Managing Users

Table 1: Feature History

Feature Name	Release Information	Description
Support for Open Lightweight Directory Access Protocol (LDAP) and Multiple LDAP Servers	Cisco Operations Hub 22.2	Cisco Operations Hub supports LDAP compatible directory servers, including Open LDAP and Microsoft Active Directory (AD). As an administrator, you can enable LDAP authentication and provide access to other users. You can add multiple LDAP servers for LDAP authentication.
Support for LDAP Connectivity Checks	Cisco Operations Hub 22.3	After adding the LDAP configuration, you can perform a connectivity check and verify end-to-end LDAP connectivity.

Cisco Operations Hub provides user management functionality where you can create local users and configure LDAP users for external authentication.

For information on user types and how to configure local and LDAP users, see:

- User Roles, on page 1
- Configuring Local Users, on page 2
- Configuring LDAP Users, on page 5

User Roles

Cisco Operations Hub supports three user roles based on the HTTP actions:

Table 2: User Roles

API User Roles	Allowed HTTP Method
api-admin	GET, POST, PUT, DELETE

API User Roles	Allowed HTTP Method
api-editor	GET, POST, PUT
api-viewer	GET

By default, the **admin** user is already mapped under these three groups.

Configuring Local Users

Note Only Administrators can manage users and provide access.

Related Topics

Adding Local Users, on page 2
Editing Local Users, on page 3
Removing Local Users, on page 3
Exporting User Details, on page 3
Using Filter Options, on page 4
Viewing Session History, on page 4
Changing Passwords, on page 4

Adding Local Users

This procedure adds a new user and assign role to the user.

Step 1 At the main menu, select **System** > **Users & Roles**.

The **Users & Roles** page appears.

Step 2 Click **Add User** to open the **Add User** window at the right side of the page.

Step 3 Enter the username in the **Username** field. The username can be a name or email ID.

Step 4 Choose the user role in the **Select Role** drop-down list. The options are Admin, Editor, and Viewer.

Step 5 Enter a password and confirm the password for the new user.

The password must contain at least eight characters. Ensure that you meet the password requirements that are listed in the **PASSWORD REQUIREMENTS** area.

The **Force password change on next login** option is selected by default.

Step 6 Click **Add User**.

A success confirmation message appears that a new user is added.

Note Once the new user is created, the new user must change the password during the first login.

Editing Local Users

This procedure edits the user role and password expiration period to the existing local user.

Step 1 At the main menu, select **System** > **Users & Roles**.

The **Users & Roles** page appears.

Step 2 Click the radio button against the user you wish to edit.

Step 3 Click **Edit User** to open the **Edit User** window at the right side of the page.

Step 4 Choose the user role in the **Role** drop-down list.

Step 5 By default, the password expiration period is 0. Move the slide bar in the **Password Expiration Period (days)** field or you can enter the value in the **Enter Value** field.

Step 6 Click **Save**.

A success message appears that the user details are updated.

Removing Local Users

This procedure removes the user from the existing local user list.

Step 1 At the main menu, select **System** > **Users & Roles**.

The **Users & Roles** page appears.

Step 2 Click the radio button against the user that you want to delete.

Step 3 Click **Remove User**.

A pop-up message appears that the user will no longer have access to the Operations Hub.

Step 4 Click **Remove**.

A Success message appears that the user is removed.

Exporting User Details

This procedure exports the user details into an Excel sheet.

Step 1 At the main menu, select **System** > **Users & Roles**.

The **Users & Roles** page appears.

Step 2 Click **Export** at the top-right of the home page.

The Excel sheet with user details is downloaded in the CSV format.

Using Filter Options

This procedure uses filter options that are based on user roles and password status.

Step 1 At the main menu, select **System** > **Users & Roles**.

The **Users & Roles** page appears.

Step 2 Click **Admin**, **Editor**, or **Viewer** button against **Role** area to filter users based on roles.

Step 3 Choose Password Expired or Password Valid in the **Focus** drop-down list to filter users based on password status.

Viewing Session History

This procedure views a session history of a specific user.

Step 1 At the main menu, select **System** > **Users & Roles**.

The **Users & Roles** page appears.

Step 2 Click a username in the **Users & Roles** page..

A **User Details** window appears at the right side of the page.

Step 3 Click the **Sessions History** tab to view user access history as Events with Date table. By default, the **All** is selected and you can view the whole session history of the user.

Click **Login** and **Logout** next to the **Event** area to view a login and logout event history details of a specific user.

Step 4 Click **Export** to download the user session details in the CSV format.

Changing Passwords

You can change the password from the **My Account** page or using the Alert banner.

Use the following procedure to changes the password from the **My Account** page:

Step 1 Click the main menu at the top-left of the home page, and click **My Account** at the left-end of the main menu page.

Step 2 In the **My Account** page, click **Update Password** to open **Update Password** window.

Step 3 Enter current password, new password, and confirm the password.

The password must adhere to the password requirements.

Step 4 Click **Update**.

A Success message appears that the user password is updated.

Changing Passwords In Alert Banner

Use the following procedure to change the password in the Alert banner:

Step 1 Click the link in the alert banner.

Step 2 If your password has expired, you must reset the password during login.

Alert banner appears 30 days before password expiry.

Configuring LDAP Users

In Operations Hub, local authentication is enabled by default. Administrators can switch the authentication method from local to LDAP.

Note:

- Cisco Operations Hub supports LDAP compatible directory servers, including OpenLDAP and Microsoft Active Directory (AD).
- When using multiple LDAP servers (for example, primary and secondary), ensure that these servers must have similar parameters.
- Multiple LDAP servers can be configured for high availability scenarios.

This procedure configures the LDAP user.

Step 1 At the main menu, select **Systems** > **Security** > **Authentication**.

The **Authentication** page appears.

Step 2 Click **Edit** and choose **LDAP** radio button.

Step 3 In the **LDAP Configuration** area, enter the following fields:

LDAP Parameters	Description
Primary LDAP Server URL	Specifies URL of the primary LDAP server.
Secondary LDAP Server URL	Specifies URL of the Secondary LDAP server.
Base Domain Name	Specifies domain name as configured on your LDAP server.
LDAP User Name Domain	Specifies to validate the username against the domain controller.
LDAP Filter	Specifies a subset of data items in an LDAP data type.
LDAP Group Attribute	Specifies a list of comma-separated LDAP attributes on a group object that can be used in a user-member attribute.

LDAP Parameters	Description
LDAP Group Mapping	Enables you to map LDAP group to Operations Hub role.

Step 4 Click **Validate LDAP Configuration** to perform a connectivity check and verify the LDAP connectivity end to end. See LDAP Connectivity Checks.

Step 5 Click **Save**.

LDAP Connectivity Checks

When adding an LDAP configuration, you can perform a connectivity check and verify end to end LDAP connectivity. You must provide valid LDAP user credentials to perform this connectivity check. If you trigger **Validate LDAP Configuration** and if there is LDAP connectivity failure, then an error message with the reason for the failure is displayed.