in the network, use the drop-down box to select the node.

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

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

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

Figure 10: Topology Application



Note

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

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

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

- In the **Topology** map if two nodes have the same geo location then they appear as a single node due to overlapping with each other which is a constraint.
- If any node in the **Topology** screen does not have a geo location specified, the button in the upper right corner which is used to enter the geo location value displays an orange highlight or dot. This orange dot is used to represent that there is atleast one node which does not have any geo location specified. When you click this orange dot a pop-up menu appears displaying all such nodes that are lacking geo locations. Click the **Edit** icon and then select any node to move it to any desired location om the map. This will add the geo locations to the node. You can move the node and the **Topology** maps the geo location automatically for these node based on the location.
- Once the geo location is selected, Cisco ONC displays a message to indicate that the **Topology** has been updated and to view the updated changes you must refresh the page by clicking the **Refresh** or **Reload** button.

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

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

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

Figure 11: Topology Live PM

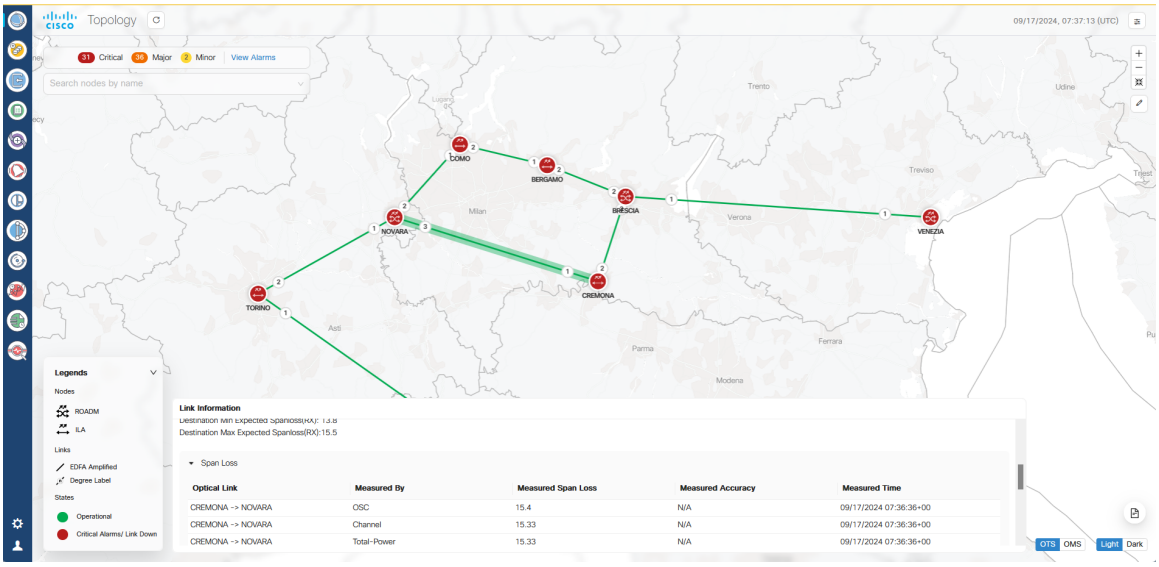
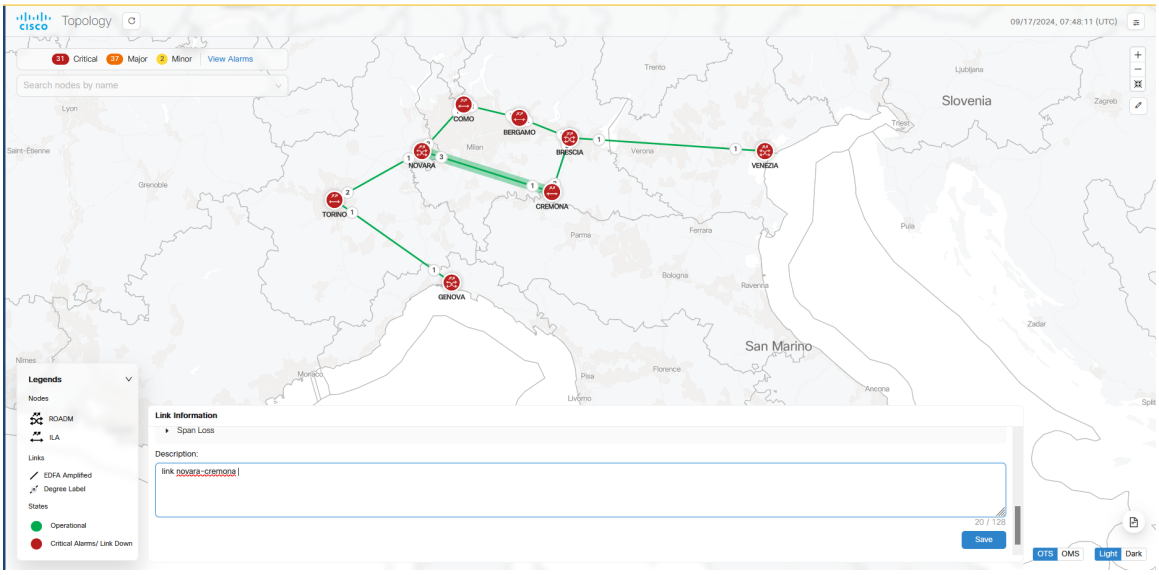


Figure 12: Tool Tip



Troubleshooting in Topology

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

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

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

Nodes

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

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

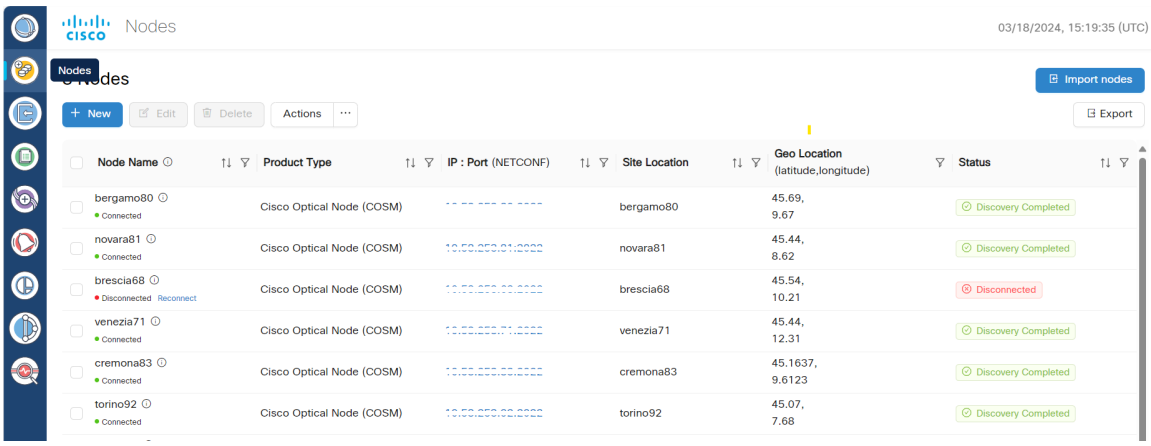
- **Node Name**: The name of the node. The node name provided by you must match the original node name used in the network. In case of any mismatch or discrepancy issues, the original node name in the network is used for outgoing payloads.
- **Product Type**: The type of product the node belongs to. For example: Cisco Optical Site Manager.
- **IP: Port (NETCONF)**: The IP address of each node along with the part number.
- **Site Location**: The location of the site that each node belongs to. For example: COSMp2p83_Site1
- **Geo Location**: The geo location of each node in terms of the latitude and longitude values based on where exactly the node is situated in the world at any given time.

Note If the geo location values that are coming from Cisco Optical Site Manager in a pre-filled format has more than four digits, then the length of the go localtion value is truncated to only four digits.

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

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

Figure 13: Nodes

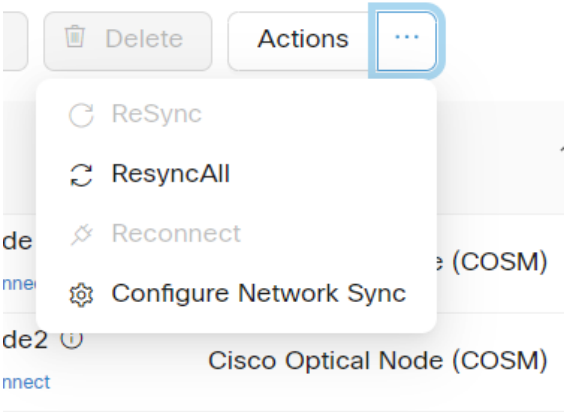


Use the sort or filter options to sort and filter values in the table. You can also cross launch to other supported pages using the links provided in this table.

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

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

Figure 14: Actions



Note

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

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

Troubleshooting in Nodes

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

- **Bulk import failure**

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

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

- **Nodes possible status**

Node Status	Description	User Action
In Progress	Cisco ONC is collecting information about the onboarded device.	No action is needed, wait for the status to change.
Resync Pending	Cisco ONC has gone out of sync with device and is scheduled for a resync.	Either wait for scheduled resync or start the resync manually.

Resync In-progress	Cisco ONC is re-collecting information about the onboarded devices.	No action is needed, wait for the status to change.
Disconnected	Cisco ONC was unable to establish a session with COSM.	Attempt re-connect or resync. If the problem still persists contact Cisco TAC.
Discovery Completed	All information has been collected from the device and it is ready for operations. **Note** It is recommended to wait for 60 secs once the device is turned to Discovery Completed state which ensures the device is ready for accepting requests.	

- **Nodes connection status**

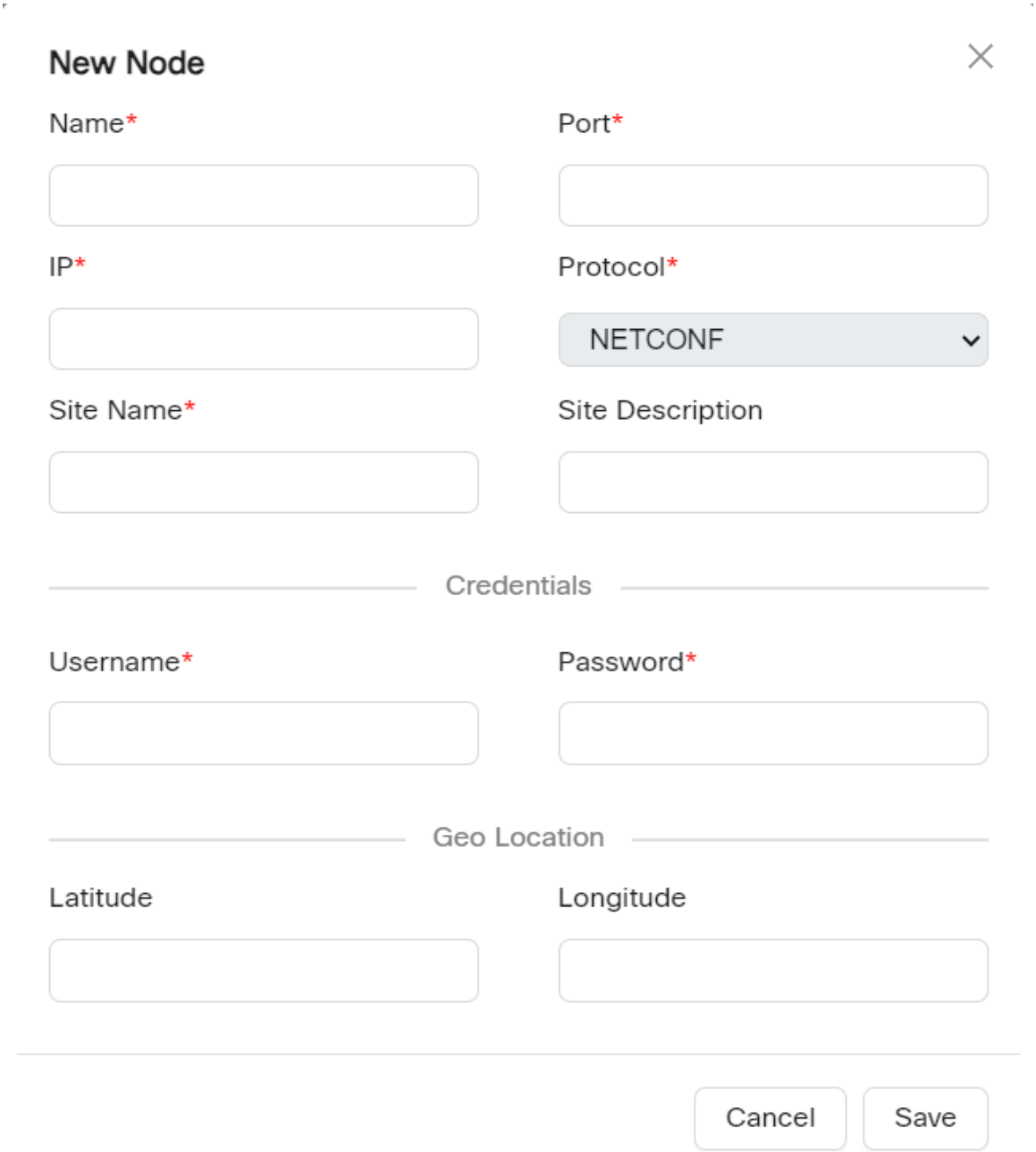
Connection State	Description	User Action
Connected	Cisco ONC has successfully established the session with the COSM device provided user/password information.	No action is needed.
Disconnected	Cisco ONC was unable to establish session with COSM.	Attempt re-connect or resync. If the problem still persists contact Cisco TAC.
Waiting for connection	Cisco ONC is attempting to establish connection with COSM.	No action is needed.
Resync_needed	Cisco ONC has gone out of sync with device and is scheduled for a resync.	Either wait for scheduled resync or start the resync manually.

- **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.

Add Nodes on Cisco Optical Network Controller

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

Figure 15: Add New Node



Before you begin

To add nodes to Cisco Optical Network Controller:

- The NCS 1010 nodes must run IOS XR Release 24.3.1.
- Cisco Optical Site Manager must be installed on the node.
- All NCS 1010 nodes must be added to Cisco Optical Network Controller with port number 2022.

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

Step 2 Click **New**.

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

Table 3: Add new node

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

Note

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

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

Import Nodes on Cisco Optical Network Controller

Before you begin

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

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

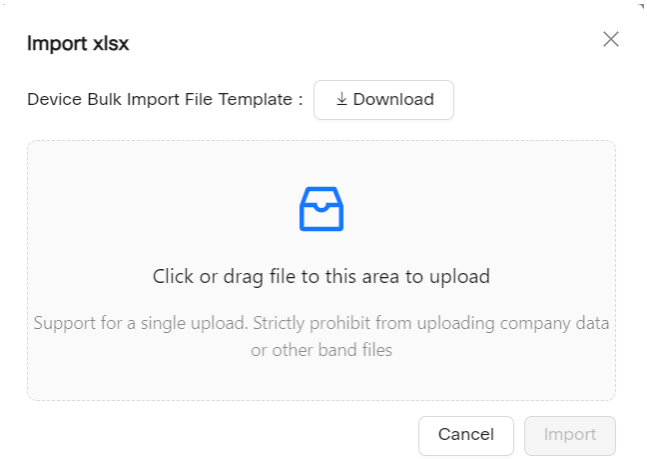
Step 2 Click **Import** to import the table details from external files.

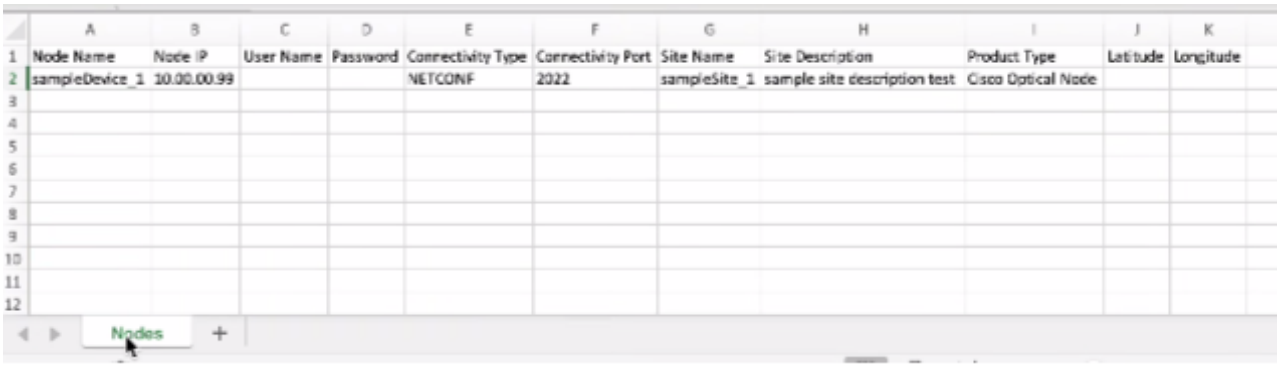
Step 3 Select the spreadsheet which has all the node details and click **Open**. The new nodes are onboarded and added to the **Nodes** table.

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

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

Figure 16: Import Nodes





Node Name	Node IP	User Name	Password	Connectivity Type	Connectivity Port	Site Name	Site Description	Product Type	Latitude	Longitude
sampleDevice_1	10.00.00.99			NETCONF	2022	sampleSite_1	sample site description test	Cisco Optical Node		

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

Table 4: Bulk Import File Template

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

Export Nodes on Cisco Optical Network Controller

Before you begin

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

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

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

Edit Nodes on Cisco Optical Network Controller

Before you begin

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

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

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

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

Delete Nodes on Cisco Optical Network Controller

Before you begin

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

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

Step 2 Select the node or nodes to be deleted.

Step 3 Click **DELETE**.

This will delete the selected node from the table.

Note If the circuits are active and flowing over the nodes or if the resync is in progress, then deletion of the node fails. In this case you will receive an error message for the **Circuit Deletion Failure** when the circuit is spanning through the node.

For example: <Device A> cannot be deleted because circuit spanning across the device.

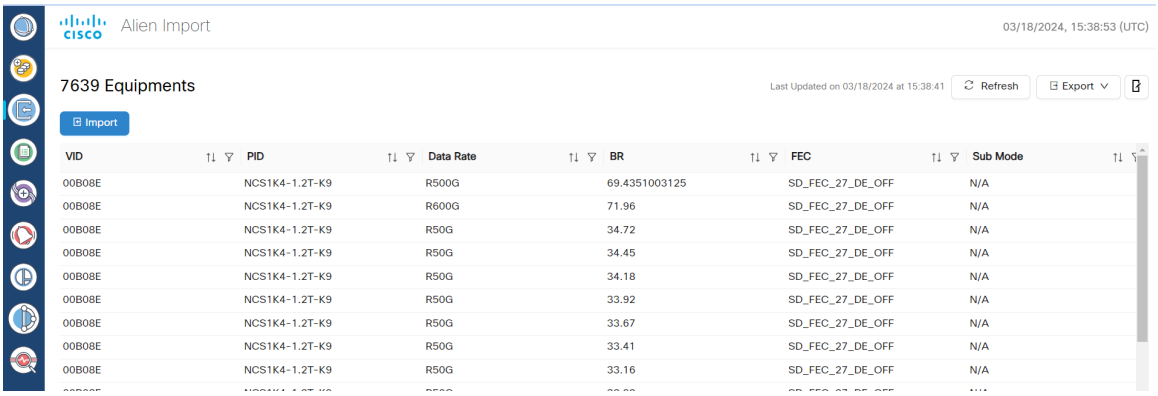
Alien Import

Before you begin

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

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

Figure 17: Alien Import



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

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

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

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

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

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

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

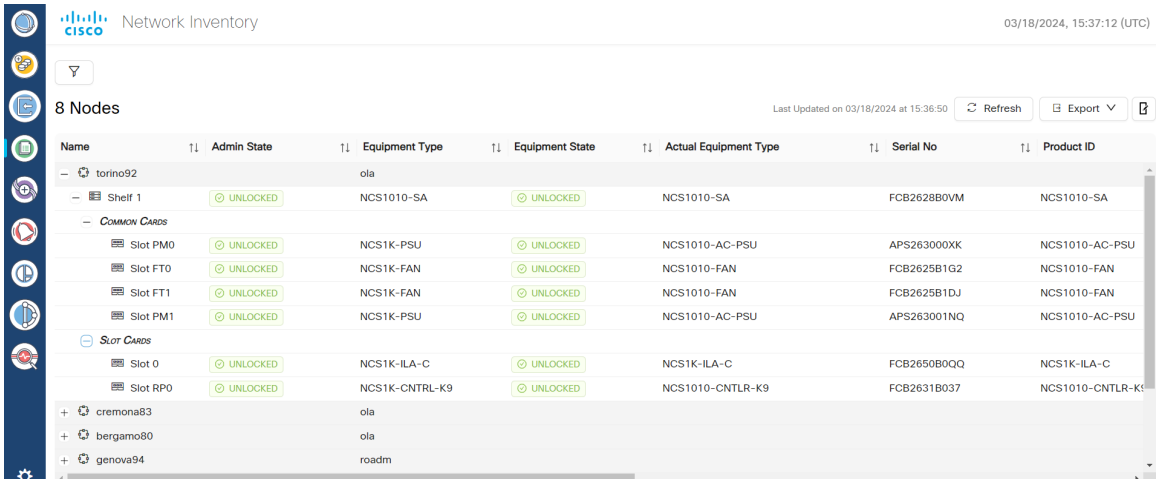
Step 6 Use the sort or filter options to sort and filter values in the table.

Network Inventory

Before you begin

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

Figure 18: Network Inventory



Step 1 Click **Network Inventory** in the left panel.

Cisco Optical Network Controller displays the Inventory tab. This tab displays all the inventory at the selected site.

Step 2 Click the node that you want to view the details of.

There is an option for selecting cascading windows for each node to view the Common Cards and the Slot Cards.

Step 3 (Optional) To export inventory data into an excel file, click **Export**.

Step 4 Click the **Refresh** button to refresh the inventory status.

Step 5 Use the filter to search using **Custom Search** or **Quick Search** options.

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

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

Service Manager

Before you begin

Circuits are referred to as services. The **Service Manager** screen helps in viewing and creating services. **Service List** page displays the list of services which can be viewed and exported anytime. The **Provision Service** option allows to create a new service.

Note

- The recommended number of circuits that you can create or delete at once are up to a maximum of five circuits, even though it is possible to create or delete more than five circuits at any given point in time. In such cases, you can stop provisioning these additional circuits as required. Also, it is recommended that you wait until reaching the final status before you can work with other circuits.

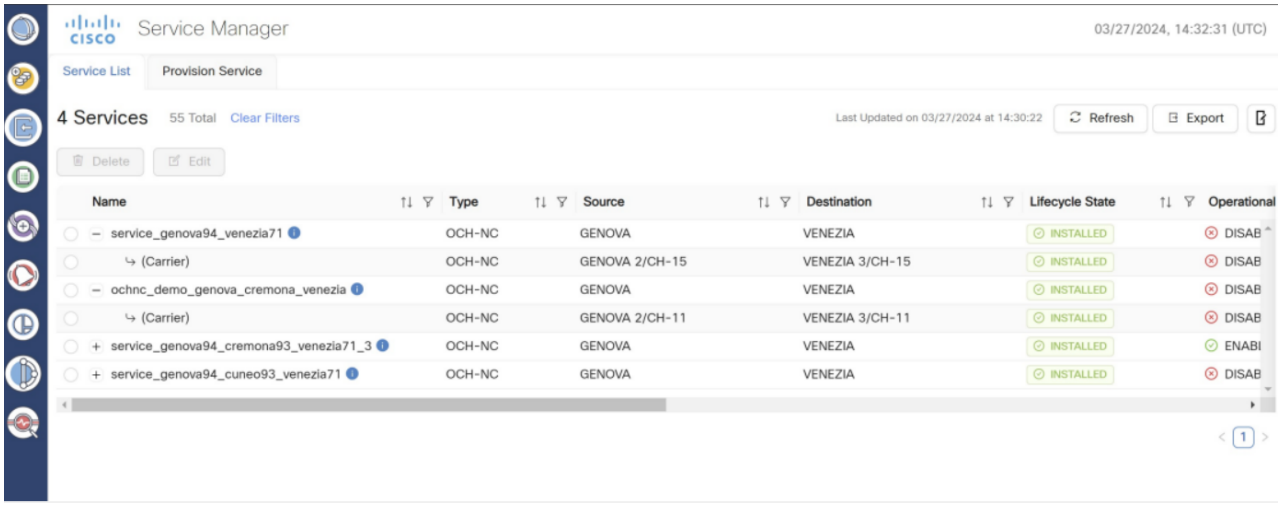
There are circuits called brownfield circuits which can be already present on the devices before the onboarding proceeds. The configuration of these brownfield circuits happens outside Cisco ONC.

Brownfield circuits are circuits that are already existing on devices. The configuration of these circuits is done either outside of Cisco ONC like in COSM or through NCS 1010 CLI. It can be configured through a different instance of Cisco ONC as well which is managing the same network. The brownfield circuit's service names have the following format:
onc_*<SourceNode-Name>*_*<Source-Port>*_*<DestinationNode-Name>*_*<Destination-Port>*.

To create a new service, follow the procedure given below.

Step 1 Click **Provision Service** in the left panel

Figure 19: Service Manager

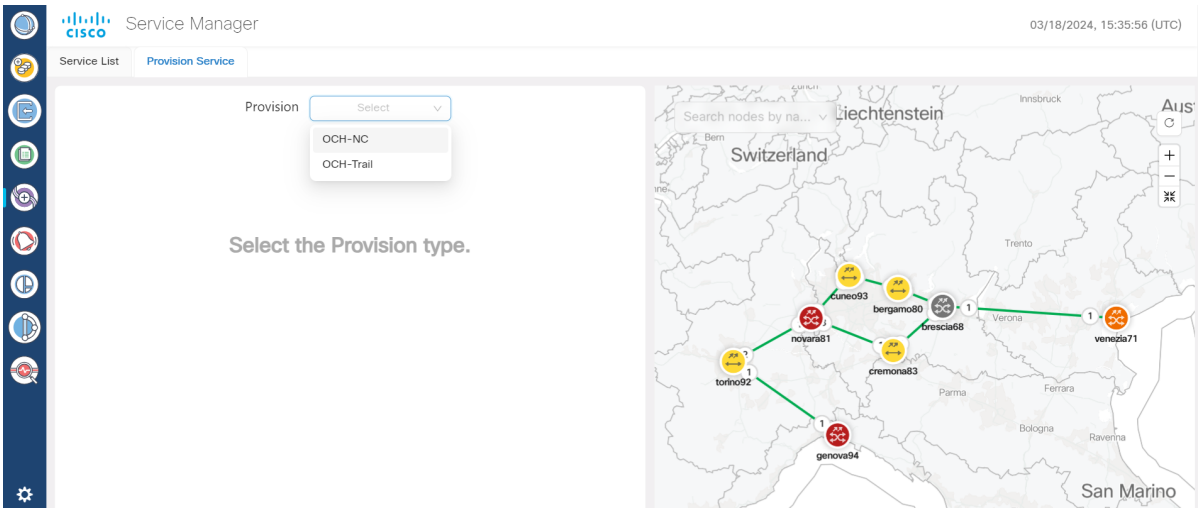


Step 2 Click **Provision** and select **OCH-NC** or **OCH-Trail.**

Note

- **OCH-NC**: The circuit is created between Add/Drop ports on the terminal OLTs or ROADMs.
- **OCH-Trail**: The circuit is created between trunk ports of transponders or muxponders.

Figure 20: Provision Service



Step 3 Enter the details as per the sequential steps listed for the type of circuit and channel selected along with the other required preferences by clicking **Next** after each page. Fill each tab as per the details given below.

Figure 21: Provision Service Tabs

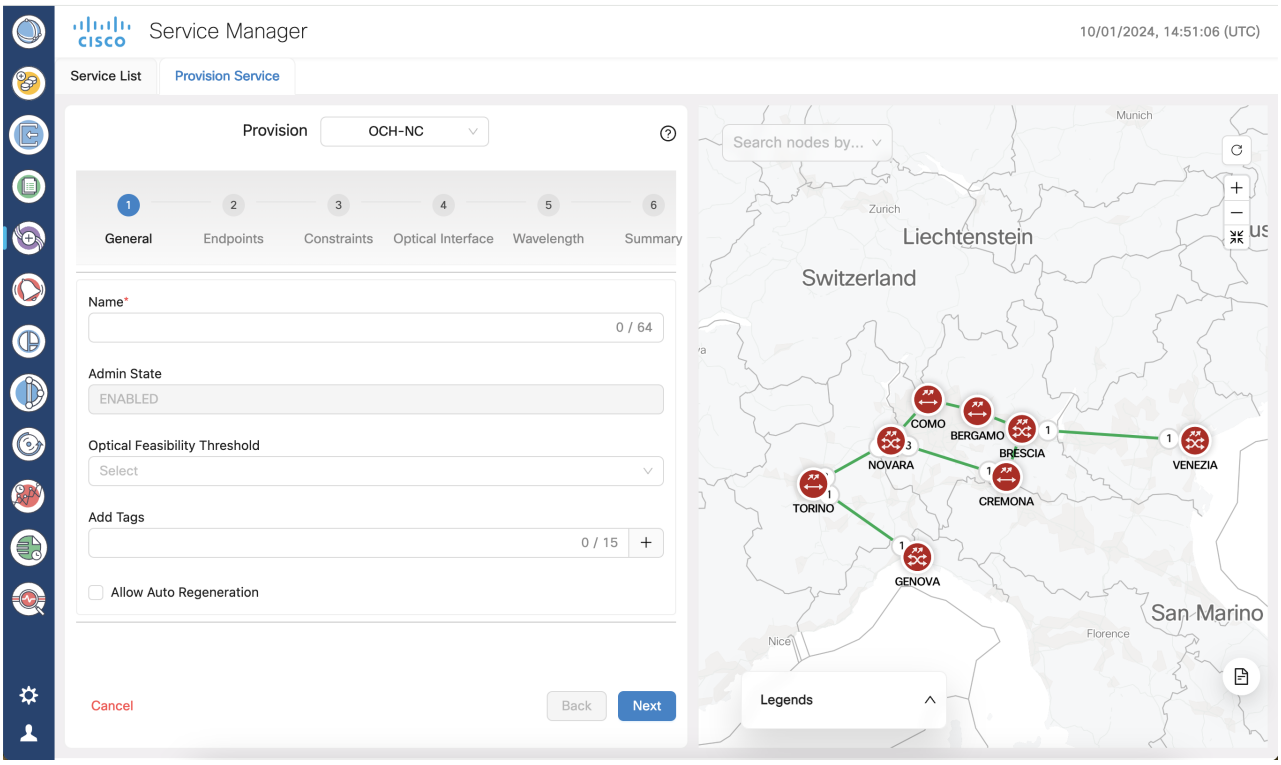


Table 5: Provision Service Tabs

Provision Service Tabs	Description
GENERAL	**Name**: The unique user defined name of the **OCH-NC** link. (Allowed characters are a-z, A-Z, 0-9 and _. <Space not allowed>). **Admin State**: only **ENABLED** is supported in 24.3.1. **Optical Feasibility Threshold**: Select **RED, GREEN, YELLOW** or **ORANGE**. GREEN = mean value YELLOW = +1 sigma ORANGE = +2 sigma RED = +3 sigma **Add Tags**: If user wants to add any tags to the service. **Allow Auto Regeneration**: Whether to allow auto regeneration (*not supported in 24.3.1).
ENDPOINTS	**Single Channel/Multiple Channel** In case of multi channel between the same **Endpoints**, the user can add multiple carriers, using the **Add** button, in a single OCH-NC service provisioning using different channel ports. **Endpoint A/Endpoint B**: Source and Destination Nodes. This can be selected either from the drop down menu or by clicking on the map icon and then selecting the node. **Select port**: Source port or Destination port from where you need to provision the service.

Provision Service Tabs	Description
CONSTRAINTS	**Optimization goal** (optional): The optimization goal (**Length or Hops** or **OSNR**). **Disjoint from service** (optional): The new **OCH-NC** line is not allowed to use the specified path. **Include nodes or links** (optional): Used to add **Constraints** for the new service by selecting from the drop down or by using the map. **Exclude nodes or links** (optional): Same as the above option but the **Constraints** here are used for excluding nodes or links. Click the re-cycle icon to remove any of the included or excluded items.
Optical Interface	◦ **Customer Name**: The Customer name. ◦ **Product ID**: The product ID. ◦ **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**: This may appear depending on the other settings. **Reload application code**: Use this for a allenWL recently imported with Alien Import feature to reload the list of the Application code available for OCHNC provisioning. Reset can be used for resetting all the fields. **Note** For OCH-trail Optical Interface field is auto populated and non-editable.
Wavelength	Central Frequency (THz): This can be filled in two ways. • By filling the frequency value in the field. • By spectrum occupancy
Summary:	Summary of all the previous five steps given above.

Step 4 Click **Preview** to the preview the circuit before it is created.

Step 5 Click **Finish** to create the circuit.

Step 6 Click **OK** once the circuit is provisioned successfully.

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

Step 7 Click **Edit** option to edit any selected service name from the table.

Step 8 Click **Delete** option to delete a selected service from the table.

Step 9 Click + icon after selecting any node 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.

Note While provisioning a service you can also click and select any object from the map and that object's details gets added in the Endpoints tab automatically.

Troubleshooting in Service Manager

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

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

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

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

Failure Scenario	Cisco ONC Error	Recovery Step
COSM Node gets disconnected as soon as a service is provisioned in CONC	Config Failure	Delete the circuit and reprovision from the CONC.
COSM nodes are in sync state during CONC provisioning.	Config Failure	Check the COSM node and wait for synchronisation to complete.

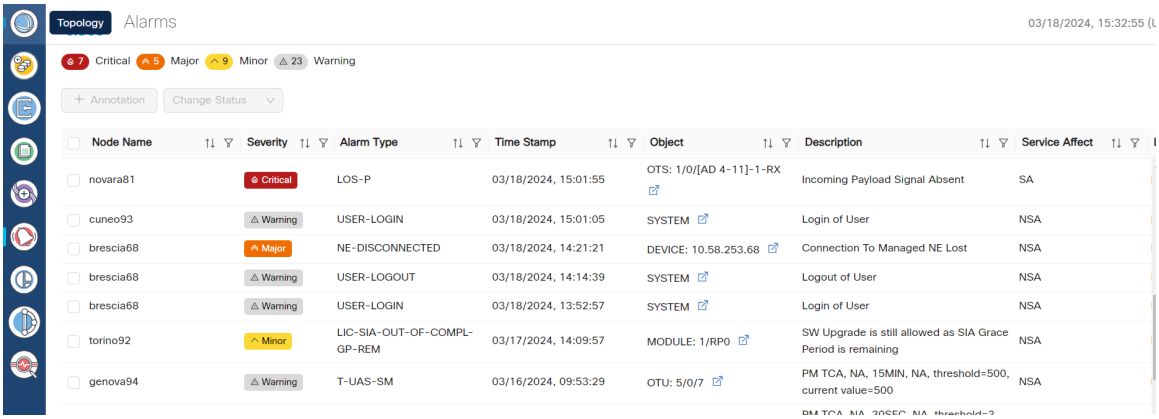
NCS 1010 Devices under COSM Nodes are locked	Config Failure	• Check COSM and unlock the NCS 1010 device. • Verify COSM synchronisation status to be completed.
COSM node Restart during provisioning	Config Failure	Wait for CONC to re-establish the connection successfully after restart and its status moved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

Alarms

Before you begin

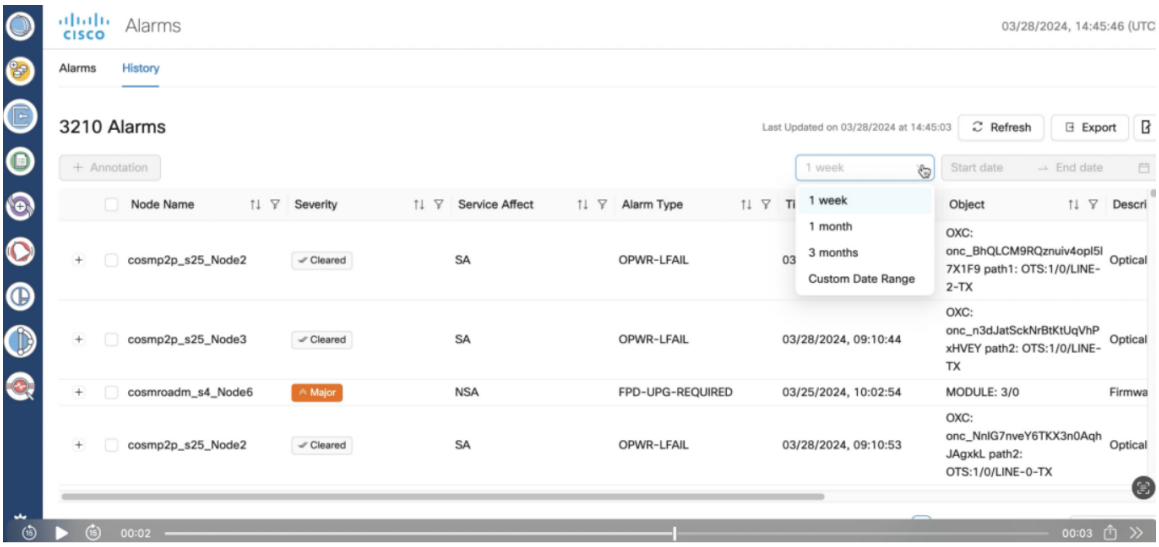
The **Alarms** screen displays all the alarm details for each node based on the severity level. You can view both the active alarms and the previously active alarms in this screen.

Figure 22: Alarms



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

Figure 23: Alarms History



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

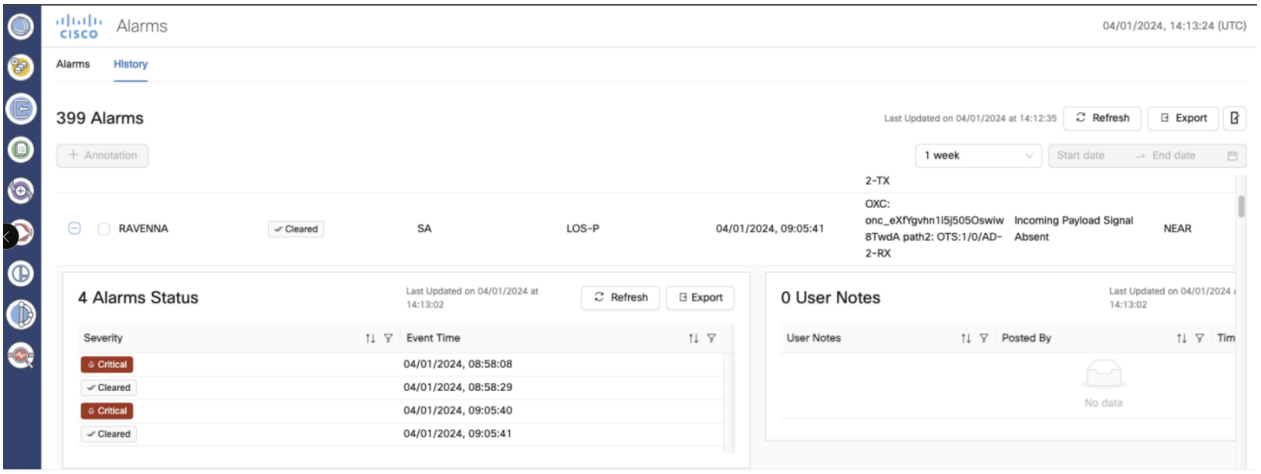
Step 2 Select the **Alarms** tab to view the active alarms of each node.

Step 3 Click **Annotation** to add user notes to any alarm, select the node and c. Add the user notes and click **Add**. This will send a notification to the user for the alarm. You can add multiple notes to multiple alarms in the form of a list.

Step 4 Click **Change Status** to acknowledge or unacknowledged alarms.

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

Figure 24: Alarm History Expanded View



Step 6 Click any cross-launch icon for any node to cross launch to the linked COSM.

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

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

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

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

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

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

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

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

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

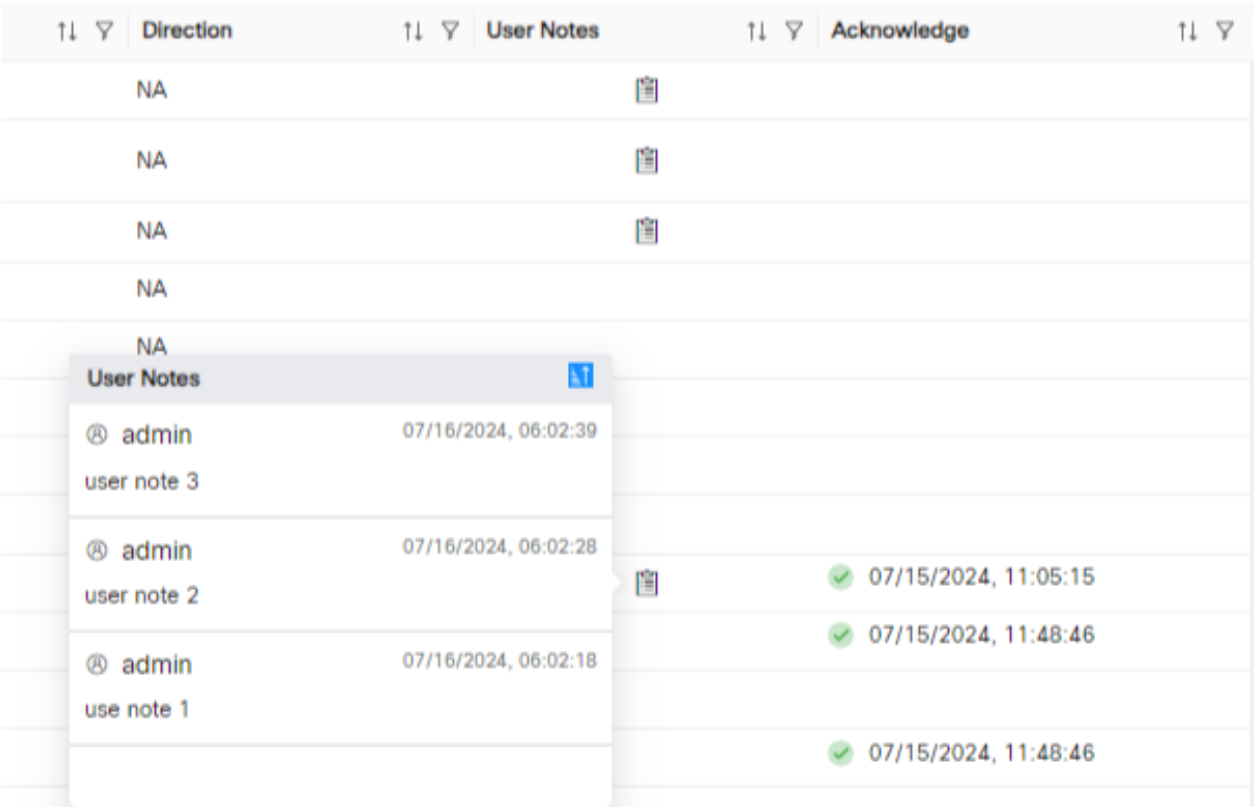
Step 12 Use the **Acknowledge** column in the table to view the acknowledged or unacknowledged alarms.

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

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

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

Figure 25: User Notes



Workspaces

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** and **Circuit Monitoring**.

Figure 26: Workspaces

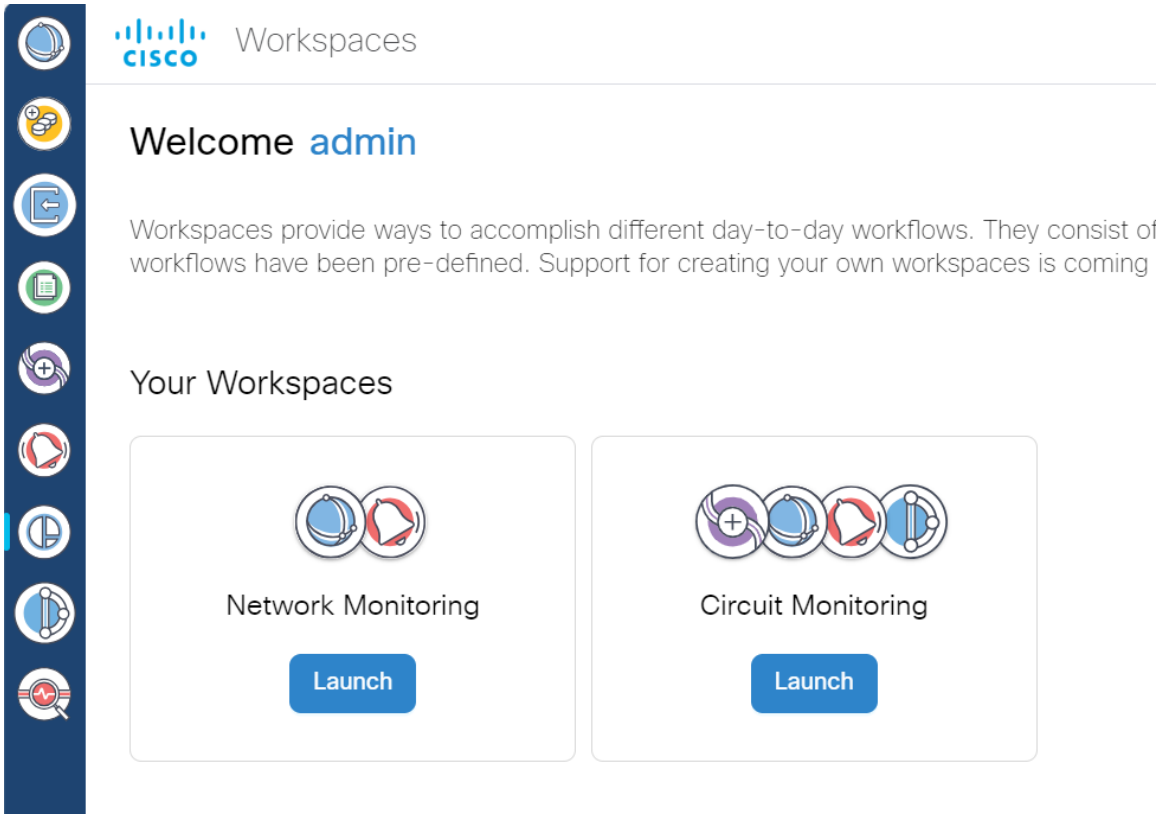
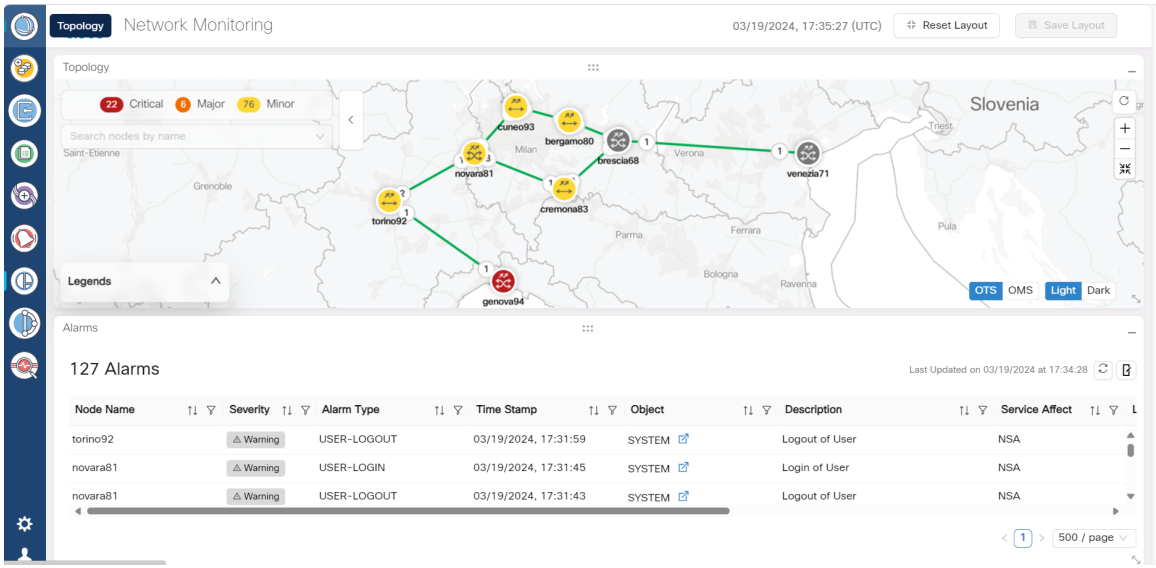
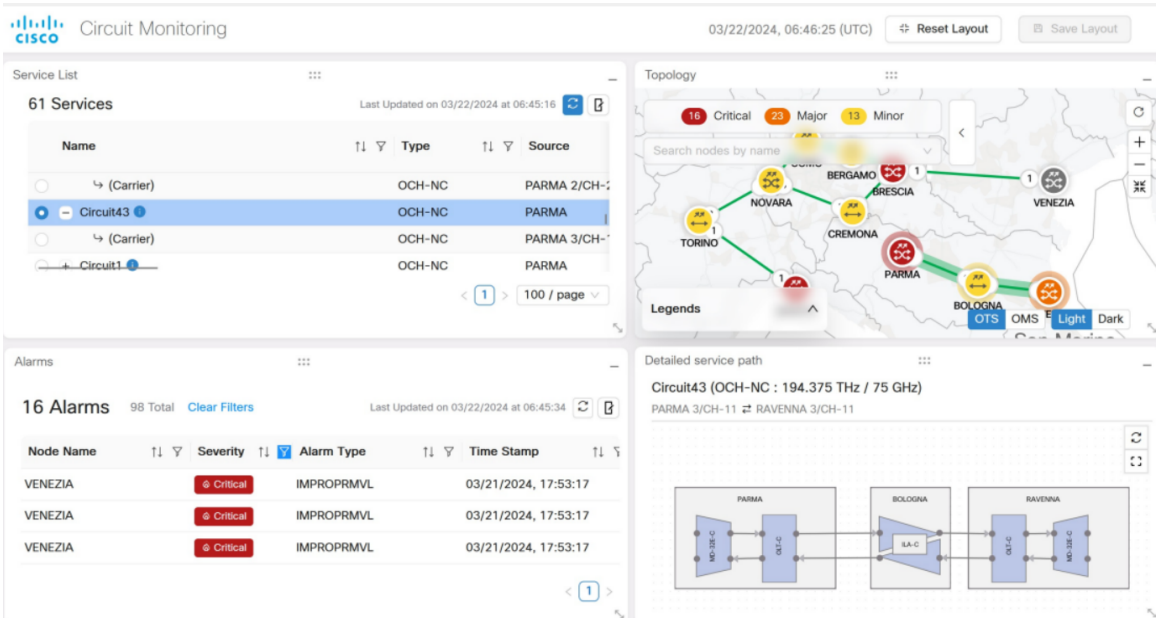


Figure 27: Workspaces Network Monitoring



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

Figure 28: 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.

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.

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

Step 2 Select the workspace and click **Launch**.

Step 3 Click **Save Layout** to save the layout at any given point in time.

Step 4 Click **Reset Layout** to revert to the default layout.

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

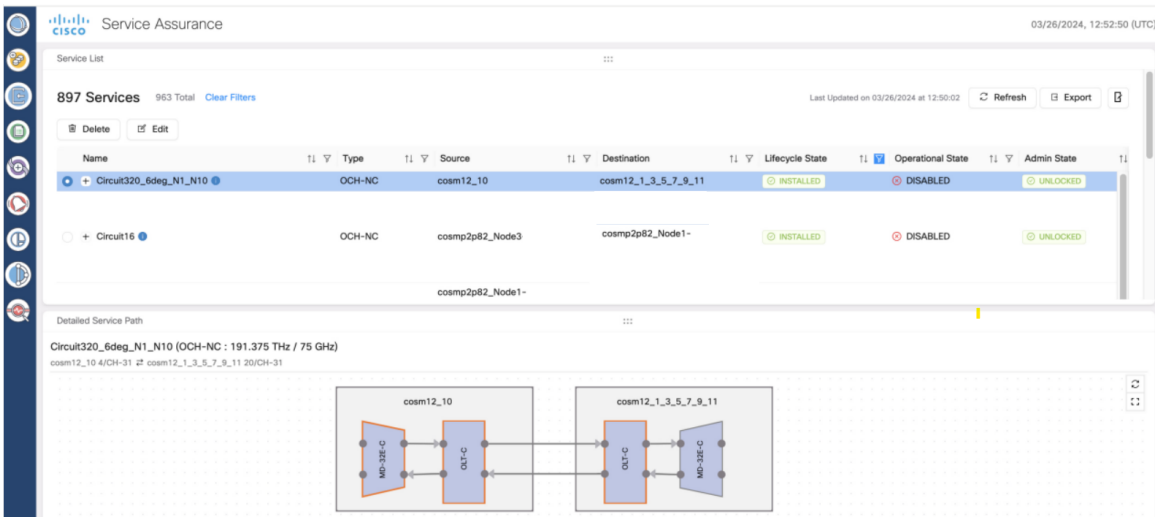
- Hovering on the nodes displays the node name and the alarm severity.
- Hovering on the equipment displays the equipment name, service state as enabled or disabled and the count of the severity of the alarms.
- Hovering on the port which is displayed as a round icon on the panel displays the port name, service state, and the alarms severity counts.
- Connectivity between each equipment is highlighted with arrows.
- If you right click at the node level it will cross launch to the Nodal UI to verify OXC's.
- If you right click at the equipment level it will cross launch to View Nodal UI: Equipment.
- If you right click on any port it will cross launch to View Nodal UI: Port.
- Connectivity between the nodes are represented with arrows.

Service Assurance

Before you begin

The **Service Assurance** option helps in visualizing the circuits and the related nodes, links, and the circuit paths.

Figure 29: Service Assurance



Step 1 Click **Service Assurance** in the left panel.

Step 2 Select the service from the **Service List**.

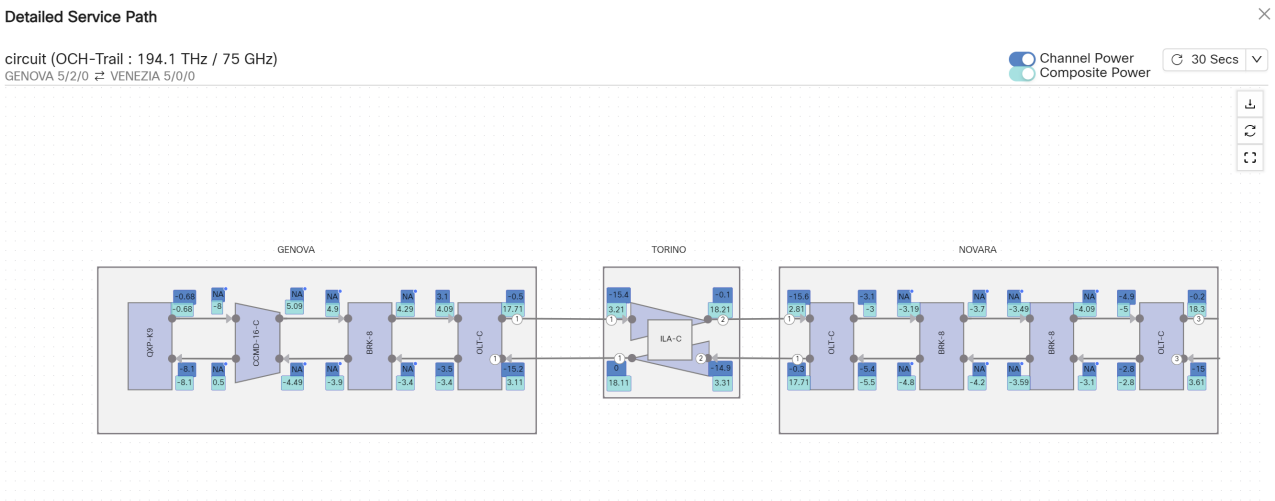
Step 3 In the **Detailed Service Path** layout, you can view the service details by hovering over the visual circuit for each node, ports, links, and paths of any service at any given time. These details are available when the **Lifecycle State** is either **INSTALLED** or **DELETION FAILED**.

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.

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

Figure 30: 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.

Step 5 Click **Refresh** to efresh rates or intervals mentioned for fetching live PM data.

Monitoring

- **Audit Log**: You can view the audit logs related to the user login or logout, device enrollment, device re-sync service for circuit create, delete or edit options. Also the create, edit or delete user options.
- **Detailed Node Resources**: You can monitor the CPU, memory or disk consumption of the host.
- **Log Viewer**: Displays the internal logs of microservices.
- **Pod Monitoring**: You can monitor the CPU, memory or disk consumption of the microservices within the kubernetes cluster.

Before you begin

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

Click to view each option separately.

General Troubleshooting

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:

  ```
  sedo diagnostics archive-logs
  ```

  Collect it along with the Grafana view.

Support for NCS1K4-OTN-XP and NCS1K4-2-QDD-C-K9 Line Cards

From CONC 24.3.1 onwards, the following line cards are enabled on the NCS 1004 chassis:

- NCS1K4-OTN-XP
- NCS1K4-2-QDD-C-K9

NCS1K4-OTN-XP Supported Component

The NCS1K4-OTN-XP line card supports three pluggables, each with two trunks. Each pluggable supports different card modes based on its type. See COSM Configuration Guide for more details.

The **NCS1K4-OTN-XP** pluggables are:

- CFP2
- QDD-400G-ZRP
- DP04CFP2-M25-K9

NCS1K4-OTN-XP FEC Modes

The Forwarding Error Correction (FEC) modes supported on the NCS1K4-OTN-XP line card are:

- CFEC
- OFEC

NCS1K4-2-QDD-C-K9 Supported Components

The NCS1K4-2-QDD-C-K9 line card supports fixed trunks and the components as given in the table.

Table 6: NCS1K4-2-QDD-C-K9 Supported Components

Supported Component	Description
Two trunks	Each with 100G, 200G, 300G and 400G trunk rates.
Card modes	The two card modes supported are: • MXP Slice 1K- Trunk with 100G, 200G, 300G and 400G trunk rate. • MXP 1K – Trunk rate up to 400G.
FEC modes	The four FEC modes supported are : • SD-FEC-27 • SD-FEC-15

OCH Circuit Trail Provisioning for NCS1K4-OTN-XP and NCS1K4-2-QDD-C-K9 Cards

CONC 24.3.1 supports and provides OCH circuit trail provision for the NCS1K4-OTN-XP and NCS1K4-2-QDD-C-K9 line cards.

Unmanaged Equipment Support

Unmanaged devices are third party devices that can be included in the Cisco Optical Network Controller 24.3.1 circuit trails connected to transponders.

Cisco Optical Network Controller 24.3.1 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 31: Unmanaged Equipment Support in Topology

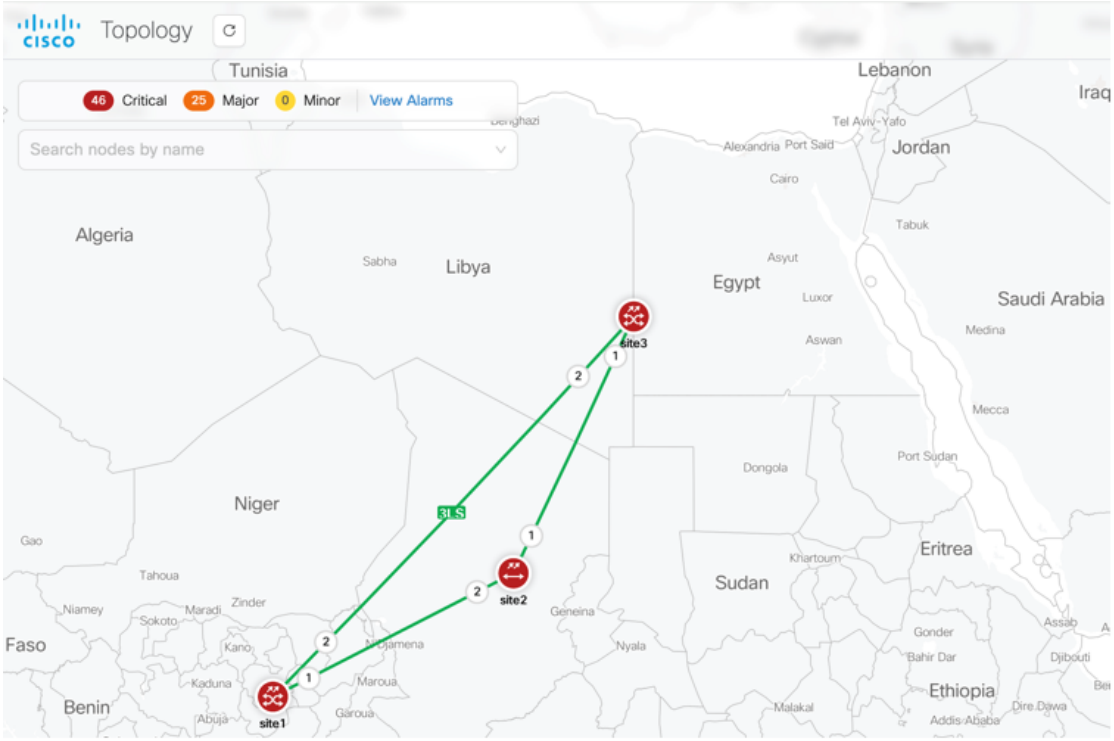
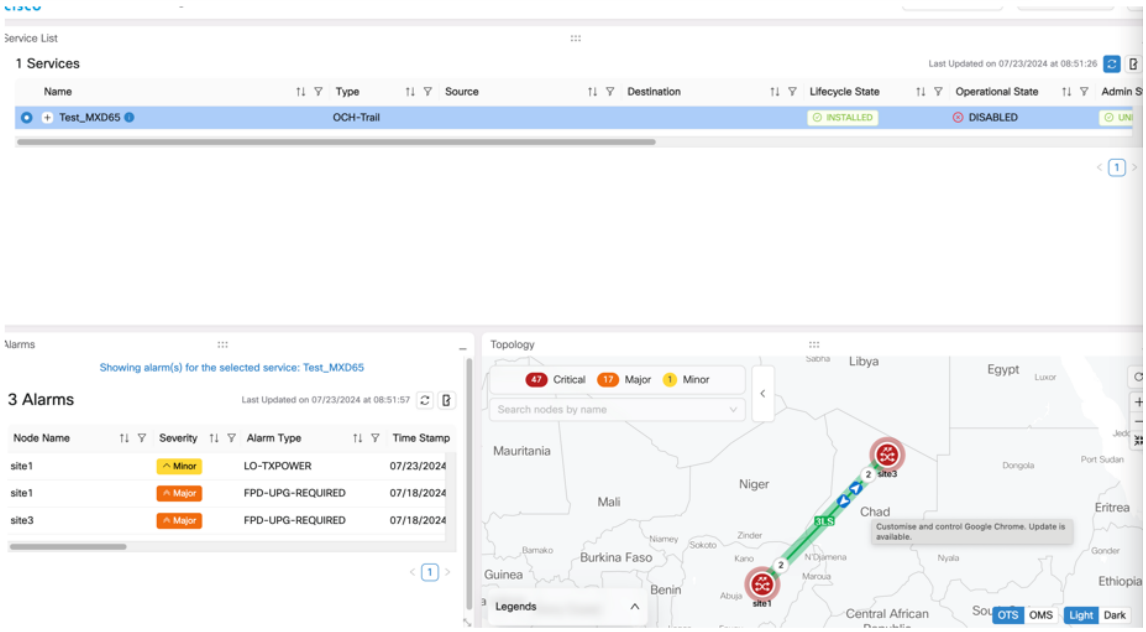


Figure 32: Unmanaged Equipment Support in Service Assurance



Log Viewer Application

Cisco Optical Network Controller supports two sets of logs:

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

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

Audit Logs

The **Audit** logs option helps in:

- Auditing all the Cisco Optical Network Controller operations which include provisioning, Cisco Optical Network Controller and COSM user login or logout procedures and traffic related operations that are done on COSM or node.
- The logs can be used to learn about all the changes that have occurred as a result of external notifications that come from connected nodes.

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

Display Features

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

Categorization of Audit Logs

Audit logs are categorized into:

Table 7: Audit Logs Category

Category Field	Description
System	The events that are part of this category are: • Login. • Logout. • Create user. • Delete user.
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.

Category Field	Description
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.
Alarm	All the events related to **Alarms**.
Alien_Import	All the events related to **Alien_Import**.

Note

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

Debug Logs

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

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

Retention and Archiving and Archive Logs

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

- **Audit** logs are retained for up to seven days which can be viewed online using the **Logs** application.
- Logs beyond seven days are archived and kept in the Cisco Optical Network Controller storage. The **Archive** logs are maintained for three months and are deleted later.
- The archived logs can be downloaded any time by using the **Archive** tab in the **Logs** application.

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

Archive Logs

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

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

Note **Techdump**: 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.

Note

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

Sedo Commands

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

The sedo commands are as given:

1. Step 1:

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

2. Step 2:

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

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

1. Step 1:

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

   For example:

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

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

2. Step 2:

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

3. Step 3:

   You can download the file to the local system.

Figure 33: Audit Logs

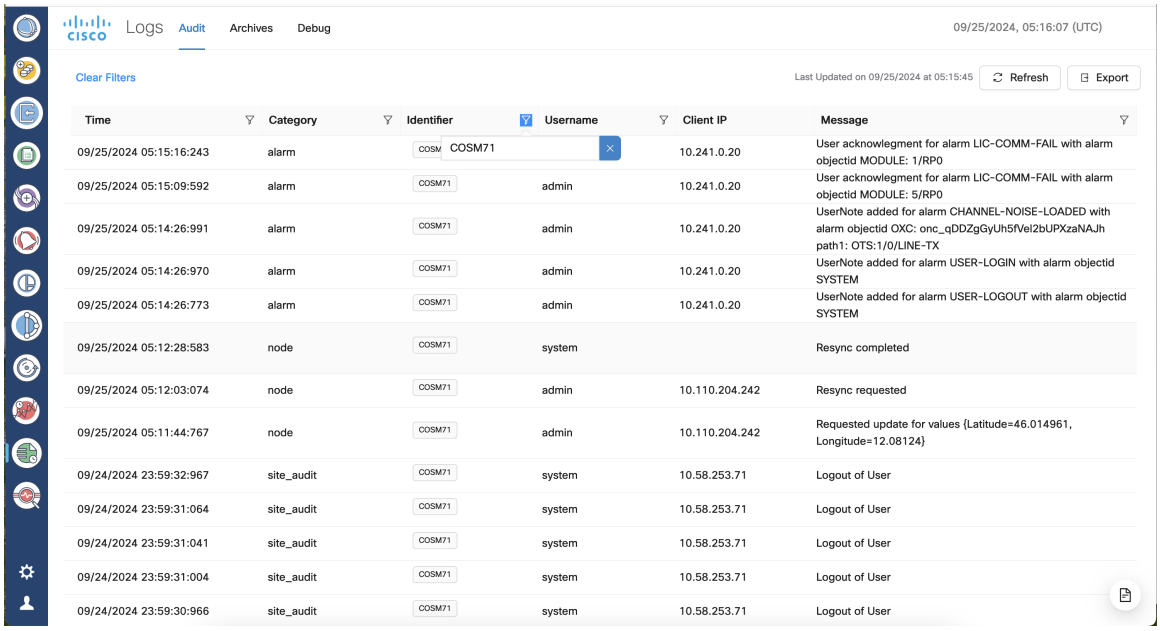


Figure 34: Archive Logs

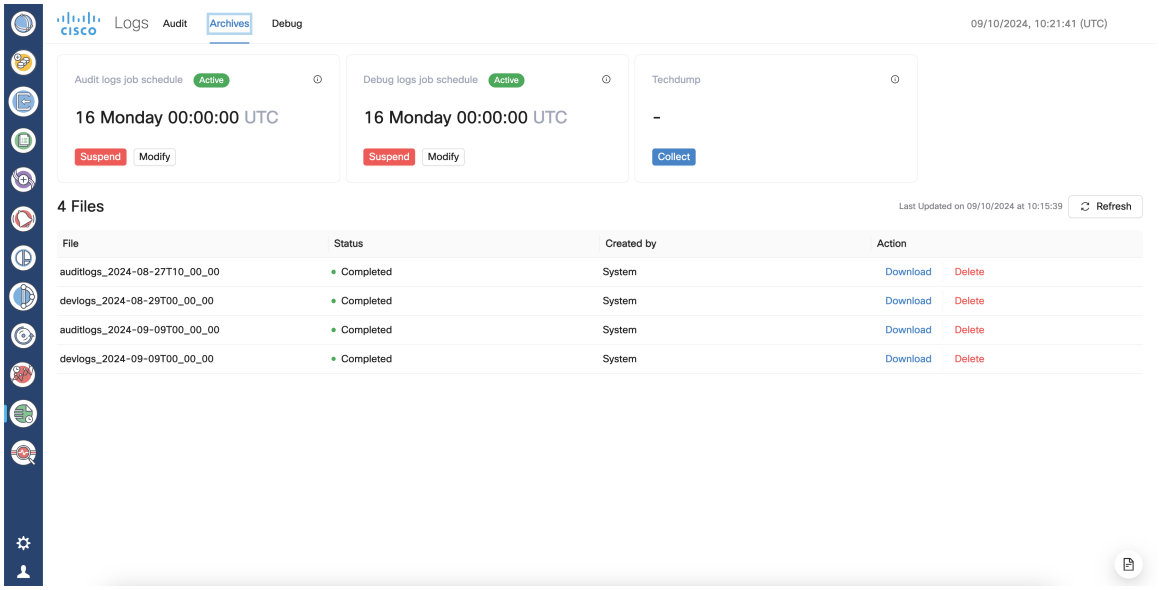


Figure 35: Scheduling Audit Logs Job

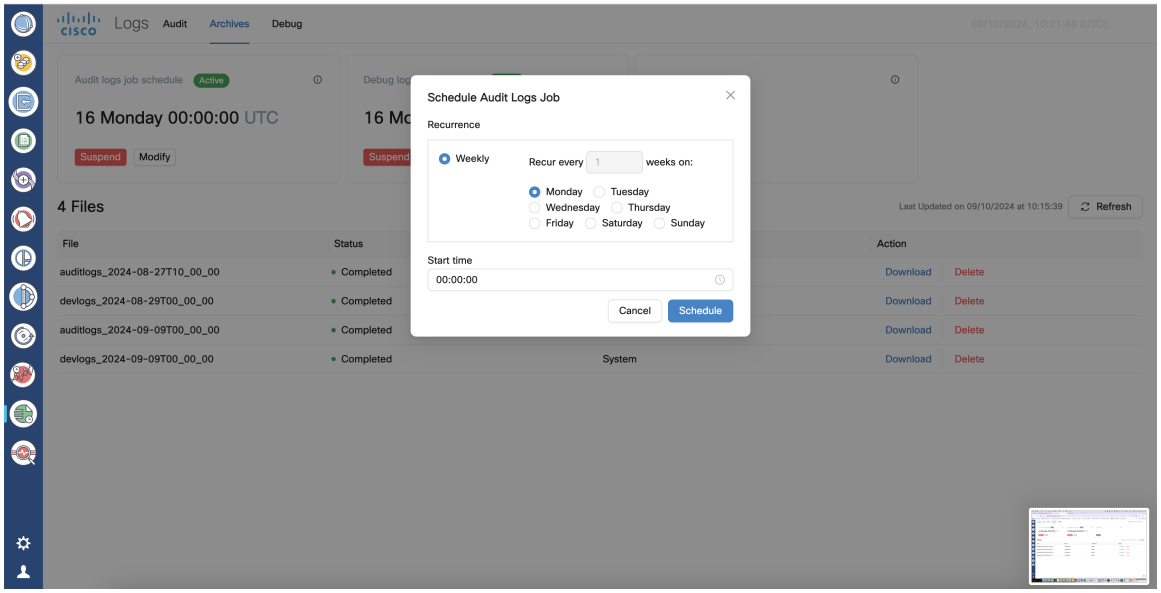
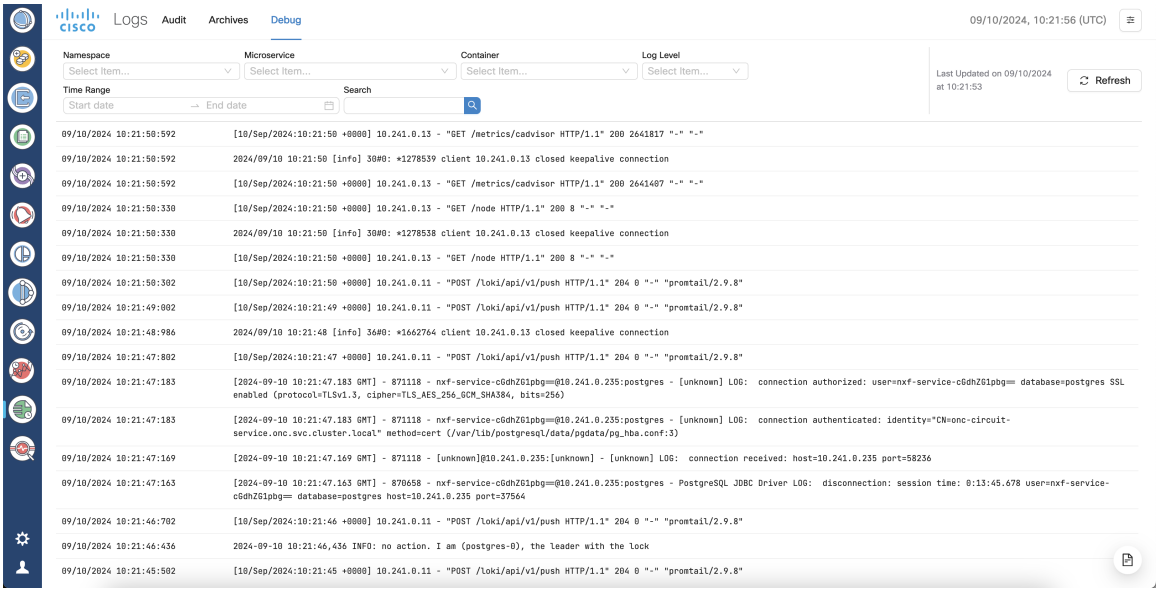


Figure 36: Debug Logs



Benefits of Logs Enhancement

Log enhancements help in:

Table 8: Benefit of Log Enhancements

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

Accessing Logs

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

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

The **Logs** screen is displayed.

Step 2 Click **Audit** tab.

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

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

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

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

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

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

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

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

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

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

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

Acknowledged Alarm Mute

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

Purpose of Acknowledged Alarm Mute

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

Benefits of Using Acknowledged Alarm Mute Option

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

Muting the Acknowledged Alarms

To mute the alarms on the screen:

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

Note

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

Notifications for Acknowledged Alarm Mute

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

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

- Acknowledged alarms are excluded from the **Topology**, **Service Assurance**, **Network Monitoring** and **Circuit Monitoring** applications when the **Mute Acknowledged Alarms** toggle switch is set to **True**.

Note

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

Figure 37: Mute Acknowledged Alarms in Topology

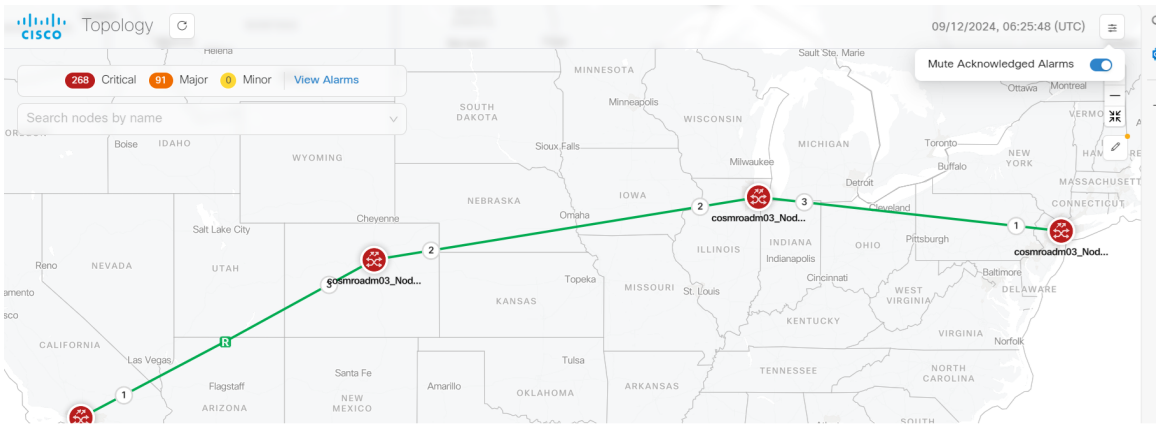
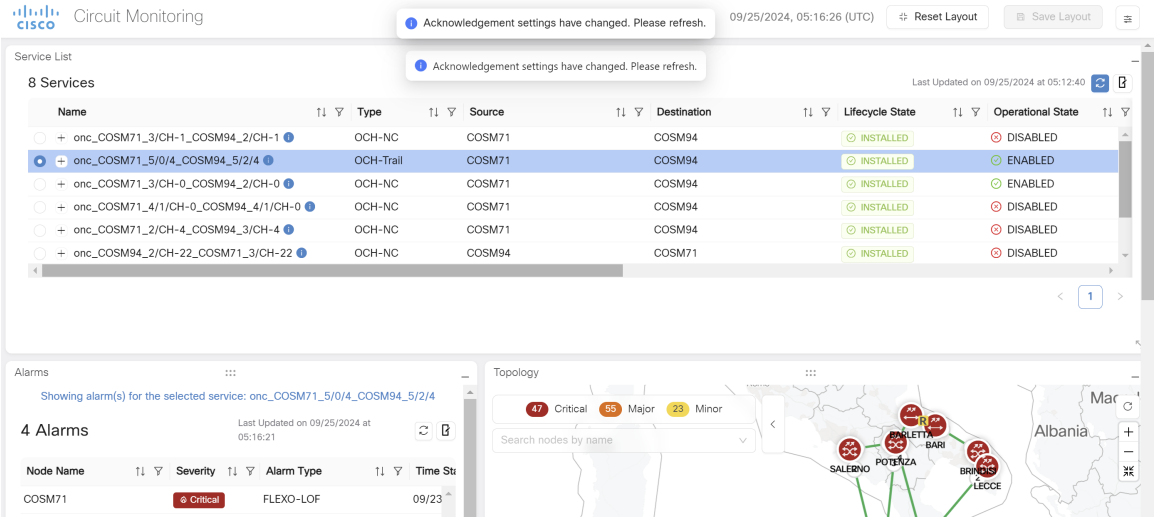


Figure 38: Mute Acknowledged Alarms in Circuit Monitoring



PM History

The Cisco Optical Network Controller 24.3.1 release includes a new application called PM History. The PM history application is made available in **Network Monitoring** workspace and it interacts with **Topology** for links. It is also available in the **Service Monitoring** workspace interacting with the **Detailed Service Path** if circuits are available.

Purpose of Implementing PM History Application

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

Benefits of Using PM History

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

Table 9: 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 10: Time Range for Fetching Data

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

Data Collection and Storage

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

Types of PM History Reports

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

Table 11: Types of PM History Report

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

Type of PM History Report	Description
24-Hour Granularity PM Report	• **Availability**: Real-time reports are accessible for up to 31 days from the time the report is generated. • **Archiving**: Data is archived and accessible for up to 93 days from the time the report was first generated.

Note

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

Figure 39: 15-Minute Granularity PM Report

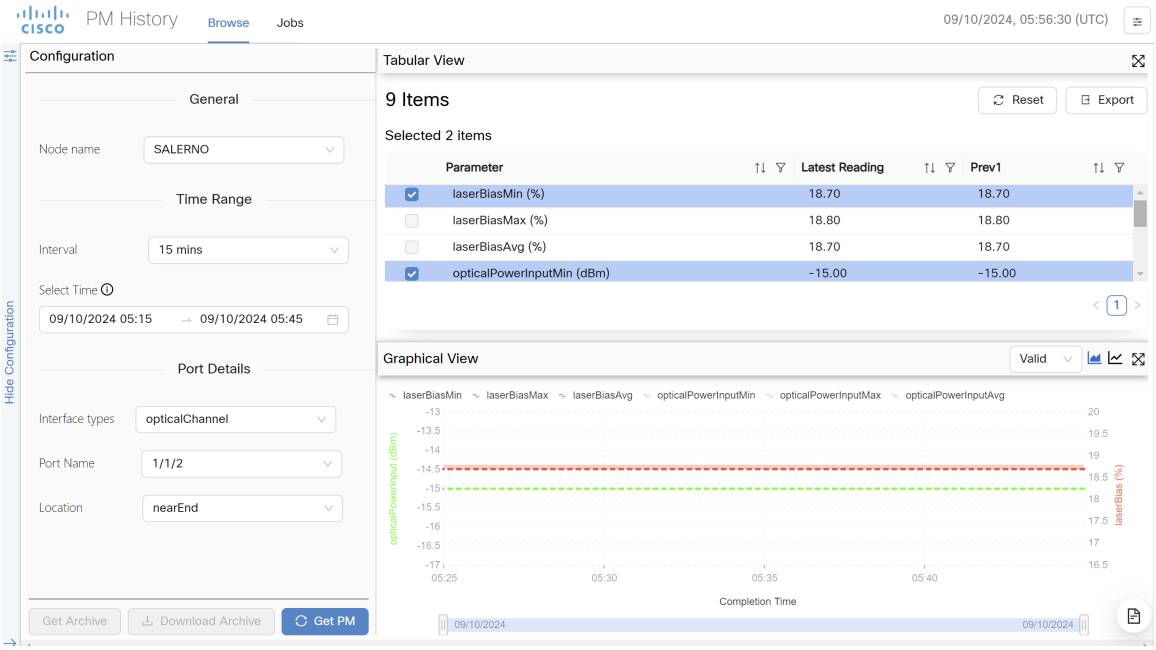
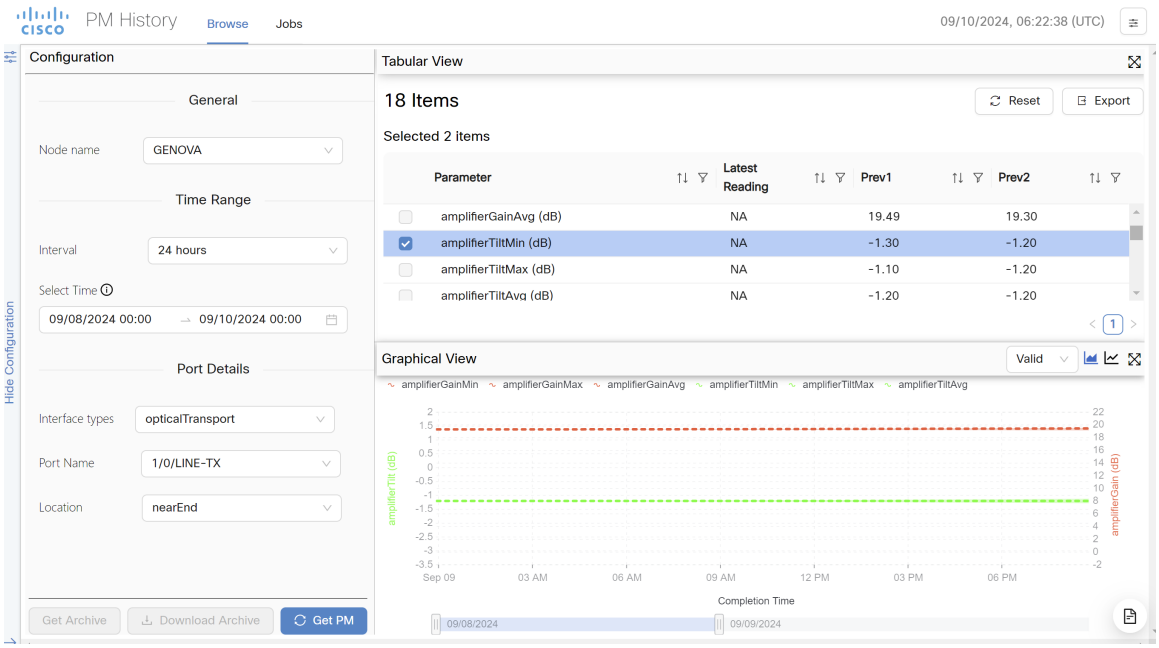


Figure 40: 24-Hour Granularity PM Report



Data Representation

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

PM Job Scheduler

The PM job scheduler manages the PM tasks as given:

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

Note

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

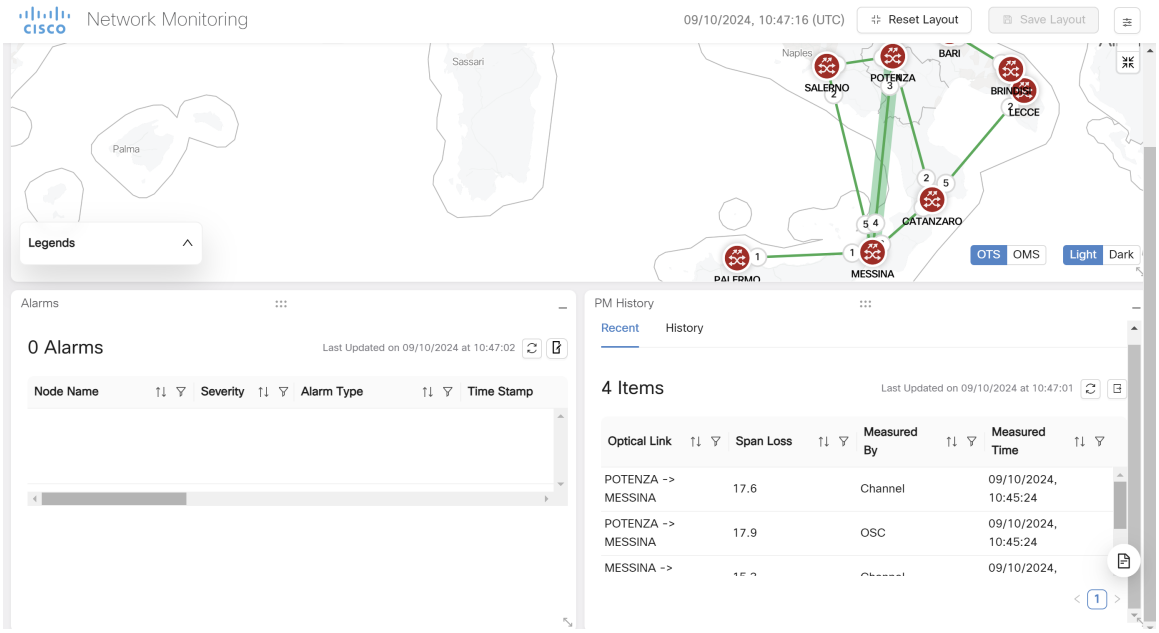
- Reports are sent through email which is configured through SMTP server and which are not password protected.

PM History in Network Monitoring

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

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

Figure 41: PM History in Network Monitoring



PM History in Topology

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

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

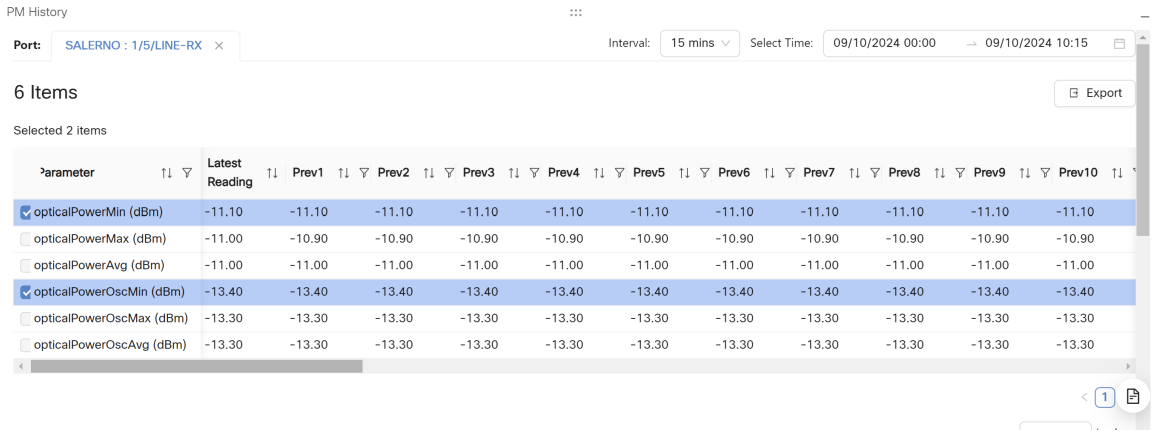
PM History in Circuit Monitoring

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

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

Note Right click on the port on **Detailed Service Path** and use the option to launch PM History for that port. Also you can choose up to two ports.

Figure 42: PM History in Circuit Monitoring



Parameter	Latest Reading	Prev1	Prev2	Prev3	Prev4	Prev5	Prev6	Prev7	Prev8	Prev9	Prev10
opticalPowerMin (dBm)	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10	-11.10
opticalPowerMax (dBm)	-11.00	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90	-10.90
opticalPowerAvg (dBm)	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00	-11.00
opticalPowerOscMin (dBm)	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40	-13.40
opticalPowerOscMax (dBm)	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30
opticalPowerOscAvg (dBm)	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30	-13.30

Service Endpoint PM History Report

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

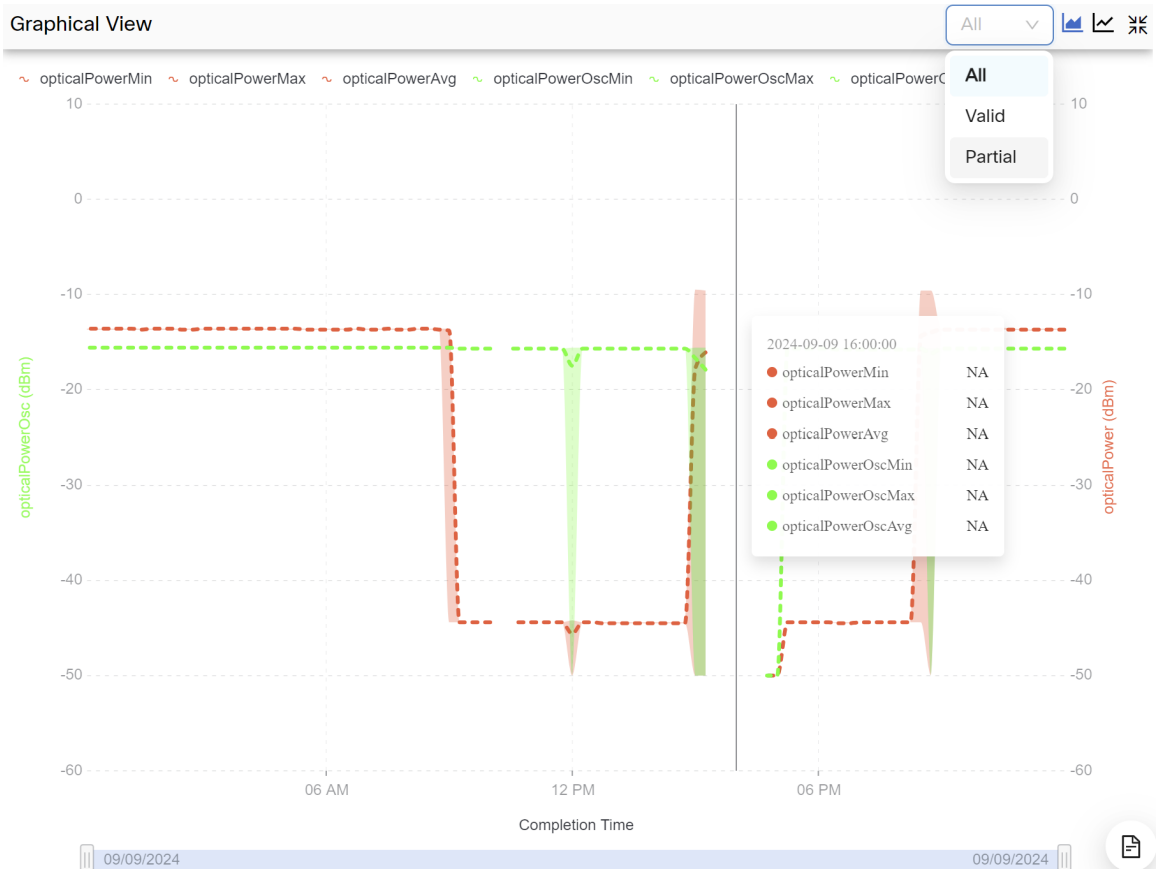
- Calculating and presenting total availability or outage time and percentage.
- Exporting to Excel and scheduling job options if available.

Graphical Representation within PM History Application

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

Note Partial is represented in yellow.

Figure 43: NA Values in Linear Graph



Accessing PM History Report

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

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

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

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

Note

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

Figure 44: PM History Data Collection

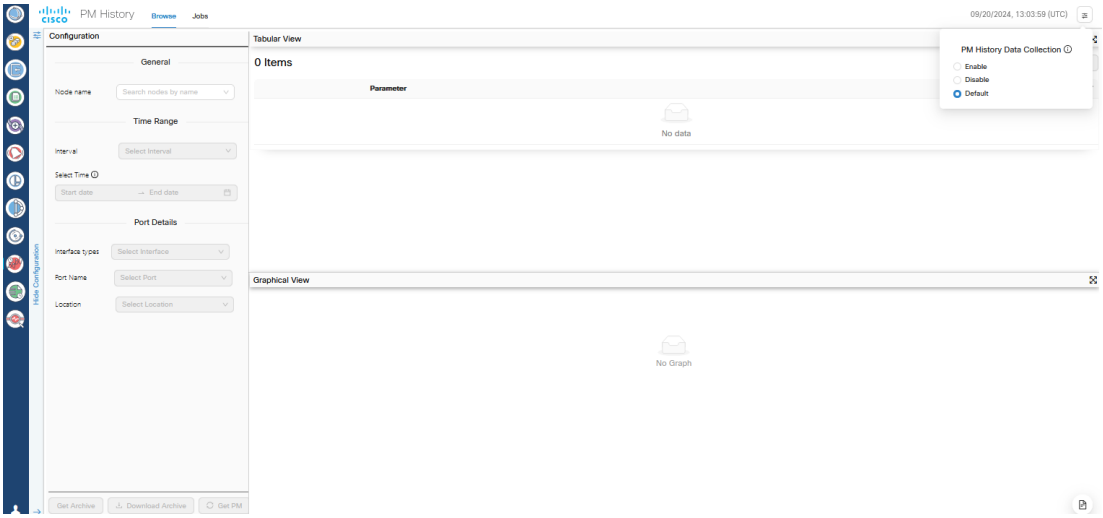
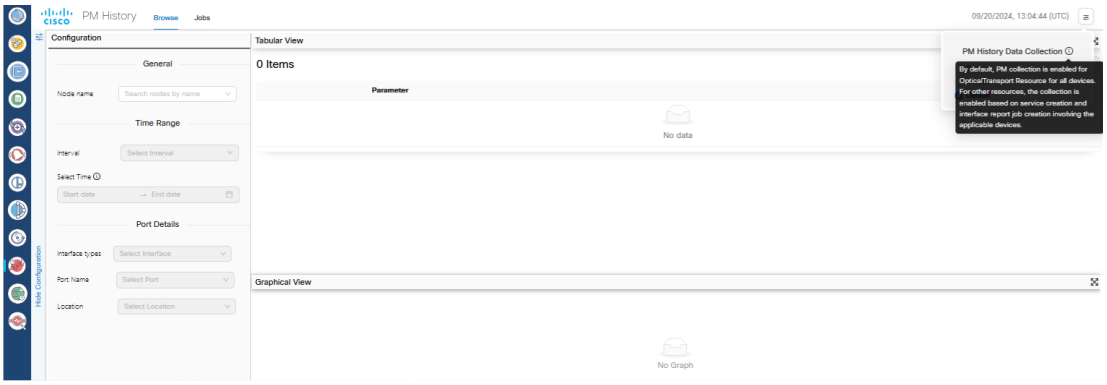


Figure 45: More Information about PM History Data Collection



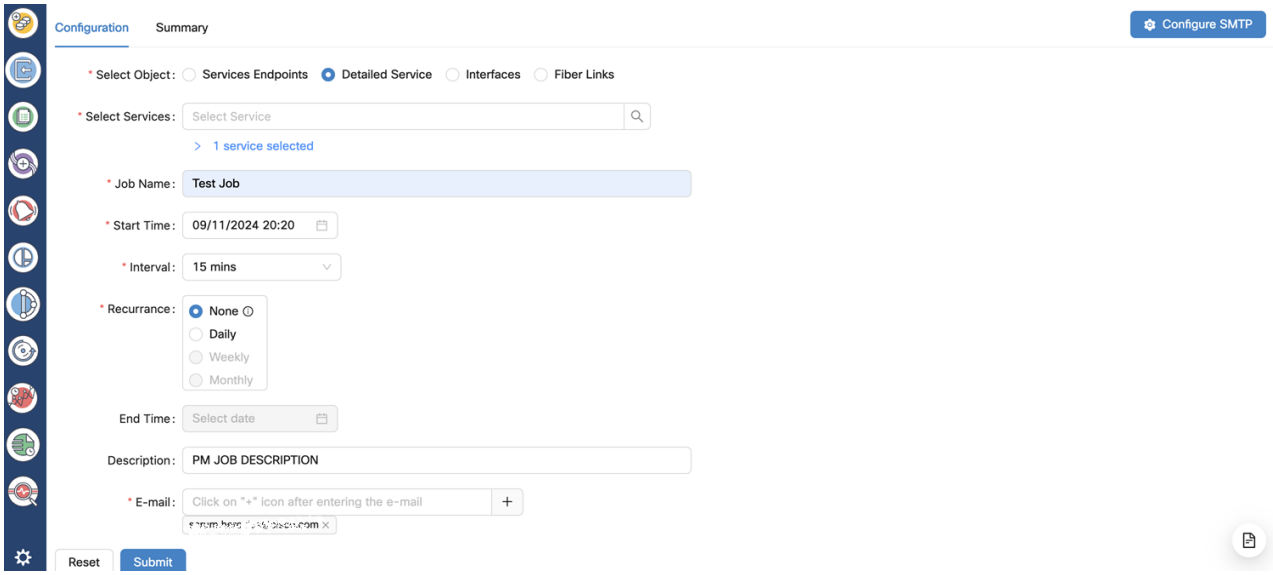
To browse or view the job scheduling details follow the steps given:

a) Click **Jobs** tab.

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

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

Figure 46: Configure SMTP



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

To schedule the jobs follow the steps given:

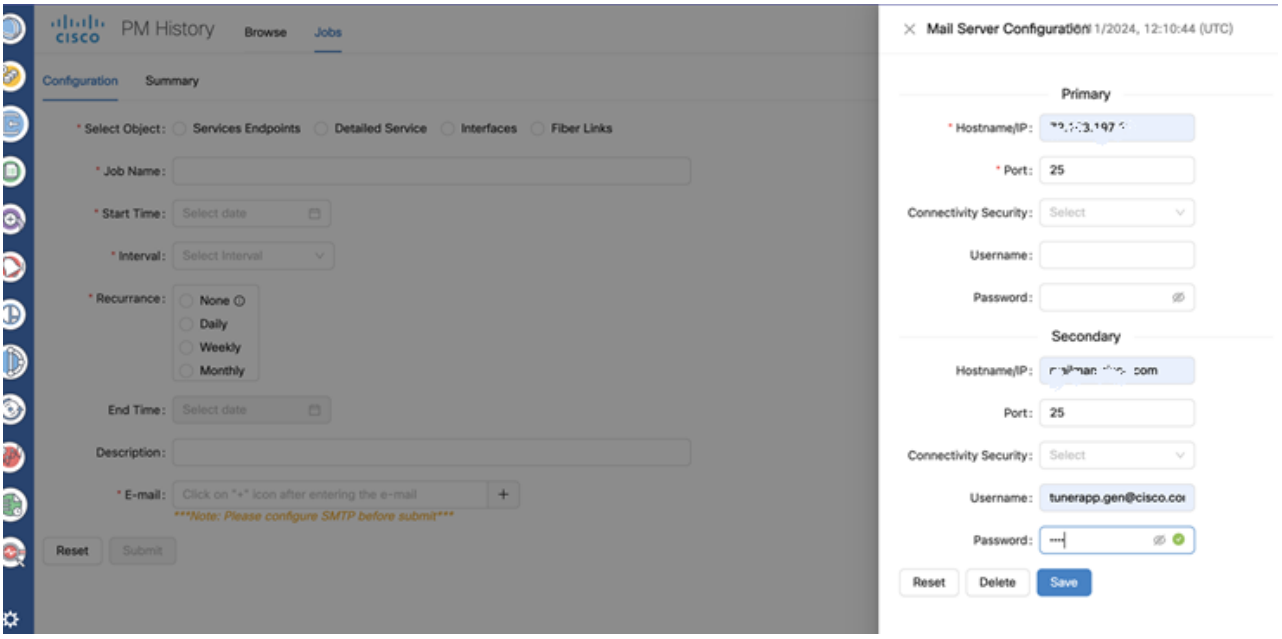
a) Use **Select Object** from **Services Endpoint** for OCH trail circuit or **Detailed Service** for OCH trail or OCHNC circuit or **Interfaces** to select site, equipments, shelves, cards, ports and layers or **Fiber Links**.

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

b) Enter **Job Name**.
c) Enter **Start Time**.
d) Enter **Interval** which can be 15 mins or 24 Hours.
e) Enter **Recurrence** which can be either None, Daily, Weekly or Monthly.
f) Enter **End Time**.
g) Enter **Description**.
h) Enter **E-mail** address.

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

Figure 47: 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.

PSM Fiber Protection

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

Note PSM card is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.

Configuration in PSM Circuits

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

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

Benefits of PSM

The benefits of using PSM are:

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

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

Additional PSM Functions

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

PSM Circuit in Service Manager

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

PSM Circuit in Service Assurance Screen

To view the selected PSM circuit follow the steps:

Step 1 Select the PSM circuit you created from **Services**.

Step 2 Click on the **Detailed Service Path** screen.

This will display the PSM path in the circuit. You can also cross launch to COSM by clicking on the equipments.

Note It is possible to cross launch to the COSM UI on target PSM equipment for running the Protection Switch command present in COSM.

PSM Circuit in Workspace Screen

To view the selected PSM circuit follow the steps:

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

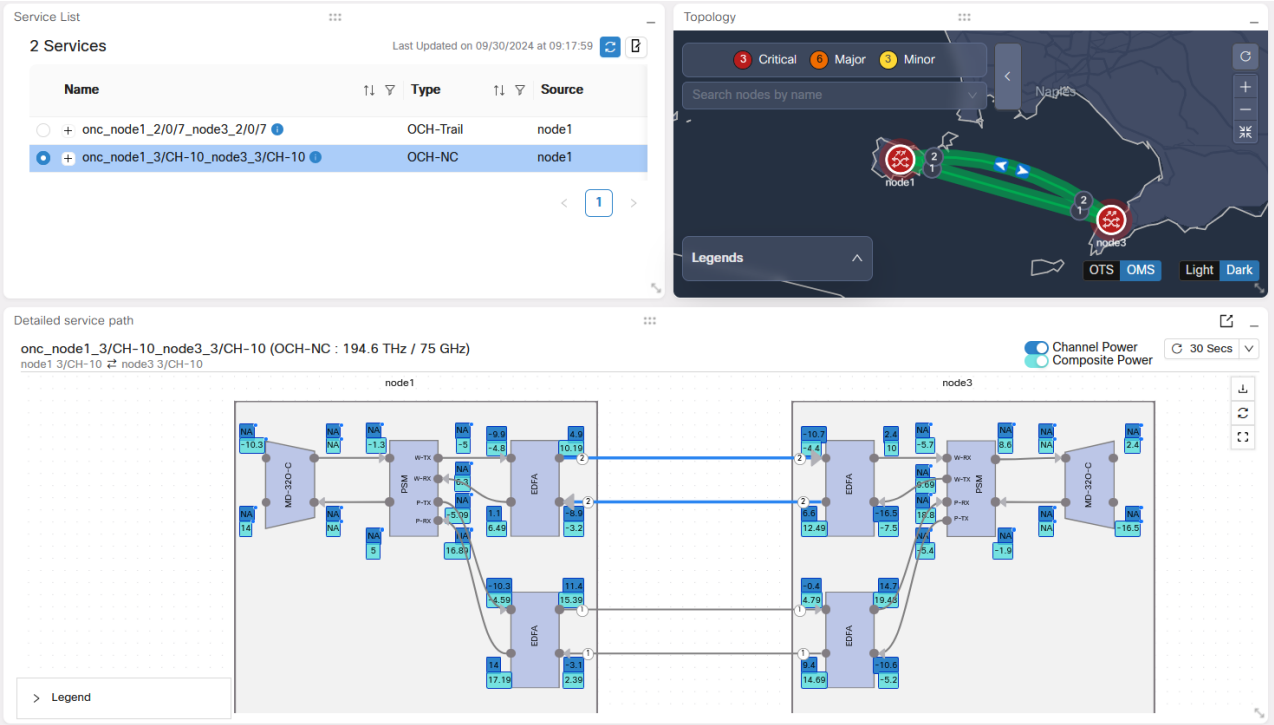
Step 2 Click **Circuit Monitoring**.

Step 3 Select the PSM circuit.

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

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

Figure 48: PSM Circuit in Workspace



Software Image Management and Upgrade

Software Image Management and Upgrade (SWIMU) application manages the software image backups, restores, and upgrades in Cisco Optical Network Controller.

Purpose of Using SWIMU in Cisco Optical Network Controller

To enable support for the Cisco Optical Network Controller software image and node configuration database files storage and distribution. To help in the backup, restoration and upgrade of the software.

Note For 24.3.1 release only the node configuration database backup and restore is supported.

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 COSM 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 managing 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 COSM nodal UI using the cross-launch option in Cisco Optical Network Controller **Nodes** or **SWIM** applications.

Backup Capabilities

Backup capabilities include:

- Creating backup tasks by selecting groups, scheduling, and providing descriptions.
- Scheduling options for hourly, daily, weekly, and monthly configurations.
- Storage of backup files for at least 12 weeks, with user-configurable storage size for external SFTP server.
- Local SFTP server will retain up to five backup files per node.

Note User-configurable storage size is supported, and Cisco Optical Network Controller can initiate file overwriting to prevent disk memory from becoming full.

SFTP Servers

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

- One 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.
- Two external SFTP servers: It is the external SFTP servers that you can configure for Cisco Optical Network Controller DB backup or restore as part of external server storage or upload.

Restore Capabilities

Download backup files to the node from SFTP servers and initiate the restoration process once the download is completed.

- You can initiate file upload from external or internal SFTP server to COSM node(s) through Cisco Optical Network Controller.
- You can cross launch to COSM nodal UI from Cisco Optical Network Controller by clicking on the IP address of the node. You can also use the SWIMU application **Nodes** table, with additional information present in a separate column called **Upload to Node** option for restoration.

Note

- Cisco Optical Network Controller UI job summary table indicates the status of the on-going jobs for success or failure for backup and upload jobs.
- Restoration is applicable outside of Cisco Optical Network Controller, after cross launching to COSM nodal UI.

Types of Backup

There are two types of backup:

Table 12: Backup Types

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

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 Re-occurrence

Table 13: External SFTP Server Storage Formula Parameters

Parameter	Description
Network Total Devices	The number of on-boarded devices.
Size of the Device	The size of an individual device.
Requested Archive Period	The duration upto which the backup files are stored in days
Backup Re-occurrence	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 14: 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.

Configuring SWIMU in Cisco Optical Network Controller

To configure **SWIMU** follow the steps given:

Before you begin

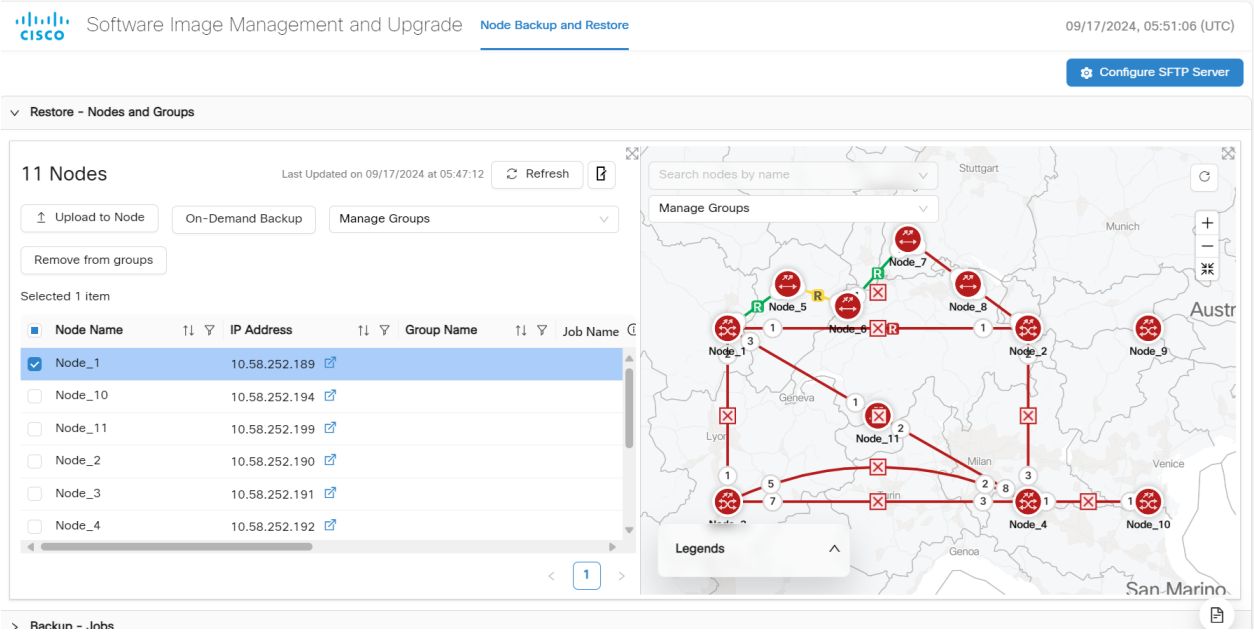
Note

- While configuring external SFTP servers you have to specify the remote path along with other details for the backup to work successfully. When downloading or uploading backup files, the COSM device, which is managed by the Cisco Optical Network Controller, uses the remote path as input. This folder has write permission enabled, allowing the external user to perform the upload.
- Before using the external SFTP server, check if the SFTP server's SSH version is either 7.x or 8.x as otherwise the backup or upload will fail.
- For the backend upload to proceed you must configure the router static settings for each node separately. See *COSM:* **Configure Static Route on Peer Devices** guide for more details on how to configure the static routes of a node.
- Once the SFTP servers are configured the refresh will take a few seconds to complete. This is because the SFTP server checks for memory availability before connecting.
- Also, the Cisco Optical Network Controller VM time must be the same as the device backend time before proceeding with any backup or upload.
- Cisco Optical Network Controller uses the COSM CRON based scheduler to manage and control recurrence of a scheduled backup job.

Step 1 Click **SWIMU** option on the left panel of the Cisco Optical Network Controller screen.

This will display the **Nodes Backup and Restore** screen which has the **Nodes and Groups**, **Topology** and the **Backup Jobs** panels.

Figure 49: SWIMU

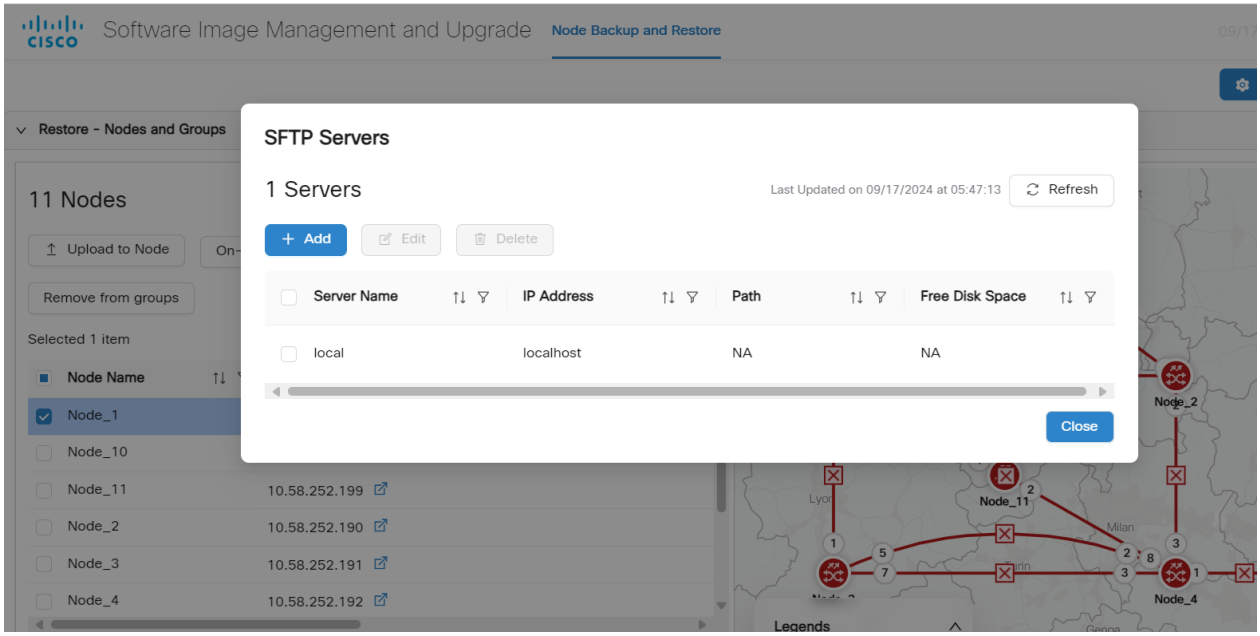


Step 2 Click **Configure SFTP Server** option with the gear icon on the top right corner of the **SWIMU** screen.

This will display the **SFTP Servers** option for configuration. The local SFTP server appears by default and you can configure upto two external SFTP servers.

Note **Check Connectivity Status** is a mandatory step that needs to be followed before you save the SFTP configuration. Only after you have clicked the **Check Connectivity Status** and are able to see the **Connection Successfully Established** you will be able to save the SFTP server details.

Figure 50: Configure SFTP Server

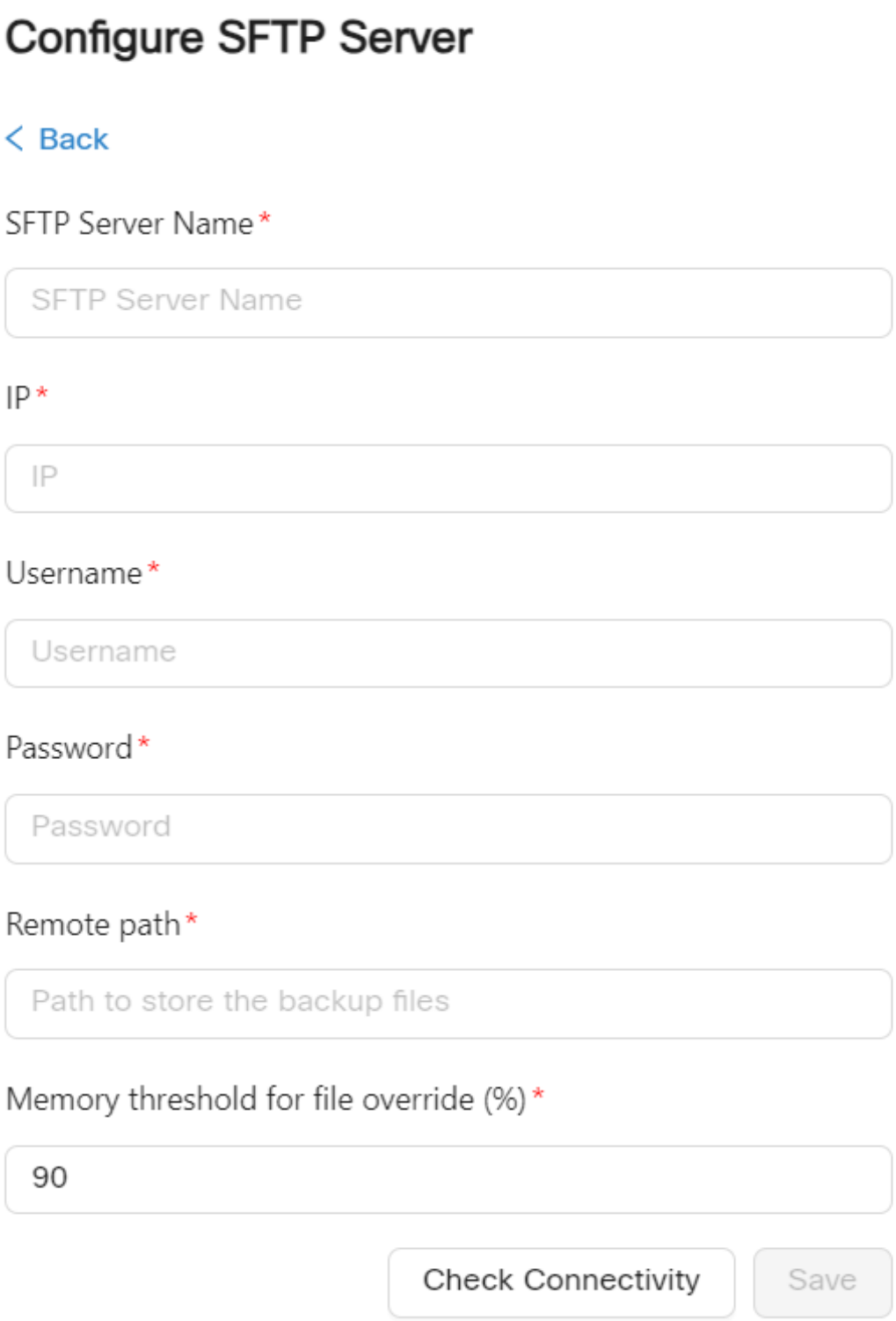


Step 3 Click **Add** to add SFTP servers.

This will display the **Configure SFTP Server** option screen.

a) Enter the **SFTP Server Name**.
b) Enter the **IP** address of the SFTP server.
c) Enter the **Username**.
d) Enter the **Password**.
e) Enter the **Remote path** of the SFTP server.
f) Enter the **Memory threshold for file override (%)** for specifying the percentage of memory threshold allowed for each SFTP server. The minimum threshold value is 50 and anything more than the threshold value will be cleaned up.

Figure 51: Add SFTP Server



Note

- It is recommended to avoid editing or deleting the SFTP server, when an active job is in progress while using the same SFTP server. When you try to edit or delete the SFTP server for an active job then you will receive a notification in the form of pop-up alert message.

  If you want to delete any SFTP server then click **Delete**.

Step 4 Click **Edit** to edit the selected SFTP servers.

Step 5 Click **Refresh** the **SFTP Servers** option screen.

Step 6 Click **Close** to exit from the **SFTP Servers** option screen.

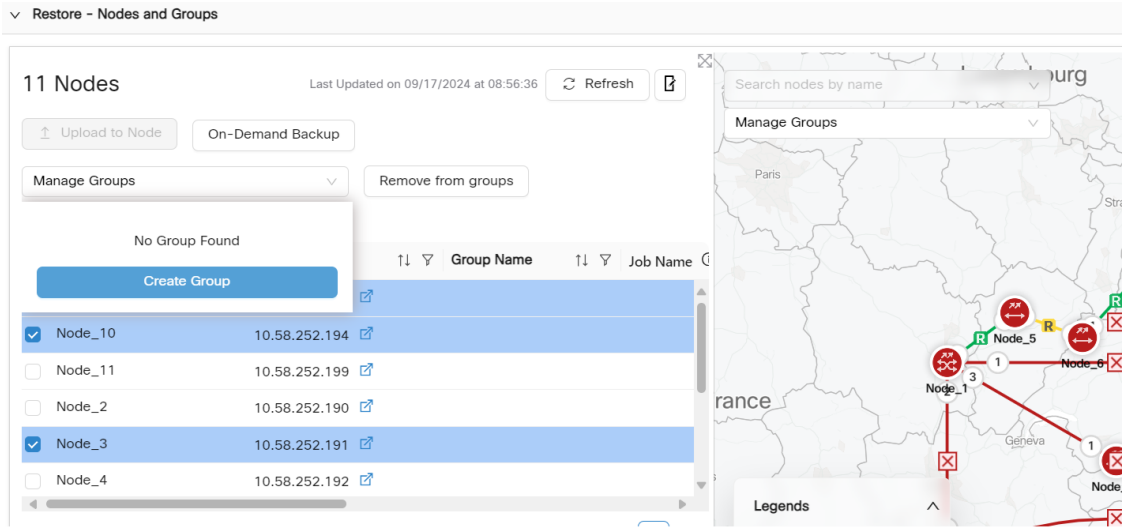
Step 7 To create a nodes group, click **Manage Groups**>**Create Group** option after selecting the nodes from the **Nodes** table, that are going to be added as part of the group.

Step 8 Enter the **Group Name** and **Description** and click **Save**.

Note

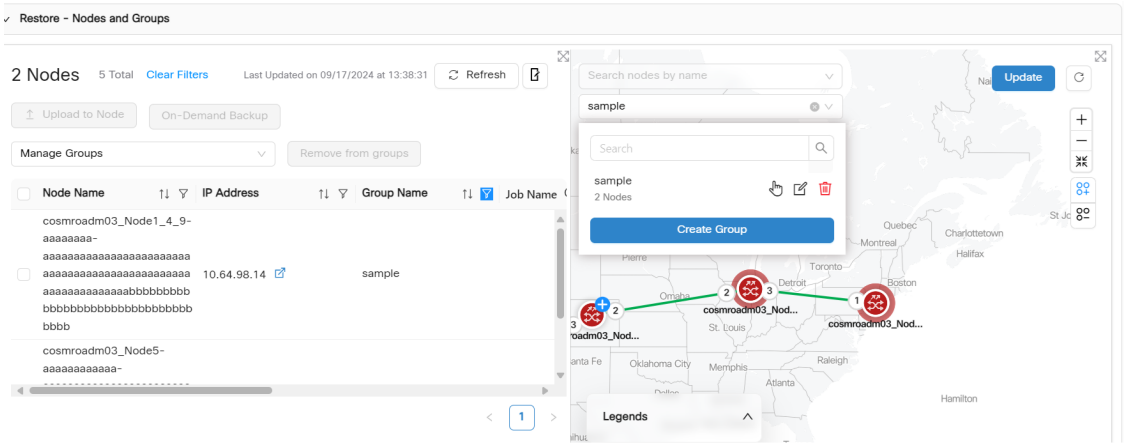
- You can also click and select any node from the **Topology** screen on the right and click the + icon appearing on top of the node and click **Update**. This will add these nodes to the group.

Figure 52: Create Group



- Before scheduling backup jobs, you need to create a node group using the **Manage Groups** option.

Figure 53: Add Nodes Using Topology



Step 9 Click **Restore -Nodes and Groups** screen where you can select the job and use options **Upload to Node** or create **On-Demand Backup** or **Manage Groups** and **Remove from Groups** by clicking each one of them.

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

a) For scheduling the **On-Demand Backup** jobs. Click **On-Demand Backup** after selecting the nodes.

This will schedule the on-demand jobs in the **Backup -Jobs** scheduler.

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

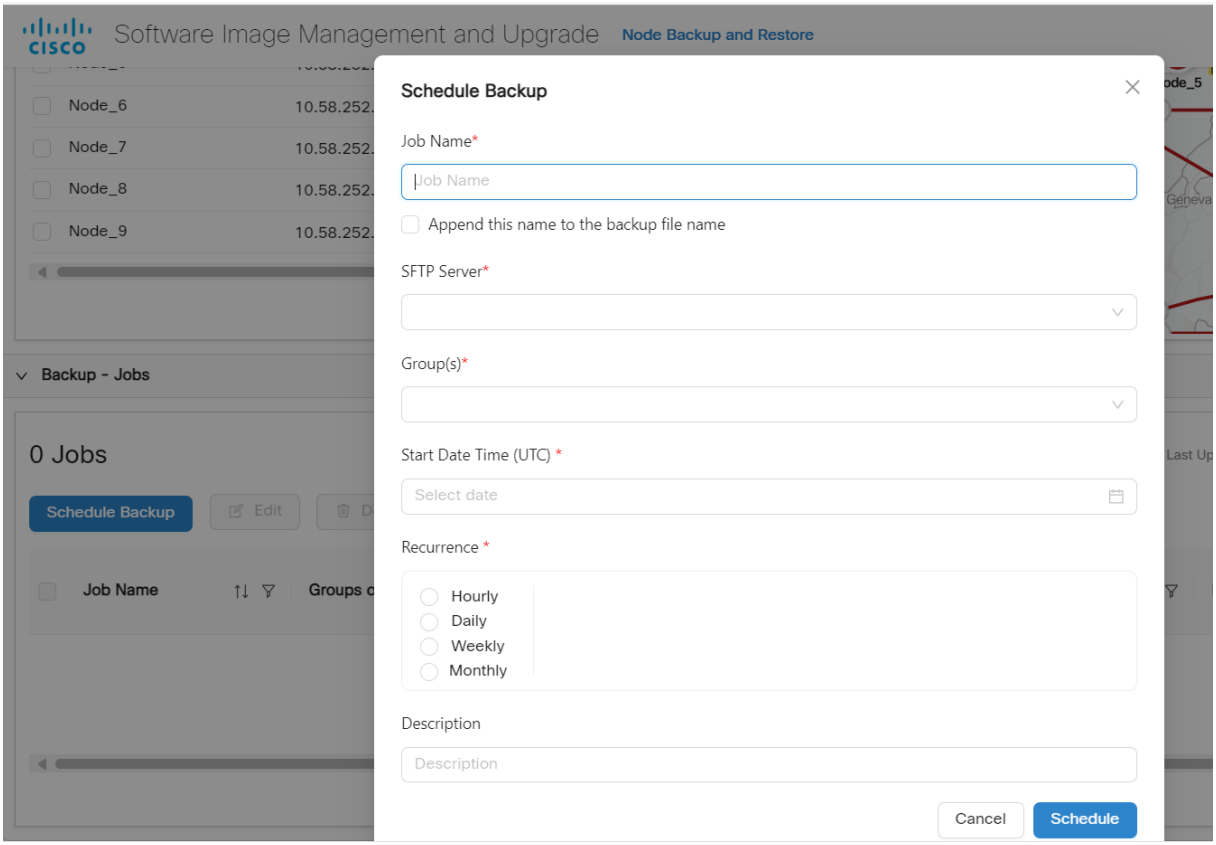
Step 10 Click **Backup -Jobs** to view the job summary and scheduler panel.

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.

Figure 54: Schedule Backup



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**.

Network Level Alarm Correlation

Network Level Alarm Correlation (NLAC) identifies and correlates the root cause alarm with other alarms in a network circuit during a loss of network connection.

Note The node or site level correlation is done by COSM and the network level correlation is done by Cisco Optical Network Controller.

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:

- **Efficient Alarm Management**: Ensures that only the root cause alarm is focused on, reducing the noise from multiple alarms.
- **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**:
  - **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.

Note In the bidirectional scenario, we will 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.

NLAC LOC and LOS-P Alarms

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

Figure 55: LOS and LOS-P Correlation

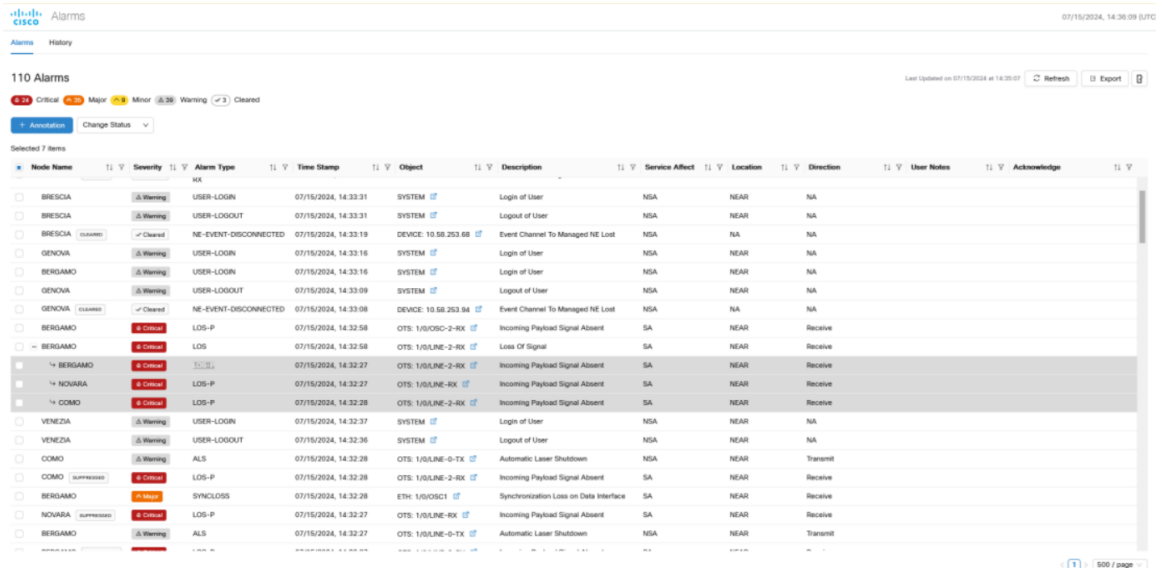
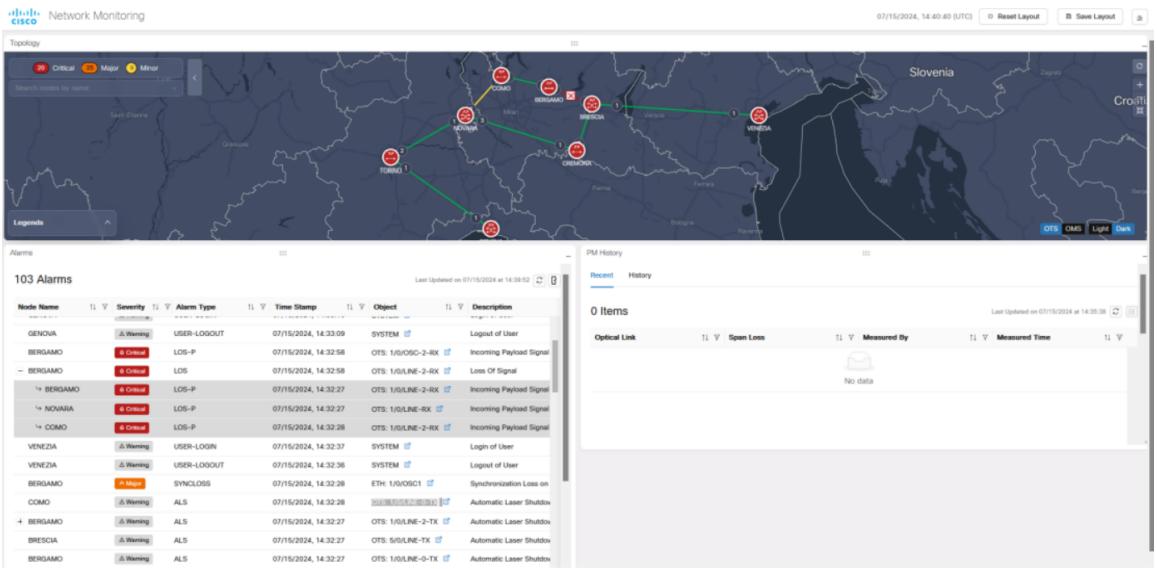


Figure 56: LOS and LOS-P Correlation in Network Monitoring



Note

- Alarms that are suppressed display a suppressed tag in the alarms panel till you refresh.
- 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 LOS-P does not consider LOs-P as its highest severity

Forwarding Syslogs

The syslog forwarding feature help in:

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

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

Installing Syslog on Server

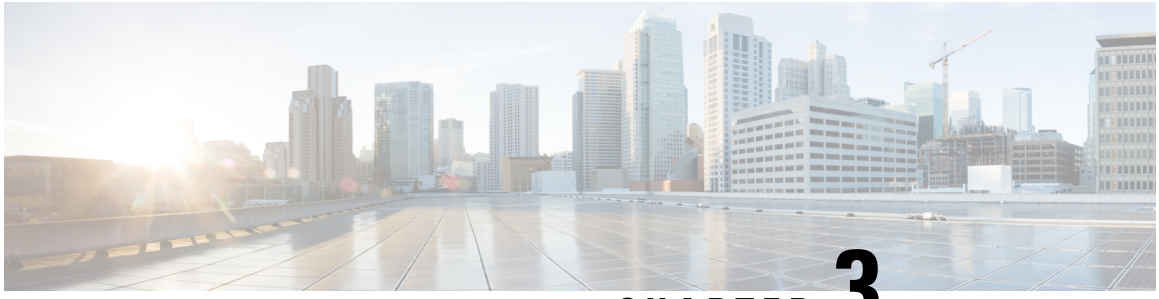
To install syslog feature on the server run the CLI commands given in the example:

```
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
```

Installing Syslog on Client

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

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

To create a syslog query to forward the apllication logs of a particular ONC app:
 sedo syslog query create '{namespace="onc", app="<app_name>", container="app"}' LOG_INFO
LOG_USER <app_name> <IP>

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

To list all syslog queries:
 sedo syslog query list

To list all syslog servers:
 sedo syslog server list

To delete a syslog query:
 sedo syslog query delete <QUERY_ID>

To delete a syslog server:
 sedo syslog server delete <IP>
```



CHAPTER 3

Alarm Troubleshooting

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

- Troubleshooting Guide for Cisco NCS 1014
- Troubleshooting Guide for Cisco NCS 1010
- Troubleshooting Guide for Cisco NCS 1004