Overview of Cisco Optical Network Controller

Cisco Optical Network Controller Overview

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

- Collects information about the inventory (device types, circuits and more) and topology (node arrangment) of the managed network.
- Monitors the physical or virtual topology of the network.
- Notifies of changes in topology and service changes.
- Supports the creation and deletion of optical paths.

Optical SDN controller

Optical SDN controller is a specialized SDN controller that

- manages and controls devices within a optical technology domain, and
- communicates with the higher-level SDN controller via east-west interfaces

Core functions of Cisco Optical Network Controller

Cisco Optical Network Controller collects data necessary for optical applications. This data is used to provide abstract network information to higher layer controllers. This abstraction enables centralized control of optical network.

Cisco Optical Network Controller supports several functions.

- Optical Domain Controller

  Cisco Optical Network Controller behaves as a domain controller for Cisco optical products. The domain controller feeds data into hierarchical controllers for high-level network orchestration. Cisco Optical Network Controller has a North Bound Interface (NBI) based on the OIF transport API (T-API) standard which enables it to connect to any hierarchical controller which has a TAPI compliant South Bound Interface (SBI) and provides 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 to compute the optical path.

- 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 Cisco Optical Network Controller (CONC) Data Sheet .

Important

- TAPI is disabled by default to ensure proper device integration and data collection, enabling seamless operation. You must enable it before onboarding devices.
- You must not enable TAPI after onboarding devices 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.

  To enable or disable TAPI, see Enabling and Disabling the TAPI Northbound Interface

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.

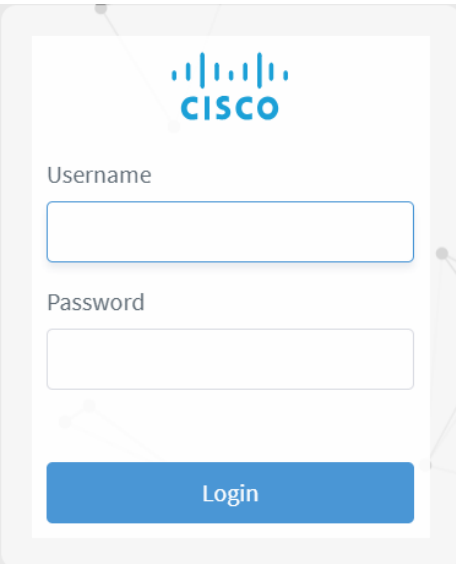
The browser displays the login page.

Step 2 Enter the username and password.

Username and password are provided by your system administrator.

Step 3 Click **Login**.

Figure 1: Log into Cisco Optical Network Controller



User access in Cisco Optical Network Controller

Users, Roles, and Permissions

Cisco Optical Network Controller allows you to manage user access and permissions. It adds an additional layer of security. It works as a Single Authentication Agent, thus sharing local, Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML) users. The Single Authentication Agent simplifies user management and provides a unified login experience across different authentication sources.

Cisco Optical Network Controller provides different permission levels for user access. See *Set up Permission Mapping*. To allow access to Cisco Optical Network Controller to a larger group of regular users, set the user

authentication through LDAP or SAML Single Sign-On (SSO) protocols. You can use both protocols simultaneously, depending on your environment.

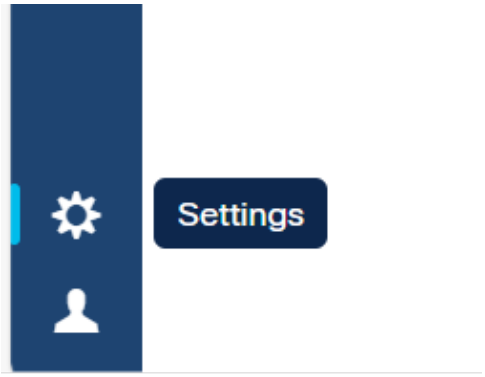
Table 1: User roles and permissions

User role	Permission	Access level
Admin	permission/admin	has no restrictions
Supervisor	permission/supervisor	has similar permission as admin but with restrictions on user management and log checks
Read-only	permission/readonly	can check data, but cannot provision.
Internal	permission/internal	collects debug logs in case of any triage or troubleshooting. **Note** We recommend using it only under the supervision of the Cisco Technical Assistance Center (TAC).

Accessing Settings

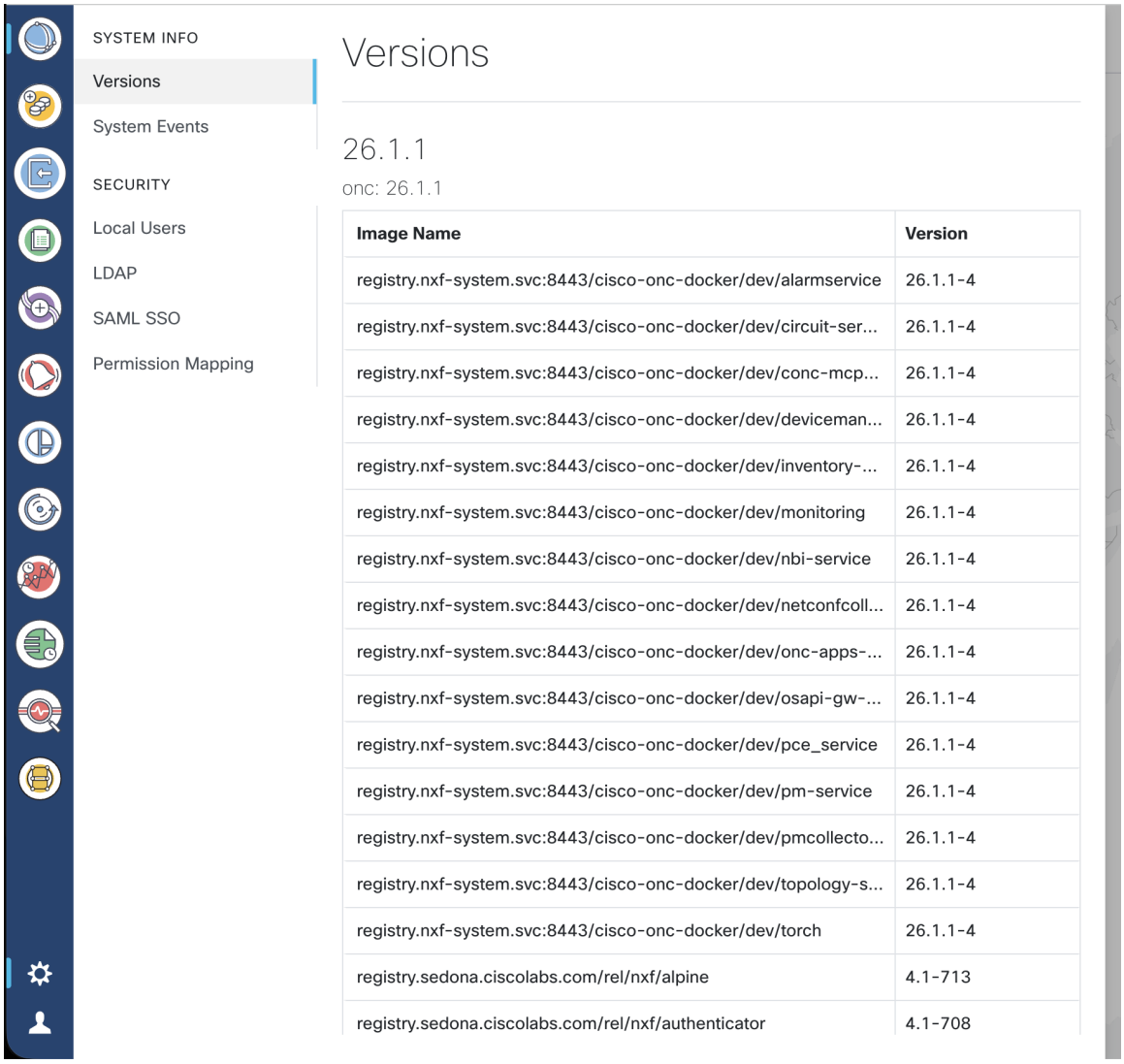
The settings button is available on the left navigation bar of Cisco Optical Network Controller.

Figure 2: Settings



After clicking **Settings** you see the settings panel.

Figure 3: Settings Options



System Info

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

Security

The **Security** section is for access management and offers several options.

- **Local Users**: Display, create, and edit local users through the UI.
- **LDAP**: Set LDAP settings for user authentication.
- **SAML SSO**: Set SAML Single-Sign-On settings for user authentication.
- **Permission Mapping**: Handle permission management through the Cisco Policy Management Tool.

Note Cisco Optical Network Controller does not allow the configuration of timeout and retry client parameters for LDAP and SAML SSO authentication. Instead, it automatically applies the default values to the timeout and retry settings.

Add local users to Cisco Optical Network Controller

Add local user accounts to Cisco Optical Network Controller by completing these steps.

Before you begin

You need administrative user privileges to access Cisco Optical Network Controller.

Procedure

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

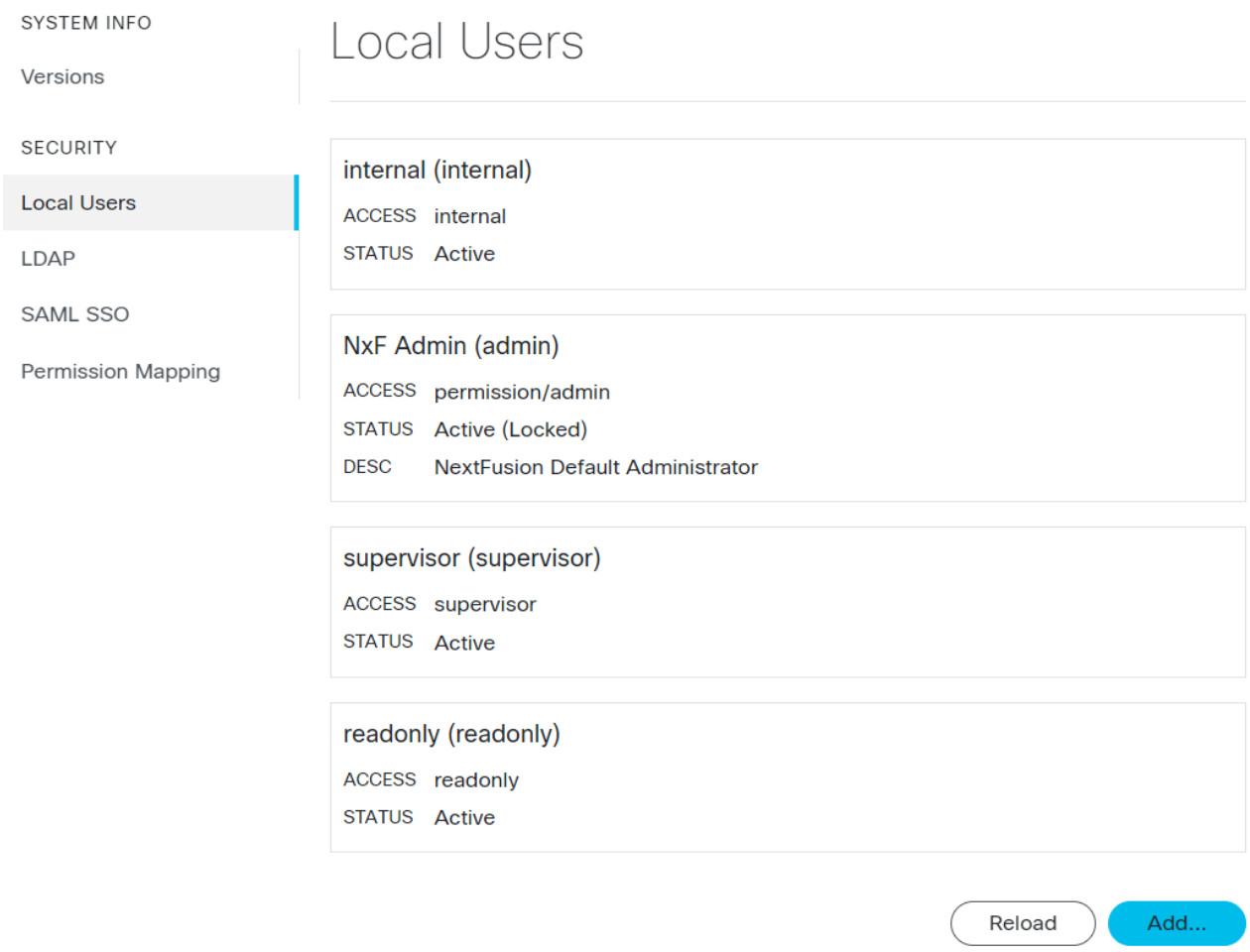
Step 2 From the panel list, select **Local Users** and click **Add**.
The **Add User** screen appears.

Step 3 In the **Add User** screen, fill these mandatory fields.

a) Enter a username in **Username***.
b) In **Password***, enter a password.
c) In **Confirm Password***, re-enter the password to confirm the password.

Step 4 Select the access permissions from the list **Access Permissions***.

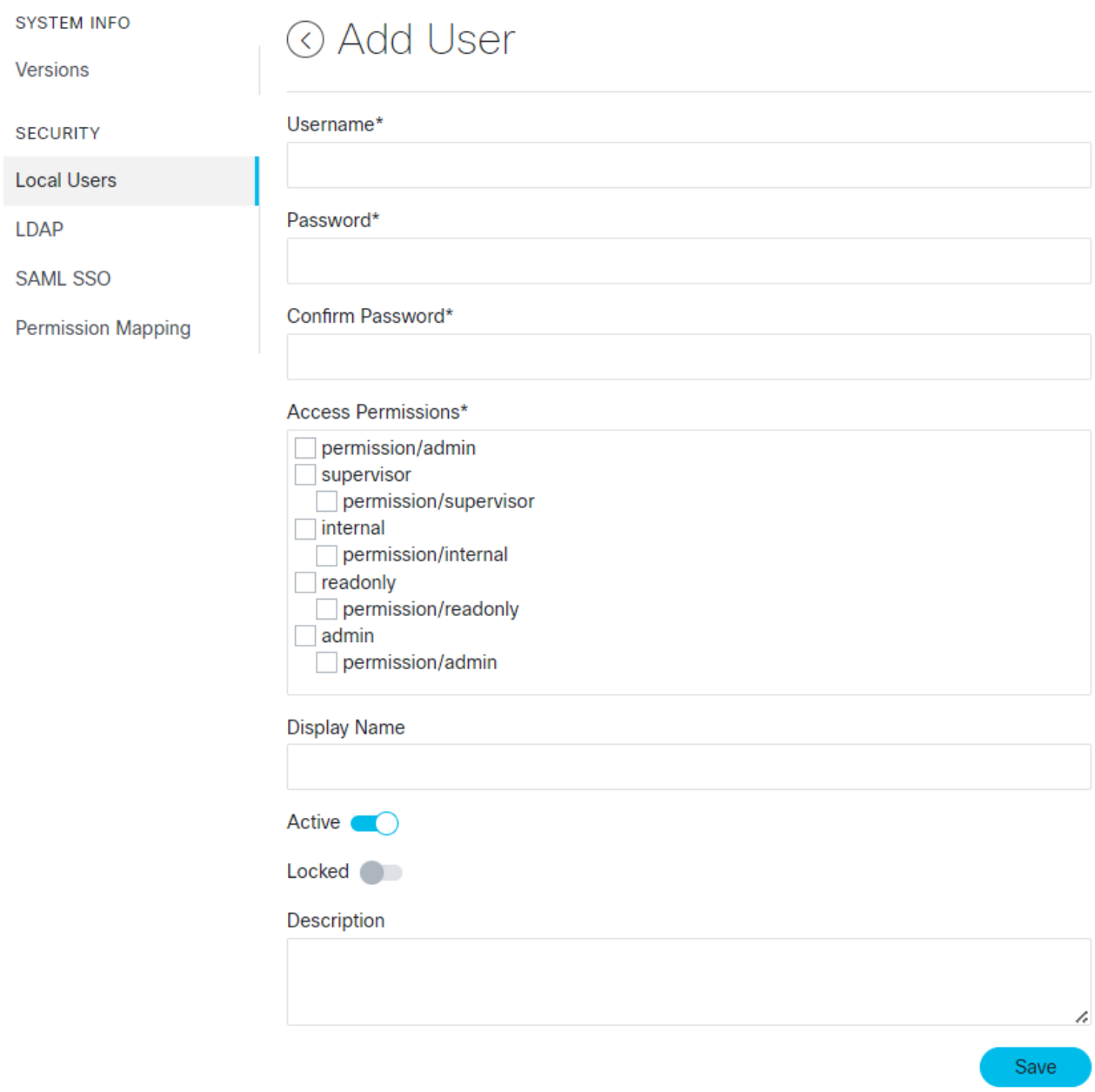
Figure 4: Local Users



For example *permission/<admin>*

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

Figure 5: Add User



Step 5 Use the toggle switches to set the user status.

Note
The toggle switches are independent of each other, they can both be disabled or enabled at the same time.

- **Active enabled**: Allows the user to log into Cisco Optical Network Controller.
- **Active disabled**: Forbids the user from logging into Cisco Optical Network Controller.

- **Locked enabled**: Prevents deleting the user for auditing purposes or to retain historical data associated with that user.
- **Locked disabled**: Allows removal of the user

Table 2: Toggle combinations

Active status	Locked status	User status
Active enabled	Locked enabled	Prevents accidental deletion of user
Active enabled	Locked disabled	Allows user deletion
Active disabled	Locked disabled	Temporarily disables a user and allows user deletion
Active disabled	Locked enabled	Temporarily disables a user but prevent accidental deletion

Step 6 Click **Save**.

Cisco Optical Network Controller successfully saves the new user.

Set up authentication using LDAP

Set up user authentication using the Lightweight Directory Access Protocol (LDAP) on Cisco Optical Network Controller can be performed by following these instructions.

Before you begin

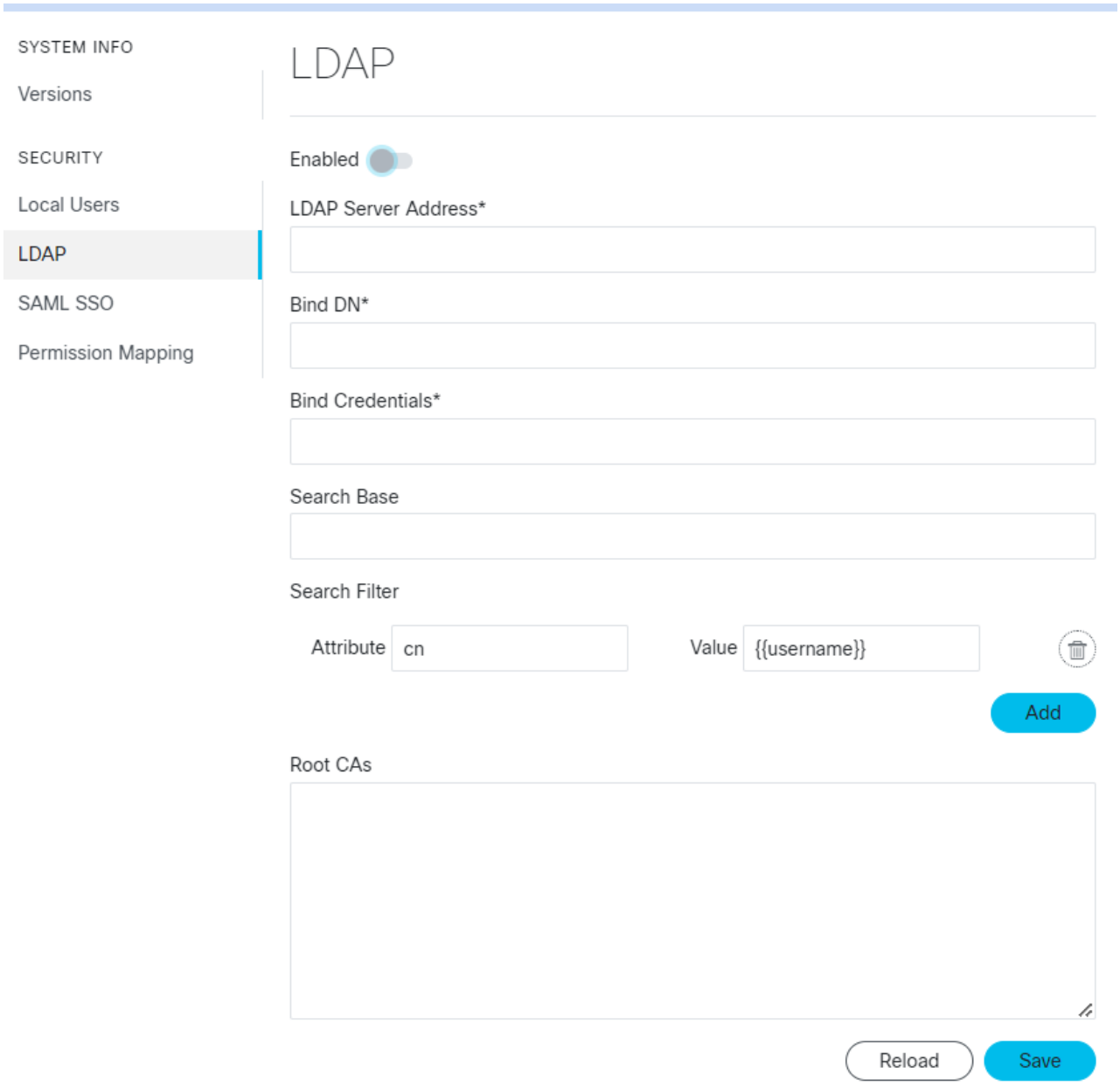
You need administrative user privileges to access Cisco Optical Network Controller.

Procedure

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

Step 2 Click **LDAP**.

Figure 6: LDAP



Step 3 Enable **Enabled** toggle switch.

Step 4 Fill in the mandatory fields marked with an asterisk.

Table 3: Madatory LDAP fields

Field	Description	Value
LDAP Server Address	The IP address to your LDAP server.	This server address is set by your organization's LDAP administrator.

Field	Description	Value
Bind DN	The Distinguished Name of the user account used to connect to the LDAP directory.	This value is provided by your organization's LDAP administrator.
Bind Credentials	The password to authenticate your user account.	This value is provided by your organization's LDAP administrator.

LDAP Server Address, **Bind DN** and **Bind Credentials** are mandatory fields. The **Search Filter**, **Search Base** and **Root CAs** are optional fields.

Step 5 Click **Save**.

You have successfully completed the LDAP authentication setup.

Set up authentication using SAMLv2 SSO

The Security Assertion Markup Language (SAML) SSO allows you to gain single sign-on access based on the SAMLv2 protocol. Both local and external users can authenticate using SSO user credentials if their accounts are mapped.

Follow these instructions to set up SAML SSO authentication.

Before you begin

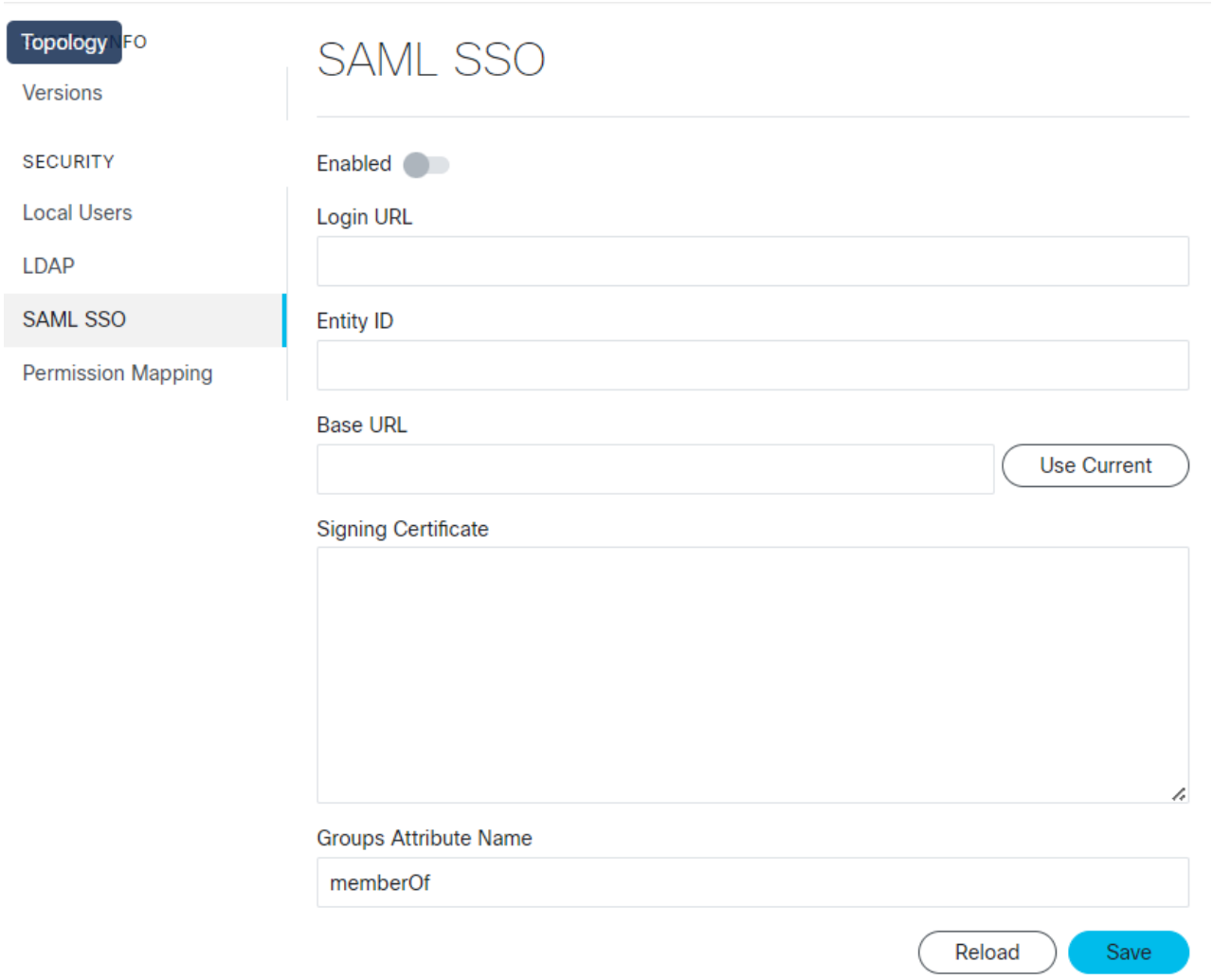
Ensure you have administrative user privileges to access Cisco Optical Network Controller.

To set up authentication using SAMLv2 SSO, ensure your SSO server is installed and configured for the application.

Procedure

Step 1 From the Cisco Optical Network Controller UI click **Settings** and select **SAML SSO**.

Figure 7: SAML SSO



Step 2 Enable **Enabled** toggle switch.

Step 3 Fill in the fields.

Table 4: SAML SSO fields

Field	Description	Value
Login URL	Sign on URL for the Cisco ONC	Cisco ONC URL
Entity ID	A unique identifier for Cisco ONC within the SAML federation, provided by your Identity Provider.	This value is provided by your organization's SSO administrator or identity provider (IdP)

Field	Description	Value
Base URL	Click **Use Current** to use the current URL.	Current URL
Signing Certificate	A downloaded certificate for Cisco ONC within the SAML federation, provided by your Identity Provider.	This value is provided by your organization's SSO administrator or identity provider (IdP)
Groups Attribute Name	Name of the group attribute that is assigned to you by your IdP.	memberOf

Step 4 Click **Save**.

You successfully completed the SAMLv2 SSO authentication setup.

Set up Permission Mapping

Cisco Optical Network Controller offers different permission levels for user access. Specific permissions can be granted to a user or group of users using this option. Follow these steps to set up permission mapping.

Before you begin

You need administrative user privileges to access Cisco Optical Network Controller.

Procedure

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

Step 2 Select **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 the **Match** field.

For example, enter a specific username like 'jsmith' or a group name like 'network_admins' from your SAML/LDAP directory.

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

Step 7 Click **Save**.

Figure 8: Permission Mapping

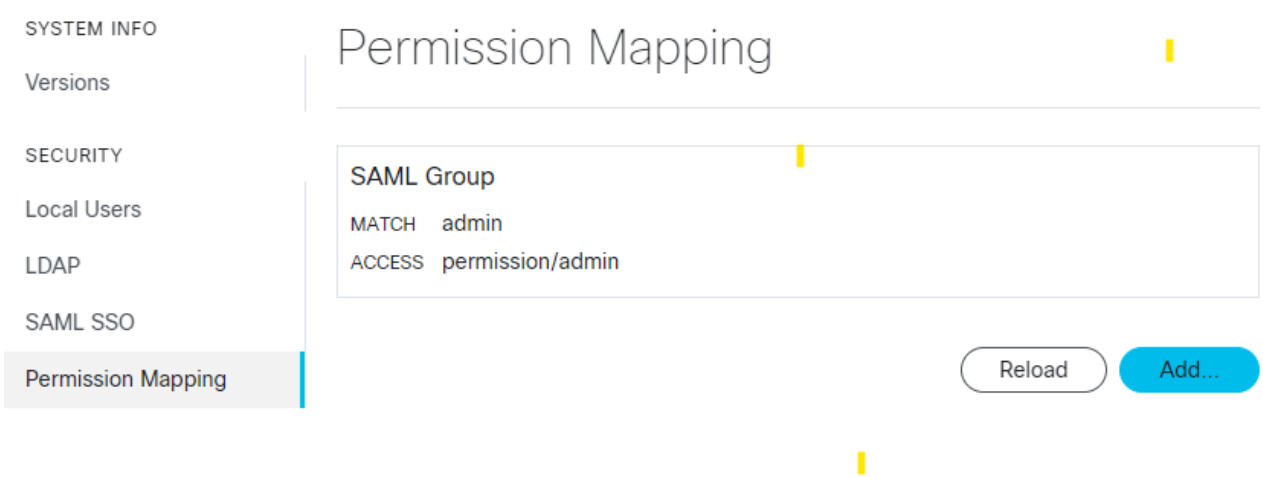
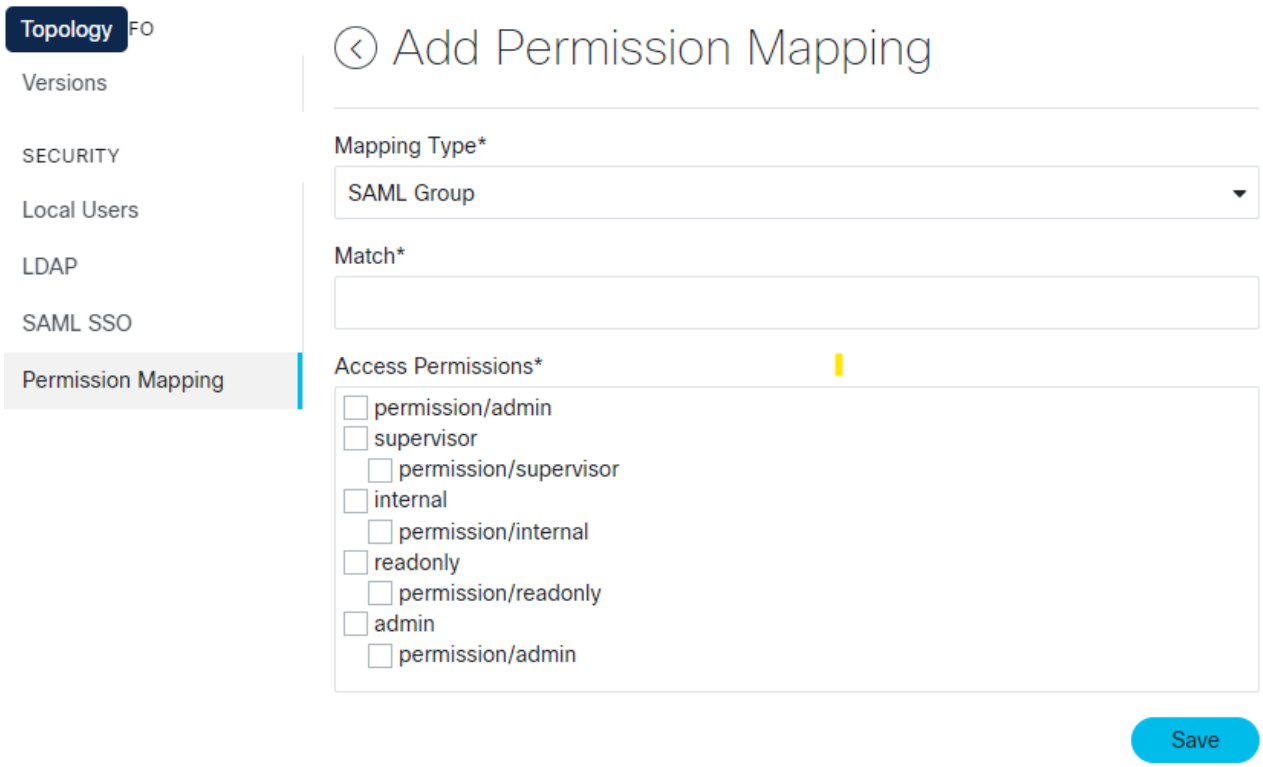


Figure 9: Add Permission Mapping



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. Ingress-proxy is the component that handles incoming network traffic and routes traffic to various services within the cluster. 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 command-line interface (CLI) administration tool, a powerful tool for system administration.

Before you begin

This section requires advanced knowledge of certificate management, command-line interfaces, and security concepts.

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).

This is an external process. Submit the generated CSR to your organization's Certificate Authority (CA) or a trusted public CA 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 │         │ 144555732895016570685800348441338175498552228260 4 │
│ 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 │         │ 123259484163739452258161110198693132486685704514 3 │
└──┴──────┴──────────────────────────────────────┴──────────────────────────────────────┴──────────────────────┴──────────┴──────────┴─────────┴──────────────────┘
```

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. This helps avoid conflicts and ensure the system uses the newly uploaded, trusted certificate.

```
sedo security certs delete ec
```

Cisco Optical Network Controller MCP server

The Cisco Optical Network Controller MCP server is a Model Context Protocol (MCP) service that exposes supported Cisco Optical Network Controller APIs as tools for AI agents.

- Cisco Optical Network Controller MCP server is an optional component that requires an additional patch installation. If you want to deploy the MCP server, contact Cisco TAC for guidance and assistance with the installation process.
- AI agents connect to the server by using an MCP client configuration that includes the Cisco Optical Network Controller MCP endpoint and an `Authorization` header with Base64-encoded Cisco Optical Network Controller credentials.
- Installing a Cisco Optical Network Controller service pack disables the MCP Server. Contact Cisco TAC to enabled the MCP server again.

How AI agents use the Cisco Optical Network Controller MCP server

Use the Cisco Optical Network Controller MCP server when you want an MCP-compatible agent to query Cisco Optical Network Controller by calling supported tools instead of directly invoking individual REST APIs.

- The agent discovers the tools that the Cisco Optical Network Controller MCP server publishes and selects the required tool or tools based on the user request.
- The MCP server acts as an integration layer between the AI agent and Cisco Optical Network Controller and returns live data from the target system.
- If the Cisco Optical Network Controller deployment uses a self-signed HTTPS certificate, the MCP client must trust that certificate or use a client-specific workaround before it can connect successfully.

Additional hardware requirements

This table lists the minimum additional hardware requirements to run the Cisco Optical Network Controller MCP server. These CPU requirements are in addition to the vCPU requirements that are listed in the Minimum Hardware Requirements table in the Installation requirements section.

Table 5: MCP server additional hardware requirements

Sizing	CPUs
Extra Small (XS)	16 vCPU baseline + 2 additional vCPU
Small (S)	32 vCPU baseline + 2 additional vCPU
Medium (M)	48 vCPU baseline + 4 additional vCPU

Configure Cisco Optical Network Controller MCP server settings in an AI agent

Create the MCP client configuration that allows an MCP-compatible AI agent to connect to the Cisco Optical Network Controller MCP server and use the published tools.

The Cisco Optical Network Controller MCP server is a feature that is packaged with this release but disabled by default. Cisco TAC or CX must enable the server before you start this procedure.

Before you begin

Before you begin, verify that you have these items:

- Access to a Cisco Optical Network Controller deployment where the Cisco Optical Network Controller MCP server is enabled
- A valid Cisco Optical Network Controller username and password
- An AI agent or MCP client that supports HTTP-based MCP server connections

Follow these steps to configure an MCP-compatible AI agent for the Cisco Optical Network Controller MCP server.

Procedure

Step 1 Enable the Cisco Optical Network Controller MCP server.

a) Contact Cisco TAC to enable the MCP server.

Warning

Installing a Cisco Optical Network Controller service pack disables the MCP Server. Contact Cisco TAC to enabled the MCP server again.

b) Reboot the VM.

The Cisco Optical Network Controller MCP server is enabled and ready for client configuration.

Step 2 Run this command in the operating system terminal to generate the Base64-encoded credentials for the *Authorization* header.

Example:

```
printf '%s:%s' "<conc-username>" "<conc-password>" | base64
```

When you add the encoded value to the MCP configuration file, prefix it with `Basic` and a space.

Example:

If your output is *aW50ZXJuXYw6Q2lZZ29ATMIz*, your configuration entry should look like this:

```
"Authorization": "Basic aW50ZXJuXYw6Q2lZZ29ATMIz"
```

You have the encoded credential string that the AI agent uses in the MCP server configuration.

Step 3 Open the MCP server configuration for your AI agent.

The exact location and method depends on the AI agent.

Step 4 Add the Cisco Optical Network Controller MCP server configuration.

```
{
  "servers": {
    "conc-mcp-server": {
      "url": "https://<conc-hostname-or-ip>:8443/onc-mcp-server/mcp",
      "type": "http",
      "headers": {
        "Authorization": "Basic <base64-encoded-credentials>"
      }
    }
  },
  "inputs": []
}
```

Replace `<conc-hostname-or-ip>` with the Cisco Optical Network Controller host name or IP address that the client can reach.

Example:

```
{
  "servers": {
    "conc-mcp-server": {
      "url": "https://10.0.10.1:8443/onc-mcp-server/mcp",
      "type": "http",
      "headers": {
        "Authorization": "Basic aW50ZXJuXYw6Q2lZZ29ATMIz"
      }
    }
  },
  "inputs": []
}
```

Step 5 CONC MCP server uses a self-signed certificate by default, which some agents may not support, in this case:

- Use a CA signed certificate by raising a certificate signing request.

For more details on creating a certificate signing request, see Manage Certificates in Cisco Optical Network Controller.

- Use an agent that can handle self-signed certificate.

Note
If the deployment uses a CA-signed certificate, you do not need this workaround.

Step 6 Enable **conc-mcp-server** in the AI agent and test the connection.

Ask a question such as `What tools are available from the MCP server?`.

The AI agent returns the list of tools that the Cisco Optical Network Controller MCP server publishes.

The AI agent is configured to use the Cisco Optical Network Controller MCP server and can query live Cisco Optical Network Controller data through the published MCP tools.

Cisco Optical Network Controller MCP server tool descriptions

Cisco Optical Network Controller MCP server tools provide access to specific controller data, such as alarms, services, inventory, node status, and network summary information.

Cisco Optical Network Controller MCP server provides these tools:

Table 6: Cisco Optical Network Controller MCP server tool descriptions

Tool name	Description
`get_conc_agent_guide`	Returns the Cisco Optical Network Controller MCP server agent instruction guide and tool-usage guidance. This is also available as resource for agents that support it.
`get_ns_timestamp_with_current_date`	Returns nanosecond timestamps and dates for a relative or custom time range.
`get_chassis_utilization`	Analyzes rack, shelf, and chassis utilization data across the network.
`get_conc_version`	Returns the current Cisco Optical Network Controller software version.
`get_top_n_issues`	Returns the top network issues or alarms, with optional service impact information.
`get_nodes_status`	Returns the current status of nodes in the network.
`analyze_alarms`	Analyzes one or more alarms and provides occurrence statistics and resolution guidance.
`get_network_summary`	Returns a summary dashboard of overall network status metrics.

Tool name	Description
`get_top_n_history_of_alarms`	Returns the top historical alarms for a selected time period.
`get_conc_services_mini_data`	Returns minimal service or circuit details for the network.
`get_services_by_site`	Returns the services for a specific site or node.
`get_services_by_ppm_and_card`	Returns the services that pass through a specific PPM or card.
`get_historical_flapping_alarms`	Returns historical flapping or fluctuating alarms.
`get_services_affected_count_by_top_alarms`	Returns the count of services that are affected by the top alarms.
`get_services_affected_details_by_top_alarms`	Returns detailed information about services that are affected by the top alarms.
`get_current_alarm_details`	Returns current alarm details with field selection and severity filtering.
`get_historical_alarm_details`	Returns historical alarm details and trends for a selected time range.
`get_services_data_details`	Returns detailed information about network services or circuits.
`quick_search`	Performs a unified search across network inventory tables.
`get_nodes_data`	Returns detailed node or site inventory data from the node inventory API.