Overview of Cisco Optical Network Controller

Overview of Cisco Optical Network Controller

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

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

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

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

- Optical Domain Controller

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

- Path Compute Engine (PCE)

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

- Model Based Network Abstraction

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

Note

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

Log into Cisco Optical Network Controller

Before you begin

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

Procedure

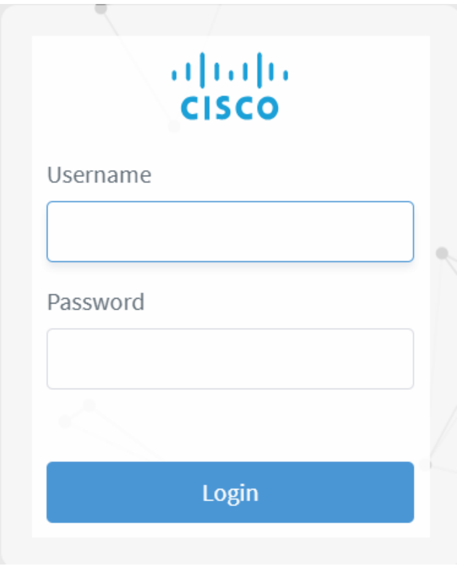
Step 1 In the browser URL field, enter **https://<virtual-ip>:8443/**

Login page is displayed.

Step 2 Enter the username and password.

Step 3 Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



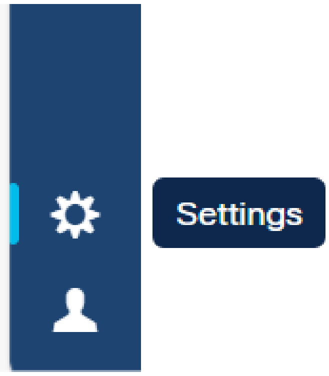
User Access in Cisco Optical Network Controller 24.3.1

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

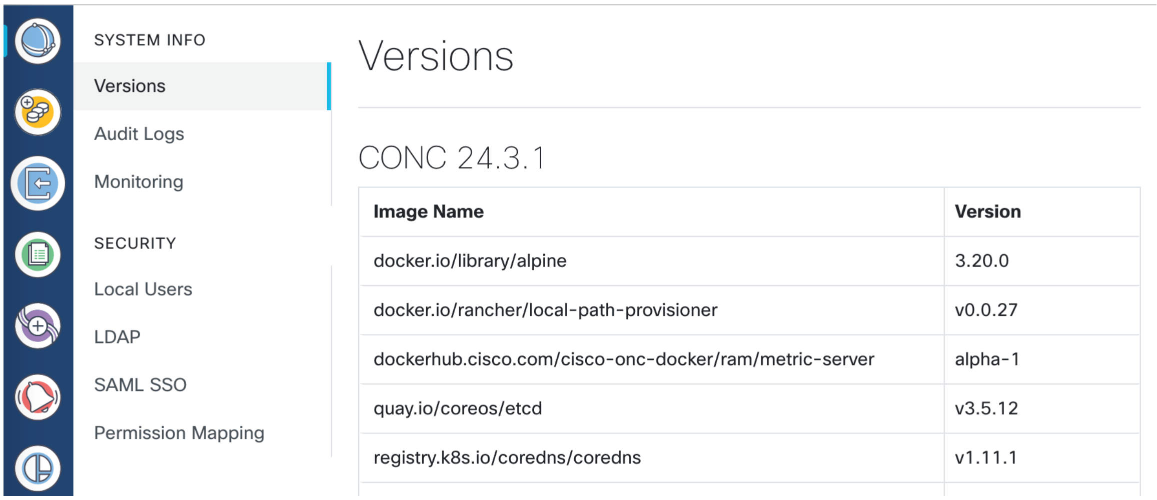
User can have have different permission levels. See *Set up Permission Mapping*. To allow access to Cisco ONC to a larger group of regular users, set the user authentication through LDAP or SAML SSO protocols. You can use both at the same time as well, depending on your environment.

Figure 2: Settings



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

Figure 3: Settings Options



Versions

CONC 24.3.1

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*** .

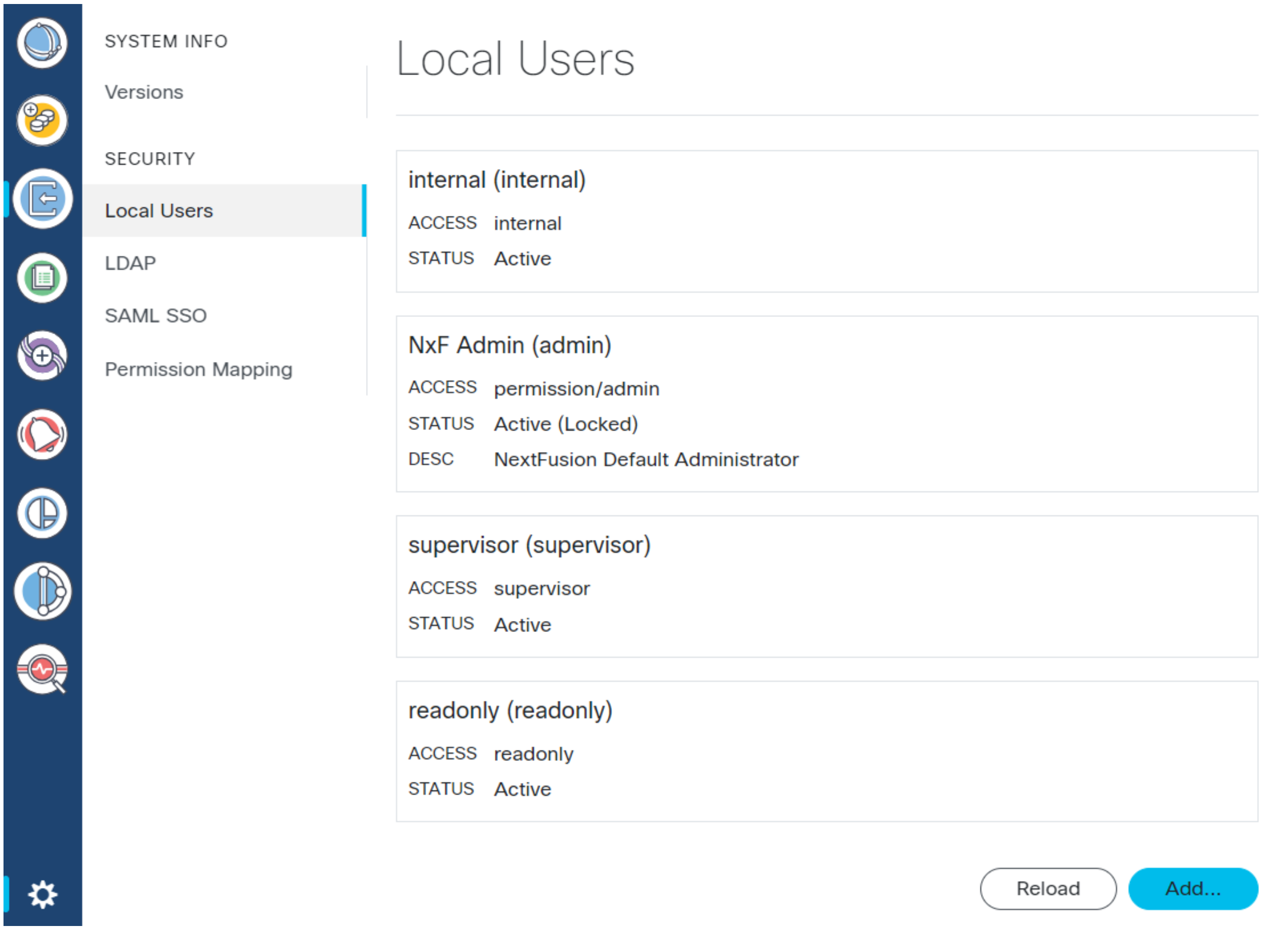
Step 5 Next confirm the password using **Confirm Password*** .

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



Local Users

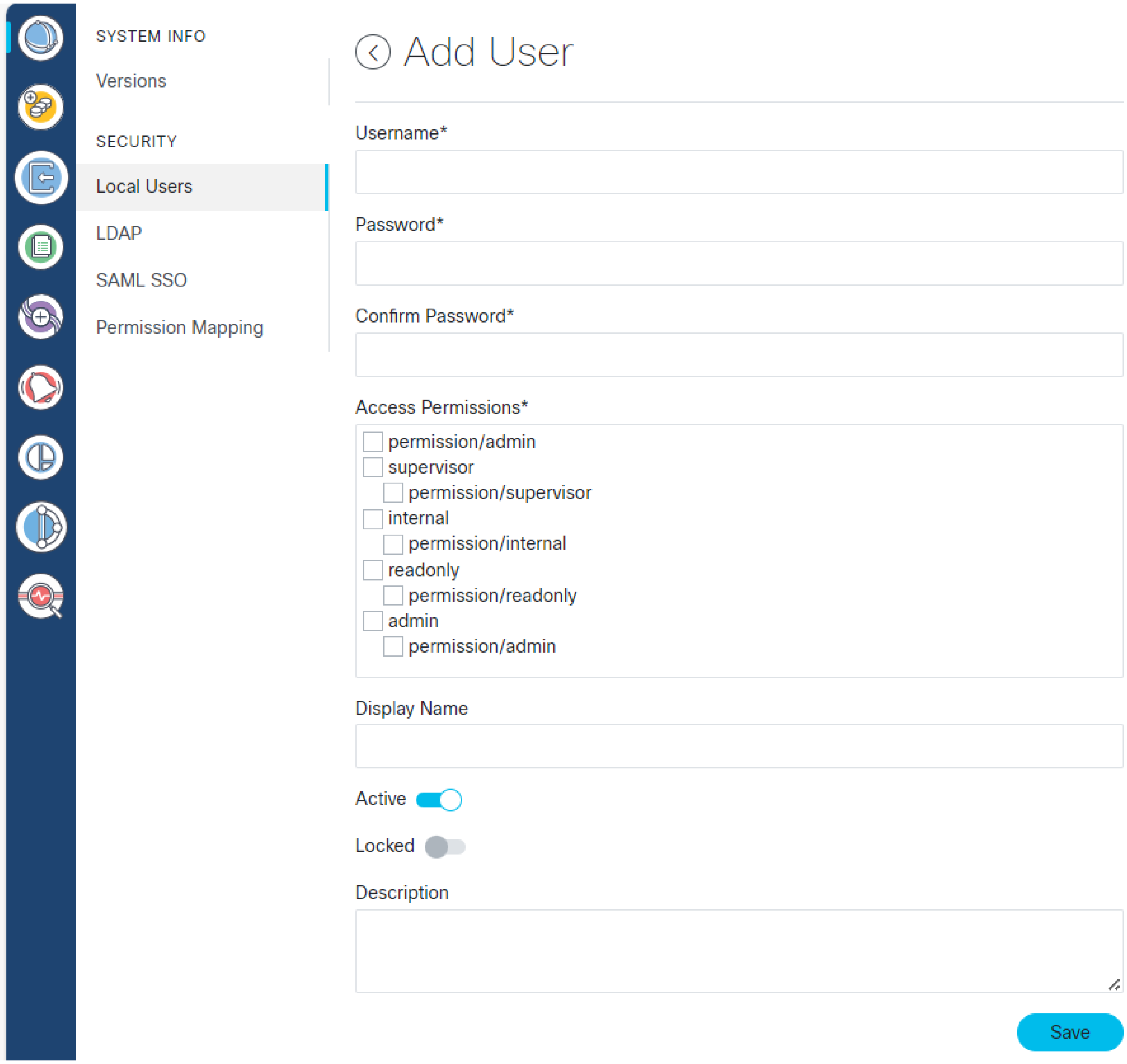
internal (internal)
ACCESS internal
STATUS Active

NxF Admin (admin)
ACCESS permission/admin
STATUS Active (Locked)
DESC NextFusion Default Administrator

supervisor (supervisor)
ACCESS supervisor
STATUS Active

readonly (readonly)
ACCESS readonly
STATUS Active

Figure 5: 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

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**.

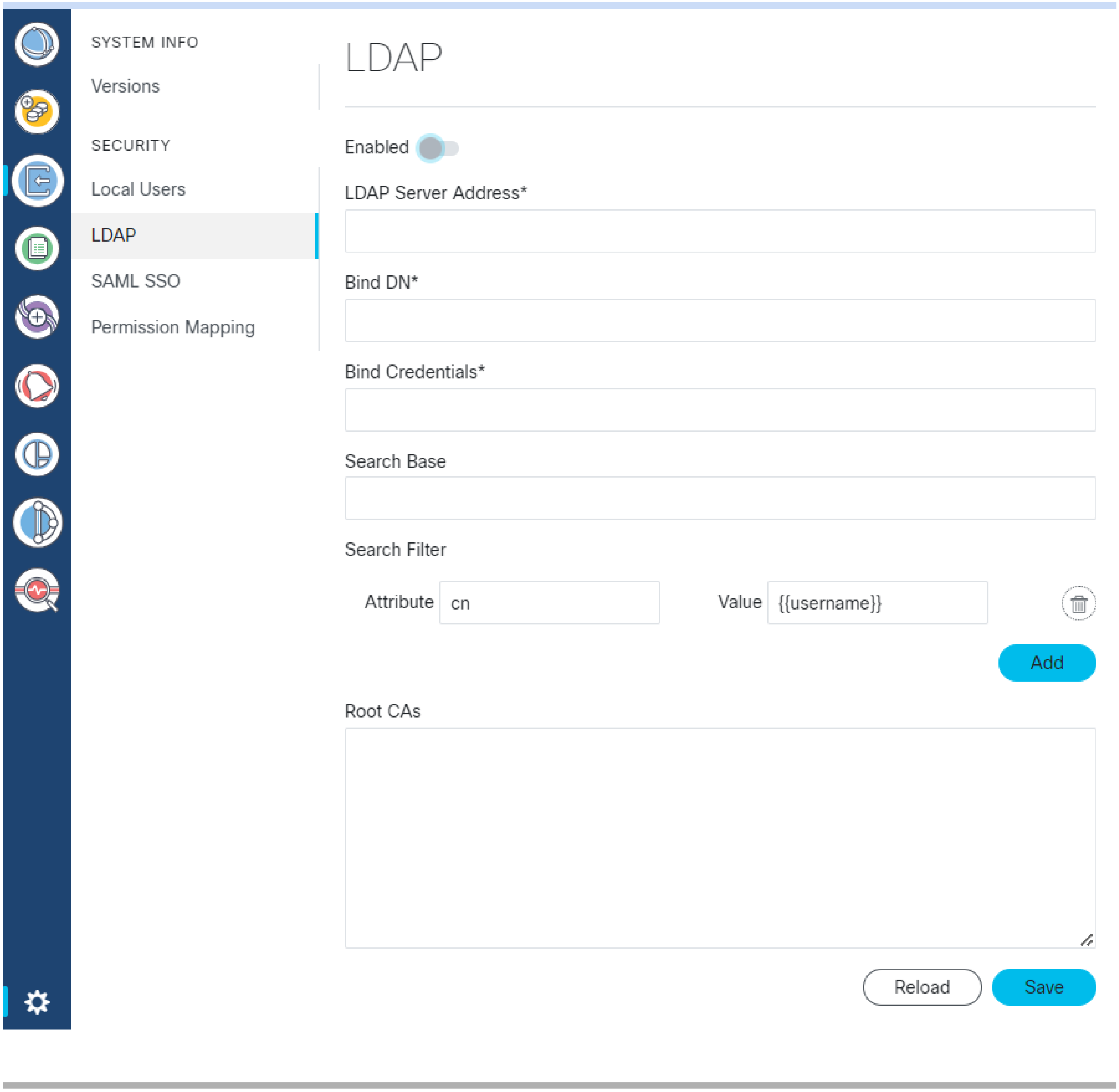
Step 2 Click **LDAP**.

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



Attribute cn

Value {{username}}

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.

Before you begin

To set up Authentication through SAMLv2 SSO, ensure you have your own SSO server installed and configured to use for the SSO application.

Procedure

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

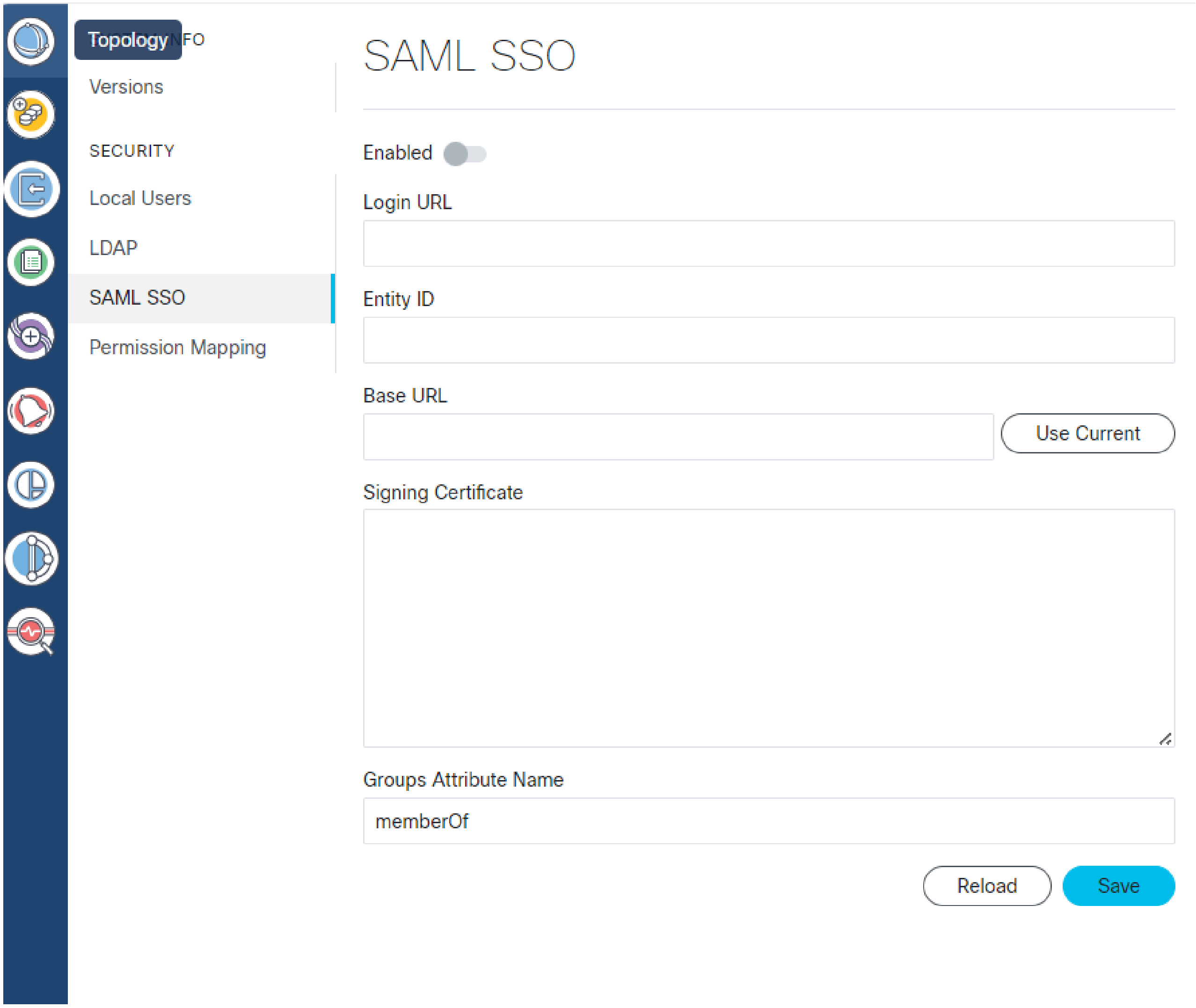
Step 2 From the Cisco Optical Network Controller 24.3.1 home page click **Settings** and navigate to **SAML SSO** tab.

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



SAML SSO

Enabled ○

Login URL

Entity ID

Base URL

Signing Certificate

Groups Attribute Name

memberOf

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**.

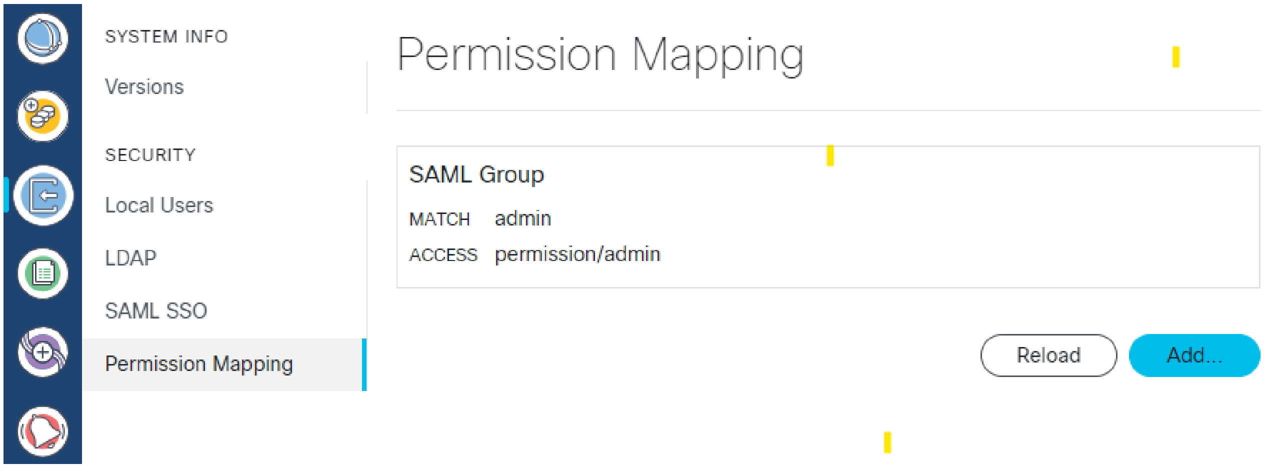
Step 4 In the **Add Permission Mapping** panel, choose one **Mapping Type** from the dropdown menu: **SAML User**, **SAML Group**, **LDAP User**, or **LDAP Group**.

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

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

Step 7 Click **Save**.

Figure 8: Permission Mapping

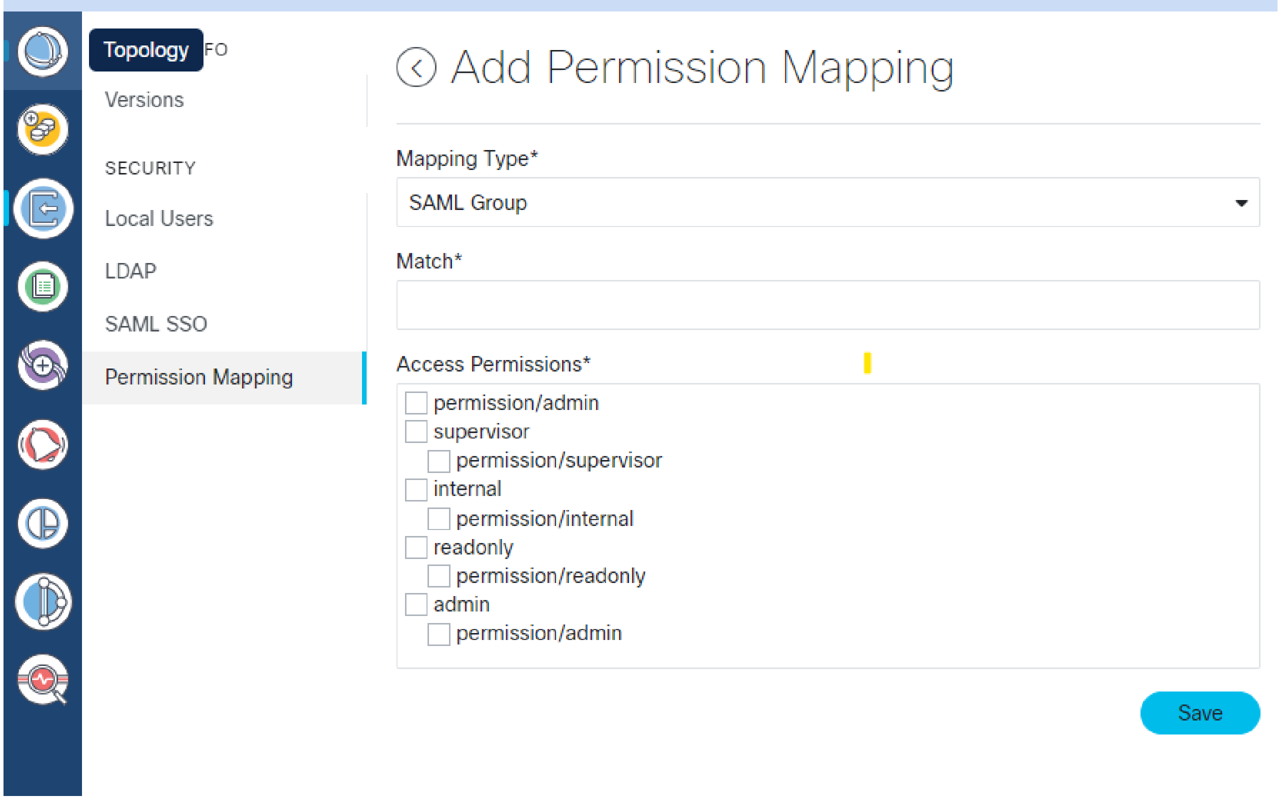


SAML Group

MATCH admin

ACCESS permission/admin

Figure 9: Add 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

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).

Manage Certificates in Cisco Optical Network Controller

When a Cisco Optical Network Controller cluster is created, unique self-signed EC/RSA certificates are generated for incoming HTTPS connections to the ingress-proxy. These certificates are intended for initial configuration only. From Cisco Optical Network Controller Release 24.3.1, you can create a Certificate Signing Request (CSR) and upload a signed certificate bundle using the sedo CLI administration tool.

Procedure

Step 1 Create a Certificate Signing Request (CSR) using the sedo CLI tool. You can choose between RSA and EC certificates.

Example:

For RSA:

```
sedo security certs request rsa --country <Country Name> --organization <Organization Name> <Domain
 Name or IP>
```

Example:

For EC:

```
sedo security certs request ec --country <Country Name> --organization <Organization Name> <Domain
Name or IP>
```

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

Submit the generated CSR to a Certificate Authority to obtain a signed certificate.

Step 3 If your CA provides individual certificates instead of certificate chain, create a certificate chain. You must follow the exact order to create the chain. Copy the signed certificate to the CONC virtual machine location /data and create a chain of certificates in output.crt:

Example:

```
cat /data/signed_certificate.crt /path/to/issuing_ca_certificate.crt /path/to/root_ca_certificate.crt
 > /data/output.crt
```

Example:

Replace the paths with the actual paths to your Issuing CA and Root CA certificates. Ensure that the paths are accessible from the VM, and adjust the command as needed based on your specific environment and file paths.

Step 4 Upload the prepared certificate chain to the system:

Example:

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

Step 5 Verify the uploaded certificates:

Example:

```
 sedo security certs list

┌──────────────────────────────────────────────────────────────────────────────────────────────────┐
│ Installed Certificates
                               │
├──┬──────────────────┬──────────────────┬─────────────┬────────────┬────┬────┬──────────────────────┤
│ TYPE │ SUBJECT                                  │ ISSUER                                   │ ISSUED
                      │ EXPIRES                               │ DNS SANS   │ IP SANS │ SERIAL NUMBER
                            │
├──┼──────────────────┼──────────────────┼─────────────┼────────────┼────┼────┼──────────────────────┤
│ EC    │ CN=NextFusion,O=Cisco,ST=California,C=US │ CN=NextFusion,O=Cisco,ST=California,C=US │ Mon
```

```
Nov 18 22:46:18 GMT 2024 │ Thu Nov 18 22:46:18 GMT 2027 │ nxf.local │         │
1445557328950165706858003484413381754985522282604 │

│ RSA  │ CN=NextFusion,O=Cisco,ST=California,C=US │ CN=NextFusion,O=Cisco,ST=California,C=US │ Mon
Nov 18 22:46:18 GMT 2024 │ Thu Nov 18 22:46:18 GMT 2027 │ nxf.local │         │
1232594841637394522581611101986931324866857045143 │

└──┴──────────────────┴──────────────────┴─────────────┴────────────┴────┴────┴─────────────────────┘
```

If you are replacing the self-signed certificate with the active `output.crt` (CA-signed chain certificate), ensure to delete any other certificates if only one certificate is being replaced.

```
sedo security certs delete ec
```