

Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.4

First Published: 2024-05-07

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **New and Changed Information for this Release** 1

New and Changed Information for this Release 1

CHAPTER 2 **Overview** 3

About Cisco IMC Supervisor 3

About Licenses 4

Fulfilling the Product Access Key 5

Common Terms in the Cisco IMC Supervisor User Interface 6

Rack Groups 6

Rack Account 6

Policies 6

Profiles 6

Cisco IMC Supervisor User Interface 7

Landing Page 8

Common User Interface Options 10

Setting Up a Secure Connection to the Cisco IMC Supervisor User Interface 11

Setting up Non-Secure Connection to the Cisco IMC Supervisor User Interface 11

CHAPTER 3 **Getting Started** 13

Overview 13

Launching Cisco IMC Supervisor 14

Licensing Tasks 15

Updating the License 15

Replacing a License 16

Viewing Deactivated Licenses 16

Migrating a License 17

Running License Audit 17
Managing User Access Profiles 18
Multi-Role Access Profiles 18
Creating a User Access Profile 18
Logging in to a Profile 19
Default Profile 19
Changing a Default Profile 19
Authentication and LDAP Integration 20
Configuring Authentication Preferences 20
Configuring LDAP 20
LDAP Integration 20
LDAP Integration Rules and Limitations 21
Adding LDAP Configurations 23
Configuring LDAP Servers 24
Viewing LDAP Server Summary Information 27
Testing LDAP Server Connectivity 28
Searching BaseDN 28
Requesting Manual LDAP Sync 29
Executing LDAP Synchronization and Viewing LDAP Synchronized Results 29
Modifying LDAP Server Details 30
Viewing Group Membership Information 31
Deleting LDAP Server Information 32
Configuring SFTP User Password 32
Configuring Mail Setup 33
Configuring Cisco.com User Credentials and Proxy Configuration 33
Configuring Cisco.com User 34
Configuring Proxy Settings 34
Setting Up CMDB Integration 35
Branding 36
Adding New Login Branding Page 36
Configuring User Interface Settings 37

CHAPTER 4 **Managing Users, User Roles and Groups** 39
Overview 39

Creating a User Account 40
Viewing Online Users 41
Reviewing Recent Login History of Users 42
Configuring Session Limits for Users 42
Adding a User Role 43
Branding a User Group 44

CHAPTER 5 **Managing Server Discovery, Rack Groups, and Rack Accounts** 45
Overview 45
Discovering and Importing a Server 46
Configuring Auto Discovery Profile 46
Performing Auto Discovery 48
Importing a Server 49
Setting Properties for Discovered Devices 50
Adding a Rack Group 51
Adding a Rack Account 51
Collecting Inventory for Rack Accounts or Rack Groups 53
Assigning Rack Accounts to a Rack Group 54
Testing an Account Connection 54

CHAPTER 6 **Viewing Inventory Data and Faults** 57
Viewing Rack-Mount Server Details 57
Viewing Smart Information for SSD 60
Overview of Controller Drive Security 61
Viewing Controller Drive Security Details 61
Viewing Fault Details for a Rack Mount Server 63
Summary Reports for a Rack Group 63
Adding Email Alert Rules for Server Faults 64

CHAPTER 7 **Managing Rack Servers** 67
Viewing Rack-Mount Server Details 67
Viewing Fault Details for a Rack Mount Server 70
Powering On and Off a Rack Mount Server 71
Tagging Assets for a Rack Mount Server 72

Shutting Down a Rack Mount Server 72
Performing a Hard Reset on Rack Mount Server 73
Performing a Power Cycle on a Rack Mount Server 74
Launching KVM Console for a Rack-Mount Server 74
Launching GUI for a Rack Mount Server 75
Setting Locator LED for a Rack Mount Server 76
Setting Label for a Rack Mount Server 77
Managing Tags for a Rack-Mount Server 78
Adding Tags for a Rack-Mount Server 80
Exporting Technical Support Data to a Remote Server 81
Clearing SEL 82
Managing System Tasks 83
Running a Task 85

CHAPTER 8 **Managing Policies and Profiles** 87
Credential Policies 87
Creating a Credential Policy 87
Hardware Policies 88
Creating Hardware Policies 89
BIOS Policy 91
Disk Group Policy 92
FlexFlash Policy 92
IPMI Over LAN Policy 96
LDAP Policy 97
Legacy Boot Order Policy 98
Network Configuration Policy 99
Network Security Policy 102
NTP Policy 103
Password Expiration Policy 104
Precision Boot Order Policy 105
Power Restore Policy 106
RAID Policy 107
Serial Over LAN Policy 109
SNMP Policy 110

SSH Policy 111
User Policy 112
Virtual KVM Policy 113
VIC Adapter Policy 114
vMedia Policy 115
Zoning Policy 116
Creating a Policy from an Existing Configuration 117
Applying a Hardware Policy 118
General Tasks Under Hardware Policies 119
Hardware Profiles 120
Creating a Hardware Profile 121
Creating a Profile from an Existing Configuration 121
Applying a Hardware Profile 123
General Tasks Under Hardware Profiles 123
Tag Library 124
Creating a Tag Library 124
REST API and Orchestration 126

CHAPTER 9 **Managing Cisco UCS Hardware Compatibility Report** 127
Overview 127
Tagging OS Vendor and Version 128
Creating Hardware Compatibility Reports 128
Synchronizing Hardware Compatibility Reports 129

CHAPTER 10 **Firmware Profiles** 131
Firmware Management Menu 131
Adding Images to a Local Server 131
Adding Images to a Local Cisco UCS Director System 133
Uploading Images from a Local File System 135
Adding Images from a Network Server 136
Upgrading Firmware 137
Host Image Mapping 139
Adding a Network Host Image Mapping Profile 139
Creating an Upload Profile for Host Image Mapping 142

Applying a Host Image Profile 144
Downloading a Firmware Image 144
Running a Host Image Upgrade Manually 145
Deleting a Downloaded Image 146
Mapping and Unmapping a Host Image 146
Viewing Status Details of a Host Image Profile 147
Deleting a Host Image Mapping Profile 148
Firmware Upgrades From SD Cards 148
Downloading Firmware Image to an SD Card 148
Running Firmware Upgrade from an SD Card 149
Deleting Image Download Messages 150

CHAPTER 11 **Updating Cisco IMC Supervisor Patches** 151
Overview of Updating Cisco IMC Supervisor Patches 151
Checking for Cisco IMC Supervisor Patch Updates 151

CHAPTER 12 **Managing Schedules** 153
Overview of Managing Schedules 153
Creating Schedules 153

CHAPTER 13 **Running Server Diagnostics** 155
Overview of Server Diagnostics 155
Configuring Server Configuration Utility Image Location 156
Running Diagnostics 156

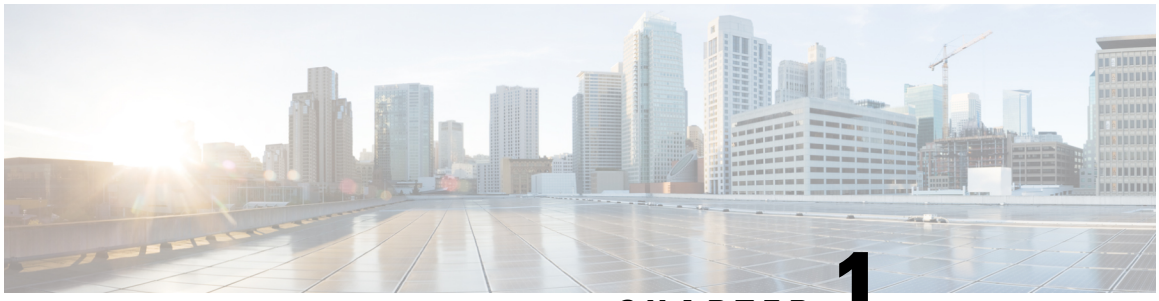
CHAPTER 14 **Smart Call Home for Cisco IMC Supervisor** 159
Overview of Smart Call Home 159
Configuring Smart Call Home 159
Fault Codes 160

CHAPTER 15 **Managing Cisco UCS S3260 Dense Storage Rack Server** 163
About Cisco UCS S3260 Dense Storage Rack Server 163
Cisco UCS S3260 Dense Storage Rack Server Architectural Overview 164

Cisco IMC Supervisor with Cisco UCS S3260 Dense Storage Rack Server 165
Adding a Rack Account 165
Managing Cisco UCS S3260 Rack Server 166
Restarting Chassis Management Controller 166
Tagging Assets for Cisco UCS S3260 Rack Server 166
Setting Front Locator LED for Cisco UCS S3260 Rack Server 167
Managing Tags for Cisco UCS S3260 Rack Server 167
Adding Tags for Cisco UCS S3260 Rack Server 167
Policies and Profiles 168
Upgrading Firmware 169
Viewing Cisco UCS S3260 Dense Storage Rack Server Details 169

CHAPTER 16 **Viewing Support Information** 173
Support Information 173
Viewing Support Information 173

CHAPTER 17 **Frequently Performed Tasks and Procedures** 175
Frequently Performed Procedures 175
Miscellaneous Procedures 175
Enabling Dashboard View 175
Creating Additional Dashboards 176
Enabling Dashboard Auto Refresh 176
Adding Summary Reports to Dashboard 177
Deleting a Dashboard 177
Adding a Menu or Tab to Favorites 178
Favorites 178
Customizing Report Table View 178
Filtering Reports 179
Exporting a Report 179
Viewing System Information 180
Site Map 180



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following section:

- New and Changed Information for this Release, on page 1

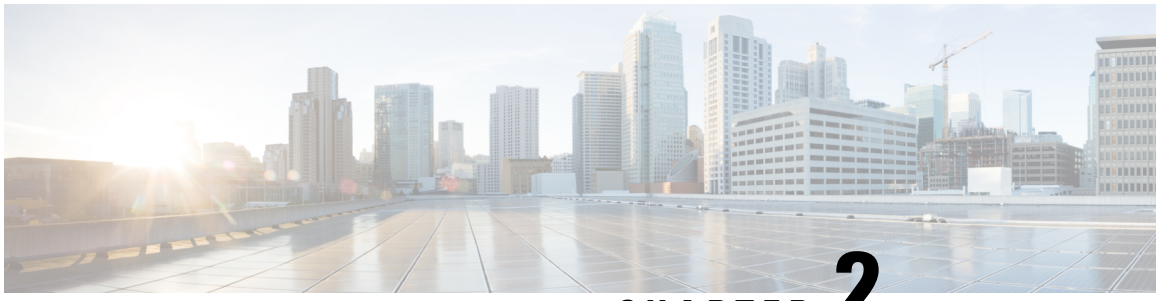
New and Changed Information for this Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco IMC Supervisor, Release 2.4(0.0)

Feature	Description	Where Documented
Support for Local Firmware download for a Rack Mount server. Support for downloading new version of patches for Cisco IMC Supervisor	Starting with Cisco IMC Supervisor version 2.4(0.0), you must activate the device every hour once using **Activate Device** under the **Images – Local** screen and the **Update IMCS** page to download the Rack Mount server firmware to the local appliance and to trigger download for the new version of Cisco IMC Supervisor patches.	Adding Images to a Local Server, on page 131 Checking for Cisco IMC Supervisor Patch Updates, on page 151

New and Changed Information for this Release



CHAPTER 2

Overview

This chapter contains the following topics:

- About Cisco IMC Supervisor, on page 3
- About Licenses, on page 4
- Fulfilling the Product Access Key, on page 5
- Common Terms in the Cisco IMC Supervisor User Interface, on page 6
- Cisco IMC Supervisor User Interface, on page 7
- Landing Page, on page 8
- Common User Interface Options, on page 10
- Setting Up a Secure Connection to the Cisco IMC Supervisor User Interface, on page 11
- Setting up Non-Secure Connection to the Cisco IMC Supervisor User Interface, on page 11

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 5.
3. After you install Cisco IMC Supervisor, update the license as described in Updating the License, on page 15.
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, on page 15.

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, on page 175. In addition, you can create multiple dashboards and delete them when you no longer need them. See Creating Additional Dashboards, on page 176 and Deleting a Dashboard, on page 177.

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.

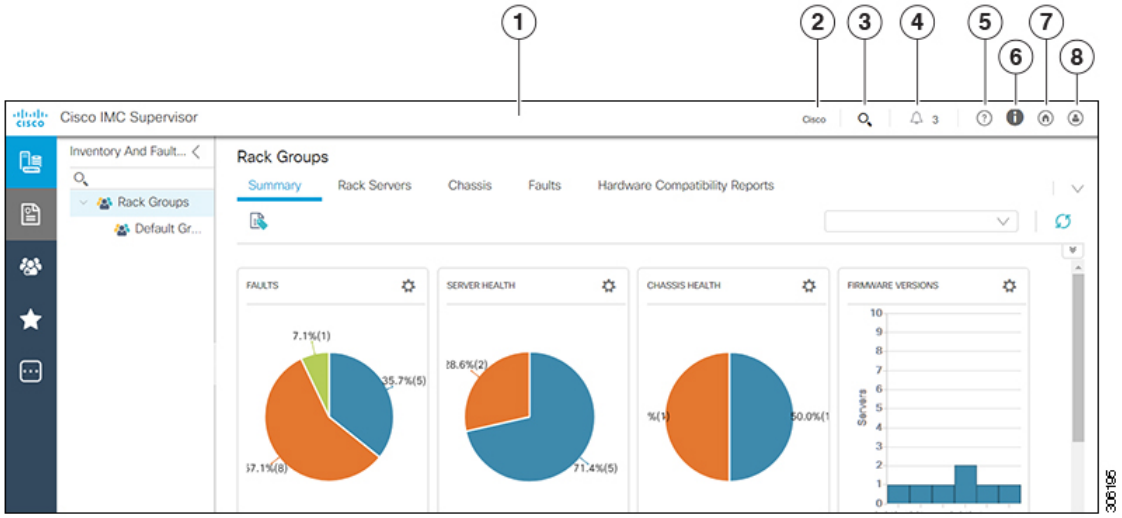
The following are the available elements for your landing page:

- 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>
-->
```

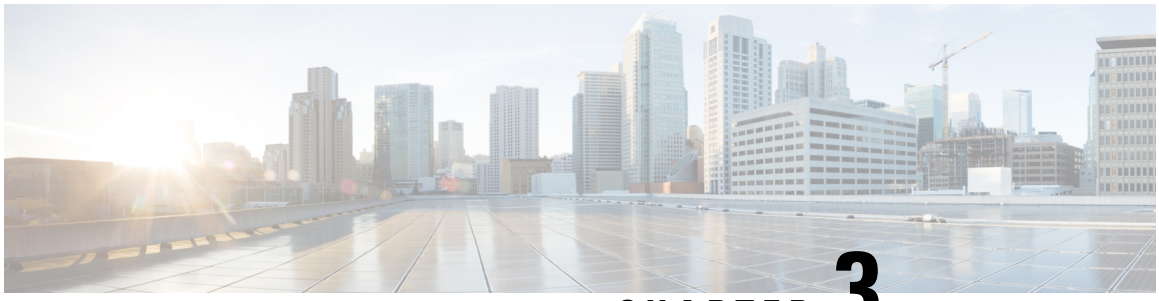
Step 4 Restart the services.

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.



CHAPTER 3

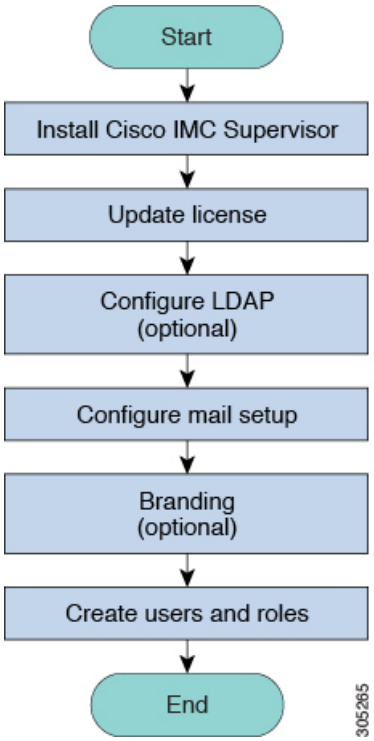
Getting Started

This chapter contains the following topics:

- Overview, on page 13
- Launching Cisco IMC Supervisor, on page 14
- Licensing Tasks, on page 15
- Managing User Access Profiles, on page 18
- Authentication and LDAP Integration, on page 20
- Configuring LDAP, on page 20
- Configuring SFTP User Password, on page 32
- Configuring Mail Setup, on page 33
- Configuring Cisco.com User Credentials and Proxy Configuration, on page 33
- Setting Up CMDB Integration, on page 35
- Branding, on page 36
- Configuring User Interface Settings, on page 37

Overview

The following figure illustrates the workflow to setup your environment using Cisco IMC Supervisor:



Launching Cisco IMC Supervisor

Cisco IMC Supervisor should have been successfully installed, with a correctly configured IP address.

Before you begin

- Verify if Cisco IMC Supervisor is installed successfully.
- Ensure you have the IP address configured during the Cisco IMC Supervisor installation.

Procedure

Type the Cisco IMC Supervisor IP address in any browser URL and log in with the following credentials:

- User Name - **admin**
- Password - **admin**

Once you have logged in, Cisco IMC Supervisor will launch. You will see the default dashboard view of Cisco IMC Supervisor.

Licensing Tasks

You can use the **License** menu to view the license details and the usage of resources. The following licensing procedures are available from **Administration** > **License** menu.

Tab	Description
License Keys	This tab displays the details of the license used in Cisco IMC Supervisor. You can also use this tab to update, replace and migrate the license. You can update the license when a new version of Cisco IMC Supervisor is available.
License Utilization	This tab shows the licenses in use and details about each license, including license limit, available quantity, status, and remarks. License audits can also be run from this page. **Note** 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.
Resource Usage Data	This tabs displays the details of the various resources used.
Deactivated Licenses	This tab displays a list of deactivated licenses.

Updating the License

You must perform the following procedure to update the license before you start using Cisco IMC Supervisor. For the list of valid licenses, see About Licenses, on page 4. You must generate a license key, claim and register the Product Access Key. After installing Cisco IMC Supervisor, the license is validated and you can start using Cisco IMC Supervisor.

Before you begin

If you received a zipped license file by email, extract and save the **.lic** file to your local machine.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, choose **License Keys**.

Step 3 On the **License Keys** page, click **Update License**.

Step 4 On the **Update License** screen, do one of the following:

- To upload a **.lic** file, click **Browse**, navigate to and select the **.lic** file, then click **Upload**.
- For a license key, check the **Enter License Text** check box then copy and paste the license key only into the **License Text** field. The license key is typically at the top of the file, after Key ->.

You can also copy and paste the full text of a license file into the **License Text** field.

Step 5 Click **Submit**.
The license file is processed, and a message appears confirming the successful update.

Replacing a License

You can use this procedure to replace a license in the system. This action will deactivate all other existing licenses on the systems.

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, choose **License Keys**.
Step 3 Choose **Replace License**.
Step 4 In the **Upload License** field, you can either drag and drop a PAK file or click **Select a File** to browse and select a file.
Step 5 (Optional) Check **Enter License Text** to copy and paste the license text.
Step 6 Click **Submit**.

All existing licenses are replaced with the new license.

Viewing Deactivated Licenses

You can view the list of deactivated licenses from the user interface. You can view the following information on deactivated licenses:

- PAK file name
- File ID
- License Entry
- Licence Value
- Expiry Date
- Deactivated Time
- Name of user who deactivated the license

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, choose **Deactivated Licenses**.

Step 3 Review the information displayed for all the deactivated licenses.

Migrating a License

Cisco IMC Supervisor allows you to migrate a license using the graphical user interface. For example, you can migrate from a perpetual license to a subscription license.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, choose **License Keys**.

Step 3 On the **License Keys** page, click **Migrate License**.

Step 4 In the **Upload License** field, you can either drag and drop a PAK file or click **Select a File** to browse and select a file.

Step 5 (Optional) Check **Enter License Text** to copy and paste the license text.

Step 6 Click **Submit**.

Running License Audit

Perform this procedure when you want run license audits.

Before you begin

The license should be updated. To upgrade the license, refer Updating the License, on page 15.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Utilization**.

Step 3 From the **More Actions** drop-down list, choose **Run License Audit**.

Step 4 On the **Run License Audit** screen, click **Submit**.
This process takes some time to complete.

Managing User Access Profiles

Multi-Role Access Profiles

A user can be assigned to more than one role, which is reflected in the system as a user access profile. For example, a user might log into Cisco IMC Supervisor as a group administrator and as an all-policy administrator, if both types of access are appropriate. Access profiles also define the resources that can be viewed by a user.

When LDAP users are integrated with Cisco IMC Supervisor, if a user belongs to more than one group, then the system creates a profile for each group. But by default, the domain users profile is added for LDAP users.



Note The **Manage Profiles** feature enables you to add, log into, edit, or delete a user access profile.

Creating a User Access Profile

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Choose a user from the list.

Step 4 From the **More Actions** drop-down list, choose **Manage Profiles**.

Step 5 On the **Manage Profile** page, click **Add +**.

Step 6 On the **Add Entry to Access Profiles** page, complete the following fields:

Field Name	Description
Name field	The profile name.
Description field	The description of the profile.
Type drop-down list	Choose the user role type.
Customer Organizations drop-down list	Choose the organization to which this user profile applies.
Show Resources From All Other Groups the User Has Access check box	Select this checkbox to specify that the user can view resources from all other groups that they have access to or are a part of.
Shared Groups field	Click **Select** to choose the groups to which the user profile applies. The user will be able to access all the resources associated with the selected groups.

Field Name	Description
Default Profile check box	Check the check box if this is the default user access profile. Uncheck the check box if it is not the default.

Step 7 Click **Submit**.

What to do next

Create additional user access profiles as needed.

Logging in to a Profile

As a user in the system, if you have multiple profiles for your account, then you can log in to the system with a specific profile.

Procedure

Step 1 On the **Cisco IMC Supervisor login** page, enter your username in the **Username** field, in the format Username: Access Profile Name.

For example, Alex: GrpAdmin

Step 2 In the **Password** field, enter your password.

Step 3 Click **Login**.

Default Profile

The default profile is the first profile that you created in the system. You can change the default to another profile. Using the new default profile, you log in by entering the username and password.

Changing a Default Profile

Procedure

Step 1 In the user interface, click the username displayed on the top right corner.

The username is displayed to the left of the **logout** option.

Step 2 On the **User Information** page, choose the **Access Profiles** tab.

Step 3 Choose a user profile, and click **Set as Default Profile**.

Note

A profile can also be set as default while it is being added, or being edited.

Authentication and LDAP Integration

You can configure an authentication preference with a fallback choice for LDAP. You can also configure a preference with no fallback for Verisign Identity Protection (VIP) authentication.

Name	Description
Local First, fallback to LDAP	Authentication is done first at the local server (Cisco IMC Supervisor). If the user is unavailable at the local server, the LDAP server is checked.

Configuring Authentication Preferences

Perform this procedure when you want to change the login authentication type.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Choose **Authentication Preferences**.

Step 3 From the **Authentication Preferences** drop-down list, you can choose one of the following options:

- **Local First, fallback to LDAP**

  If you select this option, then you must configure LDAP servers. For more information, see Configuring LDAP Servers, on page 24.

Step 4 Click **Save**.

Configuring LDAP

Configuring LDAP in Cisco IMC Supervisor involves adding LDAP configurations and configuring LDAP servers. You can also test the LDAP connectivity and view LDAP summary information. The following sections explain how to perform these procedures.

LDAP Integration

You can use LDAP integration to synchronize the LDAP server's users with Cisco IMC Supervisor. LDAP authentication enables synchronized users to authenticate with the LDAP server. You can synchronize LDAP users automatically or manually. While adding an LDAP account, you can specify a frequency at which the

LDAP account is synchronized automatically with Cisco IMC Supervisor. Optionally, you can manually trigger the LDAP synchronization by using the **LDAPSyncTask** system task.

When new organizational units (OU) are added in the LDAP directory, and a synchronization process is run, either manually or automatically, the recently added LDAP users are displayed in Cisco IMC Supervisor.

In addition to running a system task, Cisco IMC Supervisor also provides an additional option for you tosynchronize the LDAP directory with the system:

Cleanup LDAP Users system task—This system task determines if the synchronized users in the system are deleted from the LDAP directories or not. If there are user records that have been deleted from the LDAP directories, then after this system task is run, these users are marked as disabled in the system. As an administrator, you can unassign resources of these inactive users. By default, this task is in the enabled mode. It is only after you restart the services twice that this system task is set to the disabled mode.

You cannot choose users that exist locally or are synchronized externally in Cisco IMC Supervisor.



Important Users that do not belong to a group or a domain user's group display in LDAP as **Users with No Group**. These users are added under the domain user's group in Cisco IMC Supervisor.

You can add LDAP users that are in different LDAP server accounts but have the same name. The domain name is appended to the login user name to differentiate the multiple user records. For example, abc@vxedomain.com. This rule applies to user groups as well.

When a single LDAP account is added, and a user logs in by specifying only the user name, Cisco IMC Supervisor first determines if the user is a local user or is an LDAP user. If the user is identified as a local user and as an external LDAP user, then at the login stage, if the user name matches the local user name, then the local user is authenticated into Cisco IMC Supervisor. Alternatively, if the user name matches that of the external user, then the LDAP user is authenticated into Cisco IMC Supervisor.

LDAP Integration Rules and Limitations



Note Recommended version for security PSB is TLS: 1.2 and above.

If you do not want to upgrade and break the existing functionality, you need to update the `service.properties` manually and configure to the older version.The path for the `service.properties` file is **/resources/properties/service.properties**.The supported versions of **ldap.ssl.socket.protocols** for Cisco IMC Supervisor, Release 2.3 are TLSv1.2 and TLSv1.3.

Group Synchronization Rules

- If a chosen LDAP group already exists in Cisco IMC Supervisor and the source is type **Local**, the group is ignored during synchronization.
- If a chosen LDAP group already exists in Cisco IMC Supervisor and the group source is type **External**, the group's description and email attributes are updated in Cisco IMC Supervisor.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a group filter, all users that belong to the specified group are added to the system. In addition, the following actions are also performed:

- If the specified group includes sub-groups, then the group, the sub-groups and the users in those sub-groups are added to the system (only applicable when you manually synchronize the LDAP directory).
- If the user is part of multiple groups, and the other groups do not match the group specified as the group filter, then those additional groups are not added to the system.

- A user can be part of multiple user groups. However, the group that is mentioned first in the list of groups that the user is part of is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**.



Note You can view information on all the groups that a user is part of only after the **LDAPSyncTask** system task is run.

- When an LDAP group is synchronized, all users that are in the group are first added to the system. Also, if users in the specified LDAP group are associated with other groups that are in the same OU or in a different OU, then those groups are also retrieved and added to the system.
- The LDAP synchronization process will retrieve the specified LDAP groups for the system, along with nested groups, if any.
- Prior to this release, a user was part of only one group. After an upgrade to the current release, and only after the **LDAPSyncTask** system task is run, the **Manage Profiles** dialog box displays the other groups that the user is part of. This is applicable only when the other groups match the group filters that you specified while configuring the LDAP server.

User Synchronization Rules

- LDAP users that have special characters in their names are now added to Cisco IMC Supervisor.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a user filter, all the users that match the filter you specified, and the groups that they belong to, are retrieved for the system.
- Cisco IMC Supervisor now displays the User Principal Name (UPN) for each user that is added into the system. This is applicable for users that have been added into the system in prior releases. Users can log in to the system using their login name or their user principal name. Logging in using the user principal name along with the profile name is not supported.
- If a chosen LDAP user already exists in Cisco IMC Supervisor and the source is type **Local**, the user is ignored during synchronization.
- If a chosen LDAP user already exists in Cisco IMC Supervisor and the source type is **External**, the user's name, description, email, and other attributes are updated for use.
- If a user account is created in two different LDAP directories, then the user details of the LDAP directory that was synchronized first is displayed. The user details from the other LDAP directory is not displayed.
- After LDAP directories are synchronized, the LDAP external users must login to Cisco IMC Supervisor by specifying the complete domain name along with the user name. For example, vxedomain.cisco.com\username. However, this rule does not apply if there is only one LDAP server directory added to Cisco IMC Supervisor.

User Synchronization Limitations

- If a user has multiple group membership, that user has single group membership in Cisco IMC Supervisor.

Note

- We recommend to keep the total number of users and groups (both local and LDAP) in Cisco IMC Supervisor to 10,000 or less. If this number is exceeded, the appliance may become slow or unresponsive.
- After an LDAP synchronization process, verify that the user is assigned to the correct group.

Best Practices

The synchronization of thousands of LDAP objects to Cisco IMC Supervisor can lead to some performance issues in the appliance. Use the following procedure to synchronize only the required LDAP objects.

1. Create LDAP groups that contain all users that should have access to Cisco IMC Supervisor.
2. Synchronize only those groups to Cisco IMC Supervisor.

Adding LDAP Configurations

Perform this procedure to add LDAP configurations.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Click + to add LDAP configurations.

Step 3 On the **Add LDAP Configurations** page, complete the following fields:

Field	Description
Account Name field	An LDAP account name.
Server Type drop-down list	Choose either Microsoft Active Directory or Open LDAP.
Server field	Host name or the IP address of the server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name for the LDAP user.
Username field	Enter a name for the LDAP user.
Password field	Enter a password associated with the username.
Synchronization Freqency drop-down list	Select the frequency (hours) at which the LDAPserver must be synchronized. It can be one of the following:

Field	Description
	• 1 • 4 • 12 • 24

Step 4 Click **Next**.

Step 5 On the **LDAP Search Base** page, click **Select** and choose search criteria for retrieving users based on OU from the table displayed.

Note
Cisco IMC Supervisor supports only users and not groups. Search criteria is not mandatory based on **OU** as it can have both users as well as groups. The system sync up task runs every 24 hours and syncs up LDAP users based on the search criteria. Hence, you must perform a manual sync of only user information. To perform a manual LDAP sync, refer Requesting Manual LDAP Sync, on page 29.

Step 6 Click **Select** in the **Select** dialog box.

The search criteria you have selected is displayed next to the **Search Base** field.

Step 7 Click **Next** in the **LDAP Search Base** dialog box.

Step 8 Click **+** to add entry to user role filters table in the **LDAP User Role Filter** dialog box.

Step 9 Enter the user role details in the **Add Entry to User Role Filters** dialog box.

Step 10 Click **Submit**.

You can edit or delete these filters. You can also use the up or down arrows to move the filters to set priority.

Step 11 Click **Submit** in the **LDAP User Role Filter** dialog box.

Configuring LDAP Servers

You can configure multiple LDAP servers and accounts in Cisco IMC Supervisor. While adding LDAP accounts, you can specify the following:

- An organization unit (OU) that is part of the search base distinguished name (DN).
- A frequency at which the LDAP account is automatically synchronized with the system.
- A group or user filter to limit the results, and specify an LDAP role filter on the groups and users

Soon after an LDAP server account is added, a system task for this account is created automatically, and it immediately begins to synchronize the data. All the users and groups in the LDAP server account are added to the system. By default, all the users from the LDAP account are automatically assigned to the service end-user profile.

Before you begin

You should have set the authentication preferences to **Local First, fallback to LDAP**.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Click **Add**.

Step 3 On the **LDAP Server Configuration** page, complete the following fields:

Name	Description
Account Name field	The name of the account. This name must be unique.
Server Type field	The type of LDAP server. It can be one of the following: • OpenLDAP • MSAD - Microsoft Active Directory
Server field	The IP address or the host name of the LDAP server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name. If you selected **OpenLDAP** as the LDAP Directory Type, then this domain name must match the domain specified with the user name. **Important** You must specify the complete domain name. For example, vxedomain.com.
Username field	The user name. If you selected **OpenLDAP** as the LDAP Directory Type, then specify the user names in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where **ou** specified is the one all the other users are placed in the directory hierarchy.
Password field	The user password.

Name	Description
Synchronization Frequency drop-down list	Select the frequency (hours) at which the LDAP server must be synchronized. It can be one of the following: • 1 • 4 • 12 • 24

Step 4 Click **Next**.

Step 5 In the **LDAP Search Base** pane, click **Select** to specify LDAP search base entries and click **Select**.

All organization units (OU) that are available in Cisco IMC Supervisor are displayed in this list.

Step 6 Click **Next**.

Step 7 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system. All groups that the selected users are part of are retrieved and added into the system.
Group Filters	Click the + sign to select groups that must be synchronized with the system. All users that are part of the groups you have selected are retrieved and added into the system. However, if the users in the group you have selected are also part of other non-selected groups, then those groups are not retrieved unless they are also selected in this field.
Add Entry to User Filters or **Add Entry to Group Filters** dialog box (displayed based on your previous selection)	
Attribute Name drop-down list	Choose either **Group Name** or **User Name**.
Operator drop-down list	Choose the filter to retrieve groups and users. It can be one of the following: • **Equals to** • **Starts with**
Attribute Value field	Specify a keyword or a value that must be included in the search.

Based on the filters, the groups or users are retrieved.

Step 8 Click **Next**.

Step 9 In the **LDAP User Role Filter** pane, click the + sign to add a user role filter.

Step 10 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	The drop-down list can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco IMC Supervisor: • Group Admin • Operator • System Admin

Step 11 Click **Submit**.

The user role filters are added to the **User Role Filters** table.

Note
If you have multiple user role filters specified, then the filter specified in the first row is processed.

If you manually update the role for a user, then the user role that you earlier mapped the group to, is no longer applied on the user.

What to do next

If you have not set the authentication preference to LDAP, then you are prompted to modify the authentication preference. See Configuring Authentication Preferences, on page 20.

Viewing LDAP Server Summary Information

Perform this procedure to view the summary information of the LDAP server.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Choose an LDAP account name from the table.

Step 3 Click **View**.

The **View LDAP Account Information** screen displays LDAP account summary information.

Step 4 Click **Close**.

Testing LDAP Server Connectivity

Perform this procedure to text the LDAP connection.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Choose an LDAP account name from the table.

Step 3 Click **Test Connection**.

The status of the connection is displayed.

Step 4 Click **Close** in the **Test LDAP Connectivity** dialog box.

Searching BaseDN

Perform this procedure to search the BaseDN.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Click **Search BaseDN**.

Note
Cisco IMC Supervisor supports only users and not groups. Search criteria is not mandatory based on **OU** as it can have both users as well as groups.

Step 3 Click **Select** in the **LDAP Search Base** dialog box.

Step 4 Choose one or more users and click **Select** in the **Select** dialog box.

Step 5 Click **Submit** in the **LDAP Search Base** dialog box.

Requesting Manual LDAP Sync

Requesting manual LDAP synchronization enables you to specify either basic or advanced search criteria to retrieve LDAP users and groups. Perform this procedure for manual LDAP synchronization.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Click **Request Manual LDAP Sync**.

Step 3 On the **Manual LDAP Sync** page, complete the following fields:

Name	Description
Basic Search check box	Enables basic search by organization unit.
Advanced Search check box	Enables advanced search.

Note
When you use either of the search options, if the users and groups already exist in Cisco IMC Supervisor, then the same users and groups are not populated after performing the search.

Step 4 For basic search, click **Select** to specify the search base.

Step 5 Choose the search base DN, and click **Select** and continue to Step 9.

Step 6 For advanced search, in the **Advanced Filtering Options** pane, add or edit attribute names for **User Filters** and **Group Filters**.

Step 7 Click **Next**.

Step 8 On the **Select Users and Groups** page, complete the following fields:

Name	Description
LDAP Groups field	The LDAP groups from which the users must be synchronized.
LDAP Users field	The LDAP users that must be synchronized.

Step 9 Click **Submit**.

Choose **Administration** > **Users and Groups** and click **Users** to see the synchronized users.

Executing LDAP Synchronization and Viewing LDAP Synchronized Results

Perform this procedure to execute and view the LDAP synchronized results.

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **System Tasks**.
Step 3 Expand **User and Group Tasks** and select **LDAPSyncTask**.
Step 4 Click **Run Now**.
Step 5 Click **Submit**.
Step 6 (Optional) Click **Manage Task** to enable or disable the synchronization process.

What to do next

The results of the synchronization process are displayed in Cisco IMC Supervisor. On the **LDAP Integration** page, select an LDAP account and click **Results** to view the summary of the synchronization process.

Modifying LDAP Server Details

You can only modify the following details for a configured LDAP server:

- Port numbers and SSL configuration
- User name and password
- Synchronization frequency
- Search BaseDN selections
- User roles and groups that are mapped

Perform the following procedure to modify the LDAP server details.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.
Step 2 Select an LDAP account.
Step 3 Click **Modify**.
Step 4 On the **LDAP Server Configuration** page, edit the following fields:

Name	Description
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.

Name	Description
Username field	The user name. If you selected **OpenLDAP** as the LDAP Directory Type, then specify the user names in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where **ou** specified is the one all the other users are placed in the directory hierarchy.
Password field	The user password.
Synchronization Frequency drop-down list	Choose the frequency (in hours) at which the LDAP server is synchronized with the system database. It can be one of the following: • 1 • 4 • 12 • 24

Step 5 Click **Next**.

Step 6 Edit the **LDAP Search Base** entries and click **Next**.

Step 7 Select and edit the required attributes in the **User Filters** and **Group Filters** table and click **Next**.

Step 8 Select and edit entries in the **LDAP User Role Filter** table.

Step 9 Click add, edit, delete, or move table entries using up and down arrows.

Step 10 Click **Submit**.

Viewing Group Membership Information

Any user in the system can be part of multiple user groups. When a user is added to the system, all groups that the user is part of are also added to the system. However, the group that the user was most recently added to is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**. While you can use the **Manage Profiles** option to view and modify group membership for users, Cisco IMC Supervisor also provides you with an additional option to view a list of all groups that a specific user is part of.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Users**.

Step 3 Select a user from the table.

Step 4 Click **Group Membership**.

The **Member Of** screen displays all the groups that the user is part of.

Step 5 Click **Close**.

Deleting LDAP Server Information

Deleting an LDAP server account only results in deleting the search criteria, BaseDNs, and system entries related to this LDAP server. Users attached to the LDAP server are not deleted. Perform this procedure to delete the LDAP server information.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Choose **LDAP Integration**.

Step 3 Choose an LDAP account name from the table.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Delete**.

This initiates the deletion of the LDAP account in Cisco IMC Supervisor. Based on the number of users in the LDAP account, this deletion process could take a few minutes to complete. During such time, the LDAP account may still be visible in Cisco IMC Supervisor. Click **Refresh** to ensure that the account has been deleted.

Configuring SFTP User Password

An SFTP user is used by server diagnostics and tech support upload operations for transferring file to the Cisco IMC Supervisor appliance using SFTP. An SFTP user account cannot be used to login to the Cisco IMC Supervisor UI or the shelladmin.

Perform this procedure to configure a password for an SFTP user.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **SFTP User Configuration**.

Step 3 Enter the SFTP user password in the **Password** field.

Step 4 Click **Submit**.

Configuring Mail Setup

All outgoing emails from Cisco IMC Supervisor require an SMTP server. Cisco IMC Supervisor generated emails such as alerts for faults and so on are sent to the mail setup you have configured using the following procedure. For more information about adding email alert rules, see Adding Email Alert Rules for Server Faults, on page 64.

Note The NTLM protocol and any of its versions are not supported by the Cisco IMC Supervisor.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 Click **Mail Setup**.

Step 3 On the **Mail Setup** page, complete the following fields:

Field	Description
Outgoing Email Server (SMTP)	IP address of the server or the domain name.
Outgoing SMTP Port	Port number for the SMTP server.
Outgoing SMTP User	(Optional) The outgoing SMTP user ID to use for SMTP authentication.
Outgoing SMTP Password	(Optional) The password for the outgoing SMTP user ID to use for SMTP authentication.
Outgoing Email Sender Email Address	The From address of the outgoing Cisco IMC Supervisor generated emails.
Server IP Address	IP address of the server running Cisco IMC Supervisor.
Send Test Email checkbox	Check this check box to send a test email to the configured address.

Step 4 Click **Save**.

Configuring Cisco.com User Credentials and Proxy Configuration

You can configure Cisco user credentials and proxy details from **Administration** > **System**. The Cisco.com user and proxy credentials are application wide settings. Cisco smart call home also uses these proxy details.

Configuring Cisco.com User

Perform this procedure when you want to configure your Cisco.com user name and password.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Cisco.com User Configuration**.

Step 3 Complete the following fields for configuring the Cisco.com user:

Field	Description
User Name (cisco.com) field	Enter your Cisco login user name.
Password (cisco.com) field	Enter your Cisco login password.

Step 4 Click **Save**.

Configuring Proxy Settings

Perform this procedure when you want to configure your proxy settings.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Proxy Configuration**.

Step 3 Complete the following for proxy configuration:

Field	Description
Enable Proxy Configuration check box	(Optional) Check this check box to enable proxy and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.
Enable Proxy Authentication check box	(Optional) Check this check box to enable proxy authentication and complete the following: • **Proxy User Name** field - Enter a proxy user name for the proxy authentication. • **Proxy Password** field - Enter the password for the proxy user name.

Step 4 Click **Save**.

Setting Up CMDB Integration

The Configuration Management Database (CMDB) is used to track and manage changes in the system. CMDB typically displays ADD, DELETE, or MODIFY event types on resources such as service requests, groups, and so on.

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **CMDB Integration Setup**.

Step 3 In the **CMDB Integration Setup** screen, complete the required fields, including the following:

Name	Description
Export to FTP Server check box	Check the check box to export change records to an FTP server.
Export Format drop-down list	Choose the type of export format: CSV or XML.
FTP Server field	The FTP server address.
FTP Port field	The FTP server port number.
FTP User field	The FTP user ID.
FTP Password field	The FTP user password.
FTP Export Frequency drop-down list	Choose how often the change records are exported to the FTP server.
FTP File Name field	The filename for the exported change records. The following variables can be used to create new filenames each time that a file is exported to the target FTP server: MONTH, WEEK, DAY, YEAR, HOUR, MIN, SEC, MLLIS. Example: XYZ-$DAY-$HOUR-$MIN-$SEC
Test FTP check box	Check the check box to test FTP settings.

Step 4 Click **Save**.

Branding

A login page can be configured to display a logo that is associated with a domain name. When the end user logs in from that domain, the user sees the custom logo on the login page. The optimal image size for a logo is 890 pixels wide and 470 pixels high, with 255 pixels allowed for white space. Cisco recommends that you keep the image size small to enable faster downloads.

Adding New Login Branding Page

Perform this procedure when you want to add a new login branding page.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Login Page Branding**.

Step 3 Click **Add**.

Step 4 On the **Domain Branding** page, complete the following:

Field	Description
Domain Name field	A domain name for branding. For example, imcs.xxxx.com. **Note** For creating a domain name in your local machine, navigate to `C:\Windows\System32\drivers\etc` and specify the <*ipaddress*> and <*domainname*> in the hosts file. For example, 10.10.10.10 imcs.xxxx.com.
Custom Domain Logo checkbox	(Optional) If you want to add a logo, check this checkbox and do the following: **a.** Click **Browse**. **b.** Navigate to a logo and choose the file. **c.** Click **Open**.

Step 5 Click **Submit**.

Step 6 In the confirmation dialog box, click **OK**.

Note
You can edit, delete, and clone the customized login page you have created.

Configuring User Interface Settings

You can use this procedure to customize the Cisco IMC Supervisor application. You can modify the application header, the administrator and end-user portal based on your requirement. The header containing the logo, application name, and links such as logout can also be hidden.

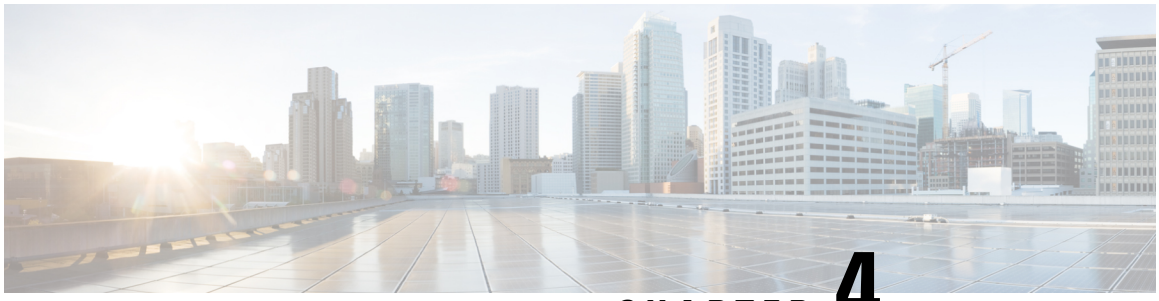
Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, complete the following:

Field	Description
Hide Entire Header check box	Use this check box to enable or disable the header.
Product Name field	Main title of the header.
Product Name 2nd Line field	Sub-title of the header.
Enable About Dialog checkbox	Use this checkbox to enable or disable the **About** dialog box for Cisco IMC Supervisor.
Administrator Portal	
Custom Link 1 Lable field	You can configure this field to change the text on header bar.
Custom Link 1 URL field	You can configure the URL for the **Custom Link 1 Lable**
Custom Link 2 Lable field	You can configure this field to change the text on header bar.
Custom Link 2 URL field	You can configure the URL for the **Custom Link 2 Lable**
End-user Portal	
Custom Link 1 Lable field	You can configure this field to change the text on header bar.
Custom Link 1 URL field	You can configure the URL for the **Custom Link 1 Lable**
Custom Link 2 Lable field	You can configure this field to change the text on header bar.
Custom Link 2 URL field	You can configure the URL for the **Custom Link 2 Lable**

Step 3 Click **Save**.



CHAPTER 4

Managing Users, User Roles and Groups

This chapter contains the following topics:

- Overview, on page 39
- Creating a User Account, on page 40
- Viewing Online Users, on page 41
- Reviewing Recent Login History of Users, on page 42
- Configuring Session Limits for Users, on page 42
- Adding a User Role, on page 43
- Branding a User Group, on page 44

Overview

Cisco IMC Supervisor supports the following system-defined user roles by default:

- **System Admin** — A user with all privileges including adding users. As an administrator in Cisco IMC Supervisor, you can assign users to system-provided user roles or to custom-defined user roles. In addition, at a later point, you can view information on any assigned role. You can make the following assignments:
  - Create a custom user role in the system, and create new user accounts with this role or assign the role to existing users.

    When you create a new user role, you can specify if the role is that of an administrator or an operator. For more information about creating user accounts, see Creating a User Account, on page 40. For more information about creating user roles, see Adding a User Role, on page 43.
  - Modify existing user roles, including default roles, to change menu settings and read/write permissions for users associated with that role.

    The procedure to modify menu settings and permissions for a role is the same as the procedure followed to create a user role.
- **Group Admin** — A user with all privileges. A system-defined user group **Default Group** is available by default in Cisco IMC Supervisor. As a group administrator, you can create and assign user accounts to this group or you can assign them to the groups you have created. A user can be part of multiple user groups. However, the group that the user was most recently added to is set as the default primary group for the user.

- **Operator** — Because the system administrator's role type is admin, you can modify the existing Operator role as required with any combination of access restrictions (menu settings and user permissions). By default, following menu settings and user permissions are assigned to an Operator.

Menu Settings	User Permissions
Systems : • Inventory and fault status • Physical Accounts • Firmware Management • Server Diagnostics	• Read - Physical Computing • Write - Physical Computing • Read - System Admin • Read - Users • Read - Read Tag Library • Write - Write Tag Library • Read - Orchestration • Write - Orchestration
Policies: • Manage Schedules • API and Orchestration	
Administration: • Users and Groups • Integration	

Note Reports such as **SCP User Configuration**, **Authentication Preferences** and **Password Policy** are enabled for Operator role under **Users and Groups**.

Creating a User Account

Note You cannot edit the **User Role** and **Login Name** fields in the **Edit User** dialog box.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Users**.

Step 3 Click **Add**.

Step 4 On the **Add User** page, complete the following:

Field	Description
User Role drop-down list	Choose **Group Admin**, **Operator**, or **System Admin**.
User Group drop-down list	Select the group that the user will have access to. You can either select a group already available, or you can add a new group. **Note** This field is visible only when you select **Group Admin** as the user role.
Login Name field	The login name for the user.
Password field	The password for the user. If the Lightweight Directory Access Protocol (LDAP) authentication is configured to the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	Repeat the password from the previous field.
User Contact Email field	The email address.
First Name field	(Optional) The first name of the user.
Last Name field	(Optional) The last name of the user.
Phone field	(Optional) The phone number of the user.
Address field	(Optional) The physical address of the user.

Step 5 Click **Add**.

Step 6 Click **OK**.

Viewing Online Users

Perform this procedure when you want to view users who are currently online.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Current Online Users**.
You can see the details such as username, IP address, session start time and so on of users who are currently logged on to Cisco IMC Supervisor.

Reviewing Recent Login History of Users

As an administrator in the system, you can review the recent login history for all users. The system records the following details for every login attempt:

- Login Name
- Remote Address
- Client Detail
- Client Type
- Authentication Status
- Comments
- Accessed On

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **All Users Login History**.

Step 3 Review the information displayed on the screen.

Configuring Session Limits for Users

You can configure the number of user interface sessions and REST API requests that users can initiate on the system.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Session Management**.

Step 3 In the **Session Management** screen, complete the required fields, including the following:

Name	Description
Maximum Concurrent Sessions Per User field	The maximum number of concurrent GUI sessions that are supported for each user. Enter a number between 1 and 128. The default value is 16.

Name	Description
Maximum Concurrent REST API Requests Per User field	The maximum number of concurrent REST API requests that are supported for each user. Enter a number between 1 and 256. The default value is 128.

Step 4 Click **Submit**.

What to do next

When users initiate a GUI session or a REST API request to exceed the limit specified on this screen, an error message is displayed in the **System Messages** screen. In this scenario, either users should clear their sessions and API requests, or as an administrator, you can use the Shell utility and clear the sessions and requests for a user. For more information, see the *Cisco IMC Supervisor Shell Guide*.

Adding a User Role

On a newly installed Cisco IMC Supervisor appliance, by default, a **GroupAdmin** role and an **Operator** role are available. Because the group admin's role type is admin, you can modify the existing **Operator** role as required with any combination of access restrictions (menu settings and user permissions). Similarly, you can create new roles, as in the following procedure, and assign users to them.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 Click **User Roles**.

Step 3 Click **Add**.

Step 4 On the **Add User Role** page, complete the following for the **User Role** pane:

Field	Description
User Role field	A descriptive name for the user role.
Role Type drop-down list	Choose **Admin**.
Description field	(Optional) A description of the user role.

Step 5 Click **Next**.

Step 6 In the **Menu Settings** pane, select the required menu options.

To choose the menu option, check the checkbox for the menu setting field.

Step 7 Click **Next**.

Step 8 In the **User Permissions** pane, select the required operations.

To choose the operation, check the checkbox for the operation.

Step 9 Click **Submit**.

Note
You can also, edit, clone, or delete user roles.

Branding a User Group

Perform the following procedure when you want to customize the Cisco IMC Supervisor application for a group of users. When users who belong to a selected group login to the system, they will see the customized page.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **User Groups**.

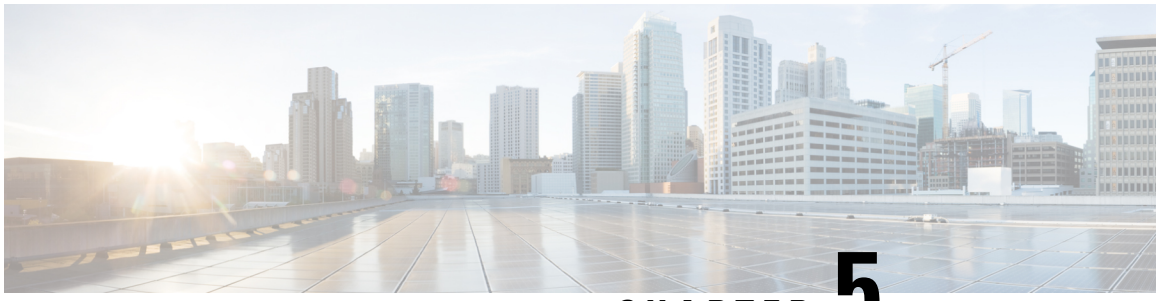
Step 3 Select a user group.

Step 4 Click **Branding**.

Step 5 On the **Group Branding** page, complete the following:

Field	Description
Logo Image checkbox	If checked, the logo appears on the top left corner of the application .
Application Labels checkbox	If checked, the application labels appear on top header section of the application.
URL Forwarding on Logout checkbox	If checked, user will be forwarded to the provided URL on logout.
Custom Links checkbox	If checked, custom links will appear on the top right corner of the application.

Step 6 Click **Submit**.



CHAPTER 5

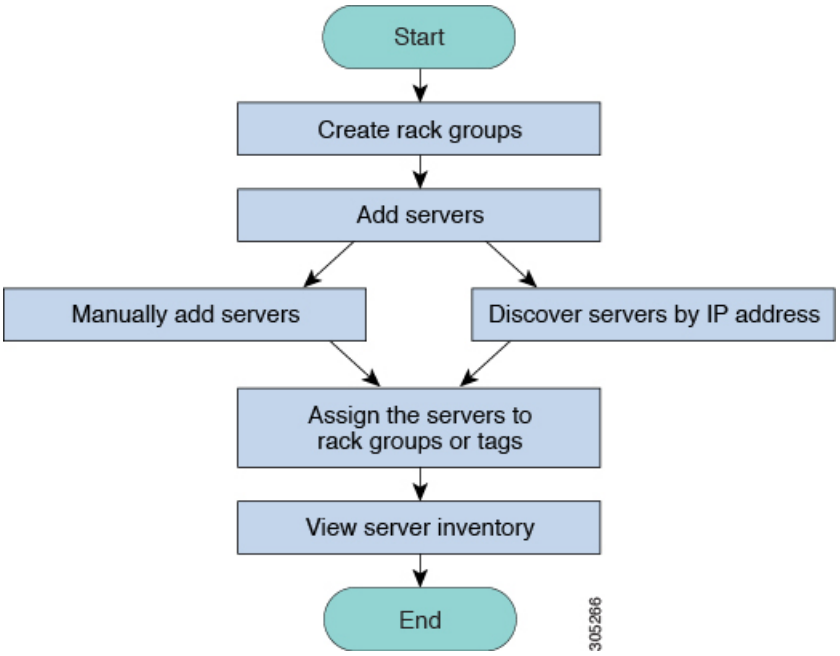
Managing Server Discovery, Rack Groups, and Rack Accounts

This chapter contains the following topics:

- Overview, on page 45
- Discovering and Importing a Server, on page 46
- Adding a Rack Group, on page 51
- Adding a Rack Account, on page 51
- Collecting Inventory for Rack Accounts or Rack Groups, on page 53
- Assigning Rack Accounts to a Rack Group, on page 54
- Testing an Account Connection, on page 54

Overview

The following figure illustrates the workflow for managing groups, rack accounts and discovering servers in Cisco IMC Supervisor. Ideally you would create a rack group and add servers to these rack groups. You can either manually add the servers or discover the servers. You can view detailed inventory of these servers.



Use Case: When you install Cisco IMC Supervisor for the first time, you must set up the environment as there is nothing preconfigured. There may be hundreds of systems across the globe which you will need to manage. You can bring these servers into Cisco IMC Supervisor either by adding them manually or by discovering them by IP address. Before doing so, you can think of logically filtering these servers and tagging them based on your organization's requirement. For example, you can group them into regions, building numbers, operating systems and so on. With the help of tag management, finer granular grouping of servers coming into Cisco IMC Supervisor is possible. For example, you can add tags to servers which contain Windows, Linux, and so on and group them under the Operating Systems rack group. You also have the flexibility of adding tags on the fly for an existing server.

There is no set way of naming the rack groups or tags. You can be creative with coming up with names as per your requirement. Names of rack groups and tags can be interchanged. For example, you can have rack groups named Windows, Linux and so on and then tag them under the Operating System tag name.

Discovering and Importing a Server

You can automatically discover rack mount servers and import them into Cisco IMC Supervisor. The following sections cover topics such as configuring auto discovery profile, performing auto discovery, and importing auto discovered servers.

Configuring Auto Discovery Profile

You should configure the auto-discovery profile based on which Cisco IMC Supervisor can discover the devices. You can have any number of profiles in Cisco IMC Supervisor.

Perform this procedure when you want to add or edit an auto-discovery profile.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Discovery Profiles**.

Step 3 Click **Add**.

Step 4 On the **Add Discovery Profile** page, complete the following:

Field	Description
Profile Name Field	A descriptive name for the profile.
Search Criteria drop-down list	Select **IP Address Range**, **Subnet Mask Range**, **IP Address CSV File**, or **IP Address List** from the drop-down list.
Starting IP Field	Valid IP address
Ending IP Field	Valid IP address
If you check **Use Credential Policy** checkbox	
Credential Policy drop-down list	Choose a policy from the drop-down list or click the + icon and create new policy. Refer to Creating a Credential Policy, on page 87, to create a new policy.
If you uncheck **Use Credential Policy** checkbox	
User Name field	The server login name.
Password field	The server login password **Important** Do not include special characters such as + in the password.
Protocol drop-down list	Choose **https** or **http** from the list.
Port field	Enter a port number.

Field	Description
The following fields are available only if the **Search Criteria** you have chosen is **IP Address Range**, **Subnet Mask Range**, and **IP Address List**. **Note** If you have chosen **IP Address CSV File**, these fields can be specified in the csv file in the following format. The sample csv file is available when you click **File Template**. You must add the entries from the first row of the csv file without any headings. • <*ip*> • (optional) <*description*> • (optional) <*location*> • (optional) <*contact*> • (optional) <*rack group*> • (optional) <*tag name:tag value*>;<*tag name:tag value*> **Note** • You can specify either an existing value or a new value for Rack Group and Tags. Specifying these fields is optional. If you do not specify a value for Rack Group in the csv file, the Default Group will be used. • When you upgrade to the current Cisco IMC Supervisor version, replace the existing csv file with the csv file you have created in the new format using the **Select a File** option. • The tag type will only be of type **STRING**.	
Description field	Enter a description of the server.
Contact field	Enter the contact details of the server.
Location field	Enter the address of the server.
Select Rack Group drop-down list or + icon	Choose a rack group or create a rack group.

Step 5 Click **Submit**.

Note
You can also modify, delete, and view profiles. Click **Edit**, **Clear**, **Delete**, or **View** to perform these tasks.

Performing Auto Discovery

Perform this procedure when you want the system to automatically discover rack-mounted servers and import them into Cisco IMC Supervisor.

Before you begin

You should configure a profile based on which Cisco IMC Supervisor can discover the devices.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Discovered Devices**.

Step 3 Click **Discover**.

Step 4 On the **Discover Devices** page, complete the following fields:

Field	Description
Select Profile drop-down list	Click **Select** to choose the profiles to discover. Check the check boxes of all the profiles you want to discover.
Schedule Later check box	Check this check box and select an existing schedule to auto discover servers at a later time or click on **+** to create a new schedule. For more information on creating schedules, see Creating Schedules, on page 153. You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to view the scheduled task or click **Remove Scheduled Tasks** to delete scheduled tasks.
Schedule(s) drop-down list	If you have chosen the **Schedule Later** check box, you can select a schedule you have created from the drop-down list. **Note** You can also create a new schedule from this dialog box.

Step 5 Click **Submit**.

Importing a Server

Perform this procedure when you want to import a server using auto discovery.

Before you begin

- You should configure a profile based on which Cisco IMC Supervisor can discover the devices.
- You have already performed a auto discovery.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Discovered Devices**.

Step 3 Click **Import**.

Step 4 On the **Import Discovered Devices** page, complete the following:

Field	Description
Select Device(s) field	Click **Select** to choose the devices to import. Check the check boxes of all the servers you want to import. **Note** If the **Import Status** of a particular rack account is imported then the status will be imported and will not show that rack account for import.
User Prefix	Enter a prefix for the user.

Step 5 Click **Submit**.

Note
You can import discovered devices multiple times without having to wait for the previous import process to complete.

Setting Properties for Discovered Devices

Perform this procedure when you want to set the properties for discovered devices.

Before you begin

You should configure a profile based on which Cisco IMC Supervisor can discover the devices.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Discovered Devices**.

Step 3 Select the device in the **Discovered Devices** table.

Step 4 Click **Set Properties**.

Step 5 On the **Set Properties** page, complete the following fields:

Field	Description
Description field	Enter a description of the server.

Field	Description
Contact field	Enter the contact details of the server.
Location field	Enter the address of the server.
Select Rack Group drop-down list or + icon	Choose a rack group or create a rack group.

Step 6 Click **Submit**.

Adding a Rack Group

Perform this procedure when you want to add a new rack group in Cisco IMC Supervisor. By default, a system-defined group **Default Group** is available.

Before you begin

If you have logged in for the first time, ensure that the license is updated for Cisco IMC Supervisor. To upgrade the license, see Updating the License, on page 15.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Add**.

Step 3 On the **Create Rack Group** page, complete the following fields:

Field	Description
Group Name field	A descriptive name for the rack group.
Description field	(Optional) A description of the rack froup.

Step 4 Click **Create**.

What to do next

Add one or more rack accounts to the rack group.

Adding a Rack Account

You can add a rack-mount server to any of the existing rack group you have already created or you can create a new rack group and add the rack-mount server. After the account is added, you can use Cisco IMC Supervisor to manage the server.

Perform this procedure when you want to add a new rack-mounted server to an existing rack group.

Before you begin

- If you have logged in for the first time, ensure that the license is upgraded for Cisco IMC Supervisor. To upgrade the license, see Updating the License, on page 15.
- Ensure that a rack group exists.

Note You can add a rack account under the system-provided default group or under a rack group that you have created.

- Ensure that you have enabled XML API in Cisco IMC Supervisor. This ensures that you can add and manage the rack-mount servers from Cisco IMC Supervisor.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Rack Accounts**.

Step 3 Click **Add**.

Step 4 On the **Create Account** page, complete the following fields:

Field	Description
Account Name field	A descriptive name for the rack account.
Server IP or Hostname field	The IP address of the rack-mount server or the virtual management IP address for Cisco UCS S3260 Dense Storage Rack Server. **Note** You can also enter a Fully Qualified Domain Name (FQDN) or hostname.
Description field	(Optional) A description of the rack account.
Use Credential Policy check box	(Optional) If you have already created credential policies, then check this check box to select the policy from the drop-down list.
If you check **Use Credential Policy** check box	
Credential Policy drop-down list	Choose a policy from the drop-down list.
If you uncheck **Use Credential Policy** check box	
User Name field	Login ID for the rack-mount server.
Password field	Password for the login ID for the rack-mount server.

Field	Description
Protocol drop-down list	Choose https or http from the list.
Port field	The port number associated with the selected protocol.
Rack Group drop-down list or + icon	Choose a rack group from the list or click + to create a rack group. For more information on creating a rack group, see Adding a Rack Group, on page 51.
Contact field	(Optional) The contact email address for the account.
Location field	(Optional) The location of the account.

Step 5 Click **Submit**.

Note

- You can create a rack account again without having to wait for the previous command of creating a rack account to complete.
- You can edit, delete, collect inventory, assign rack accounts to a rack server and test the account connection.
- You can select multiple rack accounts and delete them. You cannot delete an account if inventory collection, fault-health collection, firmware upgrade, applying policy or profile, server diagnostics tasks are running on any of the accounts.

What to do next

Test the rack server connection. Refer Testing an Account Connection, on page 54.

Collecting Inventory for Rack Accounts or Rack Groups

Perform this procedure when you want to collect inventory for a rack account or a rack group.

Before you begin

The rack account or rack group is already created under rack accounts.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.
Step 2 Click **Rack Accounts**.
Step 3 A list of rack accounts is displayed.
Step 4 Click **Inventory**.

Step 5 On the **Collect Inventory for Account(s)** page, choose **Rack Group** or **Rack Account** to choose the servers from the drop-down list.

Step 6 Click **Select** to select the servers.

Step 7 In the **Select** dialog box, choose the servers and click **Select**.

Note
You can use the search bar at the top of the report if you want to filter rack groups or rack accounts for selection.

Step 8 Click **Submit**.

Assigning Rack Accounts to a Rack Group

Perform this procedure when you want to assign servers to a rack group.

Before you begin

The rack account or server has already been created under Rack Accounts.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Rack Accounts**.

Step 3 A list of servers is displayed.

Step 4 Select a server or multiple servers and click **Assign Rack Group**.

Step 5 On the **Assign Rack Groups** page, select the rack group you want to assign the servers to.

Note
Click on the + icon next to **Assign Rack Group to selected server(s)** drop-down list to create a rack group.

Step 6 Click **Submit**.

Testing an Account Connection

Perform this procedure when you want to test one or more rack account connections. We recommend you to perform this procedure for every new account added in Cisco IMC Supervisor.

Procedure

Step 1 Choose **Systems** > **Physical Accounts**.

Step 2 Click **Rack Accounts**.

Step 3 From the list of rack accounts, select the accounts for which you want to test the connection.

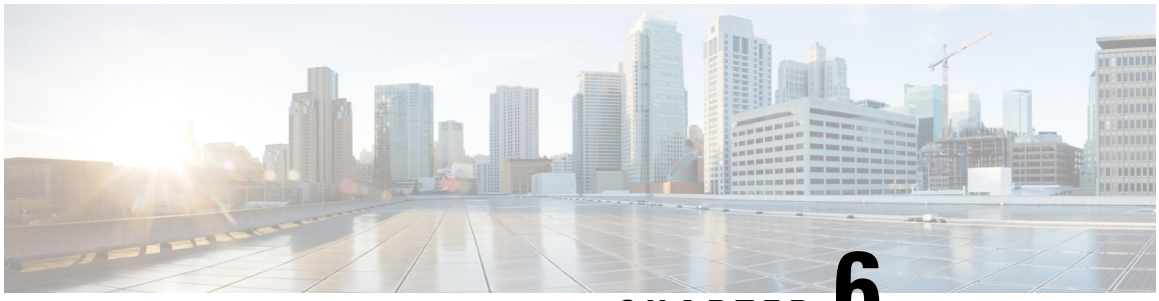
Step 4 Click **Test Connection**.

Note
You cannot see the **Test Connection** button till you select at least one rack account from the list.

Step 5 In the **Test Connection** dialog box, click **Submit**.

Testing the connection may take several minutes.

The connection status and the reason for success or failure are displayed in the **Rack Accounts** page.



CHAPTER 6

Viewing Inventory Data and Faults

This chapter contains the following topics:

- Viewing Rack-Mount Server Details, on page 57
- Viewing Fault Details for a Rack Mount Server, on page 63
- Summary Reports for a Rack Group, on page 63
- Adding Email Alert Rules for Server Faults, on page 64

Viewing Rack-Mount Server Details

Perform this procedure when you want to view the details for a rack mount server, such as memory, CPUs, and PSUs used in the server.

Note You can also select **Rack Groups** and perform the procedure to view the rack-mount server details.

Before you begin

Ensure that the server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Expand **Rack Groups** and select the rack group that contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Step 4 Double-click the server in the list to view the details, or select the server in the list and click the down arrow on the far right, then choose **View Details**.

Note
You cannot see the down arrow on the far right until you select a server from the list.

The following details are available for a rack-mount server:

Tab	Description
Summary	An overview of the rack account.
CPUs	The details of the CPU used in the server.
Memory	The details of the memory used in the server.
PSUs	The details of the power supply unit used in the server. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
PCI Adapters	The details of the PCI adapters used in the server.
VIC Adapters	The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click **View Details** to view information such as **External Ethernet Interfaces** and **VM FEXs**.
Network Adapters	The details of the network adapters used in the server. Select any of the Network Adapters listed and click **View Details** to view information on **External Ethernet Interfaces**.
Storage Adapters	The details of the storage adapters used in the server. Select any of the Storage Adapters listed and click **View Details** to view information such as **Controller Info** and **Physical Drives**, and **Virtual Drives**. See, Viewing Smart Information for SSD, on page 60.
FlexFlash Adapters	The details of the FlexFlash adapters used in the server. Select any of the FlexFlash Adapters listed and click **View Details** to view information such as **Controller Info** and **Physical Drives**. If you are upgrading Cisco IMC Supervisor from a previous version, you must run the inventory by going to **Systems** > **Physical Accounts** > **Rack Accounts** > **Inventory**, or wait for the periodic inventory to run, for the FlexFlash details to appear in the report. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Communication	The information on the protocol, such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.
Remote Presence	The details of vKVM, Serial Over LAN, and vMedia.
Faults	The details of the faults logged in the server.

Tab	Description
Users	The details about users under **Default Group**. You can also view the strong password policy and password expiration details that you have set while creating a user policy and password expiration policy respectively. See, User Policy, on page 112 and Password Expiration Policy, on page 104. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Cisco IMC Log	The details of the Cisco IMC logs for the server. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
System Event Log	The details of the server logs. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
TPM	Information on the TPM inventory.
BIOS	Details about the BIOS settings and Boot Order for the server. Select the server and click on **View BIOS Settings**, **View Boot Settings**, or **View Boot Order**.
Fault History	Historical information on the faults that occurred on the server.
Tech Support	Details about the tech-support log files, such as the file name, destination type, and status of the upload are displayed in the **Tech Support** table. An option to export the tech-support log files to a remote server or on the local Cisco IMC Supervisor appliance is available. For more information about exporting, see Exporting Technical Support Data to a Remote Server, on page 81. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Host Images	Details of an image such as name, size, MD5 checksum, last modified time, and if the image is mapped are displayed. You can select an image and click **Map Image**, **Unmap Image**, and **Delete Image** to perform the various actions. **Note** Host image mapping is applicable only for E-Series servers.
Associated Hardware Profiles	Details of policies that are associated to a hardware profile.

Step 5 Click the **Back** button on the far right to return to the previous window.

Viewing Smart Information for SSD

Perform this procedure when you want to view smart information for a Solid State Drive (SSD) under Storage Controller.

Before you begin

Ensure that the server is already added as a Rack Account under a Rack Groups.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Expand **Rack Groups** and select the rack group that contains the SSD drive.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Double-click the server that contains SSD in the list.

Step 5 On the Rack Server page, click **Storage Adapters**.

Step 6 Double-click the SSD drive and click **Controller Info**.

The following Controller Settings are available:

- **Enable Copyback on SMART**
- **Enable Copyback to SSD on SMART Error**

Step 7 Double-click the SSD drive and click **Physical Drives**.

Step 8 Double-click the SSD physical drive and click **View Smart Information**.

The following details are available for a SSD drive:

Tab	Description
Power Cycle Count field	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours field	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left field	The number of write cycles remaining in a solid state drive (SSD). For instance, if an SSD is capable of 100 write cycles during its life time, and it has completed 15 writes, then the percentage of life left in the drive is 85%. Each percentage range is represented in a different color. For instance, green for 75% to 100% and red for 1 to 25%. **Note** You can see a bar graph added for SSDs in **SSD - Percentage Life Left** under **Controller Info**.

Tab	Description
Wear Status in Days field	The number of days an SSD has gone through with the write cycles. SSD vendors provide a finite number of writes per day on the SSD, based on which, you can calculate the total number of years the SSD would continue to work.
Operating Temperature field	The current temperature of the drive at which the selected SSD operates at the time of selection.
Percentage Reserved Consumed field	The total capacity (out of the percentage reserved for it)consumed by the SSD.
Time of Last Refresh field	Time period since the drive was last refreshed.

Step 9 Click **Close**.

Note
On the Storage Adapter page, click **Controller Info** to view the controller settings such as **Percentage LIFE LEFT**, **Enable Copy back on SMART**, and **Enable Copy back to SSD on SMART Error**.

Overview of Controller Drive Security

Self-Encrypting Drives (SEDs) are used for encrypting data while writing it onto the drives and decrypting them before reading the data. This ensures that the data on the drives are secure. Cisco IMC Supervisor supports enabling security at the controller, physical drive, and virtual drive level for this feature.

The controller level security has two options, Remote Key Management and Local Key Management. For Remote Key Management, the Security KeyId and the Security Key are retrieved from the KMIP server. In case of Local Key Management, the Security KeyId and the Security Key are either provided by you or provided as a suggestion from the CIMC server. These parameters are used to secure data on the drives.

The physical drive level security can have the SED drives in locked and foreign locked state. The locked state indicates that the drives have been locked with the security key of the controller in this server. The foreign locked state indicates that the drives are locked with the security key of another controller but the drives are placed in this controller. Unlocking the foreign locked drives require the security key of that controller. Once unlocked you can perform any security related operations on the drive.

Note Cisco IMC Supervisor supports only Local Key Management and not Remote Key Management. See, Viewing Controller Drive Security Details, on page 61.

Viewing Controller Drive Security Details

Perform this procedure when you want to view the controller drive security details under **Controller Info**, **Physical Drives**, and **Virtual Drives**.

Before you begin

The M4 rack-mount server or the UCS S3260 storage server must have SED connected in it.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Expand **Rack Groups** and select the sub rack group.

Step 3 Click **Rack Servers**.

Step 4 Double-click the server.

Step 5 On the Rack Server page, **Storage Adapters**.

Step 6 Double-click the selected server or click **View Details**.

Step 7 On the Storage Adapter page, click **Controller Info**.
The following details are available for a SSD drive:

Tab	Description
Power Cycle Count field	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours field	Total number of hours that the drive is in the Power On mode.
Percentage Life Left field	The number of write cycles remaining in a solid state drive (SSD). For instance, if an SSD is capable of 100 write cycles during its life time, and it has completed 15 writes, then the percentage of life left in the drive is 85%. Each percentage range is represented in a different color. For instance, green for 75% to 100% and red for 1 to 25%. **Note** You can see a bar graph added for SSDs in **SSD - Percentage Life Left** under **Controller Info**.
Wear Status in Days field	The number of days an SSD has gone through with the write cycles. SSD vendors provide a finite number of writes per day on the SSD, based on which, you can calculate the total number of years the SSD would continue to work.
Operating Temperature field	The current temperature of the drive at which the selected SSD operates at the time of selection.
Percentage Reserved Consumed field	The total capacity (out of the percentage reserved for it) consumed by the SSD.
Time of Last Refresh field	Time period since the drive was last refreshed.

Step 8 On the Storage Adapter page, click **Physical Drives**.
Details such as the controller name, physical drive number, status, health, serial number, firmware, FDE capable, FDE enabled, Secured, Locked, Foreign Locked and so on are displayed.

Step 9 On the Storage Adapter page, click **Virtual Drives**.
Details such as the virtual drive number, name, status, health, size, RAID level, Boot drive, FDE capable, FDE enabled and so on are displayed.

Step 10 Click **Submit**.

Viewing Fault Details for a Rack Mount Server

Perform this procedure when you want to view the fault details of a rack mount server such as the reason for the issue and the recommended steps to resolve the issue.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the Rack Groups page, click **Faults**.

Step 3 Double-click the server from the list to view the details. You can also click the server from the list, click the down arrow on the far right and choose **View Details**.

Note
You cannot see the down arrow on the far right till you select the server from the list.

The following details are available for a rack mount server:

Tab	Description
Explanation	Brief reason for the issue.
Recommendation	Steps to resolve the issue.

Step 4 Click **Close**.

Summary Reports for a Rack Group

The Inventory and Fault Status for Rack Groups page contains a list of Rack Groups. When you select groups under **Rack Groups**, a **Summary** report is available in the selected rack group page which displays the following reports:

- **Faults**—represents the overall fault count for selected rack groups. The fault counts are categorized based on their severity such as Critical, Major, Warnings, Minor, and Info.

- **Server Health**—represents the overall health status of the server. The overall server health status can be in any of the states such as Good, Memory Test In Progress, Moderate Fault, and Severe Fault.



Note The Moderate Fault and Severe Fault correlates to faults with severity as Major and Critical respectively. However, note that the sever health status will be determined based on the status reported by CIMC and this may not always have a direct mapping to the fault severities stated above. Other factors such as the fault type and associated components influence the overall server health status.

- **Chassis Health**—represents the health status of the chassis. The health status can be in any of the states such as Good, Memory Test In Progress, Moderate Fault, and Severe Fault.
- **Firmware Versions**—represents the overall server count of the firmware versions that are managed for the selected rack groups.
- **Server Models**—represents the overall server count of the models that are managed for the selected rack groups.
- **Power State**—represents the overall server count of the power state which is managed for the selected rack groups. The power states can either be On or Off.
- **Server Connection Status**—represents the overall server count of the connection status of servers for the selected rack groups. The connection status can either be Success or Failed.
- **Overview**—represents the total number of servers and number of critical faults.

Adding Email Alert Rules for Server Faults

You can create one or more email rules. For each rule, an email alert is sent when faults that match the conditions specified in alert rule are met. Perform the following procedure to receive email alerts for such faults.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 Click **Email Alert Rules**.

Note
The **Email Alert Rules** table displays details of an alert rule such as the email alert rule name, the alert scope, the servers and server groups you have selected for an alert rule and so on.

Step 3 Click **Add**.

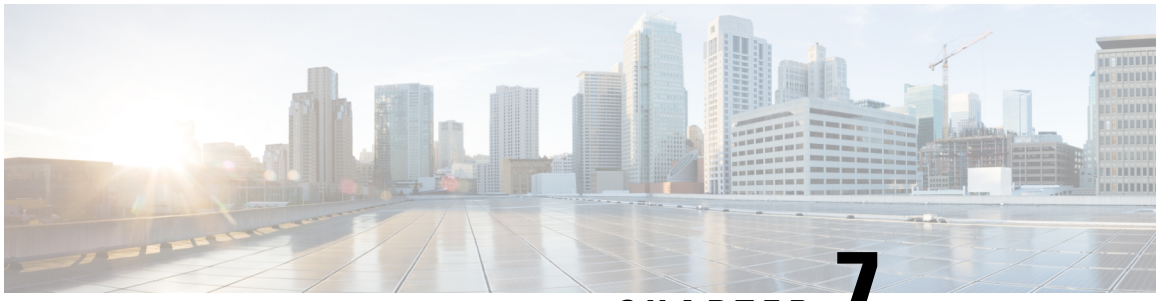
Step 4 On the **Add Email Alert Rule** page, complete the following:

Field	Description
Name	Enter a unique name for the rule.

Field	Description
Alert Scope	Choose **System** for receiving all system level alerts for new faults discovered on any server. Choose **ServerGroup** for receiving email alerts for new faults discovered on a server which is part of the specified Rack Group. Choose **Server** for receiving email alerts for new faults discovered on a specified server.
Server Groups	If you choose the Alert Level as **ServerGroup**, this option is displayed. **a.** Click **Select**. **b.** Check one or more rack server groups in the **Select** dialog box and click **Select**. The selected server group names for which email alerts will be sent are listed next to this field.
Servers	If you choose the Alert Level as **Server**, this option is displayed. **a.** Click **Select**. **b.** Check one or more servers in the **Select** dialog box and click **Select**. The selected server names for which email alerts will be sent are listed next to this field.
Email Addresses field	The email addresses of the intended recipients of the email alert. You can enter multiple email addresses, separated by a comma.
Severity	Perform the following procedure to select fault severity levels for which email alerts will be sent to the email addresses configured in the **Email Addresses** field. **a.** Click **Select...**. **b.** Check one or more severity levels from the list and click **Select**. **Note** The selected values will be displayed next to the **Select...** button.
Enable Alert check box	Check this check box to enable email alerts to the configured email address.
Send alert for all faults every 24 hours check box	Check this check box to send email alerts once every 24 hours. This email alert will contain all active and open faults based on the configured email alert rule.

Note

- You can modify and delete the email alert rules. The **Edit** and **Delete** options are visible only when you select a rule. Click **Edit** and modify the required fields displayed or click **Delete** and confirm deletion.
- You can select multiple rules concurrently and click **Delete** to delete them.
- The number of email alerts sent are based on the number of rules you have created.
- If you have a system level rule present in 1.0 or 1.0.0.1, when you upgrade to 1.1, you can see that the name of the rule by default is added as **system-default**. You cannot modify the **Alert Level** field for this group, but you can delete this system level rule.



CHAPTER 7

Managing Rack Servers

This chapter contains the following topics:

- Viewing Rack-Mount Server Details, on page 67
- Viewing Fault Details for a Rack Mount Server, on page 70
- Powering On and Off a Rack Mount Server, on page 71
- Tagging Assets for a Rack Mount Server, on page 72
- Shutting Down a Rack Mount Server, on page 72
- Performing a Hard Reset on Rack Mount Server, on page 73
- Performing a Power Cycle on a Rack Mount Server, on page 74
- Launching KVM Console for a Rack-Mount Server, on page 74
- Launching GUI for a Rack Mount Server, on page 75
- Setting Locator LED for a Rack Mount Server, on page 76
- Setting Label for a Rack Mount Server, on page 77
- Managing Tags for a Rack-Mount Server, on page 78
- Adding Tags for a Rack-Mount Server, on page 80
- Exporting Technical Support Data to a Remote Server, on page 81
- Clearing SEL, on page 82
- Managing System Tasks, on page 83

Viewing Rack-Mount Server Details

Perform this procedure when you want to view the details for a rack mount server, such as memory, CPUs, and PSUs used in the server.

Note You can also select **Rack Groups** and perform the procedure to view the rack-mount server details.

Before you begin

Ensure that the server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Expand **Rack Groups** and select the rack group that contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Step 4 Double-click the server in the list to view the details, or select the server in the list and click the down arrow on the far right, then choose **View Details**.

Note
You cannot see the down arrow on the far right until you select a server from the list.

The following details are available for a rack-mount server:

Tab	Description
Summary	An overview of the rack account.
CPUs	The details of the CPU used in the server.
Memory	The details of the memory used in the server.
PSUs	The details of the power supply unit used in the server. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
PCI Adapters	The details of the PCI adapters used in the server.
VIC Adapters	The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click **View Details** to view information such as **External Ethernet Interfaces** and **VM FEXs**.
Network Adapters	The details of the network adapters used in the server. Select any of the Network Adapters listed and click **View Details** to view information on **External Ethernet Interfaces**.
Storage Adapters	The details of the storage adapters used in the server. Select any of the Storage Adapters listed and click **View Details** to view information such as **Controller Info** and **Physical Drives**, and **Virtual Drives**. See, Viewing Smart Information for SSD, on page 60.

Tab	Description
FlexFlash Adapters	The details of the FlexFlash adapters used in the server. Select any of the FlexFlash Adapters listed and click **View Details** to view information such as **Controller Info** and **Physical Drives**. If you are upgrading Cisco IMC Supervisor from a previous version, you must run the inventory by going to **Systems** > **Physical Accounts** > **Rack Accounts** > **Inventory**, or wait for the periodic inventory to run, for the FlexFlash details to appear in the report. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Communication	The information on the protocol, such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.
Remote Presence	The details of vKVM, Serial Over LAN, and vMedia.
Faults	The details of the faults logged in the server.
Users	The details about users under **Default Group**. You can also view the strong password policy and password expiration details that you have set while creating a user policy and password expiration policy respectively. See, User Policy, on page 112 and Password Expiration Policy, on page 104. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Cisco IMC Log	The details of the Cisco IMC logs for the server. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
System Event Log	The details of the server logs. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
TPM	Information on the TPM inventory.
BIOS	Details about the BIOS settings and Boot Order for the server. Select the server and click on **View BIOS Settings**, **View Boot Settings**, or **View Boot Order**.
Fault History	Historical information on the faults that occurred on the server.

Tab	Description
Tech Support	Details about the tech-support log files, such as the file name, destination type, and status of the upload are displayed in the **Tech Support** table. An option to export the tech-support log files to a remote server or on the local Cisco IMC Supervisor appliance is available. For more information about exporting, see Exporting Technical Support Data to a Remote Server, on page 81. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Host Images	Details of an image such as name, size, MD5 checksum, last modified time, and if the image is mapped are displayed. You can select an image and click **Map Image**, **Unmap Image**, and **Delete Image** to perform the various actions. **Note** Host image mapping is applicable only for E-Series servers.
Associated Hardware Profiles	Details of policies that are associated to a hardware profile.

Step 5 Click the **Back** button on the far right to return to the previous window.

Viewing Fault Details for a Rack Mount Server

Perform this procedure when you want to view the fault details of a rack mount server such as the reason for the issue and the recommended steps to resolve the issue.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the Rack Groups page, click **Faults**.

Step 3 Double-click the server from the list to view the details. You can also click the server from the list, click the down arrow on the far right and choose **View Details**.

Note
You cannot see the down arrow on the far right till you select the server from the list.

The following details are available for a rack mount server:

Tab	Description
Explanation	Brief reason for the issue.

Tab	Description
Recommendation	Steps to resolve the issue.

Step 4 Click **Close**.

Powering On and Off a Rack Mount Server

Perform this procedure when you want to power on or power off a rack mount server.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 From the list of servers, select the server you want to power on/off.

Note
You can also select multiple rack servers.

Step 5 Click **Power ON**. From the **More Actions** drop-down list, choose **Power OFF**.

Note
You can also right-click and choose the options.

Step 6 In the confirmation dialog box, click **OK**.

Note
A message that the servers were powered on or powered off is displayed. The message will also indicate if any servers could not be powered on or off. Refresh the table after a while so that the current power states are reflected.

Tagging Assets for a Rack Mount Server

Asset tag is a user-defined tag for the server. You can use the **Asset Tag** option to add the Cisco IMC server property through Cisco IMC Supervisor

You can tag assets for both rack servers and for chassis. For tagging assets for chassis, see Tagging Assets for Cisco UCS S3260 Rack Server, on page 166. Perform this procedure when you want to tag an asset.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Rack Groups** page, click **Rack Servers**.

Note
You can also select any sub group under **Rack Groups** in the **Inventory and Fault Status** pane.

Step 3 Select the server you want to tag.

Step 4 From the **More Actions** drop-down list, choose **Asset Tag**.

Note
You can also right-click and choose the option.

Step 5 Click **Submit**.

Note
Asset Tag option is available only from Cisco IMC release 3.0.(1c) onwards. For lower version platforms, the **Asset Tag** column in the **Rack Groups** page displays a blank entry.

Shutting Down a Rack Mount Server

Perform this procedure when you want to shut down a rack mount server.

Note You can also select multiple rack servers.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **Shut Down**.

Note
You can also right-click and choose the option.

Step 6 Click **OK**.

Performing a Hard Reset on Rack Mount Server

Perform this procedure to reset the server.



Note You can also select multiple rack servers.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **Hard Reset**.

Note
You can also right-click and choose the option.

Step 6 Click **OK**.

Performing a Power Cycle on a Rack Mount Server

Perform this procedure when you want to power off and on a rack mount server in one cycle.



Note You can also select multiple rack servers.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **Power Cycle**.

Note
You can also right-click and choose the option.

Step 6 Click **OK**.

Launching KVM Console for a Rack-Mount Server

You can launch the KVM console for C-Series M4 or C-Series M5 servers running on firmware versions 4.1(1c) or later using explicit authentication.

Note The launch of KVM console for servers running firmware versions below 4.1(1c) is deprecated and will not work as expected.

Before you begin

- Ensure that the server is already added as a Rack Account under a Rack Group.
- Ensure that you have a valid Java Runtime Environment (JRE) installed for the KVM feature to work.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **KVM Console**.

Note
- You can also right-click and choose the option.
- You can select a maximum of 5 servers to launch KVM console.

Step 6 Click **Submit**.

For the Rack servers running on firmware 4.1(1c) or above, a new browser window with a link to launch KVM login page will be displayed after certificate verification. On clicking the link, the KVM login page of the corresponding Rack server is displayed.

Launching GUI for a Rack Mount Server

Perform this procedure to launch the Cisco IMC Supervisor GUI from a separate browser.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **Launch GUI**.

Note
You can also right-click and choose the option.

Step 6 Cllick **Submit**.

The launch GUI option will open the Login page of the corresponding Rack server in aseparate window. This is displayed only when the **HTTP Enabled** and **Redirect HTTP to HTTPS Enabled** checkboxes are enabled while configuring the communication services in the Rack server. For more information, see Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide.

Setting Locator LED for a Rack Mount Server

A server locator LED helps you to identify a specific server among many servers in a data center. Perform this procedure to set the LED to on or off.



Note You can also select multiple rack servers.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note

You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **Locator LED**.

Note
You can also right-click and choose the option.

Step 6 From the **Turn** drop-down list, choose **ON**/**OFF**.

Step 7 Click **Submit**.

Setting Label for a Rack Mount Server

Setting label names to servers help you in classifying servers. This makes it easier to find, view, and compare the servers that you require. Perform this procedure to set the labels for a rack mount server.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Select the server from the list.

Step 5 From the **More Actions** drop-down list, choose **Set Label**.

Note
You can also right-click and choose the option.

Step 6 Enter a new label.

Step 7 Click **Submit**.

Managing Tags for a Rack-Mount Server

Tagging is used to assign a label to an object, such as a resource group or a rack server. Tags can be used to provide information such as rack locations, responsible support groups, purpose, or Operating System. Perform this procedure to add tags or modify tags.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 In the Inventory and Fault Status pane, expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 Click **Rack Servers** or **Chassis**.

Note
You can select any sub groups under **Rack Groups**.

Step 4 From the **More Actions** drop-down list, choose **Manage Tags**.

Note
You can also right-click and choose the option.

Step 5 Click **+** to add an entry to the **Manage Tags** table.

Step 6 In the **Add Entry to Tag** screen, complete the following:

Field	Description
Tag Name	Select the tag name from the drop-down list and click **Submit** or create a new tag. **a.** Click the + icon. **b.** In the **Create Tag** window, do the following: **1.** In the **Name** field, enter a descriptive name for the tag. **2.** In the **Description** field, enter a description of the tag. **3.** In the **Type** field, select String or Integer from the drop-down list. **4.** In the **Possible Tag Values** field, enter a possible value for the tag. **5.** Click **Next**. **6.** Click the + icon to add a new category. **c.** In the **Add Entry to Entities** window, from the **Category** drop-down list, choose the category. It can be one of the following: • **Physical_Compute** category creates tag entities for a Rack Server. • **Administration** category creates tag entities for users. **Note** You can also add tags for a chassis. For more information about adding tags for a chassis, see Adding Tags for Cisco UCS S3260 Rack Server , on page 167. **d.** Check the **Rack Servers** or **Chassis** check box. **e.** Click **Submit**. **Note** The tags are displayed under the respective category according to the set taggable entities. **f.** In the confirmation dialog box, click **OK**.
Tag Value	Select the tag value from the drop-down list.

Step 7 Click **Submit**.

Step 8 Select a tag in the **Manage Tags** screen and click **Edit** to edit a tag.

Step 9 Choose the Tag Name and Tag Value to modify the tags.

Step 10 Click **Submit**

Adding Tags for a Rack-Mount Server

Tagging is used to assign a label to an object, such as a resource group or a rack server. Tags can be used to provide information such as rack locations, responsible support groups, purpose, or Operating System. Perform this procedure to add tags to a rack mount server.

Before you begin

The server is already added as a rack account under a rack group.



Note You can also select multiple rack servers.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 From the **More Actions** drop-down list, choose **Add Tags**.

Note
You can also right-click and choose the option.

Step 5 Choose the **Tag Name** from the drop-down list.

Step 6 Choose the **Tag Value** from the drop-down list.

Step 7 Click on the plus icon to create a new tag. Refer Managing Tags for a Rack-Mount Server, on page 78 to create tags.

Note
You can also clone, edit, delete, and view tag details.

Exporting Technical Support Data to a Remote Server

Perform this procedure to upload the technical support files to a specified server.

Note The exporting technical support option does not support Cisco UCS S3260 Dense Storage Rack Server.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Double-click the rack-mount server in the list to view its details, or click the rack-mount server from the list and click the down arrow on the far right, then choose **View Details**.

Step 5 Click **Tech Support**.

Step 6 Click **Create Tech Support**.

Step 7 On the **Create Tech Support** screen, complete the following fields:

Name	Description
Destination Type drop-down list	You can export the file to a remote server or to a local Cisco IMC Supervisor appliance. Choose either **REMOTE** or **LOCAL**.
Network Type drop-down list	The network type. This can be one of the following: • **SCP** • **SFTP** • **FTP** • **TFTP**
Server IP/Hostname field	The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Network Type** drop-down list, the name of this field will vary.
Path and Filename field	The path and filename that must be used when exporting the file to the remote server.

Name	Description
Username	The username the system should use to log in to the remote server. This field does not apply if the network type is TFTP.
Password	The password for the remote server username. This field does not apply if the network type is TFTP.

Step 8 Click **Submit**.

Note
- You can only select and download the tech-support files you have created choosing **LOCAL** as the **Destination Type**.
- You can select the existing technical support files and download only those files that are stored within the Cisco IMC Supervisor appliance. Select a specific file and click **Download**. This creates a `<hostname>_<timestamp>. tar.gz` file.

Clearing SEL

The System Event Log (SEL) records most server-related events that can be used for troubleshooting issues. Perform this procedure to clear the SEL logs.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Inventory and Fault Status** pane, select **Rack Groups**.

Note
You can also expand **Rack Groups** and select the rack group which contains the server.

Step 3 On the selected rack group page, click **Rack Servers**.

Note
You can also select any sub groups under **Rack Groups**.

Step 4 Double-click the rack-mount server from the list to view its details or click the rack-mount server from the list and click the down arrow on the far right and choose **View Details**.

Step 5 Click **System Event Log**.

Step 6 Click **Clear IMC SEL Log**.

Step 7 (Optional) On the **Clear IMC SEL Logs** screen, check the **Delete historical logs from Cisco IMC Supervisor** check box.

Selecting this option clears the system event logs from the Cisco IMC Supervisor GUI.

Step 8 Click **Submit**.

Managing System Tasks

The **System Tasks** tab displays all the system tasks that are currently available in Cisco IMC Supervisor. However, this list of system tasks is linked to the type of accounts that you have created in Cisco IMC Supervisor. For example, if you have logged in for the first time, then only a set of general system-related tasks are visible on this page. As and when you add accounts, such as rack accounts, or Cisco IMC Supervisor accounts, system tasks related to these accounts are populated on this page.

Expand the tasks on the left pane, select the individual tasks such as purging, rack server, and user and group tasks and manage them.

In circumstances when there are multiple processes or tasks running on the appliance, you can choose to disable a system task. If you do so, then until such time that you manually enable it, the system task will not run. This will affect the data that is populated in other reports. For example, if you disable an inventory collection system task, then reports that require this data may not display accurate data. In this case, you will have to manually run an inventory collection process, or enable the system task.



Note It is not recommended to edit any of the system tasks.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 Click **System Tasks**.

Step 3 Select a task from the list and click **Manage Task**.

Step 4 On the **Manage Task** screen, complete the following:

Field	Description
Task Execution drop-down list	(Optional) Choose enable or disable.
System Task Policy drop-down list	Choose one of the following options: • **default-system-task-policy** • **local-run-policy**

Field	Description
Schedule Type drop-down list	Specify the schedule type for the system task. It can be one of the following options: • **Fixed Delay**—Implies the time period between the completion of one task execution and the initiation of the next task execution. • **Fixed Rate**—Implies the time period between successive tasks executions. If there is a delay in the execution of one task or if one task takes longer to execute than its scheduled time, it results in delays in subsequent task executions. Systems tasks that are configured with this setting will not run concurrently. These tasks will not run concurrently.
Hours drop-down list	Choose the hourly frequency to run the task. If you chose **Fixed Delay** as the schedule type, then this number indicates the time gap, in hours, between the completion of one task exection and the initiation of the next task execution. If you chose **Fixed Rate**, then this number indicates time period, in hours, between successive task executions.
Minutes drop-down list	Choose the frequency, in minutes, to run the task.
Enable Custom Frequency check box	Check this check box to enable a custom frequency for the system task.
Recurrence Type drop-down list	Specify the recurrence schedule for the system task.It can be one of the following: • **No End** • **Only Once**
Start Time field	Specify the date and time for the recurrence schedule.
Frequency drop-down list	Choose a frequency for the system task. It can be one of the following: • **Hourly** • **Daily** • **Weekly** • **Monthly** **Note** This field is displayed only when you select **No End** in the **Recurrence Type** drop-down list.
Frequency Interval drop-down list	Choose a frequency interval from the drop-down list. The values in this list vary depending on the frequency you have specified.

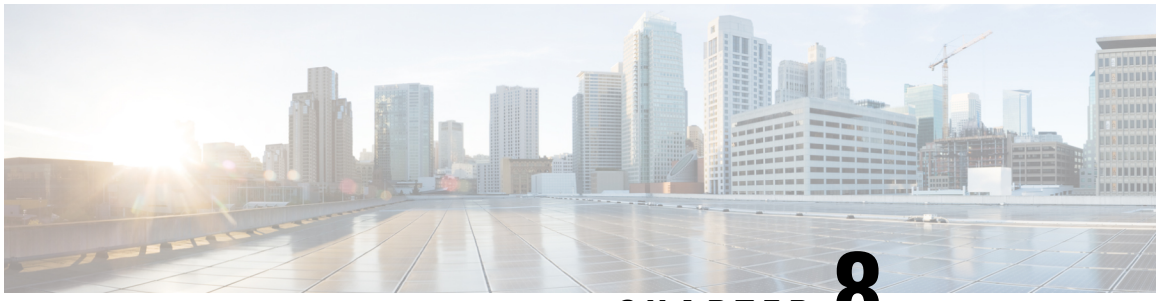
Step 5 Click **Submit**.

Running a Task

Each task is schedule to run at a user-defined time interval. However, you can override this and run it manually. After running a task manually, the task is then scheduled to run again as defined in the frequency column. Perform this procedure when you want to run a system task manually.

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 Click **System Tasks**.
Step 3 Choose a system task from the table.
Step 4 Click **Run Now**.
Step 5 Click **Submit**.



CHAPTER 8

Managing Policies and Profiles

This chapter contains the following topics:

- Credential Policies, on page 87
- Hardware Policies, on page 88
- Hardware Profiles, on page 120
- Tag Library, on page 124
- REST API and Orchestration, on page 126

Credential Policies

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned to user accounts control the authentication process in Cisco IMC Supervisor. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application.

The **Credential Policies** page displays the following details:

Field	Description
Policy Name	User defined name of the policy.
Description	User defined brief description of the policy.
Username	Cisco user name.
Protocol	Protocol followed by the policy.
Port	Port for the policy.

You can perform various tasks such as adding, editing, and deleting policies from this page. For information about creating a credential policy, see Creating a Credential Policy, on page 87.

Creating a Credential Policy

Perform this procedure to create a credential policy.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Credential Policies**.

Step 3 Click **Add**.

Step 4 On the **Add Credential Policy** screen, complete the following fields:

Field	Description
Policy Name field	A descriptive name for the policy.
Description field	(Optional) A description of the policy.
User Name field	Cisco IMC user name or the rack mount server user name.
Password field	Cisco IMC password or the rack mount server password.
Protocol drop-down list	Choose a protocol from the drop-down list.
Port field	Enter a port number for the policy.

Step 5 Click **Submit**.

Note
You can edit, clone, delete, view, apply and view server mappings of the credential policy you have created.

Hardware 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.

Use Case: As an administrator, you may have identified a "Golden Server" which contains the required configurations including the right Networking, BIOS, RAID configurations and so on. You can replicate these configurations across other servers which are out of compliance. You can retain this configuration within Cisco IMC for any new servers that you may need to add in future and roll-out the configured server. You have the flexibility of changing the configuration on the fly before applying the same. For example, a component may need an update, ntp ip address, baud rate and so on. You may have forgotten the configuration on the "Golden Server" and may want to verify it before applying to other servers.

Individual policies are processed one after the other. Policies bundled into profiles are multi-threaded and helps starting a bunch of processes at the same time.

The following workflow indicates how you can work with hardware policies in Cisco IMC Supervisor:

1. Create a hardware policy such as BIOS policy or an NTP policy. You can create a policy in one of the following methods:
   a. Create a new policy. For more information about the various policy types and creating a new policy, see Creating Hardware Policies, on page 89.
   b. Create a policy from the configuration existing on a server. For more information about creating a policy from the configuration existing on a server, see Creating a Policy from an Existing Configuration, on page 117.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Hardware Policy, on page 118.
3. Perform any of the following optional tasks on the policy:
   a. Edit
   b. Delete
   c. Clone
   d. You can also view the list of servers that are mapped to a specific policy. For more information on performing these tasks, see General Tasks Under Hardware Policies, on page 119.
   e. You can apply profiles to servers after creating various policies and grouping them into profiles. For more information about applying profiles, see Applying a Hardware Profile, on page 123.

Creating Hardware Policies

Perform this procedure to create hardware policies.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 On the **Add** screen, choose a policy type from the drop-down list.

For more information on creating a policy based on a policy type, select the policy type listed in the table below. The various properties required to configure these policies are available in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide. The respective sections in this guide are listed against each policy type.

Note
A check box is introduced to select the Cisco UCS S3260 platform for creating policy. This option is disabled by default. If you need to create a policy for Cisco UCS S3260, you must check the check box and enable the same.

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
BIOS Policy, on page 91	*Configuring BIOS Settings*
Disk Group Policy, on page 92	*Managing Storage Adapters*
FlexFlash Policy, on page 92	*Managing the Flexible Flash Controller*
IPMI Over LAN Policy, on page 96	*Configuring IPMI*
LDAP Policy, on page 97	*Configuring the LDAP Server*
Legacy Boot Order Policy, on page 98	*Server Boot Order*
Network Configuration Policy, on page 99	*Configuring Network-Related Settings*
Network Security Policy, on page 102	*Network Security Configuration*
NTP Policy, on page 103	*Configuring Network Time Protocol Settings*
Password Expiration Policy, on page 104	*Password Expiry*
Precision Boot Order Policy, on page 105	*Configuring the Precision Boot Order*
Power Restore Policy, on page 106	*Configuring the Power Restore Policy*
RAID Policy, on page 107	*Managing Storage Adapters*
Serial Over LAN Policy, on page 109	*Configuring Serial Over LAN*
SNMP Policy, on page 110	*Configuring SNMP*
SSH Policy, on page 111	*Configuring SSH*
User Policy, on page 112	*Configuring Local Users*
VIC Adapter Policy, on page 114	*Viewing VIC Adapter Properties*
Virtual KVM Policy, on page 113	*Configuring the Virtual KVM*
vMedia Policy, on page 115	*Configuring Virtual Media*
Zoning Policy, on page 116	*Dynamic Storage* in the *Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Storage Servers*

What to do next

Apply the policy to a server. See Applying a Hardware Policy, on page 118.

BIOS Policy

A BIOS policy automates the configuration of BIOS settings on servers. You can create one or more BIOS policies that contain a specific grouping of BIOS settings, matching the needs of a server or a set of servers. If you do not specify a BIOS policy for a server, the BIOS settings will default to set of values for a brand new baremetal server or to a set of values previously configured using Cisco IMC. If a BIOS policy is specified, its values replace any previously configured values on the server.

For details about configuring BIOS properties, see *Configuring BIOS Settings* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **BIOS Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, select values for the main BIOS properties, such as **Boot Option Retry**, **Post Error Pause**, and entries in **TPM Support** drop-down list. The **Power ON Password Support** drop-down list allows you to enable or disable power on password support. You can also choose the default platform setting. Enabling this prevents you from making any changes to the server, including configuration changes and entering the BIOS setup.

Note
Ensure that a BIOS password is set in the BIOS Configuration screen using the CIMC UI.

Step 6 On the **Advanced** screen, choose the BIOS property values from the drop-down lists and click **Next**.

Step 7 On the **Server Management** screen, choose the server property values from the drop-down lists and click **Submit**.

Note
BIOS policy displays tokens for all the available platforms.

- If an attribute is not valid for a particular server platform it is ignored. For example, Power On Password Support BIOS token is applicable only for servers running a 3.x firmware. If this token is applied on a server running firmware below 3.x, it is ignored.
- If an attribute is present for the target platform and the value is not applicable, an error occurs. For example, Extended APIC BIOS token has values Enabled and Disabled which is applicable only for platform A based server models. However, if this token is applied on platform B server models, you will get an xml parsing error.

Disk Group Policy

Using a Disk Group policy, you can select the physical disks used for Virtual Drives and also configure various attributes associated with a virtual drive. A group of physical disks used for creating a virtual drive is called a Disk Group.

A disk group policy defines how a disk group is created and configured. The policy specifies the RAID level to be used for the virtual drive. You can use a disk group policy to manage multiple disk groups. A single Disk Group policy can be associated with multiple virtual drives. If so, the virtual drives share the same Virtual Drive group space. Disk Group policies associated with different virtual drives in a RAID policy do not have any physical disk repeated across different Disk Group policies. For more information about RAID policy, see RAID Policy, on page 107.

For details about configuring the various disk group properties, see section *Managing Storage Adapters* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Disk Group policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Disk Group Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field and click **Next**.

Step 4 On the **Virtual Drive Configuration** screen, choose the RAID level from the **RAID Level** drop-down list and click **Next**.

Step 5 On the **Local Disk Configuration** screen, click **+** to add an entry to reference a local disk configuration and click **Submit**.

Note

- You cannot create a Disk Group policy from current configuration of the server.
- When a RAID policy is created from current configuration of the server, the Disk Group policy is also created automatically from the server configuration.

FlexFlash Policy

A FlexFlash policy allows you to configure and enable the SD card.

For details about configuring the various properties, see section *Managing the Flexible Flash Controller* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Note

- The minimum Cisco Integrated Management Controller firmware version for FlexFlash support is 2.0(2c).
- Flex Flash policies are not available for Cisco UCS S3260 Rack Server.

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **FlexFlash Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field and click **Next**.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 On the **Configure Cards** page, complete the following fields:

Field	Description
Firmware Mode pane	Choose any of the following firmware operating modes: • **Mirror Mode** - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers. • **Util Mode** - In this mode one card with four partitions and one card with a single partition is created. This mode is available only for C220 M4 and C240 M4 servers. • **Not Applicable** - No firmware operating modes are selected. Go to step 5 if you select **Not Applicable**. This mode is available only for C220 M3, C240 M3, C22, C24, and C460 M4 servers.
Mirror radio button	Check **Enable Virtual Drive** to enable the **Hypervisor** virtual drive or check **Erase Virtual Drive** to erase it.
Util radio button	Check **Enable Virtual Drive** to enable virtual drives such as **SCU**, **Hypervisor**, **Drivers**, **HUU**, and **User Partition** or check **Erase Virtual Drive** to erase them. **Note** You can select multiple virtual drives.
Not Applicable radio button	Check **Enable Virtual Drive** to enable virtual drives such as **SCU**, **HV**, **Drivers**, and **HUU**. **Note** • You can select multiple virtual drives. • **Erase Virtual Drive** check box is not available.

Field	Description
Partition Name field (available only for **Mirror** and **Util** mode	The name of the partition.
Non Util Card Partition Name field	The name that you want to assign to the single partition on the second card, if it exists. **Note** This option is available only for util mode.
Select Primary Card (available for mirror mode) or **Select Util Card** (available for Util mode) drop-down list	Select the slots **Slot 1** or **Slot 2** where the SD cards are present or select **None** if only one SD card is present on the server. **Note** **None** is available only for **Select Util Card** option.
Auto Sync check box	Automatically synchronizes the SD card available in the selected slot. **Note** This option is available only for mirror mode.
Slot-1 Read Error Threshold field	The number of read errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Slot-1 Write Error Threshold field	The number of write errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

Field	Description
Slot-2 Read Error Threshold field	The number of read errors that are permitted while accessing Slot 2 of the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero). **Note** This option is available only for util mode. In case of mirror mode, the slot-1 Read/Write threshold will be applied to Slot-2 as well.
Slot-2 Write Error Threshold field	The number of write errors that are permitted while accessing Slot 2 of the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero). **Note** This option is available only for util mode. In case of mirror mode, the slot-1 Read/Write threshold will be applied to Slot-2 as well.

Step 5 If you selected **Not Applicable** in the **Details** pane in step 4, complete the following fields:

Field	Description
Virtual Drive Enable drop-down list	The virtual drives that can be made available to the server as a USB-style drive.
RAID Primary Member drop-down list	The slot in which the primary RAID member resides.
RAID Secondary Role drop-down list	The role of the secondary RAID.
I/O Read Error Threshold field	The number of read errors that are permitted while accessing the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

Field	Description
I/O Write Error Threshold field	The number of write errors that are permitted while accessing the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy The number of write errors that are permitted while accessing the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy.
Clear Errors check box	If checked, the read/write errors are cleared when you click **Submit**.

Step 6 Click **Submit**.

You can also select an existing FlexFlash policy from the **Hardware Policies** table and delete, edit, clone, apply or view the apply status by selecting the respective options in the user interface.

Note
Applying a FlexFlash policy is a two step process as follows:

a. The settings on the server will be set to default.

b. The new settings on the policy will be applied. If there is any failure in this step, you will lose the existing settings prior to applying the policy.

IPMI Over LAN Policy

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus. Configure an IPMI over LAN policy when you want to manage Cisco IMC with IPMI messages.

For details about configuring the various properties, see section *Configuring IPMI* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create an IPMI Over LAN policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **IPMI Over LAN Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field and click **Next**.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 If you are creating this policy for a rack-mount server, then complete the following steps:

a) In the **Main** dialog box, complete the following fields.

Option	Description
Enable IPMI Over LAN	Check this check box to configure the IPMI properties.
Privilege Level Limit	Choose a privilege level from the drop-down list.
Encryption Key	Enter a key in the field.

Note
Encryption key must contain even number of hexadecimal characters, not exceeding 40 characters in total length. If less than 40 characters are specified, the key will be padded with zeros to the length of 40.

b) Click **Next**.

c) On the **Confirm** screen, click **Submit**.
You can see the rack-mount server listed in the **Server Platform** column under **Hardware Policies**.

Step 5 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 6 On the **CMC Settings** screen, check the **Enable IPMI Over LAN** checkbox for both CMC 1 and CMC 2 if required.

Step 7 Click **Next**.

Step 8 On the **BMC Settings** screen, check the **Enable IPMI Over LAN** checkbox for both BMC 1 and BMC 2 if required.

Step 9 On the **Confirm** screen, click **Submit**.
You can see the Cisco UCS S3260 Dense Storage Rack Server listed in the Server Platform column in the **Hardware Policies** page.

LDAP Policy

Cisco C-series and E-series servers support LDAP. Cisco IMC Supervisor supports the LDAP configuration settings on the servers using an LDAP policy. You can create one or more LDAP policies that contain a specific grouping of LDAP settings, matching the needs of a server or a set of servers.

For details about configuring the various LDAP properties, see *Configuring LDAP Server* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **LDAP Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, enter the LDAP properties and click **Next**

Step 6 On the **Configure LDAP Servers** screen, enter the LDAP server details and click **Next**

Step 7 On the **Group Authorization** screen, enter the group authorization details and click **+** to add an LDAP group entry to the table.

Step 8 On the **Add Entry to LDAP Groups** screen, fill in the group details and click **Submit**.

Note

- Any existing LDAP Role Groups configured previously on the server are removed and replaced with the role groups that you configured in the policy. If you have not added any role groups to the policy, then the existing role groups on the server are simply removed.
- **Nested Group Search Depth** is applicable only to Cisco IMC versions 2.0(4c) and above. This value cannot be applied using the policy on a server that is running Cisco IMC versions prior to 2.0(4c).

Legacy Boot Order Policy

A Legacy Boot Order Policy automates the configuration of boot order settings. You can create one or more Legacy Boot Order policies which contain a specific grouping of boot order settings that match the needs of a server or a set of servers. Using Cisco IMC Supervisor, you can configure the order in which the server attempts to boot from available boot device types. You can also configure the precision boot order which allows linear ordering of the devices. See Precision Boot Order Policy, on page 105.

For details about configuring the various server boot order properties, see section *Server Boot Order* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Note Legacy Boot Order policies are not available for Cisco UCS S3260 Rack Server.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Legacy Boot Order Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field and click **Next**.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 On the **Main** screen, click + and select the device type from the drop-down list. The table lists the devices you have added.

In the **Select Devices** table, select an existing device and click **x** to delete a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

You cannot add the same device type again.

Step 5 Click **Submit** in the **Add Entry to Select Devices** screen.

Note
This policy is applicable only for Cisco IMC versions prior to 2.0. An error message is displayed if the policy is applied to a server running higher Cisco IMC versions. Use Precision Boot Order policy instead.

Network Configuration Policy

Cisco IMC Supervisor allows you to create a Network Configuration policy which can specify the following network settings on a server:

- DNS Domain
- DNS Server for IPv4 and IPv6
- VLAN configuration

For details about configuring the various network configuration properties, see section *Configuring Network-Related Settings* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Network Configuration policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 In the **Add** dialog box, choose **Network Configuration Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field and click **Next**.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117

Step 4 If you are creating this policy for a rack-mount server, complete the following steps:

a) On the **Main** screen, complete the following fields:

Field	Description
Common Properties	

Field	Description
Use Dynamic DNS check box	Dynamic DNS is used to add or update the resource records on the DNS server from Cisco IMC Supervisor
If you check **Use Dynamic DNS** check box	
Dynamic DNS Update Domain field	You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of Cisco IMC Supervisor for the DDNS update.
IPv4 Properties	
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC Supervisor retrieves the DNS server addresses from DHCP.
If you do not check **Obtain DNS Server Addresses from DHCP** check box	
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.
IPv6 Properties	
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC Supervisor retrieves the DNS server addresses from DHCP.
If you do not check **Obtain DNS Server Addresses from DHCP** check box	
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.
VLAN Properties	
Enable VLAN check box	If checked, is connected to a virtual LAN.
If you check **Enable VLAN** check box	
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

b) Click **Next**.
c) On the **Confirm** xreen, click **Submit**.
You can see the rack-mount server listed in the Server Platform column in the Hardware Policies page.

Step 5 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 6 On the **Main** screen, complete the following fields:

Field	Description
Common Properties	

Field	Description
Use Dynamic DNS check box	Dynamic DNS is used to add or update the resource records on the DNS server from Cisco IMC Supervisor
If you check **Use Dynamic DNS** check box	
Dynamic DNS Update Domain field	You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of Cisco IMC Supervisor for the DDNS update.
IPv4 Properties	
Use DHCP check box	If checked, the **Obtain DNS Server Addresses from DHCP** check box is displayed.
Obtain DNS Server Addresses from DHCP check box	If checked, enables DHCP for DNS.
If you do not check **Obtain DNS Server Addresses from DHCP** check box	
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.
IPv6 Properties	
Enable IPv6 check box	If checked, the **Use DHCP** check box is displayed.
Use DHCP check box	If checked, the **Obtain DNS Server Addresses from DHCP** check box is displayed.
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC Supervisor retrieves the DNS server addresses from DHCP.
If you do not check **Use DHCP** check box	
Management IP Address field	Enter the Management IP address.
Prefix Length field	Enter the number of characters for the prefix length.
Gateway field	Enter the Gateway IP address.
If you do not check **Obtain DNS Server Addresses from DHCP** check box	
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.
VLAN Properties	
Enable VLAN check box	If checked, is connected to a virtual LAN.
If you check **Enable VLAN** check box	

Field	Description
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 7 Click **Next**.

Step 8 On the **CMC Settings** screen, enter the following fields for both CMC 1 and CMC 2 if required:

Field	Description
Hostname field	The hostname of the server.
IPv4 Address field	The IPv4 IP address.
IPv6 Address field	The IPv6 IP address.

Step 9 Click **Next**.

Step 10 On the **BMC Settings** screen, enter the following fields for both BMC 1 and BMC 2 if required:

Field	Description
Hostname field	The hostname of the server.
IPv4 Address field	The IPv4 IP address.
IPv6 Address field	The IPv6 IP address.

Step 11 Click **Next**.

Step 12 On the **Confirm** screen, click **Submit**.

Caution
To prevent breaking the communication between Cisco IMC Supervisor and the rack server which depends on the DHCP settings in your network, exercise caution when using the following setting.

If you choose to use DHCP for obtaining the DNS IP addresses, the system will also configure the rack server (where this policy is applied) to use DHCP for the Management IP Address of the server.

Network Security Policy

Cisco IMC Supervisor uses IP blocking as network security. IP blocking prevents the connection between a server or a website and certain IP addresses or a range of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers. You can create one or more Network Security policies which contain a specific grouping of IP properties that match the needs of a server or a set of servers.

You can set four IP filtering properties while creating the Network Security policy. IP Filtering allows a selected set of IPs to access the servers. You can either input a single IP address or a range of IP Addresses separated by hyphen in any of the four filter fields. An IP address can either be a IPv4 or IPv6 address.

For details about configuring the various network security properties, see section *Network Security Configuration* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Network Security policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Network Security** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **IP Blocking** window, check **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 6 Click **Next**.

Step 7 On the **IP Filtering** screen, check **Enable IP Filtering** checkbox to enable the IP, and enter either single or a range of IP addresses.

Note
Filter 1 displays the IP address of Cisco IMC Supervisor by default.

Step 8 Click **Submit**.

NTP Policy

With an NTP service, you can configure a server managed by Cisco IMC Supervisor to synchronize the time with an NTP server. By default, the NTP server does not run in Cisco IMC Supervisor. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco IMC Supervisor synchronizes the time on the managed server with the configured NTP server.

For details about configuring the various NTP properties, see section *Configuring Network Time Protocol Settings* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a NTP policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **NTP Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, check **Enable NTP** check box to enable alternate servers and specify up to 4 NTP servers.

Step 6 Click **Submit**.

Note
This policy is not applicable to E-series server models.

Password Expiration Policy

You can set a shelf life for a password, after which it expires. As an administrator, you can set this time in days. This configuration is common to all users. Users can set and derive the configuration as part of User policy and create Password Expiration policy.

For details about configuring the various properties, see section *Configuring Password Expiry for Users* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Password Expiration policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Password Expiration Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

Step 4 On the **Main** screen, complete the following:

Field	Description
Enable Password Expiry check box	Check this check box to enable a specified password expiry duration and complete the following: **Password Expiry Duration** - Set the number of days for the password to expire.
Password History field	Set the number of occurrences that will be displayed when you view the password history.
Notification Period field	Set the number of days before which you will be notified about the password expiry.
Grace Period field	Set the grace period after which the password will expire.

Step 5 Click **Submit**.

Note

- You can also select an existing policy and click **Properties** or **Delete** to edit or delete a policy from the **More Actions** drop-down list.
- This policy must be applied along with the User policy. You cannot apply a Password Expiration policy individually.
- E-Series servers do not suppport Password Expiration policy.

Precision Boot Order Policy

Configuring the precision boot order allows linear ordering of the devices. In Cisco IMC Supervisor you can change the boot order and boot mode, add multiple devices under each device types, re-arrange the boot order, and set parameters for each device type.

For details about configuring the various boot order properties, see section *Configuring the Precision Boot Order* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

You can create this policy for servers that are running Cisco IMC version 2.x and above. For servers that are running versions prior to 2.x, you must configure the Legacy Boot Order policy instead.

Perform the following procedure to create a Precision Boot Order policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **Precision Boot Order Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check UEFI Secure Boot check box or select the boot mode from the **Configure Boot Mode** drop-down list.

Step 6 Click **+** and select or enter device details. The table lists the devices you have added.

You can also select an existing device in the **Select Devices** table and click **x** to delete or click edit icon to edit a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

Note
HTTP Boot is supported from CIMC version 4.1(3b).

Step 7 On the **Add Entry to Select Devices** page, click **Submit**.

Step 8 Check **Configure One Time Boot Device** check box to set the device from which the server must boot once.

Step 9 Select the device from the **One Time Boot Device** drop-down list.

Note
Configure One Time Boot Device is not applicable for CIMC versions older than 3.0(1c).

Step 10 Check **Reboot On Update** check box to reboot the selected server after the one time boot device has been updated in the server.

Step 11 Click **Submit**.

Power Restore Policy

Create this policy when you want to modify the value for the Power Restore policy set on a C-series or E-series server without having to login to the Cisco IMC of that server.

Note You cannot create this policy on an ENCS server.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Power Restore Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 Choose a setting from the **Power Restore Policy** drop-down list.

It can be one of the following options:

- **Power Off**
- **Power On**

  If you select this option, the **Power Delay Type** field is displayed. This option is applicable only for Cisco UCS C-series servers.
- **Restore Last State**

Step 6 Choose a value in the **Power Delay Type** drop-down list.

It can be one of the following options:

- **Fixed**—If you select this option, the **Power Delay Value** field is displayed.
- **random**—If you select this option, the **Power Delay Value** field is not displayed.

Step 7 Specify a value between 0 and 240 seconds in the **Power Delay Value** field.

Step 8 Click **Submit**.

What to do next

You must apply this policy. For more information, see Applying a Hardware Policy, on page 118.

RAID Policy

You can use a RAID policy to create virtual drives on a server. You can also configure the storage capacity of a virtual drive. Each virtual drive in a RAID policy is associated with a disk group policy. Using a disk group policy you can select and configure the disks to be used for a particular virtual drive.

RAID policy is supported only on the following:

- Storage controllers that support RAID configurations.
- Cisco IMC firmware version 2.0(4c) and above.

For details about configuring the various properties, see section *Managing Storage Adapters* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a RAID policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **RAID Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Drive Security** window, check the **Configure Drive Security** check box to configure the security for the drive.

Important
If you checked the **Create policy from current configuration of the server** check box, the Drive Security properties for the policy are retrieved only if the security properties, such as the security Key ID, are common for all controller slots associated with the server. If the security Key ID is not common across all controller slots in the server, deriving the drive security configuration fails and subsequently the RAID policy is not created.

Step 6 Select the **Enable Drive Security** or **Disable Drive Security** radio buttons to enable or disable the security for the drive.

Note
Enabling drive security will allow you to enter the security key details.

Step 7 Select **Enable Drive Security** and complete the following fields:

Field	Description
Local Key Management check box	This check box is selected by default.
Security Key field	Enter a security key.
Security Key Identifier field	Enter a security key identifier.
Confirm Security Key field	Confirm the previously entered security key.
Current Security Key field	Enter the key only when modifying the security key.

Note
When Cisco IMC Supervisor exports a RAID policy with security keys, the security key parameters are left empty so that Cisco IMC Supervisor does not expose the security key. You must manually key in the values.

Step 8 On the **Virtual Drive Configuration** window, click + to add virtual drives that you want to configure on the server.

Virtual drives from all controller slots on the server and the corresponding disk group policies on those virtual drives are retrieved and displayed in the user interface.

Step 9 Click + to add an entry to the virtual drives table. On the **Add Entry to Virtual Drives** page, complete the following:

Field	Description
Virtual Drive Name field	Check this check box to enable a specified password expiry duration and complete the following: **Password Expiry Duration** - Set the number of days for the password to expire.
Virtual Drive Strip Size	The size of each strip, in KB. M2 RAID controller supports only 32K and 64K. Other RAID controllers support 64k, 128k, 256k, 612k, and 1024k.
Disk Group Policy drop-down list	Select an existing Disk Group policy from the **Disk Group Policy** drop-down list or click + to add a new Disk Group policy to specify local disks. See Disk Group Policy, on page 92. **Note** If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.
Access Policy drop-down list	Select from the options listed.
Read Policy drop-down list	Select from the options listed.
Write Policy drop-down list	Select from the options listed.

Field	Description
IO Policy drop-down list	Select from the options listed.
Drive Cache drop-down list	Select from the options listed.
Expand to available check box	Expands the virtual drive size to use maximum capacity available on the disks.
Boot Drive check box	Sets the virtual drive you are creating as a boot drive. **Note** You cannot have more than one boot drive.
Set disks in JBOD state to Unconfigured Good check box	Sets the disks which are in JBOD state to unconfigured good state before they are used for virtual drive creation.
Enable Full Disk Encryption check box	Creates virtual drive from unused physical drives.

Step 10 Click **Submit**.
You can see the virtual drives you have created in the **Virtual Drives** table.

Step 11 Check the **Delete existing Virtual Drives** check box to delete all existing virtual drives on the server.

If you select this check box, all existing virtual drives on the server will be deleted when the policy is applied. This may result in loss of existing data.

Step 12 Click **Next**.

Step 13 On the **Physical Drive Configuration** page, complete the following:

Step 14 Check **Configure Unused Disks** check box and select an option to configure the unused disks as either **Unconfigured Good** or **JBOD** state.

Note
If you select **Unconfigured Good**, the **Clear Secure Drive** check box is displayed. If you select **JBOD**, the **Enable Secure Drive** check box is displayed.

Step 15 Check **Clear Secure Drive** to delete all data on the physical drive or check **Enable Secure Drive** to enable the secure drive.

Step 16 Click **Submit**.

Serial Over LAN Policy

Serial over LAN enables the input and output of the serial port of a managed system to be redirected over IP. Configure and use a serial over LAN on your server when you want to reach the host console with Cisco IMC Supervisor. You can create one or more Serial over LAN policies which contain a specific grouping of Serial Over LAN attributes that match the needs of a server or a set of servers.

For details about configuring the various Serial Over LAN properties, see section *Configuring Serial Over LAN* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Serial Over LAN policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Serial Over LAN Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check the **Enable SoL** check box and select the **CoM Port** and **Baud Rate** values from the drop-down list or use the existing values.

Step 6 Click **Submit**.

SNMP Policy

Cisco IMC Supervisor supports configuration of the Simple Network Management Protocol (SNMP) settings and for sending fault and alert information by SNMP traps from the managed server.

For details about configuring the various SNMP properties, see section *Configuring SNMP* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a SNMP policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **SNMP Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **SNMP Users** window, click **+** to add a SNMP user and fill in the user details. You can use the **+** icon to add up to 15 SNMP Users.

Select an existing SNMP entry to edit or delete an entry from the table.

Note
The **DES** privacy type is not supported from CIMC version 4.1(3b) and Cisco IMC Supervisor version 2.3.

Step 6 Click **Next**.

Step 7 On the **SNMP Traps** window, click + to add a SNMP trap and fill in the trap details. You can use the + icon to add up to 15 SNMP Traps.

Select an existing SNMP entry to edit or delete an entry from the table.

Step 8 Click **Next**.

Step 9 On the **SNMP Settings** window, configure the SNMP properties.

Step 10 Click **Submit**.

Note

- Any existing **SNMP Users** or **SNMP Traps** configured previously on the server are removed and replaced with users or traps that you configured in the policy. If you have not added any users or traps into the policy, the existing users or traps on the server are removed but not replaced.
- The **SNMP Port** cannot be configured on a C-series server that is running Cisco IMC versions prior to 2.x; it must be excluded for such servers using the check box.
- The **SNMP Port** cannot be configured on a E-series server that is running Cisco IMC version 2.x; it must be excluded for such servers using the check box.

SSH Policy

The SSH server enables a SSH client to make a secure, encrypted connection and the SSH client is an application running over the SSH protocol to provide device authentication and encryption. You can create one or more SSH policies which contain a specific grouping of SSH properties that match the needs of a server or a set of servers.

For details about configuring the various SSH properties, see section *Configuring SSH* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create an SSH policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **SSH Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check **Enable SSH** check box, and enter SSH properties or use the existing properties.

Step 6 Click **Submit**.

User Policy

A User policy automates the configuration of local user settings. You can create one or more user policies which contain a list of local users that need to be configured on a server or a group of servers.

For details about configuring the various properties, see section *Configuring Local Users* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a User policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **User Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, you can add users that need to be configured on the server to the **Users** list.

Step 6 Check **Enforce Strong Password** check box if you want to enforce strong password on users you will configure in the next step.

This feature is applicable only on servers running CIMC 2.0(9c) and above.

Step 7 Click + to add a user.

Step 8 On the **Add Entry to Users** window, complete the following fields:

Field	Description
Username	Enter a name for the user in the field.
Role	Choose a role for the user such as read-only, admin and so on from the drop-down list.
Enable User Account	Check this check box to activate the user.
New Password	Enter a password associated with the username.
Confirm New Password	Repeat the password from the previous field.

Step 9 Click **Submit**.

Step 10 Check **Add Password Expiration Policy** check box to apply a Password Expiration policy.

Note
You cannot apply a Password Expiration policy individually.

Step 11 Choose an existing Password Expiration policy from the drop-down list or click + to add a new Password Expiration policy. See Password Expiration Policy, on page 104.

Step 12 Click **Submit**.

You can also select an existing user from the **Users** table on the **Main** window and click **Edit** or **Delete** icons to edit or delete a user.

Note

- The first user in the **Users** table is the admin user. You cannot delete this admin user but can change the password.
- For servers running CIMC older than version 2.0(8d), Cisco IMC Supervisor created dummy user entries on the server along with the ones defined in the policy. When you now apply the policy on servers running CIMC 2.0(8d) and higher, these blank user entries are no longer created. The previously existing dummy user entries (applied through an earlier policy) will now be cleared.
- Ensure that the account used to manage Cisco IMC Supervisor is not deleted from the user list in the policy. If deleted, Cisco IMC Supervisor loses connection to the server being managed.

Virtual KVM Policy

The KVM console is an interface accessible from Cisco IMC Supervisor that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location. You can create one or more KVM policies which contain a specific grouping of virtual KVM properties that match the needs of a server or a set of servers.

For details about configuring the various KVM properties, see section *Configuring the Virtual KVM* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform this procedure when you want to create a Virtual KVM policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **Virtual KVM Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 Check the **Enable vKVM** check box.

Step 6 Choose or enter the virtual server properties or use the existing properties.

Step 7 Click **Submit**.

VIC Adapter Policy

For details about configuring the various VIC adapter properties, see *Viewing VIC Adapter Properties* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **VIC Adapter Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, click + to add a VIC adapter entry in the table.

Step 6 On the **Add Entry to VIC Adapters** screen, you can either edit or review the following adapter details:

- **PCI Slot Selection**—Specifies if the adapter is installed in any available PCI Slot or in a specific PCI slot. If you choose Any, then the **PCI Slot** field is not displayed.
- **PCI Slot**—The PCI slot in which the adapter is installed.
- **Description**—Description of the adapter.
- **FIP Mode**—Specifies if FCoE Initialization Protocol (FIP) mode is enabled or disabled.
- **Configure LLDP**—If checked, then Link Layer Discovery Protocol (LLDP) enables all the Data Center Bridging Capability Exchange protocol (DCBX) functionality, which includes FCoE, and priority based flow control.
- **VNTAG Mode**—Specifies if VNTAG mode is enabled or disabled.
- **Port Channel**—Sets the port channel to **Enabled**, **Disabled**, or **Not Applicable** state. For Cisco VIC 1455 and 1457 adapters, the port channel is set to **Enabled** by default. For adapters that do not support port channel configuration, this field is set to **Not Applicable**. vNICs and vHBAs are configured, by default, based on the port channel state selected in this field. The existing configuration is overwritten with the latest configuration when you change the port channel state. When the **Port Channel** field is set to **Enabled** or **Not Applicable**, a minimum of two vNIC(s) (eth0 and eth1) and two vHBA(s) (fc0 and fc1) are configured, by default. If the **Port Channel** field is set to **Disabled**, then a minimum of four vNIC(s) (eth0, eth1, eth2, and eth3) and four vHBA(s) (fc0, fc1, fc2, and fc3) are configured, by default. However, you can create additional vHBAs or vNICs on these adapters.
- **External Ethernet Interface**—Configures the Admin Forward Error Correction (FEC) mode for Cisco VIC 1455, Cisco VIC 1457, Cisco VIC 1495, and Cisco VIC 1497 adapters. By default, four ports are available and you cannot delete them. However, the number of ports configured with the Admin FEC mode is based on the adapter model selected. For example, in a Cisco VIC 1497 adapter, only two ports are available. So, the Admin FEC mode is configured only on the first two ports (port 0 and port1), ignoring the remaining ports (port 2 and port 3).

For existing policies, this field is set to **Auto**. But you can change this value to **cl91**, **cl74**, and **Off**. If the adapter model does not support Admin FEC mode, then these values would be ignored.

Note
The **cl74** option is not supported for Cisco VIC 1495 and Cisco VIC 1497 adapters.

- **vNIC**—Default properties are eth0 and eth1. You can only edit these properties and cannot delete them. These properties are also available for usNIC properties. When the **Port Channel** field is set to **Enabled** or **Not Applicable**, a minimum of two vNIC(s) (eth0 and eth1) are configured, by default, with an uplink port as 0 and 1. If the **Port Channel** field is set to **Disabled**, then a minimum of four vNIC(s), eth0, eth1, eth2, and eth3, are configured, by default, with an uplink port from 0 to 3. However, you can create additional vNICs on these adapters.
- **vHBA**—Default properties are fc0 and fc1. You can only edit these properties and cannot delete them. When the **Port Channel** field is set to **Enabled** or **Not Applicable**, a minimum of two vHBA(s) (fc0 and fc1) are configured, by default. If the **Port Channel** field is set to **Disabled**, then a minimum of four vHBA(s), fc0, fc1, fc2, and fc3, are configured by default. However, you can create additional vHBAs on these adapters.

Step 7 Click **Submit**.

vMedia Policy

You can use Cisco IMC Supervisor to install an OS on the server using the KVM console and VMedia. You can create one or more vMedia policies which contain vMedia mappings for different OS images that match the needs of a server or a set of servers. You can configure upto two vMedia mappings in Cisco IMC Supervisor - one for ISO files (through CDD) and the other for IMG files (through HDD).

For details about configuring the various vMedia properties, see section *Configuring Virtual Media* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a VMedia policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **vMedia Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check the **Enable vMedia** check box to enable vMedia and check the **Enable Virtual Media Encryption** for enabling vMedia encryption.

Step 6 Click **Next**.

Step 7 Check the **Add CDD vMedia Mapping** check box and complete the CDD mapping details.

Step 8 Click **Next**.

Step 9 Check the **Add HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 10 Click **Submit**.

Note

- **Low Power USB State** cannot be configured currently via Cisco IMC Supervisor.
- Applying a vMedia policy removes any existing vMedia mappings previously configured on the server, even if the policy does not contain any vMedia mappings.

Zoning Policy

Zoning policy is used to assign physical drives to a server. The Cisco UCS S3260 dense storage rack servers support dynamic storage of Serial Attached SCSI (SAS) drives in the Cisco Management Controller (CMC). This dynamic storage support is provided by the SAS fabric manager located in the CMC. Dynamic storage supports the following options:

- Assigning physical disks to server 1 and server 2
- Chassis Wide Hot Spare (supported only on RAID controllers)
- Shared mode (supported only in HBAs)
- Unassigning physical disks
- Viewing SAS expander properties
- Assigning physical drives to servers
- Moving physical drives as Chassis Wide Hot Spare
- Unassigning physical drives
- Choosing the controller slot to which you want to assign the chosen physical drive

For details about configuring the various disk group properties, see section *Dynamic Storage* in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers.

Perform the following procedure to create a Zoning policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Zoning Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** window. See Creating a Policy from an Existing Configuration, on page 117.

Note

Zoning Policy is only applicable to Cisco UCS 3260 Rack Server, and the **Cisco UCS S3260** check box in the UI is checked by default.

Step 4 On the **Zoning** page, click + to add local disks that you want to configure on the server.

Step 5 On the **Add Entry to Local Disks** window, enter **Slot Number** where the local disk is present.

Step 6 From the **Ownership** drop-down list, assign the ownership of the local disk to a specific server.

Step 7 Check the **Choose Controller** check box to assign the local disk to a specific controller in the server.

Choosing a controller slot for the local disk is not mandatory. If you do not choose a specific controller slot, the zoning policy is applied to the first controller slot that is available in the server that you selected.

Step 8 From the **Controller Slot** drop-down list, choose a specific controller name of the server.

Step 9 Check the **Force** check box when assigning disks owned by one server to another server.

Step 10 Click **Submit**.

Step 11 On the **Zoning** page, check the **Modify Physical Drive Power Policy** check box to set the policy.

Step 12 Select the power state from the **Physical Drive Power State** drop-down list.

Step 13 Click **Submit**.

Creating a Policy from an Existing Configuration

You can choose to create a policy using a server that you have previously configured. By re-using the existing configuration on a server, you can reduce the time and effort involved in creating similar configurations.

Note When you create a policy from current configuration of a server, the password fields are not retrieved from the server.

Perform the following procedure when you want to create a policy from current configuration of a server.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 Check **Create policy from current configuration of the server** check box and click **Next**.

Step 3 In the **Server Details** screen, you can specify the server details in one of the following methods:

Note
If you are creating a policy for Cisco UCS S3260 servers, go to step 5.

a) Check the **Enter Server Details Manually** check box and fill in the following fields:

1. Enter the IP address in the **Server IP** field.
2. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy on the **Credential Policy Add Form** screen.

3. Enter the server login name in the **User Name** field.
4. Enter the server login password in the **Password** field.
5. Select http or https from the **Protocol** drop-down list.
6. Enter the port number associated with the selected protocol in the **Port** field.

b) Click **Select** and choose a server from where you can retrieve the configurations.

Step 4 Click **Next**.

You will go to the **Main** screen. Continue creating a policy.

Step 5 For Cisco UCS S3260 servers, check both the **Create policy from current configuration of the server** and **Cisco UCS S3260** check boxes and click **Next**.

Attention
You cannot create a power restore policy on Cisco UCS S3260 servers. You can create this policy only for E-series servers.

Step 6 Check the **Enter Server Details Manually** check box in the **Server Details** screen and fill in the following fields or click **Select** to select a Cisco UCS S3260 server to apply the policy to.

a. Enter the Virtual Management IP address in the **Server IP** field for Cisco UCS S3260 platforms.

b. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy in the **Credential Policy Add Form** dialog box.

c. Enter the server login name in the **User Name** field.

d. Enter the server login password in the **Password** field.

e. Select http or https from the **Protocol** drop-down list.

f. Enter the port number associated with the selected protocol in the **Port** field.

Step 7 Select either Server Node 1 or 2 radio buttons.

Step 8 Click **Next**.

You will go to the **Main** screen. Continue creating a policy.

Applying a Hardware Policy

Perform this procedure when you want to apply an existing policy to a server.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Policies**.

Step 3 Select a policy you want to apply.

Step 4 Click **Apply** from the options available at the top.
In the **Apply Policy** screen, you can either choose **Chassis** or **Server(s)** to which you want to apply the policy. These options are displayed based on either the User Administration or Compute Node policy you have selected.

Step 5 Click **Select** to select the chassis or servers to which you want to apply the policy.

Note
On clicking **Select**, all servers such as C-series servers (except Cisco UCS 3260 servers), E-series servers, and ENCS servers are displayed. If you are applying a power policy, the ENCS servers are greyed out and you cannot select these servers. If you have created a power policy for Cisco UCS 3260 servers, then clicking Select will display only Cisco UCS 3260 servers. Other servers are not displayed.

For Cisco UCS 3260 type policies, chassis is shown as Administration policies and server is shown as Compute Node policies. See Policies and Profiles, on page 168.

Step 6 Check the **Schedule Later** check box to schedule the apply policy task at a later time.

Step 7 Select an existing schedule from the **Schedule** drop-down list or click on + create a new schedule. See Creating Schedules, on page 153.

Note
You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to view the scheduled task or click **Remove Scheduled Tasks** to delete scheduled tasks.

Step 8 Click **Submit**.

The process of applying the policy to the specified set of servers begins. This process can take a few minutes depending on the policy type and network connectivity to server(s) to which the policy is being applied.

General Tasks Under Hardware Policies

Perform the following procedure when you want to edit, delete, clone, or view server mapping details of an existing policy.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Policies**.

Step 3 Expand a policy from the left pane and select a policy in the **Hardware Policies** page. Perform the following optional steps:

a) (Optional) To delete a policy, click **Delete**. In the **Delete Policy** dialog box, click **Select** and select the policies you want to delete. Click **Select** and **Submit**.

You can delete one or more selected policies even if you have associated the policy to a server. If you try to delete a policy which is associated to a profile, an error occurs.

b) (Optional) To modify a policy click **Properties** and modify the required properties.

When you modify a policy name, ensure that you do not specify a name which already exists.

c) (Optional) To clone a policy, click **Clone** to copy the details of a selected policy to a new policy.

d) (Optional) Click **View Details** to view the status of the policy you have applied and the server IP address to which you have applied the policy. If the policy is not successfully applied an error message is displayed in the **Status Message** column.

Step 4 To apply a policy to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Hardware Policy, on page 118.

Step 5 Click **Submit** or **Close** if applicable.

Hardware 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.

The following workflow indicates how you can work with a hardware profile in Cisco IMC Supervisor:

1. Create a hardware profile. You can create a profile in one of the following methods:
   a. Create a new profile. For more information about creating a new profile, see Creating a Hardware Profile, on page 121.
   b. Create a profile from the configuration existing on a server. For more information about creating a profile from the configuration existing on a server, see Creating a Profile from an Existing Configuration, on page 121.
2. Apply the profile on a server. For more information about applying a profile, see Applying a Hardware Profile, on page 123.
3. Perform any of the following optional tasks on the profile.
   a. Edit
   b. Delete
   c. Clone

   You can also view the list of servers that are mapped to a specific profile and view details of policies tied to this profile. For more information on performing these tasks, see General Tasks Under Hardware Profiles, on page 123.

Creating a Hardware Profile

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Profiles**.

Step 3 Click **Add**.

Step 4 In the **Hardware Profile** screen, enter a name for the profile that you want to create in the **Profile Name** field.

You can also check **Create profile from current configuration of the server** check box, if you want use the existing server configuration. This takes you to the **Server Details** screen. See Server Details.

Step 5 Check **Cisco UCS S3260** check box if the profile is for a Cisco UCS S3260 server and click **Next**.

Step 6 On the **Profile Entities** window, click **+** to add a profile entry.

You can also click the delete icon to delete existing entries.

Step 7 In the **Add Entry to Profile Name** window, choose **Policy Type**.

Step 8 Select the policy name from the **Policy Name** drop-down list, which lists the names of policies you have already created.

You can click the **+** next to **Policy Name** to create a new policy based on the policy type you selected earlier. See Creating Hardware Policies, on page 89

Step 9 Select the servers to which you want to apply the policy to from the **Apply Policy To** drop-down list.

Step 10 Click **Submit**.

What to do next

You can also edit, delete or clone a profile, or view the server mapped to a selected profile. See General Tasks Under Hardware Profiles, on page 123

Creating a Profile from an Existing Configuration

You can choose to create a profile using a server that you have previously configured. By re-using the existing configuration on a server, you can reduce the time and effort involved in creating similar configurations.



Note When you create a profile from current configuration of a server, the password fields are not retrieved from the server.

Perform the following procedure when you want to create a profile from the current configuration of a server.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Profiles**.

Step 3 Click **Add**.

Step 4 Enter a name for the profile in the **Profile Name** field.

Step 5 Check the **Create profile from current configuration of the server** check box. You can use the server details in the following methods. For Cisco UCS S3260 servers go to step 10.

a) Check the **Enter Server Details Manually** check box and fill in the following fields:

1. Enter the IP address in the **Server IP** field.
2. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy in the **Credential Policy Add Form** dialog box.
3. Enter the server login name in the **User Name** field.
4. Enter the server login password in the **Password** field.
5. Select http or https from the **Protocol** drop-down list.
6. Enter the port number associated with the selected protocol in the **Port** field.
7. Click **Select**, select the policies, and click **Select**.

b) Click **Select** and choose a server from where you can retrieve the configurations.

c) Click **Select**, choose the policies, and click **Select**.

Step 6 Click **Next**.

Step 7 In the **Profile Entities** window, click **+** to add an entry to the profile name.

Click **x** to delete an existing entry from the **Profile Name** table.

Step 8 Click **Submit**.

Step 9 For Cisco UCS S3260 servers, check **Cisco UCS S3260** check box and click **Next**.

a) Check the **Enter Server Details Manually** check box and fill in the following fields:

1. Enter the Virtual Management IP address in the **Server IP** field for Cisco UCS S3260 platforms.
2. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy in the **Credential Policy Add Form** dialog box.
3. Enter the server login name in the **User Name** field.
4. Enter the server login password in the **Password** field.
5. Select http or https from the **Protocol** drop-down list.
6. Enter the port number associated with the selected protocol in the **Port** field.
7. Click **Select**, select the policies, and click **Select**.

b) Click **Select** and choose a server from where you can retrieve the configurations.
c) Click **Select**, choose the policies you want to create from the servers, and click **Select**.

Step 10 Click **Next**.

Step 11 In the **Profile Entities** window, click **+** to add an entry to the profile name.

Click **x** to delete an existing entry from the **Profile Name** table.

Note
For Cisco UCS S3260 profile type, only policies of platform type Cisco UCS S3260 can be added. If the policies are Compute Node type, you must specify the server node in the **Apply Policy To** field. For example, **Server-1**, **Server-2**, and **Both**. For Administration policies this field is not relevant.

Step 12 Click **Submit**.

Applying a Hardware Profile

Perform this procedure when you want to apply a hardware profile to a rack server.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Profiles**.

Step 3 Select an existing hardware profile and click **Apply**.
On the **Apply Profile** screen, you can either choose **Chassis** (applicable for Cisco UCS S3260 type profiles) or **Server(s)** to which you want to apply the profile. These options are displayed based on the server platform you have selected.

Step 4 In the **Apply Profile** screen, click **Select** to select the chassis or servers to which you want to apply the profile.

Step 5 Check the **Schedule Later** check box to schedule the apply profile task at a later time.

Step 6 Select an existing schedule from the **Schedule** drop-down list or click on **+** create a new schedule. See Creating Schedules, on page 153.

Note
You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to view the scheduled task or click **Remove Scheduled Tasks** to delete scheduled tasks.

Step 7 Click **Submit**.

The process of applying a profile to the specified set of servers begins. This process can take a few minutes depending on the profile type and network connectivity to servers to which the profile is being applied.

General Tasks Under Hardware Profiles

Perform the following procedure when you want to edit, delete, clone, or view server mapping details of an existing profile.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Profiles**.

Step 3 Expand the **Hardware Profile** and select a profile. Perform the following optional tasks:

a) (Optional) To delete a profile, click **Delete**. Click **Select** in the **Delete Profile** dialog box, select one or more profiles and click **Select**. Click **Submit** to delete a profile.

You can delete a profile even if it is associated to a server.

b) (Optional) To modify a profile, select a profile, click **Edit** and modify the required properties.

When you modify a profile name, ensure that you do not specify a name which already exists.

c) (Optional) To copy the details of an existing profile to a new profile, click **Clone**.

d) (Optional) To apply a profile to a server or server group, click **Apply**. See Applying a Hardware Profile, on page 123.

e) (Optional) Click **View Details** to view the status of the profile you have applied and the server IP address to which you have applied the profile. If the profile is not successfully applied an error message is displayed in the **Status Message** column.

Step 4 Click **Submit** and/or **Close** if applicable.

Tag Library

Tagging is when you assign a label to an object. As an administrator, you can decide to tag objects such as resource groups and user groups in Cisco IMC Supervisor. You can assign tags to a category such as a rack account. You can also apply a tag to a specific type of account in the selected category.

Tag Library has only one tab which displays the following details:

Field	Description
Name	User defined name of the tag library.
Description	User defined brief description of the tag library.
Type	String or an integer.
Possible Tag Values	User defined tag values.
Applies To	Rack mount servers or users.

Creating a Tag Library

Perform this procedure when you want to create a tag library.

Procedure

Step 1 Choose **Policies** > **Tag Library**.

Step 2 Click **Create**.

Step 3 In the **Create Tag** screen, complete the following fields for **Tag Details**:

Field	Description
Name field	A descriptive name for the tag.
Description field	(Optional) A description of the tag.
Type drop-down list	Select String or Integer.
Possible Tag Values field	The possible values for the tag.

Step 4 Click **Next**.

Step 5 In the **Applicability Rules** pane, complete the following:

Name	Description
Taggable Entities field	Choose the entities on which the tag needs to be applied. To add an entity, do the following: **a.** Click the + icon. **b.** From the **Category** drop-down list, choose the category. It can be one of the following: • **Physical_Compute** • **Administration** **c.** Choose the taggable entities from the table. **d.** Click **Submit**. **Note** The tags are displayed under the respective category according to the set taggable entities.

Step 6 Click **Submit**.

Note
You can perform various tasks such as cloning, editing, deleting, viewing tag and tag association details by clicking on the available options.

REST API and Orchestration

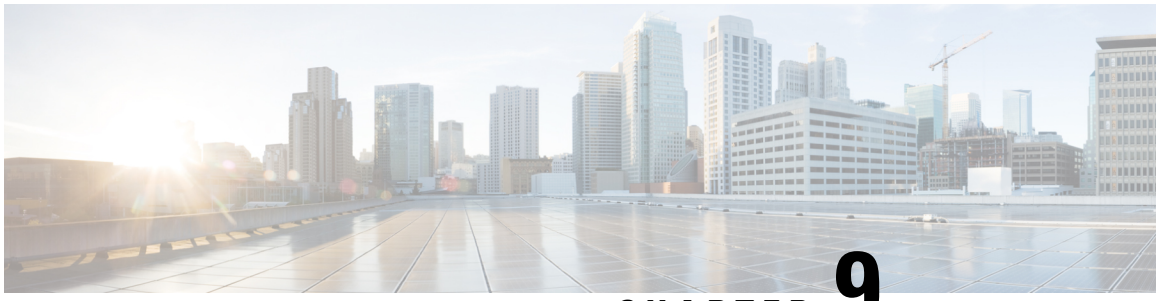
The **REST API Browser** screen lists all the APIs that are provided with Cisco IMC Supervisor that you can use. The APIs are categorized into the following groups:

- Firmware Management Tasks
- General Tasks
- Platform Tasks
- Policy Tasks
- Policy and Profile Tasks
- Server Tasks
- User and Group Tasks

You can use the controls on the screen to perform the following actions:

- Expand and collapse the entire list
- Add this screen to **Favorites**
- Use the **Search** or **Advanced Filter** options to locate a specific API
- Export the report
- Add servers to manage

For more information on how to use these APIs, see *Cisco IMC Supervisor REST API Cookbook* available at: http://www.cisco.com/c/en/us/support/servers-unified-computing/integrated-management-controller-imc-supervisor/products-programming-reference-guides-list.html.



CHAPTER 9

Managing Cisco UCS Hardware Compatibility Report

This chapter contains the following topics:

- Overview, on page 127
- Tagging OS Vendor and Version, on page 128
- Creating Hardware Compatibility Reports, on page 128
- Synchronizing Hardware Compatibility Reports, on page 129

Overview

Cisco UCS Hardware Compatibility Report allows you to check interoperability information for Cisco UCS components and configurations that have been tested and verified by Cisco, Cisco partners, or both. You can run reports and check the status against your current software version or a target software version.

The hardware compatibility report checks the compatibility of the operating systems on servers, and then checks the adapter drivers associated with that operating system.

Cisco IMC Supervisor integrates with the Cisco UCS Hardware Compatibility Report tool to provide information on whether the server, firmware and related components (Storage, Network Adapters, VIC adapters) are supported for a given server model, OS Vendor, Version and processor combination.

Note Cisco UCS Hardware Compatibility Report tool is available only for Cisco C-Series/S-Series servers.

An independent version of this tool is available at https://ucshcltool.cloudapps.cisco.com/public. Cisco IMC Supervisor Connector leverages the REST APIs exposed by this tool to obtain the compatibility report.

To use the Cisco UCS Hardware Compatibility Report tool, you must ensure the following:

- The DNS is properly configured and the url https://ucshcltool.cloudapps.cisco.com/ is reachable from the Cisco IMC Supervisor appliance
- You have entered cisco.com credentials. See Configuring Cisco.com User, on page 34.

Tagging OS Vendor and Version

You must tag the rack server with an Operating System vendor and version. You can select the servers at the system, rack groups or at a rack server level and tag them by performing the following procedure.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Select a rack server under **Rack Servers** or expand **Rack Groups** or rack servers and select the rack server to tag.

Step 3 Click **Manage OS Tag For HCR**.

Note
OS Tags are not applicable for E-Series servers.

Step 4 Select the **Operating System Vendor** from the drop-down list.

Step 5 Select the **Operating System Version** from the drop-down list.

Note
If the OS vendor or the OS version is not listed in the drop-down lists, verify that the DNS is properly configured and the url https://ucshcltool.cloudapps.cisco.com/ is reachable from the Cisco IMC Supervisor appliance. Also, manually run the **Synchronize Hardware Compatibility Reports** system task available from the **Administration** > **System** > **System Tasks** screen.

Step 6 Click **Submit**.

Note
You can select a rack server and click **Delete OS Tag For HCR** to delete the tag you have created.

Creating Hardware Compatibility Reports

Once you have added tags and entered cisco.com credentials, you can generate a compatibility report.

Before you begin

- Ensure you have entered cisco.com credentials before generating the report. See Configuring Cisco.com User, on page 34.
- Ensure that you have tagged the rack server with the operating system vendor and version. See Tagging OS Vendor and Version, on page 128.

Procedure

Step 1 Choose **Policies** > **Hardware Compatibility Report**

Step 2 Click + to create hardware compatibility report.

Step 3 Enter a profile name in the **Select Profile** field.

Step 4 Expand **Choose Server** and select servers for which you want to retrieve configurations.

Step 5 Click **Validate**.

Step 6 Click **Submit**.
On the Hardware Compatibility Report screen, you can view the reports you have created. You can also view the reports by selecting a rack group or rack server and clicking **Hardware Compatibility Reports**.

What to do next

You can select the report you have created and **Delete**, **Edit**, **Synchronize HCL Report** and or **View Status Details**. The report determines if the server is supported and if it is compliant. Compliance can be in any of the following states:

- Fully Compliant—If the server OS Vendor, version or processor and its related components are fully supported.
- Partially Compliant—If a few of the components are found to be unsupported.
- Not Compliant—If there is a compliance error or if the given combination of server or related components are invalid.
- Error or Cannot Determine—If the given server is not tagged or if there is an error while trying to retrieve the response from the backend.

Synchronizing Hardware Compatibility Reports

The **Synchronize Hardware Compatibility Reports** system task runs every week to synchronize the Hardware Compatibility Reports with the backend periodically. Perform this procedure to synchronize the reports manually.

Before you begin

- Configure the URL https://ucshcltool.cloudapps.cisco.com.
- Configure the cisco.com credentials. See Configuring Cisco.com User, on page 34.

Procedure

Step 1 Choose **Administration** > **System**.

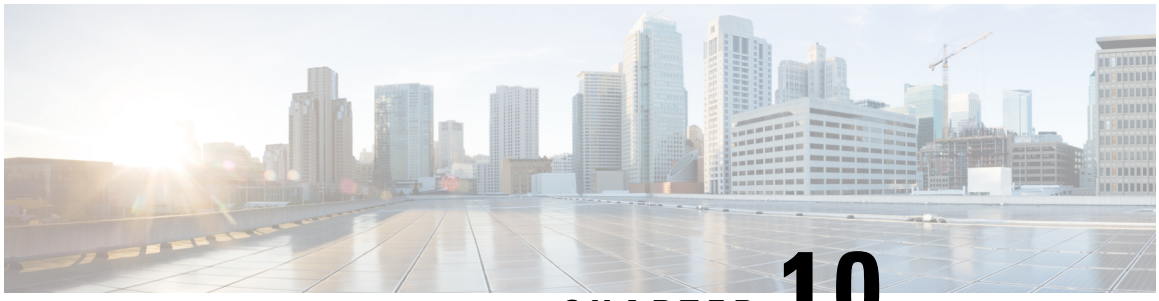
Step 2 On the **System** page, click **System Tasks**.

Step 3 Expand **Rack Server Tasks** and select **Synchronize Hardware Compatibility Reports**.

Step 4 Click **Run Now**.

Step 5 Click **Submit**.

Note
Synchronize HCL Report option is also available to manually synchronize the report from the Hardware Compatibility Report page.



CHAPTER 10

Firmware Profiles

This chapter contains the following topics:

- Firmware Management Menu, on page 131
- Host Image Mapping, on page 139
- Firmware Upgrades From SD Cards, on page 148

Firmware Management Menu

Firmware images may either be uploaded from a local or a network server. The profile name must be unique across both local and network image profiles

Cisco delivers firmware updates in a single bundle to upgrade all Cisco IMC Supervisor components. Firmware updates can be downloaded from cisco.com. You cannot upgrade if a server is not managed in Cisco IMC Supervisor. For downloading the E-Series firmware images you must associate a contract access to the cisco.com account.

Adding Images to a Local Server

Perform this procedure when you want to add a firmware image from your local machine. You cannot perform this task on E-series servers. To add firmware images on E-series servers, see Uploading Images from a Local File System, on page 135.

Note Starting with Cisco IMC Supervisor version 2.2(0.3), to perform firmware upgrade through **Images – Local** or through uploading images from a local file system on Cisco IMC versions prior to 3.0(3e), you must enable HTTP using the Shell menu.

Note Starting with Cisco IMC Supervisor version 2.4(0.0), to download server firmware software from Cisco, you must activate your device first using the **Activate Device** action found under **Images – Local** screen and then proceed to download server firmware software from Cisco by clicking on + icon under **Images – Local screen**.

Device activation stays active for an hour post which re-activation is required to download software again from Cisco.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 Click **Images - Local** tab and click on the **Activate Device** action to activate your device first following the onscreen instructions.

Step 3 Click **+** to add an image. On the **Add Firmware Image - Local** screen, complete the following:

Field	Description
Profile Name field	Enter a descriptive and unique profile name.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server is listed here.
Available Image drop-down list	Choose the .iso image from the drop-down list.
Download Now check box	Check this check box to download the .iso image immediately after adding a profile. If not, you can click on **Download Image** to download the image later.
Graceful Timeout check box	Check this check box to specify a time period within which the host system must shutdown to initiate the firmware upgrade process. **Note** You can configure graceful timeout for systems running Cisco IMC 3.1(3a) or higher. If you do not provide a timeout period, then the system is forcibly shut down after 120 seconds.
Timeout (in mins) field	Specify a time period, in minutes, within which the host system must shutdown to initiate the firmware upgrade process. You can specify a value between 0 and 60.
Force Shutdown Server check box	Check this check box to forcibly shut down the host system if it did not shut down within the time specified in the **Graceful Timeout (in mins)** field. This option is enabled by default.
Allow Downloads for Images having Software Advisory check box	Check this check box to download images that have a software advisory associated with it.
Accept License Agreement	Check this check box to accept the license agreement. Click on the Terms and Conditions link to read the End User License Agreement. **Note** You cannot create a firmware profile without accepting the license agreement even if you want to download the image later.

Step 4 Click **Submit**.

Note

- You can view profile configuration details, modify the firmware image details, and delete the image profile. You can also select multiple profiles concurrently and delete them.
- Cisco IMC Supervisor appliance should be able to remotely map to these images.
- You can select an image from the **Images-Local** window and download the image from cisco.com. For firmware profiles that require images to be downloaded, you can defer and initiate the download process later using the **Download Image** option. You can also delete an image downloaded from cisco.com using the **Delete Image** option.

Adding Images to a Local Cisco UCS Director System



Note Starting with Cisco UCS Director 6.9(0.0), to download server firmware software from Cisco, you must activate your device first using **Activate Device** under the **Images – Local** . Then download server firmware software by clicking the + (plus) icon under **Images – Local** .

Device activation stays active for an hour post which re-activation is required to download software again from Cisco.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Images - Local**.

Step 3 Click **Activate Device**. Follow the on-screen instructions.

Step 4 Click **Add**.

Step 5 In the **Add Firmware Image - Local** screen, complete the required fields, including the following:

Field	Description
Profile Name field	Enter a descriptive and unique profile name. The profile name must be unique across both Local and Network image profiles.
Proxy Configuration check box	(Optional) Check this check box to enable proxy configuration and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.

Field	Description
Platform drop-down list	Choose a platform from the drop-down list. This list displays only those platforms that have at least one server being managed.
Available Image drop-down list	Choose the .iso image from the drop-down list.
Download Now check box	Check this check box to download the .iso image immediately after adding a profile.
Graceful Timeout check box	Check this check box to specify a time period within which the host system must shutdown to initiate the firmware upgrade process. **Note** You can configure graceful timeout for systems running Cisco IMC 3.1(3a) or higher. If you do not provide a timeout period, then the system is forcibly shut down after 120 seconds.
Timeout (in mins) field	Specify a time period, in minutes, within which the host system must shutdown to initiate the firmware upgrade process. You can specify a value between 0 and 60.
Force Shutdown Server check box	Check this check box to forcibly shut down the host system if it did not shut down within the time specified in the **Graceful Timeout (in mins)** field. This option is enabled by default.
Accept License Agreement check box	Check this check box to accept the license agreement. Click on the **Terms and Conditions** link to read the End User License Agreement. **Note** You must accept the license agreement to create a firmware profile, irrespective of the time you choose to download the image.

Step 6 Click **Submit**.

Note

- You can click **View Location Details** to view profile configuration details, click **Modify** to modify the firmware image details, and click **Delete Profile** to delete the image profile. You can select multiple profiles concurrently and delete them.
- For downloading the E-Series firmware images, you must associate a contract access to the cisco.com account.

Uploading Images from a Local File System

Perform this procedure to upload iso images from your local file system to the Cisco IMC Supervisor system.

Note Starting with Cisco IMC Supervisor version 2.2(0.3), to perform firmware upgrade through Images – Local or through uploading images from a local file system on Cisco IMC versions prior to 3.0(3e), you must enable HTTP using the Shell menu.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 Choose **Upload** to add an image.

Step 3 On the **Upload Firmware Image - Local** screen, complete the following:

Field	Description
Profile Name field	Enter a descriptive and unique profile name.
Platform drop-down list	Select the C-Series or E-Series platform.
File field	Select a file and drop it in this field or click **Select a File** to upload on your local file system.
Graceful Timeout check box	Check this check box to specify a time period within which the host system must shutdown to initiate the firmware upgrade process. **Note** You can configure graceful timeout for systems running Cisco IMC 3.1(3a) or higher. If you do not provide a timeout period, then the system is forcibly shut down after 120 seconds.
Timeout (in mins) field	Specify a time period, in minutes, within which the host system must shutdown to initiate the firmware upgrade process. You can specify a value between 0 and 60.
Force Shutdown Server check box	Check this check box to forcibly shut down the host system if it did not shut down within the time specified in the **Graceful Timeout (in mins)** field. This option is enabled by default.

Step 4 Click **Submit**.

Note

- You can view profile configuration details, modify the firmware image details, and delete the image profile. You can also select multiple profiles concurrently and delete them.

- The **Delete Profile** option removes the image associated with the profile. If you uploaded a wrong image or if a file is no longer associated with a profile, a purge system task which runs periodically (once a month) will delete the files from the Cisco IMC Supervisor appliance.

Adding Images from a Network Server

Perform this procedure to add firmware images from a network server by providing the profile name, remote IP, remote filename and so on.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, choose **Images - Network**.

Step 3 Click + to add an image.

Step 4 On the **Add Firmware Image - Network** screen, complete the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile. The profile name must be unique.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server are listed here.
Mount Type drop-down list	Choose either Network File System (NFS), Common Internet File System (CIFS) or HTTP server types.
Remote IP field (only for NFS and CIFS server types)	Enter remote IP address.
Remote Share field (only for NFS and CIFS server types)	Enter remote share path.
Remote File Name field (only for NFS and CIFS server types)	Enter a remote filename. **Note** The remote filename is the Host Upgrade Utility ISO file.
Location Link field (only for HTTP server type)	Enter a valid http/https URL link for the image location.
User Name field	Enter a network path user name.
Password field	Enter a network path password.

Field	Description
Mount Options drop-down list (only for CIFS server type)	Select valid mount options from the **Mount Options** drop-down list. **Note** You can select a mount option for servers that are running Cisco IMC version 2.0(8) and later.
Graceful Timeout check box	Check this check box to specify a time period within which the host system must shutdown to initiate the firmware upgrade process. **Note** You can configure graceful timeout for systems running Cisco IMC 3.1(3a) or higher. If you do not provide a timeout period, then the system is forcibly shut down after 120 seconds.
Timeout (in mins) field	Specify a time period, in minutes, within which the host system must shutdown to initiate the firmware upgrade process. You can specify a value between 0 and 60.
Force Shutdown Server check box	Check this check box to forcibly shut down the host system if it did not shut down within the time specified in the **Graceful Timeout (in mins)** field. This option is enabled by default.

Step 5 Click **Submit**.

Note

- You can view profile configuration details, modify the firmware image details, and delete the image profile. You can also select multiple profiles concurrently and delete them.
- Cisco IMC Supervisor appliance should be able to remotely map to these images.

Upgrading Firmware

Before you begin

- If you are upgrading to Cisco IMC version 2.0(x), you must change the default Cisco IMC password.
- If you are upgrading firmware using a local firmware image profile on servers running Cisco IMC versions prior to 3.0(3e), then you must enable HTTP in Cisco IMC Supervisor. For information on enabling and disabling HTTP using the Cisco IMC Supervisor Shell Admin console, see the Cisco IMC Supervisor Shell Guide, Release 2.2.

Note Cisco does not recommend simultaneous upgrade of both servers that are part of a single Cisco UCS S3260 Dense Storage Rack Server chassis.

Before upgrading Cisco IMC Supervisor and if a firmware profile was already set up, ensure that the CCO credentials and proxy details are configured. See Configuring Cisco.com User, on page 34 and Configuring Proxy Settings, on page 34.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** screen, click **Firmware Upgrades**.

Step 3 Click **Run Upgrade**.
A warning message appears, advising you that running the upgrade on the selected servers will cause the host to reboot into the firmware update tool. On completion of the firmware update, the servers will reboot back to the host OS.

Step 4 Click **OK** to confirm.

Step 5 On the **Upgrade Firmware** screen complete the following:

Field	Description
Select Profile drop-down list	Choose a profile from the drop-down list.
Platform	You can view details such as server platform, firmware image version, and path for the selected firmware profile.
Image Version	
Image Path	
Server(s) button	Click **Select** and choose the servers from the list. The list displays only those servers whose platforms match the one configured in the selected profile.
Schedule later check box	Check this check box and select an existing schedule to run an upgrade. You can also click on the + icon to create a new schedule. For more information on creating schedules, see Creating Schedules, on page 153. You can go to **Policies** > **Manage Schedules**, select a schedule, and click **View Scheduled Tasks** to verify the scheduled task and its progress. You can also select a scheduled task and click **Remove Scheduled Tasks** to remove the associated scheduled task.

Step 6 Click **Submit**.

Note
You can also view firmware upgrade details and delete the status records for the specified upgrade operation.

Host Image Mapping

Host Image Mapping is a commonly used feature for the E-Series servers which allows you to download a firmware file to Cisco IMC, and upgrade the firmware. Using Cisco IMC Supervisor, you can create a host image mapping profile to download and upgrade either one of the following:

- ISO firmware image
- CIMC image or
- BIOS image

You can download the firmware image on Cisco IMC in one of the following methods:

- Provide a location on the network (an FTP, FTPS, HTTP or HTTPS server) where the firmware file is currently available.

  For more information, see Adding a Network Host Image Mapping Profile, on page 139
- Choose the firmware file from a location on your system.

  For more information, see Creating an Upload Profile for Host Image Mapping, on page 142



Important To perform these tasks, Cisco IMC version 3.2.4 must be installed on the E-series servers. This feature does not work with prior versions of Cisco IMC.

For information on creating a profile to upgrade the firmware, see Adding a Network Host Image Mapping Profile, on page 139.

Adding a Network Host Image Mapping Profile

Before you begin

You should have created rack accounts for UCS E-series servers in the system.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Choose **Network Profile**.

Click this button if you have downloaded the firmware image from a location on the network.

Step 4 On the **Create Host Image Mapping Profile - Network** screen, complete the required fields, including the following:

Field	Description

Profile Name field	A descriptive name for the profile.
Platform drop-down list	Choose a server platform. While applying this profile, the list of available servers is populated based on the platform you select in this drop-down list. **Attention** This drop-down list is populated by the rack accounts that you have created for UCS E-series servers.
Download Image From drop-down list	Select the type of server where the firmware image is available. It can be one of the following: • FTP Server • FTPS Server • HTTP Server • HTTPS Server
Server IP Address field	IP address of the server.
File Path field	The path to the location where the fimware file is available.
File Type drop-down list	Choose the file type of the image. It can be one of the following: • **ISO** • **CIMC** • **BIOS**
File Name field	Enter the name of the file.
User name field	The user name. **Note** This field is only displayed when you select **FTP Server** or **FTPS Server** in the **Download Image From** drop-down list.
Password field	The user password. **Note** This field is only displayed when you select **FTP Server** or **FTPS Server** in the **Download Image From** drop-down list.

Map After Download check box	Maps the downloaded image. **Important** This check box is displayed only if you selected **ISO** in the **File Type** drop-down list. You can map the image while creating the profile, or you can map the image at a later point in time. Mapping an ISO image is mandatory for initiating an upgrade on the server. If you have not mapped the image on the server, and attempt to upgrade the firmware, an error message stating that the image is not mapped is displayed.For information on mapping an image in this scenario, see Mapping and Unmapping a Host Image, on page 146.
Delete All Existing Images check box	Deletes all the currently downloaded images available in Cisco IMC of the server chosen for the firmware upgrade.
Run Upgrade After Download check box	Check this check box if you want to initiate the upgrade process immediately after the firmware file is downloaded. If you prefer to initiate the upgrade process manually at a later time, then do not check this check box. To run this process at a later time, see Running a Host Image Upgrade Manually, on page 145. **Important** If you chose **ISO** in the **File Type** drop-down list, and if you check this check box, then you must also check the **Map After Download** check box to proceed. By checking both these check boxes, the firmware file is downloaded and mapped to Cisco IMC.

Step 5 Click **Submit**.

What to do next

After creating a profile, you must select a server on which this profile must run on. For more information, see Applying a Host Image Profile, on page 144.

Following are some of the other actions you can perform after creating a profile:

- Edit or delete a profile
- View status information for a profile
- Initiate the upgrade process if not previously indicated while creating the profile.

Creating an Upload Profile for Host Image Mapping

Follow this procedure to upload a firmware file from your system to Cisco IMC.

Before you begin

You should have created rack accounts for UCS E-series servers in the system.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Choose **Upload Profile**.

Step 4 In the **Create Host Image Mapping Profile – Upload** screen, complete the required fields including the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile. The profile name must be unique.
Platform drop-down list	Choose a platform from the drop-down list. While applying this profile, the list of available servers is populated based on the platform you select in this drop-down list **Attention** This drop-down list is populated by the rack accounts that you have created for UCS E-series servers.
File Type drop-down list	Choose the file type of the image. It can be one of the following: • ISO • CIMC • BIOS
File Name field	Click **Select a File** to browse for and select a file from your system.

Field	Description
Map After Download check box	Maps the downloaded image. **Important** This check box is displayed only if you selected **ISO** in the **File Type** drop-down list. You can map the image while creating the profile, or you can map the image at a later point in time. Mapping an ISO image is mandatory for initiating an upgrade on the server. If you have not mapped the image on the server, and attempt to upgrade the firmware, an error message stating that the image is not mapped is displayed.For information on mapping an image in this scenario, see Mapping and Unmapping a Host Image, on page 146.
Delete All Existing Images check box	Deletes all the currently downloaded images available in Cisco IMC of the server chosen for the firmware upgrade.
Run Upgrade After Download check box	Check this check box if you want to initiate the upgrade process immediately after the firmware file is downloaded. If you prefer to initiate the upgrade process manually at a later time, then do not check this check box. To run this process at a later time, see Running a Host Image Upgrade Manually, on page 145. **Important** If you chose **ISO** in the **File Type** drop-down list, and if you check this check box, then you must also check the **Map After Download** check box to proceed. By checking both these check boxes, the firmware file is downloaded and mapped to Cisco IMC.

Step 5 Click **Submit**.

What to do next

After creating a profile, you must select a server on which this profile must run on. For more information, see Applying a Host Image Profile, on page 144.

Following are some of the other actions you can perform after creating a profile:

- Edit or delete a profile
- View status information for a profile
- Initiate the upgrade process if not previously indicated while creating the profile.

Applying a Host Image Profile

After creating a host image mapping profile, you can select a server on which:

- A profile can be run to download the image to Cisco IMC or
- Firmware upgrade must be initiated immediately, provided you selected the **Run Upgrade After Download** check box while creating the profile.

Note If you do not apply a host image profile, then blank reports are generated when you choose the **View Status** option. Also, you cannot initiate a firmware upgrade without applying a profile, or when the Apply Host Image Profile action is in progress.

Before you begin

You should have created a host image mapping profile in the system.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Select a profile from the table and click **Apply**.

Alternatively, you can select and profile, and choose **Apply** from the **More Actions** drop-down list.

Step 4 In the **Apply Profile** screen, click **Select** to select the servers on which this firmware image must be applied on.

You can select multiple servers. The list of servers is populated based on the server platforms you selected while creating the profile.

Step 5 Click **Select** to return to the **Apply Profile** screen.

Step 6 Check the **Schedule Later** check box to select the date and time on when this process must be completed.

You can either select an existing schedule or click **+** to create a new schedule.

For information on creating a new schedule, see Creating Schedules, on page 153.

Step 7 Click **Submit**.

Downloading a Firmware Image

Complete this procedure to download a firmware image on the Cisco IMC of the server.

Before you begin

You should have created a Cisco.com profile for downloading the firmware image.

- You have created a Cisco.com profile for downloading the firmware image.
- While creating the profile, you have not checked the Download Now check box.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Choose a CCO profile from the list of profiles.

Step 4 From the **More Actions** drop-down list, choose **Download Image**.

Step 5 In the **Download Image** screen, review the information displayed and click **Download**.

The firmware image specified in the profile is downloaded from Cisco.com using the Cisco.com credentials that you configured.

What to do next

At a later point in time, you can delete the image that you have downloaded. For more information, see Deleting a Downloaded Image, on page 146.

Running a Host Image Upgrade Manually

While creating a host image mapping profile, if you did not check the **Run Upgrade After Download** check box, then you manually initiate the upgrade process by completing the following procedure.

Before you begin

You should have created a host image mapping profile in the system.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Choose **Run Upgrade**.

Step 4 In the **Upgrade Host Image** screen, complete the required fields, including the following:

Field	Description
Select Profile drop-down list	Choose a profile. After you choose a profile, the details of the profile are displayed on the screen.
Servers field	Click **Select** to choose the servers on which the upgrade must be run.

Field	Description
Schedule Later check box	Check this check box and select an existing schedule to upgrade the server at a later time, or click + to create a new schedule. For information on creating a new schedule, see Creating Schedules, on page 153.

Step 5 Click **Submit**.

Deleting a Downloaded Image

While creating a Cisco.com profile, you can choose to download the firmware image immediately after creating the profile, or you can download it at a later point in time. After an image is downloaded, you can delete it from the Cisco IMC Supervisor. This option is only available for images downloaded with the Cisco.com profile.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.
Step 2 On the **Firmware Management** page, click **Host Image Mapping**.
Step 3 Choose the CCO profile from the list of created profiles.
Step 4 From the **More Actions** drop-down list, choose **Delete Image**.
Step 5 In the **Delete Image(s)** screen, click **Delete**.

Mapping and Unmapping a Host Image

Complete this procedure to map or unmap a host image on a specific Cisco IMC server. You can map and unmap only an ISO host image. For other host images such as BIOS and CIMC, you can only delete them from this screen.

Before you begin

You should have created a host image mapping profile in the system.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.
Step 2 Expand **Rack Groups** and select the rack group that includes the server.
Step 3 On the selected rack group page, click **Rack Servers**.

Step 4 Double-click the server in the list to view the details, or select the server in the list and click the down arrow on the far right, then choose **View Details**.

Note
You cannot see the down arrow on the far right until you select a server from the list.

Step 5 Choose the **Host Images** tab.

The screen lists all the images that are available on the Cisco IMC server.

Step 6 Choose an ISO host image and select **Map Image** or **Unmap Image** or **Delete Image**.

From this screen, you can only select **Delete Image** for BIOS and CIMC images.

Viewing Status Details of a Host Image Profile

Before you begin

You should have created a host image mapping profile in the system.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Select a profile from the table and choose **View Status Details** from the **More Actions** drop-down list.

You can also select a profile from the table and right-click to choose **View Status Details**.

The **View Host Image Mapping Profile Status** screen displays the following information:

- Profile name
- Server IP address
- Download status
- Upgrade status

  The status information is displayed for an upload profile and for a Cisco.com profile.

Note
If you chose a BIOS file to upgrade the firmware, then you must wait for about 3-4 minutes for the changes to reflect in the Cisco IMC of that server.

Deleting a Host Image Mapping Profile

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Host Image Mapping**.

Step 3 Select a profile from the table and click **Delete Profile**.

Step 4 In the **Delete Profile** screen, click **Delete**.

The profile is deleted from the system.

Firmware Upgrades From SD Cards

As an administrator, you can now perform firmware upgrades on rack servers by downloading ISO images to Miscro SD cards or FlexFlash cards. The user interface provides you with the following options to perform these firmware upgrades:

- **Download Image**—Use this option to download a firmware image for specific servers. You can also choose to initiate the firmware upgrade immediately after the image is downloaded. See Downloading Firmware Image to an SD Card, on page 148.
- **Run Upgrade**—Use this option to initiate a firmware upgrade at a later point in time after the image is downloaded. See Running Firmware Upgrade from an SD Card, on page 149.
- Delete Status Messages—Use this option to delete all firmware upgrade-related status messages from the user interface. See Deleting Image Download Messages, on page 150.

To use these options, you must first create rack accounts in the system, and then create either local image profiles or network image profiles in the system. For more information on creating these profiles, see Adding Images to a Local Cisco UCS Director System and Adding Images from a Network Server, on page 136.

Downloading Firmware Image to an SD Card

Before you begin

- Racks accounts are added in the system.
- Local and network image profiles are created in the system.
- On Cisco UCS M4 servers, ensure that the FlexFlash controller is configured in the Util mode and not the mirror mode. If the controller is configured in the mirror mode, you cannot download the ISO file to the SD card. Use the FlexFlash policy to configure the controller in the Util mode.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 Choose **Firmware Upgrades - SD**.

Step 3 Choose **Download Image**.

Step 4 In the **Download Image** screen, complete the required fields, including the following:

Field Name	Description
Download Image From drop-down list	Choose if you want to use a local profile or a network profile to download the image.
Select Profile drop-down list	Choose a profile from the list. This drop-down list displays profiles for only M4 and M5 servers.
Run Upgrade After Download check box	Check this check box if the firmware upgrade process must be initiated immediately after the image is downloaded. By default, this check box is not checked.
Servers field	Click **Select** to check the check boxes of the servers on which you want the firmware upgrade process to run on. Click **Select** to return to the **Download Image** screen.

Step 5 Click **Submit**.

The firmware image is downloaded to the servers that you selected.

What to do next

Initiate the firmware upgrade on the servers. See Running Firmware Upgrade from an SD Card, on page 149.

Running Firmware Upgrade from an SD Card

Before you begin

You have downloaded the firmware image using the **Download Image** option. See Downloading Firmware Image to an SD Card, on page 148.

Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 Choose **Firmware Upgrades - SD**.

Step 3 Click **Run Upgrade**.

Step 4 Click **Select** to check the check boxes of the servers on which you want the firmware upgrade process to run on.

Step 5 Click **Select**.

Step 6 Click **Submit**.

The firmware upgrade process is initiated on the selected servers. You can review the progress of the upgrade from the **Images -SD** screen. The status is displayed in the **Upgrade Status** column.

Deleting Image Download Messages

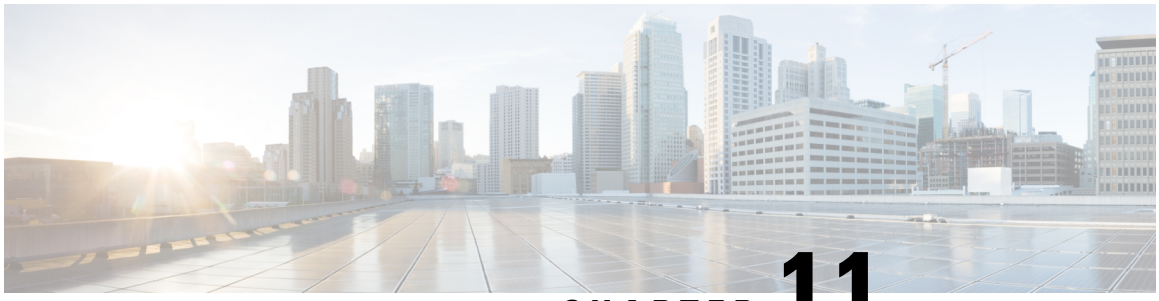
Procedure

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 Choose **Firmware Upgrades - SD**.

Step 3 Choose a profile from the list and click **Delete Status**.

Step 4 In the **Delete Image Download Messages** screen, click **Delete**.



CHAPTER 11

Updating Cisco IMC Supervisor Patches

This chapter contains the following topics:

- Overview of Updating Cisco IMC Supervisor Patches, on page 151
- Checking for Cisco IMC Supervisor Patch Updates, on page 151

Overview of Updating Cisco IMC Supervisor Patches

Automated patch update notifications is available in Cisco IMC Supervisor. Cisco IMC Supervisor periodically (every 14 days) checks for any new patch updates that are available in cisco.com using the Cisco Automated Software Distribution (ASD) service. If there are any patch updates later than the current release, the Cisco IMC Supervisor update manager will download the patch into a location within Cisco IMC Supervisor. For example, if the **Location** displays **/opt/infra/uploads/external/downloads/imcs/<*filename.zip*>**, you can use the **file:////opt/infra/uploads/external/downloads/imcs/<filename.zip>** ftp command in the patch URL. You can then go to the Shell Admin and apply the signed patch. For more information about applying a signed patch, see section *Applying a Signed Patch to Cisco IMC Supervisor* in the Cisco IMC Supervisor Shell Guide. You can also manually check for availability of any new versions using the **Check For Updates Now** option.

Note You will be notified only for new patch updates for the current release. The Cisco IMC Supervisor based update is not applicable for OVF files.

Checking for Cisco IMC Supervisor Patch Updates

Starting with Cisco IMC Supervisor version 2.4(0.0), you must activate your device first using the **Activate Device** action under the **Update IMCS** page. Then you can check for the new version of patch updates using the **Check for Updates Now** action, which will download the new version of patch updates into the Cisco IMC Supervisor appliance.

Note Device activation stays active for an hour , after which re-activation is required to download software again from Cisco.

Procedure

Step 1 Choose **Administration** > **Update IMCS**.

Step 2 On the **Update IMCS** page, click on the **Activate Device** action to activate your device first following the on-screen instructions.

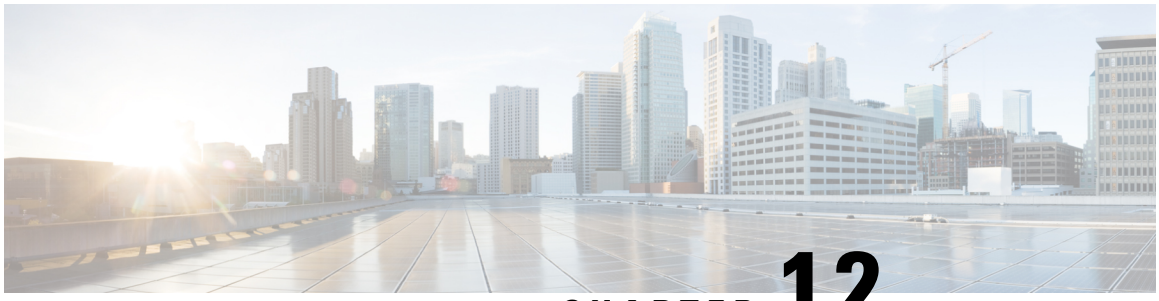
Step 3 After the device is activated, click on the **Check For Updates Now** action button to check for Cisco IMC Supervisor updates.

Step 4 Click **Submit**.
The report displays the latest updates.

Step 5 Click the **Export Report** icon to export the report to either PDF, CSV, or XLS format.

Step 6 Click **Generate Report** to generate a report.

Step 7 Click **Download** to download the report or click **Close**.



CHAPTER 12

Managing Schedules

This chapter contains the following topics:

- Overview of Managing Schedules, on page 153
- Creating Schedules, on page 153

Overview of Managing Schedules

Defining a schedule allows you to defer certain tasks to occur at a different time. For example, tasks such as firmware updates, server discovery, or applying policies and profiles can be scheduled to run at a pre-defined time or at a pre-defined frequency. You could schedule tasks during off-peak hours where the workloads on servers are low.

Creating Schedules

Perform this procedure when you want to create a new schedule.

Procedure

Step 1 Choose **Policies** > **Manage Schedules**.

Step 2 On the **Manage Schedules** page, click **Add**.

Step 3 In the **Create Schedule** dialog box, complete the following:

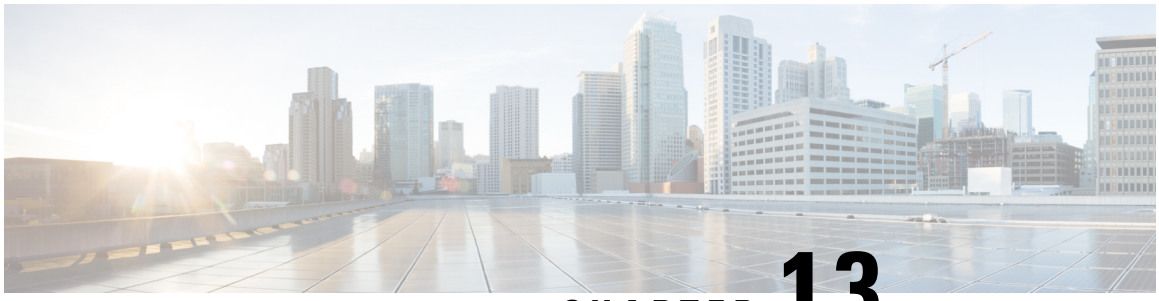
Field	Description
Schedule Name field	Enter a name for the schedule task.
Enable Schedule check box	Check this check box to enable a schedule. By enabling or disabling a schedule (using the **Enable** or **Disable** options), you can enable or disable the tasks associated with the schedule from running.

Field	Description
Scheduler Type radio button	Select a one time schedule or recurring schedule frequency. If you choose a **One Time** schedule, select the date, time, and AM or PM radio buttons. **Note** The schedule time is based on the time on the appliance. However, the time zone is of the local client browser. If you choose a **Recurring** schedule, select the days (0 to 30 days), hours and minutes from the drop-down lists.

Step 4 Click **Submit**.

What to do next

- You can select an existing schedule and modify, delete, or view scheduled tasks. **View Scheduled Tasks** displays a report which allows you to view the status of the upgrade firmware, auto discovery, apply policy and profile tasks you associated with the schedule while Upgrading Firmware, Auto Discovering Servers, Applying a Hardware Policy, on page 118, or Applying a Hardware Profile, on page 123.
- You can select one or more tasks associated with the schedule and disassociate them from the schedule using the **Remove Scheduled Tasks** option.



CHAPTER 13

Running Server Diagnostics

This chapter contains the following topics:

- Overview of Server Diagnostics, on page 155
- **Configuring Server Configuration Utility Image Location** , on page 156
- Running Diagnostics, on page 156

Overview of Server Diagnostics

Server diagnostics is available through UCS Server Configuration Utility (UCS-SCU). You can use diagnostics tools to diagnose hardware problems with your Cisco servers and run tests on various server components to find out hardware issues along with analysis of the test results in a tabular format.

You must download, configure, and save the UCS-SCU image to a remote location.

Note Running a diagnostic test using the UCS-SCU image results in the server being temporarily unavailable as the server reboots with the UCS-SCU image.

Cisco IMC Supervisor gives you the ability to have multiple diagnostic images set up across different geographic locations where the servers are present. Diagnostics run much faster as this facilitates a low latency network between a server and the image within that location.

When you run diagnostics on any rack server, it reboots with the UCS-SCU image hosted on the location you have configured. The diagnostics tabular report displays the status of diagnostics for each server on which you have run diagnostics. Also, details of the server, the date and time the report was generated, diagnostics status and so on are displayed. You can delete or download diagnostic reports for a single or for multiple servers.

Note You must configure the SFTP user password to run server diagnostics. To configure the SFTP user password, see Configuring SFTP User Password, on page 32.

Configuring Server Configuration Utility Image Location

Perform this procedure to configure and save the location of the UCS-SCU image.

Procedure

Step 1 Choose **Systems** > **Server Diagnostics**.

Step 2 Click **SCU Image Profiles**.

Step 3 On the Server Diagnostics page, click +.

Step 4 On the **Configure SCU Image Location** page, complete the following:

Field	Description
Profile Name field	A descriptive name for the profile.
ISO Share Type drop-down list	Choose either Network File System (NFS), Common Internet File System (CIFS), World Wide Web (WWW) or LOCAL share types.
If you select **LOCAL**	
SCU Image field	Browse, select, and upload a SCU image file.
If you select **NFS**, **CIFS**, or **WWW (HTTP/HTTPS)**	
ISO Share IP field	Enter the ISO share IP address.
ISO Share Path field	Enter the ISO share path.
Username field	Enter your ISO share login user name.
Password field	Enter your ISO share login password.

Step 5 Click **Save**.

Running Diagnostics

Perform this procedure when you want to run diagnostics for servers or server groups.

Note If you are running diagnostics using a local SCU image profile on servers that are running Cisco IMC versions prior to 3.0(3e), then you must enable HTTP in Cisco IMC Supervisor. For information on enabling and disabling HTTP using the Cisco IMC Supervisor Shell Admin console, see the Cisco IMC Supervisor Shell Guide, Release 2.2.

Procedure

Step 1 Choose **Systems** > **Server Diagnostics**.

Step 2 Click **Run Diagnostics**.

Step 3 On the **Run Diagnostics** page, complete the following:

Field	Description
Select Profile drop-down list	Select an existing profile from the drop-down list.
Choose drop-down list	Choose whether you want to run the diagnostics on a server or server group from the drop-down list.
Server(s) or **Server Group(s)** drop-down list	Choose the server(s) or server group(s) for which you want to run the diagnostics.

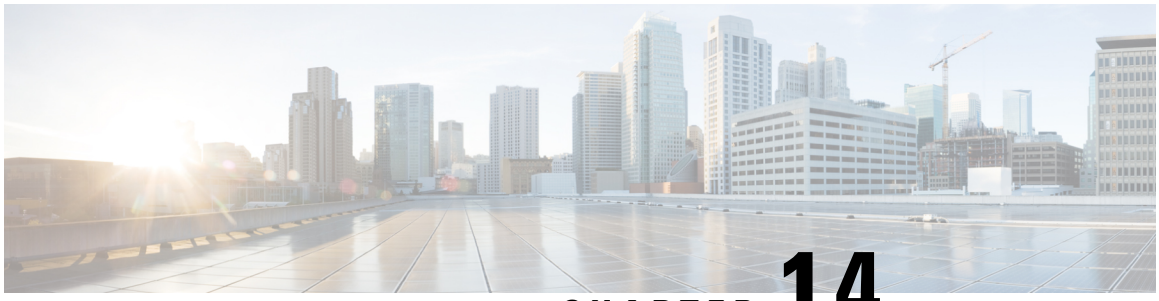
Step 4 Click **Select** and select the server(s) or server group(s) from the **Select** dialog-box.

Step 5 Click **Select**.
The selected server(s) or server group(s) are displayed next to the **Server(s)** or **Server Group(s)** field.

Step 6 Click **Submit**.

Note
You can perform the following actions on a server or multiple servers:

- Select a server and click **View Report** to view reports.
- Select a server or multiple servers and click **Delete Report** to delete reports.
- Select a server or multiple servers and click **Download Report** to download reports. When you select multiple servers to download diagnostics reports, a zip file containing all the reports are downloaded.
- You cannot choose a server which is already running a diagnostics operation. Wait for the diagnostics operation to complete before triggering another diagnostics on this server.
- Diagnostics may take around 40 minutes to complete. This varies depending on the number of components present in the server.



CHAPTER 14

Smart Call Home for Cisco IMC Supervisor

This chapter contains the following topics:

- Overview of Smart Call Home, on page 159
- Configuring Smart Call Home, on page 159
- Fault Codes, on page 160

Overview of Smart Call Home

Cisco Smart Call Home is an automated support capability that provides continuous monitoring, proactive diagnostics, alerts, and remediation recommendations on select Cisco devices. Smart Call Home can help identify and resolve issues quickly to achieve higher availability and increased operational efficiency. This capability is available with an active support contract for hardware managed by Cisco IMC Supervisor. When enabled, Smart Call Home looks for a specific set of faults that Cisco has identified through interaction with Cisco Technical Assistance Center (TAC) engineers, the Cisco support community, and developers. Instead of waiting for a user to notice a problem or a fault to escalate and be reported, Smart Call Home proactively identifies and diagnoses faults.

Cisco IMC Supervisor managed server tasks such as **Group Rack Server Inventory**, **Rack Server Fault**, and **Health System** are run at periodic intervals and send relevant information to the Smart Call Home backend. The backend processes this data and if issues are identified, it will automatically raise cases with the TAC for resolution of issues.

You can configure Smart Call Home using the Cisco IMC Supervisor user interface. For more information, see Configuring Smart Call Home, on page 159.

Configuring Smart Call Home

Perform this procedure to configure Smart Call Home.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Smart Call Home**.

Step 3 Check the **Enable Smart Call Home** check box so that collected faults are forwarded to the Smart Call Home backend.

Note
By default, Smart Call Home is disabled.

Step 4 Enter **Contact Email** address.

Note
You can enter only one contact email at a time in this field.

Step 5 The **Destination URL** of the Smart Call Home backend is set by default.

Note
- We recommend that you must not change the default URL.
- The **Proxy Configuration** check box is selected by default. Smart call home uses the proxy details that you have already set. See Configuring Proxy Settings, on page 34.

Step 6 (Optional) Check the **Send Group Inventory Now** check box to send inventory details of the servers. One inventory message per managed server is sent to the Smart Call Home backend. This can be used as additional information for resolving issues by the TAC team.

Step 7 Click **Save**.

Note
- Any faults that occur on the managed servers are sent to the backend. For various fault codes and its severity, see Fault Codes, on page 160. For logging in to Smart Call Home and performing various tasks, see information on the Cisco Smart Call Home Community.

Fault Codes

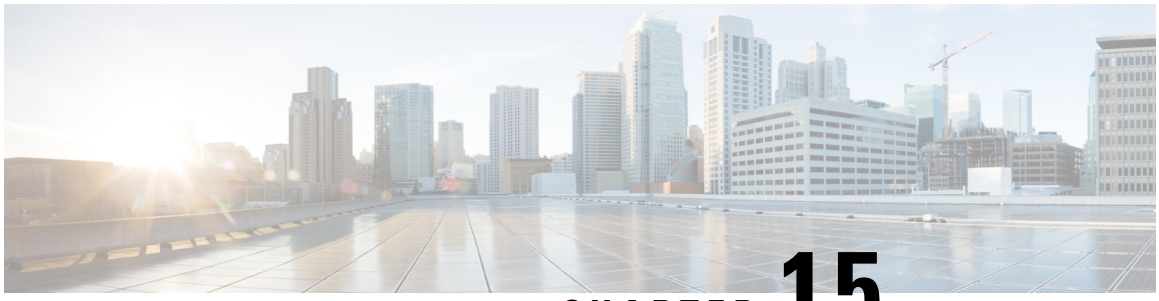
Fault Codes in Smart Call Home

Following are a list of error messages that Cisco IMC Supervisor sends to the Smart Call Home backend.

Fault Code	Fault Name	Message	Severity	Create Service Request
F0174	fltProcessorUnitInoperable	Processor [id] on [serverId] operability: [operability]	critical|major	Y
F0177	fltProcessorUnitThermalThresholdNonRecoverable	Processor [id] on [serverid] temperature:[thermal]	critical	Y

Fault Code	Fault Name	Message	Severity	Create Service Request
F0181	fltStorageLocalDiskInoperable	Local disk [id] on [serverid] operability: [operability]	major| warning	Y
F0185	fltMemoryUnitInoperable	DIMM [location] on [serverid] operability: [operability]	major	Y
F0188	fltMemoryUnitThermalThresholdNonRecoverable	DIMM [location] on [serverid] temperature: [thermal]	critical	N
F0379	fltEquipmentIOCardThermalProblem	IOCard [location] on server [id] operState: [operState]	major	N
F0385	fltEquipmentPsuThermalThresholdNonRecoverable	Power supply [id] in [serverid] temperature: [thermal]	critical	Y
F0389	fltEquipmentPsuVoltageThresholdCritical	Power supply [id] in [serverid] voltage: [voltage]	major	N
F0391	fltEquipmentPsuVoltageThresholdNonRecoverable	Power supply [id] in [serverid] voltage: [voltage]	critical	Y
F0407	fltEquipmentPsuIdentity	Power supply [id] on [serverid] has a malformed FRU	critical	N
F0411	fltEquipmentChassisThermalThresholdNonRecoverable	Thermal condition on [serverid] cause: [thermalStateQualifier]	critical	N
F0424	fltComputeBoardCmosVoltageThresholdCritical	CMOS battery voltage on [serverid] is [cmosVoltage]	major	N
F0425	fltComputeBoardCmosVoltageThresholdNonRecoverable	CMOS battery voltage on [serverid] is [cmosVoltage]	critical	Y
F0531	fltStorageRaidBatteryInoperable	RAID Battery on [serverid] operability: [operability]	major	Y

Fault Code	Fault Name	Message	Severity	Create Service Request
F0868	fltComputeBoardPowerFail	Motherboard of [serverid] power: [power]	critical	N
F0997	fltStorageRaidBatteryDegraded	Raid battery [id] on [serverid] operability: [operability]	major	N
F1004	fltStorageControllerInoperable	Storage Controller [id] operability: [operability]	critical	N
F1007	fltStorageVirtualDriveInoperable	Virtual drive [id] on [serverid] operability: [operability]	critical	N



CHAPTER 15

Managing Cisco UCS S3260 Dense Storage Rack Server

This chapter contains the following topics:

- About Cisco UCS S3260 Dense Storage Rack Server, on page 163
- Cisco UCS S3260 Dense Storage Rack Server Architectural Overview, on page 164
- Cisco IMC Supervisor with Cisco UCS S3260 Dense Storage Rack Server, on page 165
- Adding a Rack Account, on page 165
- Managing Cisco UCS S3260 Rack Server, on page 166
- Policies and Profiles, on page 168
- Upgrading Firmware, on page 169
- Viewing Cisco UCS S3260 Dense Storage Rack Server Details, on page 169

About Cisco UCS S3260 Dense Storage Rack Server

The Cisco UCS S3260 is a dense storage rack server that supports dual server nodes. It can also have one optimized for large datasets used in environments such as Big data, cloud, object storage, and content delivery. It belongs to the Cisco UCS C-Series rack-mount servers product family.

The Cisco UCS S3260 Dense Storage Rack Server is designed to operate in a standalone environment and as part of the Cisco Unified Computing System with Cisco IMC Supervisor integration. The Cisco UCS S3260 Dense Storage Rack Server includes the following features:

- Enterprise-class redundancy with full featured Redundant Array of Independent Disks (RAID) plus Just a Bunch of Disks (JBOD)
- Standalone management interface (Cisco Integrated Management Controller)
- No data migration required when replacing or upgrading server nodes
- No need for extended depth racks

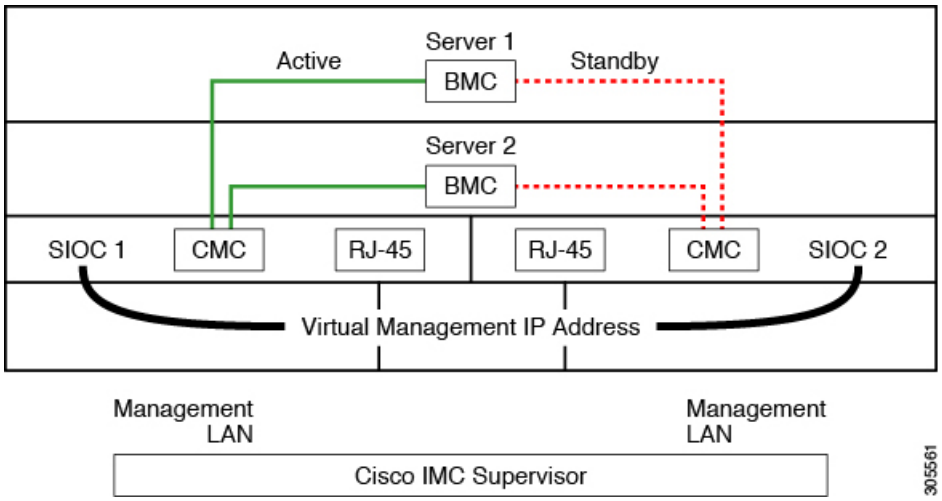
For more information about Cisco UCS S3260 dense storage rack server, see Cisco UCS S3260 Rack Server.

Cisco UCS S3260 Dense Storage Rack Server Architectural Overview

Architectural Overview

The Cisco UCS S3260 uses a modular server architecture that, using Cisco's blade technology expertise, allows you to upgrade the computing or network nodes in the system without the need to migrate data from one system to another. It delivers:

- Dual server nodes
- Up to 24 computing cores per server node
- Up to 60 drives mixing a large form factor (LFF) with up to 14 solid-state disk (SSD) drives plus 2 SSD SATA boot drives per server node
- Up to 512 GB of memory per server node (1 terabyte [TB] total)
- Support for 12-Gbps serial-attached SCSI (SAS) drives
- A system I/O Controller with Cisco VIC 1300 Series Embedded Chip supporting Dual-port 40Gbps
- High reliability, availability, and serviceability (RAS) features with tool-free server nodes, system I/O controller, easy-to-use latching lid, and hot-swappable and hot-pluggable components



The system uses a chassis management controller (CMC) to manage the server nodes. Each system I/O controller (SIOC) module contains an onboard CMC. If you have two SIOCs, the two CMCs act in an active/standby organization. The CMC in the SIOC that you log into with the Cisco IMC interface becomes the active CMC and it allows you to manage the BMCs in both server nodes.

When you connect to the system to manage the server nodes' BMCs via the Cisco IMC interface, you physically connect to the management port (RJ-45) on a SIOC. When you log into the Cisco IMC interface, you use the Virtual Management IP address that has been assigned to the CMC in that SIOC.

All user interfaces run only on the active CMC. Configuration changes are automatically synchronized between the active and standby CMCs.

When you power-cycle the system, the CMC in SIOC 1 is the active CMC by default. The active CMC will fail over to the standby CMC when any of the following conditions occur:

- The active CMC is rebooted or fails.
- The SIOC with active CMC is removed.
- Network connectivity is lost on the active CMC.

For configuring the S3260 rack server, see Cisco UCS S3260Rack Server Specification Sheet.

Cisco IMC Supervisor with Cisco UCS S3260 Dense Storage Rack Server

Cisco IMC Supervisor-Managed Dense Storage Rack Servers support all features that come along with C-Series Rack Servers. It also provides additional reports for the These features and concepts are detailed in the following sections:

- Overview —Provides detailed information about the architecture of Cisco UCS S3260, and its connectivity when managed through Cisco IMC Supervisor.
- Adding a Rack Account—Describes, and provides detailed information about adding a Cisco UCS 3260 chassis rack account.
- Managing Chassis—Describes, and provides detailed information about the management of the Dense Storage Rack Chassis.
- Policies and Profiles— Describes, and provides detailed information about the Cisco UCS 3260 chassis related policies and profiles.
- Upgrading Firmware—Provides detailed information about Chassis Firmware Packages and the endpoints of Cisco UCS S3260 on which firmware can be updated manually.
- Viewing Cisco UCS S3260 rack server details—View details such as PSUs, VIC Adapters, Chassis Summary, and SAS Expander.

Adding a Rack Account

To add a rack account you can now provide a Virtual Management IP in the **Server IP** field. For more information about adding a rack account, see Adding a Rack Account, on page 51. You can view the servers managed by the Cisco UCS S3260 Rack Server after inventory collection from the **Rack Servers** tab.

Note If you add a CMC 1 or CMC 2 IP address, an error occurs.

Managing Cisco UCS S3260 Rack Server

Restarting Chassis Management Controller

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Rack Groups** page, click **Chassis**.

Step 3 Click **Reboot CMC**.

Step 4 On the **Reboot Chassis Management Controller** window, select either **CMC1** or **CMC2**.

Step 5 Click **Submit**.
The chassis you have selected, restarts.

Tagging Assets for Cisco UCS S3260 Rack Server

Asset tag is a user-defined tag for the server. You can use the **Asset Tag** option to add the Cisco IMC server property through Cisco IMC Supervisor

You can tag assets for both rack servers and for chassis. To tag assets for a rack-mount server, see Tagging Assets for a Rack Mount Server, on page 72. Perform this procedure when you want to tag an asset for chassis.

Before you begin

The server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Rack Groups** page, click **Chassis**.

Note
You can also select any sub group under **Rack Groups** in the **Inventory and Fault Status** pane.

Step 3 From the list of chassis, select the chassis you want to tag.

Step 4 From the **More Actions** drop-down list, choose **Asset Tag**.

Note
You cannot see the **Asset Tag** option until you select the server from the list.

Step 5 Click **Submit**.

Note

The **Asset Tag** option is available only from Cisco IMC release 3.0.(1c) onwards. For lower version platforms, the **Asset Tag** column in the **Rack Groups** page displays a blank entry.

Setting Front Locator LED for Cisco UCS S3260 Rack Server

A server locator LED helps you to identify a specific server among many servers in a data center. Perform this procedure when you want to turn on or turn off the front locator LED for a selected chassis.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 On the **Rack Groups** page, click **Chassis**.

Step 3 Click **Front Locator LED**.

Step 4 From the **Turn the Front Locator LED for selected chassis on/off** drop-down list, choose **ON** or **OFF**.

Step 5 Click **Submit**.

Managing Tags for Cisco UCS S3260 Rack Server

Tagging is used to assign a label to an object, such as a resource group, Cisco UCS S3260 Dense Storage Rack Server, or a rack-mount server. Tags can be used to provide information such as rack locations, responsible support groups, purpose, or Operating System. For information about adding or modifying tags for Cisco UCS S3260 Dense Storage Rack Server or for rack-mount server, see Managing Tags for a Rack-Mount Server, on page 78.

Note You can manage tags for aserver only when the server is included as a Rack Account within a Rack Group.

Adding Tags for Cisco UCS S3260 Rack Server

Tagging is used to assign a label to an object, such as a resource group or a rack server. Tags can be used to provide information such as rack locations, responsible support groups, purpose, or operating system. Perform this procedure to add tags to a Cisco UCS S3260 Rack Server.

Before you begin

The server is already added as a rack account under a rack group.

Note You can also select multiple rack servers.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Click **Add Tags**.

Note
You cannot see **Add Tags** button till you select the server from the list.

Step 3 Choose the **Tag Name** from the drop-down list.

Step 4 Choose the **Tag Value** from the drop-down list.

Step 5 Click on the plus icon to create a new tag. See Managing Tags for Cisco UCS S3260 Rack Server, on page 167 to create tags.

Note
You can also edit, delete, and view tag details.

Policies and Profiles

Cisco IMC Supervisor includes a new **Cisco UCS S3260** option to create Cisco UCS S3260 chassis policies and profiles where you can add the chassis information.

These new chassis policies will be known as the User Administration policies and the existing rack mount server policies will be known as the Compute Node policies in this document. You can view the differentiated User Administration policies and Compute Node policies listed in the **Hardware Policies** table. The Server Platform for User Administration policies are displayed as **Cisco UCS S3260** and Compute Node policies are displayed as **All C-Series and E-Series except Cisco UCS S3260**.

The policies and profile reports have a column **Server Platform** indicating if the policy is Cisco UCS S3260 or others. Chassis policies irrespective of User Administration Policies or Compute Node polices are displayed as **Cisco UCS S3260**. For the other C-Series and E-Series platforms or non Cisco UCS S3260 policies it is displayed as **All C-Series and E-Series except Cisco UCS S3260**.

You can either create a Cisco UCS S3260 chassis profile or a rack-mount server profile. Selecting a Compute Node policy allows you to choose the server nodes where you want to apply the policy.

Applying a Policy

To apply a policy you have created, select from a list of Cisco UCS 3260 Rack Servers and Rack Mount servers. You can either select a Cisco UCS S3260 chassis or a rack-mount server based on the selected server platform. For more information about creating and applying policies, see Hardware Policies, on page 88.

The following policies are User Administration Policies and Compute Node policies:

User Administration Policies	Compute Node Policies
User	BIOS
SNMP	Precision Boot Order

User Administration Policies	Compute Node Policies
LDAP	RAID
NTP	KVM
Network Security	vMedia
SSH	VIC
NTP	Serial Over LAN

Note

- IPMI Over LAN and Network Policy have a mix of both BMC and CMC configuration details for Cisco UCS 3260 Rack Server.
- Zoning Policy is only applicable to Cisco UCS 3260 Rack Server. Hence, the **Cisco UCS S3260** check box in the UI is checked.
- Legacy Boot Order and Flex Flash policies are not applicable for Cisco UCS 3260 Rack Server.

Applying a Profile

To apply a Cisco UCS S3260 profile you have created, select from a list of Cisco UCS 3260 Rack Servers. You can only select a Cisco UCS S3260 chassis. Only Cisco UCS S3260 policies can be added to the profile. For Compute Node Policies, you can choose the **Apply Policy To** field to indicate the server node to which the policy should be applicable while applying a profile. For more information about creating and applying profiles, see Hardware Profiles, on page 120.

Upgrading Firmware

Cisco IMC Supervisor firmware upgrade can be performed at a server level. However, during server upgrade, the chassis components as well as the Hard Disk Drive components associated with the server are upgraded too. When you upgrade a server, the chassis and disk drive firmware are automatically updated. For more information about upgrading firmware, see Upgrading Firmware, on page 137.

Note You can upgrade only one server node at a time.

Viewing Cisco UCS S3260 Dense Storage Rack Server Details

Perform this procedure when you want to view the details for a Cisco UCS S3260 Dense Storage Rack Server, such as PSUs, VIC Adapters, Chassis Summary, and SAS Expander.

Before you begin

Ensure that the server is already added as a Rack Account under a Rack Group.

Procedure

Step 1 Choose **Systems** > **Inventory and Fault Status**.

Step 2 Expand **Rack Groups** and select the rack group that contains the Cisco UCS S3260 Dense Storage Rack Server.

Step 3 On the **Rack Groups** page, click **Chassis**.

Step 4 Double-click the Cisco UCS S3260 Dense Storage Rack Server in the list to view the details, or click the Cisco UCS S3260 Dense Storage Rack Server in the list and then choose **View Details**.

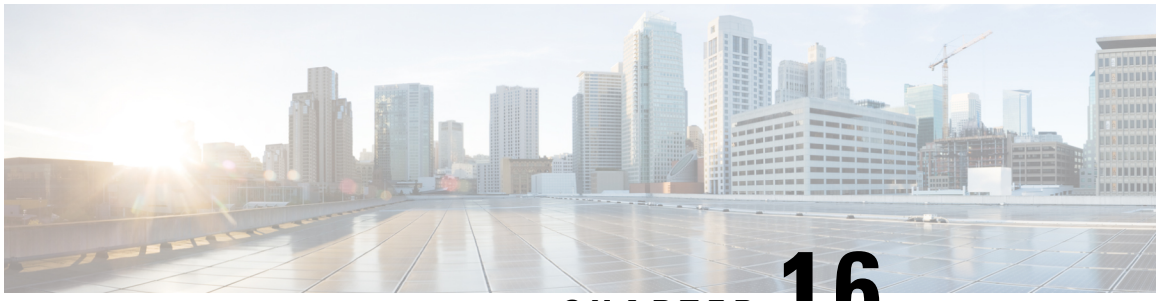
Note
You cannot see the **View Details** option until you select a Cisco UCS S3260 Dense Storage Rack Server from the list.

The following details are available for a Cisco UCS S3260 Dense Storage Rack Server:

Tab	Description
PSUs	The details of the power supply unit used in the server. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
VIC Adapters	The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click **View Details** to view information such as **External Ethernet Interfaces** and **VM FEXs**.
Communication	The information on the protocol, such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.
Remote Presence	The details of vKVM, Serial Over LAN, and vMedia.
Faults	The details of the faults logged in the server.
Users	The details about users under **Default Group**. You can also view the strong password policy and password expiration details that you have set while creating a user policy and password expiration policy respectively. See, User Policy, on page 112 and Password Expiration Policy, on page 104. **Note** • Not applicable for Cisco UCS S3260 dense storage rack server. • You can view **Users** at the chassis level and not at the server level.
Cisco IMC Log	The details of the Cisco IMC logs for the server. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.

Tab	Description
System Event Log	The details of the server logs. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Fault History	Historical information on the faults that occurred on the server.
Tech Support	Details about the tech-support log files, such as the file name, destination type, and status of the upload are displayed in the **Tech Support** table. An option to export the tech-support log files to a remote server or on the local Cisco IMC Supervisor appliance is available. For more information about exporting, see Exporting Technical Support Data to a Remote Server, on page 81. **Note** Not applicable for Cisco UCS S3260 dense storage rack server.
Associated Hardware Profiles	Details of policies that are associated to a hardware profile.
Chassis Summary	Summary of properties such as CMC 1 network, common, and NIC.
Rack Servers	Rack server details such as hostname, IP address, and connection status.
System IO Controller	Details such as IP address, MAC address, and firmware version.
SAS Expander	Details such as ID, SAS name, and firmware version.
Zoning	Details such as health, presence, ownership, and size.

Step 5 Click the **Back** button on the far right to return to the previous window.



CHAPTER 16

Viewing Support Information

This chapter contains the following topics:

- Support Information, on page 173

Support Information

Cisco IMC Supervisor support provides basic and advanced system information, displaying and downloading logs. It also allows you to record debug logging and download API logs.

Viewing Support Information

You can use this procedure to view the support information for Cisco IMC Supervisor.

Before you begin

Ensure that the pop-up blocker is disabled for your web browser.

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 In the **Support Information** window, you can view:

Table 2: System information (basic)

Field	Description
Support Information drop-down list	Choose **System Information (Basic)** and click **Submit** to view basic information.

Table 3: System information (advanced)

Field	Description
Support Information drop-down list	Choose **System Information (Advanced)** and click **Submit** to view advanced information such as processor, memory, disk information and so on.

Table 4: View Logs

Field	Description
Support Information drop-down list	Choose **Show log**.
Show Log drop-down list	Choose the log type you want to view and click **Show Logs**.

Table 5: Download All Logs

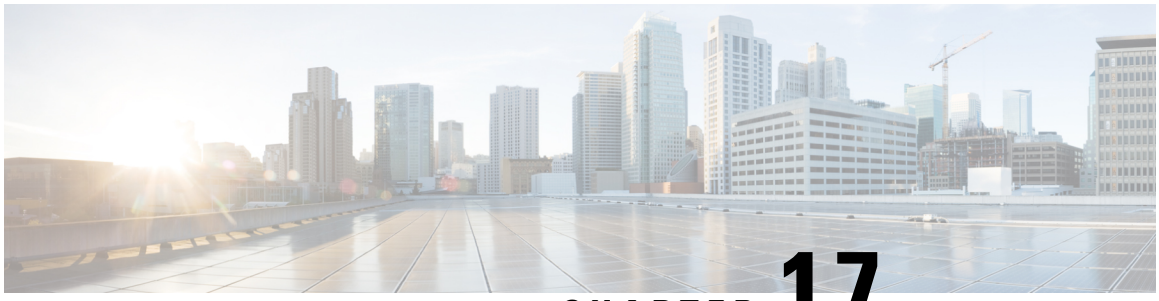
Field	Description
Support Information drop-down list	Choose **Download All Logs** and click **Download**.

Table 6: Download Debug Logging

Field	Description
Support Information drop-down list	**a.** Choose **Debug Logging** and click **Start Debug Logging**. **b.** To stop and download log data, click **Stop Debug Logging** and click the download debug link.

Table 7: API Logging

Field	Description
Support Information drop-down list	**a.** Choose **API Logging** and click **Start API Logging**. **b.** To stop and download log data, click **Stop API Logging** and click the download API debug logs link.



CHAPTER 17

Frequently Performed Tasks and Procedures

This chapter contains the following topics:

- Frequently Performed Procedures, on page 175
- Miscellaneous Procedures, on page 175

Frequently Performed Procedures

This section provides a quick access to frequently performed procedures in Cisco IMC Supervisor. The reference directs you to the section of the document where the detailed procedures has already been described.

Procedure	Reference
How to log in Cisco IMC Supervisor	Launching Cisco IMC Supervisor, on page 14
How to upgrade license	Updating the License, on page 15
How to add login users in Cisco IMC Supervisor	Creating a User Account, on page 40
How to add a rack group	Adding a Rack Group, on page 51
How to create a rack account	Adding a Rack Account, on page 51

Miscellaneous Procedures

The following sections include miscellaneous procedures that you would perform using Cisco IMC Supervisor.

Enabling Dashboard View

Perform this procedure to enable the dashboard view in the Cisco IMC Supervisor menu bar.

Procedure

Step 1 Click the username with which you logged in to the application. The username is on the far right of the application header.

Step 2 In the **User Information** window, click **Dashboard**.

Step 3 Check the **Enable Dashboard (in the top level menu)** check box to enable the dashboard.

Step 4 Click **Apply** and close the window.

Note
You can see the **Dashboard** tab in the menu bar.

Creating Additional Dashboards

Before you begin

You should have enabled the **Dashboard** in the user interface.

Procedure

Step 1 Log into Cisco IMC Supervisor user interface.

The default **Dashboard** screen is displayed.

Step 2 Click the + icon to create a new dashboard.

Step 3 Enter the name of the dashboard.

Step 4 Set **Automatic Refresh** to **ON** if you want to automatically refresh the reports on the dashboard.

Step 5 Set the **Interval** in minutes. The reports in the dashboard will be refreshed based on the interval you set here.

Step 6 Set the **Widget Size** for dashboard widgets.

Step 7 Click **Submit**.

Enabling Dashboard Auto Refresh

Perform this procedure to enable auto refreshing for the reports added on the dashboard. You can also define the refresh rate.

Procedure

Step 1 From the menu bar, choose **Dashboard**.

Step 2 In the **Dashboard** panel, beside the **Automatic Refresh** option, click **OFF**.

Automatic Refresh option changes to **ON** and **Interval** slide bar is visible.

Step 3 Using the **Interval**, set the refresh rate.

Note
You can set the refresh rate in multiples of 5 minutes up to a maximum of 60 minutes.

Adding Summary Reports to Dashboard

Perform this procedure to add a summary report to dashboard for quick access.



Note Only summary reports can be added to dashboard.

Procedure

Step 1 Browse to the summary report you want to add to the dashboard.

Step 2 Click the down arrow on the right upper corner of the report panel.

Step 3 Click **Add to Dashboard**.

Note
Add to Dashboard option is available only if the summary report supports dashboard view.

Step 4 From the menu bar, choose **Dashboard** and verify that the report appears on the dashboard.

Deleting a Dashboard

You cannot delete the default dashboard.

Procedure

Step 1 Log into Cisco IMC Supervisor user interface.

The default **Dashboard** screen is displayed.

Step 2 Click the drop-down list to view the list of dashboards that you have created.

Step 3 Click the **X** mark displayed next to the dashboard name.

Step 4 Confirm that you want to delete the dashboard.

A message confirming that the dashboard has been deleted is displayed.

Adding a Menu or Tab to Favorites

Perform this procedure to add a menu option or tab to **Favorites** menu.

Procedure

Step 1 Browse to the menu or tab you want to add to **Favorites** menu.

Step 2 Click **Favorite**.

Note
You can see the **Favorite** button only if the menu or tab supports it.

Step 3 In the **Favorite Report** dialog box, you may edit the **Menu Label** field.

Step 4 Click **Save**.

Step 5 From the menu bar, choose **Favorites** and verify the new menu is visible.

Favorites

Cisco IMC Supervisor allows you to mark any screen that displays a tabular report as a favorite. Choosing **Favorites** on the menu bar allows you to view the list of screens that you have identified as a favorite, and navigate to those screens quickly.

Customizing Report Table View

Perform this procedure to add or remove any field in a report table.

Before you begin

If any window supports customizing the table, it will display the **Customize Table View** icon on the far right of the page.

Procedure

Step 1 Locate and click the **Customize Table View** icon on the far right of the page.

Step 2 In the **Customize Report Table** dialog box, you may do the following:

- To display any field in the table report, check the checkbox against that field.
- To remove any field from the table report, uncheck the checkbox against that field.
- To reset to default table view, click **Reset to Default**.

Step 3 Click **Save**.

Filtering Reports

Perform this procedure to filter the data based on user defined criteria.

Before you begin

If any window supports filtering the data, it will display the **Add Advanced Filter** icon on the far right of the page.

Procedure

Step 1 Locate and click the **Add Advanced Filter** icon on the far right of the page.
Every time you click the icon, it adds a filter criteria on top of the report table.

Step 2 In the **Match Condition** drop-down list, choose **Match All Conditions** or **Match Any Condition** as required.

Step 3 In **Search in Column** drop-down list, choose the field based on which you want to filter the data.

Step 4 In **Text** field, enter a value based on which you want to filter the data.

Step 5 If you have more than one filter criterion, then repeat Step 3 and Step 4 for all the criteria.

Step 6 Click **Search**.

Exporting a Report

Perform this procedure to export the report data based in PDF, CSV, or XLS format.

Before you begin

If any window supports exporting the report data, it will display the **Export Report** icon on the far right of the page.

Procedure

Step 1 Locate and click the **Export Report** icon on the far right of the page.

Step 2 In the **Export Report** dialog box, complete the following:

a. From **Select Report Format** drop-down list, choose PDF, CSV, or XLS.

b. Click **Generate Report**.

c. Once the report is generated, click **Download**.

Report is generated in the selected format in a new window.

Step 3 In the **Export Report** dialog box, click **Close**.

Viewing System Information

The **System Information** screen displays information on the following:

- Primary node
- Service nodes
- DB nodes
- System memory
- System disk

From this screen you can either refresh the data on the screen, or edit the number of reports displayed on the screen.

Site Map

The **Site Map** option allows you to see all the main options available to you in the Cisco IMC Supervisor user interface. From this screen, you can choose an option, and navigate directly to the relevant screen. For example, from the **Site Map** screen, you can choose **Firmware Management**, listed under **Systems** instead of choosing **Systems** > **Firmware Management** from the side pane.