Securing Operations Hub

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 2
Configuring Local Users, on page 2
Configuring LDAP Users, on page 6

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-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 4
Using Filter Options, on page 4
Viewing Session History, on page 4
Changing Passwords, on page 5

Adding Local Users

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

Procedure

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. Creating a password with dictionary words or common sequences such as *123* is not recommended.

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.

Procedure

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.

Procedure

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.

Procedure

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.

Procedure

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.

Procedure

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:

Procedure

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:

Procedure

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.

Procedure

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.
Bind Distinguished Name	Allows you to capture the user and the location of the user in the LDAP directory tree
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 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.

Configuring TLS Certificate

Table 3: Feature History

Feature Name	Release Information	Description
Support for Configuring TLS Certificate	Cisco Operations Hub, Release 23.1	Cisco Operations Hub supports the replacement of the cluster's current TLS (CA signed or self-signed) certificate using Operations Hub WebUI.
Certificate Signing Requests	Cisco Operations Hub, Release 23.2	You can initiate the Certificate Signing Request (CSR) from within Operations Hub.

You can initiate the TLS Certificate creation process from Operations Hub. Once a certificate request is completed, you can download it and get it signed by an appropriate signing authority. Once signed, you can upload the certificate and override the default self-signed Ingress Certificate.

You can also override the Signed Ingress certificate.

Working with TLS Certificates

By default, Operations Hub uses an internally created self-signed TLS certificate to securely encrypt the connection between its web server and your browser or API clients. Operations Hub automatically renews this certificate 30 days before expiration.

Users with admin privileges can replace Operations Hub's TLS certificate by uploading a valid X.509 certificate and its corresponding private key. The replacement TLS certificate can either be externally self-signed or signed by a Certificate Authority (CA).

Note Operations Hub is not capable of automatically renewing externally created self-signed certificates or CA-signed certificates. If Operations Hub has been configured to use either of those certificate types an Administrator must manually replace the certificate before its expiration.

Replacing the Current TLS Certificate

Use the following procedure to replace Operations Hub's current TLS certificate.

1. Log in to the Operations Hub WebUI with a user account which has admin privileges.
2. From the main menu, select **System > TLS Certificate**.

3. Click **Replace TLS Certificate** to open the *Replace TLS Certificate* panel. Carefully review any banner messages that may be displayed at the top of the panel.
4. Click **Choose files** to upload an X.509 certificate and private key in PEM encoded format. If you are uploading a CA-signed certificate that is created from an Operations Hub generated CSR, then you must not upload a private key. The private key is already stored in the cluster.
5. Click **Upload & Validate** to complete the procedure.

After upload, Operations Hub will attempt to validate the selected X.509 certificate and private key. If the validation succeeds the current TLS certificate is replaced.

Creating a Certificate Signing Request

Users with admin privileges can create a Certificate Signing Request (CSR) from within Operations Hub. The generated CSR can then be submitted to a Certificate Authority, thus simplifying the certificate signing process. Use the following procedure to generate a Certificate Signing Request:

1. Log in to the Operations Hub WebUI with a user account which has admin privileges.
2. From the Main menu, select **System > TLS Certificate**.
3. Locate the button labeled **Replace TLS Certificate** at the bottom right of the page.
4. Hover your mouse over the **three vertical dots** on the right side of the button.
5. Click **Generate Certificate Signing Request (CSR)**.
6. Enter the requested Cluster Information and Organization Information, then click **Generate**. The panel updates when the generation of the CSR and private key has completed.
7. Once the CSR and private key are ready, a copy of the CSR is downloaded to your local computer, and the corresponding private key will be saved internally within the cluster. If you must download another copy of the CSR click **Download CSR**.

Once the CSR is in your possession, follow your Certificate Authorities' process to submit the CSR, and have it signed. After the CA provides you with a CA-signed certificate, you can upload it to Operations Hub by following the procedure in the **Replace the current TLS Certificate section**.

Note Operations Hub generates a CSR with a sha512 with RSA encryption and an RSA key length of 4096 bytes.

Canceling a Certificate Signing Request

Users with admin privileges can cancel a previously created Certificate Signing Request (CSR). Use the following procedure to cancel a previously created Certificate Signing Request:

1. Log in to the Operations Hub WebUI with a user account which has admin privileges.
2. From the Main menu, select **System > TLS Certificate**.
3. Locate the button labeled **Replace TLS Certificate** at the bottom right of the page.
4. Hover your mouse over the **three vertical dots** on the right side of the button.
5. Click **Cancel Certificate Signing Request (CSR)**.

Configuring LDAPS Certificate

Feature Name	Release Information	Description
LDAPS Support	Cisco Smart PHY, Release 26.1	With this release, Smart PHY supports LDAPS using TLS or SSL to encrypt LDAP packets. This ensures that data cannot be intercepted by third parties while in transit. This feature enhances security as without encryption, credentials could be intercepted or a server response could be modified if is unencrypted.

LDAPS (Lightweight Directory Access Protocol over SSL/TLS) is a secure version of LDAP, designed to encrypt data transmissions between clients and directory servers like Microsoft Active Directory. It operates on port 636 to protect authentication credentials and directory information, preventing unauthorized interception during transit.

Server validation: Verify server certificate against a trusted CA(CA cert).

Client validation: If mTLS is enabled in LDAP server, client presents certificate and key; server validates client cert chain (CA cert, Client cert, Client key).

LDAPS certs files supported formats are:

- Server validation: CA cert (*.crt/.cer*).
- Client validation: CA cert (*.crt/.cer*), Client cert (*.crt/.cer*), Client key (*.key*).

Note Operations Hub is not capable of automatically renewing externally created self-signed certificates or CA-signed certificates. If Operations Hub has been configured to use either of those certificate types an Administrator must manually replace the certificate before its expiration.

Prerequisites

- LDAP server is reachable and supports LDAPS (default port 636).
- Ensure that you place **CA.crt** in the */etc/ssl/certs* path, and place **ldap-server.crt** and **ldap-server.key** in the */etc/ssl/ldap* path on the LDAP server.
- For mTLS, the server is configured to accept/require client certificates and trusts the client certificate issuer.

Creating a Certificate Signing Request

Users with admin privileges can create a Certificate Signing Request (CSR) from within Operations Hub. The generated CSR can then be submitted to a Certificate Authority, thus simplifying the certificate signing process. Use these steps to generate a Certificate Signing Request:

1. Log in to the Operations Hub WebUI with a user account, which has admin privileges.
2. From the Main menu, select **System > Security > LDAPS Certificate**.
3. Locate the button labeled **Replace LDAPS Certificate** at the bottom right of the page.

4. Hover your mouse over the **three vertical dots** on the right side of the button.
5. Click **Generate Certificate Signing Request (CSR)**.
6. Enter the requested Cluster Information and Organization Information, then click **Generate**. The panel updates when the generation of the CSR and private key has completed.
7. Once the CSR and private key are ready, a copy of the CSR is downloaded to your local computer, and the corresponding private key will be saved internally within the cluster. If you must download another copy of the CSR click **Download CSR**.

Once the CSR is in your possession, follow your Certificate Authorities' process to submit the CSR, and have it signed. After the CA provides you with a CA-signed certificate, you can upload it to Operations Hub by following the procedure in the **Updating the Current LDAPS Certificate** section.

Canceling a Certificate Signing Request

Users with admin privileges can cancel a previously created Certificate Signing Request (CSR). Use these steps to cancel a previously created Certificate Signing Request:

1. Log in to the Operations Hub WebUI with a user account, which has admin privileges.
2. From the Main menu, select **System > Security > LDAPS Certificate**.
3. Locate the button labeled **Replace LDAPS Certificate** at the bottom right of the page.
4. Hover your mouse over the **three vertical dots** on the right side of the button.
5. Click **Cancel Certificate Signing Request (CSR)**.

Updating the Current LDAPS Certificate

Use these steps to update Operations Hub's current LDAPS Certificate.

1. Log in to the Operations Hub WebUI with a user account, which has admin privileges.
2. From the main menu, select **System > Security > LDAPS Certificate**.
3. Click **Update LDAPS Certificates** to open the *Update LDAPS Certificates* panel. Carefully review any banner messages that may be displayed at the top of the panel.

Note When the certificates are uploaded, secrets are created in the **opshub-data** namespace:

- A CA certificate Secret for server validation (ldaps-ca-secret).
- An optional client TLS Secret for mTLS (client-generated certificates) (ldaps-client-cert).

4. Click **Choose files** to upload an CA certificate, X.509 certificate and client key in PEM encoded format.
5. Click **Upload & Validate** to complete the procedure.

After upload, Operations Hub attempts to validate the selected CA certificate, X.509 certificate and client key. If the validation succeeds the current LDAPS Certificates is uploaded.

Enabling LDAPS

Post updating the LDAPS Certificate, you can enable LDAPS using these steps:

1. From the main menu, select **System > Security > Authentication**.
2. Select the **Enable Secure LDAP** checkbox.