



Configuring Operations Hub

The Cisco Operations Hub allows you to create and configure users.

This section provides details on how to configure the Cisco Operations Hub and to use the Cisco Operations Hub UI and APIs.

- [Accessing Operations Hub, on page 1](#)
- [Navigation in Operations Hub, on page 1](#)
- [Customizing Login Banner, on page 2](#)
- [Using REST APIs, on page 2](#)
- [Deploying the Cluster with CA-signed Certificate Through Autodeloyer, on page 3](#)

Accessing Operations Hub

You can access the **Operations Hub** home page using the following URL:

```
https://{Hostname}
```

`Hostname` is the Fully Qualified Domain Name (FQDN) of the Cisco Operations Hub cluster, which is configured using the `ingress-hostname` key of the deployer configuration. If the Cisco Operations Hub cluster is deployed without the `ingress-hostname` key, then you must use the `Hostname` format as `{vip}.nip.io`, where `vip` is the virtual IP address of the Cisco Operations Hub cluster.

We recommend that you use FQDN for the Operations Hub cluster.

Navigation in Operations Hub

Once you deploy the Operations Hub successfully, you can navigate through the Operations Hub Web User Interface (UI) from the Main Menu.

The following table highlights the navigation options in Operations Hub:

Top-Level Menu Items	Second Level Menu Header	Second Level Menu Items	Description
Dashboards			View, search, and interact with Operations Hub's prepackaged Grafana visualization dashboards..

Top-Level Menu Items	Second Level Menu Header	Second Level Menu Items	Description
API Explorer			View and execute Operations Hub's APIs.
System		Logs	View and search Operations Hub's audit and debug logs.
	Configuration	Import & Export	Import & Export Operations Hub configuration.
	Security	Authentication	View or configure Operations Hub's authentication method (Local or LDAP).
		Login Banner Message	View or configure Operations Hub's login banner.
		User & Roles	View or configure local user accounts (name, credentials, and roles).
	Settings	Appearance	Modify Operation Hub's appearance.
Welcome		View and configure application login behavior.	

Customizing Login Banner

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

Use this task to customize the banner.

Step 1 At the main menu, select **System** > **Login Banner Message**.

The **Login Banner** window appears.

Step 2 Enter the banner message in the **Login Banner Message** field. You can enter a maximum of 500 characters.

Using REST APIs

This section explains how you can use REST APIs.

1. Create a user.

To create a new user, see **Adding Users** procedure in [Managing Users](#).

2. Call auth REST API to create a token.

Encode the username and password with base 64. Fill the encode output into the Authentication Header.

The following is a sample configuration to use REST API:

```
User: admin
Password: bell
```

```
Get the Base64 under Linux: echo -n 'admin:lab' | base64
Base64 encode output: YWRtaW46bGFi
```

```
curl -X POST "https://{Hostname}/api/auth/v1/token" -H "accept: application/json" -H
"authorization: Basic YWRtaW46bGFi"
```

```
Response code: 201
Response body
{
  "access_token":
  "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyY2x1IjoiYXBpLWZkbWluIiwic2FsdCI6IiViQ2daamt
  IWhd6RUNzS1EiLCJleHAiOiJlNjQ2NTA2MTd9.x7ccHcOn6fLvHc_ajLJxQEY1ftvR1ZaJH9K_YZx1ues",
  "refresh_token": "lYYtZqgVhnsnBJgSHbigRzeEaLnWziMpHJKVzgHA",
  "refresh_token_expire": 1567221017,
  "token_type": "jwt"
}
```

Deploying the Cluster with CA-signed Certificate Through Autodeloyer

When you deploy the Cisco Operations Hub cluster, the cluster is configured with a selfsigned certificate by default. You can deploy the cluster with a CA-signed certificate before running deploy script.

Use this task to deploy the cluster with the CA-signed certificate.

1. Generate a CA-signed certificate with a common name as "ingress-hostname" used in the day 0 configuration YAML file.
2. On the staging server, create a directory with the cluster name as the directory name under the path: "/certs/client_certificates". For example, if you use the cluster name as "testcluster", then the directory name must be "/certs/client_certificates/testcluster". This directory is the cluster ingress certificates directory.
3. Create the "cert-api-ingress" and "default-ssl-certificate" directories under the cluster ingress certificates directory.
4. Place the CA-signed certificate and keys under the "cert-api-ingress" directory. The CA signed certificate file has ".crt" extension and key file has ".key" extension.

