Manage Users and Roles

User Roles in Cisco ONP

Initially, the administrator performs access control management tasks, like activating users after user sign-up, creating user groups, roles, and assigning roles and users to user groups. The admin or user with admin access grants access to the newly created user by activating the user. After the admin grants access, the new user will be notified by email (sent to the email address registered while signing up). It is only then that the new user is able to log in. By default, the following user roles are available in Cisco ONP.

1. **Admin**: The Admin user can create new user groups and assign user to user groups. Users are categorized into groups. There are certain predefined user groups in Cisco ONP. You cannot edit or delete these user groups. Admin can assign a group with a particular role. The role describes the actions that a particular user group can perform.

2. **Designer**: The Designer user can design a network. There are two ways to design a network.

   - Manual Design
   - Import Design

   The designer user can create a network topology of any type (linear, ring, mesh) with Traffic, OLA, ROADM, and Passthrough sites, and assign the fibers with suitable spans between those sites. The designer

can only design the network and cannot analyze the network. The designer can view the reports, when any user shares the analyzed network.

3. **Planner**: The Planner user can design and analyze a network. After the Sites, Fiber spans, and Service demands are created, analyze the network to determine the network performance. Cisco ONP automatically optimizes the design and summarizes the optical transmission performance. In the analyzed state, all reports are available and updated. In the analyzed state, no aspect of the network design can be changed.
4. **Reader**: The Reader user can view users, user groups, roles, and permission. The Reader can also view the network topology, layout, connections, and BOM. By default, a user is assigned in the READ_ONLY_GROUP with a READER_ROLE.

You can also create new roles. See Create a New Role, on page 6.

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.

Grant Access to a New User

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

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

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 by using either of two ways:

a. From the **State** field, click **INACTIVE** in the respective user row.

b. 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 the Admin grants access, the new user gets notified by email (sent to the email address registered while signing up). It is only then that the new user will be able to log in.
- The admin assigns a newly created user with a Role and Group that determines what actions the user can perform.

Remove Access to a User

Use this task to remove Cisco ONP access to a user.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control panel**.

The **Access Control Management** page appears.

Step 2 You can change the state of a user from ACTIVE to INACTIVE by using either of two ways:

a. From the **State** field, click **ACTIVE** in the respective user row.

b. 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.

Delete a User

Use this task to delete a user or multiple users.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control panel**.

The **Access Control Management** page appears.

Step 2 Select the user or multiple users to be deleted under the **USERS** tab and click **Delete**.

Step 3 Click **Yes** in the **Warning** dialog box.

The message *User deleted successfully* appears.

Create a New User Group

Use this task to create a new user group.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

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

Step 3 Click **Create**.

Step 4 In the **Create Group** dialog box, enter the **Group Name**.

Step 5 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 that are listed under it.

Step 6 Click **Save** to save the created user group.

Step 7 Click **OK** in the **Success** dialog box.

Assign a User to a User Group

Use this task to assign a user to a user group.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

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.

Step 3 Click **Update**.

Step 4 In the **Update User** dialog box, perform the following:

- Select the appropriate group from the **Group** drop-down list.
- Select **Active** or **Inactive** from the **State** drop-down list, to activate or inactivate the user in the group, respectively.
- Click **Save**.

Step 5 Click **OK** in the **Success** dialog box.

Note

a. A user can belong to only one group.

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

c. All the users of a group have the same role as that of the group.

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

Set Password Expiration for Individual User

Use this task to set the expiration of the password set by the user.

Before you begin

Log in to Cisco ONP Web Interface with Admin or Configuration_Management permission.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Select the user under the **USERS** tab.

Step 3 Click **Update**.

Step 4 In the **Update User** dialog box, click the **PASSWORD EXPIRY** tab.

Step 5 Enter values for the **Lifetime**, **Warning** and **Grace** fields.

Step 6 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 7 Click **OK** in the **Success** dialog box.

Set Password Expiration for All Users

Use this task to set the expiration of the password for all users.

Before you begin

Log in to Cisco ONP Web Interface with Admin or Configuration_Management permission.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

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

Step 3 Enter values for the **Lifetime**, **Warning** and **Grace** fields.

Step 4 Click **Update**.

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

Lock and Unlock an Individual User Account

Use this task to lock or unlock an individual user account.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USERS** tab.

Step 3 Select the user whose account you want to lock or unlock.

Step 4 Click **Lock** to lock the user account, or click **Unlock** to unlock the locked user account.

Note The user of a locked account must contact the admin to unlock the user account.

Expire the Password Set by an Individual User

Use the following task to expire the password set by an individual user.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USERS** tab.

Step 3 Select the user whose password you want to expire.

Step 4 Click **Expire**.

Create a New Role

Use the following task to create a new role.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **ROLES** tab.

Step 3 Click **Create**.

Step 4 In the **Create Role** dialog box, enter the **Role Name** and select the **Permissions** for the role.

Note You can select more than one permission.

Step 5 Click **Save**.

Step 6 Click **OK** in the **Success** dialog box.

Assign a Role to a User Group

Use the following task to assign a new role to a user group.

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

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

Step 3 Select the user group whose role is to be updated.

Step 4 Click **Update**.

Step 5 In the **Update Group** dialog box, select the desired role from the **Role** drop-down list, and click **Save**.

Step 6 Click **OK** in the **Success** dialog box.

Manage Password Through Dictionary

If a password exists in the predefined list of passwords under the **Content** column, the dictionary rejects the new password set by the user. You must have Admin or Configuration_Management permission to view and modify the dictionary.

By default, the **Rejection Mode** toggle button is disabled. Enable the **Rejection Mode** toggle button to verify the password against dictionary. This password verification check against the dictionary happens during any one of the following events:

- New user sign-up

- Password change
- Password reset using forgot password option

The following is the procedure to verify, whether the new password set by the user exists in the list of predefined passwords:

Before you begin

Log in to Cisco ONP Web Interface as a user with Admin role.

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **DICTIONARY** tab.

Step 3 Enter the password in the **Enter Passphrase** text box.

Step 4 (Optional) Enter the limit (maximum number of matching passphrases) in the **Enter Limit** text box.

Step 5 Click **Search**.

The matching passphrases get displayed.

Note If you have entered the limit, a number of search results matching the limit gets displayed. Otherwise, all matching passphrases get displayed.

Retrieve System Logs

The System Logs page shows at logs the events that are initiated during a specific time interval. See Logs.

Before you begin

Log in to Cisco ONP Web Interface as an admin or a user with User Management and Network Management permission.

Step 1 Click **Logs**.

Step 2 Click **Select Start Date**, and choose the start date. Similarly, click **Select End Date**, and choose the end date.

Step 3 Click **FILTER** to retrieve the logs.

The following icons are available in the **System Logs** page:

Icons	Description
Export as CSV	Exports the system logs to an Excel sheet
Export Archive	Exports the system logs as a zip file
Import Archive	Imports the zip file
Refresh	Refreshes the system logs page

Icons	Description
Clear Logs	Deletes the existing logs