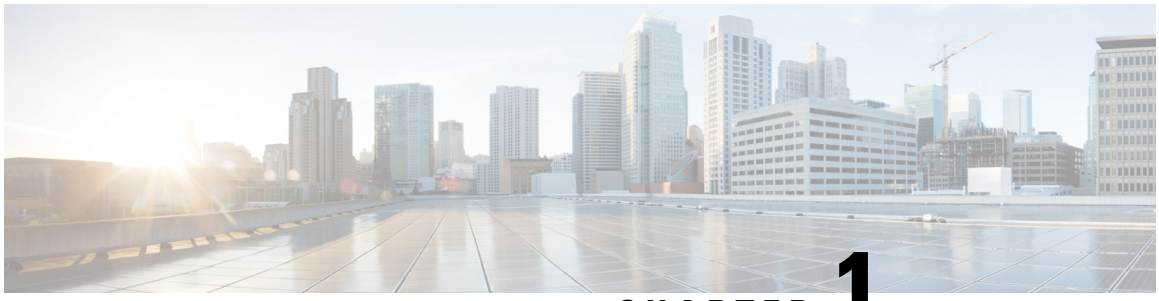
Cisco Operations Hub User Guide, Release 22.2

First Published: 2022-07-20

Last Modified: 2023-01-18

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

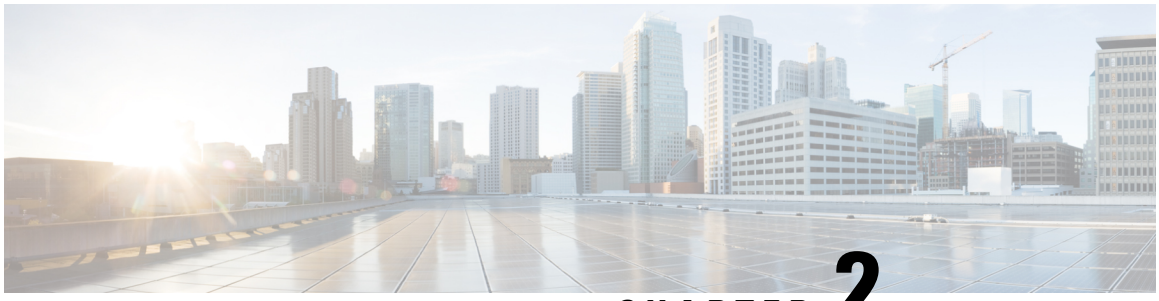
CONTENTS



CHAPTER 1

Cisco Operations Hub

Cisco Operations Hub 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.



CHAPTER 2

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

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, on page 7.

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:

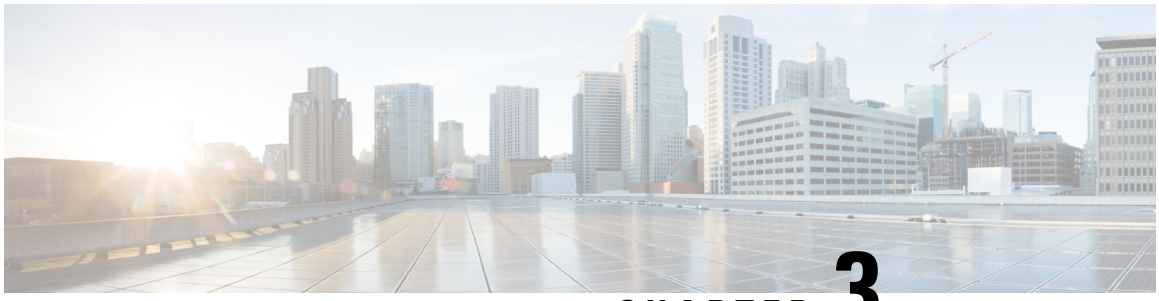
```
User: admin
Password: bell

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"
}
```

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.



CHAPTER 3

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.

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 7
- Local Users, on page 8
- Configuring LDAP Users, on page 11

- User Roles, on page 7
- Local Users, on page 8
- Configuring LDAP Users, on page 11

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 User Roles	Allowed HTTP Method
api-editor	GET, POST, PUT
api-viewer	GET

By default, the **admin** user is already mapped under these three groups.

Local Users

Note: Only Administrators can manage user and provide access.

Adding Local Users

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

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.

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.

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.

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.

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.

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.

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.

Step 1 This procedure changes the password from the **My Account** page:

a) 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.
b) In the **My Account** page, click **Update Password** to open **Update Password** window.
c) Enter current password, new password, and confirm the password.

The password must adhere to the password requirements.

d) Click **Update**.

A Success message appears that the user password is updated.

Step 2 This procedure changes the password in the Alert banner:

a) Click the link in the alert banner.

b) 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.

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

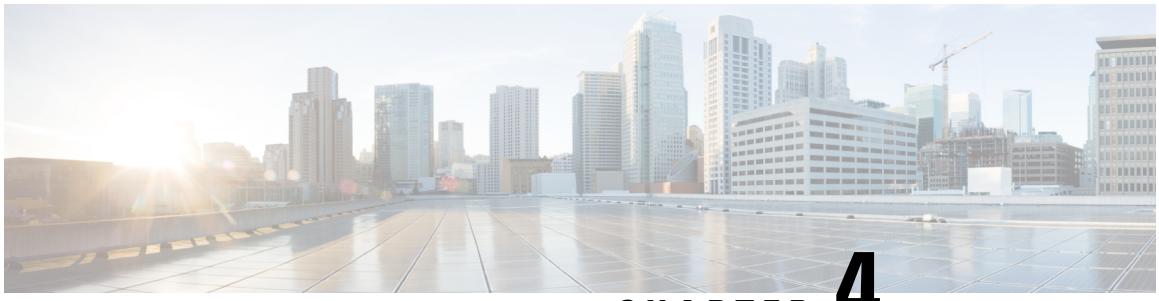
The **Authentication** page appears.

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.
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 **Save**.



CHAPTER 4

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.

Note: Only Administrators can perform the import and export 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

Importing Configuration Using Cisco Operations Hub

This procedure imports the Cisco Operations Hub configuration.

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.

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.

Importing Configuration Using RESTful API

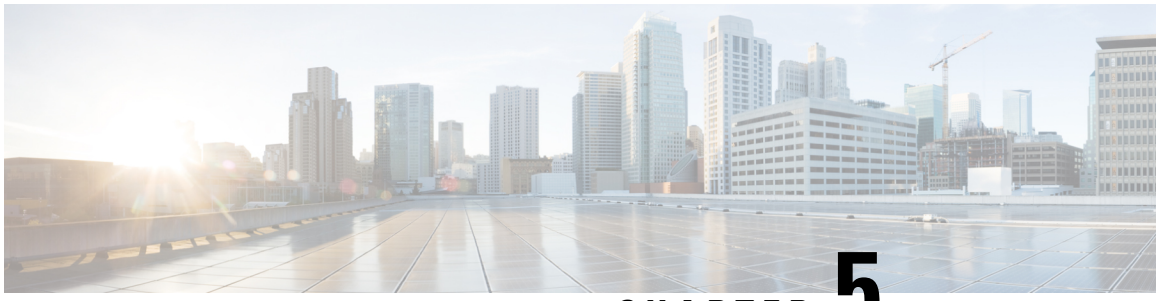
You can import the Cisco Operations Hub configuration and check the status of the import operation using the following APIs:

```
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
```



CHAPTER 5

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

Alert Management records all alerts that are generated in the Cisco Operations Hub cluster. The **Alert Management** dashboard display an alert summary and detailed information about those alerts.

Viewing Alert Summary

The **Alerts Overview** dashboard displays the alerts summary of total number of firing, pending, and warning alerts categorized based on severity. Cisco Operations Hub supports the following alert severity:

- Critical
- Major
- Minor

Use this task to view a summary of alerts.

1. Click the main menu at the top-left of the home page, and select **Dashboards** to view the **Dashboard Gallery** page.
2. Navigate to the **Operations Hub Dashboard** area and click **Alerts Overview** under the KPI section to open the **Alert Overview** page. You can view a total number of firing, pending, and warning alerts at a glance and a detailed list of these alerts based on severity.

Viewing Alert Information

You can view a list of firing alerts that are currently open and a list of resolved alerts.

This procedure enables you to view the lists of firing or resolved alerts.

Step 1 At the main menu, select **Dashboards** to view the **Dashboard Gallery** page.

Step 2 Navigate to the **Operations Hub Dashboard** area and click **Alert Management** under the **KPI** section to open the **Alert Management** page.

Step 3 In **KPI Alert Information** area, you can view the following lists:

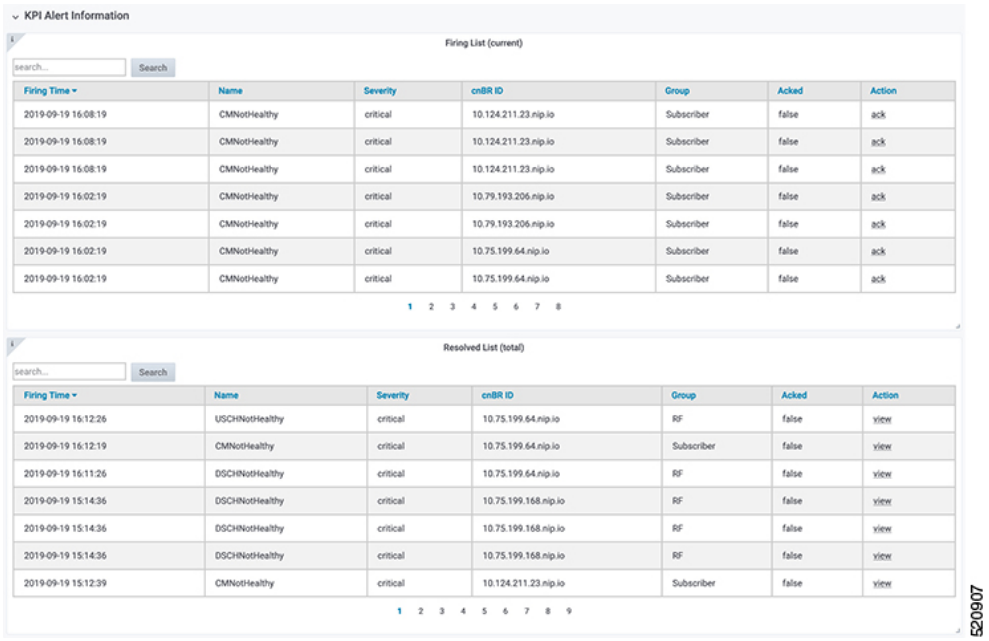
Table 3: Firing List (current)

Field	Description
Firing Time	Alert fired time
Name	Alert name.
Severity	Critical or warning
ID	Source where the alert is fired
Alert Group	Category of the KPI alert
Acknowledge status	Shows whether acknowledged or not
Action	Acknowledge or view an alert. Click the **View** link to display the **Alert Action** pane at the right side. The **Alert Action* pane displays the alert details such as status, severity, firing time, notify time with description. You can view details and acknowledge firing alerts.

Table 4: Resolved List (total)

Field	Description
Firing Time	Alert fired time
Resolved Time	Alert resolved time
Name	Alert name.
Severity	Critical or warning
Summary	Alert summary
Action	View an alert. Click the **View** link to display the **Alert Action** pane at the right side. The **Alert Action* pane displays the alert details such as status, severity, firing time, notify time with description. You can view details of each alert.

Figure 1: KPI Alert Information



Acknowledging Alerts

You can acknowledge the firing alerts. By default, every three hours, you are notified about the firing alerts by email. You can stop receiving the alert emails by setting the silence time, creator, and comments.

Configuring Alerts

KPIs

Key Performance Indicators (KPIs) provide insights into Operations Hub's overall system stability as well as components that are impacting system stability.

The Operations Hub supports the following KPI Alert Groups:

- Cluster
- OperationsHubInfra
- DbUpgrade
- InternalUserPasswordExpiry

Configuring Alerts Using SMTP

This procedure configures alerts globally using Simple Mail Transfer Protocol (SMTP).

SUMMARY STEPS

1. At the main menu, select to view the **Dashboard Gallery** page.
2. Navigate to the **Operations Hub Dashboard** area and click **Alert Management** under the KPI section to open the **Alert Management** page. You can configure global alerts in this page.
3. On the **Global Configuration** pane under the **KPI Alert Configuration** area, enter the **SMTP General Configuration** details.
4. Click **Config**.

DETAILED STEPS

Step 1 At the main menu, select to view the **Dashboard Gallery** page.

Step 2 Navigate to the **Operations Hub Dashboard** area and click **Alert Management** under the KPI section to open the **Alert Management** page. You can configure global alerts in this page.

Step 3 On the **Global Configuration** pane under the **KPI Alert Configuration** area, enter the **SMTP General Configuration** details.

Table 5: SMTP General Configuration Details

Field	Description
SMTP From	The default **SMTP From** header field.
SMTP Smarthost	The default SMTP smarthost used for sending emails, including the port number. The port number is 25 or 587 for SMTP over TLS (STARTTLS). Example: `smtp.example.org:587`

Field	Description
SMTP Hello	The default hostname to identify to the SMTP server.
SMTP TLS Require	The default SMTP TLS requirement (Default: false).

Step 4 Click **Config**.

Configuring Alert groups

This procedure enables or disables an alert group and add or delete email addresses of receivers for each alert group.

SUMMARY STEPS

1. At the main menu, select **Dashboards** to view the **Dashboard Gallery** page.
2. Navigate to the **Operations Hub Dashboard** area and click **Alert Management** under the KPI section to open the **Alert Management** page. You can configure global alerts in this page.
3. On the **Group Configuration** pane under the **KPI Alert Configuration** area, choose the alert group from the **Alert Group** drop-down list.
4. Click the radio button next to **Enabled** to enable the alert group.
5. Click **+** to add email addresses under the **Send To List** so the recipients receive notification when an alert is generated under that respective group.
6. Click **Config**.

DETAILED STEPS

Step 1 At the main menu, select **Dashboards** to view the **Dashboard Gallery** page.

Step 2 Navigate to the **Operations Hub Dashboard** area and click **Alert Management** under the KPI section to open the **Alert Management** page. You can configure global alerts in this page.

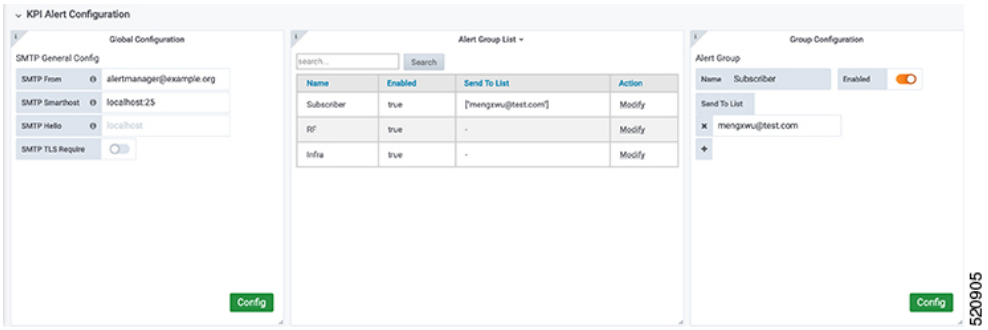
Step 3 On the **Group Configuration** pane under the **KPI Alert Configuration** area, choose the alert group from the **Alert Group** drop-down list.

Step 4 Click the radio button next to **Enabled** to enable the alert group.

Step 5 Click **+** to add email addresses under the **Send To List** so the recipients receive notification when an alert is generated under that respective group.

Step 6 Click **Config**.

Figure 2: KPI Alert Configuration



Monitoring Cluster Health

Table 6: Feature History

Feature Name	Release Information	Description
Cluster Health Monitoring	Cisco Operations Hub 22.2	Using the alert management functionality, you can view and monitor the cluster health. An alert is raised when there is an issue, and you can take necessary action based on the alert severity. Use the **Kubernetes Cluster Health dashboard** dashboard to view the cluster health information. .

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 to be 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.

Use the **Operations Hub Infra Alert Management API** to configure alert groups. You can access the **Operations Hub Infra Alert Management API** using the following steps:

1. Click the main menu at the top-left of the home page, and select **API Explorer**. The **API Explorer** page appears.
2. Click **KPI Alert Management** under **OPERATIONS HUB API**.

   The **Operations Hub Infra Authentication API** page appears.
3. Choose **GET /v1/cluster/health** under **Alert** to access the cluster health API.
4. Choose **GET /v1/alerts/groups** under **Alert Group** to access and configure the alert-groups. There are four alert-groups:
   a. `Cluster`
   b. `DbUpgrade`
   c. `InternalUserPasswordExpiry`
   d. `OperationsHubInfra`

Health alerts for a cluster can have the following severity:

- **Critical**—Indicates that the cluster has critical problems. Take immediate action before the service degrades further.
- **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.
- **Clear**—Indicates that the cluster has no alerts and everything is working as expected.

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's health severity is **Critical**.

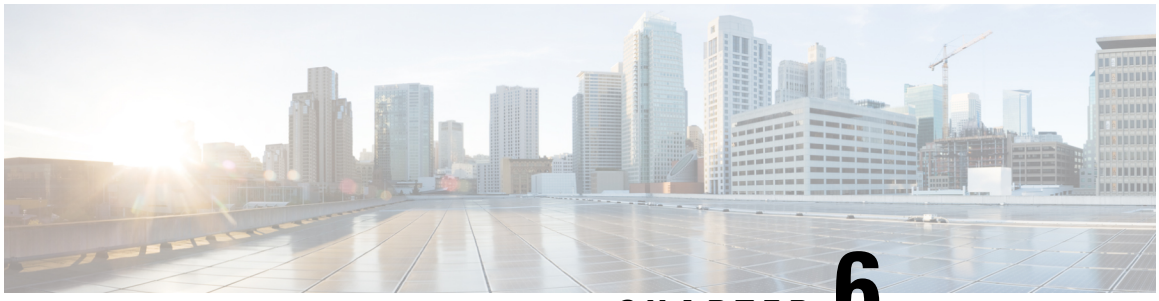
Similarly, if there are no critical alerts for the `InternalUserPasswordExpiry` alert-group, and all the pods are running in the cluster, then the cluster's health severity is **Clear**.

You can access the following dashboards to view the cluster health:

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

   The **Kubernetes Cluster Health** dashboard displays.
3. Click **Alerts Overview**.

   The **Alerts Overview** dashboard displays.



CHAPTER 6

Viewing and Managing System Logs

Operations Hub provides a tool for log aggregation and management leveraging the power of ElasticSearch-Logstash-Fluentd-Kibana (ELFK) 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 ELFK 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.

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 7: Audit Log

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

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.

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 8: Debug Log

Field	Description
Time	The time when the debug event was logged.
Source	The application (cnBR or Operations Hub) where the event happened.
ContainerName	The microservice in the application that generated the event.
LogLevel	The log level.
Message	The entire log content.

Viewing Logs Using Advanced Option

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

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

- **Dashboards**—The **Dashboard** page allows you us 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.

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.

TAC Debug Package

Feature History

Feature Name	Release Information	Description
TAC Debug Package	Cisco Operations Hub 22.2	You can create 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.

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

Note You can perform the TAC debug operations only using API and this feature is not supported in the Operations Hub GUI yet. For more information, see the Cisco Operations Hub and Smart PHY REST API Guide.