Overview

This chapter contains the following topics:

About Cisco IMC Supervisor

Cisco IMC Supervisor is a management system that allows you to manage rack-mount servers on a large scale. It allows you to create groups of rack-mount servers for monitoring and inventory purposes.

You can use Cisco IMC Supervisor to perform the following tasks:

- Logically grouping servers and viewing summary per group
- Collecting inventory for the managed servers
- Monitoring servers and groups
- Managing firmware including firmware download, upgrade, and activation
- Provide Northbound REST APIs to discover, monitor and manage servers and perform firmware upgrades programmatically.
- Managing standalone server actions including power control, LED control, log collection, KVM launch, and CIMC UI launch.
- Restricting access using Role Based Access Control (RBAC)
- Configuring email alerts
- Configuring server properties using policies and profiles
- Defining schedules to defer tasks such as firmware updates or server discovery

- Diagnosing server hardware issues using UCS Server Configuration Utility
- Cisco Smart Call Home provides proactive diagnostics, alerts, and remediation recommendations
- Managing Cisco UCS S3260 Dense Storage Rack Server
- Configuring the DNS server and other network settings through the Network Configuration policy
- Assigning physical drives to server through the Zoning policy
- Setting up multiple diagnostic images across different geographic locations
- Customizing email rules to include individual servers within a group

About Licenses

Cisco IMC Supervisor requires you to have the following valid licenses:

- A Cisco IMC Supervisor base license.
- A Cisco IMC Supervisor bulk endpoint enablement license that you install after the Cisco IMC Supervisor base license.
- A Cisco IMC Supervisor advanced license. You can add, edit, and delete policies and profiles with the base license but you cannot apply a policy or a profile to a server without the advanced license. An error occurs if this license is unavailable when you apply a policy.
- A default embedded Cisco IMC Supervisor evaluation license. The evaluation license is generated automatically when the end user installs Cisco IMC Supervisor and all the services start for the first time. It is applicable for 50 servers.

Important

- If you are using an evaluation license for Cisco IMC Supervisor, note that when this license expires (90 days from the date the license is generated), retrieving inventory and system health information, such as faults, will not work. You will not be able to refresh system data, or even add new accounts. At that point, you must install a perpetual license to use all features of Cisco IMC Supervisor.
- If the number of servers you have added during evaluation exceeds the number of server license purchased, inventory collection will go through fine for the servers already added during evaluation, but will prevent you from adding new servers. For example, if you have added about 100 servers during evaluation and you have purchased a 25 server license, once the evaluation license expires, you will be unable to add new servers. Also, you will be unable to perform configuration related operations without an advanced license.
- While discovering and importing servers, if the number of imported servers exceed the license utilization limit, Cisco IMC Supervisor imports servers only until the limit and displays an error for additional servers.
- Licenses for Cisco IMC Supervisor is based on the number of servers. Cisco UCS S3260 chassis is a 2-server node. As a result, in Cisco IMC Supervisor, the license utilization for this chassis is considered as 2 servers.

The process for obtaining and installing the licenses is the same. For obtaining a license, perform the following procedures:

1. Before you install Cisco IMC Supervisor, generate the Cisco IMC Supervisor license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in Fulfilling the Product Access Key, on page 3.
3. After you install Cisco IMC Supervisor, update the license as described in Updating the License.
4. After the license has been validated, you can start to use Cisco IMC Supervisor.

For various other licensing tasks you can perform, see Licensing Tasks.

Fulfilling the Product Access Key

Perform this procedure to register the Product Access Key (PAK) on the Cisco software license site.

Before you begin

You need the PAK number.

Procedure

Step 1 Navigate to the Cisco Software License website.

Step 2 If you are directed to the Product License Registration page, you can take the training or click **Continue to Product License Registration**.

Step 3 On the Product License Registration page, click **Get New Licenses from a PAK or Token**.

Step 4 In the **Enter a Single PAK or TOKEN to Fulfill** field, enter the PAK number.

Step 5 Click **Fulfill Single PAK/TOKEN**.

Step 6 Complete the additional fields in **License Information** to register your PAK:

Field	Description
Organization Name	The organization name.
Site Contact Name	The site contact name.
Street Address	The street address of the organization.
City/Town	The city or town.
State/Province	The state or province.
Zip/Postal Code	The zip code or postal code.
Country	The country name.

Step 7 Click **Issue Key**.

The features for your license appear, and an email with the Digital License Agreement and a zipped license file is sent to the email address you provided.

Common Terms in the Cisco IMC Supervisor User Interface

Rack Groups

A Rack Group is a logical grouping of physical rack-mount servers. A Rack Group represents a single converged infrastructure stack of C-Series and/or E-Series servers. You may add, modify, and delete Rack Groups as required.

Note When you login for the first time, Cisco IMC Supervisor provides a rack group titled **Default Group**. You can add rack accounts to this rack group, or you can create new rack groups and add rack accounts to them. But, you cannot delete this default rack group account.

Rack Account

Rack Account is a standalone rack-mount server added to Cisco IMC Supervisor. You can add multiple rack-mount servers in Cisco IMC Supervisor. After you add a rack-mount server to Cisco IMC Supervisor as an account, Cisco IMC Supervisor provides you with complete visibility into the rack-mount server configuration. In addition, you can use Cisco IMC Supervisor to monitor and manage the C-Series and E-Series rack-mount servers. Rack accounts should be added to the rack groups either to the default group or to a group you have created.

Policies

Policies are a primary mechanism for defining configuration of various attributes on Cisco IMC. Policies help ensure consistency and repeatability of configurations across servers. Defining and using a comprehensive set of policies enables greater consistency, control, predictability, and automation as similar configurations are applied across many servers.

Profiles

Multiple policies combined together form a hardware profile. You can apply configuration details of a rack hardware profile for example, to multiple rack-mount servers. You can associate this hardware profile to specific rack-mount servers. This helps ensure consistency and repeatability of configurations across servers. Defining and using a profile enables greater consistency, control, predictability, and automation as similar configurations are applied across many servers.

Cisco IMC Supervisor User Interface

Cisco IMC Supervisor introduces a new user interface for the administrative portal. This section introduces you to some of the key features of the user interface.

Change in Navigation

In earlier releases, you could access screens using the main menu bar. Starting with this release, all navigation options are now available from a side bar, and not from the horizontal main menu bar. As a result, the main menu bar is no longer visible in the user interface. You can use your mouse or the cursor to hover over an option on the side navigation bar, and then click on any of the menu options.

Absence of User Interface Labels

The user interface no longer includes labels for actions such as Add, Edit, Delete, Export, and Filter. These actions are represented only with icons. If you use your mouse or cursor to hover over the icon, the label will display the action you can perform using that icon.

Using Dashboard to Access Detailed Reports

If you have enabled the **Dashboard**, then it is the first screen that you will see when you login to Cisco IMC Supervisor. Typically, you can use this dashboard to add important or frequently accessed report widgets. Now, you can click on any of the reports that are displayed on the **Dashboard**, and immediately access the screen in the user interface where more detailed information is displayed. See Enabling Dashboard View. In addition, you can create multiple dashboards and delete them when you no longer need them. See Creating Additional Dashboards and Deleting a Dashboard.

Enhanced Capabilities with Tabular Reports

Following are some of the enhanced capabilities with tabular reports available in the user interface:

- Right-click to view additional options

  After you select a row, if you right-click on your mouse, a list of options relevant to the row you selected are displayed.

- Filter and Search

  You can use a **Filter** option or a **Search** option with tabular reports in the Cisco IMC Supervisor interface. On any page with a tabular report, you can use the **Filter** option that allows you to narrow down the tabular report results with a specific criteria. You can use this **Filter** option on tabular reports that do not span across pages. For tabular reports that do span across multiple pages, you can use the **Search** option to narrow down your search result.

- Adding tabular reports to the **Favorites** menu

  You can add any tabular report displayed in the user interface as a Favorite. By adding a report as a favorite, you can access this report from the **Favorites** menu.

- Resizing of columns

  You can resize all the columns that are displayed in the tabular report, including the last column. After you expand the columns, you can use the horizontal scroll bar to view the complete screen.

- Informational message displayed in the absence of data

If there is no information to be displayed in a report, the following message is displayed.

No Data

Removing and Restoring Tabs

On any screen that has multiple tabs available, you can choose the number of tabs that you would like to see on that screen. If you close a tab on a screen, it will no longer be displayed in the row of tabs displayed in the user interface. If you would like to bring it back on the screen, then click the arrow facing downwards that is visible on the far right of the screen. It displays a drop-down list of tabs that are available but hidden from view. Choose the tab you would like to restore.

Note You can remove and restore tabs on a screen only when there are a minimum of two tabs. This functionality is not available when there is only one tab displayed on a screen in the interface.

Enhancements to Reporting Capabilities

Following are some of the enhanced reporting capabilities available in the user interface:

- Introduction of pie charts and bar graphs

  Each individual pie chart or bar graph can be exported out of the system in PDF, CSV or XLS format, or can be added to the **Dashboard**.

- Availability of **More Reports** option

  Using the **More Reports** option, you can now generate reports Faults, Server Health, Chassis Health, Firmware Versions, Server Models, Power State, and Server Connection Status.

Landing Page

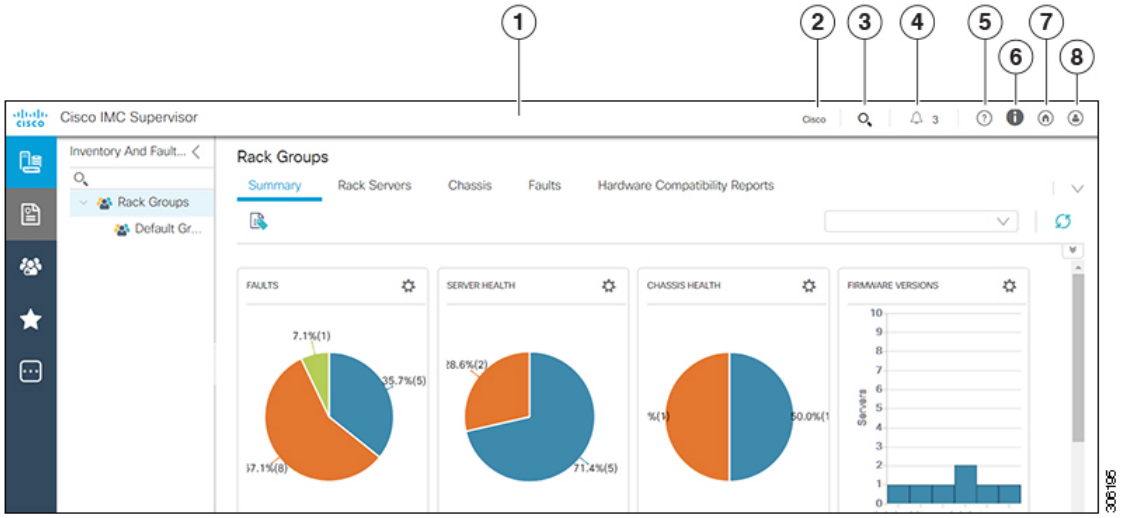
The landing page opens when you log in to the Cisco IMC Supervisor administrator portal. The elements that you see on the landing page depend upon how you have configured the display. By default, the Converged View is displayed when you login to the portal.

The following are the available elements for your landing page:

- Header—Displays across the top of the screen.
- Navigation menu—The main navigation bar is no longer on the top of the screen. It is now available as a vertical menu on the left-side of the screen.

Note The menu does not have a scroll bar. The menu only displays the number of options that fit in the space available. Some options may not appear if you minimize your screen or zoom in. You can click **Site Map** to view all available options.

Figure 1: New User Interface



Number	Name	Description
1	Header	Contains frequently accessed elements, including the menu. The header is always visible.
2	Link	Provides a link to the Cisco website from where you can access information on using the software.
3	Search icon	Allows you to search for and navigate directly to a specific report in the portal.
4	Diagnostic System Messages icon	Displays the number of diagnostic system messages that have been logged. Clicking on this link takes you to the Diagnostic System Messages screen from where you can view detailed information.
5	Help icon	Links to the online help system for the administrator portal.
6	About icon	Displays information about the software, and the version that is currently installed.
7	Home icon	Returns you to the landing page from any location in the user interface.
8	User icon	Allows you to edit your profile, enable or disable the dashboard, access the classic view of the user interface, and log out.

Common User Interface Options

The following table describes the options that are available on all pages of the application user interface. These options perform the same task on every page.

Icon	Label	Description
	**Refresh**	Refreshes the reported data on the page.
	**Favorite**	Adds a page to the **Favorites** menu. You can use this option to view frequently accessed pages more quickly.
	**Add**	Brings up the **Add** dialog box, from which you can add a new resource.
	**Edit**	Brings up the **Edit** dialog box, from which you can edit a resource.
	**Customize Table**	Brings up the **Customize Report Table** dialog box, in which you choose what columns you want to include on the screen.
	**Export Report**	Brings up the **Export Report** dialog box, from which you download a report to your system. You can generate a report in one of the following formats: • PDF • CSV • XLS
	**Expand**	Expands all the folders that are displayed on the page.
	**Collapse**	Collapses all the folders that are displayed on the page.
	**Add Advanced Filter**	Provides extra filtering parameters on the page.
	**Search Field**	Accepts a keyword to filter for specific records on the page.

Setting Up a Secure Connection to the Cisco IMC Supervisor User Interface

Perform this procedure to set up a secure connection to the system.

Procedure

Step 1 Update the value for the redirectPort parameter to **443** in the `server.xml` file.

This file is located in the `/opt/infra/web_cloudmgr/apache-tomcat/conf/` directory.

```
<Connector port="80" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="443"
maxHttpHeaderSize="65536"/>
```

Step 2 Uncomment the following lines in the `web.xml` file:

```
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

You can add these lines anywhere in the file.

Step 3 Launch the user interface and login to the system.

Setting up Non-Secure Connection to the Cisco IMC Supervisor User Interface

By default, the Cisco IMC Supervisor user interface launches in the secure mode. If you want to bypass the secure mode, and launch the user interface in a non-secure mode (HTTP), you must follow this procedure.

Procedure

Step 1 Log in as root.

Step 2 Make the following changes in the `/opt/infra/web_cloudmgr/apache-tomcat/conf/server.xml` file:

a) Comment out the existing port 8080 Connector tag

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
redirectPort="443" maxHttpHeaderSize="65536"
URIEncoding = "UTF-8"/>
-->
```

b) Add the following as a new port 8080 Connector tag:

```
<Connector port="8080" protocol="HTTP/1.1"
maxThreads="150" minSpareThreads="4"
connectionTimeout="20000"
URIEncoding = "UTF-8" />
```

Step 3 Comment the <security-constraint> tag in the `/opt/infra/web_cloudmgr/apache-tomcat/webapps/app/WEB-INF/web.xml` file.

```
<!--
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
-->
```

Step 4 Restart the services.

Step 5 Launch the user interface and log in to the system.

You can now log into the system in the non-secure mode using the following URL format:

http://<IP-Address>:8080 or http://<IP-Address>

You can launch the user interface in both, secure and non-secure modes.