



Overview of Cisco Optical Network Controller

- [Overview of Cisco Optical Network Controller, on page 1](#)
- [Log into Cisco Optical Network Controller, on page 2](#)
- [User Access in Cisco Optical Network Controller 24.3.1, on page 3](#)
- [Add Local Users to Cisco Optical Network Controller 24.3.1, on page 4](#)
- [Set up Authentication through LDAP, on page 7](#)
- [Set up Authentication through SAMLv2 SSO, on page 8](#)
- [Set up Permission Mapping, on page 10](#)

Overview of Cisco Optical Network Controller

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

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

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

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

- Optical Domain Controller

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

- Path Compute Engine (PCE)

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

- Model Based Network Abstraction

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

**Note**

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

Log into Cisco Optical Network Controller

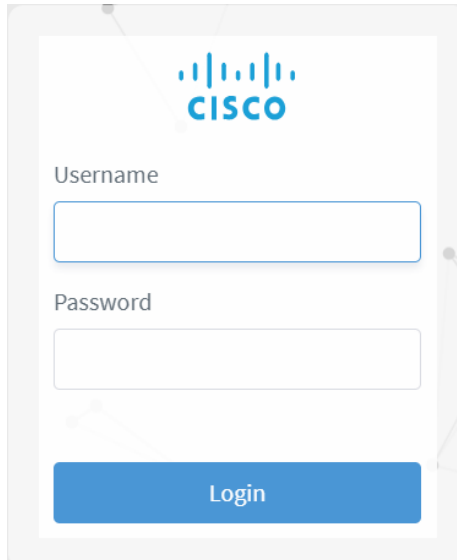
Before you begin

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

Procedure

-
- Step 1** In the browser URL field, enter **https://<virtual-ip>:8443/**
Login page is displayed.
- Step 2** Enter the username and password.
- Step 3** Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



The screenshot shows the login interface for the Cisco Optical Network Controller. At the top center is the Cisco logo. Below it, there are two input fields: one for 'Username' and one for 'Password'. At the bottom of the form is a blue button labeled 'Login'.

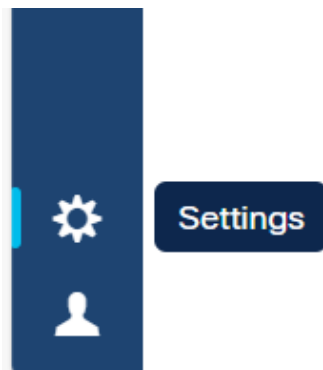
User Access in Cisco Optical Network Controller 24.3.1

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

Users, Roles, and Permissions

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

Figure 2: Settings



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

Figure 3: Settings Options

Image Name	Version
docker.io/library/alpine	3.20.0
docker.io/rancher/local-path-provisioner	v0.0.27
dockerhub.cisco.com/cisco-onc-docker/ram/metric-server	alpha-1
quay.io/coreos/etcd	v3.5.12
registry.k8s.io/coredns/coredns	v1.11.1

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

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

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

Add Local Users to Cisco Optical Network Controller 24.3.1

Before you begin

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

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

Procedure

- Step 1** From the Cisco Optical Network Controller 24.3.1 home page click **Settings** .
- Step 2** From the panel list, select **Local Users** tab and click **Add** .
- Step 3** In the **Add User** screen, enter **Username*** .
- Step 4** After entering the user name, enter **Password*** .
- Step 5** Next confirm the password using **Confirm Password*** .

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

For example *permission/<admin>*

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

Figure 4: Local Users

The screenshot shows the 'Local Users' configuration page in the Cisco Optical Network Controller. The left sidebar is dark blue with white icons and text. The 'SECURITY' section is highlighted, and 'Local Users' is selected. The main content area is white and titled 'Local Users'. It displays a list of four local users, each in a white box with a light blue border. The users are: 'internal (internal)', 'NxF Admin (admin)', 'supervisor (supervisor)', and 'readonly (readonly)'. Each user entry shows their 'ACCESS' and 'STATUS'.

Display Name	Access Permissions	Status
internal (internal)	internal	Active
NxF Admin (admin)	permission/admin	Active (Locked)
supervisor (supervisor)	supervisor	Active
readonly (readonly)	readonly	Active

At the bottom right of the page, there are two buttons: 'Reload' and 'Add...'.

Figure 5: Add User

SYSTEM INFO

Versions

SECURITY

Local Users

LDAP

SAML SSO

Permission Mapping

← Add User

Username*

Password*

Confirm Password*

Access Permissions*

permission/admin

supervisor

permission/supervisor

internal

permission/internal

readonly

permission/readonly

admin

permission/admin

Display Name

Active

Locked

Description

Save

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

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

Step 8 Click **Save**.

Set up Authentication through LDAP

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

Procedure

- Step 1** From the Cisco Optical Network Controller 24.3.1 home page click **Settings**.
- Step 2** Click **LDAP**.
- Step 3** Click the **Enabled** radio button.
- Step 4** Fill in the mandatory fields that are marked with an asterisk (*): **LDAP Server Address**, **Bind DN** and **Bind Credentials**. The **Search Filter**, **Search Base** and **Root CAs** are optional.
- Step 5** Click **Save**.

Figure 6: LDAP

LDAP

Enabled

LDAP Server Address*

Bind DN*

Bind Credentials*

Search Base

Search Filter

Attribute Value

Root CAs

Set up Authentication through SAMLv2 SSO

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

Procedure

- Step 1** In the CWM, go to the outermost navigation menu on the left
- Step 2** From the Cisco Optical Network Controller 24.3.1 home page click **Settings** and navigate to **SAML SSO** tab.
- Step 3** Click the **Enabled** radio button.
- Step 4** Fill in the fields: **Login URL**, **Entity ID**, **Base URL**, **Signing Certificate** and **Groups Attribute Name**.
- Step 5** Click **Save**.

Figure 7: SAML SSO

The screenshot displays the SAML SSO configuration interface. On the left, a vertical navigation menu includes options like Topology, Versions, SECURITY, Local Users, LDAP, SAML SSO (highlighted), and Permission Mapping. The main panel is titled 'SAML SSO' and features an 'Enabled' toggle switch. Below this are input fields for 'Login URL', 'Entity ID', and 'Base URL' (with a 'Use Current' button). A large text area for 'Signing Certificate' is present, followed by a 'Groups Attribute Name' field containing the text 'memberOf'. At the bottom right, there are 'Reload' and 'Save' buttons.

Set up Permission Mapping

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

Procedure

- Step 1** From the Cisco Optical Network Controller 24.3.1 home page click **Settings**.
- Step 2** Navigate to **Permission Mapping**.
- Step 3** Click **Add**.
- Step 4** In the **Add Permission Mapping** panel, choose one **Mapping Type** from the dropdown menu: **SAML User**, **SAML Group**, **LDAP User**, or **LDAP Group**.
- Step 5** Fill in the **Match** field.
- Step 6** Select the appropriate **Access Permission**.
- Step 7** Click **Save**.

Figure 8: Permission Mapping

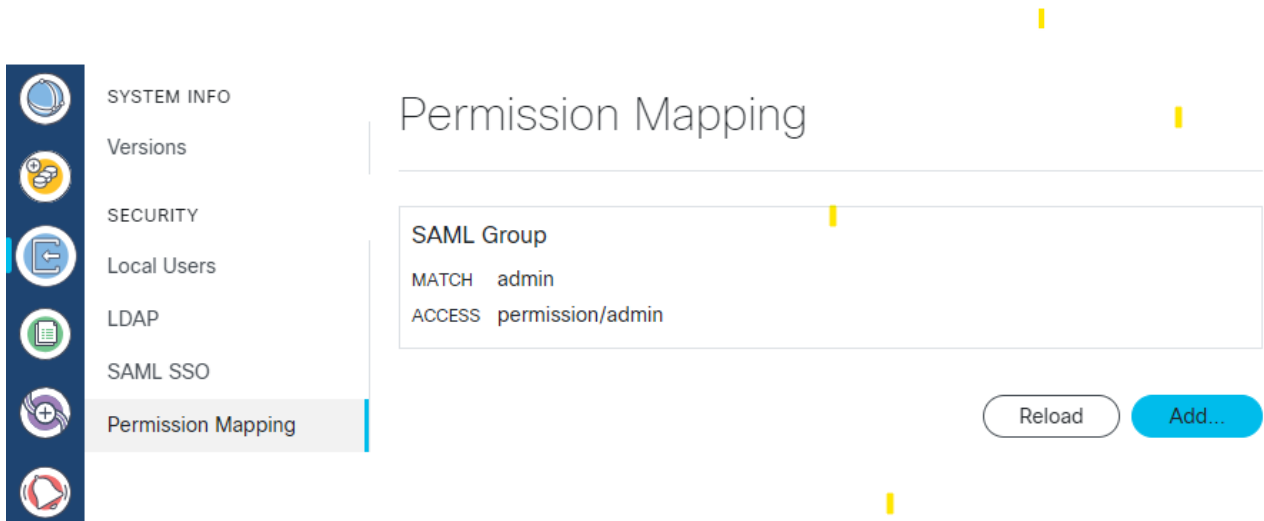


Figure 9: Add Permission Mapping

Topology FO

Versions

SECURITY

Local Users

LDAP

SAML SSO

Permission Mapping

← Add Permission Mapping

Mapping Type*

SAML Group

Match*

Access Permissions*

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

Save

Note User can have different levels of permission mapping.

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

