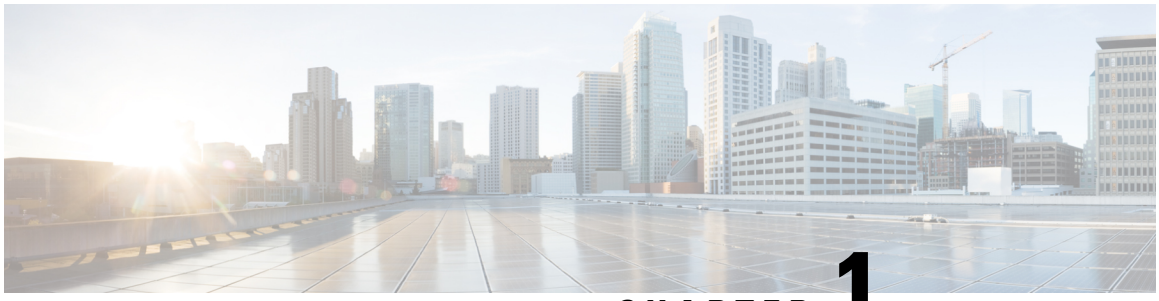
# Cisco Optical Automation Solution Workflow, IOS XR Release 26.1.1

**First Published:** 2026-07-01

**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

# Deploy the Cisco Optical Automation Solution in Seven Steps

### Optical Automation Solution

An Optical Automation Solution (OAS) provides a unified approach for planning, deploying, and operating optical networks while keeping design intent consistent across tools and teams. It connects the planning, installation, and controller stages to ensure that data, configurations, and validations remain aligned from day-0 through day-2 operations. OAS also standardizes prerequisites and access controls to reduce deployment variance across sites.

The solution offers several key functions.

- It streamlines deployment and lifecycle management of optical networks through repeatable workflows.
- It enables collaboration among planners, site engineers, and automation administrators with shared artifacts and checkpoints.
- It integrates Cisco Optical Network Planner, Cisco Optical Site Manager, and Cisco Optical Network Controller for end-to-end orchestration.
- It preserves configuration intent from initial design through service provisioning and operational assurance.

### Key components and roles in OAS

OAS relies on a structured approach involving specific Cisco platforms and dedicated roles to achieve end-to-end automation:

This table lists the primary solution components for the OAS workflow and describes the function of each.

***Table 1: Components***

| Component | Description |
|---|---|
| Cisco Optical Network Planner | Design and validate networks for the NCS 1000 series platforms. |
| NCS 1010, NCS 1014, NCS 1004 | Provide hardware platforms for optical transport and connectivity within the solution. |
| Cisco Optical Site Manager | Serves as the software platform for site configuration import, management, and automation tasks. |

| Component | Description |
|---|---|
| Cisco Optical Network Controller | Delivers centralized control and monitoring across the optical network infrastructure. |

This table outlines the primary roles and the responsibilities required to maintain alignment from planning through operations.

***Table 2: Roles***

| Role | Responsibilities |
|---|---|
| Planner | Maintains topology fidelity in Cisco Optical Network Planner, aligns fiber parameters, and generates Cisco Optical Site Manager Netconf XML exports. |
| Site engineer | Handles the physical installation and powering of Cisco hardware, confirms day-0 configurations, and reports site readiness. |
| Automation administrator | Operates Cisco Optical Site Manager and Cisco Optical Network Controller, manages authentication, imports configurations, and validates telemetry data. |

### Interconnected stages

The fundamental principle of OAS is to ensure that the configuration intent defined during the planning phase is accurately translated, applied, and monitored across the entire optical network infrastructure.

The deployment of an Optical Automation Solution typically involves these stages:

| Stage | Focus |
|---|---|
| Model preparation | Validate the network design in Cisco Optical Network Planner by confirming the site inventory, fiber types, connector loss values, and service cards. Resolve any design errors. Capture reports, including the bill of materials, layout, NFV, and cabling details. Generate the site configuration in Netconf XML format for consumption by Cisco Optical Site Manager. |
| Hardware installation | Deploy optical platforms (NCS 1010, NCS 1014, NCS 1004), rack equipment, install components, connect power, boot devices, configure root credentials and management addresses, and verify interface status. |
| Cabling validation | Verify that all fiber and cabling work are completed accurately, according to the planned design standards. |
| Cisco Optical Site Manager activation | Install and configure Cisco Optical Site Manager, including TACACS, authentication groups, and smart licensing. Import Netconf XML bundles, synchronize devices, and push ANS parameters. |
| Cisco Optical Network Controller onboarding | Install Cisco Optical Network Controller, set up users, import Cisco Optical Site Manager nodes, and verify topology, alarms, performance monitoring, and circuits. |

### Advantages of OAS

Implementing an Optical Automation Solution offers significant advantages:

- **Repeatable and Consistent Deployments:** Provides a standardized, evidence-backed playbook for deploying optical networks, reducing errors and increasing efficiency.

- **Enhanced Planning and Design:** Facilitates continuous planning by enabling the re-import of live topology data into Cisco Optical Network Planner and supporting proactive upgrade analyses for new network configurations.
- **Operational Assurance:** Ensures reliable service provisioning with comprehensive assurance capabilities and continuous monitoring within Cisco Optical Network Controller.
- **Streamlined Workflow:** Integrates various tools and roles into a cohesive workflow, from initial design to active network management.

- Optical Automation Solution, on page 3
- Deploy the Optical Automation Solution in seven steps, on page 5

# Optical Automation Solution

An Optical Automation Solution (OAS) provides a unified approach for planning, deploying, and operating optical networks while keeping design intent consistent across tools and teams. It connects the planning, installation, and controller stages to ensure that data, configurations, and validations remain aligned from day-0 through day-2 operations. OAS also standardizes prerequisites and access controls to reduce deployment variance across sites.

The solution offers several key functions.

- It streamlines deployment and lifecycle management of optical networks through repeatable workflows.
- It enables collaboration among planners, site engineers, and automation administrators with shared artifacts and checkpoints.
- It integrates Cisco Optical Network Planner, Cisco Optical Site Manager, and Cisco Optical Network Controller for end-to-end orchestration.
- It preserves configuration intent from initial design through service provisioning and operational assurance.

### Key components and roles in OAS

OAS relies on a structured approach involving specific Cisco platforms and dedicated roles to achieve end-to-end automation:

This table lists the primary solution components for the OAS workflow and describes the function of each.

***Table 3: Components***

| Component | Description |
|---|---|
| Cisco Optical Network Planner | Design and validate networks for the NCS 1000 series platforms. |
| NCS 1010, NCS 1014, NCS 1004 | Provide hardware platforms for optical transport and connectivity within the solution. |
| Cisco Optical Site Manager | Serves as the software platform for site configuration import, management, and automation tasks. |
| Cisco Optical Network Controller | Delivers centralized control and monitoring across the optical network infrastructure. |

This table outlines the primary roles and the responsibilities required to maintain alignment from planning through operations.

***Table 4: Roles***

| Role | Responsibilities |
|---|---|
| Planner | Maintains topology fidelity in Cisco Optical Network Planner, aligns fiber parameters, and generates Cisco Optical Site Manager Netconf XML exports. |
| Site engineer | Handles the physical installation and powering of Cisco hardware, confirms day-0 configurations, and reports site readiness. |
| Automation administrator | Operates Cisco Optical Site Manager and Cisco Optical Network Controller, manages authentication, imports configurations, and validates telemetry data. |

### Interconnected stages

The fundamental principle of OAS is to ensure that the configuration intent defined during the planning phase is accurately translated, applied, and monitored across the entire optical network infrastructure.

The deployment of an Optical Automation Solution typically involves these stages:

| Stage | Focus |
|---|---|
| Model preparation | Validate the network design in Cisco Optical Network Planner by confirming the site inventory, fiber types, connector loss values, and service cards. Resolve any design errors. Capture reports, including the bill of materials, layout, NFV, and cabling details. Generate the site configuration in Netconf XML format for consumption by Cisco Optical Site Manager. |
| Hardware installation | Deploy optical platforms (NCS 1010, NCS 1014, NCS 1004), rack equipment, install components, connect power, boot devices, configure root credentials and management addresses, and verify interface status. |
| Cabling validation | Verify that all fiber and cabling work are completed accurately, according to the planned design standards. |
| Cisco Optical Site Manager activation | Install and configure Cisco Optical Site Manager, including TACACS, authentication groups, and smart licensing. Import Netconf XML bundles, synchronize devices, and push ANS parameters. |
| Cisco Optical Network Controller onboarding | Install Cisco Optical Network Controller, set up users, import Cisco Optical Site Manager nodes, and verify topology, alarms, performance monitoring, and circuits. |

### Advantages of OAS

Implementing an Optical Automation Solution offers significant advantages:

- **Repeatable and Consistent Deployments:** Provides a standardized, evidence-backed playbook for deploying optical networks, reducing errors and increasing efficiency.
- **Enhanced Planning and Design:** Facilitates continuous planning by enabling the re-import of live topology data into Cisco Optical Network Planner and supporting proactive upgrade analyses for new network configurations.

- **Operational Assurance:** Ensures reliable service provisioning with comprehensive assurance capabilities and continuous monitoring within Cisco Optical Network Controller.
- **Streamlined Workflow:** Integrates various tools and roles into a cohesive workflow, from initial design to active network management.

# Deploy the Optical Automation Solution in seven steps

Use this task to move a planned optical network from design to an operational state with continuous planning enabled.

The OAS deployment workflow coordinates Cisco Optical Network Planner, Cisco Optical Site Manager, and Cisco Optical Network Controller for design, configuration, onboarding, and circuit provisioning.

**Before you begin**

- Confirm access to Cisco Optical Network Planner and Cisco Optical Network Controller, and ensure devices are installed and cabled at the site.

  Ensue that day-0 parameters are available, including IP address assignments, DCN plans, and access to servers such as NTP, TACACS, and Smart Licensing for software downloads.

Follow these steps to deploy the Optical Automation Solution.

**Procedure**

**Step 1** Plan and design the network in Cisco Optical Network Planner.

Define topology and circuit requirements, then generate planning reports including the Cisco Optical Site Manager configuration file.

For details, see Design the topology in Cisco Optical Network Planner and Generate Cisco Optical Site Manager Netconf XML Files.

Design artifacts are ready for device initialization.

**Step 2** Perform device turn-up (Day-0) at the site.

Power on devices and initialize Day-0 parameters such as IP address assignments, DCN plans, and access to servers such as NTP, TACACS, and Smart Licensing for software downloads.

For day-0 procedures, see Configure NCS 1010 day-0 settings.

Devices are powered on and visible in Cisco Optical Site Manager.

**Step 3** Apply Day-1 configuration and validate in Cisco Optical Site Manager.

Push the Day-1 configuration generated by Cisco Optical Network Planner to devices via Cisco Optical Site Manager and validate the configuration on all devices.

For details, see Import a Cisco Optical Network Planner configuration file, on page 65 and Synchronize devices in Cisco Optical Site Manager.

Devices are validated and ready for onboarding.

**Step 4** Onboard nodes to Cisco Optical Network Controller.

Add validated nodes to Cisco Optical Network Controller and confirm they appear in inventory.

For details, see Onboard Cisco Optical Site Manager nodes in Cisco Optical Network Controller.

Nodes are managed by Cisco Optical Network Controller.

**Step 5** Provision circuits in Cisco Optical Network Controller based on the Cisco Optical Network Planner plan.

Review planned paths in Cisco Optical Network Planner and provision circuits in Cisco Optical Network Controller according to the planned design.

For details, see Provision CPCE services.

Circuits are provisioned according to the approved plan.

**Step 6** Monitor the live network and synchronize data with Cisco Optical Network Planner.

Use Cisco Optical Network Controller to monitor network status and import live network details into Cisco Optical Network Planner with one click.

For details, see Perform live network import, on page 103.

Planning data reflects the live network state.

**Step 7** Perform continuous planning and upgrades.

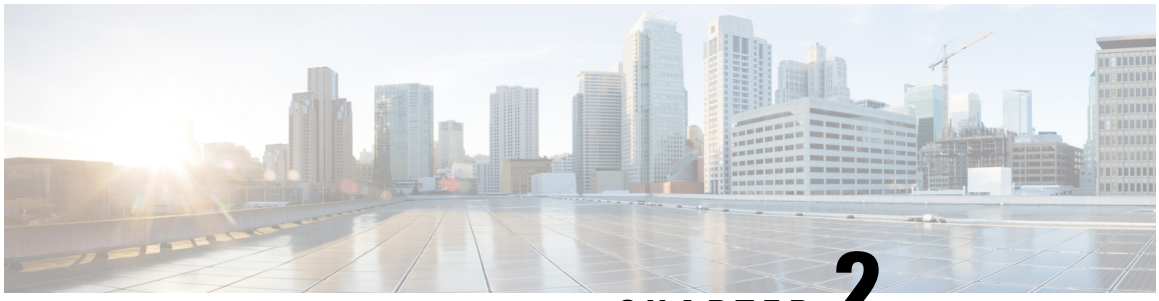
Use live network information in Cisco Optical Network Planner, generate new ANS parameters after upgrade analysis, and push updates via Cisco Optical Site Manager.

For details, see Analyze the network.

The network evolves through continuous planning and upgrades.

---

OAS deployment is complete and the network enters a continuous planning loop supported by Cisco Optical Network Planner, Cisco Optical Site Manager, and Cisco Optical Network Controller.



CHAPTER 2

# Plan Your Network with Cisco Optical Network Planner

This chapter provides an overview of Cisco Optical Network Planner and its primary functions for optical network design and validation.

Cisco ONP enables users to model and test Optical Transport Network (OTN) and Dense Wavelength Division Multiplexing (DWDM) optical networks in a graphical environment.

- Cisco ONP is used to design and validate networks for the NCS 1000 and NCS 2000 series platforms.
- The tool generates the Bill of Materials (BoM) based on the modeled network.
- Cisco ONP provides detailed network information, including rack views, cabling reports, optical reports, traffic matrices, and optical setup files used for bringing up the COSM network.



# Cisco Optical Network Planner prerequisites and user management

Understand the minimum system requirements and administrative considerations required before deploying Cisco Optical Network Planner.

This table describes the prerequisites and recommended configurations that are essential for Cisco Optical Network Planner installation and operation:

*Table 5: Cisco Optical Network Planner prerequisites*

| Item | Description |
|---|---|
| Installation | Install Cisco Optical Network Planner in the customer environment. For more details, see:<br>• Cisco Optical Network Planner Installation Guide for detailed installation steps.<br>• To install a Cisco Optical Network Planner SMU package, see Install the SMU.<br>• See Troubleshoot for troubleshooting common Cisco Optical Network Planner issues. |
| System requirements | • **Operating system:** Ubuntu Server 22.04 or 24.04, or Red Hat Enterprise Linux 8.8 or 8.10<br>• **CPU:** 8 cores<br>• **Memory:** 96 GB RAM<br>• **Storage:** 500 GB free disk space after installation<br>• **Capacity:** Supports 10 concurrent parallel Cisco Optical Network Planner analyses |
| Download and licensing | Cisco Optical Network Planner can be downloaded from CCO with a valid license agreement. Contact the account team for download issues. |
| First-time login | After installing Cisco Optical Network Planner, log in as admin and change the default password during the first-time Cisco Optical Network Planner login. |
| User access | Users must register in Cisco Optical Network Planner, and an administrator must authorize their accounts before GUI access. |
| Planning inputs | Have topology details available, including site or device details, fiber parameters, and circuit details. |

Users with administrator privileges can:

- Approve new users by assigning a role to a user group.
- Receive email notifications when new users register.
- For more details, see Assign a role to a user group.

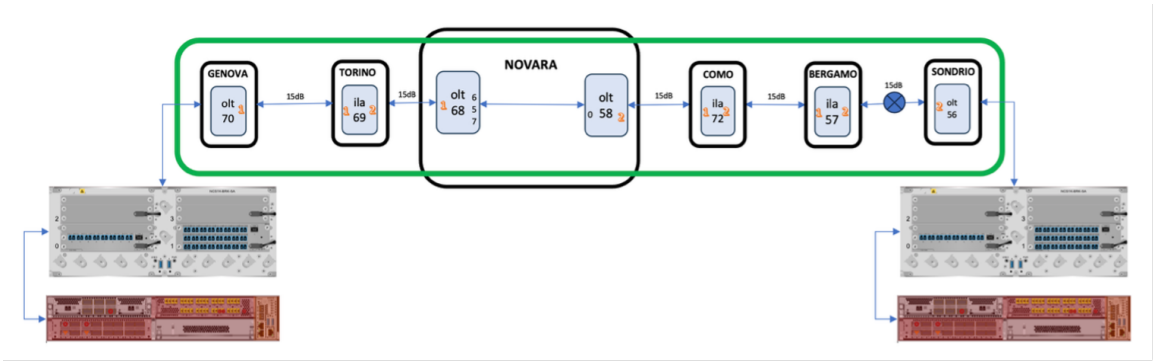
# Plan your NCS1010 Network

Plan an NCS 1010-based network using Cisco Optical Network Planner to design a topology with the required specifications, analyze it, and generate planning data. For detailed instructions, see Design and Analyze Networks.

This reference network topology described here illustrates these NCS 1010 bring-up scenarios.

- It is a two-degree topology that uses seven NCS 1010 nodes.
- The BRK-8 modules are used to create express interconnect in Site-Novara using MPO cables.

***Figure 1: Multi-degree Topology***




# Design the topology in Cisco Optical Network Planner

Use this procedure to create a Cisco Optical Network Planner model that matches the physical design for a new region or pilot network.

The output is a topology file that you can use for Cisco Optical Site Manager exports and downstream bill of materials validation.

The sample node names (Genova, Novara, Sondrio, Torino, Como, Bergamo) correspond to the reference network and should be adapted as necessary.

Consider these inputs before you create the network plan. Apply them according to your network design requirements.

- Create the number of circuits based on the channel plan and use the appropriate card type for each circuit.
- Force the add/drop type according to the design requirements. For details about add/drop configuration, see Modify Network Properties.

**Before you begin**

- Confirm licensing for Cisco Optical Network Planner and verify that your account can create and save projects.
- Gather topology notes: number of ROADM and OLA sites, fiber lengths, and circuit/service requirements.
- Clarify whether the design needs colored or colorless add/drop behavior per site.

Follow these steps to design the topology.

## Procedure

**Step 1** Create the base network in Cisco Optical Network Planner.

a) Log in to the Cisco Optical Network Planner home page with a valid user.

b) Choose **File**, then click **New**.
c) In **Create New Network** dialog box, set **L0 Network Platform** to **NCS 1010** and **Band Type** to **C-Band**.

You can set the system release values as follows:

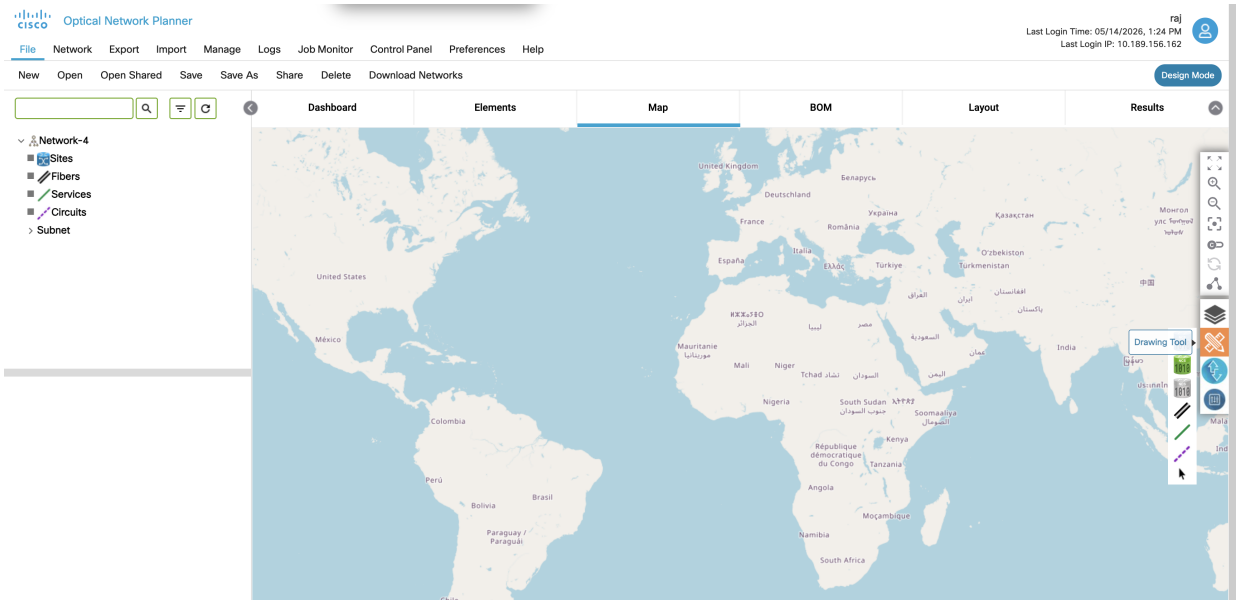
| Platform | System Release |
|---|---|
| NCS 1010 | 26.1.1 |
| NCS 1014 | 26.1.1 |
| NCS 1004 | 25.4.1 |

Name the network consistently with your deployment tracker (for example, REGION_TOPOLOGY_MMDD).

A new, empty network canvas opens with the drawing tool enabled.

**Step 2** Follow these steps to add sites, fibers, circuits, and services with the drawing tool.

a) Click the **Drawing Tool** icon (pencil and ruler).




b) Add ROADM and OLA sites (for example, ROADM: Genova, Novara, Sondrio; OLA: Torino, Como, Bergamo).
c) Use the **Fiber** tool to connect sites following the target topology.
d) Click on the source site and then the destination site in the map to select **Circuit** (purple) to add demands.

Both Alien and NCS1000 TXP Trunk to Trunk demands can be created with this option.

e) Select **Service** (green) to create client services of native NCS1000 TXP.

The service automatically creates a trunk-to-trunk circuit.

**Note**
For the specified topology, create a circuit, a service, or both. Define at least one before you run an analysis.

The visual topology reflects the required sites, fibers, circuits, and services.

**Step 3** Follow these steps to set site properties using **Entity Editor**.

a) Choose **Network**, then click **Entity Editor**.
b) Under **Site**, then click **Name**, rename the ROADM and OLA nodes.
c) Add the **NCS 1010 Line Card** property value as *Enhanced Faceplate* or *Standard Faceplate*.

   By default, *Enhanced Faceplate* is selected.

d) For OLA nodes, set **Functionality**, then click **Line amplifier** within the C-Band section.
e) Drill down into **Fibers** to update **Fiber Type**, **Aging Loss**, and **SOL Loss** values.
f) Update the fiber values in **Properties**.
g) Click **Show Advance properties** to update advanced parameters.
h) Expand **Subnet**, then click **OpticalSubnet** and adjust **spectral density** (for example, **Flexgrid-SD-81%**).

- Keep a change log of any forced parameters so installers know which passives to deploy.
- By default fibers are 1 km. Enable **Use Coordinates Distance** under **Network Properties** if you want lengths derived from coordinates.
- To apply Raman amplification, expand a site to C-band and set **Raman Amp** accordingly.

Sites, fibers, and subnet properties match the physical design data.

**Step 4** Optional: To select specific colored Add/drop MD-32-E/MD-32-O Mux/Demux patch panels based on the topology, set these properties.

**Note**
If you do not force this setting and leave it set to **Auto**, Cisco Optical Network Planner automatically selects the default Add/drop.

a) Choose **Network**, click **Entity Editor**, and then click the **Service** tab.
b) In the left tree panel, expand the circuit that connects to the site where the patch panel is connected, and then drill down to the trail properties.
c) Under the trail properties, set **Add/Drop Type** to **Colored**.
d) Click **Select Similar** to apply the properties in bulk to all the trails.
e) Click **Update**.
f) Click the **Site** tab.
g) Expand the ROADM site interface, drill down to the Add/Drop properties of the side, and then under **General**, set **Colored Add/Drop** to **MD-32-Even** or **MD-32-Odd** as per the topology.
h) Click **Select Similar** to apply the properties in bulk to all the add/drops.
i) Click **Update**.

**Step 5** Optional: To select specific BRK-24 and BRK-8 breakout panels, set these properties.

**Note**
If **Auto** is selected, Cisco Optical Network Planner automatically selects the default Add/drop.

a) Choose **Network**, click **Entity Editor**, and then click the **Service** tab.
b) In the left tree panel, expand the circuit that connects to the site where the breakout panel is connected, and then drill down to the trail properties.
c) Under the trail properties, set **Add/Drop Type** to **Colorless**.
d) Click **Select Similar** to apply the properties in bulk to all the trails.

e) Click **Update**.
f) Click the **Site** tab.
g) Expand the site interface, drill down to the Add/Drop properties of the side, and then under **MPO Connector Add Drop**, set **Colorless Add/Drop** to **BRK-8** or **BRK-24**.
h) Click **Select Similar** to apply the properties in bulk to all the add/drops.
i) Click **Update**.

**Step 6** To add NCS 1014 (NCS1K14-2.4T-K9=), set these properties in the left tree panel:

a) Expand the service that connects to the site where NCS 1014 (NCS1K14-2.4T-K9=) is connected in the left tree panel, and then drill down to the service properties.
b) Under **Service Properties**, in **Primary Channel Source**, set **Card Type** to **NCS1K14-2.4T-X-K9** and **TXP Chassis** to **NCS1014**.
c) Click **Update**.
d) Click **Show Advance Properties**, and set **Src Add/drop Type** and **Dst Add/drop Type** to **Colorless/Colored**.

**Note**
If **Show Advance Properties** is not displayed, check whether a service is selected in the left panel. If a service is selected, clear the selection, and then click the service again.

e) Click **Update**.

**Step 7** To add NCS 1004 (NCS1K4-QXP-K9=), set these properties in the left tree panel:

a) Expand the service that connects to the site where NCS 1004 (NCS1K4-QXP-K9) is connected in the left tree panel, and then drill down to the service properties.
b) Under **Service Properties**, in **Primary Channel Source**, set **Card Type** to **NCS1K4-QXP-K9** and **TXP Chassis** to **NCS1004**.
c) Click **Update**.
d) Click **Show Advance Properties**, and set **Src Add/drop Type** and **Dst Add/drop Type** to **Colorless/Colored**.
e) Click **Update**.

**Step 8** Choose **File**, then click **Save** to store the project.

Alternatively, you can click Cisco Optical Network Planner Excel import/export workflow to create a network. For more details, see Import a network using an Excel sheet

The project file captures the designed topology and is ready for analysis.

---

You now have a fully defined Cisco Optical Network Planner network that aligns with physical requirements and can proceed to Analyze and Cisco Optical Site Manager export stages.

### What to do next

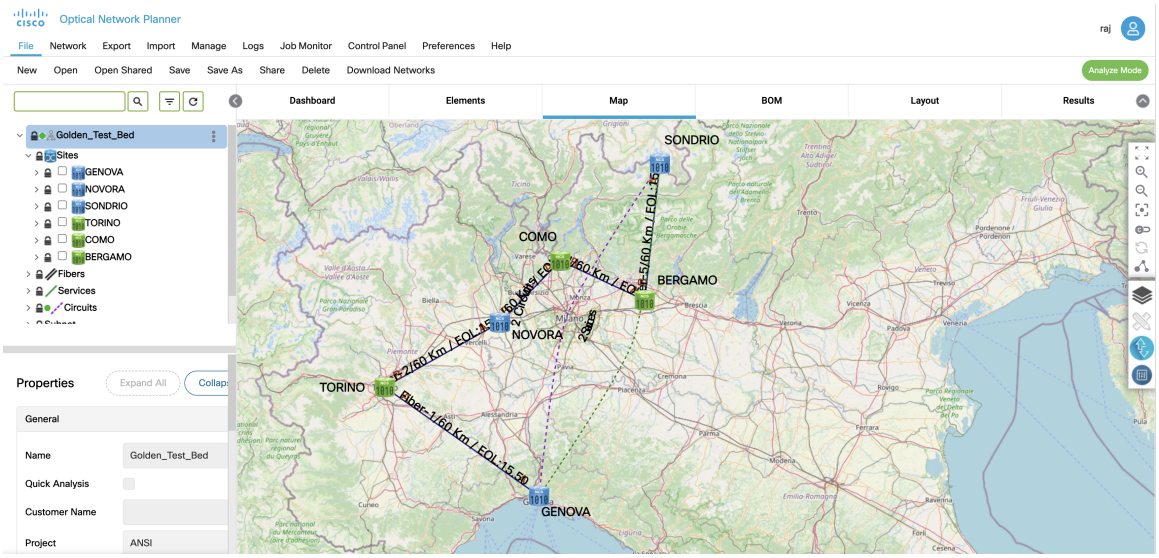
- Analyze the network, on page 13
- Share the screenshots and any Excel import artifacts with reviewers.

# Analyze the network

To analyze the designed sample network and check its feasibility using the Cisco Optical Network Planner Web Interface.

After a successful network analysis, you can validate the design by reviewing various reports available in Cisco Optical Network Planner, including Layout, NFV, BOM, and Optical Reports. These reports provide detailed information about hardware placement, interconnections, inventory, and circuit feasibility.

*Figure 2: CONP Analyzed Network*




## Before you begin

Ensure you have access to the Cisco Optical Network Planner Web Interface and have a sample topology network created.

Follow these steps to analyze the network.

## Procedure

**Step 1** Log in to Cisco Optical Network Planner Web Interface.

**Step 2** Click **File**, then click **Open**.

The **Select Network To Open** dialog box appears.

**Step 3** Click the sample topology network that you have created, from the list of networks.

**Step 4** Click **Network**, then click **Analyze**.

The Cisco Optical Network Planner analysis progress indicator indicates the analysis status.

*Table 6: Analysis Status*

| If... | Then... |
|---|---|
| After successful analysis | The network goes to Analyze Mode. |
| If there is any failure in the analysis stage | A pop-up window appears with the message, “Analysis Failed.” |

**Step 5** Choose the **Elements** > **Messages** tab to see the list of error details in the analyzed network.

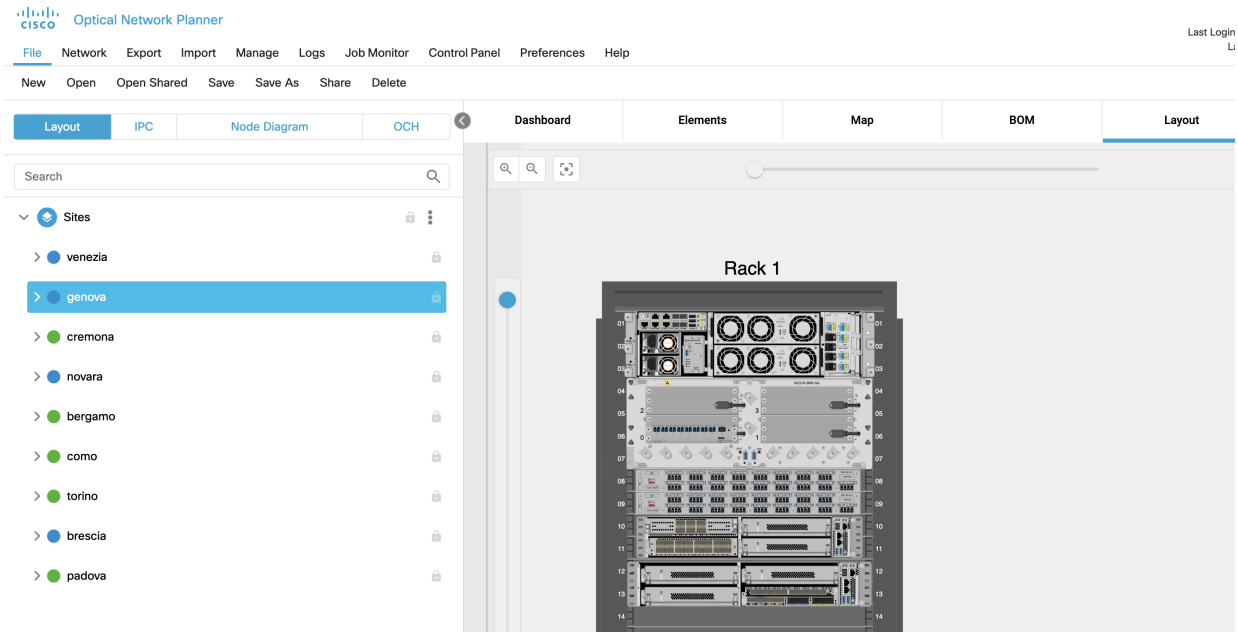
- By default, it shows only the key messages when the **Critical Only** toggle button is enabled.
- If you want to view the entire network message, disable the **Critical Only** toggle button.

**Step 6** If you find an error message under the **Messages** tab, resolve the error and analyze the network again. Repeat this step until all errors are resolved.

**Step 7** Validate the design by navigating to the **Network View** and reviewing these reports:

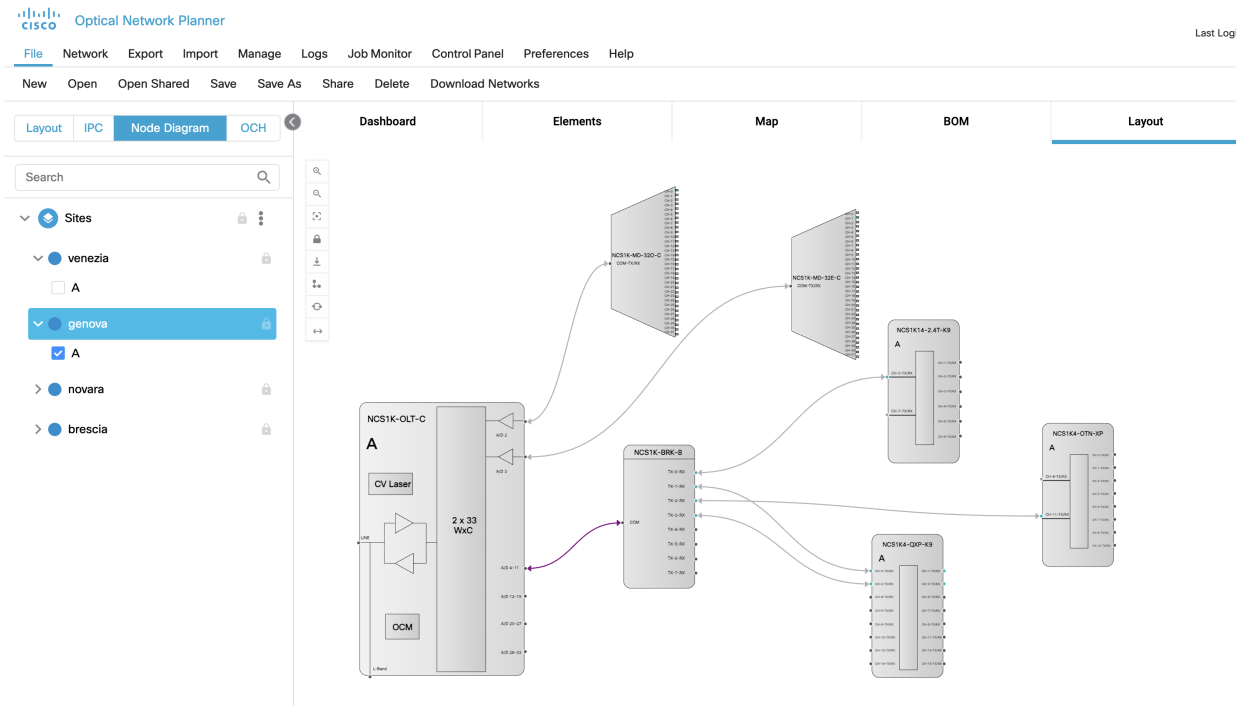
a) **Layout Tab**: View hardware placement, rack level details, and site interconnections (via **Node Diagram** in the left panel).

***Figure 3: CONP Layout***




b) **Node Diagram**: View the site interconnections.

*Figure 4: CONP Node Functional View*




c) **BOM Tab**: See the inventory list for each site.
d) **Results** (including **Optical Reports**, **Installation Parameters**, and **Cabling Report**): Validate circuit feasibility and other design parameters.

   For more details about the report parameters, see Optical Report.

---

The network should be in an analyzed state, and you should have validated the design using the CONP reports.

### What to do next

Refer to the **Troubleshoot** section in CONP Analysis Troubleshooting for understanding common analysis errors.

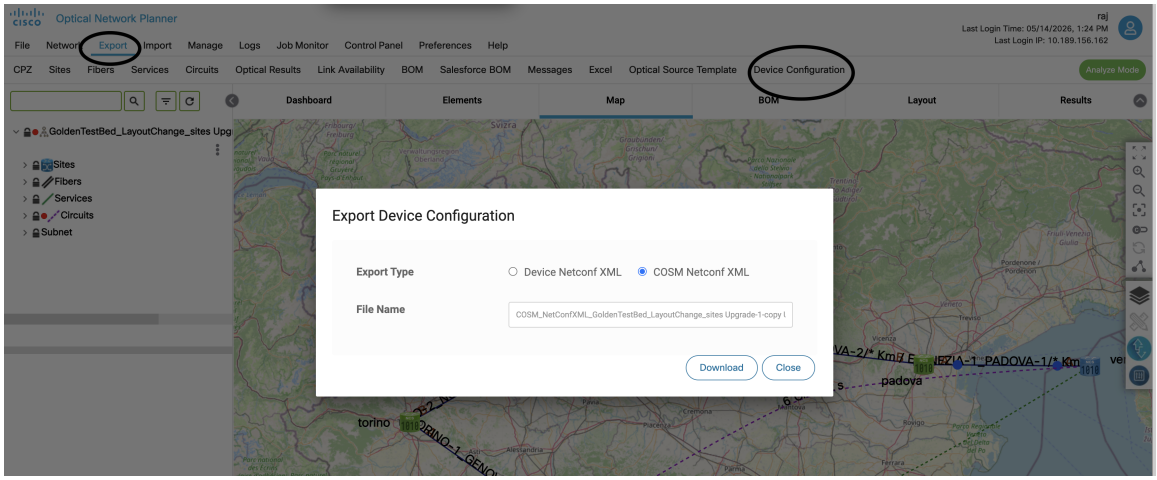
# Generate Cisco Optical Site Manager Netconf XML Files

Generate and prepare Cisco Optical Site Manager Netconf XML files from Cisco Optical Network Planner.

After the network has undergone analysis and validation, it is necessary to export the configuration data from Cisco Optical Network Planner in a Netconf XML format.

The exported files are packaged into a Zip archive, and each file within this archive corresponds to a specific site, identified by its unique naming convention.

*Figure 5: Export device configurationfrom Cisco Optical Network Planner*




### Before you begin

Ensure that the network has been thoroughly analyzed and validated.

Follow these steps to generate Cisco Optical Site Manager Netconf XML files.

### Procedure

**Step 1** Export the Cisco Optical Site Manager Netconf XML file from Cisco Optical Network Planner.

Refer to Export Cisco Optical Site Manager Netconf XML File for detailed instructions on the export process.

Figure 5 illustrates the Cisco Optical Network Planner export interface: **Export** → **Device Configuration** → **Cisco Optical Site Manager Netconf XML**.

A Zip file with a specified name is downloaded.

**Step 2** Identify the individual site configuration files within the downloaded Zip file.

The Zip file contains a list of files, where each file represents a distinct site. The file name helps to identify the individual site using the format:

```
<NetworkName-SiteName>
```

.

**Step 3** Upload each individual site file into Cisco Optical Site Manager after it is operational.

For details, see Import Cisco Optical Network Planner XML.

The Cisco Optical Site Manager Netconf XML files are successfully generated, extracted, and prepared for Day1 device configuration in Cisco Optical Site Manager.

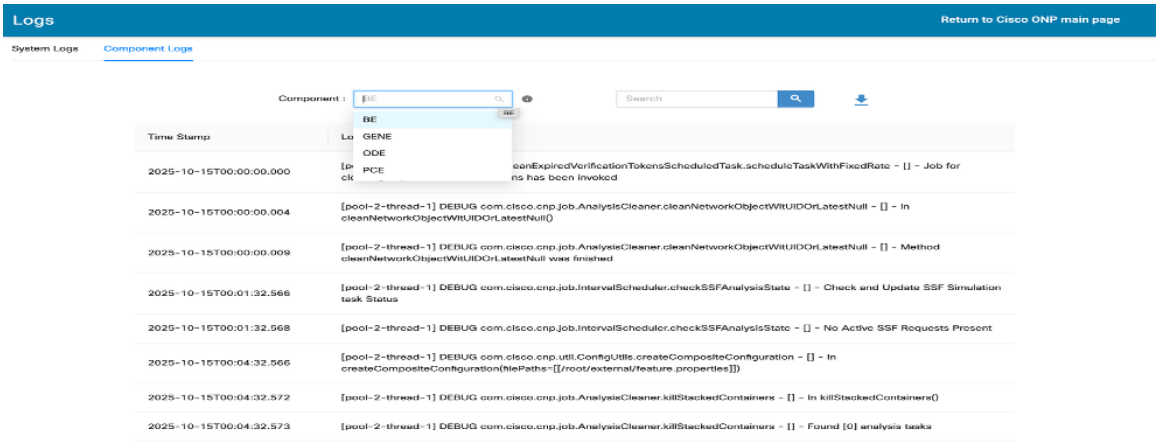
### What to do next

Bring up the platform and Cisco Optical Site Manager, and then configure the Day 1 device settings in Cisco Optical Site Manager by using the uploaded files.

# Troubleshooting and log collection

Collect the network export and component logs required by engineering support.

***Figure 6: Cisco Optical Network Planner logs collection***




To resolve any issues encountered during installation, see Troubleshooting Guide.

**Before you begin**

- Ensure you have administrator access to Cisco Optical Network Planner.
- Verify the target network project is available in the Cisco Optical Network Planner workspace.

Follow these steps to collect troubleshooting logs for engineering support.

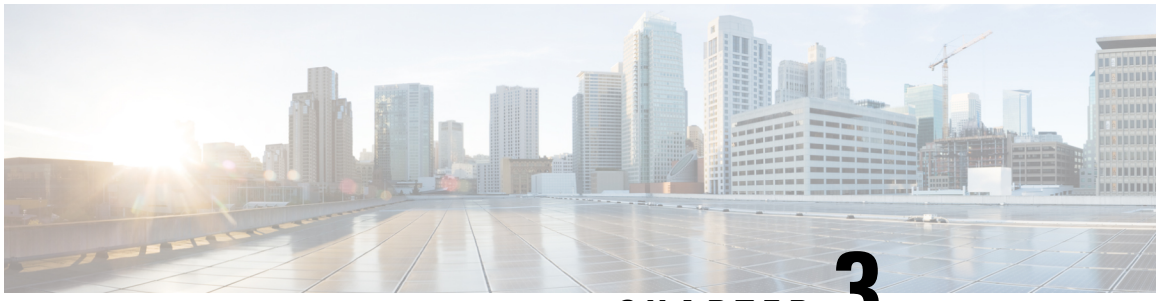
### Procedure

**Step 1** Open the network in Cisco Optical Network Planner, select **Export**, then click **CPZ** to export the CPZ file of the network.

**Step 2** Export the component logs.

a) Click **Logs**, then click **Component Logs**.

b) Collect these logs: BE (CONP Backend log), GENE (NCS1010 and NCS1000 TXP Analysis Engine), ODE (NCS4k Analysis Engine), and PCE (NCS1010 Path Computation & Simulation Engine).



CHAPTER 3

# Bring Up Your NCS 1000 Devices

This chapter describes the overall architecture of the Optical Automation Solution (OAS) and explains the roles of the Cisco Network Convergence System (NCS) 1010, NCS 1014, and NCS 1004 platforms within the solution.



# NCS 1000 platform architecture overview

The OAS solution integrates the NCS 1010 Optical Line System (OLS) with NCS 1014 and NCS 1004 transponder shelves to support metro, long-haul, and submarine deployments.

- Supports advanced coherent optics, including 400G ZR and ZR+ modules and digital coherent optics.
- Runs Cisco IOS XR operating system (IOS XR) with automation features such as Zero Touch Provisioning and streaming telemetry.
- Uses integrated optical line cards to simplify field deployments and monitoring.

### Platform components

The sample topology in this document uses these platforms to build the Optical Automation Solution network.

- NCS 1010: 3RU OLS chassis with chassis, breakout patch panel, and 32-channel mux and demux panels.
- NCS 1014: 2RU transponder chassis for high-performance transport applications.
- NCS 1004: 2RU transponder chassis for universal transport deployments.

### Topology context and analogy

This table describes how OAS and non-OAS deployments differ in architecture, platform roles, and topology placement.

*Table 7: Deployment context*

| Focus | Description |
|---|---|
| Example topology | An OAS deployment can place NCS 1010 Optical Line Terminal (OLT) and In-Line Amplifier (ILA) nodes at the line system layer and connect NCS 1014 and NCS 1004 shelves at sites that need transponder capacity. |
| Non-OAS deployment | Deployments that use only transponder shelves without an optical line system do not meet the OAS end-to-end architecture described in this guide. |
| Transport backbone analogy | Think of the NCS 1010 as the backbone roadway, while the NCS 1014 and NCS 1004 shelves provide the lanes that carry the traffic. |

# NCS 1010 hardware and software support

Identify the major hardware components and the software stack used by the NCS 1010 Optical Line System.

Main chassis components.

- Backplane and embedded timing unit (EITU) are fixed in the chassis.
- Power supply unit (PSU), CPU, fan trays, and optical tray are field replaceable.

*Table 8: NCS 1010 hardware inventory*

| Item | Role | Replaceable | Notes |
|---|---|---|---|
| Backplane | Chassis interconnect | No | Fixed in chassis |
| EITU | Timing | No | Embedded timing unit |
| Optical tray | Line system optics | Yes | Customer configurable |
| PSU and fans | Power and cooling | Yes | Redundant fan trays |

Software components and features.

- IOS XR 7 provides administration and control plane services.
- OSA and CMA are IOS XR components that enable NCS 1010 functionality.

*Table 9: Software stack components*

| Item | Role | Component type | Notes |
|---|---|---|---|
| IOS XR 7 | Control Plane | Operating system | Supports automation features |
| OSA | Optical Service Agent | IOS XR component | Works between control/management planes and hardware abstraction layers |

| Item | Role | Component type | Notes |
|---|---|---|---|
| CMA | Cisco Multiplexer Agent | IOS XR component | Software abstraction layer that manages optical muxponder/transponder hardware |
| Third-party apps | Platform extensibility | Containers | Supported on the platform |

*Table 10: IOS XR capabilities*

| Attribute | Availability | Notes |
|---|---|---|
| **Zero Touch Provisioning** | Supported | Use for automated bring-up |
| **Streaming telemetry** | Supported | Use for monitoring |

**Note** Validate the exact feature set against the IOS XR release notes for your deployment.

# NCS 1014 overview

The NCS 1014 chassis delivers a universal transponder solution that supports metro, long-haul, and submarine deployments.

- Supports transponder and line system cards in a 2RU form factor.
- Designed for high-performance optical transport applications.
- Integrates with the OAS end-to-end solution alongside NCS 1010.

### Deployment guidance

Use the NCS 1014 where transponder capacity is required.

- Install the chassis in a rack that meets EIA, ANSI, or ETSI requirements.
- Follow the power and grounding requirements for the site.
- Deploy NCS 1014 shelves at aggregation sites that terminate optical channels from the NCS 1010 line system.
- If a site only requires line system functions, use the NCS 1010 without adding transponder shelves.
- Think of the NCS 1014 as the translator that converts high-speed optical signals for network transport.

For more details about NCS 1014 deployment guidance, see Hardware Installation Guide for Cisco NCS 1014.

# NCS 1004 overview

The NCS 1004 provides high-performance transponder capabilities for metro, long-haul, and submarine applications.

- Delivers a 2RU chassis optimized for transport use cases.
- Supports universal transponder functions in the Optical Access System (OAS) architecture.
- Pairs with NCS 1010 line system nodes in OAS deployments.

### Deployment guidance

Use the NCS 1004 where a compact transponder shelf is required.

- Install the chassis in an EIA, ANSI, or ETSI rack.
- Follow site power and grounding requirements.
- Use NCS 1004 shelves at sites that require a smaller footprint while maintaining high-capacity transport.
- If a site requires only line system functions, use the NCS 1010 without transponder shelves.
- Think of the NCS 1004 as a compact transponder rack that fits in tighter spaces while still carrying heavy traffic.

For more details about the NCS 1004 deployment guidance, see Hardware Installation Guide for Cisco NCS 1004.

# Prerequisites

Collect the required addressing and host information for each node in the topology.

Required details to gather before installation for each node in the topology.

- Hostname for each node.
- Management and loopback IP addresses.
- Indicate the node role, such as OLT, ILA, OLA, or transponder shelf.
- DCN plans to ensure proper management connectivity.
- Access to servers such as NTP, TACACS, and Smart Licensing for software downloads.

*Figure 7: Sample topology addressing*

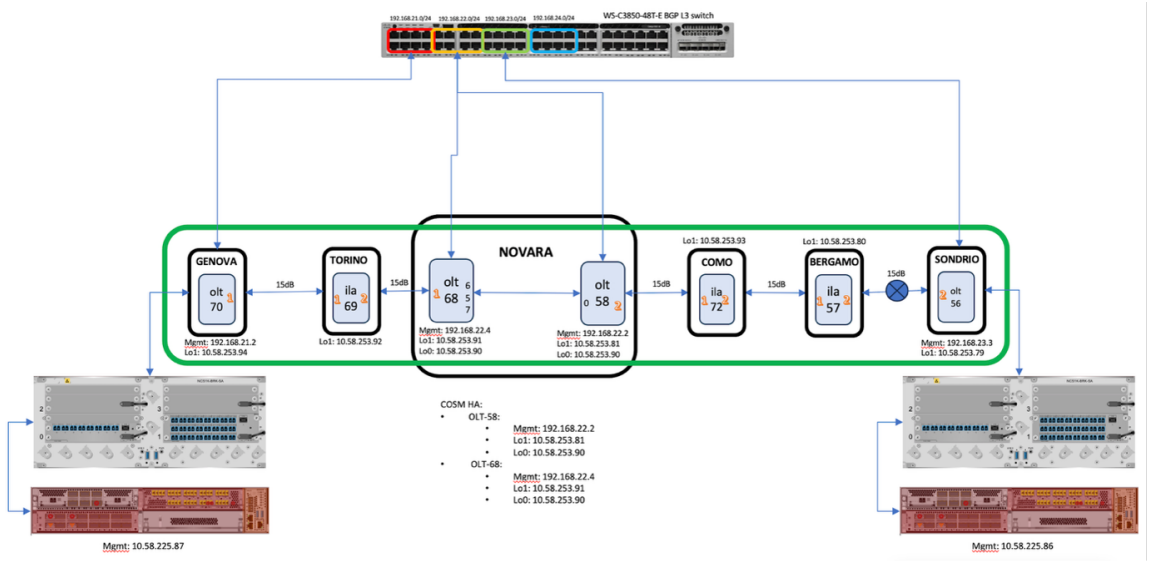



*Table 11: Sample topology addressing*

| Node type | Hostname | Mgmt0 IP | Mgmt2 IP | Loopback1 IP (OSC/COSM) | Loopback0 IP (COSM- HA) |
|---|---|---|---|---|---|
| NCS1K-OLT-C | onc-oltc-225-70 | 10.58.225.70 | 192.168.21.2 | 10.58.253.94 | – |
| NCS1K-ILA-C | onc-ilac-225-69 | 10.58.225.69 | – | 10.58.253.92 | – |
| NCS1K-OLT-C | onc-oltc-225-68 | 10.58.225.68 | 192.168.22.4 | 10.58.253.91 | 10.58.253.90 |
| NCS1K-OLT-C | onc-oltc-225-58 | 10.58.253.58 | 192.168.22.2 | 10.58.253.81 | 10.58.253.90 |
| NCS1K14 | onc-kepler-225-87 | 10.58.225.87 | – | – | – |
| NCS1K04 | onc-bh-225-93 | 10.58.225.93 | – | – | – |

### Management interface requirements

This table describes the data that must be confirmed before installation, along with its status and related notes.

*Table 12: Data to confirm before installation*

| Item | Status | Notes |
|---|---|---|
| **IP plan** | Complete | Validated with design team |
| **Hostname list** | Complete | Aligned with naming standards |

**Note** Adjust the addressing table to match the customer topology.

# Install Cisco NCS 1010, NCS 1014, and NCS 1004 hardware

Prepare the hardware so it is ready for initial configuration.

Use these hardware-installation tasks in sequence. Each linked procedure is kept as a separate task step in the child topics.

**Before you begin**

Verify that the rack, power, grounding, hardware placement, cabling, and passive-connection details meet the site design and Cisco installation requirements.

**Procedure**

**Step 1** Prepare and install the NCS 1010 chassis and required modules for the site.

For more details, see Install the NCS 1010 chassis and modules.

**Step 2** Connect the NCS 1010 chassis to the approved site power feed.

For more details, see Connect power to the NCS 1010.

**Step 3** Install the NCS 1010 passive modules and breakout hardware from the site design.

For more details, see Install NCS 1010 passive modules.

**Step 4** Prepare and install the NCS 1014 chassis and required modules for the site.

For more details, see Install the NCS 1014 chassis and modules.

**Step 5** Install NCS 1014 power components, pluggables, and air-filter hardware.

For more details, see Complete NCS 1014 power, pluggables, and air-filter installation.

**Step 6** Prepare and install the NCS 1004 chassis in the site rack.

For more details, see Install the NCS 1004 chassis.

**Step 7** Install the NCS 1004 controller and line cards required by the bill of materials.

For more details, see Install NCS 1004 controller and line cards.

**Step 8** Install the NCS 1004 FRUs, pluggables, air filter, and fiber-management hardware.

For more details, see Install NCS 1004 field-replaceable units and fiber management.

**Step 9** Connect NCS 1004 power and complete final fiber and passive connections.

For more details, see Connect NCS 1004 power and complete passive connections.

All hardware is installed and ready for console access and initial configuration.

# Install the NCS 1010 chassis and modules

Install the NCS 1010 chassis and field-replaceable modules required for the site.

Complete these procedures before applying site power or completing passive-module connections.

**Before you begin**

Verify rack space, grounding, and site installation readiness for NCS 1010.

**Procedure**

**Step 1** Verify rack space, grounding, airflow, tools, and safety requirements before installing Cisco NCS 1010.

For more details, see Prepare to install Cisco NCS 1010.

**Step 2** Mount the Cisco NCS 1010 chassis in the approved EIA, ANSI, or ETSI rack.

For more details, see Install Cisco NCS 1010 on an EIA, ANSI, or ETSI rack.

**Step 3** Install the required Cisco NCS 1010 modules in their assigned chassis slots.

For more details, see Install Cisco NCS 1010 modules.

**Step 4** Insert and seat the NCS 1010 power supply unit in the assigned slot.

For more details, see Install PSU.

**Step 5** Install and secure the NCS 1010 controller card.

For more details, see Install controller.

**Step 6** Install and secure the required NCS 1010 line card.

For more details, see Install line card.

**Step 7** Install the fan tray and confirm it is fully seated.

For more details, see Install fan tray.

**Step 8** Install the fan filter after the fan tray is in place.

For more details, see Install fan filter.

**Step 9** Install the protection cover as required by the hardware procedure.

For more details, see Install the protection cover.

The NCS 1010 chassis and modules are installed.

# Connect power to the NCS 1010

Connect AC or DC power to the NCS 1010 chassis.

Select the procedure that matches the power design for the site.

**Before you begin**

Install the NCS 1010 chassis, PSU, and required protection hardware.

**Procedure**

**Step 1** Connect the NCS 1010 chassis to the approved AC power source when the site uses AC feeds.

For more details, see Connect AC power to Cisco NCS 1010.

**Step 2** Connect the NCS 1010 chassis to the approved DC power source when the site uses DC feeds.

For more details, see Connect DC power to Cisco NCS 1010.

Power connections for NCS 1010 are complete.

# Install NCS 1010 passive modules

Install passive modules and breakout patch panels according to the site design.

Confirm module placement, port labels, and LED states before completing fiber connections.

**Before you begin**

Review the CONP design for required passive modules and breakout patch panels.

**Procedure**

**Step 1** Identify the breakout patch panels and passive modules required for the NCS 1010 site.

For more details, see Cisco NCS 1000 breakout patch panel and modules overview.

**Step 2** Install the Cisco NCS 1000 breakout patch panel in the planned location.

For more details, see Cisco NCS 1000 breakout patch panel.

**Step 3** Install the Cisco NCS 1000 breakout modules required by the site design.

For more details, see Cisco NCS 1000 breakout modules.

**Step 4** Match breakout module port labels to the cabling plan before connecting fibers.

For more details, see Breakout modules port label descriptions.

**Step 5** Check breakout module LED states after installing and cabling the passive modules.

For more details, see Breakout module LEDs.

NCS 1010 passive module references are reviewed and the passive hardware can be installed according to the site design.

# Install the NCS 1014 chassis and modules

Install the NCS 1014 chassis and core modules required for the OAS site.

Complete these procedures before power, pluggable, and air-filter installation.

**Before you begin**

Verify rack, power, grounding, and fiber-management readiness for NCS 1014.

**Procedure**

**Step 1** Mount the Cisco NCS 1014 chassis in the approved EIA, ANSI, or ETSI rack.

For more details, see Install the Cisco NCS 1014 chassis on an EIA, ANSI, or ETSI rack.

**Step 2** Confirm NCS 1014 power and grounding requirements before installing powered components.

For more details, see General power and grounding requirements.

**Step 3** Attach the fiber management bracket to the slider rail before routing fibers.

For more details, see Attach the fiber management bracket to the slider rail.

**Step 4** Install the SSD in the NCS 1014 chassis.

For more details, see Install the solid state drive (SSD).

**Step 5** Install the fan unit and confirm it is fully seated.

For more details, see Install the fan unit.

**Step 6** Install and secure the NCS 1014 controller.

For more details, see Install the controller.

**Step 7** Attach the fiber management bracket for the installed module layout.

For more details, see Attach the fiber management bracket.

**Step 8** Adjust the fiber management bracket for the planned fiber routing.

For more details, see Adjust the fiber management bracket.

**Step 9** Install and secure the required NCS 1014 line card.

For more details, see Install the line card.

The NCS 1014 chassis and core modules are installed.

# Complete NCS 1014 power, pluggables, and air-filter installation

Complete the remaining NCS 1014 hardware installation after the chassis and core modules are installed.

Select the AC or DC power procedure that matches the site design.

**Before you begin**

Install the NCS 1014 chassis, controller, fan unit, and line cards.

**Procedure**

**Step 1** Install the NCS 1014 power supply units in the assigned slots.

For more details, see Install the power supply units (PSUs).

**Step 2** Connect the NCS 1014 chassis to the approved DC power source when the site uses DC feeds.

For more details, see Connect DC power to the Cisco NCS 1014 chassis.

**Step 3** Connect the NCS 1014 chassis to the approved AC power source when the site uses AC feeds.

For more details, see Connect AC power to the Cisco NCS 1014 chassis.

**Step 4** Install the required pluggables in the NCS 1014 ports.

For more details, see Install the pluggables.

**Step 5** Install the NCS 1014 air filter after module installation is complete.

For more details, see Install the air filter.

NCS 1014 power, pluggables, and air-filter installation is complete.

# Install the NCS 1004 chassis

Install the NCS 1004 chassis according to site rack and grounding requirements.

Complete chassis installation before installing controllers, line cards, and field-replaceable units.

**Before you begin**

Verify rack compatibility, grounding, and power-feed readiness for NCS 1004.

**Procedure**

**Step 1** Confirm that the site rack supports the NCS 1004 chassis before installation.

For more details, see Rack compatibility.

**Step 2** Mount the NCS 1004 chassis in the approved EIA, ANSI, or ETSI rack.

For more details, see Install NCS 1004 on an EIA, ANSI, or ETSI rack.

**Step 3** Apply the NCS 1004 stacking requirements if multiple chassis share the rack space.

For more details, see Stacking NCS 1004.

**Step 4** Confirm NCS 1004 power and grounding requirements before installing powered components.

For more details, see General power and grounding requirements.

**Step 5** Verify the NCS 1004 power supply type against the site power design.

For more details, see Power supply.

The NCS 1004 chassis is installed and ready for module installation.

# Install NCS 1004 controller and line cards

Prepare and install the NCS 1004 controller and supported line-card hardware.

Use the line-card-specific references that match the hardware in the site bill of materials.

**Before you begin**

Install the NCS 1004 chassis.

**Procedure**

**Step 1** Review the NCS 1004 module installation sequence before inserting cards.

For more details, see Install Cisco NCS 1004 modules.

**Step 2** Confirm that the controller card is supported for the NCS 1004 chassis.

For more details, see Supported controller cards.

**Step 3** Install and secure the NCS 1004 controller card.

For more details, see Install controller.

**Step 4** Identify the NCS 1004 line-card type required by the site bill of materials.

For more details, see About line cards.

**Step 5** Use the 1.2T line-card requirements when the site includes a 1.2T card.

For more details, see 1.2T line card.

**Step 6** Use the 1.2TL line-card requirements when the site includes a 1.2TL card.

For more details, see 1.2TL line card.

**Step 7** Use the 2-QDD-C line-card requirements when the site includes a 2-QDD-C card.

For more details, see 2-QDD-C line card.

**Step 8** Use the OTN-XP line-card requirements when the site includes an OTN-XP card.

For more details, see OTN-XP line card.

**Step 9** Use the QXP-K9 line-card requirements when the site includes a QXP-K9 card.

For more details, see QXP-K9 line card.

---

The NCS 1004 controller and line-card references are complete for the installed hardware.

# Install NCS 1004 field-replaceable units and fiber management

Complete NCS 1004 module, field-replaceable unit, pluggable, air-filter, and fiber-management installation.

Use the fiber-management procedure that matches the installed line-card type.

**Before you begin**

Install the NCS 1004 chassis and identify the installed line-card type.

**Procedure**

---

**Step 1** Insert and secure the selected NCS 1004 line card in the assigned slot.

For more details, see Install line card.

**Step 2** Install the NCS 1004 power supply in the assigned slot.

For more details, see Install power supply.

**Step 3** Install the fan unit and confirm it is fully seated.

For more details, see Install fan unit.

**Step 4** Attach the fiber management bracket before routing fibers to the line cards.

For more details, see Attach fiber management bracket.

**Step 5** Adjust fiber management for installed 1.2T, 1.2TL, 2-QDD-C, or QXP-K9 line cards.

For more details, see Adjust fiber management bracket of the 1.2T, 1.2TL, 2-QDD-C, and QXP-K9 line cards.

**Step 6** Adjust fiber management for an installed OTN-XP line card.

For more details, see Adjust fiber management bracket of the OTN-XP line card.

**Step 7** Install the required pluggables in the NCS 1004 ports.

For more details, see Install pluggables.

**Step 8** Confirm the NCS 1004 air-filter requirements for the installed chassis.

For more details, see Air filter.

**Step 9** Install the NCS 1004 air filter.

For more details, see Install air filter.

---

The NCS 1004 field-replaceable units, pluggables, air filter, and fiber-management hardware are installed.

# Connect NCS 1004 power and complete passive connections

Complete NCS 1004 power connections and final OAS fiber and passive connections.

Complete all fiber and port connections according to the network design. Use the Brk-8 module for internal degree connections when required. Based on the design, internal degree connections can also be established directly through LC ports instead of through the Brk-8 module.

**Before you begin**

Install the required NCS 1004 modules and review the CONP design output for site passive connections.

**Procedure**

**Step 1** Connect the NCS 1004 chassis to the approved DC power source when the site uses DC feeds.

For more details, see Connect DC power to NCS 1004.

**Step 2** Connect the NCS 1004 chassis to the approved AC power source when the site uses AC feeds.

For more details, see Connect AC power to NCS 1004.

**Step 3** Use the CONP NFV and connection reports to complete passive and fiber connections.

For more details, see Review the CONP NFV and connection reports.

NCS 1004 power and final site passive connections are complete.

**What to do next**

Proceed to day-0 configuration for each node.

# NCS 1010 setup and initial configuration

This subsection covers the essential steps to prepare and configure the NCS 1010 device for operation.

- Boot the chassis and access the XR console.
- Complete day-0 configuration using the recommended manual approach or ZTP.
- Configure management, loopback, and neighbor interfaces based on the topology.

### NCS1010 bootup process

After installing the hardware, boot the Cisco NCS 1010 system. Connect to the XR console port and power on the system. NCS 1010 completes the boot process using the pre-installed OS image. If no image is available, NCS 1010 can be booted using iPXE or an external bootable USB drive.

Use any one of the tasks to boot the NCS 1010 chassis.

- Boot NCS 1010 using Console (Recommended)
- Connect Console Port to Terminal: Establish a console connection to the device and follow procedure mention in Day 0 configuration.
- Boot NCS 1010 Using USB Drive
- Boot Using iPXE

Once booted, please verify the system using the steps in the Cisco NCS 1010 Deployment Guide.

# Configure NCS 1010 day-0 settings

Prepare the NCS 1010 for day-1 configuration and network onboarding by completing the day-0 sub tasks.

**Procedure**

**Step 1** Complete the manual bring-up workflow.

See Manually bring up NCS1000.

**Step 2** Configure NTP for time synchronization.

See NTP server configuration.

**Step 3** Configure SNMP if monitoring is required.

See SNMP configuration (optional).

## Manually bring up NCS1010, NCS1014, and NCS1004

Complete the manual day-0 bring-up for NCS1010, NCS1014, and NCS1004 by following the prerequisite setup and configuration tasks in sequence.

NCS1010 supports two different approaches for bring-up: manual and ZTP. This workflow covers the manual approach.

**Before you begin**

- Ensure that the NCS 1010 bring-up configuration is completed on all nodes in the topology before proceeding with this section.
- The interfaces come up only after the configuration is applied across all nodes and the fiber connections are completed correctly.

Follow these steps to complete the manual day-0 bring-up for NCS 1010, NCS 1014, and NCS 1004.

**Procedure**

**Step 1** Complete prerequisites and access setup.

See Prepare access and initial credentials.

**Step 2** Configure management and loopback addressing.

See Configure management and loopback addressing.

**Step 3** Configure OSPF and verify neighbors.

See Configure OSPF and verify neighbors.

**Step 4** Configure routing policies and BGP, then update OSPF.

See Configure routing policies, static routes, and BGP.

**Step 5** Validate controllers, alarms, and span loss.

See Validate controllers and alarms.

---

The NCS1010/NCS1014/NCS1004 system is brought up to day-0 configuration and ready for downstream workflows.

## Prepare access and initial credentials on NCS1010

Establish console access, set root credentials, and apply a hostname so the node can be configured.

Follow these steps to prepare access and initial credentials on the node.

### Procedure

---

**Step 1** Configure DHCP settings if required for IP address assignment.

A DHCP server is required for this configuration.

For more details, see Cisco NCS 1010 Deployment Guide, Cisco IOS XR Releases.

**Step 2** Connect to the node through the console port, configure the root-system username, and use these credentials to log in later.

**Example:**

```
          ---------------------
Enter root-system username: xxxxxx
Enter secret:
Enter secret again:
Use the 'configure' command to modify this configuration.
User Access Verification
Username:
Password: xxxxxx
---------------------
```

**Step 3** Assign a hostname to the node.

**Example:**

```
RP/0/RP0/CPU0:ios#config
RP/0/RP0/CPU0:ios(config)#hostname onc-oltc-225-70
```

```
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#end
```

The node is accessible with root credentials and has a hostname assigned.

### What to do next

Next, complete Configure management and loopback addressing.

## Configure management and loopback addressing

Assign management and loopback IP addressing and verify interface status before and after addressing.

**Before you begin**

- Complete Prepare access and initial credentials on NCS1010.
- Refer to the Table 11: Sample topology addressing, on page 23 for sample IP address configuration.

Follow these steps to configure management and loopback addressing.

### Procedure

**Step 1** View the interface status before addressing.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70#show ipv4 interface brief
```

*Table 13: Interface status before addressing*

| Interface | IP-Address | Status | Protocol | Vrf-Name |
|---|---|---|---|---|
| Loopback1 | unassigned | Down | Down | default |
| GigabitEthernet0/0/0/0 | unassigned | Down | Down | default |
| MgmtEth0/RP0/CPU0/0 | unassigned | Down | Down | default |
| PTP0/RP0/CPU0/0 | unassigned | Down | Down | default |
| MgmtEth0/RP0/CPU0/1 | unassigned | Down | Down | default |
| PTP0/RP0/CPU0/1 | unassigned | Down | Down | default |
| MgmtEth0/RP0/CPU0/2 | unassigned | Down | Down | default |
| MgmtEth0/RP0/RCOM0/0 | unassigned | Down | Down | default |

**Step 2** Assign IP addresses for management, GigabitEthernet, and Loopback interfaces based on the addressing plan.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70#configure
RP/0/RP0/CPU0:onc-oltc-225-70(config)#interface Loopback1
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# ipv4 address 10.58.253.94 255.255.255.255
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# interface MgmtEth0/RP0/CPU0/0
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# ipv4 address 10.58.225.70 255.255.255.0
```

**Step 3** Configure the management interface.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)#interface MgmtEth0/RP0/CPU0/2
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# ipv4 address 192.168.21.2 255.255.255.0
```

These items outline the management interface design choices by node type for this topology document

- OLT: MgmtEth0/RP0/CPU0/2 required for DHCP relay and remote management.
- ILA: MgmtEth0/RP0/CPU0/2 required for neighbor connectivity.

This table describes the management interface requirements:

***Table 14: Interface requirements***

| Node type | MgmtEth0/RP0/CPU0/2 | Required | Purpose |
|---|---|---|---|
| OLT | Yes | Required | DHCP relay and remote management |
| ILA | Yes | Required | Neighbor connectivity |
| TXP shelves | No | Not required | Not applicable |

**Step 4** Configure loopback addresses on both NCS 1010 OLTs participating in Cisco Optical Site Manager HA.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-58(config)#interface Loopback0
RP/0/RP0/CPU0:onc-oltc-225-58(config-if)#ipv4 address 10.58.253.90 255.255.255.255
RP/0/RP0/CPU0:onc-oltc-225-68(config)#interface Loopback0
RP/0/RP0/CPU0:onc-oltc-225-68(config-if)#ipv4 address 10.58.253.90 255.255.255.255
```

**Example:**

**Note**
These IP address should be same on the NCS 1010 HA hosts.

**Step 5** Configure neighbor connectivity for OLT and ILA nodes.

Not required for TXP shelves for NCS 1014 and NCS 1004.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)#interface GigabitEthernet0/0/0/0
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# ipv4 point-to-point
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# ipv4 unnumbered Loopback1
RP/0/RP0/CPU0:onc-oltc-225-70(config-if)# lldp
```

```
RP/0/RP0/CPU0:onc-oltc-225-70(config-lldp)#  enable
RP/0/RP0/CPU0:onc-oltc-225-70(config-lldp)#  commit
```

**Step 6** For ILA nodes, configure the second neighbor interface.

**Example:**

```
RP/0/RP0/CPU0:onc-ilac-225-69(config-if)#interface GigabitEthernet0/0/0/2
RP/0/RP0/CPU0:onc-ilac-225-69(config-if)# ipv4 point-to-point
RP/0/RP0/CPU0:onc-ilac-225-69 (config-if)# ipv4 unnumbered Loopback1
RP/0/RP0/CPU0:onc-ilac-225-69 (config-if)# lldp
RP/0/RP0/CPU0:onc-ilac-225-69 (config-lldp)#  enable
RP/0/RP0/CPU0:onc-ilac-225-69 (config-lldp)#  commit
RP/0/RP0/CPU0:onc-ilac-225-69 (config-lldp)#  end
```

**Step 7** View the interface status after addressing.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70#show ipv4 interface brief
```

***Table 15: Interface status after addressing***

| Interface | IP-Address | Status | Protocol | Vrf-Name |
|---|---|---|---|---|
| Loopback1 | 10.58.253.94 | Up | Up | Default |
| GigabitEthernet0/0/0/0 | 10.58.253.94 | Up | Up | Default |
| MgmtEth0/RP0/CPU0/0 | 10.58.225.70 | Up | Up | Default |
| PTP0/RP0/CPU0/0 | unassigned | Down | Down | Default |
| MgmtEth0/RP0/CPU0/1 | unassigned | Down | Down | Default |
| PTP0/RP0/CPU0/1 | unassigned | Down | Down | Default |
| MgmtEth0/RP0/CPU0/2 | 192.168.21.2 | Up | Up | Default |
| MgmtEth0/RP0/RCOM0/0 | unassigned | Down | Down | Default |

**Step 8** Configure SSH (secure shell).

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#config
RP/0/RP0/CPU0:onc-oltc-225-70(config)#ssh server rate-limit 600
RP/0/RP0/CPU0:onc-oltc-225-70(config)#ssh server session-limit 110
RP/0/RP0/CPU0:onc-oltc-225-70(config)#ssh server v2
RP/0/RP0/CPU0:onc-oltc-225-70(config)#ssh server vrf default
RP/0/RP0/CPU0:onc-oltc-225-70(config)#ssh server netconf vrf default
RP/0/RP0/CPU0:onc-oltc-225-70(config)#commit
```

**Step 9** Configure NETCONF-YANG over SSH to enable device management by Cisco Optical Site Manager.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#netconf agent tty
RP/0/RP0/CPU0:onc-oltc-225-70(config-netconf-tty)#netconf-yang agent
RP/0/RP0/CPU0:onc-oltc-225-70(config-ncy-agent)# ssh
RP/0/RP0/CPU0:onc-oltc-225-70(config)#commit
```

IP addresses are assigned to the management and loopback interfaces.

### What to do next

Next, complete Configure OSPF and verify neighbors, on page 37.

## Configure OSPF and verify neighbors

Configure OSPF on OLT and ILA nodes and verify neighbor adjacencies. The neighbours are visible only after the configuration is applied across all nodes and the fiber connections are completed correctly.

Follow these steps to configure OSPF and verify neighbors.

### Procedure

**Step 1** Configure OSPF in NCS1010 OLT nodes.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#router ospf 1
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# distribute link-state
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# router-id 10.58.253.94
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# network point-to-point
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# area 0
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar)#  interface Loopback1
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar-if)#  interface GigabitEthernet0/0/0/0
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar-if)#commit
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar-if)# end
```

**Note**
**router-id** must be modified for each node.

**Step 2** Configuring OSPF settings for the interface on the ILA node and commit the changes.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#router ospf 1
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# distribute link-state
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# router-id 10.58.253.94
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# network point-to-point
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# area 0
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar)#  interface Loopback1
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar-if)#  interface GigabitEthernet0/0/0/0
RP/0/RP0/CPU0: onc-ilac-225-69(config-ospf-ar-if)#  interface GigabitEthernet0/0/0/2
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar-if)#commit
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf-ar-if)# end
```

**Note**

**router-id** must be modified for each node.

**Step 3** View OSPF neighbors using the **show ospf neighbor** command.

**Example:**

```
RP/0/RP0/CPU0:OLT-R-C-SITE-4#show ospf neighbor
Mon Jul 25 09:22:58.684 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up
Neighbors for OSPF 1
Total neighbor count: 2


Neighbor ID     Pri    State           Dead Time   Address              Interface
10.58.253.94     1     FULL/  -        00:00:38    10.58.253.94        GigabitEthernet0/0/0/0
    Neighbor is up for 1w1d
10.58.253.91     1     FULL/  -        00:00:38    10.58.253.91        GigabitEthernet0/0/0/2
    Neighbor is up for 3d06h
```

OSPF is configured and neighbor adjacency is verified.

### What to do next

Next, complete Configure routing policies, static routes, and BGP.

## Configure routing policies, static routes, and BGP

Configure routing policy, static routes, and BGP (OLT only), then update OSPF redistribution.

**Before you begin**

- Complete Configure OSPF and verify neighbors.
- The static routes and IP address need to be updated based on DCN configuration and topology.

Follow these steps to configure routing policies and BGP, then update OSPF.

### Procedure

**Step 1** Configure route policy and static routes on OLT and ILA nodes.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70#config
RP/0/RP0/CPU0:onc-oltc-225-70(config)#route-policy pass-all
RP/0/RP0/CPU0:onc-oltc-225-70(config-rpl)# pass
RP/0/RP0/CPU0:onc-oltc-225-70(config-rpl)#end-policy
RP/0/RP0/CPU0:onc-oltc-225-70(config)#router static
RP/0/RP0/CPU0:onc-oltc-225-70(config-static)# address-family ipv4 unicast
RP/0/RP0/CPU0:onc-oltc-225-70(config-static-afi)# 0.0.0.0/0 10.58.225.1
RP/0/RP0/CPU0:onc-oltc-225-70(config-static-afi)# 10.58.251.0/24 10.58.253.1
```

**Step 2** Configure BGP for SSH connectivity from DCN on OLT nodes only.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#router bgp 1
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp)# bgp router-id 10.58.253.94
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-af)#  redistribute connected
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-af)#  redistribute ospf 1 route-policy pass-all
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-af)#neighbor 192.168.21.1
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-nbr)#  remote-as 100
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-nbr)#  address-family ipv4 unicast
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-nbr-af)#   route-policy pass-all in
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-nbr-af)#   route-policy pass-all out
```

**Step 3** Redistribute routes between OSPF and BGP.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config-bgp-nbr-af)#router ospf 1
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# default-information originate
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# redistribute connected
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# redistribute bgp 1 route-policy pass-all
RP/0/RP0/CPU0:onc-oltc-225-70(config-ospf)# commit
```

Routing policy, static routes, and BGP are configured and OSPF redistribution is updated.

### What to do next

Next, complete Validate controllers and alarms.

## Validate controllers and alarms

Validate controller status, review alarms, and confirm span-loss after bring-up.

**Before you begin**

- Complete Configure routing policies, static routes, and BGP.
- Verify that the configuration is applied across all nodes and the fiber connections are completed correctly.

Follow these steps to validate controllers and alarms.

### Procedure

**Step 1** Verify the OSC **Controller State** is *UP*.

For ILA nodes, check both controllers.

**Example:**

```
RP/0/RP0/CPU0:onc-ilac-225-69#show controllers osc 0/0/0/0
Controller State: Up
Transport Admin State: In Service
```

```
Laser State: On
Last link flapped: 1w1d
Alarm Status:
-------------
Detected Alarms: None

Alarm Statistics:
-----------------
RX-LOS-P = 0
TX-POWER-FAIL-LOW = 0

Parameter Statistics:
---------------------
Total Tx Power = -7.92 dBm
Total Rx Power = -22.88 dBm
OSNR = 41.50 dB
```

```
RP/0/RP0/CPU0:onc-ilac-225-69#show controllers osc 0/0/0/2
```

**Step 2** Check for active alarms and refer to the troubleshooting guide to clear them if necessary.

**Example:**

```
          RP/0/RP0/CPU0:onc-ilac-225-69#sh alarms brief system active
------------------------------------------------------------------------------------
Active Alarms
------------------------------------------------------------------------------------
Location        Severity     Group            Set Time                    Description
------------------------------------------------------------------------------------
0/PM1           Major        Environ          09/19/2025 13:29:25 UTC    Power Module Error
(PM_VIN_VOLT_OOR)
0/PM1           Major        Environ          09/19/2025 13:29:25 UTC    Power Module Output Disabled
 (PM_OUTPUT_DISABLED)
0               Major        Environ          09/19/2025 13:29:25 UTC    Power Group Redundancy lost
0/RP0/CPU0      Minor        Software         09/19/2025 13:31:02 UTC    SW Upgrade is still allowed
 as SIA Grace Period is remaining
0/RP0/CPU0      Major        Software         09/19/2025 13:31:05 UTC    Communications Failure With
 Cisco Licensing Cloud
0/0/NXR0        Minor        Software         11/22/2025 11:50:38 UTC    Ots0/0/0/0 - Span Loss Value
 Out Of Range
0/0/NXR0        Minor        Software         11/24/2025 12:15:35 UTC    Ots0/0/0/2 - Span Loss Value
 Out Of Range
```

**Step 3** Verify SSH connectivity to all nodes and check span loss after neighbor or full topology bring-up.

**Example:**

```
          RP/0/RP0/CPU0:onc-ilac-225-69#sh olc span-loss
------------------------------------------------------
Controller                              : Ots0/0/0/0
Neighbour RID                           : 10.58.253.94
Rx Span Loss                            : 14.62 dB
Rx OSC Span Loss                        : 14.91 dB
Rx Signal Span Loss                     : 14.62 dB
Rx Span Loss (with pumps off)           : NA
Estimated Rx Span Loss                  : NA
Tx Span Loss                            : 14.96 dB
Tx OSC Span Loss                        : 15.02 dB
Tx Signal Span Loss                     : 14.96 dB
Tx Span Loss (with pumps off)           : NA
Estimated Tx Span Loss                  : NA

Controller                              : Ots0/0/0/2
```

```
Neighbour RID                           : 10.58.253.91
Rx Span Loss                            : 14.41 dB
Rx OSC Span Loss                        : 14.59 dB
Rx Signal Span Loss                     : 14.41 dB
Rx Span Loss (with pumps off)           : NA
Estimated Rx Span Loss                  : NA
Tx Span Loss                            : 15.48 dB
Tx OSC Span Loss                        : 15.17 dB
Tx Signal Span Loss                     : 15.48 dB
Tx Span Loss (with pumps off)           : NA
Estimated Tx Span Loss                  : NA
```

Controllers are up, alarms are reviewed, and span-loss is validated.

## NTP server configuration

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communication uses Coordinated Universal Time (UTC). An NTP network usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP distributes this time across the network.

An NTP broadcast client listens for broadcast messages sent by an NTP broadcast server at a designated IPv4 address. The client synchronizes the local clock using the first received broadcast message.

Below are the steps for NTP configuration:

### Procedure

**Step 1** Synchronize Clock with NTP Server

**Step 2** Verify the Status of the External Reference Clock

### What to do next

Troubleshoot NTP Issues

## SNMP configuration (optional)

SNMP is a framework that provides facilities for managing and monitoring network resources on the Internet. SNMP uses UDP for transport and uses port 161 for SNMP messages like walk and 162 for traps. This document lists the SNMP configuration(s) for monitoring the network if needed by the customer. SNMPv3 for walk and SNMP v2c for traps is covered.

### Procedure

**Step 1** Review the SNMP procedures and supported MIBs.

The procedure to configure SNMP on a 1010 device, along with the supported MIBS can be found Configuring SNMP.

**Step 2** Set up SNMPv3 for secure access.

SNMPv3 is the most secure version of the protocol and setting it up can be found in the Setup SNMP Version 3.

For retrieving information from the device using snmpwalk, the following configurations are required.

**Step 3** Configure the SNMP view.

Setup SNMP View: The Setup SNMP view command can block the user with only access to limited Management Information Base (MIB). By default, there is no SNMP view entry exists.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server view testview 1.3.6.1.2 included
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server view testview ospf excluded
```

**Step 4** Create an SNMP group and users.

Create snmp-server group: Create a group to map users with views.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server group testgroup v3 priv notify testview read testview
```

Create snmp users and assign to group.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server user snmpuser testgroup v3 auth sha <authpassword>
 priv aes 128 <privpassword>
```

**Step 5** Verify SNMP configuration and optional tuning.

Note: The show running config shows additional key word encrypted for the passwords, followed by encrypted passwords.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70#sh run snmp
snmp-server user snmpuser testgroup v3 auth sha encrypted 01100F175804575D72 priv aes 128 encrypted
 110A1016141D595F50
```

Below additional configurations are typically used to ensure the queries don't overload the system and also to retrieve information for long names.

**Example:**

```
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server ifmib ifalias long
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server ifindex persist
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server ifmib stats cache
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server logging threshold
RP/0/RP0/CPU0:onc-oltc-225-70(config)#oid-processing 1000
RP/0/RP0/CPU0:onc-oltc-225-70(config)#snmp-server logging threshold pdu-processing 2000
```

Sample configuration for SNMPwalk from the server.

**Example:**

```
snmpwalk -v3 -u snmpuser -l authpriv -a sha -A <authpassword> -x AES -X <privpassword> 10.78.60.234
 .1.3.6.1.2
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS XR Software, Version 25.1.1


 (NCS1010)


Copyright (c) 2013-2025 by Cisco Systems, Inc.
```

```
SNMPv2-MIB::sysObjectID.0 = OID: CISCO-SMI::ciscoProducts.3153

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (38083) 0:06:20.83

SNMPv2-MIB::sysContact.0 = STRING: sirius-dt@cisco.com

SNMPv2-MIB::sysName.0 = STRING: ios

SNMPv2-MIB::sysLocation.0 = STRING: IN, BGL-17-4-Y BLR [12.9629, 77.5775]

SNMPv2-MIB::sysServices.0 = INTEGER: 78

IF-MIB::ifNumber.0 = INTEGER: 16

IF-MIB::ifIndex.2 = INTEGER: 2

IF-MIB::ifIndex.3 = INTEGER: 3

IF-MIB::ifIndex.4 = INTEGER: 4
.....
.....
```

**Step 6** Configure SNMP traps.

For receiving the automatic notifications from the device via snmp traps the following configurations are required as mentioned in SNMP Traps.

Different types of traps can be enabled. Trap types include alarms, configuration changes, authentication framework events, IEEE 802.1X events, and many Cisco-specific notifications.

Sample examples:

**Example:**

```
RP/0/RP0/CPU0:ios(config)#snmp-server traps alarm
RP/0/RP0/CPU0:ios(config)#snmp-server traps power
RP/0/RP0/CPU0:ios(config)#snmp-server traps config
RP/0/RP0/CPU0:ios(config)#snmp-server traps optical
RP/0/RP0/CPU0:ios(config)#snmp-server traps optical-ots
```

For V3 traps, server IP, userid and UDP port are needed as in the example given below.

**Example:**

```
RP/0/RP0/CPU0:ios(config)#snmp-server host <server-ip> traps version 3 priv <userid> udp-port <port#>
```

For V2 traps, server IP, protocol 2c, community name and UDP ports are needed.

**Example:**

```
RP/0/RP0/CPU0:ios(config)#snmp-server host <server-ip> traps version 2c public udp-port <port#>
RP/0/RP0/CPU0:ios(config)#snmp-server community snmpcommunity RO
```

---

The following output shows an SNMP trap received after the listener starts waiting for traps:

```
Received SNMPv2c Trap:

Community: snmpcommunity

From: 10.78.60.234

sysUpTimeInstance = 01:13:42.70

snmpTrapOID.0 = clogMessageGenerated

clogHistFacility.0 = SECURITY-SSHD_SYSLOG_PRX

clogHistSeverity.0 = info(7)

clogHistMsgName.0 = INFO_GENERAL

clogHistMsgText.0 = sshd[64262]: Connection closed by 10.78.60.234 port 58463

clogHistTimestamp.0 = 01:13:42.00


Received SNMPv2c Trap:

Community: public

From: 10.78.60.234

sysUpTimeInstance = 01:13:42.92

snmpTrapOID.0 = clogMessageGenerated

clogHistFacility.0 = SECURITY-SSHD_SYSLOG_PRX

clogHistSeverity.0 = info(7)

clogHistMsgName.0 = INFO_GENERAL

clogHistMsgText.0 = sshd[64760]: Accepted authentication/pam for cisco from 10.78.60.234
port 58685 ssh2

clogHistTimestamp.0 = 01:13:42.00
```

# Day-1 configuration

Direct operators to Cisco Optical Site Manager workflows for day-1 configuration tasks.

Day-1 configuration is performed in Cisco Optical Site Manager.

- Follow the Cisco Optical Site Manager section for detailed workflows.
- Ensure node credentials and IP addresses are available.

Typical day-1 activities.

- Device onboarding and synchronization.
- Topology and service configuration.

# Validate the NCS 1010 setup

Confirm that software, hardware, and licensing are operational.

Perform these checks after initial configuration and before day-1 workflows.

**Before you begin**

Ensure the node is reachable and interfaces are up.

**Procedure**

**Step 1** Verify Smart Licensing status.

**Example:**

```
show license status
```

**Step 2** Run preliminary checks on the default setup.

Use the site checklist for preliminary validation items. Refer to preliminary checks for detailed procedures.

**Step 3** Verify software and hardware status.

**Example:**

```
show platform
show inventory
```

The NCS 1010 is ready for operational use or day-1 configuration in Cisco Optical Site Manager (COSM).

# Back up the current configuration

The ability to recover from a disaster is an essential part of any system maintenance plan. We recommend you backup the configurations in a secure remote location and verify that the transfer is a success, both before and after upgrade.

**Before you begin**

Verify connectivity to the local hard disk or remote server.

### Procedure

**Step 1** Copy the running configuration to the local hard disk.

**Example:**

```
RP/0/RP0/CPU0:ios#copy running-config harddisk:/running_config-<mmddyyyy>
Destination filename [running_config-<mmddyyyy>]?
Building configuration...
[OK]
Verifying checksum... OK
```

**Step 2** Copy the configuration to a remote server.

**Example:**

```
RP/0/RP0/CPU0:ios#scp harddisk:/running_config-<mmddyyyy> <user>:<password>@<ip-address>:<location>
```

**Step 3** Verify that the backup completed successfully.

Confirm the file exists on the local disk and the remote server.

The configuration backup is available for recovery if needed.

### What to do next

Provide this information for Day1 configuration and to bring the network to operational IP's of individual nodes with credentials.

# Troubleshooting

Identify the correct troubleshooting guide based on the symptom.

Troubleshooting coverage areas.

- Hardware alarms and platform issues.
- Data path and optical application alarms.
- Infrastructure alarms and system health.

***Table 16: Troubleshooting entry points***

| Issue type | Primary guide |
|---|---|
| Troubleshoot NCS 1010 setup and upgrade | NCS 1010 troubleshoot guide |
| Data path alarms | Data path alarms guide |
| Optical application alarms | Optical application alarms guide |
| Infrastructure alarms | Infrastructure alarms guide |

*Table 17: Command quick reference*

| Command | Purpose | When to use | Notes |
|---|---|---|---|
| **show alarms brief system active** | Active alarms | During alarm triage | Check severity and timestamps |
| **show controllers osc 0/0/0/0** | Controller status | When OSC issues appear | Verify optical status |
| **show olc span-loss** | Span loss | After topology bring-up | Compare with design values |
| **show ospf neighbor** | OSPF adjacency | Neighbor device issues | Confirm adjacency state |

*Table 18: Alarm triage guide*

| Severity | Action | Notes |
|---|---|---|
| **Major** | Escalate | Follow hardware troubleshooting guide |
| **Minor** | Monitor | Review for recurring issues |

# Cisco IOS XR SMU installation procedures

Use the procedure that matches the software maintenance update workflow required for the selected Cisco IOS XR fixes.

You can install Cisco IOS XR SMUs by using a Golden ISO, the `install source` command, or the `install package add source` command. Use the method that matches the required fix and the reload control needed for the maintenance window.

*Table 19: SMU installation procedures*

| Method | Use case | Procedure |
|---|---|---|
| Using a Golden ISO | Install the Cisco IOS XR software image and selected SMUs in one operation. | Install using a Golden ISO with bug fixes, on page 48 |
| Using the `install source` command | Install a software image or SMU package directly from a device path such as `/harddisk:/`. | Install using the install source command, on page 51 |
| Using the `install package add source` command | Install multiple SMUs together when control over reload timing is required. | Install additional RPMs and bug fixes |

# Install using a Golden ISO with bug fixes

Install a customized Golden ISO (GISO) that includes the Cisco IOS XR software image and selected SMUs in one operation.

A Golden ISO is a customized ISO that includes the standard base image with basic functional components, additional RPMs, SMUs, and configuration files as required. A Golden ISO upgrades the device to a version that has a predefined list of SMUs in a single operation.

**Before you begin**

- Obtain the required Golden ISO for the device platform and Cisco IOS XR release.
- Obtain the expected checksum for the Golden ISO.
- Ensure that the device is reachable from the server that stores the Golden ISO.
- Schedule a maintenance window because the installation can reload the device.

**Procedure**

**Step 1** Verify the checksum of the downloaded Golden ISO, copy the image to the device hard disk, and confirm that the copied file is present.

**Example:**

```
server$ md5sum <giso-file>.iso
server$ scp <giso-file>.iso <username>@<device-ip>:/harddisk:/
RP/0/RP0/CPU0:router#run
[node0_RP0_CPU0:~]$ cd /harddisk\:
[node0_RP0_CPU0:/harddisk:]$ ls -ltra | grep -i <giso-file>.iso
```

Example from the OAS guide:

```
[syedsaah@vxr-sirius-04 Image]$ md5sum ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
44dcd5214add0314116d109918bb926f  ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
[syedsaah@vxr-sirius-04 Image]$ scp ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
cisco@4.33.7.61:/harddisk:/
Password:
ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
       100% 2497MB  85.5MB/s   00:29
RP/0/RP0/CPU0:P2A_DT_07#run
Mon Feb 23 13:29:40.542 IST
[node0_RP0_CPU0:~]$ cd /harddisk\:
[node0_RP0_CPU0:/harddisk:]$ ls -ltra | grep -i ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
-rwxrwxrwx.  1 root  root        2618347520 Feb 23 13:27 ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
```

**Step 2** Verify that the checksum of the copied Golden ISO matches the checksum that was calculated before the copy.

**Example:**

```
[node0_RP0_CPU0:/harddisk:]$ md5sum <giso-file>.iso
```

Example from the OAS guide:

```
[node0_RP0_CPU0:/harddisk:]$ md5sum ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
44dcd5214add0314116d109918bb926f  ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso
```

**Step 3** Install the Golden ISO from `/harddisk:/`.

**Example:**

```
RP/0/RP0/CPU0:router#install replace harddisk:/<giso-file>.iso commit noprompt
```

The install operation runs in the background.

Example from the OAS guide:

```
RP/0/RP0/CPU0:P2A_DT_07#install replace harddisk:/ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso commit
 noprompt
Mon Feb 23 13:31:48.714 IST
Install replace operation 204 has started
Install operation will continue in the background
```

**Step 4** After the node is up, verify the software version and install request status.

**Example:**

```
RP/0/RP0/CPU0:router#show version
RP/0/RP0/CPU0:router#show install request
```

Confirm that the expected Cisco IOS XR version is active, the install request state is **Success**, and the current activity shows that no install operation is in progress.

Example from the OAS guide:

```
RP/0/RP0/CPU0:P2A_DT_07#show version
Mon Feb 23 13:50:15.241 IST
Cisco IOS XR Software, Version 25.1.1 LNT
Copyright (c) 2013-2025 by Cisco Systems, Inc.
Build Information:
Built By     : swtools
Built On     : Fri Feb 20 08:58:11 UTC 2026
Build Host   : iox-ucs-037
Workspace    : /auto/srcarchive12/prod/25.1.1/ncs1010/ws
Version      : 25.1.1
Label        : 25.1.1-Feb27Drop2
cisco NCS1010 (C3758 @ 2.20GHz)
cisco NCS1010-SA (C3758 @ 2.20GHz) processor with 32GB of memory
P2A_DT_07 uptime is 7 minutes
NCS 1010 - Chassis
RP/0/RP0/CPU0:P2A_DT_07#show install request
Mon Feb 23 13:50:29.368 IST
User request: install replace /harddisk:/ncs1010-golden-x86_64-25.1.1-Feb27Drop2.iso commit
Operation ID: 204
State:        Success since 2026-02-23 13:46:53 UTC+05:30
Current activity:    No install operation in progress
The following actions are available:
install package add
install package remove
install package upgrade
install package downgrade
install package replace
install package rollback
install replace
install rollback
install source
install replace reimage
```

**Step 5** Verify the active and committed package summaries.

**Example:**

```
RP/0/RP0/CPU0:router#show install active summary
RP/0/RP0/CPU0:router#show install committed summary
```

Confirm that the expected label, optional packages, mandatory packages with bug fixes, and active or committed fixes are shown.

Example from the OAS guide:

```
RP/0/RP0/CPU0:P2A_DT_07#show install active summary
Mon Feb 23 13:51:05.379 IST
Active Packages:    XR: 156    All: 1400
Label:              25.1.1-Feb27Drop2
XR Software Hash:      3b41e8017f18853a6a9c1a9d5b3463a4c91b07e2cace3b746ef5a755138c3210
Optional Packages                                                          Version
---------------------------------------------------- ---------------------------
xr-bgp                                                                25.1.1v1.0.0-1
xr-healthcheck                                                        25.1.1v1.0.0-1
xr-ipsla                                                              25.1.1v1.0.0-1
xr-is-is                                                              25.1.1v1.0.0-1
xr-lldp                                                               25.1.1v1.0.0-1
xr-mpls-oam                                                           25.1.1v1.0.0-1
xr-netflow-stubs                                                      25.1.1v1.0.0-1
xr-netsim                                                             25.1.1v1.0.0-1
xr-olc                                                                25.1.1v1.0.0-1
xr-ospf                                                               25.1.1v1.0.0-1
xr-perfmgmt                                                           25.1.1v1.0.0-1
xr-track                                                              25.1.1v1.0.0-1
Mandatory Packages With Active Bugfixes                                    Version
---------------------------------------------------- ---------------------------
xr-diskboot                                                           25.1.1v1.0.1-1
xr-ncs1010-core                                                       25.1.1v1.0.1-1
xr-ncs1010-dri                                                        25.1.1v1.0.1-1
xr-ncs1010-forwarder                                                  25.1.1v1.0.1-1
xr-ncs1010-fpd                                                        25.1.1v1.0.2-1
xr-ncs1010-os-oe                                                      25.1.1v1.0.1-1
Active Fixes (selected XR entries):
CSCwn69606: xr-diskboot, xr-ncs1010-dri, xr-ncs1010-os-oe
CSCwq77633: xr-ncs1010-core
CSCwr31650: xr-ncs1010-forwarder
CSCws41649: xr-ncs1010-fpd
CSCws74922: xr-ncs1010-fpd
RP/0/RP0/CPU0:P2A_DT_07#show install committed summary
Mon Feb 23 13:51:31.334 IST
Committed Packages: XR: 156    All: 1400
Label:              25.1.1-Feb27Drop2
XR Software Hash:      3b41e8017f18853a6a9c1a9d5b3463a4c91b07e2cace3b746ef5a755138c3210
Mandatory Packages With Committed Bugfixes                                 Version
---------------------------------------------------- ---------------------------
xr-diskboot                                                           25.1.1v1.0.1-1
xr-ncs1010-core                                                       25.1.1v1.0.1-1
xr-ncs1010-dri                                                        25.1.1v1.0.1-1
xr-ncs1010-forwarder                                                  25.1.1v1.0.1-1
xr-ncs1010-fpd                                                        25.1.1v1.0.2-1
xr-ncs1010-os-oe                                                      25.1.1v1.0.1-1
Committed Fixes (selected XR entries):
CSCwn69606: xr-diskboot, xr-ncs1010-dri, xr-ncs1010-os-oe
CSCwq77633: xr-ncs1010-core
CSCwr31650: xr-ncs1010-forwarder
CSCws41649: xr-ncs1010-fpd
CSCws74922: xr-ncs1010-fpd
```

The Golden ISO software changes are installed and committed on the device.

# Install using the install source command

Install a Cisco IOS XR software image or SMU package from `/harddisk:/` by using the **install source** command.

Use **install source** for the Installing Software image from harddisk workflow. Use this method when you want fewer commands and do not need control over the timing of the reload or restart. This method automatically applies changes, including reload or restart actions as required, without changing the entire image.

If you install SMUs individually, repeat this procedure for each SMU. Each individually installed SMU is treated as a separate transaction.

**Before you begin**

- Obtain the required software image or SMU package for the device platform and Cisco IOS XR release.
- Obtain the expected checksum for the software image or SMU package.
- Ensure that the device is reachable from the server that stores the software image or SMU package.
- Schedule a maintenance window if the installation requires a reload or process restart.

**Procedure**

**Step 1** Copy the software image or SMU package to the device harddisk and verify the checksum of the copied file.

**Example:**

```
server$ scp <smu-package>.tgz <username>@<device-ip>:/harddisk:/
[node0_RP0_CPU0:/harddisk:]$ md5sum <smu-package>.tgz
```

Confirm that the checksum matches the expected checksum before installing the file.

Example from the OAS guide:

```
server$ scp ncs1010-x86_64-25.1.1-CSCwp05477-swtools-2025-10-08-2334.tgz
<username>@<device-ip>:/harddisk:/
[node0_RP0_CPU0:/harddisk:]$ md5sum ncs1010-x86_64-25.1.1-CSCwp05477-swtools-2025-10-08-2334.tgz
4e156140f4481452599c44afbdadd13d  ncs1010-x86_64-25.1.1-CSCwp05477-swtools-2025-10-08-2334.tgz
```

**Step 2** Install the software image or SMU package from `/harddisk:/`.

**Example:**

```
RP/0/RP0/CPU0:router#install source /harddisk:/<smu-package>.tgz
```

Example from the OAS guide:

```
RP/0/RP0/CPU0:router#install source
/harddisk:/ncs1010-x86_64-25.1.1-CSCwp05477-swtools-2025-10-08-2334.tgz
```

**Step 3** Wait for the install request state to change to **Success**, and then commit the installed SMU.

**Example:**

```
RP/0/RP0/CPU0:router#show install request
RP/0/RP0/CPU0:router#install commit
```

If the request shows **Current activity: Await user input** and **install commit** is available, run **install commit**.

Example from the OAS guide:

```
RP/0/RP0/CPU0:router#show install request
Mon Oct 13 07:40:19.516 UTC
User request: install source /harddisk:/ncs1010-x86_64-25.1.1-CSCwp05477-swtools-2025-10-08-2334.tgz
Operation ID: 26.1
State:        Success since 2025-10-13 07:38:28 UTC
Current activity:    Await user input
Time started:        2025-10-13 07:38:28 UTC
The following actions are available:
install package add
install package remove
install package upgrade
install package downgrade
install package replace
install package rollback
install replace
install rollback
install source
install commit
install replace reimage
RP/0/RP0/CPU0:router#install commit
```

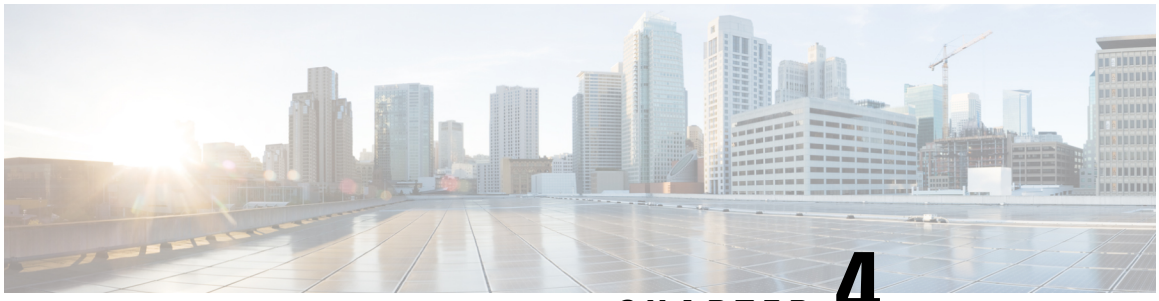
**Step 4** Repeat the copy, checksum, install, status, and commit actions for each SMU that must be installed individually.

Each individually installed SMU is treated as a separate transaction.

---

The Cisco IOS XR software image or SMU package is installed and committed on the device.

To install using package add source, see Install additional RPMs and bug fixes.



CHAPTER 4

# Manage Your Sites with Cisco Optical Site Manager

Use this chapter to prepare, install, and activate Cisco Optical Site Manager, then onboard managed devices.



## Cisco Optical Site Manager

Cisco Optical Site Manager is a software application that aggregates NCS 1000 optical devices at a site, abstracts the site topology for controller or web UI access, and supports software-defined turn-up, operations, and maintenance.

Cisco Optical Site Manager runs on NCS 1000 controller cards. It can operate as a standalone local craft interface, integrate with Cisco Optical Network Controller, or provide an open NETCONF/YANG northbound interface for third-party controllers.

Cisco Optical Site Manager allows you to:

- Aggregate site-level optical devices under a single management view.
- View site topology, inventory, alarms, performance monitoring data, and mechanical layouts for chassis, cards, and passive devices.
- Use operations, administration, and maintenance functions such as connection verification, loopbacks, PRBS, OTDR, and threshold crossing alerts.
- Configure cards and modules for site-level operations.

- Manage NCS 1000 device topologies for standalone and high availability deployments.

Cisco Optical Network Controller can consume the site-level data streamed by Cisco Optical Site Manager and use it for network-level provisioning, monitoring, troubleshooting, topology views, and analytics.

For details about Cisco Optical Site Manager, see Cisco Optical Site Manager Data Sheet.

## Supported configurations

Cisco Optical Site Manager can manage the these NCS 1000 configurations in standalone or high availability deployments.

Supported host configurations include:

- NCS1010 OLT host managing NCS1010, NCS1014, NCS1004, NCS 1001 in a terminal SA configuration.
  - 2-degree pass through NCS1010 (Novara) site in HA configuration
  - NCS1010 ILA and support for greenfield configuration
- NCS1014 host managing NCS1014, NCS1004, and NCS1001.
- NCS1004 host managing NCS1004 and NCS1001 (from NCS 1000 R25.4.1).
- NCS1001 host managing NCS1001 (from 25.4.1, up to two devices).
- Choose the supported deployment configurations based on your network requirements.

  For more information about HA deployment models, see Deployment models for HA in Cisco Optical Site Manager.

# Cisco Optical Site Manager installation workflow

This workflow helps you install and configure Cisco Optical Site Manager. You will set up Cisco Optical Site Manager, configure it for standalone or high availability (HA) operation, manage interfaces, and activate the application as needed.

**Before you begin**

Verify that the installation requirements are met before proceeding. For details, see Cisco Optical Site Manager installation prerequisites for NCS 1000 devices.

Perform these tasks to install and configure Cisco Optical Site Manager on NCS 1010.

**Procedure**

**Step 1** Install Cisco Optical Site Manager on NCS 1010. For more details, see Install Cisco Optical Site Manager on NCS 1010, on page 56 or Install Cisco Optical Site Manager on NCS 1001 or NCS 1004.

**Step 2** Configure Cisco Optical Site Manager in standalone or high availability mode. For more details, see Configure Cisco Optical Site Manager on NCS 1000.

**Step 3** Activate Cisco Optical Site Manager. For more details, see Activate Cisco Optical Site Manager, on page 62.

# Enable NETCONF over SSH for secure host device communication

Enable NETCONF over SSH so that Cisco Optical Site Manager can connect to host devices for configuration and monitoring. Enable NETCONF on each Cisco Optical Site Manager host device.

**Before you begin**

Follow these steps to enable NETCONF:

**Procedure**

**Step 1** Enter the configuration mode using the **configure terminal** command.

**Example:**

```
RP/0/RP0/CPU0:ios#configure terminal
```

**Step 2** Enable NETCONF-YANG agent over SSH connection using the **netconf-yang agent ssh** command.

**Example:**

```
RP/0/RSP0/CPU0:ios(config)# netconf-yang agent ssh
```

**Step 3** Configure the device to use SSH protocol v2 using the **ssh server v2** command.

**Note**
Only SSH version 2 is supported.

**Example:**

```
RP/0/RP0/CPU0:ios(config)# ssh server v2
```

**Step 4** Set the rate limit for incoming SSH connection requests to 600 per minute using the **ssh server rate-limit** *rate-limit* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config)# ssh server rate-limit 600
```

**Step 5** Set the SSH session limit to 110 using the **ssh server session-limit** *session-limit* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config)# ssh server session-limit 110
```

**Step 6** Enable SSH server access in the default VRF using the **ssh server vrf** *vrf-name* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config)# ssh server vrf default
```

**Step 7** Enable NETCONF over SSH in the default VRF using the **ssh server netconf vrf** *vrf-name* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config)# ssh server netconf vrf default
```

**Step 8** Enable NETCONF protocol over SSH connection using the **ssh server netconf** command.

**Example:**

```
RP/0/RP0/CPU0:ios(config)# ssh server netconf
```

**Step 9** Commit the changes using the **commit** command.

After you enable NETCONF, Cisco Optical Site Manager can establish a secure communication with the device using the NETCONF protocol over SSH.

This example describes the commands to enable NETCONF over SSH:

```
RP/0/RP0/CPU0:ios# configure terminal
                RP/0/RSP0/CPU0:ios(config)# netconf-yang agent ssh
                RP/0/RP0/CPU0:ios(config)# ssh server v2
                RP/0/RP0/CPU0:ios(config)# ssh server rate-limit 600
                RP/0/RP0/CPU0:ios(config)# ssh server session-limit 110
                RP/0/RP0/CPU0:ios(config)# ssh server vrf default
                RP/0/RP0/CPU0:ios(config)# ssh server netconf vrf default
                RP/0/RP0/CPU0:ios(config)# ssh server netconf
```

### What to do next

Configure static route on peer devices

# Install Cisco Optical Site Manager on NCS 1010

Cisco Optical Site Manager can be installed on NCS 1010 in these two ways:

1. As part of a Golden ISO (GISO) image where the Cisco Optical Site Manager package is already bundled with Cisco IOS XR image.
2. On NCS 1010 where Cisco IOS XR is already installed, you can install Cisco Optical Site Manager as an optional software component.

In the second scenario, you must manually install the Cisco Optical Site Manager software using the provided *.rpm* files. You can download the Cisco Optical Site Manager software image from the Software Download page.

**Before you begin**

Download the *NCS1010/NCS1020 and NCS1014 IOS XR Software optional-rpms* optional package from Software Download page.

Follow these steps to install Cisco Optical Site Manager:

### Procedure

**Step 1** Copy all the *.rpm* files in the **cosm** folder of the downloaded package to the device storage.

```
RP/0/RP0/CPU0:vmxCisco_T1#mkdir /misc/disk1/cosm
RP/0/RP0/CPU0:vmxCisco_T1# scp user@[RPM_SERVER]:/nobackup/ncs1010_image/*.rpm    /misc/disk1/cosm
Password: ********
```

**Step 2** Add the Cisco Optical Site Manager package source folder to the Cisco IOS XR software management system in synchronous mode using the **install package add source file:** *rpm-folder* **synchronous** command.

**Example:**

```
RP/0/RP0/CPU0:ios#install package add source file:/harddisk:/cosm/ synchronous
Install add operation 2.1.1 has started
```

Installation in synchronous mode is optional and runs in the foreground and waits for the operation to complete before returning control to the user.

**Step 3** Install the Cisco Optical Site Manager RPM in synchronous mode using the **install package add** *package-name* **synchronous** command.

**Example:**

```
RP/0/RSP0/CPU0:ios#install package add xr-cosm synchronous
```

**Step 4** Apply the latest changes in synchronous mode on the NCS 1000 device using the **install apply restart synchronous** command.

**Example:**

```
RP/0/RP0/CPU0:ios#install apply restart synchronous
```

The latest changes are applied to all processes, including the impacted processes.

**Step 5** Commit the changes using the **install commit synchronous** command.

**Example:**

```
RP/0/RP0/CPU0:ios#install commit synchronous
```

**Step 6** Verify that Cisco Optical Site Manager rpm is installed using the **show install active | include xr-cosm** command.

**Example:**

```
RP/0/RP0/CPU0:ios#show install active | include xr-cosm
Fri Nov 14 11:07:17.877 UTC
xr-cosm                                                    25.1.1v1.0.2-1
```

Cisco Optical Site Manager is installed on the device.

This example describe the commands to install Cisco Optical Site Manager:

```
RP/0/RP0/CPU0:ios#install package add source file:/harddisk:/cosm/ synchronous
RP/0/RSP0/CPU0:ios#install package add xr-cosm synchronous
RP/0/RP0/CPU0:ios#install apply restart synchronous
RP/0/RP0/CPU0:ios#install commit synchronous
RP/0/RP0/CPU0:ios#sh install active | include xr-cosm
Fri Nov 14 11:07:17.877 UTC
xr-cosm                                                    25.1.1v1.0.2-1
```

### What to do next

Configure Cisco Optical Site Manager in Standalone or High Availability mode.

# Configure Cisco Optical Site Manager in standalone mode for NCS 1010

Cisco Optical Site Manager can be configured in standalone mode on a single NCS 1010 controller card.

The configuration involves setting up Cisco Optical Site Manager interfaces, defining management interface parameters, and establishing user credentials for access.

**Before you begin**

Verify that these configurations are enabled before configuring Cisco Optical Site Manager in standalone mode on NCS 1010:

- Enable NETCONF over SSH for secure host device communication, on page 55
- Configure static routes on peer devices.
- Keep these configuration parameters at their default values unless there is a specific need to change them.

Follow these steps to configure Cisco Optical Site Manager in standalone mode:

### Procedure

**Step 1** Enter into the IOS XR and COSM configuration mode using the **configure terminal** and **cosm** commands.

**Example:**

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RSP0/CPU0:ios(config)# cosm
```

**Step 2** Configure the interface of the device running the Cisco Optical Site Manager by using **mgmt-interface-name MgmtEth** *R/S/I/P* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# mgmt-interface-name Loopback1
```

This is the interface used to reach Cisco Optical Site Manager. This interface can be a physical interface or a loopback interface. For a standalone Cisco Optical Site Manager deployment, use the same interface for device onboarding.

**Step 3** Configure the username using the **user-name** *user name* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# user-name cisco
```

**Note**
The username must match the username of the host device.

**Step 4** Configure the password using the **user-password** *password* command.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# user-password ***
```

**Note**
The Cisco Optical Site Manager username and password can be the same as, or different from, the XR host device credentials. These credentials are saved in the Cisco Optical Site Manager application database and are not displayed in the XR show running-config output.

**Step 5** Commit the changes and exit the configuration modes using the **commit** and **end** commands.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm) commit
RP/0/RP0/CPU0:ios(config-cosm) end
```

**Step 6** Verify the configuration using the **show running-config cosm** command.

**Example:**

This example shows the standalone Cisco Optical Site Manager configuration.

```
RP/0/RP0/CPU0:ios#show running-config cosm
Fri Oct 18 12:53:47.056 UTC
cosm
 mgmt-interface-name Loopback1
!
```

The configured *user-name* and *user-password* are not displayed in the output of the **show running-config cosm** command.

Cisco Optical Site Manager is configured in the standalone mode.

### What to do next

Enable or disable Cisco Optical Site Manager north-bound interfaces

# High availability for NCS 1000

Cisco Optical Site Manager High Availability (HA) provides continuous management and operational resilience for Cisco optical devices. By deploying two instances, one as Active and the other as Standby, HA ensures that device management remains uninterrupted even if one instance fails.

### How does Cisco Optical Site Manager high availability ensure operational continuity?

Cisco Optical Site Manager High Availability (HA) provides a robust solution for managing device operations by utilizing dual application instances and specialized network interfaces.

The main features of Cisco Optical Site Manager high availability include:

- Two devices must be able to communicate with each other, allowing their respective Cisco Optical Site Manager instances to coordinate application roles (active or standby) and manage operations.
- Each device requires a Cisco Optical Site Manager management interface configured with the same IP address, starting in a shutdown state. This interface automatically transitions between UP and DOWN states based on whether the device is active or standby.
- A dedicated Cisco Optical Site Manager redundancy interface is used to establish the high availability communication channel and typically serves as the device's management interface.
- When in the active role, Cisco Optical Site Manager binds the HA server to the redundancy interface's IP address on port 5454.
- When in the Standby role, Cisco Optical Site Manager connects to the peer's redundancy interface IP address on port 5454 to communicate with the active instance.

### HA roles and interfaces

- **Active role**: manages all device operations and binds the HA server to its redundancy interface and port.
- **Standby role**: monitors the active instance and connects to the peer's redundancy IP and port. It is ready to take over if needed.
- **Redundancy interface**: network interface used solely for HA communication between Cisco Optical Site Manager instances.

- **Management interface**: interface with the same IP address on both devices, managed automatically depending on the instance role.

**Note** High availability is not supported on NCS 1004 and NCS 1001.

## Configure Cisco Optical Site Manager in high availability on NCS 1000

Configure High Availability (HA) on Cisco Optical Site Manager is to enable fast recovery from faults in the optical transport network and to maintain service continuity by switching to standby components when active ones fail.

Cisco Optical Site Manager HA configuration requires these interfaces configured.

- `cosm mgmt-interface-name`: This interface must be configured with same IP address on both Cisco Optical Site Manager active and standby devices. This interface must be configured in a shutdown state and will automatically transition between UP and DOWN states based on the role (Active or Stand-By) assigned by the application.
- `cosm redundancy interface-name`: This interface must be configured with the redundancy interface and is used to establish the high availability communication channel and is typically the interface used for device management.
- `redundancy gateway-ip`: Specifies the gateway IP address (for example, *10.0.2.1*) used by Cisco Optical Site Manager to reach peer devices or for routing HA traffic in environments where a direct path to the peer is not available.

**Before you begin**

Verify that Cisco Optical Site Manager rpm is installed. For more details, see Install Cisco Optical Site Manager on NCS 1010, on page 56.

Follow these steps to configure Cisco Optical Site Manager in HA mode on a NCS 1010 or NCS 1014 device:

**Procedure**

**Step 1** Enter into the IOS XR and Cisco Optical Site Manager configuration modes.

**Example:**

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RSP0/CPU0:ios(config)# cosm
```

**Step 2** Configure the gateway IP address.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# redundancy gateway-ip 192.168.22.1
```

**Step 3** Configure the peer IP address.

This is the IP address of the peer device running the Cisco Optical Site Manager HA instance.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# redundancy peer-ip 192.168.22.2
```

For releases 24.x.x and 25.x.x, verify that the *redundancy interface-name* IP address and the *redundancy peer-ip* address are not substrings of each other. For example, configuring 10.0.1.1 as the *redundancy interface-name* and 10.0.1.10 or 10.0.1.101 as the *redundancy peer-ip* (or vice-versa) causes Cisco Optical Site Manager HA to fail during startup.

**Step 4** Configure the HA interface name.

This is the interface of the device running the Cisco Optical Site Manager HA instance, which is used for all HA traffic.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# redundancy interface-name MgmtEth 0/RP0/CPU0/2
```

**Step 5** Commit the changes and exit all configuration modes.

**Example:**

```
RP/0/RP0/CPU0:ios(config-cosm)# commit
RP/0/RP0/CPU0:ios(config-cosm)# end
```

**Step 6** Perform the steps 1 to 6 on the second Cisco Optical Site Manager host device.

**Step 7** Verify the HA configuration on both host devices.

**Example:**

```
RP/0/RP0/CPU0:ios#show cosm status
Fri Nov 14 10:26:44.215 UTC
COSM state: CLIENT_REGISTERED
AppMgr app state: UNKNOWN
AppMgr container state: UNKNOWN
Container status: Not present
Last error: 'Appmgr' detected the 'warning' condition 'Application not found'
Role: UNKNOWN
```

---

You can view the active and standby application status in the **Device Software** section of the **Software Manager** menu.

**Note** If the HA node is on loopback, the MAC address of the HA device is displayed as **N/A** in the **Devices** section of the **Device Configuration** page.

This example explains how to configure Cisco Optical Site Manager HA on a NCS 1010 or NCS 1014 device.

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RSP0/CPU0:ios(config)# cosm
RP/0/RP0/CPU0:ios(config-cosm)# redundancy gateway-ip 10.0.2.1
RP/0/RP0/CPU0:ios(config-cosm)# redundancy peer-ip 10.0.1.12
RP/0/RP0/CPU0:ios(config-cosm)# redundancy interface-name MgmtEth 0/RP0/CPU0/2
RP/0/RP0/CPU0:ios(config-cosm)# commit
RP/0/RP0/CPU0:ios(config-cosm)# end
RP/0/RP0/CPU0:ios#show cosm status
Fri Nov 14 10:26:44.215 UTC
COSM state: CLIENT_REGISTERED
AppMgr app state: UNKNOWN
AppMgr container state: UNKNOWN
Container status: Not present
Last error: 'Appmgr' detected the 'warning' condition 'Application not found'
Role: UNKNOWN
```

### What to do next

Enable or disable Cisco Optical Site Manager north-bound interfaces

### HA commands for Cisco Optical Site Manager

These commands are used to configure HA in Cisco Optical Site Manager on a NCS 1000 device.

| Command | Description |
|---|---|
| **configure** | Enters global configuration mode. |
| **cosm user-name <username>** | Configures Cisco Optical Site Manager application username. |
| **cosm user-password <password>** | Configures Cisco Optical Site Manager application password. |
| **cosm mgmt-interface-name <type> <number>** | Configures the Cisco Optical Site Manager management interface. All Cisco Optical Site Manager NBI services (web UI, NETCONF, RESTCONF) are available on this interface. |
| **cosm redundancy interface-name <type> <number>** | Configures Cisco Optical Site Manager high availability interface. The interface is used to communicate with the peer device. |
| **cosm redundancy peer-ip <IP-address>** | Configures the IP address of the peer device, where other Cisco Optical Site Manager is running. |
| **cosm redundancy gateway-ip <IP-address>** | Configures the IP address of a target device that is always reachable by both devices hosting Cisco Optical Site Manager in high availability. Configuring the same gateway IP on both devices is strongly recommended.<br>Cisco Optical Site Manager uses this target device to perform checks in certain high availability scenarios. The target device must be different from the **cosm redundancy peer-ip**. The target device may be the subnet gateway, the multilayer switch connecting the two devices, or another suitable device. |
| commit | Commits the changes. |
| end | Exits the global configuration mode. |

# Activate Cisco Optical Site Manager

After configuration is complete, activate Cisco Optical Site Manager to enable the application.

After configuring Cisco Optical Site Manager in standalone or high availability mode, including setting management interfaces, user credentials, and optional features like auto-onboarding, the application remains inactive until explicitly activated.

Cisco Optical Site Manager activation takes about 11 minutes on the NCS 1001 and about eight minutes on the NCS 1004 to initialize.

**Important** The configuration of interfaces used by Cisco Optical Site Manager should not be changed after activation.

### Before you begin

- Before activating Cisco Optical Site Manager in HA mode, verify that these parameter values are same on both host devices, if configured.
  - *netconf (optional)*
  - *restconf (optional)*
  - *webui (optional)*
  - *user-name*
  - *user-password*
- All the Cisco NCS 1000 devices on the network are reachable from the device hosting Cisco Optical Site Manager.
- SSH is configured on all the devices.
- Netconf-Yang agent is configured to use SSH for communication.
- The SSH rate limit is set to 600.
- Before Release 24.3.1, use the *MgmtEth0/RP0/CPU0/1* interface for auto-onboarding of subtended devices. The interface uses IP addresses *192.168.1.1/30* and *192.168.1.2/30*. From Release 26.1.1, this requirement does not apply.
- Before Release 26.1.1, ensure that static routes are added on devices that belong to different subnets or configired as peer devices. For more details, see Configure static routes on peer devices.

Follow these steps to activate Cisco Optical Site Manager.

### Procedure

**Step 1** Activate Cisco Optical Site Manager using the **cosm activate** command.

**Example:**

```
RP/0/RP0/CPU0:ios# cosm activate
```

**Step 2** Verify the status of the application using the **show cosm status** command.
It may take a few minutes to activate Cisco Optical Site Manager.

- After activating, wait for few minutes before logging in to the Cisco Optical Site Manager GUI.
- Upon successful activation, the application transitions to an active state. Status commands display APP_ACTIVATED and ACTIVATED states.

This example shows the status of Cisco Optical Site Manager configured in standalone mode.

```
RP/0/RP0/CPU0:OLT-2#show cosm status
Fri Oct 18 13:06:09.862 UTC
COSM state: APP_ACTIVATED
AppMgr app state: ACTIVATED
```

```
AppMgr container state: RUNNING
Container status: Up 3 weeks
Last error: No error
COSM version: 24.3.1.D0186
```

This example shows the status of Active instance of the Cisco Optical Site Manager configured in HA mode.

```
RP/0/RP0/CPU0:HAN-1#show cosm status
Thu Oct 30 10:21:25.374 UTC
COSM state: APP_ACTIVATED
AppMgr app state: ACTIVATED
AppMgr container state: RUNNING
Container status: Up 2 days
Last error: No error
COSM version: 25.1.1.R0366
Redundancy role: ACTIVE (connected standby 2.2.2.2-COSM)
```

This example shows the status of Standby instance of the Cisco Optical Site Manager configured in HA mode.

```
RP/0/RP0/CPU0:HAN-2#show cosm status
Thu Oct 30 10:23:01.366 UTC
COSM state: APP_ACTIVATED
AppMgr app state: ACTIVATED
AppMgr container state: RUNNING
Container status: Up 2 days
Last error: No error
COSM version: 25.1.1.R0366
Redundancy role: STANDBY (connected active 1.1.1.1-COSM)
```

### What to do next

- Login to Cisco Optical Site Manager
- Auto onboarding of the NCS 1001 device hosting Cisco Optical Site Manager does not complete because the XR device communicates with the third-party docker through the east-west interface. To onboard a NCS 1001 device, manually add it in Cisco Optical Site Manager using the east-west interface. For more details, see Add a device.
- Import a Cisco Optical Network Planner configuration file.

# Onboarding models for Cisco Optical Site Manager

Cisco Optical Site Manager supports two onboarding models that determine where device configuration originates.

- Configure the complete data path, including circuits, in Cisco IOS XR, and then onboard the device to Cisco Optical Site Manager.
- Perform day-0 configuration and prerequisites on NCS1010, and then push data path configuration from Cisco Optical Site Manager using Cisco Optical Network Planner initial installation parameters.

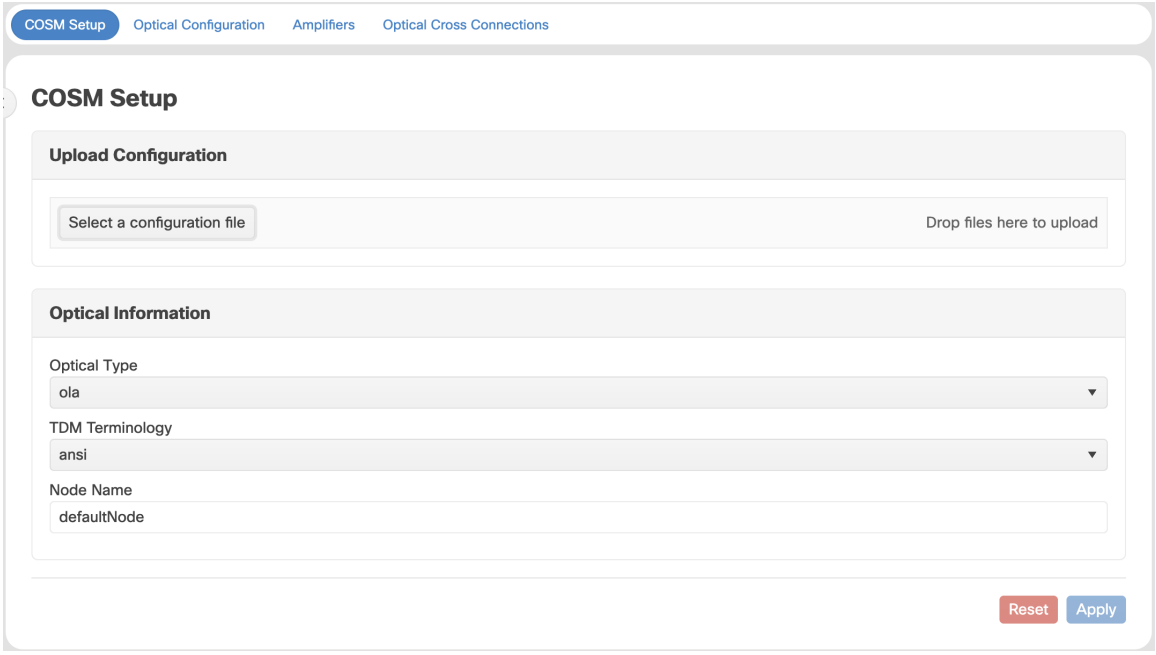
# Import a Cisco Optical Network Planner configuration file

Use this task to import a Cisco Optical Network Planner NETCONF file (.xml) into Cisco Optical Site Manager to configure device parameters automatically.

If you have a NETCONF file (.xml) exported from Cisco Optical Network Planner (Cisco ONP), you can import it to Cisco Optical Site Manager. This file includes:

- Node, shelf, card type, and port information, including wavelength
- Pluggable Port Module (PPM), OTN, and FEC parameters
- Degree, IPC, and link-related information
- Fiber attributes and other network parameters

***Figure 8: Upload Configuration***




### Before you begin

Ensure that:

- The NETCONF file (.xml) contains these parameters available on Cisco Optical Site Manager:
  - device name
  - uid
  - rack id
  - chassis/passive unit id

- Ensure the Cisco Optical Site Manager site name (in the CONP XML file or any other location) does not contain the string *IP*. If this string appears in the site name, network discovery in Cisco Optical Network Controller does not work correctly.
- Cisco Optical Site Manager is newly activated with no devices added to it.
- The Cisco Optical Network Planner configuration file does not include any Optical Cross-Connects.
- Log into Cisco Optical Site Manager.

**Procedure**

**Step 1** Click **Optical Setup** in the left panel.

**Step 2** Click the **Node Setup** tab.

**Step 3** In the **Upload Configuration** section, click **Select a configuration file**.

a) Navigate to the location where the NETCONF file (.xml) is present and select it.
b) Click **Yes**.
c) Click **Upload**.
A confirmation message appears after the upload is complete.

**Step 4** Verify these configuration before adding a device:

a) Click **Optical Setup**.
b) In the **Optical Configuration** and **ANS Parameters** tabs, verify the successful configuration of CONP XML data onto the device.

# Prerequisites for devices managed by Cisco Optical Site Manager

Verify these prerequisites are met:

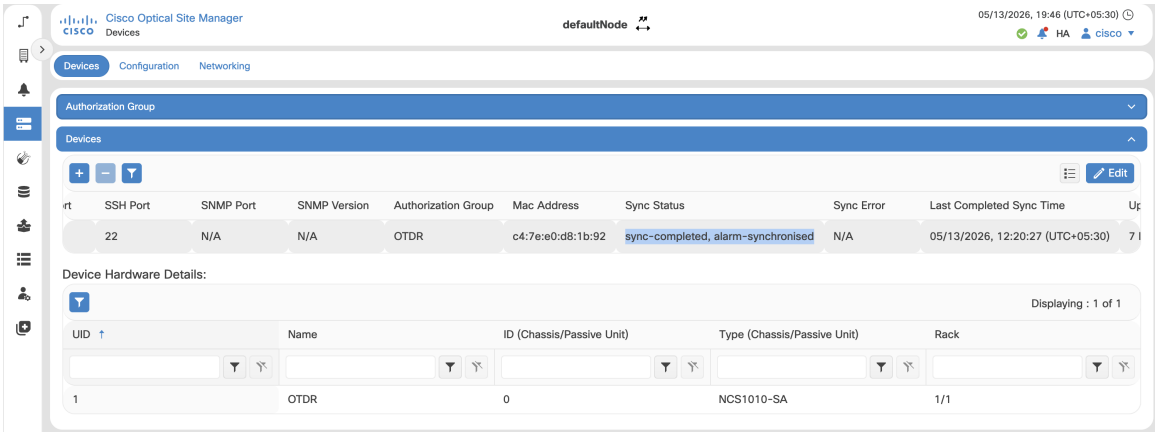
- Device reachability from the Cisco Optical Site Manager host device Cisco IOS XR Linux shell.
- SSH server is configured. Example settings include `ssh server rate-limit 600`, `ssh server session-limit 110`, `ssh server v2`, `ssh server vrf default`, and `ssh server netconf vrf default`.
- NETCONF YANG agent is configured with SSH enabled, for example `netconf-yang agent` and `ssh`.
- The device node types must match TXP, OLT or ILA.
- Confirm that the physical cabling on the device matches the Cisco Optical Site Manager Node Functional View.
- Verify that the rack positioning, degree, IPC and NFV views are aligned with the designed network of Cisco Optical Network Planner.

# Synchronize devices in Cisco Optical Site Manager

Synchronization is essential for the effective management of devices by Cisco Optical Site Manager, ensuring accurate status, timely alarms, and proper operational visibility.

Complete this task after importing the Cisco Optical Network Planner XML.

***Figure 9: Synchronize devices***




**Before you begin**

- Edit one device at a time and wait for synchronization to complete before updating the next device.
- Devices are onboarded and reachable from the Cisco Optical Site Manager host.

Follow these steps to synchronize devices.

## Procedure

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

The **Device Configuration** page appears.

**Step 2** In the **Devices** area, click **Authorization Group** to expand it.

**Step 3** Click **Add Auth Group**.

**Step 4** Enter a name in **Authorization Group Name** and the device credentials in the **Remote Name** and **Remote Password** fields.

**Step 5** Click **Add**.

The new authorization group is added to the table.

**Note**
If the devices to be managed do not share same credentials, you must create additional authorization groups to match each unique credential set. This ensures that Cisco Optical Site Manager can authenticate and manage each device securely according to its configuration.

**Step 6** Expand the **Devices** section, then click **Edit**.

**Step 7** Update these fields of the device to be managed by Cisco Optical Site Manager.

- **IP Address**
- **Authorization Group**
- **Device (XR) Netconf Port** (default 830)
- **Device (XR) SSH Port** (default 22)

**Note**

- Keep the Cisco Optical Site Manager NETCONF port and the device XR NETCONF port at their default values. If either port is required to be changed, ensure that the Cisco Optical Site Manager NETCONF port and the device XR NETCONF port use different values.

Wait for sync status to complete for all the devices

**Step 8** Wait until the **Sync Status** of all the devices is *sync-completed, alarm-synchronized state*.

**Step 9** Verify physical connectivity to confirm that all cabling is correct and to prevent installation errors.

For details about connection verification, see Connection verification.

---

Devices are synchronized and ready for operational monitoring.

# TACACS+ authentication

Use the Cisco Optical Site Manager configuration guide to configure TACACS authentication.

For details about TACACS authentication, see TACACS+ authentication.

# Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Cisco Optical Site Manager Smart Licensing is honor based, and license utilization is based on the number of active line cards managed by Cisco Optical Site Manager.

Supported Smart Licensing modes include:

- **Smart Transport:** Enables Cisco devices to send license usage information directly to Cisco Smart Software Manager (CSSM) over the internet.
- **CSLU:** Enables Cisco devices to send license usage information through Cisco Smart Licensing Utility (CSLU) without direct connectivity to CSSM.
- **Offline:** Enables Cisco devices to manage license usage locally without connectivity to CSSM.

For details about Smart Licensing, see Smart licensing for Cisco Optical Site Manager.

# Cisco Optical Site Manager software maintenance update

Use a Cisco Optical Site Manager software maintenance update (SMU) to update the Cisco Optical Site Manager application with the fixes and enhancements included in the SMU package. The Cisco Optical Site Manager image is bundled as an IOS XR RPM. Therefore, any Cisco Optical Site Manager SMU is delivered as an IOS XR SMU.

Before you install a Cisco Optical Site Manager SMU, review these points:

- The Cisco Optical Site Manager base installation must already be available on the host device.
- In a high availability deployment, install the SMU on the standby instance before installing it on the active instance.
- The SMU installation reloads the controller of the host device, which can interrupt Cisco Optical Site Manager access during the update.

For installing the Cisco Optical Site Manager SMU, see Cisco IOS XR SMU installation procedures, on page 47.

# Troubleshooting

Cisco Optical Site Manager diagnostics offer robust tools for troubleshooting issues by collecting and organizing operational data from your managed devices.

You can choose the applicable log types and devices and download the collected data as a ZIP file. Key features and capabilities include:

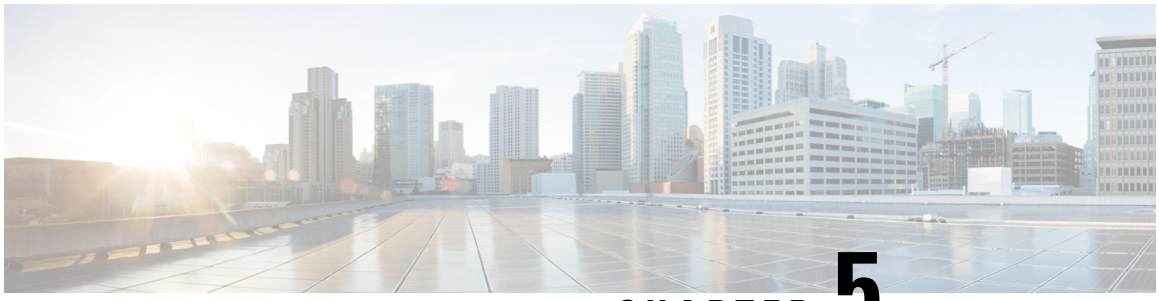
- **Customizable Log Selection:** You can choose specific log types and devices to tailor the diagnostic data to your troubleshooting needs.
- **Download Option:** All selected logs can be downloaded as a ZIP archive, simplifying data sharing.
- **Collected Data Types:**
  - Alarms
  - Audit logs
  - Operational conditions
  - Device inventory
  - Device diagnostics

For more details about Cisco Optical Site Manager diagnostics, see Diagnostics.

# Outcome

After completing this chapter, the node or Cisco Optical Site Manager is ready for Cisco Optical Network Controller onboarding. The Cisco Optical Site Manager instance IP addresses and credentials are available for Cisco Optical Network Controller onboarding and management.

Outcome



CHAPTER 5

# Operate Your Network with Cisco Optical Network Controller

Use this chapter to complete the installation of the Cisco Optical Network Controller, onboard the Cisco Optical Site Manager, provision circuits, and perform validation and troubleshooting workflows.



## Cisco Optical Network Controller

### Core capabilities

Cisco Optical Network Controller operates as a provisioning network controller for Cisco optical networks. The controller delivers these operational outcomes.

- Centralizes onboarding of Cisco Optical Site Manager nodes.
- Collects inventory and topology data from managed Cisco Optical Site Manager nodes.
- Creates and deletes optical circuits through the Service Manager application.
- Monitors topology changes and service updates.
- Unifies topology, alarm, and performance monitoring views.

## Install Cisco Optical Network Controller

The installation establishes the controller platform for user management, node onboarding, and circuit provisioning and monitoring.

**Before you begin**

- Verify that you have a Cisco account and a valid license agreement to download images.

- Identify whether this is a new deployment or a geo-redundant deployment.

Follow these steps to install Cisco Optical Network Controller.

**Procedure**

**Step 1** Download these installation files from Software Download.

- Download the `.ova` image for a new installation.
- Download the `.tar` system pack image for upgrading Cisco Optical Network Controller to a newer version.
- Download the `.tar` service pack image for updating an existing Cisco Optical Network Controller installation with bug fixes and enhancements.

For details about installation requirements, see Installation Requirements.

**Step 2** Install Cisco Optical Network Controller using the OVA workflow.

a) Review the deployment prerequisites in the installation guide.
b) Deploy the OVA in VMware vSphere and complete the installation wizard.

For details about the OVA workflow, see Install Cisco Optical Network Controller Using VMware vSphere.

**Step 3** Plan for the installation and deployment of geo-redundant Cisco Optical Network Controller.

a) Review Install and deploy geo-redundant Cisco Optical Network Controller.
b) Review Upgrade a standalone deployment to a geo-redundant deployment.

For details about switching active and standby roles, see Perform a switchover in a geo-redundant Cisco Optical Network Controller deployment.

Cisco Optical Network Controller is installed and ready for the required deployment model.

# Upgrade a standalone Cisco Optical Network Controller deployment

Upgrade the standalone deployment so that Cisco Optical Network Controller runs the required software version.

**Before you begin**

- Confirm that the target release is supported for the deployment.
- Download the required upgrade image from Cisco Software Download.

Follow this step to upgrade the standalone deployment.

**Procedure**

Upgrade the standalone deployment to the new Cisco Optical Network Controller version.

For details about upgrades, see Upgrade a Standalone Deployment of Cisco Optical Network Controller to a new version.

The standalone Cisco Optical Network Controller deployment is upgraded to the target version.

# Prepare for Cisco Optical Network Controller rollback scenarios

Rollback preparation helps you restore Cisco Optical Network Controller to a previous version when a valid database backup is available.

**Before you begin**

Follow this step to prepare for rollback scenarios.

**Procedure**

Prepare for rollback scenarios.

- Back up the database before upgrades.
- Install the older release using the matching OVA file when rollback is required.
- Restore the database backup after the installation completes.

**Note**
Direct downgrades to older releases are not supported by Cisco Optical Network Controller. You can revert to a previous version only if a backup of the target Cisco Optical Network Controller database was created before the upgrade. For more details, see Backup and Restore Database.

For detailed instructions, see Backup and Restore Database.

The rollback prerequisites are identified before the Cisco Optical Network Controller upgrade.

# Install a Cisco Optical Network Controller service pack

Install a service pack to update an existing Cisco Optical Network Controller deployment with bug fixes and enhancements.

**Before you begin**

- Verify that the service pack is compatible with the installed Cisco Optical Network Controller version.
- Download the required service pack image from Cisco Software Download.

Follow this step to install a service pack.

### Procedure

Install a service pack to update your Cisco Optical Network Controller with bug fixes and enhancements.

To install a service pack, see Install a Cisco Optical Network Controller service pack.

The Cisco Optical Network Controller service pack is installed.

# Operating Cisco Optical Network Controller

The workflow assumes Cisco Optical Network Controller is installed and reachable in the management network.

### Summary

The process outlines the steps for administrators and operators to create users, onboard Cisco Optical Site Manager nodes, validate the discovery process, and provision circuits.

### Workflow

The stages outline the complete workflow for operating the Cisco Optical Network Controller. Each stage must be completed before the next one begins to prevent circuit provisioning errors.

1. Stage 1 — Log in with the administrator credentials created during installation and create users.
   - For details about login, see Log in to Cisco Optical Network Controller, on page 75.
   - For details about creating users, see Create users in Cisco Optical Network Controller.
2. Stage 2 — Onboard Cisco Optical Site Manager by Adding nodes using the interface or bulk import with Excel.

   For details about onboarding, see Onboard Cisco Optical Site Manager nodes in Cisco Optical Network Controller.
3. Stage 3 — Validate topology and inventory.
   - Confirm Discovery Completed and Connected status for each node.
   - Review topology maps and site inventory views.

   For details about validation, see Validate Cisco Optical Site Manager inventory discovery and network topology.
4. Stage 4 — Create and monitor circuits.
   - Use Service Manager to provision optical channel circuits.
   - Monitor circuit status and alarms using the monitoring workspace.

   For details about provisioning, see Provision CPCE services.

# Log in to Cisco Optical Network Controller

Follow these steps to log into Cisco Optical Network Controller:

**Procedure**

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

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

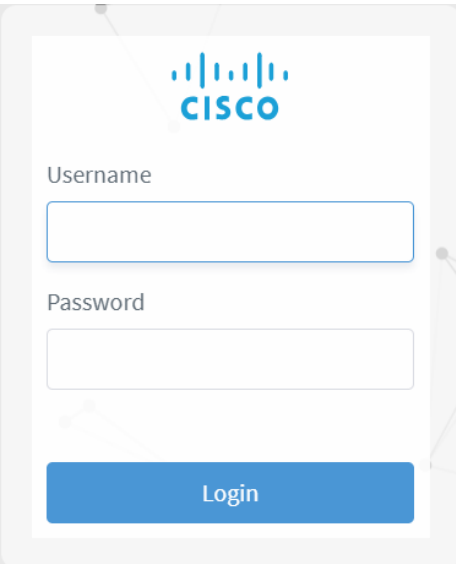
The browser displays the login page.

**Step 2** Enter the username and password.

Username and password are provided by your system administrator.

**Step 3** Click **Login**.

***Figure 10: Log into Cisco Optical Network Controller***




# Create users in Cisco Optical Network Controller

Create a local user account in Cisco Optical Network Controller and define the user's credentials, permissions, and status.

After the initial installation, use the administrator credentials established during setup to complete this task. Cisco Optical Network Controller provides these role levels.

*Table 20: User access permisisons levels*

| Role | Permissions |
|---|---|
| Admin | No restrictions. |
| Supervisor | Similar to admin, but a supervisor user cannot perform user management and check logs. |
| Readonly | Can check data, but cannot provision resources. |
| Internal | Use this role during triage or troubleshooting to collect debug logs. We recommend using it only under the supervision of the Cisco Technical Assistance Center (TAC). |

**Before you begin**

Before you begin:

- Confirm the virtual IP used by Cisco Optical Network Controller.
- Have the administrator username and password available.

Follow these steps to create users.

**Procedure**

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

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

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

**Step 4** Enter and confirm the password.

**Step 5** Select the check box in the **Access Permissions** section to choose the access level for the user.

For more details about permisisons levels, see the Table 20: User access permisisons levels, on page 76 table.

*Figure 11: Local Users*

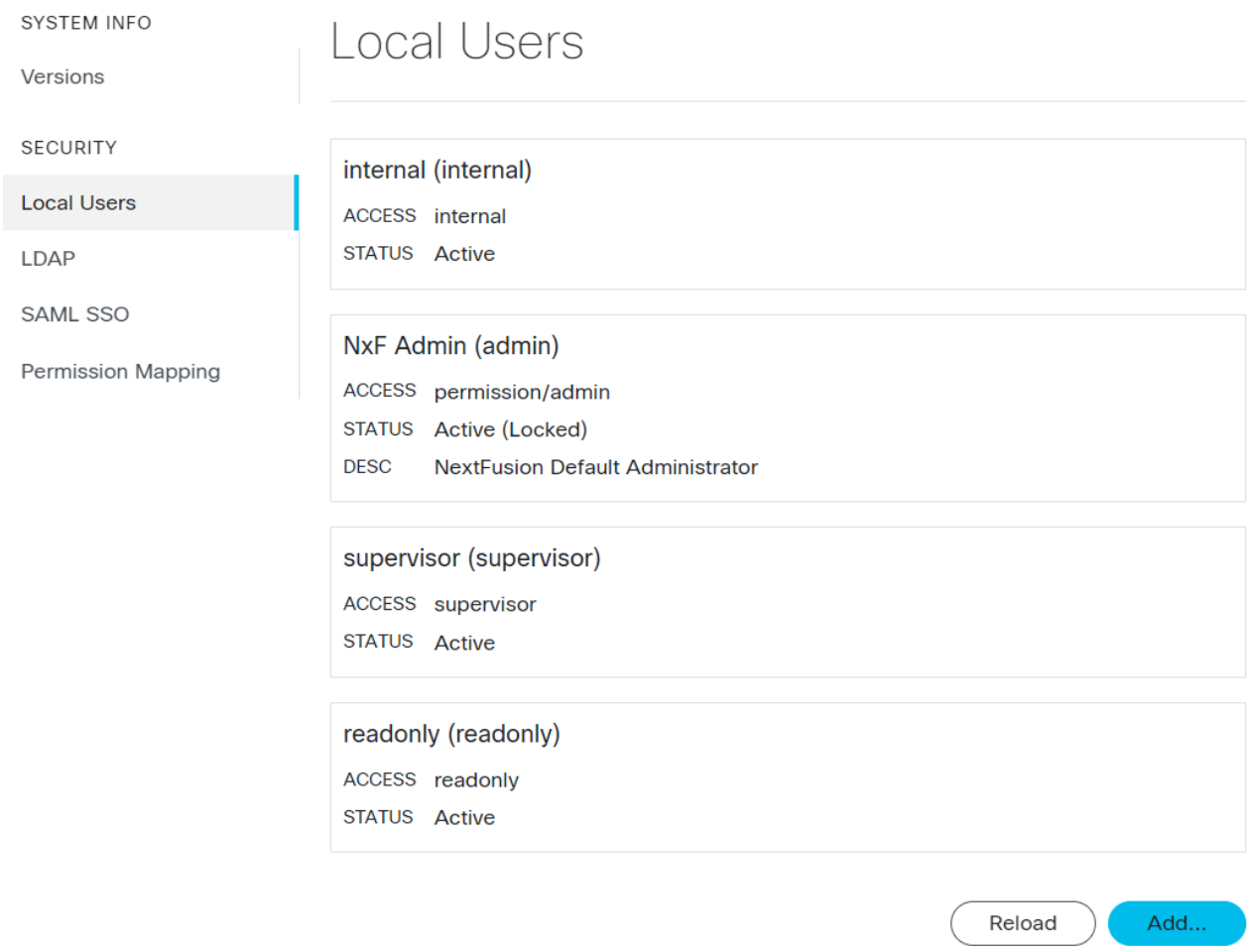
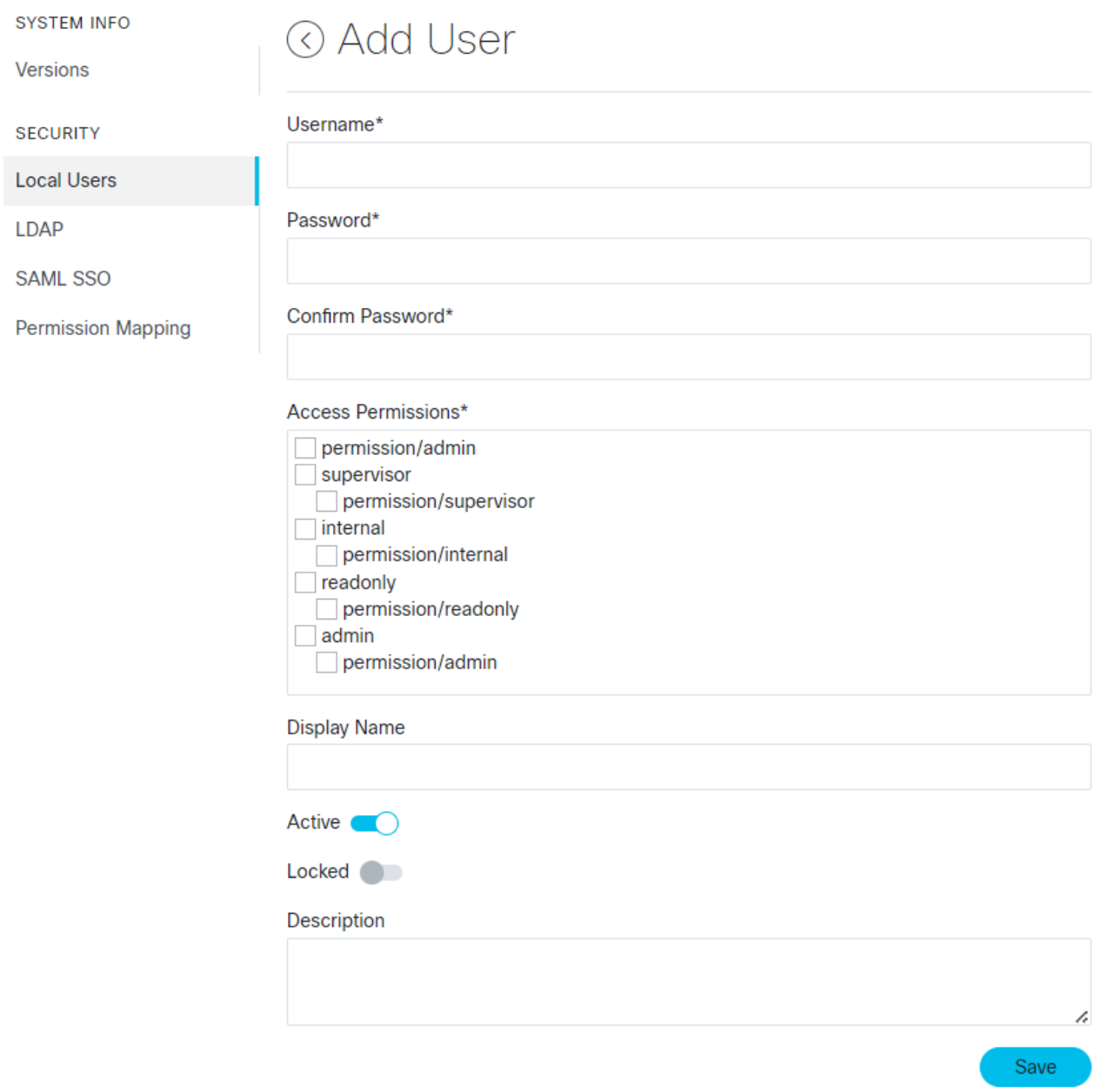


*Figure 12: Add User*




**Step 6** (Optional) Specify the **Description** and **Display Name**.

**Step 7** Configure the user status by selecting the radio buttons. These radio buttons function independently, allowing both to be either enabled or disabled simultaneously.

| Button | Action |
|---|---|
| **Active** | Enable or disable user login to Cisco Optical Network Controller. |

| Button | Action |
|---|---|
| **Locked** | Enable or disable user deletion.<br>When the lock is enabled, the user cannot be deleted. Disabling the lock allows the user to be deleted. |

**Step 8** Click **Save**.

Local users are created for ongoing Cisco Optical Network Controller operations.

# Onboard Cisco Optical Site Manager nodes in Cisco Optical Network Controller

Onboarding Cisco Optical Site Manager nodes connects them to Cisco Optical Network Controller for discovery and provisioning. Only users with administrator or supervisor permissions can onboard nodes.

**Before you begin**

Log in to Cisco Optical Network Controller as an admin/supervisor user.

Follow any of these tasks to onboard Cisco Optical Site Manager nodes.

**Procedure**

**Step 1** Onboard a single node using the Cisco Optical Network Controller interface.

For more details, see Add nodes on Cisco Optical Network Controller, on page 79.

**Step 2** Onboard multiple nodes using an Excel import.

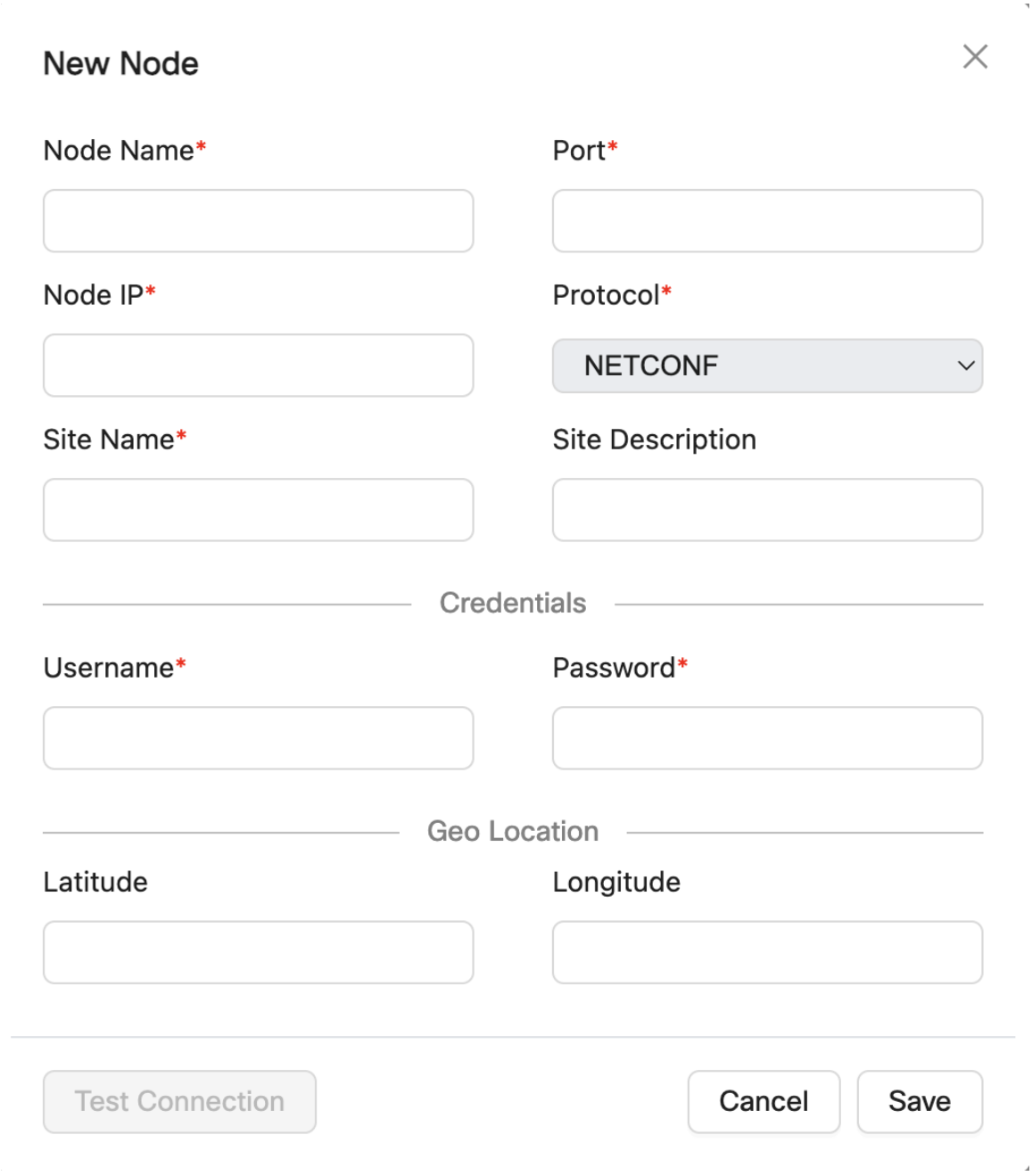
For more details, see Import multiple nodes into Cisco Optical Network Controller, on page 83.

Cisco Optical Site Manager nodes are onboarded and ready for discovery.

## Add nodes on Cisco Optical Network Controller

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

*Figure 13: Add New Node*




**Before you begin**

Verify these before addding to Cisco Optical Network Controller:

- Verify the Cisco Optical Site Manager is reachable from Cisco Optical Network Controller server via DCN.
- NETCONF port is enabled on the Cisco Optical Site Manager. For more details, see Enable NETCONF over SSH.

- The COSM1K (NCS 1000 series) nodes must be added using port number 2022.
- You must add only fully configured nodes. All passives and patchcords must already be created before you add a node.

### Procedure

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

**Step 2** Click **New**.

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

Ensure that you enter valid a username and password of the node to enable Cisco Optical Network Controller to connect to the node. For details about field descriptions, see the Table 21: Add new node field descriptions, on page 81 table.

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

**Step 4** To test connectivity from Cisco Optical Network Controller to a Cisco Optical Site Manager node, perform these steps:

a) (Optional) Click **Test Connection** to test the connectivity to the node.

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

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

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

c) Click **Ping** if you want to verify node reachability from Cisco Optical Network Controller.

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

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

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

***Table 21: Add new node field descriptions***

| Field | Description | Mandatory |
|---|---|---|
| **Node Name** | Name of the new node you are adding.<br>**Note**<br>This name replaces the already configured Cisco Optical Site Manager node name. | Yes |

| Field | Description | Mandatory |
|---|---|---|
| **Node IP** | IP address of the new node which you are adding.<br>**Note**<br>Ensure that this IP does not overlap the Reserved internal IP addresses and subnets. | Yes |
| **Port** | The port number of the new node which you are adding. | Yes |
| **Protocol** | The protocol used for the new node which you are adding. | Yes |
| **Site Name** | The name of the site to which the new node belongs. | Yes |
| **Username** | The username for accessing the new node. | Yes<br>**Note**<br>Use an administrator account to add and manage a Cisco Optical Site Manager node in Cisco Optical Network Controller. This account is required for onboarding and ongoing node operations, including performance monitoring collection, service provisioning and deletion, database backup and restore, and software download and activation. Other Cisco Optical Site Manager user roles are not supported for these operations. |
| **Password** | The password for accessing the new node. | Yes |
| **Site Description** | The description of the site to which the new node belongs. | No |
| **Latitude** | The Latitude co-ordinate value that you want to assign for the new node to set its location on the map. | No |
| **Longitude** | The Longitude co-ordinate value that you want to assign for the new node to set its location on the map. | No |

# Import multiple nodes into Cisco Optical Network Controller

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

Cisco Optical Network Controller onboards nodes in batches:

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

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

## Procedure

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

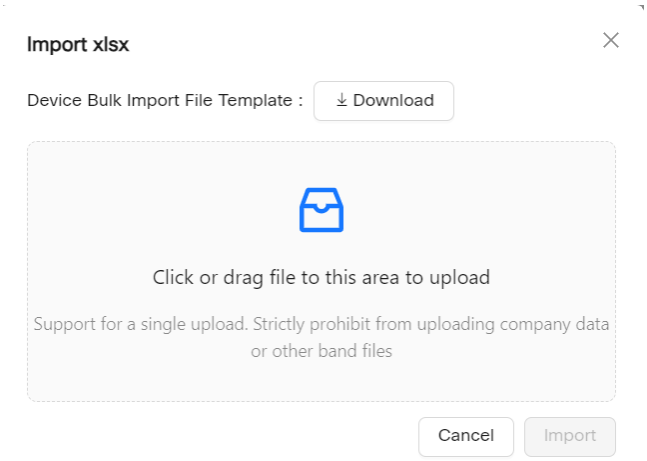
**Step 2** Click **Import nodes** to import the nodes in bulk.

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

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

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

***Figure 14: Import nodes***




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

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

*Table 22: Bulk Import File Template*

| Name | Description |
|---|---|
| **Node Name** | Name of the node Cisco Optical Site Manager node.<br>**Note**<br>This name replaces the already configured Cisco Optical Site Manager node name. |
| **Node IP** | The IP address of the node you are adding.<br>**Note**<br>Ensure that this IP does not overlap the Reserved internal IP addresses and subnets. |
| **User Name** | The username for accessing the new node.<br>**Note**<br>Use an administrator account to add and manage a Cisco Optical Site Manager node in Cisco Optical Network Controller. This account is required for onboarding and ongoing node operations, including performance monitoring collection, service provisioning and deletion, database backup and restore, and software download and activation. Other Cisco Optical Site Manager user roles are not supported for these operations. |
| **Password** | The password for accessing the new node. |
| **Connectivity Type** | The type of the protocol used for connecting the node.<br>Default: NETCONF |
| **Connectivity Port** | The port number of the node.<br>Port number 2022 for NCS 1000 series nodes. |
| **Site Name** | The name of the site to which the new node belongs. |
| **Site Description** | The description of the site to which the new node belongs. |
| **Product Type** | Set it as *Cisco Optical Node*. |
| **Latitude** | Specify the latitude co-ordinate value you want to assign to the new node to set its location on the map. |
| **Longitude** | Specify the longitude co-ordinate value you want to assign for the new node to set its location on the map. |

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

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

### What to do next

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

## Nodes

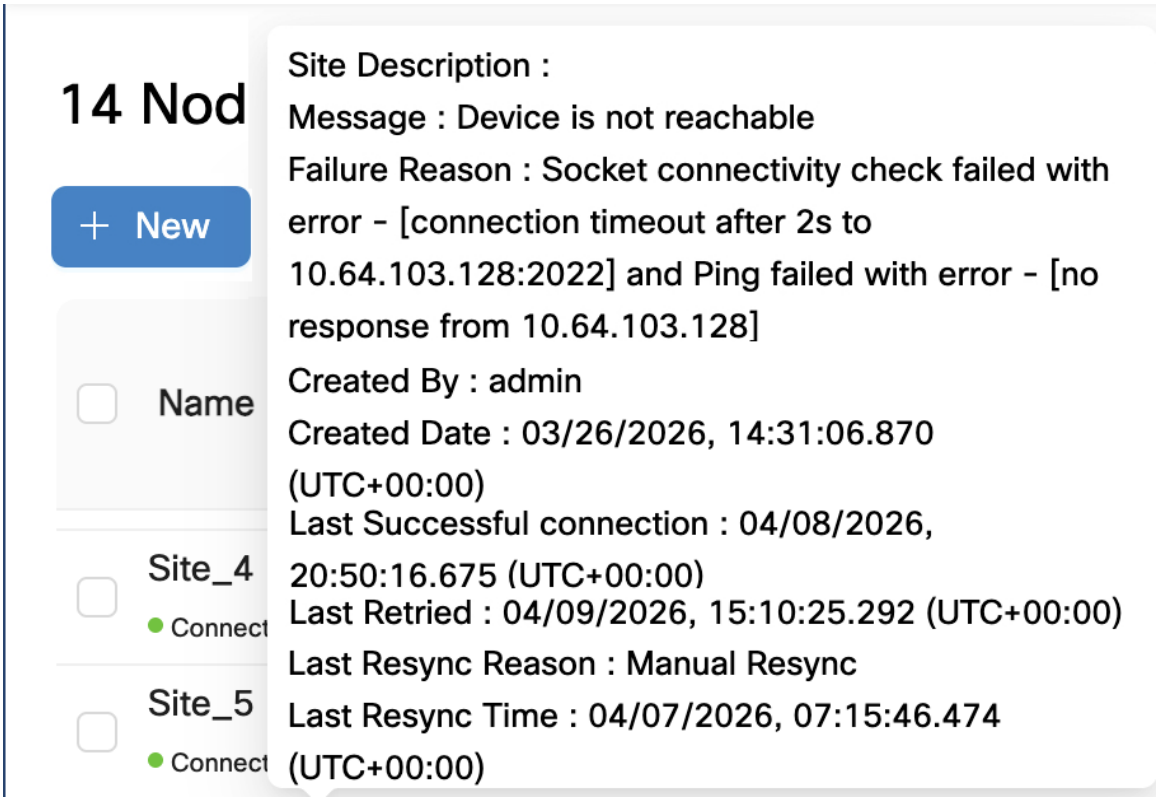
A node refers to a device in the network. You can add a single node or a set of nodes in the form of a batch at any given point in time.

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

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

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

*Figure 15: Additional details of a node*




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

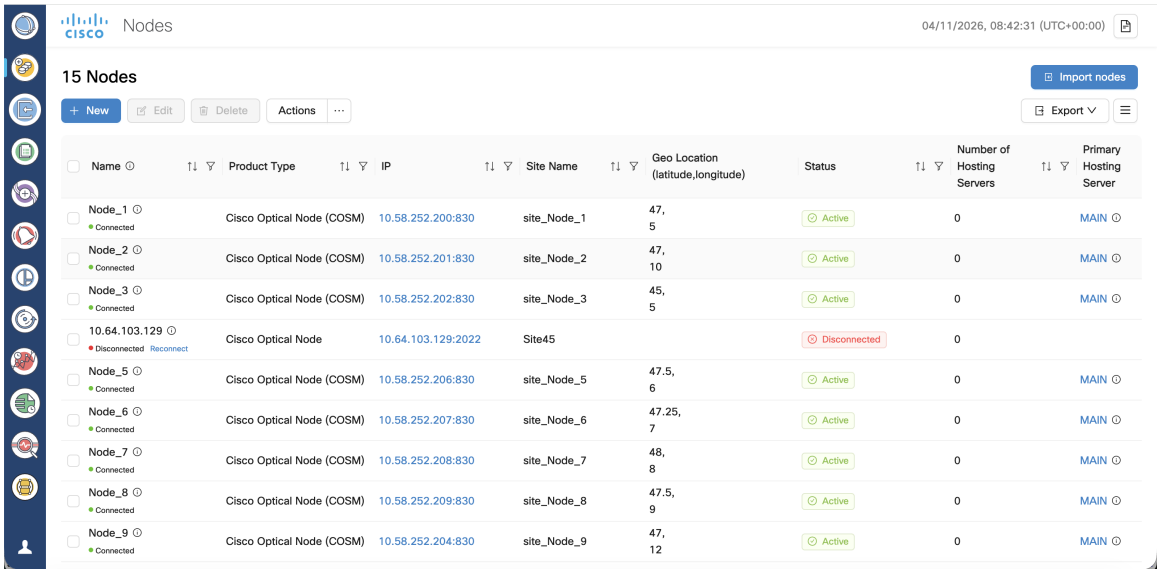
  Here are example values for the field:

  - *Socket connectivity check failed with error - [dial tcp 10.20.30.40:2020: connect: connection refused] but Ping succeeded*
  - *Socket connectivity check failed with error - [connection timeout after 2s to 10.20.30.40:22] and Ping failed with error - [no response from 10.20.30.40]*
  - *Socket connectivity check failed with error - [dial tcp 10.20.30.40:22: connect: no route to host] but Ping succeeded*

- **Created by**: Displays the user id that added the node.
- **Created Date**: Shows the date and time when the node was added.
- **Modified Date**: Shows the date and time when the node details were last updated.
- **Last Successful connection**: Shows the date and time when the node last connected successfully.
- **Last Retried**: Shows the date and time when the last connection attempt was made for this node. This field is only visible when a node is in *Waiting_for_connection* state.

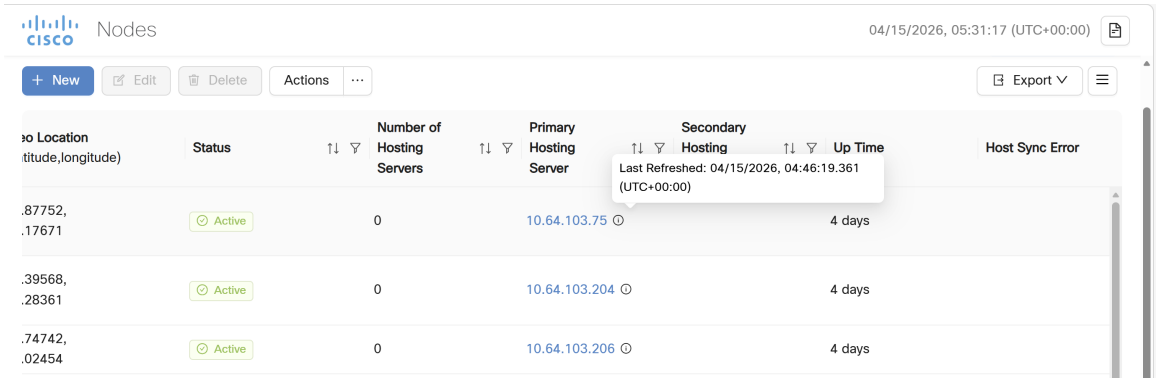
- **Last Resync Reason**: Shows the reason for the most recent resync of the node.
- **Last Resync Time**: Shows the date and time when the most recent resync of the node occurred.

***Figure 16: Nodes***




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

***Figure 17: Last Refreshed information***




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

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

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

- **Test Connection**: Used for sending pings to the far end node.
- **Resync Host Details**: Used for resyncing NCS 2000 node with SVO line cards.

**Note**

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

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

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

# Validate node discovery and network topology in Cisco Optical Network Controller

Validation confirms that Cisco Optical Network Controller is ready for service provisioning on all the onboarded Cisco Optical Site Manager nodes.

Run this task after Cisco Optical Site Manager node onboarding is complete.

Follow these steps to validate Cisco Optical Site Manager node discovery and network topology.

### Procedure

**Step 1** Verify that the connectivity status for each onboarded Cisco Optical Site Manager node under the **Node Name** column is displayed as *Connected*.

**Step 2** Verify that the **Status** for the node **Name** is displayed as *Active*.
Wait at least 60 seconds after discovery completes before sending TAPI requests.

**Step 3** Select **Topology** in the left panel to display nodes and links on the map.

For details about topology review, see Topology in Cisco Optical Network Controller Configuration Guide.

**Step 4** Verify that all the expected nodes and connections appear in the **Topology** page.

The topology view reflects the onboarded network.

**Step 5** Click **Inventory** in the left panel to verify the detailed inventory for the site.

For details about inventory review, see Network Inventory in Cisco Optical Network Controller Configuration Guide.

Cisco Optical Network Controller displays all inventory items for the selected site. Click a node to view its details.

Node discovery, network topology, and network inventory views are validated and ready for circuit provisioning.

# Circuits

The Service Manager application in Cisco Optical Network Controller provides centralized management of network services, particularly circuits. Use **Service Manager** to visualize, provision, monitor, edit, and delete circuits.

### Supported circuit types

Cisco Optical Network Controller supports these DWDM circuit types in both GMPLS and CPCE control planes:

- **OCH-NC**: Establishes connectivity between two optical nodes on a specified wavelength. The connection uses ports on multiplexer/demultiplexer and add/drop cards.
- **OCH-CC**: Extends the OCH-NC to create an optical connection from the source client port to the destination client port of the TXP/MXP cards. An OCH-CC circuit represents the end-to-end client service through the DWDM system.
- **OCH-Trail**: Transports OCH-CC circuits over the common trunk-to-trunk connection between transponder (TXP) or muxponder (MXP) line cards. When you create an OCH-CC between two TXP or MXP cards, Cisco Optical Network Controller automatically creates the corresponding OCH-Trail.

### Provisioning behavior

A circuit represents an end-to-end connection and consists of an alternating series of cross-connections and link connections. The provisioning scope depends on the control plane:

- For CPCE circuits, Cisco Optical Network Controller makes configuration changes across multiple participating nodes.

- For GMPLS circuits, Cisco Optical Network Controller sends the circuit provisioning request only to the head node.

The Provisioning Wizard collects the required circuit information in a step-by-step workflow and generates the required configuration for the participating nodes. On the final page, review the inputs, update service parameters if required, and deploy the configuration.

### Deployment and validation

Cisco Optical Network Controller deploys configuration changes as an atomic transaction. It makes a best effort to complete all operations together or none of them. If configuration fails on any device during a multi-node operation, rollback restores the participating nodes to their state before provisioning was attempted.

After provisioning is complete, the circuit appears in the Service List table. The lifecycle state initially appears as **PLANNED** and changes to **INSTALLED** after the circuit is installed. Monitor provisioned circuits by using the Circuit Monitoring Workspace. For details, see Provision CPCE services.

# Cisco Optical Network Controller alarms

Cisco Optical Network Controller alarms help monitor network conditions and support troubleshooting across managed nodes, circuits, and network resources. The Alarms application provides active and historical alarm information, including severity, affected object, service impact, acknowledgement status, user notes, and correlation details. You can use alarm information to:

You can use alarm information to:

- Review current and previous faults.
- Identify root-cause conditions through network-level alarm correlation.
- Forward selected alarms or events to external SNMP managers.

For more information, see Alarms and Alarms troubleshooting.

# Cisco Optical Network Controller workspaces

Workspaces combine information from multiple Cisco Optical Network Controller applications into a single view. They help users review related topology, alarm, service, link, and performance information without switching between separate applications.

The available workspaces support these monitoring and management views:

| Workspace | Focus |
|---|---|
| Network Monitoring Workspace | Provides a network-level view of node status, alarms, links, and performance metrics. Alarm details are displayed based on the node or link selected in the topology. |
| Circuit Monitoring Workspace | Provides a circuit-level view of the service path, associated alarms, restoration events, and performance history. |
| Link Monitoring Workspace | Provides a link-level view that integrates the links table, topology, alarms, PM history, and associated circuits. Selecting a link in the links list highlights it in topology, and selecting nodes or links in topology filters the links list. |

Workspace panels are interactive and can include Alarms, Service List, Topology, Detailed Service Path, Links, and PM History views. Layout changes can be saved or reset, and contextual actions can cross-launch to related node, equipment, port, circuit, or link information.

For more information, see Workspaces.

## Cisco Optical Network Controller PM history

The PM History application helps you view and generate performance monitoring reports for interfaces that are part of onboarded nodes. It is available in the **Network Monitoring** workspace for links and in the **Service Monitoring** workspace for circuits through the detailed service path.

PM History provides these capabilities:

- Collects PM data from onboarded Cisco Optical Site Manager nodes at 15-minute and 24-hour intervals.
- Displays PM data in tabular and graphical formats based on the selected node, interval, date and time range, interface type, port, and location.
- Generates historical PM reports for Cisco Optical Network Controller entities such as circuits or services, links, and ports.
- Retrieves older PM data from archived storage when the selected data is outside the active retention period.

For more information, see PM History.

# Common failures and troubleshooting procedures for Cisco Optical Network Controller

This section lists common errors and their troubleshooting or workaround steps. If the issues persist after trying the suggested workarounds, contact Cisco TAC and collect a tech dump as described.

This section covers these Cisco Optical Network Controller troubleshooting areas:

- Installation failures
- Node addition, deletion, and resync operation failures
- Topology failures
- Circuit creation and deletion failures
- Alien import and PM failures

If the issues are still not resolved by the suggested workarounds contact Cisco TAC after collecting tech dump.

*Figure 18:*

### Installation failure

This table lists common installation failures and provides troubleshooting steps for each issue.

*Table 23: Installation Failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| CONC UI Login Failures | Unable to login to CONC UI after installation | Check if admin password was created part of installation.<br>Also check if the password is specified correctly. | If admin password was not created during installation, create it and try login again |
| VM Login Failures | Unable to SSH to VM – It will continue to ask for password | This can happen when keys are not matched or ed25519 is not used for key generation | For accessing SSH, ed25519 key is required. The ed25519 key is different from the RSA key. So, follow the steps in installation documents for SSH Key Generation.<br>Ensure the public key specified during installation is matching with the private key used for login. |
| | SSH connection time out | This can happen if both northbound and eastbound are in same network | Keep northbound and eastbound in separate network |

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| ONC pods not coming up as ready | Some ONC pods are in Init:ContainerStatusUnknown and few others in ImagePullBackOff status when running<br>**kubectl get pods –A** command | Data Volume Size (GB) not mentioned correctly as per the VM Profile(XS, S, M) during installation<br>[OR] No Disk Space (/data) available when running "df -h" command | Reinstall ONC - Configure data volume according to the VM profile during installation |
| | VM time is not in sync with NTP time | Validate if timezone is synced with NTP and the time is up to date post bring up boot up.<br>You can do this by using the command "timedatectl status"<br>It should show:<br>System clock synchronized: yes<br>NTP service: active | Check if NTP is configured correctly and VM time is in sync with it<br>Make sure the hardware clock ( ESXi Host ) is not far off the system time on all the nodes. |
| | DNS not configured properly or DNS server not reachable | Check if DNS server was mentioned correctly during installation and the mentions DNS servers are reachable | Configure DNS server properly during installation. |

### Node addition failure

The table outlines node addition failures and the steps to resolve them.

*Table 24: Node Addition Failure*

| Reason | Description/Details | Troubleshooting | Workarounds/Remarks |
|---|---|---|---|
| Connection Failure | UI status – Disconnected | Check connectivity to the Node by –<br>Check if the user provided details like Connectivity type, IP, Port, and node credentials are correctly mentioned in Cisco Optical Network Controller UI. | Correct the details provided in the Cisco Optical Network Controller UI. |
| | | Check if Ping to the node is working | Check if the node is properly configured and has proper network configuration. |
| | | Check if the Netconf connectivity to the node on the Netconf port is working. | Check if the Netconf and XR configuration is proper on the node |
| Collection Failure | UI status – Failed/Errored | Check the release on the NCS1010/COSM node. | COSM / NCS1010 should be running Supported Release versions.<br>If the issue occurs even when the required software versions are present call TAC. |

### Node deletion failure

Use this table to identify node deletion failures and find troubleshooting guidance.

*Table 25: Node Deletion Failure*

| Reason | Description/Details | Troubleshooting | Workarounds/Remarks |
|---|---|---|---|
| Node is part of a Circuit | UI status – Circuit/Service spanning over the node | This is expected Cisco Optical Network Controller behavior. | Delete the Circuit/Connectivity-service (via NBI) and then try Node deletion. |
| Collection In Progress | UI Status – Node cannot be deleted because Collection is in Progress | This is expected Cisco Optical Network Controller behavior. | Wait for the collection to be completed and then try node deletion. |
| Resync in Progress | UI status – Node cannot be deleted because Collection is in Progress | This is expected Cisco Optical Network Controller behavior. | Wait for the Resync to be completed and then try node deletion. |

| Reason | Description/Details | Troubleshooting | Workarounds/Remarks |
|---|---|---|---|
| Connectivity Check in Progress | UI status – Node cannot be deleted because Waiting for Connection | This is expected Cisco Optical Network Controller behavior. | Wait for the Resync/Recollection to be completed and then try node deletion. |

### Resync operation failure

This table lists common resync operation failures and provides troubleshooting steps for each issue.

*Table 26: Resync Operation failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| Node not reachable | UI status –<br>Node – Disconnected<br>Status – Blank/Resync pending/Resync Failed | This is expected Cisco Optical Network Controller behavior. | Check if the node is properly configured and has proper network configuration.<br>Check if the Netconf and XR configuration is proper on the COSM/NCS1010 node.<br>Try Resync again<br>Check the release on the SVO/NCS1010 node for compatibility with Cisco Optical Network Controller release. |
| Node credentials changed on the node | UI status –<br>Node – Disconnected<br>Status –Blank/Resync pending/Resync Failed | This is expected Cisco Optical Network Controller behavior. | Edit the node credentials via Optical Network Controller UI and click OK. Resync will happen automatically. |

### Topology failure

The table outlines topology failures and the steps to resolve them.

*Table 27: Topology Failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| Lat and Long not mentioned for nodes in Import Excel/Add Node UI Dialog | Some of the nodes in Node table are not displayed in Topology | This is expected Cisco Optical Network Controller behavior. | When user enters topology, ONC will display “There are a few nodes without geographical coordinates. Please click on the pen icon to assign them manually.” User need to click Pen icon and drag the nodes to required location. Alternately the latitude and longitude can be edited in Nodes Page. Click Nodes in the left panel. Click EDIT after selecting the node from the table. |
| Links do not show up in ONC | Some of the links which are up in network might not show up in ONC topology view | Check if neighbours are shown correctly in COSM Web UI – Node Functional View and Neighbors are shown correctly in Optical Setup -> Optical Configuration | Correct COSM errors if any. |

### Circuit creation failure

Use this table to identify circuit creation failures and find troubleshooting guidance.

*Table 28: Circuit Creation Failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| No Route Available | Cisco Optical Network Controller UI status – NA | No route can be found by the Path Computation Engine. Could be expected behavior. | Check the topology and the route for the currently created services. |
| Wrong SIP Selection | Cisco Optical Network Controller status – NA | SIP UUIDs are not proper | Check the list of available SIPs and supply only SIPs returned from the T-API topology-context fetched by the Hierarchical Controller from Optical Network Controller as part of the get call. |

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| Node(s) not reachable | Cisco Optical Network Controller status – NA | Circuit will move to Pending-Removal lifecycle state. | Check the node reachability and fix it<br>Delete the connectivity-service<br>Recreate the connectivity-service. |
| Routing constraint is Invalid | Cisco Optical Network Controller status – NA | Could be due to invalid UUIDs provided in the connectivity-service request constraints. | Check the list of available constraints and supply only valid constraints. |
| Routing Constraint Not Feasible | Cisco Optical Network Controller status – NA | Could be expected behavior since a route may not be available meeting the Constraint provided. | Check the topology and the constraint provided. |

### Circuit deletion failure

This table lists common circuit deletion failures and provides troubleshooting steps for each issue.

*Table 29: Circuit Deletion Failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| Circuit Deletion attempted before circuit creation is completed | Connectivity-service lifecycle-state is Planned and same service deletion is attempted. | This is expected behavior. | Wait till the circuit lifecycle-state is either Installed or Pending-removal. |
| Invalid Circuit ID | Invalid connectivity-service UUID is provided | This is expected behavior. | Connectivity-service should be of an existing connectivity-service in the T-API connectivity-context. |

### Alien import failure

The table outlines alien import failures and the steps to resolve them.

*Table 30: Alien import failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| Alien file format is not proper | UI status – Request Failed | This is expected Cisco Optical Network Controller behavior. | Please check the file format. Cisco Optical Network Controller supports XML file format from Cisco Optical Network Planner only. |

### PM failure

Use this table to identify PM failures and find troubleshooting guidance.

*Table 31: PM failure*

| Reason | Description/Details | Troubleshooting | Workaround/Remarks |
|---|---|---|---|
| Node Reachability | Cisco Optical Network Controller UI status –<br>Node Status – Disconnected | This is expected Cisco Optical Network Controller behavior if the node is not reachable or the interface is not UP/Working on the node. | Check the node connectivity to the COSM node using Ping. |
| Node is onboarded recently | PM data is not shown for the node | This is expected Cisco Optical Network Controller behaviour – After the node is onboarded, it could take more than 15 min to show up 15 min PM data and 24 hours to show up 24 Hr PM data | Wait for the minimum duration (15 min or 24 Hr) for PM collection to start from ONC and show up in GUI |

# Cisco Optical Network Controller logs

Logs help you track user and system activity, export audit information, review developer logs, schedule archived log collection, and collect diagnostic data for support.

The Logs application organizes log data into tabs so that operators can find, filter, export, and archive log information from a single location. The log enhancements provide organized log management, filtering, pagination, export options, retention and archiving, and access control for different user roles.

- **Audit**: Displays audit log entries with fields such as time, category, identifier, username, client IP, and message. Audit categories include system, node, inventory, topology, service, alarm, alien import, and site audit events.
- **Debug**: Displays developer logs with filter options such as namespace, microservice, container, log level, time range, and search.

- **Archives**: Provides access to archived audit logs and debug logs. Archived logs can be scheduled, downloaded, deleted, suspended, resumed, or modified based on operational requirements.
- **Tech Dump**: Collects diagnostic data bundles that include system information, logs, configuration files, and operational data for troubleshooting.

For more information, see Logs.

## Generate and download tech dump logs

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

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

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

**Before you begin**

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

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

**Procedure**

**Step 1** Click **Logs**.

**Step 2** Click **Tech Dump** tab.

For details about the field descriptions on this tab, see Table 32: Tech dump tab field descriptions, on page 101.

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

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

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

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

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

Wait for the log collection to finish.

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

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

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

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

*Table 32: Tech dump tab field descriptions*

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

# Cisco Optical Network Controller references

These references help operations teams monitor health and automate workflows.

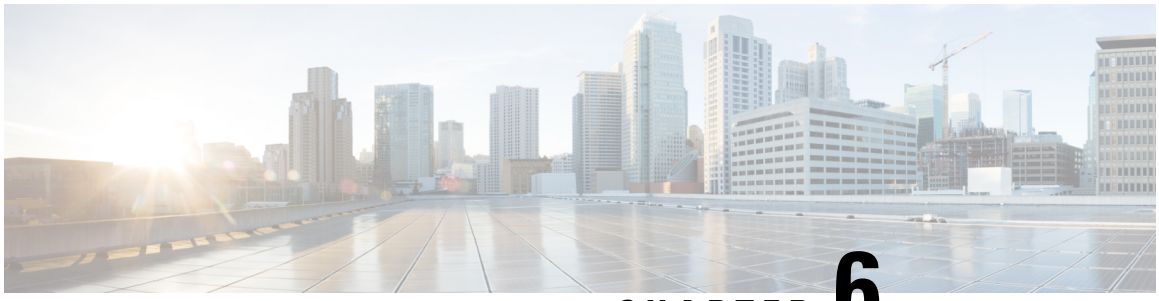
Consult the following sources for operational workflows.

- For details about API usage, see Cisco Optical Network Controller APIs.
- For details about general configuration workflows, see Cisco Optical Network Controller Configuration guide.

# Outcome

After completing this chapter, Cisco Optical Network Controller is installed, configured, and ready for network operations.

Cisco Optical Site Manager nodes are onboarded, optical circuits are provisioned, and operational workflows such as monitoring, alarms, PM history, and troubleshooting are available for ongoing management.



CHAPTER 6

# Import Your Live Network and Plan Future Expansion with Cisco Optical Network Planner

Live Network Import (LNI) is the final step after a network is created, where the deployed devices and their current configuration are imported into Cisco Optical Network Planner to reflect the actual state of the live network.

LNI is a network import capability that:

- Imports deployed optical networks into Cisco Optical Network Planner in real time
- Supports networks with NCS 1004, NCS 1010, NCS 1014, and NCS 2000 nodes
- Provides a complete view of the deployed network after import



## Perform live network import

Use this procedure to perform live import of a network from Cisco ONC.

**Before you begin**

- Perform LNI only when the Cisco ONC is in a stable or running state. Do not perform LNI during the maintenance period for software upgrade.
- Ensure that the release version of Cisco ONC you are using for the network import is 25.1.1 or above.
- Cisco ONP removes any card that is not properly connected via IPC in Cisco Optical Site Manager during LNI. To retain equipment, ensure that each card has at least one valid IPC connection in Cisco Optical Site Manager.
- Configure all the mandatory parameters on the circuit.
- Check the card label set for these NCS 2000 cards and update it if they are not aligned.

| PID | Card label |
|---|---|
| NCS2K-16-AD-CCOFS | AD-16-FS |
| NCS2K-20-SMRFS | SMR20-FS-CV |

| PID | Card label |
|---|---|
| NCS2K-20-SMRFS-L | SMR20-FS |
| NCS2K-9-SMR17FS | SMR9-17-FS |
| NCS2K-9-SMR24FS | SMR9-24-FS |
| NCS2K-9-SMR34FS | SMR9-34-FS |
| NCS2K-9-SMR34FS-L | SMR9-34-FS |
| 15454-M-RAMAN-COP= | OPT-RAMP-COP |
| 15454-M-RAMAN-CTP= | OPT-RAMP-CTP |
| NCS2K-OPT-EDFA-35 | OPT-EDFA-35 |

- Log in to the Cisco ONP web interface

.

### Procedure

**Step 1** Choose **Import** > **Live Import**.

**Step 2** In the **Import Live Network** dialog box:

a) Enter **CONC Server IP**, **Username**, and **Password**.

b) Click **Import**.

The **Import** button will be enabled only when all the values entered are valid.

**Step 3** View the status of the LNI operation:

a) Click **Job Monitor**, to view the status of the IMPORT_LIVE_NETWORK task. Click **Refresh** to see the updated status.

After LNI is completed, the job is removed from the **Job Monitor** page.

b) Click **Logs** to view the list of events that are related to the LNI operation, as logs.

**Step 4** After the completion of the LNI operation, choose **File** > **Open**.

The format of the LNI imported network filename is LNI_<Date>_<Time>.

**Step 5** Click the imported network name to view the network under the **Map** tab and its corresponding network tree in the left panel.

You can view the tag **Imported from Network** in the interface.

**Note**

- During the live import of a network with an optical source, if the configuration code of the optical source does not match, it will default to NCS1004_SP_16QAM_300G_27%SDFEC_69GBd. You can update the optical source in upgrade mode while the network is in a locked state.

- The configurations that are supported by Cisco ONC can only be imported into Cisco ONP. See Configurations and hardware supported by LNI.
- Even if errors occur during the LNI operation, the operation is not canceled. In this case, when you open the imported network, a warning message appears.
- You can view the errors under the **Elements** > **Messages** tab. See both critical and noncritical messages.

  If you find unconnected equipment in the **Messages** tab, upgrade the imported LNI network and make the necessary adjustments to reintegrate the removed equipment into Cisco ONP. However, note that the newly created equipment UID may not match the one in Cisco Optical Site Manager. You can utilize the UID edit feature to align the UIDs between Cisco ONP and Cisco Optical Site Manager. Refer to Edit the Unique ID of the chassis
- Each user is permitted to initiate only one LNI process at a time. If a user tries to start an additional concurrent LNI process, the system will terminate the new request and display an error message indicating the restriction. This limitation is applied on a per-user basis, allowing multiple users to run their own LNI processes simultaneously on the same CONC server, as long as each user adheres to the rule of having only one active process.
- If both NCS and Non-NCS PIDS are present in the inventory, Cisco ONP enables the **Enable NCS** option. You can edit this option during upgrade after unlocking the site, if necessary.

### What to do next

Click the **BOM** tab to view the BOM details of the network.

**Note** The PIDs of prototype cards are shown as "NA" in the BOM details of the LNI network.

You can export the CPZ, import the CPZ, and share the imported network. Use the **Entity Editor** to view network properties.

# Collect troubleshooting data for live network import

Use this task when you need to share live network import data with the engineering team.

**Before you begin**

Ensure that the live network import has completed or failed with an error.

Follow these steps to collect troubleshooting data for live network import.

### Procedure

**Step 1** From Cisco Optical Network Planner, export and share the Cisco Optical Network Planner CPZ file for the network.

For detailed steps about exporting, see Export the CPZ file.

**Step 2** Collect and share Cisco Optical Network Controller response data.

a) Open this URL in any browser.

```
https://<conc_server_IP>:8443/onc-osapi-gw-service/v1/network
```

b) Save the raw data response to text file in JSON format.