Manage Users and Roles

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

The roles and responsibilities of the administrator are:

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

Designer

The roles and responsibilities of the designer are:

- **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

The roles and responsibilities of the planner are:

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

Reader

The roles and responsibilities of the reader are:

- **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 a READER_ROLE.

You can also create new roles. See Create a new role, on page 7.

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.

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 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.

Procedure

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.

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

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.

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 save the created user group.

Step 4 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.

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** or **Inactive** to activate or inactivate the user in the group, respectively.
c) Click **Save**.

Step 3 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.

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 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.

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 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.

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 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 this 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.

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

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.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **ROLES** tab, and click **Create**.

a) In the **Create Role** dialog box, enter the **Role Name** and 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

Use this 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.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

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

a) Select the user group whose role is to be updated, 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

If a password exists in the predefined list of passwords under the **Content** column in the **DICTIONARY** tab, the dictionary rejects the new password set by the user.

This password verification check against the dictionary happens during any one of 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 Cisco ONP web interface as a user with Admin or Configuration_Management permission.

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 dictionary.

By default, the **Rejection Mode** toggle button remains disabled.

b) Enter the password in the **Enter Passphrase** text box.

c) If you want to enter the limit (maximum number of matching passphrases), enter the same in the **Enter Limit** text box.

d) 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.

Procedure

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.

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.

Retrieve component logs

Use this task to retrieve the critical logs for each event from the **Component Logs** page. 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.

Procedure

Step 1 Go to **Logs**>**Component Logs**.

Step 2 From the **Component** drop-down list, choose a component.

The logs for the chosen component appear. The available components are:

- BE
- GENE
- ODE
- PCE

Step 3 In the **Search** field, enter the event to locate the event logs.

The action icons available in the **Component Logs** page are:

If you want to.....	then.....
export the component logs as a text file	click the **Export** icon.

If you want to…...	then…...
see the file path of the chosen component	hover the **Information** icon.