Security and Administration

Manage Users

Administrators on the Cisco Smart PHY application can perform the following tasks from the Cisco Operations Hub main menu > **Systems** > **Users & Roles**.

Note Only administrators can access the **User & Roles** option.

Add Users Through Cisco Operations Hub

Step 1 Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.

Step 2 Click **Add User**.

The **Add User** pane appears on the right side.

Step 3 Enter the following details:

- Username: email ID of the user.
- Select Role: Choose the appropriate role for the user. The drop-down list contains three options: Admin, Editor, and Viewer.
- Password: Password for the new user.
- Force password change on next login: This option is selected by default. New users must change the password after the first login.

Step 4 Click **Add User**.

Add Users Through CLI

Use the following procedure to create a new user:

Step 1 Define a new user using the following sample commands:

```
product opshub# smiuser add-user username <username> password <password>
message User added
product opshub#
product opshub# smiuser show-user username <username>
User: <username>, Group(s): <username>, Password Expiration days: 90
```

Note The default password expires in 90 days.

Example:

```
product opshub# smiuser add-user username user123 password Abcd123@
message User added
product opshub#
product opshub# smiuser show-user username user123
User: user123, Group(s): user123, Password Expiration days: 90
```

Step 2 Add a new user to the API group using the following commands.

Applicable groups for Cisco Smart PHY are `admin` and `api-admin`. By default, the `admin` user is mapped to group `admin`.

```
product opshub# smiuser assign-user-group username <username> groupname <groupname>
message User assigned to group successfully
product opshub
```

Example:

```
product opshub# smiuser assign-user-group username user123 groupname api-admin
message User assigned to group successfully
product opshub
```

Update User Password

Step 1 Click the Cisco Operations Hub main menu and click the username that is displayed at the bottom of the left pane.

The **My Account** page opens.

Step 2 Click **Update Password**.

The **Update Password** pane appears on the right.

Step 3 Update your password and click **Update**.

Edit Users

Step 1 Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.

Step 2 Select a user and click **Edit User**.

The **Edit User** pane appears on the right side.

Step 3 You can update the user role and password expiration period.

Step 4 Click **Save**.

Delete a User

Step 1 Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.

Step 2 Select a user and click **Remove User**.

The **Remove <user>** pop-up window appears.

Step 3 Click **Remove**.

Filter Users

Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**. Use the **Focus** drop-down list and the **Role** buttons, **Admin**, **Editor**, and **Viewer** to filter the users in the user list based on the password status and user role.

View Session History

Step 1 Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.

Step 2 Click a user name to open **User Details** pane on the right.

Step 3 Click the **Sessions History** tab to view the login and logout history of the user.

Authentication

The Cisco Smart PHY application is hosted on a Cisco Operations Hub cluster. Cisco Operations Hub provides the following authentication services for Cisco Smart PHY:

- Basic authentication
- LDAP authentication

Switch the authentication method of Cisco Operations Hub from the default Basic authentication to LDAP authentication, and vice versa, through the Cisco Operations Hub main menu > **System** > **Authentication** page. The procedures for switching between the authentication methods are provided in this section.

Switch from Basic Authentication to LDAP Authentication

Local authentication is enabled by default in the Cisco Operations Hub.

Note Only administrators can access the **Authentication** page.

LDAP support is limited to Microsoft Active Directly (AD) only. Open LDAP is not supported.

Step 1 Go to the Cisco Operations Hub main menu > **System** > **Authentication** to change the authentication method to LDAP.

Step 2 Enter the following details to configure LDAP.

LDAP Parameters	Description
LDAP Server URL	URL of the LDAP server.
Base Domain Name	Domain name as configured on your LDAP server.
LDAP User Name Domain	Validate the user name against the domain controller.
LDAP Filter	Specify a subset of data items in an LDAP data type.
LDAP Group Attribute	Comma-separated list of LDAP attributes on a group object that can be used in a user member attribute.
LDAP Group Mapping	Map LDAP group to the Cisco Operations Hub role.

Switch from LDAP Authentication to Basic Authentication

Local authentication is enabled by default in the Cisco Operations Hub.

Step 1 Go to the Cisco Operations Hub main menu > **Systems** > **Authentication** to change the authentication method to basic.

Step 2 If the LDAP authentication is enabled, click **Edit** and select the **Authentication Method** as **Local**.

Step 3 Save your changes.

Customize Login Banner

An administrator can create and customize a banner for the Cisco Operations Hub login page.

To customize the banner, use the following procedure:

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **System** > **Login Banner Message**.

Step 3 Enter the message in the text box and click Save.

A maximum of 500 characters are allowed in the banner message text box.

Database Backup

The *Database Backup* section includes the following entry fields:

- Server
- Username
- Password
- Directory
- Filename (Used exclusively for the Database Import function.)

The data that you enter in the **Server** field determines the location of the DB operation.

- Local backup—localhost
- Remote operation—IP address or hostname.domain.com

Local Backup

Local backup files are saved to the `/var/smartphy/backup` directory on the local filesystem.

Step 1 Go to Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **Global Settings** > **Database Backup**.

Step 2 In the **Server** field, enter **localhost**.

Leave the remaining fields blank (Username, Password, Directory, and Filename).

Step 3 Click **Export**.

Remote Backup

Remote backup files are saved to the remote server at the specified file path.

Step 1 Go to Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **Global Settings** > **Database Backup**.

Step 2 In the **Server** field, enter the IP address or the `hostname.domain.com` of the remote server.

Step 3 Enter the user login credentials in the **Username** and **Password** fields.

Step 4 In the **Directory** field, enter the file path on the remote server.

Leave the **Filename (Import Only)** field blank.

Step 5 Click **Export**.

Import Database

You can import local and remote backup files into the Cisco Smart PHY application.

Step 1 Go to Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **Global Settings** > **Database Backup**.

Step 2 In the **Server** field, enter the IP address or the `hostname.domain.com` of the remote server.

Step 3 Enter the following details in the **Filename (Import Only *)** field:

- Local backup: Enter only the filename of the backup file. This backup file is available in the default directory: `/data/smartphy/backup`.

  In this case, **Username**, **Password**, and **Directory** are disabled.

- Remote backup: Enter the file path (absolute path) of the remote server.

Step 4 Click **Import**.

After importing the DB, Cisco Smart PHY takes a few minutes to synchronize all the database entities. After synchronizing the credential details, Cisco cBR-8 devices appear online in the Cisco Smart PHY application.

After Cisco cBR-8 devices are online, enable the CIN.

Renew Kubernetes Client TLS Certificate

Cisco Smart PHY leverages Kubernetes for container orchestration. During the Cisco Smart PHY cluster deployment, Kubernetes client TLS certificates are created to secure the communication between the Kubernetes API server and kubelets. Kubernetes client TLS certificates are valid for one year.

⚠ **Caution** Renew the Kubernetes client TLS certificates before they expire. Otherwise, the operation and functionality of the Cisco Smart PHY cluster will be impacted.

Administrators can check the current status of the Kubernetes certificates by running the following command in the Linux shell:

```
sudo openssl x509 -enddate -noout -in /data/kubernetes/pki/kubelet-client-current.pem
```

The certificates are valid through the date that is listed in the attribute `notAfter=`.

For more information on renewing the Kubernetes Client TLS Certificate, contact your Cisco Account Team.