Security and Administration

- Configure Local Users, on page 1
- Authentication, on page 3
- Customize Login Banner, on page 4
- Database Backup, on page 4
- Export and Import Configuration, on page 6
- Working with Logs, on page 7

Configure Local Users

Administrators can perform following user management actions from **Systems > Security > Users & Roles**.

Note For users other than admin, User & Roles page isn't visible.

Add User

Step 1 On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2 Click **Add User** in the Users & Roles page to open Add User side bar.

Step 3 Fill in the email, role, and password for the new user. Strictly follow the password requirement listed in the side bar.

Force password change on next login option is selected by default. Newly created user must change the password during the first login.

Step 4 Click **Add User** button to confirm creating the new user.

Edit User

Step 1 On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2 Select a user and click **Edit User** in the Users & Roles page to open Edit User side bar.

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

Step 4 Click **Save** when you finish editing.

Remove User

Step 1 On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2 Select a user and click **Remove User** in the Users & Roles page, a window pops up.

Step 3 Click **Remove** in the pop-up window to remove the selected user.

Export

Step 1 On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2 Click **Export** in the Users & Roles page to export the content of the user management table.

Filter Users in the User List

You can use the **Focus** dropdown list and the **Role** buttons **Admin**, **Editor**, and **Viewer** to filter the users in the user list based on password status and user role.

View Session History

Step 1 On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2 Click a user name in the Users & Roles page to open User Details side bar.

Step 3 Select **Sessions History** tab to view the login/logout history of the user.

Change Password

You can change the password:

- from the Cisco Operations Hub main menu by clicking the user name and updating the password in the My Account page.
- from the alert banner. Alert banner appears 30 days before password expiry. You can change your password by clicking the link in the alert banner. If your password expires, reset the password during next login.

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

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

Step 1 Log in to any one of the control-plane nodes using the following command:

```
ssh -i <private-key-file> <smartphy-user>@<control-plane-node-ip>
```

Step 2 Enter the following command.

```
kubectl get svc ops-center-smartphy-data-ops-center -n smartphy-data
```

Note the cluster IP address and TCP ports of the service ops-center-smartphy-data-ops-center.

```
Ops-center-smartphy-data-ops-center    ClusterIP     10.x.x.x    <none>
    8008/TCP,8080/TCP,2024/TCP,2022/TCP,7681/TCP        19d
```

Step 3 Enter the following command to log in to the service resource using the password previously set by the deployer.

```
ssh admin@<cluster-ip-of-svc> -p <port-number>
```

Example:

```
smartphyuser: ~$ ssh admin@10.x.x.x -p 2024
Warning: Permanently added '[10.x.x.x]:2024' (RSA) to the list of known hosts.
admin@10.x.x.x's password:
Welcome to the smartphy CLI on user/data
admin connected from172.x.x.x using ssh on ops-center-smartphy-data-ops-center-774b8cc6fb-n6qmz
[user/data] smartphy#
```

Step 4 Run the following command to enter the configuration mode and get a list of available commands.

```
config
```

Use the `kong` command and its sub-commands.

Step 5 Display a list of configuration options available to configure the LDAP authentication plugin using the following command.

```
kong ldap_plugin configure ?
```

Step 6 Enter the required details of the Active Directory you want to use with the LDAP authentication plugin and enter `commit` to save.

Example:

```
kong ldap_plugin configure attribute cn ldap_host ldap.example.com ldap_port 309 base_dn
dc=example,dc=com
```

Step 7 Enter the following command to enable the LDAP authentication plugin.

```
kong ldap_plugin enable true
commit
```

By default, the LDAP plugin is disabled. However, the Basic authentication plugin is enabled.

If you are using the LDAP authentication plugin for the first time, you should configure before enabling it.

Step 8 Enter `end` to exit the config mode and `exit` to exit the service resource.

You can log in to the UI using an LDAP user credentials.

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.

Export and Import Configuration

The system administrator performs the import and export of Cisco Operations Hub configurations using the Cisco Operations Hub UI or RESTful APIs. The system administrator can store the exported configuration at a secure location. For Disaster Recovery, the system administrator performs the import operation to restore the Cisco Operations Hub to their original configurations.

From Cisco Operations Hub cluster, you can import and export:

- User Management data
- LDAP configuration
- Tag information
- Login Banner content
- User created Grafana and Kibana dashboards

Export Cisco Operations Hub Configuration using Cisco Operations Hub

To export the Cisco Operations Hub configuration, complete the following steps:

Step 1 Click the Cisco Operations Hub main menu button > **System** > **Import & Export** to open the Cisco Operations Hub Export/Import pane.

Step 2 Click **Export** in the **Export Configuration** section to download the file containing the configuration.

Step 3 Rename the file and save it to a secure location.

Import Cisco Operations Hub Configuration using Cisco Operations Hub

To import the Cisco Operations Hub configuration, complete the following steps:

Step 1 Click the Cisco Operations Hub main menu button > **System** > **Import & Export** to open the Cisco Operations Hub Export/Import pane.

Step 2 On the **Import Configuration** section, browse and choose an Operations Hub configuration file in tar.gz format.

Step 3 Click **Import**.

Update the User Password in the Exported User Management File

User password is not exported when you export the Cisco Operations Hub configuration. Therefore you have to provide a password before importing any configuration file. Otherwise the user management data will not be imported.

To update the user password in the user management file, complete the following steps:

Step 1 Extract the exported Cisco Operations Hub configuration files.

Step 2 Add a password in the user management JSON file.

Step 3 Repack the files.

Working with Logs

The Cisco Operations Hub provides you with a host of utilities that helps you to view, debug, visualize, and customise your log information.

View Audit Logs

The Audit dashboard leverages Kibana to provide meaningful visualization and a search interface for the raw log data.

You can view the Audit Logs dashboard by completing these steps:

Step 1 Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2 Click **Audit Dashboard**.

The Audit Dashboard provides the following information:

- A visualization of the count of audit logs against time. You can view this as a histogram.
- All user initiated events from UI or using API interface are logged and available as audit logs.
- For every log file, the Audit Dashboard provides the following facets of information:
  - **Time**: The time of logging the event.
  - **User**: The user initiating the event.
  - **API**: The API call used.

- **Status**: The HTTP response status code that returns when API was called.
- **Response Time**: The time taken by the API to execute.
- **Method**: The HTTP method the API used.
- **Service Host**: The application that served the request.

View Debug Logs

You can view the Debug logs dashboard by completing these steps:

Step 1 Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2 Click **Debug Dashboard**.

The Debug Dashboard provides the following information:

- A visualisation of the count of logs from different components against time is provided as a histogram.
- All internal application events logged by respective services or software components are captured as debug logs.
- For every log file, the Debug Dashboard provides the following facets of information:
  - **Time**: The time of logging the event.
  - **Source**: The application where the event happened.
  - **ContainerName**: The applications microservice that generated the event.
  - **LogLevel**: The log level.
  - **Message**: The entire log content.

Discover Logs

The Discover option allows you to search and find logs based on custom search definitions.

You can view the Discover option by completing these steps:

Step 1 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **System** > **Logs** to open **Logs** page.

Step 4 Click **Advanced** > **Discover** from the left navigation menu.

Step 5 Search for the log files.

You can perform basic text search, or advanced search by using KQL (Kibana Query Language) or Lucene search. Alternatively, you can also customize your search query based on time, debug-log type, selected fields, inspect option, and so on.

You can choose to save the search for later use from the dashboard.

Visualize Logs

You can create intuitive visualizations for your log data.

To create a visualization, complete these steps:

Step 1 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **System** > **Logs** to open **Logs** page.

Step 4 Click **Advanced** > **Visualize** from the left navigation menu.

Step 5 Click **Create visualisation**.

Step 6 Choose one of these visualization type:

- Area
- Control
- Coordinate Map
- Data Table
- Gauge
- Goal
- Heat Map
- Horizontal Bar
- Line
- Markdown
- Metric
- Pie
- Region Map
- TSVB
- Tag Cloud
- Timelion
- Vega
- Vertical Bar

Step 7 Choose a source type. You can choose from `audit-log`, `debug-log`, or `logstash` objects.

You can choose to save the visualizations to generate panels when you Create Dashboards , on page 10.

Create Dashboards

The Dashboard option allows you to create a new dashboard by adding panels from the saved Discover Logs option or Visualize Logs option. You can also create a new Dashboard from scratch.

Complete these steps to create a Dashboard:

Step 1 Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2 Click **Dashboard** > **Create dashboard**.

Step 3 Click **Add**.

Step 4 On the Add panels menu, select the required searched and saved logs and visualizations.

Step 5 You can choose to change existing filters or add filters.

Step 6 Click **Create new** to choose a visualization type. You can choose from these visualization types:

- Area
- Control
- Coordinate Map
- Data Table
- Gauge
- Goal
- Heat Map
- Horizontal Bar
- Line
- Markdown
- Metric
- Pie
- Region Map
- TSVB
- Tag Cloud
- Timelion
- Vega
- Vertical Bar

Step 7 Choose a source type. You can choose from `audit-log`, `debug-log`, or `logstash` objects.

You can view the saved dashboards on the dashboard list.