Cisco Optical Network Planner Installation Guide, Releases 26.x.x

Cisco Optical Network Planner
Release: 26.x.x | Updated June 12, 2026

Topics included

1 Install Cisco Optical Network Planner....4
Cisco Optical Network Planner....5
Hardware and software requirements....5
Install Cisco ONP....6
Install the SMU for Release 26.1.1....9
Install Cisco ONP on laptop through Oracle VirtualBox....11
Upgrade Cisco ONP from Release 25.1.1 to 26.1.1....12
Log into Cisco ONP....13
Update the default self-signed certificates....14
Restart Cisco ONP....15
Uninstall Cisco ONP....15
Uninstall WSL Ubuntu....16
Docker commands....16
Cisco ONP logs....17
Monitor the Cisco ONP health....17

2 Troubleshoot....20
Troubleshooting tasks....21

1 Install Cisco Optical Network Planner

Topics:

- Cisco Optical Network Planner
- Install Cisco ONP
- Upgrade Cisco ONP from Release 25.1.1 to 26.1.1
- Log into Cisco ONP
- Restart Cisco ONP
- Uninstall Cisco ONP
- Uninstall WSL Ubuntu
- Docker commands
- Monitor the Cisco ONP health

Requirements, installation procedures, configuration steps, and maintenance tasks for Cisco Optical Network Planner, including system monitoring and troubleshooting guidelines.

Cisco Optical Network Planner

Introduces Cisco Optical Network Planner (Cisco ONP) software tool designed to model, test, and validate Optical Transport Network (OTN) and Dense Wavelength Division Multiplexing (DWDM) optical networks.

Cisco Optical Network Planner (Cisco ONP) is a software tool that

- models and tests Optical Transport Network (OTN) and Dense Wavelength Division Multiplexing (DWDM) optical networks,
- operates within a graphical environment, and
- supports the design and validation of networks of NCS 1000, NCS 2000, and NCS 4000 series.

Cisco ONP capabilities

Cisco ONP capabilities include:

- creation of multiple network instances,
- modification of parameters for each instance, and
- comparison between different network instances.

Hardware and software requirements

This section lists the required hardware and software specifications for installing and using Cisco Optical Network Planner (ONP) and Live Network Import (LNI).

The hardware and software requirements for installing Cisco ONP are:

Hardware requirements

You need to have an Ubuntu server with version 22.04 or 24.04, or Red Hat server with version 8.8 or 8.10

Recommended Server Configuration for Cisco Optical Network Planner (ONP):

- 8 CPU, 48 GB RAM, and 500GB server free space after installation, for 3 concurrent Parallel ONP analysis
- 8 CPU, 64 GB RAM, and 500GB server free space after installation, for 6 concurrent Parallel ONP analysis
- 8 CPU, 96 GB RAM, and 500GB server free space after installation, for 10 concurrent Parallel ONP analysis

Software requirements

- Supported browsers: Google Chrome, Mozilla Firefox, and Microsoft Edge
- Recommended version of the Google Chrome browser:
  - For Windows: Version 145.0.7632.117
  - For Mac: Version 145.0.7632.110

  Recommended version of the Microsoft Edge browser:
  - For Windows: Version 145.0.3800.70
  - For Mac: Version 145.0.3800.70

  Recommended version of the Mozilla Firefox browser:
  - For Windows: Version 148.0

- For Mac: Version 146.0.1

> **Note**
>
> It is recommended to use the Mozilla Firefox browser for large scale networks for better user experience.

> **Note**
>
> For an optimal Cisco ONP user experience, we recommend a minimum internet speed of 100 Mbps.

Install Cisco ONP

Use this procedure to Install Cisco ONP using the tar archive and installation script on a supported Linux server.

Set up Cisco ONP software by extracting the provided package and running the installer.

The Cisco ONP application is delivered as a bundled tar, signature file, and pubkey files package. The tar file (CONP-xx.xx.xx.xx.tar.gz) contains these files:

- ONP component
- A shell script (Installer.sh) to install ONP component
- SSF component
- README file for installation Procedure of SSF Component

Follow these steps to install Cisco ONP by using the tar archive and the installation script.

> **Note**
>
> This task is also applicable for upgrading Cisco ONP 25.1.1 to Cisco ONP 26.1.1. If you are upgrading from software version prior to R25.1.1 to R26.1.1, you must upgrade to R25.1.1 and then to R26.1.1 to retain data from software version prior to R25.1.1.
>
> If the host server is upgraded from Ubuntu 22.04 to 24.04, restart the Ubuntu host server before proceeding with the Cisco ONP installation.

Procedure

1. Log in to the Ubuntu server or Red Hat server as root or a user with sudo privileges, where Cisco ONP is to be installed.
2. Create the *26.1.1_Build* folder under *ONP_Builds* to keep all the required files for the installation.

Example

```
user@host:~/Desktop$ mkdir ONP_Builds/26.1.1_Build
```

Note

The example path here `/home/ user/Desktop/ONP_Builds/26.1.1_Build` is referenced as $ONP_HOME in this document.

The $ONP_HOME directory can be any other directory in your server. You can create a directory of your choice and copy the ONP build tar file, signature file, and pubkey file to that directory.

3. Copy or download the Cisco ONP build tar, signature file, and public key file to the created ONP_Builds directory.
4. Go to the $ONP_HOME directory and perform these steps:
   a) Assign full permission to the build tar.

      Example:

      ```
      cd /home/user/Desktop/ONP_Builds
      ```

      ```
      sudo chmod 777 CONP-xx-xx.xx.xx.tar.gz
      ```

   b) Untar the Cisco ONP build.

      ```
      tar -xvf CONP-xx-xx-xx.xx.tar.gz
      ```

   c) Set read, write, and execute permissions for the Install script, and ONP folders using these commands.

      ```
      sudo chmod -R 777 ONP
      sudo chmod 777 Installer.sh
      ```

   d) Check whether curl is installed in the server by entering this command.

      ```
      root:~/$ONP_HOME# curl
      ```

      If you see this output, curl is installed. Otherwise, install curl.

      ```
      curl: try 'curl --help' or 'curl --manual' for more information
      ```

      To install curl, run this command.

      ```
      root:~/$ONP_HOME# sudo apt install curl
      ```

   e) Enter **y** or **n** to change the default IP address.

      ```
      Would you like to change the IP (y/n)
      ```

      If you enter **n**, the installation proceeds with the same IP address as mentioned above and if you enter **y**, you must provide the IP address and the installation proceeds with the IP address that is provided by you.

      ```
      ONP Host IP: 10.76.82.14
      ```

5. Start Cisco ONP installation. Type the command sudo ./<*install file*> <*tar file*> <*public key*>," and press **Enter**.

   Example:

```
sudo ./Installer.sh CONP-xx.xx.xx.xx.tar.gz CONP-xx.xx.xx.xx_pem.pubkey
```

   a) Enter **y** or **n** to change the default IP address.

```
Would you like to change the IP (y/n)
```

   If you enter **n**, the installation proceeds with the same IP address as mentioned above and if you enter **y**, you must provide the IP address and the installation proceeds with the IP address that is provided by you.

```
ONP Host IP: 10.76.82.14
```

   b) Enter your ONP database credentials.

> **Note**
>
> Make sure to use **ONLY alphabets or numbers**. We recommend not to use any special characters.
>
> If you are installing Cisco ONP for the first time, you must set the username and password for the database.
>
> ```
> Would you like to set database username and password (y/n).
> ```
>
> The above option appears only when you already have the 25.1.1 image installed and upgrade to 26.1.1. Otherwise you are prompted to enter ONP database username.
>
> If you enter **y**, then prompt appears and asks you to enter username and password. If you enter **n**, you can proceed with the next step.

```
Enter your ONP database username, only alphanumeric characters are valid
[user]:
```

```
Enter your ONP database password, only alpha numeric characters are valid
 (len >= 8 and <= 64 characters) [password]:
```

```
Repeat your ONP database password.
```

6. Wait for the installation to complete.

> **Note**
>
> The Cisco ONP services start automatically, after you successfully install the build.
>
> The install logs are located in this path:
>
> `/var/log/cnp/install.log`

Run this command to see the list of services running:

```
root:~/$ONP_HOME# sudo docker ps
```

You can confirm the successful installation based on whether these services are up and running for more than five minutes:

- cnp_cnp
- cnp_ode.1
- cnp_ode.2
- cnp_ode.3
- cnp_pce.1
- cnp_pce.2
- cnp_cnp_frontend
- cnp_gene
- cnp_postgres

7. After you confirm that all the mentioned services in the previous step are up, you can access the Cisco ONP using the Google Chrome, Mozilla Firefox, or Microsoft Edge browser pointing to Ubuntu server hostname or IP address.
8. To install the SSF component, refer the README file for SSF installation.

   After you install the SSF component, you can add SSF server details in the Cisco ONP application at **Preferences** > **General Settings** > **SSF Server Details**.

Install the SMU for Release 26.1.1

Use this procedure to install the software maintenance update (SMU) for Release 26.1.1 to maintain optimal performance and resolve known issues.

Install the SMU package for Release 26.1.1 using the provided tar archive and installation script.

Applying a software maintenance update (SMU) keeps your system up to date with important fixes and enhancements for Release 26.1.1.

Follow these steps to install the SMU for Release 26.1.1:

Procedure

1. Log in to the Ubuntu server as root or a user with sudo privileges, where Cisco ONP 26.1.1 is already installed.

2. Create a directory named `26.1.1_SMU1` under ONP_Builds to keep all required installation files.

   Example

   ```
   user@host:~/Desktop$ mkdir ONP_Builds/26.1.1_SMU1
   ```

   Note

   This directory is referenced as `$ONP_HOME`. You may choose any directory.

3. Copy or download the `CONP-26.1.1-SMU1.tar.gz` build tar to the created ONP_Builds directory.
4. Navigate to the $ONP_HOME directory:
   a) Assign full permission to the build tar.

      Example

      ```
      cd /home/user/Desktop/ONP_Builds
      ```

      ```
      sudo chmod 777 CONP-26.1.1-SMU1.tar.gz
      ```

   b) Untar the Cisco ONP build.

      Example

      ```
      cd /home/user/Desktop/ONP_Builds
      ```

      ```
      tar -xvf CONP-26.1.1-SMU1.tar.gz
      ```

   c) Set read, write, and execute permissions for the Install script

      Example

      ```
      sudo chmod 777 CONP-26.1.1-SMU1-Install.sh
      ```

5. Start the Cisco ONP 26.1.1-SMU1 installation by running the installer script with sudo privileges.

   Example:

   ```
   sudo ./CONP-26.1.1-SMU1-Install.sh
   ```

   Follow any on-screen prompts.

6. Wait for the installation to complete.

   The services start automatically after successful installation.

   Run this command to see the list of services running.

   ```
   root:~/$ONP_HOME# sudo docker ps
   ```

   Confirm the successful installation based on whether these services are up and running for more than two minutes:

- cnp_cnp
- cnp_ode.1
- cnp_ode.2
- cnp_ode.3
- cnp_pce.1
- cnp_pce.2
- cnp_cnp_frontend
- cnp_gene
- cnp_postgres

7. After confirming all services are running, access the application using Google Chrome, Mozilla Firefox, or Microsoft Edge. Enter the Ubuntu server's hostname or IP address in the browser.

The SMU for Release 26.1.1 is installed. The relevant services will be running, and you can access the application from a supported browser.

Install Cisco ONP on laptop through Oracle VirtualBox

Use this procedure to install Cisco Optical Network Planner on a Windows laptop or Apple MacBook using Oracle VirtualBox and Ubuntu Desktop.

Use this task to install Cisco ONP on a Windows laptop or Apple MacBook.

Before you begin

Ensure that your Windows laptop or Apple MacBook has at least 16 GB of RAM.

Follow these steps to install Cisco Optical Network Planner on your laptop using Oracle VirtualBox:

Procedure

---

1. Download and install the latest version of Oracle VirtualBox on your Windows or Mac laptop. See Downloads and Youtube.

   We recommend downloading "macOS /Intel hosts" for the Apple MacBook.

2. Download the Ubuntu 22.04 Desktop AMD64 image from the link: https://releases.ubuntu.com/focal/ and install it on the VirtualBox.

   > **Note**
   >
   > Ensure that you allocate at least 30 GB of storage space on the VirtualBox, 8 GB of RAM and four virtual CPUs, and mount a directory with full access for file sharing. See How to setup shared folders in VirtualBox 6.

3. Install VirtualBox Guest Additions to share the clipboard operations and to share the folder access between the Host and Guest operating systems. See Installing and Maintaining Guest Additions.
4. Download the Cisco ONP tar build, public key, and signature files from Downloads to the Host Windows laptop or MacBook, and copy it into the shared folder mounted as in Step 3.
5. Log in to the VirtualBox and access the Cisco ONP tar build, public key, and signature files through the shared folder.

6. Open the terminal in the VirtualBox, navigate to the shared folder and, install Cisco ONP. See step 4 of the task Install Cisco ONP..
7. To log into Cisco ONP, see Log into Cisco ONP on page 13.

> **Note**
>
> Try launching Cisco ONP through https://localhost if you are not able to launch it through ipaddress/hostname.

Upgrade Cisco ONP from Release 25.1.1 to 26.1.1

Use this procedure to upgrade your Cisco ONP software to the latest release to access new features and ensure optimal performance.

Follow these steps to upgrade Cisco ONP software from Release 25.1.1 to 26.1.1.

Follow these steps to upgrade your Cisco ONP software:

Procedure

1. Install Cisco ONP 26.1.1 image using the steps 1 to 5 of the procedure Install Cisco ONP on page 6.
2. In the displayed table, find out the container ID that is corresponding to the image "cnp_postgress image - dockerhub.cisco.com/cnp-rpt-dev-docker/postgres:14.9"
3. Use this command to enter inside the container.

```
#docker exec -it <cnp_postgress container ID> bash
```

   a) Use the command in the container to log into the database.

```
psql -U <db_username> CnpDB
```

   b) After you log in the database you will see this message.

```
psql (14.9)
 Type "help" for help
 CnpDB=#
```

   c) Enter the command **Analyze;**.

      This command takes a few minutes based on your database size.

   d) Enter the command **DROP TABLE IF EXISTS databasechangeloglock**.

      This command removes Liquibase Lock if it exists and enables seamless login and design activities after upgrade from 25.1.1 to 26.1.1.

   e) Enter **Exit** to come out of the database.

4. Enter **Exit** to come out of the container.

> **Note**
>
> Reanalyze the R25.1.1 analyzed networks after the upgrade to get the updated power consumption values.

> **Note**
>
> Reanalyse R25.1.1 NCS1001 and NCS1014 networks to populate valid ports in Cisco Optical Site Manager XML.

Cisco ONP is upgraded to the required release. The database is updated and ready for post-upgrade operations.

Log into Cisco ONP

Use this procedure to log in to Cisco ONP for initial system setup and management using the default administrator account.

Access the Cisco ONP user interface using the default administrator credentials after installation.

Follow these steps to log into the Cisco ONP user interface, after installing Cisco ONP.

Procedure

1. Open the Google Chrome browser.

   > **Note**
   >
   > Clear the browser cache if you have used earlier versions of Cisco ONP.

2. In the browser's address bar, enter *https://hostname* or *https://ipaddress*, where *hostname* or *IP address* belongs to the Ubuntu server used for Cisco ONP installation, for example: *https://cisco-onp-server.cisco.com* or *https://10.76.82.14*.

   The Cisco ONP user interface displays the Login window.

3. Enter **admin** and **cisco123** as the default username and password.
4. Click **Login** to log into Cisco ONP.

> **Note**
>
> Cisco ONP prompts you to change the administrator password, when you log in for the first time after installation. Cisco recommends that you create a new user with valid email ID and administrative privileges. Do not use the default administrator username because the administrator password cannot be recovered, if forgotten.

5. To change the administrator password, perform these actions in the prompt.
   a) Enter **Old Password**.
   b) Enter **New Password**.

      As you enter the password, the Cisco ONP prompt displays the strength of the password in different colors.

   c) Enter **Repeat New Password** to confirm the new password.
   d) Click **Update**.

      Wait until the Password updated successfully message appear.

Update the default self-signed certificates

Use this procedure to configure new CA-signed certificates to replace the default self-signed certificates after installing Cisco ONP.

Use this task to update the default self-signed certificates for Cisco ONP, after installation.

Follow these steps to update the default self-signed certificates for Cisco ONP:

Procedure

1. Log into the server where Cisco ONP is hosted.
2. Use the `cd` command, to go to the path `/opt/cnp/nginx/conf/ssl`.

   Example:

   ```
   cd /opt/cnp/nginx/conf/ssl
   ```

3. Delete the existing self-signed certificates.
4. Copy the Certificate Authority (CA)-signed certificates, then paste the certificates and key.

   > **Note**
   >
   > You must have CA-signed certificates.

5. Edit the ssl_certificate and ssl_certificate_key filenames in the default.conf file (located at /opt/cnp/nginx/conf) so that they match the new certificate and key filenames.

Example

```
server {
listen 443 ssl default_server;
server_name localhost;
ssl_certificate /etc/nginx/ssl/cnp_dev_selfsigned.crt;
ssl_certificate_key /etc/nginx/ssl/cnp_dev_selfsigned.key;
ssl_protocols TLSv1.2 TLSv1.3;
client_max_body_size 200M;
```

6. Restart Cisco ONP. See Restart Cisco ONP on page 15.

Restart Cisco ONP

Use this procedure to restart the Cisco ONP server to apply updates or resolve issues.

Restart the Cisco ONP server to ensure continued proper operation after maintenance or troubleshooting.

Follow these steps to restart the Cisco ONP server:

Procedure

1. Go to $ONP_HOME.
2. Execute this command:

```
sudo docker stack rm cnp
```

3. Go to $ONP_HOME/ONP:

```
cd /home/user/Desktop/ONP_Builds/ONP
```

```
sudo docker stack deploy -c images/conf/docker-compose.yml
--resolve-image=never cnp
```

Uninstall Cisco ONP

Use this procedure to configure and run removal commands to fully uninstall Cisco ONP and all its related files.

Remove Cisco ONP and its associated files from your system by running a series of commands.

Warning: When you uninstall Cisco ONP, you will lose all created networks and users. You must again set the admin password.

> **Note**
>
> We suggest that you perform a database backup before uninstallation. For more information, see Backup Cisco ONP Database.

Follow these steps to uninstall Cisco ONP and remove all related files:

Procedure

Run these commands **one-by-one**:

```
sudo docker stack rm cnp
sudo docker swarm leave --force

sudo apt -y purge docker-ce
sudo apt -y purge docker-ce-cli
sudo rm -rf /var/lib/postgresdb_cnp
sudo rm -rf /opt/cnp
sudo rm -rf /var/log/cnp
sudo rm -rf /var/log/nginx
sudo docker image prune -a -f
sudo rm -rf ONP
sudo rm -rf Installer.sh
sudo rm -rf SSF.sh
sudo rm -rf README.md
```

Uninstall WSL Ubuntu

Use this procedure to configure Windows and use command-line options to remove the Ubuntu distribution from Windows Subsystem for Linux.

Uninstall Ubuntu from the Windows Subsystem for Linux (WSL) environment.

Follow these steps to remove the Ubuntu distribution from Windows Subsystem for Linux:

Procedure

1. Click on the Windows **Start** button and search for **Ubuntu**.
2. Right click on **Ubuntu** and select and click **Uninstall**.
3. Open **Windows PowerShell** and type the command **wsl -l**.
4. Unregister Ubuntu by typing the command **wsl --unregister Ubuntu**.

Docker commands

This section lists essential Docker commands for managing images and containers from the command line.

This table lists docker commands that you can use to perform a specific task.

Task	Docker command
Check installed docker version	docker -v docker --version
List available docker images	docker images
List all running containers	docker ps
List all running and exited containers	docker ps -a
Remove a particular container	docker rm <container ID/ container name>
Remove a particular docker image	docker rmi <Image name / Image ID>
Fetch the logs of a container	docker logs -f <container ID>
Fetch the resource utilization by a container	docker stats <container ID>

Cisco ONP logs

This section lists the available log types for Cisco ONP, their descriptions, and how to access or locate each log.

Cisco ONP provide these logs.

This table lists the different log types available for Cisco ONP, their descriptions, and the methods or locations for accessing each log.

Table 1: Logs

Logs	Description	Example

Container logs	The command *sudo docker ps* provides the list of running containers and their IDs. Copy the container ID of that container whose log you require.
	You can obtain the log or activities of the container by using this command.
	`sudo docker logs (container name/ID) > filename.log/txt`
		Example:
		`sudo docker logs cnp > file.log`
		`sudo docker logs 274a5fc1152b > file.log`

Application logs	You can find Cisco ONP application logs in these locations: • `/var/log/cnp` • `/var/log/nginx`	-
Install logs	You can find Cisco ONP install logs in this location. `/var/log/cnp`	-

Monitor the Cisco ONP health

Use this procedure to verify that all Cisco ONP containers are running.

Ensure Cisco ONP system operates reliably by confirming all containers are healthy.

Follow this step to check the status or health of Cisco ONP.

Procedure

Run this command to list all running containers.

Example

```
$sudo docker ps
```

2 Troubleshoot

Topics:

- Troubleshooting tasks

Common issues, diagnostic steps, and resolution procedures for the Cisco Optical Network Planner.

Troubleshooting tasks

This section lists common Cisco ONP installation error messages, their causes, and recommended solutions.

This table describes the common error messages that are related to Cisco ONP installation and the workarounds.

Table 2: Troubleshooting tasks forCisco ONP installation

Warning message or error	Probable reason for the error	Workaround
Non-Responsive user interface	The Server is not reachable. Or The internet connectivity is not stable.	Check whether cnp and onp_frontend containers are running using this command: `$sudo docker ps` If the containers are not up, Restart Cisco ONP on page 15. Or Check whether the internet connectivity is fine and log in to Cisco ONP again.
PostgresDb container is not starting within stipulated time Exiting.	Server disk space has exhausted.	• Check the available disk space by using the command **df -h**. • If the memory utilization is 100%, remove the unwanted files from the server. • Retain at least 20GB of free space and reinstall Cisco ONP again.
After successful installation, not able to log in to Cisco ONP with default username and password (admin/cisco123)	Check whether any special characters are used in the Cisco ONP database username or password during installation.	Uninstall and reinstall Cisco ONP. Make sure that only alphanumeric characters are used in the database username or password.
Cisco ONP keeps on reverting to the login page after logging in.	Old browser cache may not be cleaned up.	Clear browser cache, relaunch browser and log in again.
CONP 5.2 PostgresDB volume (/var/lib/postgresdb_cnp) is not present. Data Migration Not Possible. Exiting CONP installation. Re-try CONP 24.3.1 installation without data migration option.	PostgresDB is not present.	Terminate installation using **Ctrl+C** and reinstall Cisco ONP without data migration option.

Warning message or error	Probable reason for the error	Workaround
Error response from daemon : This node is not swarm manger. Use "docker swarm init" or "docker swarm join" to connect this node to swarm and try again.	Server is not in Swarm mode.	**1.** Use this command. `$docker swarm init --advirtise-addr` *`IP address of Ubuntu Server`* **2.** Use this command. `$docker swarm join` *`token`* Use the token that is generated after running the command in the previous step. **3.** Re-install Cisco ONP.