Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2

First Published: 2017-07-11

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

### Preface

- Preface xi
  - Audience xi
  - Conventions xi
  - Documentation Feedback xiii
  - Obtaining Documentation and Submitting a Service Request xiii

### Chapter 1

- New and Changed Information for this Release 1

### Chapter 2

- Overview 5
  - About Cisco IMC Supervisor 5
  - About Licenses 6
  - Fulfilling the Product Access Key 7
  - Common Terms in the Cisco IMC Supervisor User Interface 8
    - Rack Groups 8
    - Rack Account 8
    - Policies 9
    - Profiles 9
  - New User Interface of Cisco IMC Supervisor 9
    - Landing Page 11
    - Switching to the Classic View 12
    - Common User Interface Options 12
    - Setting Up a Secure Connection to the Cisco IMC Supervisor User Interface 14
    - Setting up Non-Secure Connection to the Cisco IMC Supervisor User Interface 14

### Chapter 3

- Getting Started 17
  - Overview 17
Launching Cisco IMC Supervisor 18
Licensing Tasks 19
   Updating the License 19
   Replacing a License 20
   Viewing Deactivated Licenses 20
   Migrating a License 21
   Running License Audit 21
Managing User Access Profiles 21
   Multi-Role Access Profiles 21
   Creating a User Access Profile 22
   Logging in to a Profile 23
   Default Profile 23
      Changing a Default Profile 23
Authentication and LDAP Integration 24
   Configuring Authentication Preferences 24
Configuring LDAP 24
   LDAP Integration 25
   LDAP Integration Rules and Limitations 25
   Adding LDAP Configurations 27
   Configuring LDAP Servers 28
   Viewing LDAP Server Summary Information 32
   Testing LDAP Server Connectivity 32
   Searching BaseDN 32
   Requesting Manual LDAP Sync 33
   Executing LDAP Synchronization and Viewing LDAP Synchronized Results 33
   Modifying LDAP Server Details 34
   Viewing Group Membership Information 35
   Deleting LDAP Server Information 36
Configuring a SCP User 36
Configuring Mail Setup 37
Configuring Cisco.com User Credentials and Proxy Configuration 38
   Configuring Cisco.com User 38
   Configuring Proxy 38
Setting Up CMDB Integration 39
Branding 40
Adding Email Alert Rules for Server Faults 70

Managing Rack Servers 73

Viewing Rack-Mount Server Details 73
Viewing Fault Details for a Rack Mount Server 76
Powering On and Off a Rack Mount Server 77
Tagging Assets for a Rack Mount Server 77
Shutting Down a Rack Mount Server 78
Performing a Hard Reset on Rack Mount Server 78
Performing a Power Cycle on a Rack Mount Server 79
Launching KVM Console for a Rack-Mount Server 80
Launching GUI for a Rack Mount Server 80
Setting Locator LED for a Rack Mount Server 81
Setting Label for a Rack Mount Server 82
Managing Tags for a Rack-Mount Server 82
Adding Tags for a Rack-Mount Server 84
Exporting Technical Support Data to a Remote Server 84
Clearing SEL 86
Managing System Tasks 86

Running a Task 87

Managing Policies and Profiles 89

Credential Policies 89

Creating a Credential Policy 90

Hardware Policies 90

Creating Hardware Policies 91

BIOS Policy 93
Disk Group Policy 94
FlexFlash Policy 94
IPMI Over LAN Policy 98
LDAP Policy 99
Legacy Boot Order Policy 100
Network Configuration Policy 101
Network Security Policy 105
NTP Policy 105
Password Expiration Policy 106
Precision Boot Order Policy 107
RAID Policy 108
Serial Over LAN Policy 110
SNMP Policy 111
SSH Policy 112
User Policy 112
Virtual KVM Policy 114
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 119
Creating a Hardware Profile 120
Creating a Profile from an Existing Configuration 121
Applying a Hardware Profile 122
General Tasks Under Hardware Profiles 123

Host Image Mapping 124
Adding Host Image Mapping Profile 124
Tag Library 125
Creating a Tag Library 125

REST API and Orchestration 126

CHAPTER 9
Managing Cisco UCS Hardware Compatibility Report 129
Overview 129
Tagging OS Vendor and Version 130
Creating Hardware Compatibility Reports 130
Synchronizing Hardware Compatibility Reports 131

CHAPTER 10
Firmware Profiles 133
Firmware Management Menu 133
Adding Images to a Local Server 133
Uploading Images from a Local File System 134
CHAPTER 16

Viewing Support Information 161
  Support Information 161
  Viewing Support Information 161

CHAPTER 17

Frequently Performed Tasks and Procedures 163
  Frequently Performed Procedures 163
  Miscellaneous Procedures 163
    Enabling Dashboard View 163
    Creating Additional Dashboards 164
    Enabling Dashboard Auto Refresh 164
    Adding Summary Reports to Dashboard 165
    Deleting a Dashboard 165
    Adding a Menu or Tab to Favorites 165
    Favorites 166
    Customizing Report Table View 166
    Filtering Reports 166
    Exporting a Report 167
    Viewing System Information 167
    Site Map 168
Preface

This preface contains the following sections:

- Audience, page xi
- Conventions, page xi
- Documentation Feedback, page xiii
- Obtaining Documentation and Submitting a Service Request, page xiii

Audience

This guide is intended primarily for data center administrators who use and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>GUI elements such as tab titles, area names, and field labels appear in this font.</td>
</tr>
<tr>
<td></td>
<td>Main titles such as window, dialog box, and wizard titles appear in this font.</td>
</tr>
<tr>
<td>TUI elements</td>
<td>In a Text-based User Interface, text the system displays appears in this font.</td>
</tr>
<tr>
<td>Text Type</td>
<td>Indication</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in this font.</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in this font. Variables in a CLI command appear in this font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
New and Changed Information for this Release

This chapter contains the following section:

• New and Changed Information for this Release, 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>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis Name</td>
<td>The Cisco UCS C3260 Dense Storage Rack Server is now changed to UCS S3260 Storage Servers.</td>
<td>Occurrences of UCS C3260 across the Management Guide.</td>
</tr>
<tr>
<td>Updating Cisco IMC Supervisor and Firmware Policy to automatically use CCO credentials</td>
<td>Changes in the UI to accept CCO credentials.</td>
<td>Checking for Cisco IMC Supervisor Patch Updates, on page 139 and Upgrading Firmware, on page 136</td>
</tr>
<tr>
<td>Smart Call Home to automatically use CCO credentials</td>
<td>Changes in the UI to accept proxy configuration settings.</td>
<td>Configuring Smart Call Home, on page 147</td>
</tr>
<tr>
<td>Implementing a new csv format</td>
<td>While configuring an Auto Discovery Profile, you can specify some fields in the csv file if you have chosen the IP Address CSV File option. A sample csv file is available when you click File Template.</td>
<td>Configuring Auto Discovery Profile, on page 52</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Filtering</td>
<td>Network Security policy is modified to accommodate IP Filtering properties along with IP Blocking properties.</td>
<td>Network Security Policy, on page 105</td>
</tr>
<tr>
<td>Power on password</td>
<td>Administrator password must be set under BIOS Policy which will act as a Power On password.</td>
<td>BIOS Policy, on page 93</td>
</tr>
<tr>
<td>One Time Boot Support</td>
<td>Changes in the Precision Boot Order policy UI to set the parameters for One Time Boot device.</td>
<td>Precision Boot Order Policy, on page 107</td>
</tr>
<tr>
<td>Asset Tagging</td>
<td>You can set the asset tag property for all C-series servers, except for Cisco UCS S3260 storage servers. For Cisco UCS S3260, you can set the asset tag property only on the chassis.</td>
<td>Tagging Assets for a Rack Mount Server, on page 77 and Tagging Assets for Cisco UCS S3260 Rack Server, on page 154</td>
</tr>
<tr>
<td>Include Password Expiry details in the User Inventory</td>
<td>Password expiration policy details are collected as part of the inventory collection for the servers.</td>
<td>User Policy, on page 112</td>
</tr>
<tr>
<td>Password Expiration Policy</td>
<td>A new Password Expiration Policy is added.</td>
<td>Password Expiration Policy, on page 106</td>
</tr>
<tr>
<td>Enhancements to FlexFlash Policy</td>
<td>FlexFlash policy includes options to enable and erase the virtual drives for the Mirror and Util firmware modes.</td>
<td>FlexFlash Policy, on page 94</td>
</tr>
<tr>
<td>Managing HCL Tags</td>
<td>Cisco UCS Hardware Compatibility Report tool is available for Cisco C-Series/S-Series servers.</td>
<td>Managing Cisco UCS Hardware Compatibility Report, on page 129</td>
</tr>
<tr>
<td>Adding host image mapping</td>
<td>Host Image Mapping is a commonly used feature for the E-Series servers which allows customers to upload an ISO file before installing it.</td>
<td>Host Image Mapping, on page 124</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managing controller drive security</td>
<td>Cisco IMC Supervisor supports enabling security at the controller, physical drive, and virtual drive level for this feature. It supports only Local Key Management and not Remote Key Management.</td>
<td>Overview of Controller Drive Security, on page 67</td>
</tr>
<tr>
<td>SSD smart and usage information</td>
<td>Cisco IMC Supervisor supports smart information for a Solid State Drive (SSD) under Storage Controller.</td>
<td>Viewing Smart Information for SSD, on page 65</td>
</tr>
<tr>
<td>Support for replacing a license</td>
<td>You can replace an existing license using the graphical user interface. In addition, you can view a list of deactivated licenses.</td>
<td>Replacing a License, on page 20 View Deactivated Licenses, on page 20</td>
</tr>
<tr>
<td>Support for reviewing recent login history for users</td>
<td>Using the All Users Login History option, you can review login-related information for all users in the system.</td>
<td>Reviewing Recent Login History of Users, on page 46</td>
</tr>
<tr>
<td>Introduction of session management capability for users.</td>
<td>As an administrator, you can configure the maximum number of concurrent sessions for users in the system.</td>
<td>Configuring Session Limits for Users, on page 46</td>
</tr>
</tbody>
</table>
Overview

This chapter contains the following topics:

- About Cisco IMC Supervisor, page 5
- About Licenses, page 6
- Fulfiling the Product Access Key, page 7
- Common Terms in the Cisco IMC Supervisor User Interface, page 8
- New User Interface of Cisco IMC Supervisor, page 9
- Landing Page, page 11
- Switching to the Classic View, page 12
- Common User Interface Options, page 12
- Setting Up a Secure Connection to the Cisco IMC Supervisor User Interface, page 14
- Setting up Non-Secure Connection to the Cisco IMC Supervisor User Interface, page 14

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.

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 7.

3. After you install Cisco IMC Supervisor, update the license as described in Updating the License, on page 19.

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 19.

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:
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.

New User Interface of Cisco IMC Supervisor

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

Availability of the Classic View

When you login to Cisco IMC Supervisor, by default, the new user interface is displayed. The earlier version of the interface, now referred to as the Classic View, is currently available. However, this Classic View will soon be removed from the user interface. For information on accessing the Classic View, see Switching to the Classic View, on page 12.

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 163. In addition, you can create multiple dashboards and delete them when you no longer need them. See Creating Additional Dashboards, on page 164 and Deleting a Dashboard, on page 165.
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.
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](image)

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Header</td>
<td>Contains frequently accessed elements, including the menu. The header is always visible.</td>
</tr>
<tr>
<td>2</td>
<td>Link</td>
<td>Provides a link to the Cisco website from where you can access information on using the software.</td>
</tr>
<tr>
<td>3</td>
<td>Search icon</td>
<td>Allows you to search for and navigate directly to a specific report in the portal.</td>
</tr>
</tbody>
</table>
Switching to the Classic View

The classic view is the earlier version of the administrator user interface of Cisco IMC Supervisor. You can switch to the classic view from the new user interface.

On the header, click the icon for your user name, and choose Classic View. The earlier interface opens in a new browser tab.

This Classic View option is available in the user interface only if you set the enableClassicView parameter to true.

```
cd /opt/infra/web_cloudmgr/apache-tomcat/webapps/app/ux/resources/
vi appConfigs.json
enableClassicView=true
```

You must refresh the user interface to view this option.

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.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refresh</td>
<td>Refreshes the reported data on the page.</td>
</tr>
<tr>
<td>Icon</td>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Favorite" /></td>
<td>Favorite</td>
<td>Adds a page to the Favorites menu. You can use this option to view frequently accessed pages more quickly.</td>
</tr>
<tr>
<td><img src="image" alt="Add" /></td>
<td>Add</td>
<td>Brings up the Add dialog box, from which you can add a new resource.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit</td>
<td>Brings up the Edit dialog box, from which you can edit a resource.</td>
</tr>
<tr>
<td><img src="image" alt="Customize Table" /></td>
<td>Customize Table</td>
<td>Brings up the Customize Report Table dialog box, in which you choose what columns you want to include on the screen.</td>
</tr>
</tbody>
</table>
| ![Export Report](image) | 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](image) | Expand | Expands all the folders that are displayed on the page. |
| ![Collapse](image) | Collapse | Collapses all the folders that are displayed on the page. |
| ![Add Advanced Filter](image) | Add Advanced Filter | Provides extra filtering parameters on the page. |
| ![Search Field](image) | 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.

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

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

```xml
<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

```
<!--
```
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

```
<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.
Getting Started

This chapter contains the following topics:

- Overview, page 17
- Launching Cisco IMC Supervisor, page 18
- Licensing Tasks, page 19
- Managing User Access Profiles, page 21
- Authentication and LDAP Integration, page 24
- Configuring LDAP, page 24
- Configuring a SCP User, page 36
- Configuring Mail Setup, page 37
- Configuring Cisco.com User Credentials and Proxy Configuration, page 38
- Setting Up CMDB Integration, page 39
- Branding, page 40
- Configuring User Interface Settings, page 41

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.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Keys</td>
<td>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,</td>
</tr>
<tr>
<td>License Utilization</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Usage Data</td>
<td>This tab displays the details of the various resources used.</td>
</tr>
<tr>
<td>Deactivated Licenses</td>
<td>This tab displays a list of deactivated licenses.</td>
</tr>
</tbody>
</table>

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 6. 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; License.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the License page, choose License Keys.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Replace License.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) Check Enter License Text to copy and paste the license text.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Submit. All existing licenses are replaced with the new license.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; License.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the License page, choose Deactivated Licenses.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Review the information displayed for all the deactivated licenses.</td>
</tr>
</tbody>
</table>
**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**

1. Choose **Administration > License**.
2. On the **License** page, choose **License Keys**.
3. On the **License Keys** page, click **Migrate License**.
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.
5. (Optional) Check **Enter License Text** to copy and paste the license text.
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 19.

**Procedure**

1. Choose **Administration > License**.
2. On the **License** page, click **License Utilization**.
3. From the **More Actions** drop-down list, choose **Run License Audit**.
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 UCS Director 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. With Cisco UCS Director Release 5.4, support for multiple profiles for a single user was introduced. So when you install version 5.4, and if a user account is associated with multiple groups, the system creates multiple profiles for the user account. But if you upgrade the system from a prior version to version 5.4, and if the LDAPSyncTask system task is not yet run, then, by default, only one profile is listed for a user account in the system.

When LDAP users are integrated with Cisco UCS Director, 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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The profile name.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the profile.</td>
</tr>
<tr>
<td>Type drop-down list</td>
<td>Choose the user role type.</td>
</tr>
<tr>
<td>Customer Organizations drop-down list</td>
<td>Choose the organization to which this user profile applies.</td>
</tr>
<tr>
<td>Show Resources From All Other Groups the User Has Access check box</td>
<td>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.</td>
</tr>
<tr>
<td>Shared Groups field</td>
<td>Click Select to choose the groups to which the user profile applies.</td>
</tr>
<tr>
<td>Default Profile check box</td>
<td>Check the check box if this is the default user access profile. Uncheck the check box if it is not the default.</td>
</tr>
</tbody>
</table>
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 UCS Director 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local First, fallback to LDAP</td>
<td>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.</td>
</tr>
<tr>
<td>Verisign Identity Protection</td>
<td>VIP Authentication Service (two-factor authentication) is enabled.</td>
</tr>
</tbody>
</table>

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 28.

- **Verisign Identity Protection**— If you select this option, continue to the next step.

**Step 4** If you select Verisign Identity Protection, complete the following steps:

a) Click **Browse** to upload a VIP certificate.
   - Locate and select the certificate, and click **Upload**.

b) Enter the **Password**.

**Step 5** 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 UCS Director. 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 to synchronize 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**

**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Administration &gt; LDAP Integration.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click + to add LDAP configurations.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>On the Add LDAP Configurations page, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>An LDAP account name.</td>
</tr>
<tr>
<td>Server Type</td>
<td>Choose either Microsoft Active Directory or Open LDAP.</td>
</tr>
<tr>
<td>Server</td>
<td>Host name or the IP address of the server.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Enables a secure connection to the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name for the LDAP user.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a name for the LDAP user.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password associated with the username.</td>
</tr>
</tbody>
</table>
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  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 33.

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:

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Filters</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Group Filters</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Add Entry to User Filters or Add Entry to Group Filters** dialog box (displayed based on your previous selection)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AttributeName</strong></td>
<td>Choose either <strong>GroupName</strong> or <strong>UserName</strong>.</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>Choose the filter to retrieve groups and users. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Equals to</td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
</tr>
<tr>
<td><strong>AttributeValue</strong></td>
<td>Specify a keyword or a value that must be included in the search.</td>
</tr>
</tbody>
</table>
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:

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

**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 24.
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 test 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; LDAP Integration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Request Manual LDAP Sync.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Manual LDAP Sync page, complete the following fields:</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>Basic Search check box</td>
<td>Enables basic search by organization unit.</td>
</tr>
<tr>
<td>Advanced Search check box</td>
<td>Enables advanced search.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSL check box</td>
<td>Enables a secure connection to the LDAP server.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port number.</td>
</tr>
<tr>
<td></td>
<td>It is automatically set to 636 for SSL, and 389 for non-secure mode.</td>
</tr>
</tbody>
</table>
### 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 UCS Director also provides you with an additional option to view a list of all groups that a specific user is part of.
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 a SCP User

SCP user is used by server diagnostics and tech support upload operations for transferring file to the Cisco IMC Supervisor appliance using SCP protocol. An scp user account cannot be used to login to the Cisco IMC Supervisor UI or the shelladmin. Perform this procedure for configuring scp user password.
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 70.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Users and Groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click SCP User Configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the scp user password in the Password field.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

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

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. These credentials are automatically used for firmware image download and updating Cisco IMC Supervisor. 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**

1. **Step 1** Choose **Administration > System**.
2. **Step 2** On the **System** page, click **Cisco.com User Configuration**.
3. **Step 3** Complete the following for configuring Cisco.com user:
   
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name (cisco.com) field</td>
<td>Enter your Cisco login user name.</td>
</tr>
<tr>
<td>Password (cisco.com) field</td>
<td>Enter your Cisco login password.</td>
</tr>
</tbody>
</table>

4. **Step 4** Click **Save**.

### Configuring Proxy

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

**Procedure**

1. **Step 1** Choose **Administration > System**.
2. **Step 2** On the **System** page, click **Proxy Configuration**.
3. **Step 3** Complete the following for proxy configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Proxy Configuration</td>
<td>(Optional) Check this check box to enable proxy and complete the following:</td>
</tr>
<tr>
<td>check box</td>
<td>• <strong>Host Name</strong> field - Enter a host name for the proxy configuration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port</strong> field - Enter the port for the proxy configuration.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to FTP Server</td>
<td>Check the check box to export change records to an FTP server.</td>
</tr>
<tr>
<td>Export Format drop-down</td>
<td>Choose the type of export format: CSV or XML.</td>
</tr>
<tr>
<td>FTP Server field</td>
<td>The FTP server address.</td>
</tr>
<tr>
<td>FTP Port field</td>
<td>The FTP server port number.</td>
</tr>
<tr>
<td>FTP User field</td>
<td>The FTP user ID.</td>
</tr>
<tr>
<td>FTP Password field</td>
<td>The FTP user password.</td>
</tr>
<tr>
<td>FTP Export Frequency</td>
<td>Choose how often the change records are exported to the FTP server.</td>
</tr>
</tbody>
</table>
### 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

1. **Step 1** Choose Administration > Users and Groups.
2. **Step 2** Click Login Page Branding.
3. **Step 3** Click Add.
4. **Step 4** On the Domain Branding page, complete the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name field</td>
<td>A domain name for branding. For example, imcs.xxxx.com. For creating a domain name in your local machine, navigate to C:\Windows\System32\drivers\etc and specify the &lt;ipaddress&gt; and &lt;domainname&gt; in the hosts file. For example, 10.10.10.10 imcs.xxxx.com.</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hide Entire Header</strong> check box</td>
<td>Use this check box to enable or disable the header.</td>
</tr>
<tr>
<td><strong>Product Name</strong> field</td>
<td>Main title of the header.</td>
</tr>
<tr>
<td><strong>Product Name 2nd Line</strong> field</td>
<td>Sub-title of the header.</td>
</tr>
<tr>
<td><strong>Enable About Dialog</strong> checkbox</td>
<td>Use this checkbox to enable or disable the About dialog box for Cisco IMC Supervisor.</td>
</tr>
</tbody>
</table>

**Administrator Portal**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom Link 1 Lable</strong> field</td>
<td>You can configure this field to change the text on header bar.</td>
</tr>
<tr>
<td><strong>Custom Link 1 URL</strong> field</td>
<td>You can configure the URL for the Custom Link 1 Lable</td>
</tr>
<tr>
<td><strong>Custom Link 2 Lable</strong> field</td>
<td>You can configure this field to change the text on header bar.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Link 2 URL field</td>
<td>You can configure the URL for the Custom Link 2 Label</td>
</tr>
<tr>
<td>End-user Portal</td>
<td></td>
</tr>
<tr>
<td>Custom Link 1 Label field</td>
<td>You can configure this field to change the text on header bar.</td>
</tr>
<tr>
<td>Custom Link 1 URL field</td>
<td>You can configure the URL for the Custom Link 1 Label</td>
</tr>
<tr>
<td>Custom Link 2 Label field</td>
<td>You can configure this field to change the text on header bar.</td>
</tr>
<tr>
<td>Custom Link 2 URL field</td>
<td>You can configure the URL for the Custom Link 2 Label</td>
</tr>
</tbody>
</table>

**Step 3**  Click Save.
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 44. For more information about creating user roles, see Adding a User Role, on page 47.

  • 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.

<table>
<thead>
<tr>
<th>Menu Settings</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems:</td>
<td></td>
</tr>
<tr>
<td>• Inventory and fault status</td>
<td>• Read - Physical Computing</td>
</tr>
<tr>
<td>• Physical Accounts</td>
<td>• Write - Physical Computing</td>
</tr>
<tr>
<td>• Firmware Management</td>
<td>• Read - System Admin</td>
</tr>
<tr>
<td>• Server Diagnostics</td>
<td>• Read - Users</td>
</tr>
<tr>
<td>Policies:</td>
<td></td>
</tr>
<tr>
<td>• Manage Schedules</td>
<td>• Read - Read Tag Library</td>
</tr>
<tr>
<td>• API and Orchestration</td>
<td>• Write - Write Tag Library</td>
</tr>
<tr>
<td>Administration:</td>
<td></td>
</tr>
<tr>
<td>• Users and Groups</td>
<td>• Read - Orchestration</td>
</tr>
<tr>
<td>• Integration</td>
<td>• Write - Orchestration</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Role drop-down list</td>
<td>Choose Group Admin, Operator, or System Admin.</td>
</tr>
<tr>
<td>User Group drop-down list</td>
<td>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.</td>
</tr>
<tr>
<td>Login Name field</td>
<td>The login name for the user.</td>
</tr>
<tr>
<td>Password field</td>
<td>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.</td>
</tr>
<tr>
<td>Confirm Password field</td>
<td>Repeat the password from the previous field.</td>
</tr>
<tr>
<td>User Contact Email field</td>
<td>The email address.</td>
</tr>
<tr>
<td>First Name field</td>
<td>(Optional) The first name of the user.</td>
</tr>
<tr>
<td>Last Name field</td>
<td>(Optional) The last name of the user.</td>
</tr>
<tr>
<td>Phone field</td>
<td>(Optional) The phone number of the user.</td>
</tr>
<tr>
<td>Address field</td>
<td>(Optional) The physical address of the user.</td>
</tr>
</tbody>
</table>

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:
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.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; System.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click User Roles.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Add User Role page, complete the following for the User Role pane:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Role field</td>
<td>A descriptive name for the user role.</td>
</tr>
<tr>
<td>Role Type drop-down list</td>
<td>Choose Admin.</td>
</tr>
<tr>
<td>Description field</td>
<td>(Optional) A description of the user role.</td>
</tr>
</tbody>
</table>
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.

---

## Adding a User Group

Perform this procedure when you want to add a new user group.

### Procedure

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

**Step 2** Click User Groups.

**Step 3** Click Add.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>A name of the user group.</td>
</tr>
<tr>
<td>Description field</td>
<td>(Optional) A description of the user group.</td>
</tr>
<tr>
<td>Code field</td>
<td>(Optional) A shorter name or code name for the group.</td>
</tr>
<tr>
<td>Cost Center field</td>
<td>(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with.</td>
</tr>
<tr>
<td>Contact Email field</td>
<td>The email used to notify the group owner about the status of service requests and request approvals if necessary.</td>
</tr>
<tr>
<td>First Name field</td>
<td>(Optional) The contact’s first name.</td>
</tr>
<tr>
<td>Last Name field</td>
<td>(Optional) The contact’s last name.</td>
</tr>
<tr>
<td>Phone field</td>
<td>(Optional) The contact’s phone number.</td>
</tr>
<tr>
<td>Address field</td>
<td>(Optional) The contact’s address.</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Administration &gt; Users and Groups</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>User Groups</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select a user group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Branding</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>On the <strong>Group Branding</strong> page, complete the following:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logo Image</strong> checkbox</td>
<td>If checked, the logo appears on the top left corner of the application.</td>
</tr>
<tr>
<td><strong>Application Labels</strong> checkbox</td>
<td>If checked, the application labels appear on top header section of the application.</td>
</tr>
<tr>
<td><strong>URL Forwarding on Logout</strong> checkbox</td>
<td>If checked, user will be forwarded to the provided URL on logout.</td>
</tr>
<tr>
<td><strong>Custom Links</strong> checkbox</td>
<td>If checked, custom links will appear on the top right corner of the application.</td>
</tr>
</tbody>
</table>
Step 6 Click Submit.

Group Share Policy

A group share policy provides more control to the users on the resources and what they can share with other users. With this policy, users can view resources that are currently assigned only to them or can view resources that are assigned to all groups that the users are part of.

While you are creating a group, you can define a group share policy and determine which groups have read/write permissions. Later on, when users are added to this group, their access to resources is defined by the group share policy that is applied to the group.

Adding Group Share Policy

Perform this procedure when you want to add a policy and share it with a user group.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; Users and Groups.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Group Share Policy.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Add Group Share Policy page, complete the following fields:</td>
</tr>
<tr>
<td></td>
<td><strong>Field</strong></td>
</tr>
<tr>
<td></td>
<td>Policy Name field</td>
</tr>
<tr>
<td></td>
<td>Policy Description field</td>
</tr>
<tr>
<td></td>
<td>Select Groups drop-down list</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Submit.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click OK in the Submit Result dialog box.</td>
</tr>
</tbody>
</table>

Note: You can also select an existing policy to view, edit, delete, and clone them.
Managing Server Discovery, Rack Groups, and Rack Accounts

This chapter contains the following topics:

- Overview, page 51
- Discovering and Importing a Server, page 52
- Adding a Rack Group, page 57
- Adding a Rack Account, page 57
- Collecting Inventory for Rack Accounts or Rack Groups, page 59
- Assigning Rack Accounts to a Rack Group, page 60
- Testing an Account Connection, page 60

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>A descriptive name for the profile.</td>
</tr>
<tr>
<td>Search Criteria</td>
<td>Select IP Address Range, Subnet Mask Range, IP Address CSV File, or IP Address List from the drop-down list.</td>
</tr>
<tr>
<td>Starting IP</td>
<td>Valid IP address</td>
</tr>
<tr>
<td>Ending IP</td>
<td>Valid IP address</td>
</tr>
</tbody>
</table>

If you check Use Credential Policy checkbox

<table>
<thead>
<tr>
<th>Credential Policy</th>
<th>Choose a policy from the drop-down list or click the + icon and create new policy. Refer to Creating a Credential Policy, on page 90, to create a new policy.</th>
</tr>
</thead>
</table>

If you uncheck Use Credential Policy checkbox

<table>
<thead>
<tr>
<th>User Name</th>
<th>The server login name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The server login password</td>
</tr>
<tr>
<td>Important</td>
<td>Do not include special characters such as + in the password.</td>
</tr>
<tr>
<td>Protocol drop-down list</td>
<td>Choose https or http from the list.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a port number.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Systems &gt; Physical Accounts.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Discovered Devices.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Discover.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Discover Devices page, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Profile drop-down list</td>
<td>Click Select to choose the profiles to discover. Check the check boxes of all the profiles you want to discover.</td>
</tr>
<tr>
<td>Schedule Later check box</td>
<td>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 141. You can go to Policies &gt; Manage Schedules, select a schedule and click View Scheduled Tasks to view the scheduled task or click Remove Scheduled Tasks to delete scheduled tasks.</td>
</tr>
<tr>
<td>Schedule(s) drop-down list</td>
<td>If you have chosen the Schedule Later check box, you can select a schedule you have created from the drop-down list.</td>
</tr>
</tbody>
</table>

| 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.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description of the server.</td>
</tr>
<tr>
<td>Contact</td>
<td>Enter the contact details of the server.</td>
</tr>
</tbody>
</table>
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 19.

Procedure

Step 1 Choose Systems > Physical Accounts.
Step 2 Click Add.
Step 3 On the Create Rack Group page, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location field</td>
<td>Enter the address of the server.</td>
</tr>
<tr>
<td>Select Rack Group drop-down list or + icon</td>
<td>Choose a rack group or create a rack group.</td>
</tr>
</tbody>
</table>

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 19.
- 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Name</strong> field</td>
<td>A descriptive name for the rack account.</td>
</tr>
</tbody>
</table>
| **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

<p>| <strong>User Name</strong> field | Login ID for the rack-mount server.                                         |
| <strong>Password</strong> field | Password for the login ID for the rack-mount server.                        |
| <strong>Protocol</strong> drop-down list | Choose https or http from the list.                                   |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port field</td>
<td>The port number associated with the selected protocol.</td>
</tr>
</tbody>
</table>
| 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 57. |
| 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 60.

**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.
### 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Systems &gt; Physical Accounts</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Rack Accounts</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>A list of servers is displayed.</td>
</tr>
<tr>
<td>4</td>
<td>Select a server or multiple servers and click <strong>Assign Rack Group</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>On the <strong>Assign Rack Groups</strong> page, select the rack group you want to assign the servers to.</td>
</tr>
</tbody>
</table>

**Note**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Click <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Systems &gt; Physical Accounts.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Rack Accounts.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the list of rack accounts, select the accounts for which you want to test the connection.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Test Connection.</td>
</tr>
<tr>
<td>Note</td>
<td>You cannot see the Test Connection button till you select at least one rack account from the list.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Test Connection dialog box, click Submit.</td>
</tr>
<tr>
<td></td>
<td>Testing the connection may take several minutes.</td>
</tr>
<tr>
<td></td>
<td>The connection status and the reason for success or failure are displayed in the Rack Accounts page.</td>
</tr>
</tbody>
</table>
CHAPTER 6

Viewing Inventory Data and Faults

This chapter contains the following topics:

- Viewing Rack-Mount Server Details, page 63
- Viewing Fault Details for a Rack Mount Server, page 69
- Summary Reports for a Rack Group, page 69
- Adding Email Alert Rules for Server Faults, page 70

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:
<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>An overview of the rack account.</td>
</tr>
<tr>
<td><strong>CPUs</strong></td>
<td>The details of the CPU used in the server.</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>The details of the memory used in the server.</td>
</tr>
<tr>
<td><strong>PSUs</strong></td>
<td>The details of the power supply unit used in the server.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td><strong>PCI Adapters</strong></td>
<td>The details of the PCI adapters used in the server.</td>
</tr>
<tr>
<td><strong>VIC Adapters</strong></td>
<td>The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click <strong>View Details</strong> to view information</td>
</tr>
<tr>
<td></td>
<td>such as <strong>External Ethernet Interfaces</strong> and <strong>VM FEXs</strong>.</td>
</tr>
<tr>
<td><strong>Network Adapters</strong></td>
<td>The details of the network adapters used in the server. Select any of the Network Adapters listed and click <strong>View Details</strong> to view information on <strong>External Ethernet Interfaces</strong>.</td>
</tr>
<tr>
<td><strong>Storage Adapters</strong></td>
<td>The details of the storage adapters used in the server. Select any of the Storage Adapters listed and click <strong>View Details</strong> to view information such as <strong>Controller Info</strong> and <strong>Physical Drives</strong>, and <strong>Virtual Drives</strong>. See, Viewing Smart Information for SSD, on page 65.</td>
</tr>
<tr>
<td><strong>FlexFlash Adapters</strong></td>
<td>The details of the FlexFlash adapters used in the server. Select any of the FlexFlash Adapters listed and click <strong>View Details</strong> to view information such as <strong>Controller Info</strong> and <strong>Physical Drives</strong>. If you are upgrading Cisco IMC Supervisor from a previous version, you must run the inventory by going to Systems &gt; Physical Accounts &gt; Rack Accounts &gt; Inventory, or wait for the periodic inventory to run, for the FlexFlash details to appear in the report.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td>The information on the protocol, such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.</td>
</tr>
<tr>
<td><strong>Remote Presence</strong></td>
<td>The details of vKVM, Serial Over LAN, and vMedia.</td>
</tr>
<tr>
<td><strong>Faults</strong></td>
<td>The details of the faults logged in the server.</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>The details about users under <strong>Default Group</strong>. 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, <strong>User Policy</strong>, on page 112 and <strong>Password Expiration Policy</strong>, on page 106.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
</tbody>
</table>
Tab | Description
---|---
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 84. **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 Server.
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:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Cycle Count field</td>
<td>Number of power cycles that the drive went through from the time it was manufactured.</td>
</tr>
<tr>
<td>Power on Hours field</td>
<td>Total number of hours that the drive is in the 'Power On' mode.</td>
</tr>
</tbody>
</table>
| 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. |
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.

Cisco IMC Supervisor supports only Local Key Management and not Remote Key Management. See, Viewing Controller Drive Security Details, on page 67.

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:
<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Cycle Count</strong> field</td>
<td>Number of power cycles that the drive went through from the time it was manufactured.</td>
</tr>
<tr>
<td><strong>Power on Hours</strong> field</td>
<td>Total number of hours that the drive is in the Power On mode.</td>
</tr>
<tr>
<td><strong>Percentage Life Left</strong> field</td>
<td>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%.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can see a bar graph added for SSDs in <strong>SSD - Percentage Life Left</strong> under <strong>Controller Info</strong>.</td>
</tr>
<tr>
<td><strong>Wear Status in Days</strong> field</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Operating Temperature</strong> field</td>
<td>The current temperature of the drive at which the selected SSD operates at the time of selection.</td>
</tr>
<tr>
<td><strong>Percentage Reserved Consumed</strong> field</td>
<td>The total capacity (out of the percentage reserved for it) consumed by the SSD.</td>
</tr>
<tr>
<td><strong>Time of Last Refresh</strong> field</td>
<td>Time period since the drive was last refreshed.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation</td>
<td>Brief reason for the issue.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Steps to resolve the issue.</td>
</tr>
</tbody>
</table>

**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.
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.

**Note**

- **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 will be sent when faults that match the conditions specified are discovered periodically. 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the rule.</td>
</tr>
<tr>
<td>Alert Scope</td>
<td>Choose System for receiving all system level alerts for new faults discovered on any server, ServerGroup for receiving email alerts for new faults discovered on a server which is part of the specified Rack Group, or Server for receiving  email alerts for new faults discovered on a specified server.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Server Groups | If you choose the Alert Level as **ServerGroup**, this option is displayed.
1. Click **Select**.
2. 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.
1. Click **Select**.
2. 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.
1. Click **Select**.
2. Check one or more severity levels from the list and click **Select**.

**Note** | The selected values will be displayed next to the **Select** button.

Rule Enabled check box | Check this check box to enable email alerts to the configured email address.

**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.
Adding Email Alert Rules for Server Faults
Managing Rack Servers

This chapter contains the following topics:

- Viewing Rack-Mount Server Details, page 73
- Viewing Fault Details for a Rack Mount Server, page 76
- Powering On and Off a Rack Mount Server, page 77
- Tagging Assets for a Rack Mount Server, page 77
- Shutting Down a Rack Mount Server, page 78
- Performing a Hard Reset on Rack Mount Server, page 78
- Performing a Power Cycle on a Rack Mount Server, page 79
- Launching KVM Console for a Rack-Mount Server, page 80
- Launching GUI for a Rack Mount Server, page 80
- Setting Locator LED for a Rack Mount Server, page 81
- Setting Label for a Rack Mount Server, page 82
- Managing Tags for a Rack-Mount Server, page 82
- Adding Tags for a Rack-Mount Server, page 84
- Exporting Technical Support Data to a Remote Server, page 84
- Clearing SEL, page 86
- Managing System Tasks, page 86

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Systems &gt; Inventory and Fault Status</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand <strong>Rack Groups</strong> and select the rack group that contains the server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the selected rack group page, click <strong>Rack Servers</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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 <strong>View Details</strong>.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>An overview of the rack account.</td>
</tr>
<tr>
<td><strong>CPUs</strong></td>
<td>The details of the CPU used in the server.</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>The details of the memory used in the server.</td>
</tr>
<tr>
<td><strong>PSUs</strong></td>
<td>The details of the power supply unit used in the server.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td><strong>PCI Adapters</strong></td>
<td>The details of the PCI adapters used in the server.</td>
</tr>
<tr>
<td><strong>VIC Adapters</strong></td>
<td>The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click <strong>View Details</strong> to view information such as <strong>External Ethernet Interfaces</strong> and <strong>VM FEXs</strong>.</td>
</tr>
<tr>
<td><strong>Network Adapters</strong></td>
<td>The details of the network adapters used in the server. Select any of the Network Adapters listed and click <strong>View Details</strong> to view information on <strong>External Ethernet Interfaces</strong>.</td>
</tr>
<tr>
<td><strong>Storage Adapters</strong></td>
<td>The details of the storage adapters used in the server. Select any of the Storage Adapters listed and click <strong>View Details</strong> to view information such as <strong>Controller Info</strong> and <strong>Physical Drives</strong>, and <strong>Virtual Drives</strong>. See, <strong>Viewing Smart Information for SSD</strong>, on page 65.</td>
</tr>
<tr>
<td>Tab</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FlexFlash Adapters</td>
<td>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 &gt; Physical Accounts &gt; Rack Accounts &gt; Inventory, or wait for the periodic inventory to run, for the FlexFlash details to appear in the report. <strong>Note</strong> Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td>Communication</td>
<td>The information on the protocol, such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.</td>
</tr>
<tr>
<td>Remote Presence</td>
<td>The details of vKVM, Serial Over LAN, and vMedia.</td>
</tr>
<tr>
<td>Faults</td>
<td>The details of the faults logged in the server.</td>
</tr>
<tr>
<td>Users</td>
<td>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 106. <strong>Note</strong> Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td>Cisco IMC Log</td>
<td>The details of the Cisco IMC logs for the server. <strong>Note</strong> Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td>System Event Log</td>
<td>The details of the server logs. <strong>Note</strong> Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
<tr>
<td>TPM</td>
<td>Information on the TPM inventory.</td>
</tr>
<tr>
<td>BIOS</td>
<td>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.</td>
</tr>
<tr>
<td>Fault History</td>
<td>Historical information on the faults that occurred on the server.</td>
</tr>
<tr>
<td>Tech Support</td>
<td>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 84. <strong>Note</strong> Not applicable for Cisco UCS S3260 dense storage rack server.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation</td>
<td>Brief reason for the issue.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Steps to resolve the issue.</td>
</tr>
</tbody>
</table>

**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 154. 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

Perform this procedure to download the *kvm.jnlp* file and open the KVM console.

**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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Systems &gt; Inventory and Fault Status.</strong></th>
</tr>
</thead>
</table>
| 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.**  
Cisco IMC Supervisor downloads the *kvm.jnlp* files. |
| Step 7 | Double-click on the *kvm.jnlp* files in your downloads folder.  
The KVM Console opens in a separate window.  
**Note** The launcher.jsp file that opens in a separate window displays the list of servers you have selected. You can also view if the KVM consoles were launched successfully. |

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.
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**

1. Choose Systems > Inventory and Fault Status.
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.
3. On the selected rack group page, click Rack Servers.
   **Note** You can also select any sub groups under Rack Groups.
4. Select the server from the list.
5. From the More Actions drop-down list, choose Launch GUI.
   **Note** You can also right-click and choose the option.
6. Click Submit.
   The GUI for the server is launched in a separate browser.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tag Name</strong></td>
<td>Select the tag name from the drop-down list and click <strong>Submit</strong> or create a new tag.</td>
</tr>
<tr>
<td></td>
<td><strong>1</strong> Click the + icon.</td>
</tr>
<tr>
<td></td>
<td><strong>2</strong> In the <strong>Create Tag</strong> window, do the following:</td>
</tr>
<tr>
<td></td>
<td>a  In the <strong>Name</strong> field, enter a descriptive name for the tag.</td>
</tr>
<tr>
<td></td>
<td>b  In the <strong>Description</strong> field, enter a description of the tag.</td>
</tr>
<tr>
<td></td>
<td>c  In the <strong>Type</strong> field, select String or Integer from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>d  In the <strong>Possible Tag Values</strong> field, enter a possible value for the tag.</td>
</tr>
<tr>
<td></td>
<td>e  Click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>f  Click the + icon to add a new category.</td>
</tr>
<tr>
<td><strong>Tag Value</strong></td>
<td>Select the tag value from the drop-down list.</td>
</tr>
</tbody>
</table>

**3** 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 155.

### 4
Check the **Rack Servers** or **Chassis** check box.

### 5
Click **Submit**.

**Note**
The tags are displayed under the respective category according to the set taggable entities.

### 6
In the confirmation dialog box, click **OK**.
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 82 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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination Type</strong> drop-down list</td>
<td>You can export the file to a remote server or to a local Cisco IMC Supervisor appliance. Choose either <strong>REMOTE</strong> or <strong>LOCAL</strong>.</td>
</tr>
<tr>
<td><strong>Network Type</strong> drop-down list</td>
<td>The network type. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• SCP</td>
</tr>
<tr>
<td></td>
<td>• SFTP</td>
</tr>
<tr>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• TFTP</td>
</tr>
<tr>
<td><strong>Server IP/Hostname</strong> field</td>
<td>The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the <strong>Network Type</strong> drop-down list, the name of this field will vary.</td>
</tr>
<tr>
<td><strong>Path and Filename</strong> field</td>
<td>The path and filename that must be used when exporting the file to the remote server.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The username the system should use to log in to the remote server. This field does not apply if the network type is TFTP.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for the remote server username. This field does not apply if the network type is TFTP.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task Execution</strong> drop-down list</td>
<td>(Optional) Choose enable or disable.</td>
</tr>
</tbody>
</table>
| **System Task Policy** drop-down list | Choose one of the following options:  
  • default-system-task-policy  
  • local-run-policy |
| **Hours** drop-down list | Choose the hourly frequency to run the task. |

**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.
Managing Policies and Profiles

This chapter contains the following topics:

- Credential Policies, page 89
- Hardware Policies, page 90
- Hardware Profiles, page 119
- Host Image Mapping, page 124
- Tag Library, page 125
- REST API and Orchestration, 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>User defined name of the policy.</td>
</tr>
<tr>
<td>Description</td>
<td>User defined brief description of the policy.</td>
</tr>
<tr>
<td>Username</td>
<td>Cisco user name.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol followed by the policy.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for the policy.</td>
</tr>
</tbody>
</table>
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 90.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>A descriptive name for the policy.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A description of the policy.</td>
</tr>
<tr>
<td>User Name</td>
<td>Cisco IMC user name or the rack mount server user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Cisco IMC password or the rack mount server password.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose a protocol from the drop-down list.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a port number for the policy.</td>
</tr>
</tbody>
</table>

**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 91.
   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 122.

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 about creating a policy based on the 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.
<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS Policy, on page 93</td>
<td>Configuring BIOS Settings</td>
</tr>
<tr>
<td>Disk Group Policy, on page 94</td>
<td>Managing Storage Adapters</td>
</tr>
<tr>
<td>FlexFlash Policy, on page 94</td>
<td>Managing the Flexible Flash Controller</td>
</tr>
<tr>
<td>IPMI Over LAN Policy, on page 98</td>
<td>Configuring IPMI</td>
</tr>
<tr>
<td>LDAP Policy, on page 99</td>
<td>Configuring the LDAP Server</td>
</tr>
<tr>
<td>Legacy Boot Order Policy, on page 100</td>
<td>Server Boot Order</td>
</tr>
<tr>
<td>Network Configuration Policy, on page 101</td>
<td>Configuring Network-Related Settings</td>
</tr>
<tr>
<td>Network Security Policy, on page 105</td>
<td>Network Security Configuration</td>
</tr>
<tr>
<td>NTP Policy, on page 105</td>
<td>Configuring Network Time Protocol Settings</td>
</tr>
<tr>
<td>Password Expiration Policy, on page 106</td>
<td>Password Expiry</td>
</tr>
<tr>
<td>Precision Boot Order Policy, on page 107</td>
<td>Configuring the Precision Boot Order</td>
</tr>
<tr>
<td>RAID Policy, on page 108</td>
<td>Managing Storage Adapters</td>
</tr>
<tr>
<td>Serial Over LAN Policy, on page 110</td>
<td>Configuring Serial Over LAN</td>
</tr>
<tr>
<td>SNMP Policy, on page 111</td>
<td>Configuring SNMP</td>
</tr>
<tr>
<td>SSH Policy, on page 112</td>
<td>Configuring SSH</td>
</tr>
<tr>
<td>User Policy, on page 112</td>
<td>Configuring Local Users</td>
</tr>
<tr>
<td>VIC Adapter Policy, on page 114</td>
<td>Viewing VIC Adapter Properties</td>
</tr>
<tr>
<td>Virtual KVM Policy, on page 114</td>
<td>Configuring the Virtual KVM</td>
</tr>
<tr>
<td>vMedia Policy, on page 115</td>
<td>Configuring Virtual Media</td>
</tr>
<tr>
<td>Zoning Policy, on page 116</td>
<td>Dynamic Storage in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Storage Servers</td>
</tr>
</tbody>
</table>
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 a 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 #unique_150.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firmware Mode</strong> pane</td>
<td>Choose any of the following firmware operating modes:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mirror Mode</strong> - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Util Mode</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Applicable</strong> - 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.</td>
</tr>
<tr>
<td><strong>Mirror</strong> radio button</td>
<td>Check Enable Virtual Drive to enable the Hypervisor virtual drive or check Erase Virtual Drive to erase it.</td>
</tr>
<tr>
<td><strong>Util</strong> radio button</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can select multiple virtual drives.</td>
</tr>
<tr>
<td><strong>Not Applicable</strong> radio button</td>
<td>Check Enable Virtual Drive to enable virtual drives such as SCU, HV, Drivers, and HUU.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can select multiple virtual drives.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Erase Virtual Drive</strong> check box is not available.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Partition Name</strong> field (available only for Mirror and Util mode)</td>
<td>The name of the partition.</td>
</tr>
<tr>
<td><strong>Non Util Card Partition Name</strong> field</td>
<td>The name that you want to assign to the single partition on the second card, if it exists.</td>
</tr>
<tr>
<td><strong>Select Primary Card</strong> (available for mirror mode) or <strong>Select Util Card</strong> (available for Util mode) drop-down list</td>
<td>Select the slots <strong>Slot 1</strong> or <strong>Slot 2</strong> where the SD cards are present or select <strong>None</strong> if only one SD card is present on the server.</td>
</tr>
<tr>
<td><strong>Auto Sync</strong> check box</td>
<td>Automatically synchronizes the SD card available in the selected slot.</td>
</tr>
<tr>
<td><strong>Slot-1 Read Error Threshold</strong> field</td>
<td>The number of read errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card.</td>
</tr>
<tr>
<td></td>
<td>If the number of read errors exceeds this threshold on a card, the card is marked unhealthy.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Slot-1 Write Error Threshold</strong> field</td>
<td>The number of write errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card.</td>
</tr>
<tr>
<td></td>
<td>If the number of write errors exceeds this threshold on a card, the card is marked unhealthy.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
</tbody>
</table>
### 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.

### Field | Description
--- | ---
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Drive Enable drop-down list</td>
<td>The virtual drives that can be made available to the server as a USB-style drive.</td>
</tr>
<tr>
<td>RAID Primary Member drop-down list</td>
<td>The slot in which the primary RAID member resides.</td>
</tr>
<tr>
<td>RAID Secondary Role drop-down list</td>
<td>The role of the secondary RAID.</td>
</tr>
</tbody>
</table>
| 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). |
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Write Error Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>Clear Errors check box</td>
<td>If checked, the read/write errors are cleared when you click Submit.</td>
</tr>
</tbody>
</table>

**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:

1. The settings on the server will be set to default.
2. The new settings on the policy will be applied. Hence, 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPMI Over LAN</td>
<td>Check this check box to configure the IPMI properties.</td>
</tr>
<tr>
<td>Privilege Level Limit</td>
<td>Choose a privilege level from the drop-down list.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Enter a key in the field.</td>
</tr>
</tbody>
</table>

   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 #unique_151.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Use Dynamic DNS check box</td>
<td>Dynamic DNS is used to add or update the resource records on the DNS server from Cisco IMC Supervisor</td>
</tr>
</tbody>
</table>

If you check **Use Dynamic DNS** check box
### Creating 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 **Main** screen, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Properties</strong></td>
<td></td>
</tr>
</tbody>
</table>

- **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.

- **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.

- **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.

- **VLAN ID** field
  - The VLAN ID.

- **Priority** field
  - The priority of this system on the VLAN.

b) Click **Next**.

c) On the **Confirm** screen, click **Submit**.

You can see the rack-mount server listed in the Server Platform column in the Hardware Policies page.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Dynamic DNS check box</td>
<td>Dynamic DNS is used to add or update the resource records on the DNS server from Cisco IMC Supervisor</td>
</tr>
<tr>
<td>If you check Use Dynamic DNS check box</td>
<td></td>
</tr>
<tr>
<td>Dynamic DNS Update Domain field</td>
<td>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.</td>
</tr>
<tr>
<td><strong>IPv4 Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Use DHCP check box</td>
<td>If checked, the Obtain DNS Server Addresses from DHCP check box is displayed.</td>
</tr>
<tr>
<td>Obtain DNS Server Addresses from DHCP check box</td>
<td>If checked, enables DHCP for DNS.</td>
</tr>
<tr>
<td>If you do not check Obtain DNS Server Addresses from DHCP check box</td>
<td></td>
</tr>
<tr>
<td>Preferred DNS Server field</td>
<td>The IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Alternate DNS Server field</td>
<td>The IP address of the secondary DNS server.</td>
</tr>
<tr>
<td><strong>IPv6 Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Enable IPv6 check box</td>
<td>If checked, the Use DHCP check box is displayed.</td>
</tr>
<tr>
<td>Use DHCP check box</td>
<td>If checked, the Obtain DNS Server Addresses from DHCP check box is displayed.</td>
</tr>
<tr>
<td>Obtain DNS Server Addresses from DHCP check box</td>
<td>If checked, Cisco IMC Supervisor retrieves the DNS server addresses from DHCP.</td>
</tr>
<tr>
<td>If you do not check Use DHCP check box</td>
<td></td>
</tr>
<tr>
<td>Management IP Address field</td>
<td>Enter the Management IP address.</td>
</tr>
<tr>
<td>Prefix Length field</td>
<td>Enter the number of characters for the prefix length.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>Enter the Gateway IP address.</td>
</tr>
<tr>
<td>If you do not check Obtain DNS Server Addresses from DHCP check box</td>
<td></td>
</tr>
<tr>
<td>Preferred DNS Server field</td>
<td>The IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Alternate DNS Server field</td>
<td>The IP address of the secondary DNS server.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>VLAN Properties</td>
<td></td>
</tr>
<tr>
<td>Enable VLAN check box</td>
<td>If checked, is connected to a virtual LAN.</td>
</tr>
<tr>
<td></td>
<td>If you check Enable VLAN check box</td>
</tr>
<tr>
<td>VLAN ID field</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>Priority field</td>
<td>The priority of this system on the VLAN.</td>
</tr>
</tbody>
</table>

Step 7  Click Next.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname field</td>
<td>The hostname of the server.</td>
</tr>
<tr>
<td>IPv4 Address field</td>
<td>The IPv4 IP address.</td>
</tr>
<tr>
<td>IPv6 Address field</td>
<td>The IPv6 IP address.</td>
</tr>
</tbody>
</table>

Step 9  Click Next.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname field</td>
<td>The hostname of the server.</td>
</tr>
<tr>
<td>IPv4 Address field</td>
<td>The IPv4 IP address.</td>
</tr>
<tr>
<td>IPv6 Address field</td>
<td>The IPv6 IP address.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
### Set the number of days before which you will be notified about the password expiry.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Period field</td>
<td>Set the number of days before which you will be notified about the password expiry.</td>
</tr>
<tr>
<td>Grace Period field</td>
<td>Set the grace period after which the password will expire.</td>
</tr>
</tbody>
</table>

### 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 support 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 type, rearrange 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click Add after selecting Hardware Policies. For accessing this page, see Creating Hardware Policies, on page 81.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Add window, choose Precision Boot Order Policy from the drop-down list and click Submit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check Cisco UCS S3260 check box if the policy is for a Cisco UCS S3260 server and click Next.</td>
</tr>
<tr>
<td>Step 5</td>
<td>On the Main window, check UEFI Secure Boot check box or select the boot mode from the Configure Boot Mode drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click + and select or enter device details. The table lists the devices you have added.</td>
</tr>
</tbody>
</table>
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.

**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.

---

**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.
- Servers containing single storage controllers. On servers containing multiple storage controllers, the RAID policy will be applied only on the storage controller in the first slot.

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.

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Key Management check box</td>
<td>This check box is selected by default.</td>
</tr>
<tr>
<td>Security Key field</td>
<td>Enter a security key.</td>
</tr>
<tr>
<td>Security Key Identifier field</td>
<td>Enter a security key identifier.</td>
</tr>
<tr>
<td>Confirm Security Key field</td>
<td>Confirm the previously entered security key.</td>
</tr>
<tr>
<td>Current Security Key field</td>
<td>Enter the key only when modifying the security key.</td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Drive Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Drive Size</td>
<td></td>
</tr>
<tr>
<td>Disk Group Policy drop-down list</td>
<td>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 #unique_152. Note If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.</td>
</tr>
<tr>
<td>Access Policy drop-down list</td>
<td>Select from the options listed.</td>
</tr>
<tr>
<td>Read Policy drop-down list</td>
<td>Select from the options listed.</td>
</tr>
<tr>
<td>Write Policy drop-down list</td>
<td>Select from the options listed.</td>
</tr>
<tr>
<td>IO Policy drop-down list</td>
<td>Select from the options listed.</td>
</tr>
<tr>
<td>Drive Cache drop-down list</td>
<td>Select from the options listed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Expand to available check box</td>
<td>Expands the virtual drive size to use maximum capacity available on the disks.</td>
</tr>
<tr>
<td>Boot Drive check box</td>
<td>Sets the virtual drive you are creating as a boot drive. Note: You cannot have more than one boot drive.</td>
</tr>
<tr>
<td>Set disks in JBOD state to Unconfigured Good check box</td>
<td>Sets the disks which are in JBOD state to unconfigured good state before they are used for virtual drive creation.</td>
</tr>
<tr>
<td>Enable Full Disk Encryption check box</td>
<td>Creates virtual drive from unused physical drives.</td>
</tr>
</tbody>
</table>

**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.

**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 an 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter a name for the user in the field.</td>
</tr>
<tr>
<td>Role</td>
<td>Choose a role for the user such as read-only, admin and so on from the drop-down list.</td>
</tr>
<tr>
<td>Enable User Account</td>
<td>Check this check box to activate the user.</td>
</tr>
<tr>
<td>New Password</td>
<td>Enter a password associated with the username.</td>
</tr>
<tr>
<td>Confirm New Password</td>
<td>Repeat the password from the previous field.</td>
</tr>
</tbody>
</table>

**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 106.

**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 and enter and or select the adapter details.

- **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.

- **vHBA** — Default properties are fc0 and fc1. You can only edit these properties and cannot delete them.

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

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. Hence, the Cisco UCS S3260 check box in the UI is checked by default.

Step 4  On the Zoning window, 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  Select the local disk details such as the Ownership assigning the ownership of the local disk.

Step 7  Check the Force check box when assigning disks owned by one server to another server.

Step 8  Click Submit.

Step 9  Check the Modify Physical Drive Power Policy check box to set the policy.

Step 10  Select the power state from the Physical Drive Power State drop-down list.

Step 11  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 dialog box, check the Create policy from current configuration of the server check box. You can use the server details in the following two methods. 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.

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.

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.

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** 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 156.
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 141.

**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 and/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 120.
   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 122.

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 Creating a Profile from an Existing Configuration.
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 91
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.
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 141.

**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.

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 122.

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.
Host Image Mapping

Host Image Mapping is a commonly used feature for the E-Series servers. It allows customers to upload an ISO file before installing it. This feature provides an option to upload an iso file to the E-Series servers running CIMC.

You can perform various tasks such as adding, editing, and deleting mapped profiles from this page. See Adding Host Image Mapping Profile, on page 124.

Adding Host Image Mapping Profile

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Policies &gt; Manage Policies and Profiles.</td>
</tr>
<tr>
<td>3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>4</td>
<td>On the Add Host Image Mapping Profile screen, complete the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>Profile Name</strong> field</td>
<td>A descriptive name for the profile.</td>
</tr>
<tr>
<td><strong>Download Image From</strong> drop-down list</td>
<td>Select any of the FTP, SFTP, HTTP, or HTTPS servers to download image.</td>
</tr>
<tr>
<td><strong>Server IP Address</strong> field</td>
<td>IP address of the server.</td>
</tr>
<tr>
<td><strong>File Path</strong> field</td>
<td>The path of the file.</td>
</tr>
<tr>
<td><strong>User name</strong> field (only for FTP and SFTP servers)</td>
<td>The user name.</td>
</tr>
<tr>
<td><strong>Password</strong> field (only for FTP and SFTP servers)</td>
<td>The user password.</td>
</tr>
<tr>
<td><strong>Map After Download</strong> check box</td>
<td>Maps the downloaded image.</td>
</tr>
<tr>
<td><strong>Delete All Images</strong> check box</td>
<td>Deletes all the downloaded images from the server where you apply this profile.</td>
</tr>
<tr>
<td>5</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

What to Do Next

You can also edit, delete, or apply a profile. You can see if the image is downloaded successfully and if the downloaded images are mapped (if you have checked the Map After Download check box) successfully using the View Status Details option.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User defined name of the tag library.</td>
</tr>
<tr>
<td>Description</td>
<td>User defined brief description of the tag library.</td>
</tr>
<tr>
<td>Type</td>
<td>String or an integer.</td>
</tr>
<tr>
<td>Possible Tag Values</td>
<td>User defined tag values.</td>
</tr>
<tr>
<td>Applies To</td>
<td>Rack mount servers or users.</td>
</tr>
</tbody>
</table>

Creating a Tag Library

Perform this procedure when you want to create a tag library.

Procedure

1. Choose Policies > Tag Library.
2. Click Create.
3. In the Create Tag screen, complete the following fields for Tag Details:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>A descriptive name for the tag.</td>
</tr>
<tr>
<td>Description field</td>
<td>(Optional) A description of the tag.</td>
</tr>
<tr>
<td>Type drop-down list</td>
<td>Select String or Integer.</td>
</tr>
<tr>
<td>Possible Tag Values field</td>
<td>The possible values for the tag.</td>
</tr>
</tbody>
</table>
4. Click Next.
5. In the Applicability Rules pane, complete the following:
Choose the entities on which the tag needs to be applied.

To add an entity, do the following:
1. Click the + icon.
2. From the Category drop-down list, choose the category. It can be one of the following:
   • Physical_Compute
   • Administration
3. Choose the taggable entities from the table.
4. Click Submit.

The tags are displayed under the respective category according to the set taggable entities.

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

Managing Cisco UCS Hardware Compatibility Report

This chapter contains the following topics:

- Overview, page 129
- Tagging OS Vendor and Version, page 130
- Creating Hardware Compatibility Reports, page 130
- Synchronizing Hardware Compatibility Reports, page 131

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 38.
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/](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 38.
- Ensure that you have tagged the rack server with the operating system vendor and version. See Tagging OS Vendor and Version, on page 130.

**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 cisco.com credentials. See Configuring Cisco.com User, on page 38.

**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.
Firmware Profiles

This chapter contains the following topics:

- Firmware Management Menu, page 133

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.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Systems &gt; Firmware Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Images - Local tab and click + to add an image.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Add Firmware Image - Local screen, complete the following:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Profile Name field</td>
<td>Enter a descriptive and unique profile name.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Configuration check box</td>
<td>(Optional) This check box picks up the proxy configuration details you have set.</td>
<td>The Cisco.com user credentials and proxy configuration details that you have already configured are automatically picked up. For setting up Cisco.com credentials, see Configuring Cisco.com User, on page 38 and for setting up proxy configuration, see Configuring Proxy, on page 38.</td>
</tr>
<tr>
<td>Platform drop-down list</td>
<td>Choose a platform from the drop-down list.</td>
<td>Only platforms that manage at least one server is listed here.</td>
</tr>
<tr>
<td>Available Image drop-down list</td>
<td>Choose the iso image from the drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Download Now check box</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Accept License Agreement</td>
<td>Check this check box to accept the license agreement. Click on the Terms and Conditions link to read the End User License Agreement.</td>
<td>You cannot create a firmware profile without accepting the license agreement even if you want to download the image later.</td>
</tr>
</tbody>
</table>

**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.
**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Systems &gt; Firmware Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the More Actions drop-down list, choose Upload to add an image.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Upload Firmware Image - Local screen, complete the following:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Profile Name field</td>
<td>Enter a descriptive and unique profile name.</td>
</tr>
<tr>
<td>Platform drop-down list</td>
<td>Select the C-Series or E-Series platform.</td>
</tr>
<tr>
<td>File field</td>
<td>Select a file and drop it in this field or click Select a File to upload on your local file system.</td>
</tr>
</tbody>
</table>

| 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Systems &gt; Firmware Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Firmware Management page, click Images - Network and click + to add an image.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Add Firmware Image - Network screen, complete the following:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Profile Name field</td>
<td>A descriptive and unique name for the profile. The profile name must be unique.</td>
</tr>
<tr>
<td>Platform drop-down list</td>
<td>Choose a platform from the drop-down list. Only platforms that manage at least one server are listed here.</td>
</tr>
<tr>
<td>Server Type drop-down list</td>
<td>Choose either Network File System (NFS), Common Internet File System (CIFS) or HTTP/S server types.</td>
</tr>
</tbody>
</table>
### Firmware Profiles

#### Upgrading Firmware

#### Before You Begin

If you are upgrading to Cisco IMC version 2.0(x), you must change the default Cisco IMC password.

---

**Note**

Cisco does not recommend upgrading both servers, that are part of a single Cisco UCS S3260 Dense Storage Rack Server chassis, simultaneously.

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 38 and Configuring Proxy, on page 38.
Procedure

**Step 1** Choose Systems > Firmware Management.

**Step 2** On the Firmware Management page, 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Profile</td>
<td>Choose a profile from the drop-down list.</td>
</tr>
<tr>
<td>Platform</td>
<td>You can view details such as server platform, firmware image version, and path for the selected firmware profile.</td>
</tr>
<tr>
<td>Image Version</td>
<td></td>
</tr>
<tr>
<td>Image Path</td>
<td></td>
</tr>
<tr>
<td>Server(s) button</td>
<td>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.</td>
</tr>
<tr>
<td>Schedule later</td>
<td>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 141. You can go to Policies &gt; 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.</td>
</tr>
</tbody>
</table>

**Step 6** Click Submit.

**Note** You can also view firmware upgrade details and delete the status records for the specified upgrade operation.
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 patch. For more information about applying a patch, see section Applying a 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

For Cisco IMC Supervisor to run periodic checks (once in 14 days) for new patch updates, you must provide your support credentials and other details. These details will be used by Cisco IMC Supervisor to communicate with the Cisco ASD backend service to query for any new updates. Any new versions of the patch will automatically be downloaded into the Cisco IMC Supervisor appliance.
Procedure

**Step 1** Choose Administration > Update IMCS.

**Step 2** On the Update IMCS page, click **Check For Updates Now** to check for Cisco IMC Supervisor updates.

**Step 3** Click **Submit**.

The report displays the latest updates.

**Step 4** Click the **Export Report** icon to export the report to either PDF, CSV, or XLS format.

**Step 5** Click **Generate Report** to generate a report.

**Step 6** Click **Download** to download the report or click **Close**.
Managing Schedules

This chapter contains the following topics:

- Overview of Managing Schedules, page 141
- Creating Schedules, page 141

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Name field</td>
<td>Enter a name for the schedule task.</td>
</tr>
<tr>
<td>Enable Schedule check box</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Creating Schedules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler Type radio button</td>
<td>Select a one time schedule or recurring schedule frequency.</td>
</tr>
<tr>
<td></td>
<td>If you choose a <strong>One Time</strong> schedule, select the date, time, and AM or PM radio buttons.</td>
</tr>
<tr>
<td>Note</td>
<td>The schedule time is based on the time on the appliance. However, the time zone is of the local client browser.</td>
</tr>
<tr>
<td></td>
<td>If you choose a <strong>Recurring</strong> schedule, select the days (0 to 30 days), hours and minutes from the drop-down lists.</td>
</tr>
</tbody>
</table>

**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, Performing Auto Discovery, Applying a Hardware Policy**, on page 118, or **Applying a Hardware Profile**, on page 122.

- You can select one or more tasks associated with the schedule and disassociate them from the schedule using the **Remove Scheduled Tasks** option.
Running Server Diagnostics

This chapter contains the following topics:

- Overview of Server Diagnostics, page 143
- Configuring Server Configuration Utility Image Location, page 144
- Running Diagnostics, page 144

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 scpuser password to run server diagnostics. To configure the scpuser password, see Configuring a SCP User, on page 36.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name field</td>
<td>A descriptive name for the profile.</td>
</tr>
<tr>
<td>ISO Share Type drop-down list</td>
<td>Choose either Network File System (NFS), Common Internet File System (CIFS), World Wide Web (WWW) or LOCAL share types.</td>
</tr>
</tbody>
</table>

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.
Procedure

**Step 1** Choose **Systems > Server Diagnostics**.

**Step 2** Click **Run Diagnostics**.

**Step 3** On the **Run Diagnostics** page, complete the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Profile</strong> drop-down list</td>
<td>Select an existing profile from the drop-down list.</td>
</tr>
<tr>
<td><strong>Choose</strong> drop-down list</td>
<td>Choose whether you want to run the diagnostics on a server or server group from the drop-down list.</td>
</tr>
<tr>
<td><strong>Server(s) or Server Group(s)</strong> drop-down list</td>
<td>Choose the server(s) or server group(s) for which you want to run the diagnostics.</td>
</tr>
</tbody>
</table>

**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.
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 147.

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, on page 38.
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 148. For logging in to Smart Call Home and performing various tasks, see https://supportforums.cisco.com/community/4816/smart-call-home and for viewing messages received at the Smart Call Home backend see http://tools.cisco.com/sch/.
  • Ensure that the URL https://tools.cisco.com/its/service/oddce/services/DDCEService is reachable from the Cisco IMC Supervisor appliance.

Fault Codes

Following are a list of error messages that Cisco IMC Supervisor sends to the Smart Call Home backend.

<table>
<thead>
<tr>
<th>Fault Code</th>
<th>Fault Name</th>
<th>Message</th>
<th>Severity</th>
<th>Create Service Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>F0174</td>
<td>fltProcessorUnitInoperable</td>
<td>Processor [id] on [serverId] operability: [operability]</td>
<td>critical</td>
<td>Y</td>
</tr>
<tr>
<td>F0177</td>
<td>fltProcessorUnitThermalThresholdNonRecoverable</td>
<td>Processor [id] on [serverId] temperature:[thermal]</td>
<td>critical</td>
<td>Y</td>
</tr>
<tr>
<td>Fault Code</td>
<td>Fault Name</td>
<td>Message</td>
<td>Severity</td>
<td>Create Service Request</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>F0181</td>
<td>fltStorageLocalDiskInoperable</td>
<td>Local disk [id] on [serverid] operability: [operability]</td>
<td>major warning</td>
<td>Y</td>
</tr>
<tr>
<td>F0185</td>
<td>fltMemoryUnitInoperable</td>
<td>DIMM [location] on [serverid] operability: [operability]</td>
<td>major</td>
<td>Y</td>
</tr>
<tr>
<td>F0188</td>
<td>fltMemoryUnitThermalThresholdNonRecoverable</td>
<td>DIMM [location] on [serverid] temperature: [thermal]</td>
<td>critical</td>
<td>N</td>
</tr>
<tr>
<td>F0389</td>
<td>fltEquipmentPsuVoltageThresholdCritical</td>
<td>Power supply [id] in [serverid] voltage: [voltage]</td>
<td>major</td>
<td>N</td>
</tr>
<tr>
<td>F0407</td>
<td>fltEquipmentPsuIdentity</td>
<td>Power supply [id] on [serverid] has a malformed FRU</td>
<td>critical</td>
<td>N</td>
</tr>
<tr>
<td>F0411</td>
<td>fltEquipmentChassisThermalThresholdNonRecoverable</td>
<td>Thermal condition on [serverid] cause: [thermalStateQualifier]</td>
<td>critical</td>
<td>N</td>
</tr>
<tr>
<td>F0424</td>
<td>fltComputeBoardCmosVoltageThresholdCritical</td>
<td>CMOS battery voltage on [serverid] is [cmosVoltage]</td>
<td>major</td>
<td>N</td>
</tr>
<tr>
<td>F0425</td>
<td>fltComputeBoardCmosVoltageThresholdNonRecoverable</td>
<td>CMOS battery voltage on [serverid] is [cmosVoltage]</td>
<td>critical</td>
<td>Y</td>
</tr>
<tr>
<td>F0531</td>
<td>fltStorageRaidBatteryInoperable</td>
<td>RAID Battery on [serverid] operability: [operability]</td>
<td>major</td>
<td>Y</td>
</tr>
<tr>
<td>Fault Code</td>
<td>Fault Name</td>
<td>Message</td>
<td>Severity</td>
<td>Create Service Request</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------</td>
<td>----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>F0868</td>
<td>fltComputeBoardPowerFail</td>
<td>Motherboard of [serverid] power: [power]</td>
<td>critical</td>
<td>N</td>
</tr>
<tr>
<td>F0997</td>
<td>fltStorageRaidBatteryDegraded</td>
<td>Raid battery [id] on [serverid] operability: [operability]</td>
<td>major</td>
<td>N</td>
</tr>
<tr>
<td>F1004</td>
<td>fltStorageControllerInoperable</td>
<td>Storage Controller [id] operability: [operability]</td>
<td>critical</td>
<td>N</td>
</tr>
<tr>
<td>F1007</td>
<td>fltStorageVirtualDriveInoperable</td>
<td>Virtual drive [id] on [serverid] operability: [operability]</td>
<td>critical</td>
<td>N</td>
</tr>
</tbody>
</table>
CHAPTER 15

Managing Cisco UCS S3260 Dense Storage Rack Server

This chapter contains the following topics:

• About Cisco UCS S3260 Dense Storage Rack Server, page 151
• Cisco UCS S3260 Dense Storage Rack Server Architectural Overview, page 152
• Cisco IMC Supervisor with Cisco UCS S3260 Dense Storage Rack Server, page 153
• Adding a Rack Account, page 153
• Managing Cisco UCS S3260 Rack Server, page 154
• Policies and Profiles, page 156
• Upgrading Firmware, page 157
• Viewing Cisco UCS S3260 Dense Storage Rack Server Details, page 157

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 S3260 Rack 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 57. 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 77. 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    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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Systems &gt; Inventory and Fault Status.</td>
</tr>
<tr>
<td>2</td>
<td>On the Rack Groups page, click Chassis.</td>
</tr>
<tr>
<td>3</td>
<td>Click Front Locator LED.</td>
</tr>
<tr>
<td>4</td>
<td>From the Turn the Front Locator LED for selected chassis on/off drop-down list, choose ON or OFF.</td>
</tr>
<tr>
<td>5</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

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 82.

Before You Begin
The server is already added as a Rack Account under 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Systems &gt; Inventory and Fault Status.</td>
</tr>
<tr>
<td>2</td>
<td>Click Add Tags.</td>
</tr>
</tbody>
</table>
**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. Refer Managing Tags for Cisco UCS S3260 Rack Server, on page 155 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 now have a new column **Server Platform** indicating if the policy is Cisco UCS S3260 or others. Chassis policies irrespective of User Administration Policies or Compute Node policies 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 90.

The following policies are User Administration Policies and Compute Node policies:

<table>
<thead>
<tr>
<th>User Administration Policies</th>
<th>Compute Node Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>BIOS</td>
</tr>
<tr>
<td>SNMP</td>
<td>Precision Boot Order</td>
</tr>
<tr>
<td>LDAP</td>
<td>RAID</td>
</tr>
<tr>
<td>NTP</td>
<td>KVM</td>
</tr>
<tr>
<td>Network Security</td>
<td>vMedia</td>
</tr>
<tr>
<td>SSH</td>
<td>VIC</td>
</tr>
<tr>
<td>NTP</td>
<td>Serial Over LAN</td>
</tr>
</tbody>
</table>
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 119.

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 136.

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.
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:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 106.  
                 | **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. |
| 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 84.  
<pre><code>             | **Note** Not applicable for Cisco UCS S3260 dense storage rack server. |
</code></pre>
<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated Hardware Profiles</td>
<td>Details of policies that are associated to a hardware profile.</td>
</tr>
<tr>
<td>Chassis Summary</td>
<td>Summary of properties such as CMC 1 network, common, and NIC.</td>
</tr>
<tr>
<td>Rack Servers</td>
<td>Rack server details such as hostname, IP address, and connection status.</td>
</tr>
<tr>
<td>System IO Controller</td>
<td>Details such as IP address, MAC address, and firmware version.</td>
</tr>
<tr>
<td>SAS Expander</td>
<td>Details such as ID, SAS name, and firmware version.</td>
</tr>
<tr>
<td>Zoning</td>
<td>Details such as health, presence, ownership, and size.</td>
</tr>
</tbody>
</table>

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

This chapter contains the following topics:

- Support Information, page 161

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Support Information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Support Information window, you can view:</td>
</tr>
</tbody>
</table>

**Table 2: System information (basic)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Information</td>
<td>Choose System Information (Basic) and click Submit to view basic information.</td>
</tr>
</tbody>
</table>
Table 3: System information (advanced)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Information</td>
<td>Choose System Information (Advanced) and click Submit to view advanced information such as processor, memory, disk information and so on.</td>
</tr>
</tbody>
</table>

Table 4: View Logs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Information</td>
<td>Choose Show log.</td>
</tr>
<tr>
<td>Show Log</td>
<td>Choose the log type you want to view and click Show Logs.</td>
</tr>
</tbody>
</table>

Table 5: Download All Logs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Information</td>
<td>Choose Download All Logs and click Download.</td>
</tr>
</tbody>
</table>

Table 6: Download Debug Logging

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. To stop and download log data, click Stop Debug Logging and click the download debug link.</td>
</tr>
</tbody>
</table>

Table 7: API Logging

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Information</td>
<td>1. Choose API Logging and click Start API Logging.</td>
</tr>
<tr>
<td></td>
<td>2. To stop and download log data, click Stop API Logging and click the download API debug logs link.</td>
</tr>
</tbody>
</table>
CHAPTER 17

Frequently Performed Tasks and Procedures

This chapter contains the following topics:

- Frequently Performed Procedures, page 163
- Miscellaneous Procedures, page 163

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.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to log in Cisco IMC Supervisor</td>
<td>Launching Cisco IMC Supervisor, on page 18</td>
</tr>
<tr>
<td>How to upgrade license</td>
<td>Updating the License, on page 19</td>
</tr>
<tr>
<td>How to add login users in Cisco IMC Supervisor</td>
<td>Creating a User Account, on page 44</td>
</tr>
<tr>
<td>How to add a rack group</td>
<td>Adding a Rack Group, on page 57</td>
</tr>
<tr>
<td>How to create a rack account</td>
<td>Adding a Rack Account, on page 57</td>
</tr>
</tbody>
</table>

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. The Automatic Refresh option changes to ON and Interval slide bar is visible.

**Step 3** Using the Interval, set the refresh rate.
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**

1. **Step 1** Browse to the summary report you want to add to the dashboard.
2. **Step 2** Click the down arrow on the right upper corner of the report panel.
3. **Step 3** Click **Add to Dashboard**.
   - **Note** *Add to Dashboard* option is available only if the summary report supports dashboard view.
4. **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**

1. **Step 1** Log into Cisco IMC Supervisor user interface.
   - The default **Dashboard** screen is displayed.
2. **Step 2** Click the drop-down list to view the list of dashboards that you have created.
3. **Step 3** Click the X mark displayed next to the dashboard name.
4. **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.
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 Step 3 and Step 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:

1. From Select Report Format drop-down list, choose PDF, CSV, or XLS.
2. Click Generate Report.
3. 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.