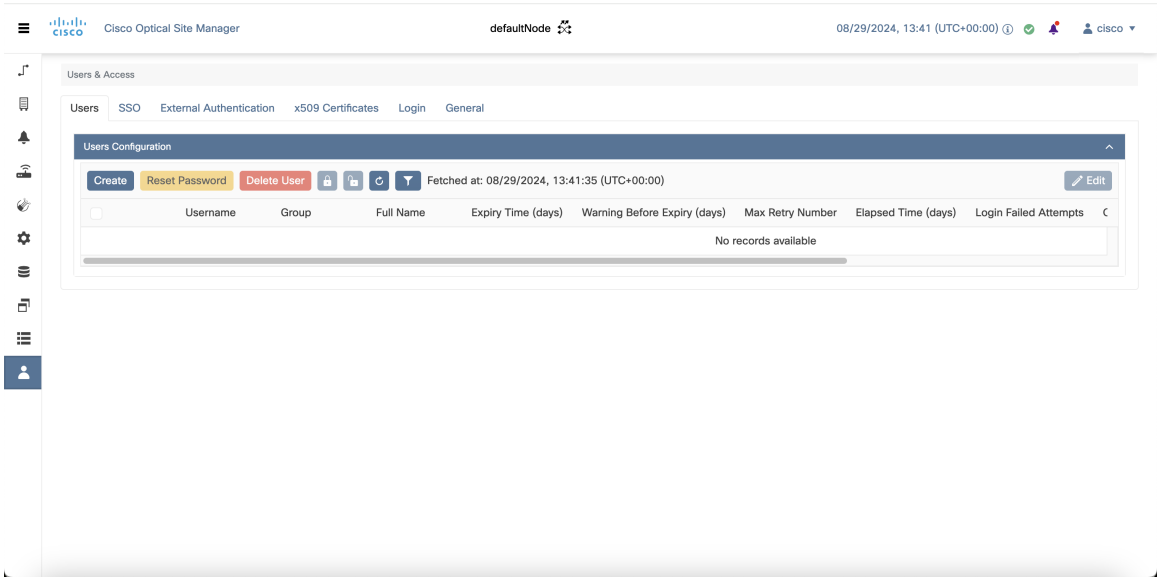


User access and authentication

This chapter describes these tasks for user access and authentication:

- Local user accounts
- Single sign-on (SSO) authentication
- External authentication
- Web certificates

Figure 1: Manage User Access and Authentication



- User configuration settings, on page 2
- Single sign-on (SSO), on page 5
- Manage External Authentication, on page 8
- x509 certificates, on page 19
- Active login user details, on page 21
- Session timeout, on page 23

User configuration settings

This section explains how to create users, manage existing users, and set user profile passwords.

-

Create users

Add new user accounts with specific roles and permissions. This enables controlled access to the Cisco Optical Site Manager for managing optical site operations, ensuring that only authorized personnel can perform configuration and monitoring tasks.

Only users with admin privileges can create new users. The process involves specifying user details such as username, password, password expiry, retry limits, and user group (for example, admin, editor, maintenance, snmp, viewer).

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to create new users.

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **Users** tab.

Step 3 In the **Users Configuration** section, click **Create**.
The **Create User** dialog box is displayed.

Step 4 Enter the details as described in the Table 1: User details, on page 2 table.

Step 5 Click **Create**.

A new user is created. The user account is added to the Cisco Optical Site Manager with the configured credentials and permissions.

Table 1: User details

Field	Description / Requirements
User Name	Type the user name. User name requirements: • Must be 6–40 characters long. • Can include alphanumeric characters (a-z, A-Z, 0-9) and special characters: @, - (hyphen), . (dot).

Field	Description / Requirements
Password	Enter the login password. Password requirements: • Must be 8–127 characters long. Must include alphanumeric (a-z, A-Z, 0-9) and special characters (+, #, %). • Must not contain the user name.
Retype Password	Re-enter the password for confirmation.
Expiry Time (days)	Enter the number of days before the user must change the password. Example: • If set to 20 days, the user must change the password before 20 days are over. • After expiry, the user is moved to the Password group and must update the password before performing any other action.
Warning Before Expiry (days)	Enter the number of days in advance to warn the user before the password expires.
Max Retry Number	Maximum number of consecutive failed login attempts. After this limit, the account is moved to the Password group.
Group	Select the group from the drop-down list. Available options: • admin • editor • maintenance • snmp • viewer

Change user password

Change a user password to maintain secure access control within Cisco Optical Site Manager. This task ensures that user credentials are updated and protected according to security policies, preventing unauthorized access.

Only an admin can change the password.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to change password for a user.

Procedure

Step 1 Click **Users & Access** in the left panel.
The **User & Access** page is displayed.

Step 2 Click the **Users** tab.

Step 3 Select the check box corresponding to the user you want to change the password in the **Users Configuration** section.

Step 4 Click **Reset Password**.

The **Reset** *Username* **Password** dialog box appears.

Step 5 Enter the new password in the **New Password** field.

The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters. The minimum number of characters in the password is eight and the maximum is 127. The password must not contain the user name.

Step 6 Retype the same password in the **Retype Password** field.

Step 7 Click **Reset Password**.

Step 8 Click **OK**.

A confirmation message or status indicates that the password has been successfully changed.

Configure user profile settings

Use this task to configure user profile settings in Cisco Optical Site Manager that allows you to manage retry limits and expiration policies.

User profile settings determine authentication behavior, password expiration, and access privileges.

You can enable or disable retry limits and expiration timers based on operational requirements.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to configure the user profile settings.

Procedure

Step 1 Click the username in the upper-right corner, then click **User Profile**.

The **User Profile** window appears.

Step 2 (Optional) Enter a value in the **Full Name** field.

Step 3 Configure retry and expiration settings.

a) Enter a value in the **Max Retry Number** field.

b) Select **Disable Max Retry Number** to remove retry restrictions.

c) Enter a value in the **Expire Time (Days)** field.
d) Select **Disable Expire Time** to prevent account expiration.
e) Enter a value in the **Warning Before Expire (Days)** field.

Step 4 Assign the user to a group.
a) Select a value from the **Group** drop-down list.

Step 5 Click **Apply**.

The updated user profile settings are saved.

The user profile settings are updated and displayed in the **User Profile** window.

For more details about the fields, see Table 1: User details, on page 2 table.

Delete users

Remove user accounts that are no longer needed. This practice maintains security and proper access control. Only authorized users will have access to the system.

Only administrators can delete users.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to delete users.

Procedure

Step 1 Click **Users & Access** in the left panel.
Step 2 Click the **Users** tab.
Step 3 Select the check-box corresponding to the user you want to delete in the **Users Configuration** section.
Step 4 Click **Delete User**.

A confirmation message appears.

Step 5 Click **OK**.

The selected user is deleted and the account is removed from Cisco Optical Site Manager.

Single sign-on (SSO)

Single Sign-On (SSO) is an authentication process. It enables a user to access multiple applications or services using a single set of login credentials, such as a username and password. This means users authenticate once. They then gain seamless access to all authorized applications without needing to log in separately to each one. The benefits of SSO include:

- Eliminates the need to remember multiple passwords.

- Reduces the frequency of login prompts during a session.

Configure and enable SSO with SAMLv2

Enable Single Sign-On (SSO) for COSM using SAMLv2. Users can authenticate once through an identity provider (IdP) and then access the system without separate logins.

Only an admin can configure SSO SAMLv2 details.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to configure and enable SSO SAMLv2 details.

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **SSO SAMLv2** section to expand it.

Step 3 Select the **Enable SAML** check box to enable the SAMLv2 protocol.

Step 4 Enter the details as mentioned in the Table 2: SSO fields, on page 6 table.

Step 5 Click **Apply**.

A trust relationship between Cisco Optical Site Manager and the IdP is established, enabling SSO functionality.

For details about each configuration field, see this table.

Table 2: SSO fields

Field	Description
IDP Entity ID	A globally unique identifier for the Identity Provider within an SSO federation. This serves as a distinct name for the IdP, allowing Service Providers to correctly identify and communicate with it.
IDP Metadata URL	The web address that points to the Identity Provider's metadata XML document. Instead of manually configuring the service provider with all the IdP's details, the service provider can simply be provided with this URL.
Proxy Address	The network IP address of a proxy server sits between users and the applications they want to access, typically in an SSO setup.
Proxy Port	Network port number on which a proxy server listens for incoming connections.

Field	Description
Group Attribute Name	Name of an attribute within a SAML assertion or other SSO token that carries information about the user's group memberships.
IDP Metadata	Details that contains all the necessary configuration information about the Identity Provider.

Create an SSO with CAS

Cisco Optical Site Manager administrators can configure SSO users with Central Authentication Service (CAS). This allows a user to access multiple applications with only one login credential.

Only administrators can add new SSO users by specifying the username and assigning a user group, either *viewer* or *editor*.

Before you begin

- Log into Cisco Optical Site Manager
- Ensure that SSO users and other users have unique usernames.

Follow these steps to add an SSO user with CAS.

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **SSO CAS** section to expand it

Step 3 Click the + button.

The **Create SSO User** dialog box appears.

Step 4 Enter the username in the **Username** field.

Step 5 Select a user group from the **Group** drop-down list.

Group	Description
editor	When mapped for SSO, can only view the Cisco Optical Site Manager configurations.
viewer	When mapped for SSO, can configure devices.

Step 6 Click **Apply**.

A confirmation message appears.

Step 7 Click **Yes**.

The SSO user is successfully created.

Enable an SSO with CAS

Cisco Optical Site Manager administrators can configure SSO users with a Central Authentication Service (CAS). This allows a user to access multiple applications with only one login credential.

Only administrators can enable SSO with CAS on Cisco Optical Site Manager.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to enable SSO with CAS:

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **SSO CAS** tab.

Step 3 Click **SETTINGS** to expand it.

Step 4 Select the **Enable CAS** check box.

Step 5 Enter the Cisco Optical Network Controller server IP address in the **IP Address** field.

Step 6 (Optional) Specify the port number in the **Port** field.

The default port number is 443.

Step 7 Click **Apply**.

A confirmation message appears.

Step 8 Click **Yes**.

SSO with CAS on Cisco Optical Site Manager is successfully enabled.

Manage External Authentication

This chapter describes the tasks related to external authentication in Cisco Optical Site Manager.

Manage External Authentication

Cisco Optical Site Manager supports RADIUS and TACACS modes of external authentication. Ensure that you enable and use either RADIUS or TACACS authentication method. You can add a maximum of up to ten servers for each of RADIUS or TACACS on Cisco Optical Site Manager.

There should be at least one RADIUS or TACACS authentication server that is configured for authentication to be enabled. In order to delete the last RADIUS or TACACS server, you must disable the external authentication first, and then delete the RADIUS or TACACS server.

When your login to Cisco Optical Site Manager with the external authentication enabled, Cisco Optical Site Manager first tries with the configured list of servers. If external authentication servers are not reachable, then

Cisco Optical Site Manager uses local authentication provided the local authentication is enabled on Cisco Optical Site Manager.

To manage Cisco Optical Site Manager, the following users are created:

- Local users (local authentication)—Specifies users who are created to manage Cisco Optical Site Manager instances.
- External users (external authentication)—Specifies users who are created on the external authentication servers.

For more information related to users, see External Authentication Users for SVO.

Note A proper privilege level must be set on the external authentication server associated to the user. See the Privilege level and user group mapping table.

If a privilege level is not set for a user in the external authentication server, the user is allowed to log in only as **Viewer**. In this case, **LOGIN-MISSING-GROUP** alarm is raised.

The following table lists some external authentication scenarios that describe some possible authentication errors, causes, and actions.

Table 3: External and Local Authentication Scenarios

External and Local Authentication Combination	Possible Authentication Scenario	Possible Cause	Action to be Taken
• External Authentication enabled and Local Authentication disabled	Server denies authentication	External username or password is incorrect	Enter the correct username and password to log in to the system.
	Server not reachable	IP address, shared secret or port number is not configured correctly although username or password could be correct	You are locked out of the system. Ensure that you have configured correct IP address, shared secret, and port number.
	User authenticated with lowest privilege (Viewer) despite the intended one	Privilege level is not set or incorrectly set on the external authentication server	Set the proper privilege level associated to the user on the external authentication server

External and Local Authentication Combination	Possible Authentication Scenario	Possible Cause	Action to be Taken
• External authentication enabled and Local authentication enabled	Server denies authentication (although local authentication is enabled)	External username or password is incorrect	Enter the correct username and password to log in to the system. Local authentication only works when the RADIUS or TACACS external servers are not reacheable.
	Server not reachable (Local authentication is enabled)	IP address, shared secret, port number is not configured correctly although username or password could be correct	Use local authentication credentials to log in to Cisco Optical Site Manager.
	User authenticated with lowest privilege (Viewer) despite the intended one	Privilege level is not set or incorrectly set on the external authentication server	Set the proper privilege level associated to the user on the external authentication server

Configure static IPv4 route

Configure a static IPv4 route on the router to the TACACS server which serves as the gateway for the Cisco Secure ISE server.

Before you begin

Log into Cisco Optical Site Manager

Procedure

Run the **router static address-family ipv4** command to configure a static IPv4 route.

Example:

```
RP/0/RP0/CPU0:R1#config
Wed Jul 12 19:12:58.900 UTC
RP/0/RP0/CPU0:R1(config)#router static address-family ipv4 unicast 10.xx.xx.0/22 10.xx.xx.1
RP/0/RP0/CPU0:R1(config)#exit
```

Configure loopback interface as source

If the Cisco Optical Site Manager management interface is configured as a loopback interface, Cisco Optical Site Manager uses it as the default source. If your network has filtering rules that restrict access to certain

servers like RADIUS or TACACS+, you can configure a specific interface IP address to be used as the source address for this traffic.

Follow these steps to configure a specific interface IP as source:

Before you begin

Log into Cisco Optical Site Manager

Procedure

Step 1 Run the **linux networking** command to enter into the linux configuration mode.

Example:

```
RP/0/RP0/CPU0:WHIT-OLT-1(config)#linux networking
```

Step 2 Run the **vrf default** command to apply the configuration to the *default* Virtual Routing and Forwarding (VRF) table.

Example:

```
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-net)#vrf default
```

Step 3 Run the **address-family ipv4** to apply the configuration for the IPv4 address family.

Example:

```
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-vrf)#address-family ipv4
```

Step 4 Run the source-hint default-route interface <interface-name> command to configure the specified interface as the source interface for that traffic.

Example:

```
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-af)#source-hint default-route interface
MgmtEth0/RP0/CPU0/0
```

Example

This example shows how to configure a specific interface as source:

```
RP/0/RP0/CPU0:WHIT-OLT-1#conf t
RP/0/RP0/CPU0:WHIT-OLT-1(config)#linux networking
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-net)#vrf default
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-vrf)#address-family ipv4
RP/0/RP0/CPU0:WHIT-OLT-1(config-lnx-af)#source-hint default-route interface
MgmtEth0/RP0/CPU0/0
```

Limitations for RADIUS or TACACS Authentication

External user list is maintained with username and its respective group (admin, editor, viewer, or maintenance). The user list is populated whenever a new username is successfully authenticated. This user list is limited to 500 users. The **Clear External Users List** button available under the **External Authentication** tab is activated when 450 users limit is reached. Whenever you click the **Clear External Users List** button, the external users are cleared. In the user list, if the user limit is reached (500 users), then the new external user (501^{th} external user) cannot login to Cisco Optical Site Manager.

If you are logged in as external user and cleared the list, ensure that you must relogin on all the logged-in sessions. If you do not relogin, the system might not respond properly and information might not appear properly.

User role mapping for TACACS+ and RADIUS authentication

User role mapping for TACACS+ and RADIUS authentication assigns specific user roles after the authentication and authorization succeeded flows. These roles determine the level of access and permissions granted to the user on the network device or management system for their session.

- User roles are assigned based on attributes returned by the authentication server.
- These roles determine the access level and permissions a user has on network devices or management systems.

Cisco Optical Site Manager interprets these privilege level values received from authorization responses and assigns the corresponding internal role:

Table 4: Privilege level and user group mapping

Privilege Level	User Group
0	viewer
1	editor
2	maintenance
3	admin
7	maintenance
15	admin

Note Viewer and maintenance users can view all paths except `/admin` and `/auth`, and can edit only their own profile information. Editor user can view and edit all paths except `/admin` and `/auth`. Admin user has full access to view and edit everything.

RADIUS Authentication

Use the following tasks to manage RADIUS authentication on Cisco Optical Site Manager.

Note Only an admin can manage RADIUS authentication on Cisco Optical Site Manager.

Create RADIUS Server Entry

Use this task to create RADIUS server entry on Cisco Optical Site Manager. Only an admin can add RADIUS server.

Before you begin

- Log into Cisco Optical Site Manager
- Ensure that you have added Cisco Optical Site Manager instances with RADIUS IP addresses in the Cisco Identity Services Engine (ISE).
- Configure or assign the privilege level settings based on RADIUS user or group in the Cisco Secure ISE server. This will allow RADIUS users to log in to and access COSM.

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **External Authentication** tab.

Step 3 In the **RADIUS Configuration** section, perform the following steps:

a) Click the + button.

The **Create RADIUS Server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the RADIUS server.
- **Host**—IPv4 address of the RADIUS server.
- **Authentication Port**—1812 is default for RADIUS. The range is from 0 to 65535. RADIUS server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the RADIUS server.
- **Confirm Secret**—Confirm the above shared secret for the RADIUS server.

c) Click **Apply**.

The RADIUS server is added to the RADIUS server list on Cisco Optical Site Manager.

Enable RADIUS Authentication

Use this task to enable RADIUS authentication. Only an admin can enable RADIUS authentication. You can add upto ten RADIUS servers on Cisco Optical Site Manager.

Before you begin

- Log into Cisco Optical Site Manager
- Create RADIUS Server Entry, on page 13

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **External Authentication** tab.

Step 3 In the **RADIUS Configuration** area, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Check the **Enable RADIUS Authentication** check box to enable RADIUS server on Cisco Optical Site Manager.

c) Check the **Enable node as final authentication when no RADIUS server is reachable** check box to enable the RADIUS server as a final authentication option.

Note It is recommended to configure the system to use local authentication if all remote RADIUS or TACACS+ servers become unreachable. Ensure that valid local user accounts with appropriate credentials are created in advance, as local authentication requires these accounts. User accounts created through remote authentication methods cannot be used for local authentication.

d) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the RADIUS server before retrying to contact the server.

e) In the **Attempts** field, enter the number of attempts to contact the first RADIUS server in the authentication list. If there is no response after the allotted number of attempts, then Cisco Optical Site Manager tries to contact the the next RADIUS server in the list.

Step 4 Click **Apply**.

Modify RADIUS Server Parameters

Use this task to modify RADIUS authentication settings. Only an admin can modify RADIUS server settings.

Before you begin

Log into Cisco Optical Site Manager and Create RADIUS Server Entry, on page 13

Procedure

Step 1 Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

Step 2 Click the **External Authentication** tab.

Step 3 In the **RADIUS Configuration** area, select the RADIUS server to edit from the list of available RADIUS servers and perform the following tasks:

a) Click the **Edit** button.

b) Edit the following fields:

- **Host**
- **Authentication Port**
- **Shared Secret**

c) Click **Apply**.

Disable the RADIUS Authentication

Use this task to disable RADIUS authentication.

Before you begin

Log into Cisco Optical Site Manager

Procedure

Step 1 Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

Step 2 Click the **External Authentication** tab.

Step 3 In the RADIUS Configuration area, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Uncheck the **Enable RADIUS Authentication** check box to disable RADIUS authentication on Cisco Optical Site Manager.

c) Uncheck the **Enable node as final authentication when no RADIUS server is reachable** check box to disable the RADIUS server as a final authentication option.

Note When external authentication is disabled, then local authentication is disabled by default.

Step 4 Click **Apply**.

Delete the RADIUS Server from Cisco Optical Site Manager

Use this task to delete the RADIUS server entry from Cisco Optical Site Manager.

Before you begin

Log into Cisco Optical Site Manager

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **External Authentication** tab.

Step 3 In the **RADIUS Configuration** area, select the RADIUS server to delete and click the **-** button.

TACACS+ Authentication

Use the following tasks to manage TACACS+ authentication.

Note Only users with admin privileges can manage TACACS+ authentication on Cisco Optical Site Manager.

Create TACACS+ Server Entry on Cisco Optical Site Manager

Use this task to create TACACS+ server entry on Cisco Optical Site Manager. Only an admin can add TACACS+ server. You can add upto ten TACACS+ servers.

Before you begin

- Log into Cisco Optical Site Manager
- Ensure that you have added Cisco Optical Site Manager instances with TACACS+ IP addresses in the Cisco Identity Services Engine (ISE).
- Configure or assign the privilege level settings based on TACACS+ user or group in the Cisco Secure ISE server. This will allow TACACS+ users to log in to and access COSM.

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **External Authentication** tab.

Step 3 In the **TACACS+ Configuration** section, perform the following steps:

a) Click the **+** button.

The **Create TACACS+ server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the TACACS+ server.
- **Host**—IP address of the TACACS+ server.

- **Authentication Port**—49 is default for TACACS+. TACACS+ server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the TACACS+ server.
- **Confirm Secret**—Confirm the above shared secret for the TACACS+ server.

c) Click **Apply**.

The TACACS+ server is added to the TACACS+ server list on Cisco Optical Site Manager.

Enable TACACS+ Authentication

Use this task to enable TACACS+ authentication.

Before you begin

- Log into Cisco Optical Site Manager
- Create TACACS+ Server Entry on Cisco Optical Site Manager, on page 16

Procedure

Step 1 Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

Step 2 Click the **External Authentication** tab.

Step 3 In the **TACACS+ Configuration** section, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Check the **Enable TACACS+ Authentication** check box to enable TACACS+ server on Cisco Optical Site Manager.

c) Check the **Enable node as final authentication when no TACACS+ server is reachable** check box to enable the TACACS+ server as a final authentication option.



Note It is recommended to configure the system to use local authentication if all remote RADIUS or TACACS+ servers become unreachable. Ensure that valid local user accounts with appropriate credentials are created in advance, as local authentication requires these accounts. User accounts created through remote authentication methods cannot be used for local authentication.

d) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the TACACS+ server before retrying to contact the server.

e) In the **Attempts** field, enter the number of attempts to contact the first TACACS+ server in the authentication list. If there is no response after the allotted number of attempts, then Cisco Optical Site Manager tries to contact the the next RADIUS server in the list.

Step 4 Click **Apply**.

Modify TACACS+ Server Parameters

Use this task to modify TACACS+ authentication settings. Only an admin can modify TACACS+ server settings.

Before you begin

Log into Cisco Optical Site Manager and Create TACACS+ Server Entry on Cisco Optical Site Manager, on page 16

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **External Authentication** tab.

Step 3 In the **TACACS+ Configuration** area, select the TACACS+ server to edit from the list of available TACACS+ servers and perform the following tasks:

a) Click the **Edit** button.

b) Edit the following fields:

- **Host**
- **Authentication Port**
- **Shared Secret**

c) Click **Apply**.

Disable the TACACS+ Authentication

Use this task to disable TACACS+ authentication.

Before you begin

Log into Cisco Optical Site Manager

Procedure

Step 1 Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

Step 2 Click the **External Authentication** tab.

Step 3 In the **TACACS+ Configuration** area, perform the following steps:

a) Click **SETTINGS** to expand it.

b) Uncheck the **Enable TACACS+ Authentication** check box to disable TACACS+ authentication on Cisco Optical Site Manager.
c) Uncheck the **Enable node as final authentication when no TACACS+ server is reachable** check box to disable the TACACS+ server as a final authentication option.



Note When external authentication is disabled, then local authentication is disabled by default.

Step 4 Click **Apply**.

Delete the TACACS+ Server from Cisco Optical Site Manager

Use this task to delete the TACACS+ server entry from Cisco Optical Site Manager.

Before you begin

Disable the TACACS+ Authentication, on page 18

Procedure

Step 1 Click **Users & Access** in the left panel.
Step 2 Click the **External Authentication** tab.
Step 3 In the **TACACS+ Configuration** area, select the TACACS+ server to delete and click the - .

x509 certificates

x509 certificates are used to establish a secure communication channel between a client and a server. In Cisco Optical Site Manager, you can automatically generate a self-signed x509 certificate or upload a CA-authorized certificate in digital or PFX format. This certificate:

- builds trust between the client and server,
- protects sensitive information from unauthorized parties
- and provides the ability to detect any tampering or modification of data during transmission.

Table 5: Feature History

Feature Name	Release Information	Description
Improved x509 Certificate Handling	Cisco IOS XR Release 24.1.1	You can now upload an x509 certificate in the Personal Information Exchange (PFX) format, which improves the security of the connection between the Cisco Optical Site Manager and its server. PFX files can be password-protected, offering an extra layer of protection against potential attackers. The options to automatically generate and upload certificates are available in the new **x509 Certificates** tab under the **Users & Access** menu.

Generate and upload x509 certificates

Establish secure communication channels between clients and servers to ensure encrypted and trusted communications. This ensures data confidentiality, integrity, and authentication. It protects sensitive information from unauthorized access and tampering during transmission.

Use this task to upload certificates in digital (.cert) or PFX (.pfx) file formats. You can generate certificates internally as self-signed, or upload them in several formats such as:

- Certificate and key (CERT + KEY)
- Personal Information Exchange (PFX) and password (PFX + PASSWORD)
- PEM

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to automatically generate and apply a x509 certificate.

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **x509 Certificates** tab.

Step 3 Click the **Certificates Configuration** section to expand it.

Step 4 Perform any one of the following steps to auto-generate or upload certificate files:

To auto generate and apply	To upload a digital certificate	To upload a PFX certificate
Click **Auto Generate and Apply Certificate** to automatically generate and apply a self signed certificate.	**a.** Select *CERT + KEY* from the **Certificate Type** drop-down list. **b.** Select the *.cert* or *.crt* file from the **Certificate File** field and click **Upload**. **c.** Select the *.key* file in the **Key File** field and click **Upload**.	**a.** Select *PFX + PASSWORD* from the **Certificate Type** drop-down list. **b.** Select the *.pfx* file from the **Certificate File** field and click **Upload**. **c.** Type the password in the **Password** field if the input private key file is password protected.

Step 5 Click **Apply**.

The uploaded ceritifcate is validated, which enables secure, encrypted communication.

Active login user details

Cisco Optical Site Manager displays details of users who are currently logged in and displays their session information. Monitoring user activity and managing sessions are made more effective with this information. These user session details are displayed:

- username
- login time
- interface name
- IP address

View active login sessions

Administrators can use Cisco Optical Site Manager to view active login sessions, monitor current user activity, and enhance security management.

You can view the users currently logged in and their details, such as username, login time, interface name, and IP address.

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to view the list of currently logged in users:

Procedure

Step 1 Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

Step 2 Click the **Login** tab.

Step 3 Click **Active Login Sessions** to view the currently logged in users and their details.

The system displays the username, login time, interface name, and IP address for each user currently logged in.

View the user login history

Administrators can access the past login activities of a user. This access facilitates auditing user activities, enables tracking of security events, and helps identify unauthorized or suspicious login attempts.

You can view user login history and details such as:

- Login ID
- username
- Last login and logout date
- Interface name
- IP address

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to view the user login history:

Procedure

Step 1 Click **Users & Access** in the left panel.

The **Users & Access** page is displayed.

Step 2 Click the **Login** tab.

Step 3 Click **Last Successful Logins** to view user login history and associated details.

The system displays the user login history for each user.

Session timeout

This section describes the tasks to configure session timeouts for these session types:

- WebUI sessions
- Netconf protocol

Configure Netconf and webUI session timeout

Configure the timeout settings for user sessions in Cisco Optical Site Manager to ensure that inactive sessions are automatically signed out after a specified period. This enhances security and resource management.

You can configure timeout values to control how long a user session can remain inactive or active before being terminated.

You can configure timeout values for two types of sessions:

- Netconf: Configure timeout for the NETCONF (Network Configuration Protocol) protocol. This includes an idle timeout (in minutes).
- WebUI: Configure timeout for a user's session in a web-based user (WebUI) interface. This includes both an idle timeout (in minutes) and an absolute timeout (in hours).

Before you begin

Log into Cisco Optical Site Manager

Follow these steps to configure timeout for WebUI and Netconf sessions:

Procedure

Step 1 Click **Users & Access** in the left panel.

Step 2 Click the **Sessions Control** tab.

Step 3 Select the time and hours from the respective drop-down lists as described in this table:

Drop-down	Description
Webui Idle Timeout	Defines the maximum period of inactivity allowed for a user's session in a WebUI before that session is automatically terminated. Valid values: 1 to 30 minutes in increments of 1 minute
Webui Absolute Timeout	Defines the maximum total duration a user's session in a WebUI user interface can remain active, irrespective of user activity. Valid values: 1 to 16 hours in increments of 1 hour

Drop-down	Description
Netconf Timeout	Defines a configurable time limit for operations performed over the NETCONF protocol. Valid values: 1 to 30 minutes in increments of 1 minute

Step 4 Click **Apply**.

The settings are saved and users are automatically signed out of their Nodal Craft or Netconf sessions based on the configured idle or absolute timeout values.