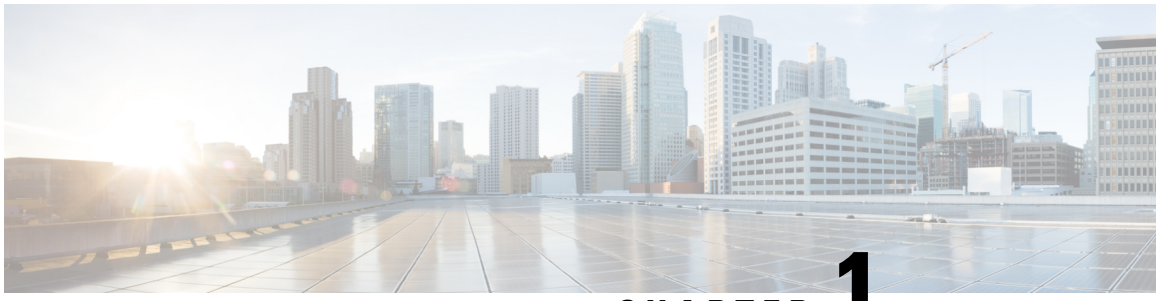
Cisco Operations Hub User Guide, Release 25.1

First Published: 2025-05-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Operations Hub

Cisco Operations Hub

Cisco Operations Hub is a scalable, highly available, resilient, cloud-native software hosting platform used by Service Providers to host applications including Cisco Smart PHY and Cisco iNode Manager. Operations Hub combines Cisco developed automation software, open-source container orchestration software, and open-source observability software into a pre-packaged solution that can be easily deployed and maintained by operations teams.

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.

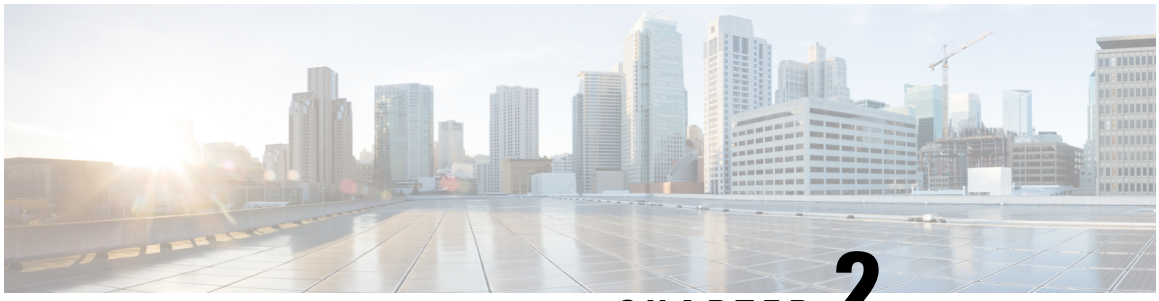
Navigation in Operations Hub

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
Alerts			View a summary of the total number of firing, pending, and warning alerts based on alert severity.
API Explorer			View Operations Hub API list.

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.
System		**Logs**	View and search Operations Hub's audit and debug logs.
System	**Configuration**	**Import & Export Configuration**	Import and export Operations Hub configuration.
System	**Security**	**Authentication**	View or configure Operations Hub's authentication method (Local or LDAP).
System	**Security**	**Login Banner Message**	View or configure Operations Hub's login banner.
System	**Security**	**TLS Certificate**	Configure the replacement of the cluster's current TLS (CA signed or self-signed) certificate using Operations Hub WebUI.
System	**Security**	**User & Roles**	View or configure local user accounts (name, credentials, and roles).
System	**Settings**	**Appearance**	Modify Operation Hub's appearance.
System	**Settings**	**Email Notifications**	Configure email notifications when alerts are triggered.
System	**Settings**	**Smart Licence**	Configure Cisco Smart Licence.
System	**Settings**	**Welcome**	View and configure application login behaviour.
System	**Support**	**TAC Debug Packages**	Create TAC debug packages for a cluster.



CHAPTER 2

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 4
Configuring Local Users, on page 4
Configuring LDAP Users, on page 8

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 4
Editing Local Users, on page 5
Removing Local Users, on page 5
Exporting User Details, on page 6
Using Filter Options, on page 6
Viewing Session History, on page 6
Changing Passwords, on page 7

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**.

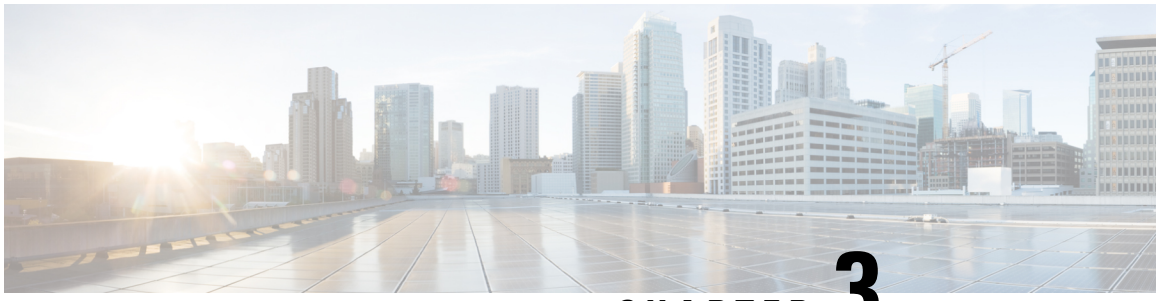
Once the CSR is in your possession, follow your Certificate Authorities' process to submit the CSR, and have it signed. After the CA provides you with a CA-signed certificate, you can upload it to Operations Hub by following the procedure in the **Replace the current TLS Certificate section**.

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)**.



CHAPTER 3

Configuring Operations Hub

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.

Exporting and Importing Configuration

You can import and export the Operations Hub configuration using the Cisco Operations Hub UI or RESTful APIs.

- **Export** - Enables you to store the exported configuration at a secure location.
- **Import** - Enables you to import the configuration during disaster recovery to restore the Cisco Operations Hub to its original configuration.

From Cisco Operations Hub cluster, you can import and export data for the following components:

- User management data
- LDAP configuration
- Tag information
- Login banner content
- User created Grafana and Kibana dashboards

Note Only Administrators can perform the import and export configuration.

Importing Configuration Using Cisco Operations Hub

This procedure imports the Cisco Operations Hub configuration.

Procedure

Step 1 At the main menu, select **System** > **Import & Export**.

The **Import & Export** page appears.

Step 2 In the **Import Configuration** area, browse and choose an Operations Hub configuration file or drag and drop the file. The Operations Hub configuration file must be in the *tar.gz* format.

Step 3 click **Import**.

Note
User passwords are 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 cannot be imported.

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

a. Extract the exported Cisco Operations Hub configuration files.

b. Add a password in the user management JSON file.

c. Repack the files.

Exporting Configuration Using Cisco Operations Hub

This procedure exports the Cisco Operations Hub configuration.

Procedure

Step 1 At the main menu, select **System** > **Import & Export**.

The **Import & Export** page appears.

Step 2 In the **Export Configuration** area, click **Export** to download the file containing the Operations Hub configuration.

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

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.

Procedure

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.

Configuring Time Zone

Table 4: Feature History

Feature Name	Release Information	Description
Configure Time Zone	Cisco Operations Hub, Release 23.3	You can change the time zone of a time stamp to be displayed in the Operations Hub GUI, on demand.

Cisco Operations Hub allows you to display and change the time zone on demand. When configured, the dates automatically change across all the Operations Hub UI pages. You may decide to temporarily set the time zone display value or retain it all the time. By default, all Operations Hub UI pages display the time based on the browser-identified time zone.

You can customize the time zone by using the following steps.

1. At the main menu, select **System > Appearance** under **Settings**. The Appearance window displays.
2. Enable the **Show Time Zone UTC offset** toggle switch and select a preferred UTC offset.
3. Disable the **Show Time Zone UTC offset** toggle switch if you want to disable the time zone offset feature.

Note Time zone setting is localized to a browser and a computer.

Configuring Email Notifications

Operations Hub is capable of sending notification emails when alerts are triggered. Administrators can customize the outbound SMTP configuration and enable or disable notifications for specific alert categories from the Operations Hub Web UI or API.

Alert categories include: Cluster, Operations Hub Infrastructure, DB Upgrade, Internal User Password Expiration, and System.

When notifications are enabled for a particular alert category, every time an alert in that category is triggered, the email addresses configured in that categories' notification recipient list are sent a notification email.

Enabling Email Notifications

Enabling Email Notifications consists of four steps:

1. Switching on Email Notifications
2. Configuring SMTP
3. Choosing Alert Categories and Recipients
4. Saving your Configuration

Switching on Email Notifications

Use this procedure to switch on Email Notifications.

1. At the main menu, select **System > Email Notifications**.
2. Click **Edit** at the bottom right of the page.
3. Locate the switch labeled **Email Notifications** and toggle it on.
4. Click **Save**.

Note Even though Email Notifications have been switched on, notifications won't be sent until you complete the SMTP configuration, choose your Alert Categories & Recipients, and save your configuration.

Configuring SMTP

Use this procedure to specify or change the email address, SMTP server hostname, and port number Operations Hub uses to send notification emails.

Before you begin, make sure that Email Notifications are switched on.

1. At the main menu, select **System > Email Notifications**.
2. Click **Edit** at the bottom right of the page.
3. Locate the **SMTP Configuration** card.
4. Enter the **SMTP configuration** details.

Field	Description
From Email Address	Operations Hub uses this email address as its *From* address when sending email notifications.
SMTP Server Hostname	Operations Hub uses this SMTP server to send email notifications.
SMTP Server Port Number (Optional)	By default, Operations Hub uses port 25 to connect to the specified SMTP server. You can optionally enter a different port number.

1. Click Save.

Choosing Alert Categories and Recipients

Use this procedure to enable or disable notifications for one or more alert categories and to add or remove email addresses from a categories' notification recipient list.

Before you begin, make sure that **Email Notifications** are switched on, and your **SMTP Configuration** is completed.

1. At the main menu, select **System > Email Notifications**.
2. Click Edit at the bottom right of the page.
3. Locate the **Alert Categories** card.
4. Enable the switch next to an Alert Category name to turn on notifications for that category or disable the switch to turn off notifications.
5. Click the Alert Category name to open its **Notification Recipient List** panel.
6. Add or remove email addresses.
7. Click Save, to save your email addresses and close the panel.

Note You must save your configuration to complete the enablement of email notifications.

Saving your Configuration

Use this procedure to save your SMTP configuration, Alert Category & Recipients choices, and enable email notifications.

1. From the **Email Notifications** page, click **Save** at the bottom of the page.

Figure 1: Email Notifications

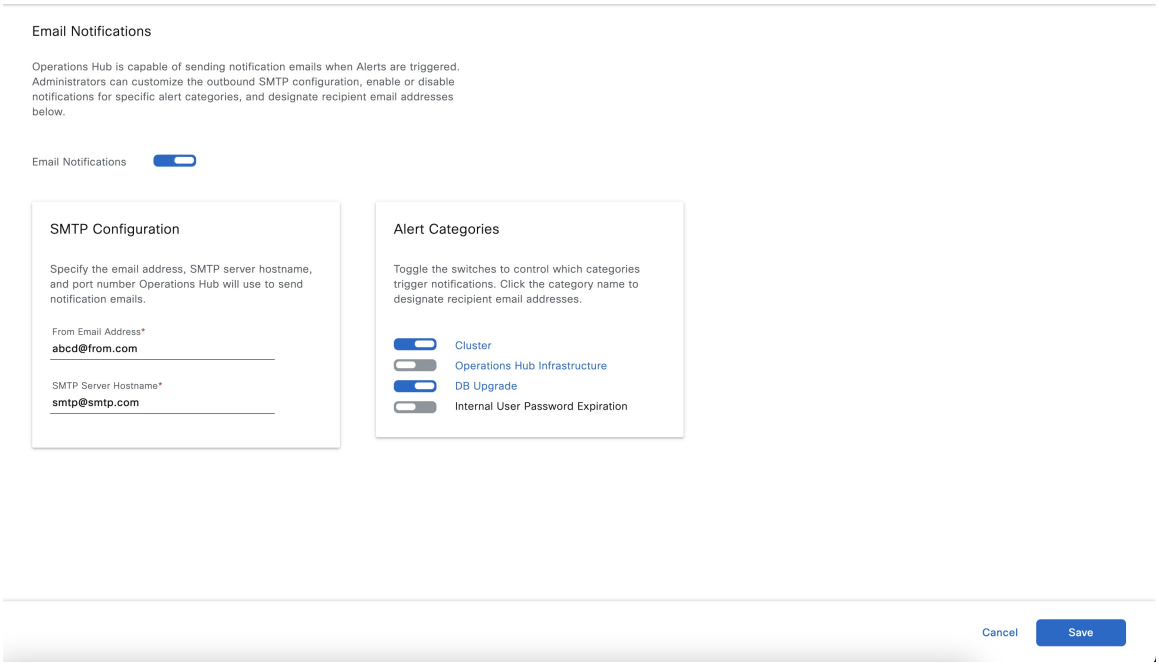
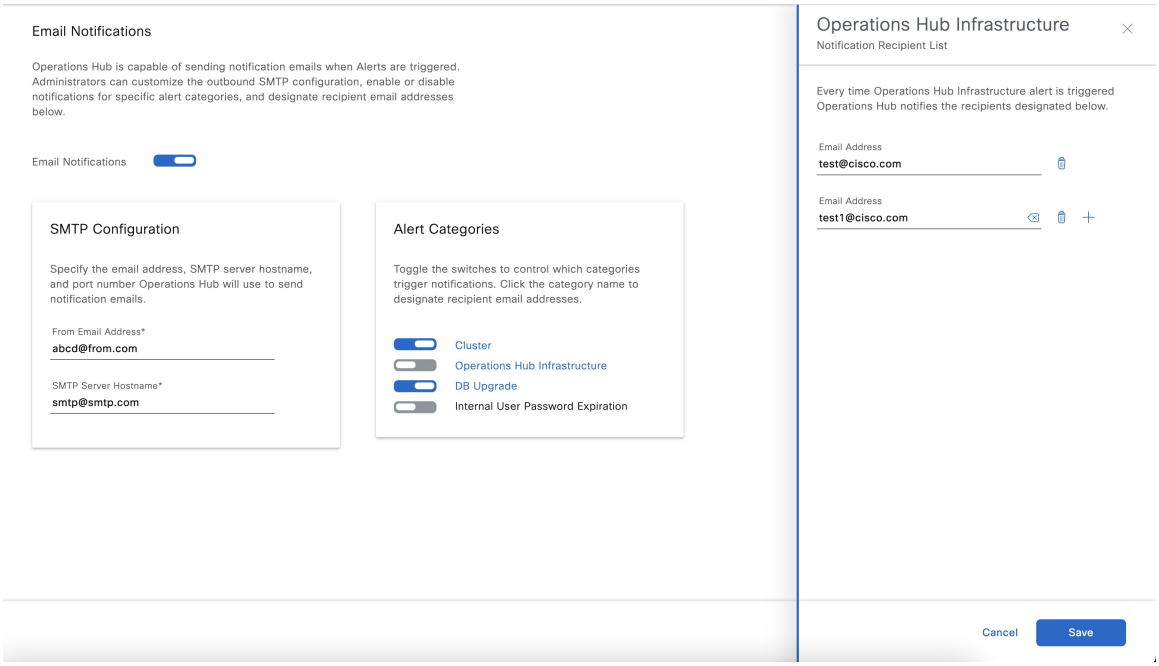


Figure 2: Notification Recipient List



Configuring Cisco Smart Licensing

Table 5: Feature History

Feature Name	Release Information	Description
Support for Configuring Cisco Smart Licensing	Cisco Operations Hub, Release 23.1	Cisco Operations Hub supports the configuration of Smart Licensing using Operations Hub WebUI.

Cisco Smart Licensing is a new and flexible method of licensing, to buy, deploy, track, and renew Cisco software. With Smart Licensing, you can configure, activate, and register your application. Smart Licensing establishes a pool of software licenses that you can use across your entire enterprise in a flexible and automated manner.

The following sections describe several utilities and processes that are necessary to complete the registration and authorization.

Prerequisites for Smart Licensing

To enable Smart Licensing on Operations Hub, ensure that you have the following components in place:

- Access to Cisco Smart Software Manager (CSSM)
- Smart Account (SA) and Virtual Account (VA). If you don't have a smart account, see Create a Smart Account.
- Cisco Operations Hub
- Cisco Smart Software Manager On-Prem (Optional)

Configuring Smart License

You can configure the Smart License using Operations Hub by selecting **System > Smart License** at the Main Menu.

Configuring CSSM URL on Device

At the Main Menu, select **System > Smart License** and click **Edit SSM Connection Mode** in Smart License page to select the connection mode.

Select one of the options provided by Operations Hub:

1. **Direct** mode requires direct internet access to Cisco SSM cloud.
2. **Cisco SSM On-Prem** offers security sensitive organizations near real-time visibility and reporting of the Cisco licenses purchased and consumed, without requiring direct internet access.
3. **Reservation** offers mechanism to reserve licenses and install them.

Click **Save** to save the SSM Connection Mode.

Performing Device Registration

At the Main Menu, select **System > Smart License** and click **Register** at the bottom right. You must also log in to Cisco Smart Software Manager (CSSM) to generate a token. Tokens are generated to register a new product instance to the virtual account. Use the following steps to generate a new token from the Cisco Smart Software Manager (CSSM) and register.

1. Click *Register*. A new panel to accept a registration token displays.
2. Keeping the Operations Hub open, log in to CSSM at https://software.cisco.com/. Ensure that you use a username and password that is provided by Cisco.
3. Click *Inventory*.
4. Select your virtual account from the Virtual Account drop-down list.
5. Click *General > New Token*.
6. Create a registration token. Provide a token description. Specify the number of days that the token must be active.
7. Switch the Export-Controlled functionality to *Allow* the products to register with this token.
8. Click *Create Token*. After the token creation, click *Copy* to copy the newly created token.
9. Come back to Operation Hub. Paste the token generated in the previous step under Registration Token and complete the registration process.
10. On successful registration, the dashboard displays the status as Registered. An error is generated if registration fails.

Deregistering a Device

At the Main Menu, select **System > Smart License** and click **Deregister** to deregister your device.

Performing License Reservation

License reservation is a mechanism to reserve licenses and install them. The following are the license reservation types:

- Specific License Reservation (SLR): Only specific licenses are reserved. Supports term licenses.
- Permanent License Reservation (PLR): All licenses are reserved.

Specific License Reservation

Specific License Reservation (SLR) is a Smart Licensing functionality that enables you to deploy a software license on a device without communicating usage information to Cisco. SLR allows you to reserve a license for your product instance from the Cisco Smart Software Manager (CSSM). This feature is used in secured networks.

To create an SLR, use the following steps:

1. Generate the reservation request code from Cisco Operations Hub Main Menu by selecting **System > Smart License**, at the Main Menu.

- Click **Edit SSM Connection Mode**, select the **Reservation** connection mode and click **At the Main Menu, select System > Smart License and click Edit SSM Connection Mode in Smart License page to select the connection mode.**.
- Hover the mouse pointer to the bottom right of the screen (Next to **Guided Licence Reservation**).
- Click **Generate Reservation Request Code** to generate a Reservation Request Code.
- Click **Generate Code** to generate a Reservation Request Code.
- Copy the Reservation Request Code displayed on the screen.

2. Log in to Cisco Smart Software Manager at https://software.cisco.com/. Log in to the portal using a username and password that is provided by Cisco.
3. Click **Inventory**.
4. Select your virtual account from the Virtual Account drop-down list.
5. Click **Licenses > License Reservation**.
6. Select **SLR entitlement**.
7. Provide a token description. Specify the number of licenses to be reserved for every entitlement.
8. Click **Create Token**. After the token is created, click **Copy** to copy the newly created token.
9. Install the reservation key on the device from Operations Hub.
   - Click **Submit Reservation Authorization Code**.
   - Paste the Reservation Authorization Code in the Reservation Authorization Code field or upload the downloaded Reservation Authorization Code file.
   - Click **Reserve**.

Permanent License Reservation

Permanent License Reservation (PLR) is a set of capabilities that are designed for highly secure environments. PLR restricts all communications with the outside environment.

To create a PLR, complete the following steps:

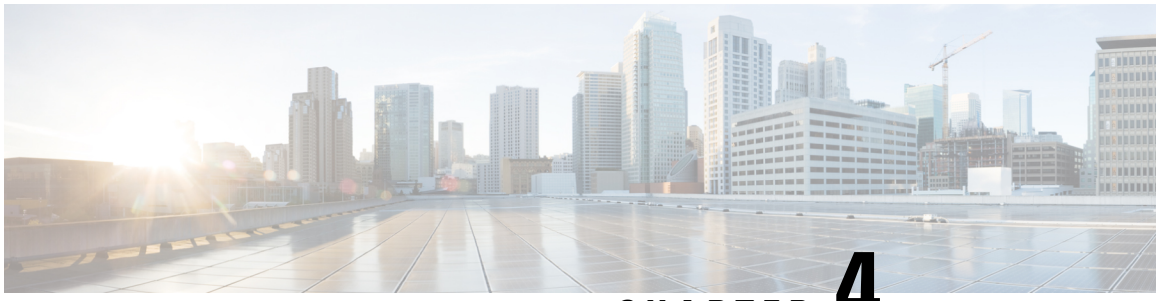
1. Generate the reservation request code from Cisco Operations Hub Main Menu by selecting **System > Smart License**, at the Main Menu.
   - Hover the mouse pointer to the bottom right of the screen (Next to **Guided Licence Reservation**).
   - Click **Generate Reservation Request Code** to generate a Reservation Request Code.
   - Click **Generate Code** to generate a Reservation Request Code.
   - Copy the Reservation Request Code displayed on the screen.
2. Log in to Cisco Smart Software Manager at https://software.cisco.com/. Log in to the portal using a username and password that is provided by Cisco.
3. Click **Inventory**.

4. Select your virtual account from the Virtual Account drop-down list.
5. Click **Licenses** > **License Reservation**.
6. Select **PLR entitlement**.
7. Provide a token description. Specify the number of licenses to be reserved for every entitlement.
8. Click **Create Token**. After the token is created, click **Copy** to copy the newly created token.
9. Install the reservation key on the device from Operations Hub.
   - Click **License Reservation > Submit Reservation Authorization Code**.
   - Paste the Reservation Authorization Code in the Reservation Authorization Code field.
   - Click **Reserve**.

Returning License Reservation

Note Ensure that you can access Cisco Smart Software Manager (SSM). Use the following steps to return a license reservation:

1. Generate the reservation request code from Cisco Operations Hub Main Menu by selecting **System > Smart License**, at the Main Menu.
   - Hover the mouse pointer to the bottom right of the screen (Next to **Guided Licence Reservation**).
   - Click **Return All License Reservations**.
   - Click **Generate Code** to generate a Reservation Request Code.
   - Copy the Reservation Return Code displayed on the screen.
2. Log in to Cisco Smart Software Manager.
3. Submit the Reservation Return Code to return your license.



CHAPTER 4

Monitoring Operations Hub

Alerts

All alerts are built based on the KPI metrics and divided into several alert groups. Each KPI metric generates one alert that belongs to a predefined alert group.

Alert Record

The **Alert Management Dashboard** captures all alerts that are generated in the Cisco Operations Hub cluster. This dashboard displays alert summary and detailed information about those alerts.

Viewing Alert Summary

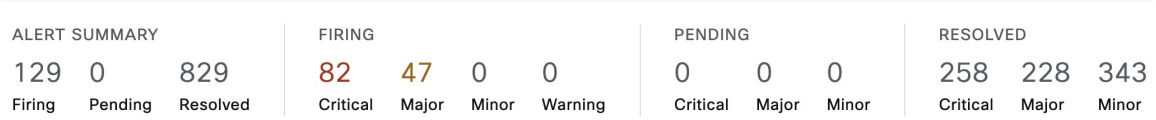
The **Alerts** page displays a summary of total number of firing, pending, and warning alerts based on alert severity. You can access the alert overview page from the main menu.

1. At the main menu, select **Alerts**. The **Alerts** page appears.
2. View **Alert Summary**.

Cisco Operations Hub supports the following alert severity:

- Critical
- Major
- Minor
- Warning

Figure 3: Alerts Summary



Viewing Alert Information

You can view a list of firing alerts that are currently active and a list of resolved alerts. At the main menu, select **Alerts** to view the alerts.

Alerts Summary Total count of firing, pending and resolved alerts. Count of alerts are based on severity.

Figure 4: Alerts Summary

You can filter alerts on any of the following conditions:

Table 6: Filter condition

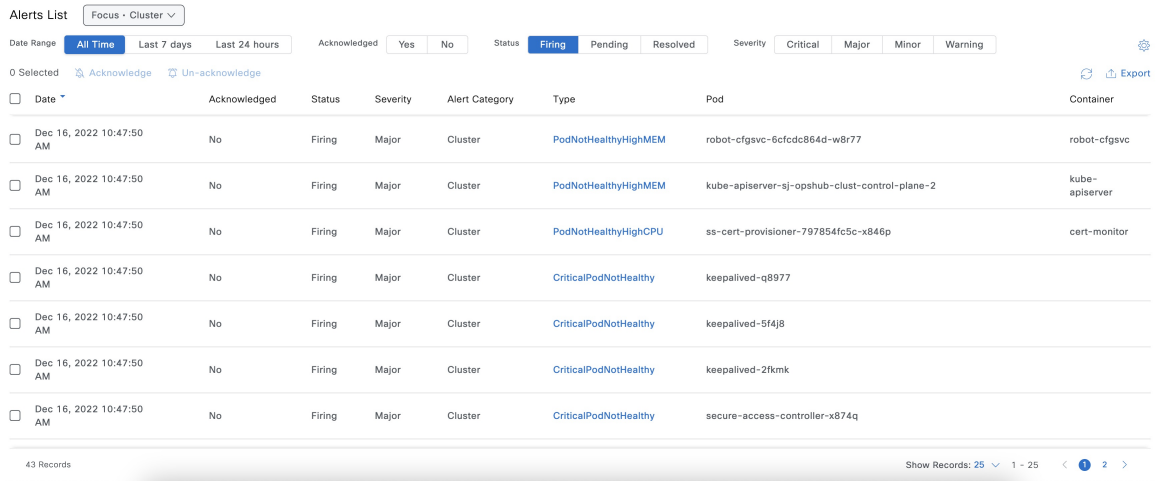
Filter condition	Description	Options
Focus filter	List of Alert categories	**Cluster** (default), **Operations Hub Infrastructure**, **DB Upgrade**, **Internal User Password Expiration**, **System**
Date Range	Filter alerts in a specific time window	**All Time** (default), **Last 7 days**, **Last 24 hours**
Acknowledged	Filter using acknowledgement status	**Yes**, **No**
Status	Status of an alert	**Firing** (default), **Pending**, **Resolved**
Severity	Severity of the alerts	**Critical**, **Major**, **Minor**, **Warning**

Table 7: Alerts table

Field	Description	Options
Date	Date and Time when the alert is fired	**Date and Time**
Acknowledged	Shows whether an alert is acknowledged or not	**Yes, No**
Status	Status of the alert	**Firing, Pending, Resolved**
Severity	Severity of the alert	**Critical, Major, Minor, Warning**
Alert Category	Category of the alert	**Cluster, OperationsHubInfra, DbUpgrade, InternalUserPasswordExpiry, System**

Field	Description	Options
Type	Type of the alert	**High CPU, High Memory**
Pod	Details of the pod generating an alert	**Pod-Details**
Container	Details of the container generating an alert	**Container-Details**

Figure 5: Alerts List



You can view the details of an alert by clicking the Alert Type. The alert details panel captures the following fields:

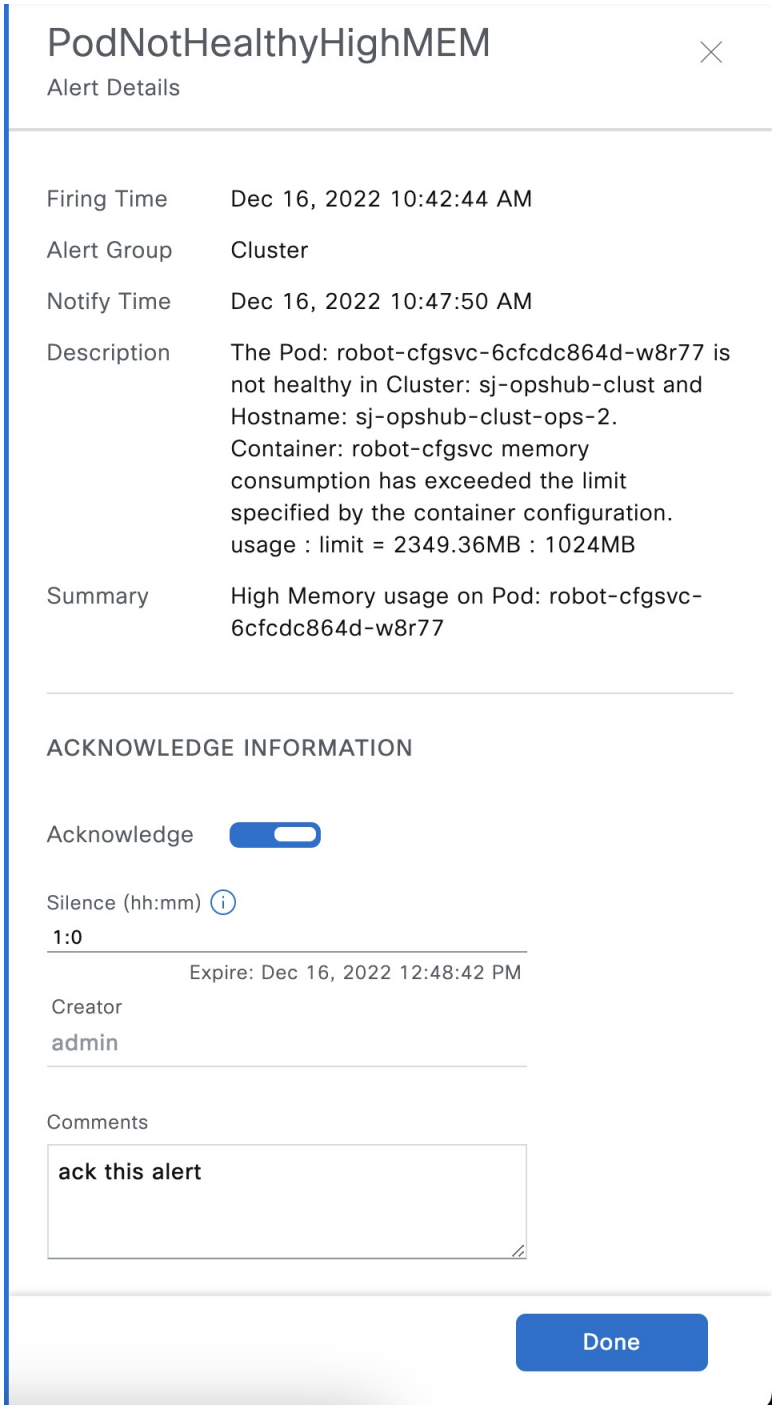
Field	Description
Status	Status of the alert
Firing Time	Time when alert is raised
Alert Category	Category of the alert
Notify Time	Displays alert notify time
Description	Description of the alert
Summary	A short summary of the alert

Figure 6: Alerts Details

Acknowledging Alerts

Once an alert is raised, you can acknowledge the firing alert. You have an option to put a comment before you acknowledge. You can also silence alerts for a predefined time in case you wish to ignore the alert during that time. By default, every three hours you are notified about the firing alerts by email.

Figure 7: Acknowledging Alerts



Monitoring Cluster Health

Table 8: Feature History

Feature Name	Release Information	Description
Cluster Health Monitoring	Cisco Operations Hub 22.2	Cisco Operations Hub supports viewing and monitoring of the cluster health using the alert management feature. An alert is raised when there is an issue and you can take necessary action based on the severity of the alert. You can view the cluster health information using the **Kubernetes Cluster Health** dashboard.
Alert UI	Cisco Operations Hub, Release 22.4	Alert UI is introduced.

Operations Hub enables you to view and monitor the cluster health using the alert management feature. For each cluster, you can map an alert-group to check the cluster health status and take required action. Each alert is categorized based on severity which helps you prioritize the action for taken for that alert. If you do not specify any alert-group for the cluster, then all available alert-groups are added to the cluster

A cluster can have the following types of health alerts:

- **Clear** - Indicates that the cluster has no alerts and everything is working as expected.
- **Minor** - Indicates that a few nonessential pods are not running in the cluster. If you see this alert, then rectify the problem at the earliest.
- **Critical** - Indicates that the cluster has critical problems. Take immediate action before the service degrades further.

Each alert-group is independent in nature, and therefore it is important to review all the alert-groups. Ensure that you take corrective actions that are based on the overall cluster health and not just for an individual alert-group.

For example, an essential pod such as **timescaledb** can have high CPU usage, which causes it to raise a **Critical** alert. This is part of the *Cluster* alert-group for which the cluster health severity is **Critical**.

Similarly, if there are no critical alerts for the *InternalUserPasswordExpiry* alert-group and all the pods are running in the cluster, then the cluster health severity is **Clear**.

For more information regarding *Operations Hub Infra Alert Management API*, see Cisco Operations Hub and Smart PHY REST API Guide

1. At the main menu, choose **Dashboards**. The **Dashboard Gallery** page appears.
2. Click **Kubernetes Cluster Health**.

   The **Kubernetes Cluster Health** dashboard displays.
3. At the main menu, select **Alerts** .

   The **Alerts** page displays.

Viewing and Managing System Logs

Feature History

Feature Name	Release Information	Description
Dedicated Application Debug Logs	Cisco Operations Hub 22.3	You can view application-specific debug logs using the Debug Dashboard.

Operations Hub provides a tool for log aggregation and management, leveraging the power of ElasticSearch-Logstash-Fluentd-Kibana (ELK) stack. The Operations Hub GUI uses Elasticsearch as the data store for logs, and Kibana provides meaningful visualization of the raw log data. You can create both macro and micro views using various visualization techniques.

Enabling Log Management using ELK stack

During deployment, the Operations Hub is configured to forward logs from all the components to ElasticSearch for aggregation and indexing, providing some default visualizations and also available for creating custom visualization, search, and analysis.

Viewing Audit Logs

This procedure enables you to view the audit logs.

Procedure

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

The **Audit Dashboard** page appears.

Step 2 You can view the preconfigured information of audit logs in the following representations:

- Histogram—A view that displays a count of audit logs against time.
- Audit Log Table—A table that displays the audit logs generated based on user-initiated events from UI or using API interface.

  You can view the following information in the audit log table:

  Table 9: Audit Log

Field	Description
Time	The time when the event is logged.
User	The user who initiated the event.
API	The API that is called.
Status	The HTTP response status code that is returned on invoking the API.

Field	Description
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.

a. You can also search the logs based on following options:

- Kibana Query Language (KQL) query or fields as specified in the logs, and save the search using **Save Current Query**.
- Time duration as absolute time period, relative time, and now.
- Using filter options based on fields and operator enables you to narrow down the search. You can also edit the filter as query DSL and create custom label to the search.

b. Click **Update** to update the query.

c. Click **Refresh** to refresh and add a new search query.

Viewing Debug Logs

This procedure enables you to view the audit logs.

Procedure

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

The **Debug Dashboard** page appears.

Step 2 You can view the preconfigured information of audit logs in the following representations:

- Histogram—A view that displays a count of audit logs against time.
- Debug Log Table—A table that displays the audit logs generated based on user-initiated events from UI or using the API interface.

  You can view the following information in the debug log table:

Table 10: Debug Log

Field	Description
Time	The time when the event is logged.
User	The user who initiated the event.
API	The API that is called.

Field	Description
Status	The HTTP response status code that is returned on invoking the API.
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.

Viewing Logs Using Advanced Option

Advanced options enable you to create and customize the dashboards and visualizations as required.

Procedure

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

The **Debug Dashboard** page displays.

Step 2 At the left-side menu, click **Advanced**. You can view the following submenus:

- **Dashboards**—The **Dashboard** page allows you to view available dashboards or create a new dashboard view using the **Create Dashboard**. To create the new dashboard, add panels from saved 'Search' or 'Visualization', or you can create a new Visualization using available visualization types. Once you save the dashboard, click the **Dashboard** in the left side menu, and you can view the new dashboard.
- **Discover**—The **Discover** page allows you to find logs based on custom search definitions. You can save the search and later access, and use the saved search in the Dashboard. You can perform basic text search and advanced search using the KQL or Lucene Search.
- **Visualize**—The **Visualize** page enables you to view available library of logs or create a new Visualization. To create a new Visualization, click **Create Visualizations**, and select one of the available visualization types such as Lens, Maps, TSVB, Custom Visualization, and Aggregation based in the **New Visualization** page. Enter required search information. Once the visualization is created, you can save and use to create panels in the Dashboard.

Dedicated Application Debug Logs

If you have installed applications such as Smart PHY on Operations Hub, you can view the application-specific debug logs.

Procedure

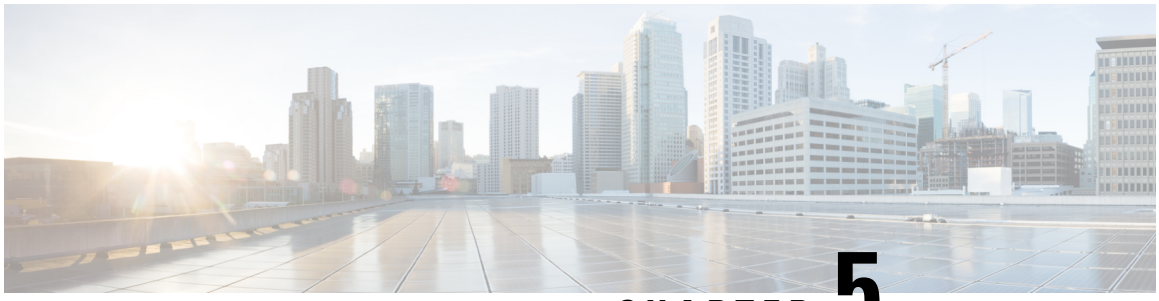
Step 1 At the main menu, select **Systems** > **Logs**.

Step 2 At the left-side menu, click **Debug Dashboard** option under the application header to view application-specific debug logs.

Refreshing the Dashboard

You can set the refresh time for each dashboard, choose the time from the drop-down list on the top-right corner of the dashboard. You can select any time from 5 sec to 1 day. If you decide to avoid page refresh, selecting "off" from drop-down menu does not refresh the page.

If data is retrieved, you can choose a time range. It can be absolute time range where you can provide a time interval or you can select the range from a predefined drop down menu.



CHAPTER 5

Maintaining Operations Hub

Performing Cluster Maintenance

Feature History

Feature Name	Release Information	Description
Support for Performing Cluster Maintenance	Cisco Operations Hub, Release 23.1	Cisco Operations Hub supports cluster maintenance tasks when there's cluster node maintenance or node failure.

This section provides information about how to handle an Operations Hub cluster when there's cluster node maintenance or node failure.

Maintenance activities for cluster nodes can be classified as:

- Planned maintenance: This activity is performed when the cluster node is still working but needs to be removed from the Kubernetes cluster for maintenance. Maintenance activity in this case drains the node, remove all the pods running on the node, and marks the node as not schedulable.
- Unplanned maintenance: This activity is performed when the node is dead. The node state is *Not Available*, and its IP address is unreachable. In this case, since the node is present in the vCenter but isn't running, it's deleted and re-created during maintenance.

Cluster Node Maintenance through Autodeploy Tool

Use the following steps to perform maintenance of cluster through the Autodeploy tool.

1. To trigger cluster maintenance, use the --maintenance option as an argument with the Autodeployer.

   ```
   ~/opshub-installer-<release-version-tag>$ ./deploy -c <config_file> --maintenance
   ```

2. Cluster maintenance provides you two options. Select one of the two available options:
   - **Node Maintenance**: Use this option to push one or more nodes into maintenance. After selecting this option, Autodeployer shows a list of node names and prompts the user to enter a list of nodes to be maintained in a comma-separated way.

- **Host Maintenance**: Use this option to push all the nodes running on the ESXi host to maintenance. Typically used when an upgrade is planned for ESXi. After selecting this option, Autodeployer shows a list of ESXi host IPs and FQDNs and prompts the user to select one of the ESXI host details. After selecting ESXi host IP/FQDN, all nodes running on top are pushed into maintenance.

Note

- During the maintenance activity, the Autodeployer ensures that the quorum criteria aren't broken.
- Maintenance procedure is application only on a Multinode installation.

Resuming Cluster Node from Maintenance through Autodeploy Tool

Use the following steps to resume cluster nodes from maintenance through Autodeployer.

1. To resume cluster nodes from maintenance, use the --resume-maintenance option as an argument with the Autodeployer.

```
~/opshub-installer-<release-version-tag>$ ./deploy -c <config_file> --resume-maintenance
```

This ensures that all the nodes under maintenance are added back to the cluster. If nodes are deleted due to unplanned maintenance, those nodes are recreated.

TAC Debug Package

Table 11: Feature History

Feature Name	Release Information	Description
Inclusion of Meta Data and `robot-cfgsvc` pod logs in TAC Debug Packages	Cisco Operations Hub, Release 23.3	TAC debug packages are more descriptive and include metadata information such as created date, file size, created user, and the start and end collection dates entered at the time of creating the packages. TAC debug packages also include `robot-cfgsvc` pod logs.
TAC Debug Package Enhancements	Cisco Operations Hub, Release 22.3	You can create a TAC debug package for a cluster using the Operations Hub GUI. You can select start and end dates, and start and end times, while creating TAC Debug Packages. You can download TAC Debug Packages locally and delete TAC Debug Packages, if necessary.
TAC Debug Package	Cisco Operations Hub, Release 22.2	You can create a TAC debug package for a cluster. The collected information helps the TAC team to debug and troubleshoot the issue at the earliest.

The TAC Debug feature in Operations Hub enables you to create and collect the debug package for a specified time duration. You can download the debug package and attach it to a TAC case.

When you trigger the create operation on the Operations Hub cluster, you can monitor the status of the operation as **ongoing** or **completed**. When the operation is complete, the TAC debug package is available for download.

Creating and Downloading TAC Debug Package

To create a TAC Debug package:

1. At the main menu, select **System** > **SUPPORT** > **TAC Debug Packages**.
2. Enter the start and end dates, and start and end times, which are required for the data collection.
3. Click **Create**.

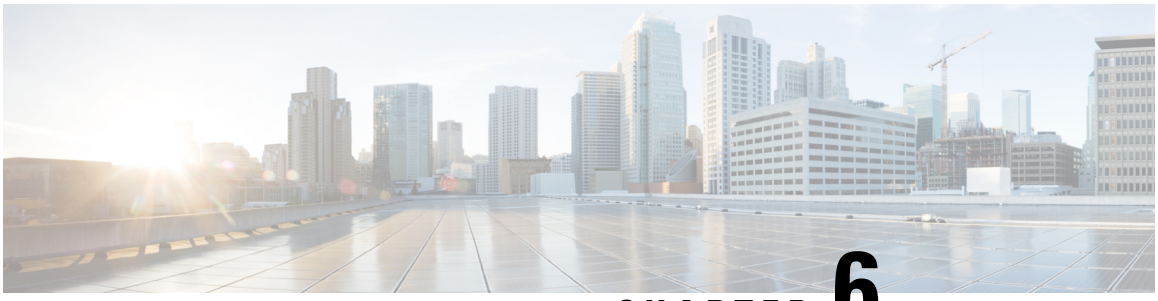
   The TAC Debug package is created along with the following metadata that is displayed below it:

   Table 12: TAC Debug Package Metadata Fields

Metadata Field	Description
Created	Date of Creation
File Size	Size of the TAC Debug package(in MB)
Created By	User who created the TAC Debug package
Created From	Start date of data collection (Entered during TAC Debug Package creation)
Created To	End date of data collection (Entered during TAC Debug Package creation)

   The latest TAC Debug package is displayed on top.
4. When a package is created:
   - You can download a package locally by clicking the package name.
   - You can delete a package by clicking the **Delete** icon.

Note TAC debug packages can be large and can demand significant storage space on the disk. To optimize the cluster disk space, Operations Hub allows you to store up to ten TAC debug packages. We recommend that you delete the old TAC debug packages from the cluster if you don't need them.



CHAPTER 6

Using REST APIs

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, on page 3.

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.eyJyb2xlIjoiYXBpLWFkbWluIiwic2FsdCI6IlViQ2daamt
IWHd6RUNzS1EiLCJleHAiOjE1NjQ2NTA2MTd9.x7ccHcOn6fLvHc_ajLJxQEY1ftvR1ZaJH9K_YZx1ues",
"refresh_token": "lYYtZqgVhnsnBJgSHbigRzeEaLnWziMpHJKVzgHA",
"refresh_token_expire": 1567221017,
"token_type": "jwt"
}
```

3. You can use the `access_token` created in the previous step to make individual REST API calls.

   The following is a sample configuration to make individual REST API calls, with user as `access_token` with header `Authorization: Bearer`.

```
curl -X GET https://{hostname}/api/rbac/v1/identitymgmt/user -H "accept: application/json"
 -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZSI6ImpUWFkbWluufGFwaS12aWV3ZXJ8YXBpLWVkaXRvcnxhcGktYWRtaW4
iLCJzYWx0IjoiZU9ZR0RtRFBsVFVwaEglWCIsImV4cCI6MTY4MTc3Nzg2NCwic3ViIjoiYWRtaW4ifQ.gYIFghIusN4uN6ok0Ey8sANPTqRw_VdWmvtqklzkNDU"
 -k
{
"userDetailList":
[
{
"groupList":
[
"admin",
"api-admin",
"api-editor",
"api-viewer"
],
"username": "admin",
"passwordExpiryPeriod": "90"
}
]
}
```

Importing Configuration Using RESTful API

You can import the Cisco Operations Hub configuration and check the status of the import operation using the following APIs:

```
https://<HostName>/utility/v1/config/import
https://<HostName>/utility/v1/config/operation/status
```

Exporting Configuration Using RESTful API

You can export the Cisco Operations Hub configuration and check the status of the export operation using the following APIs:

```
https://<HostName>/utility/v1/config/export
https://<HostName>/utility/v1/config/operation/status
```