

Manage Users and Roles

- User roles in Cisco ONP, on page 1
- Assign a role to a user group, on page 2
- Remove access to a user, on page 3
- Delete a user, on page 3
- Create a new user group, on page 4
- Assign a user to a user group, on page 5
- Set password expiration for individual user, on page 5
- Set password expiration for all users, on page 6
- Lock and unlock an individual user account, on page 6
- Expire the password set by an individual user, on page 7
- Create a new role, on page 7
- Assign a role to a user group, on page 8
- Manage password through Dictionary, on page 8
- Retrieve system logs , on page 9

User roles in Cisco ONP

Cisco ONP provides a structured approach to access control management through various user roles. Here's an overview of the default roles and their capabilities:

Administrator

As an administrator, you have these roles and responsibilities:

- **User activation**: Admin or users with admin access grant access by activating new users, who are then notified by email.
- **Group management**: Some user groups are predefined. These groups cannot be edited or deleted.
- **Role assignment**: Admins assign roles to groups, defining the actions a group can perform.

Designer

As a designer, you have these roles and responsibilities:

- **Network design**: Designers can create network topologies using either manual design or import design methods.
- **Capabilities**: They can design networks with various topologies (linear, ring, mesh) and assign fibers between sites, including Traffic, OLA, ROADM, and Passthrough sites.
- **Limitations**: Designers cannot analyze networks but can view reports shared by others after analysis.

Planner

As a planner, you have these roles and responsibilities:

- **Design and analysis**: Planners can both design and analyze networks. They evaluate network performance after creating sites, fiber spans, and service demands.

Reader

As a reader, you have these roles and responsibilities:

- **View-only access**: Readers can view users, user groups, roles, permissions, network topology, layout, connections, and the Bill of Materials (BOM).

  By default, users are assigned to the READ_ONLY_GROUP with the role called READER_ROLE.

To create a new role, see #unique_23.

Under **Control Panel** > **Roles** and **Control Panel** > **Permissions**, you can view the permissions applicable for each role and the actions that can be performed for each permission.

Assign a role to a user group

All users with the admin role receive an email notification about new user registration.

Follow these steps to assign a role to a user group:

Before you begin

Log in to the Cisco ONP web interface as a user with Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 You can change the state of a user from INACTIVE to ACTIVE in either of two ways.

- From the **State** field, click **INACTIVE** in the respective user row.
- Select a user row or multiple user rows and click **Update**.
  - In the **Update User** dialog box, select the **Group** and **State** from the respective drop-down lists.
  - Click **Save**.

Step 3 Click **OK** in the **Success** dialog box.

Note

- After your access is granted by the admin, you receive an email notification at your registered email address. ou can log in after you get this email.
- The admin assigns a Role and Group to a newly created user. These assignments determine what actions the user can perform.

Remove access to a user

This section helps you to securely revoke a user's access for security, compliance, or resource management reasons.

Follow these steps to remove Cisco ONP access to a user.

Before you begin

Log in to the Cisco ONP web interface as a user with Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Change the state of a user from ACTIVE to INACTIVE in either of two ways:

- In the **State** field, click **ACTIVE** in the user's row.
- Select a user row or multiple user rows, and click **Update**.
  - In the **Update User** dialog box, select the **Group** and **State** from the drop-down lists.
  - Click **Save**.

Step 3 In the **Success** dialog box, click **OK**.

Delete a user

Follow these steps to delete a user or multiple users.

Before you begin

Log in to the Cisco ONP web interface as a user with admin role.

Procedure

Step 1 Click **Control panel**.

The **Access Control Management** page appears.

Step 2 Delete a user:

a) Select the user or multiple users to be deleted under the **USERS** tab, and click **Delete**.

b) Click **Yes** in the **Warning** dialog box.

The message **User deleted successfully** appears.

Create a new user group

Follow these steps to create a new user group.

Before you begin

Log in to the Cisco ONP web interface as a user with Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USER GROUPS** tab.

Step 3 Click **Create**.

a) In the **Create Group** dialog box, enter the **Group Name**.

b) Choose the appropriate role from the **Role** drop-down list. The available default roles are:

- ADMIN
- PLANNER
- DESIGNER
- READER

The **Role** drop-down list may also have user-defined roles listed under it.

c) Click **Save** to create the user group.

Step 4 In the **Success**dialog box, click **OK**.

Assign a user to a user group

This task guides an administrator to assign a user to a specific user group within the system. Organizing users into groups with defined roles and permissions streamlines access management and enhances security controls.

Follow these steps to assign a user to a user group.

Before you begin

Log in to the Cisco ONP web interface with Admin permission.

Procedure

Step 1 Click **Control panel**.

The **Access Control Management** page appears.

Step 2 Under the **USERS** tab, select the user or users who are to be assigned to the new group, and click **Update**.

In the **Update User** dialog box:

a) From the **Group** drop-down list, select the appropriate group.
b) From the **State** drop-down list, select **Active** to activate the user in the group, or **Inactive** to deactivate the user in the group.
c) Click **Save**.

Step 3 In the **Success** dialog box, click **OK**.

Note

a. A user can belong to only one group.

b. Only one role can be assigned to any group.

c. All users in a group have the group's role.

d. By default, a new user is assigned to the Read_Only_Group.

Set password expiration for individual user

This section explains how to set password expiration to help maintain user account security.

Follow these steps to set the expiration of the password set by the user.

Before you begin

Log in to the Cisco ONP web interface with Admin or Configuration_Management permission.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Select the user under the **USERS** tab., and click **Update**.

In the **Update User** dialog box:

a) Click the **PASSWORD EXPIRY** tab.
b) Enter values for the **Lifetime**, **Warning** and **Grace** fields.
c) Click **Save**.

Note
The password expiry settings like lifetime, warning and grace time, take effect after the existing password is changed by the user.

Step 3 In the **Success** dialog box, click **OK**.

Set password expiration for all users

This section explains how to set password expiration to help maintain user account security.

Follow these steps to set the password expiration for all users.

Before you begin

Log in to the Cisco ONP web interface with Admin or Configuration_Management permission.

Procedure

Step 1 Click **Control Panel**.
The **Access Control Management** page appears.

Step 2 Click the **System Configuration** tab.

a) Enter values for the **Lifetime**, **Warning**, and **Grace** fields.
b) Click **Update**.

Note
The password expiry settings such as lifetime, warning, and grace time, take effect after the user changes their existing password.

Lock and unlock an individual user account

This procedure enables administrators to ensure that only authorized users can access the system.

Before you begin

Log in to the Cisco ONP web interface as a user with the admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USERS** tab.

a) Select the user whose account you want to lock or unlock.
b) Click **Lock** to lock the user account, or click **Unlock** to unlock the account.

If your account is locked, contact your administrator to unlock your account.

Expire the password set by an individual user

This task allows an administrator to manually expire the password of a specific user to enhance security by ensuring compromised or outdated credentials are not used.

Follow these steps to expire the password set by an individual user.

Before you begin

Log in to the Cisco ONP web interface with Admin permission.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USERS** tab.

a) Select the user whose password you want to expire.
b) Click **Expire**.

Create a new role

This procedure guides an administrator in defining a new role, assigning appropriate permissions, and making the role available for users.

Before you begin

Log in to the Cisco ONP web interface as a user with the admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **ROLES** tab. Then click **Create**.

a) In the **Create Role** dialog box, enter the **Role Name**, select the **Permissions** for the role, and click **Save**.

Note
You can select more than one permission.

b) In the **Success** dialog box, click **OK**.

Assign a role to a user group

This procedure helps the administrator to assign or update a role for a user group in Cisco ONP, ensuring the group has appropriate access permissions within the system.

Follow these steps to assign a role to a user group.

Before you begin

Log in to the Cisco ONP web interface as a user with the Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USER GROUPS** tab.

a) Select the user group you want to update, and click **Update**.
b) In the **Update Group** dialog box, select the desired role from the **Role** drop-down list, and click **Save**.
c) In the **Success** dialog box, click **OK**.

Manage password through Dictionary

The dictionary rejects any new password that exists in the predefined list of passwords under the **Content** column in the **DICTIONARY** tab.

The system performs this password verification check against the dictionary during these events:

- New user sign-up

- Password change
- Password reset using forgot password option

Use this task to verify whether the new password set by the user exists in the list of predefined passwords:

Before you begin

Log in to the Cisco ONP web interface as a user with the admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **DICTIONARY** tab.

a) Enable the **Rejection Mode** toggle button to verify the password against the dictionary.

By default, this toggle button remains disabled.

b) Enter the password in the **Enter Passphrase** text box.
c) To specify the maximum number of matching passphrases, enter the limit in the **Enter Limit** text box.
d) Click **Search**.

The system displays the matching passphrases.

Note
If you enter a limit, the system displays only that number of matching search results. If you do not enter a limit, the system displays all matching passphrases.

Retrieve system logs

This task guides administrators or authorized users through the steps to retrieve, filter, and manage system logs for a specified time interval on the **System Logs** page. For more information, see Logs.

Follow these steps to retrieve the system logs.

Before you begin

Log in to the Cisco ONP web interface as an admin, or a user with User Management and Network Management permissions.

Procedure

Step 1 Click **Logs**.

a) Click **Select Start Date**, and choose the start date. Similarly, click **Select End Date**, and choose the end date.
b) Choose the **Logs Category**.
c) Click **FILTER** to retrieve the logs.

Step 2 Perform the required actions in the **Logs** page.

If you want to.....	then...
export the system logs to an Excel sheet	click the **Export as CSV** icon.
export the system logs as a zip file	click the **Export Archive** icon.
import the zip file	click the **Import Archive** icon.
refresh the system logs page	click the **Refresh** icon.
delete the existing logs	click the **Clear Logs** icon.