Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 1.1

First Published: December 01, 2015

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

This preface contains the following sections:

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

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.

Text Type	Indication
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

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.

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

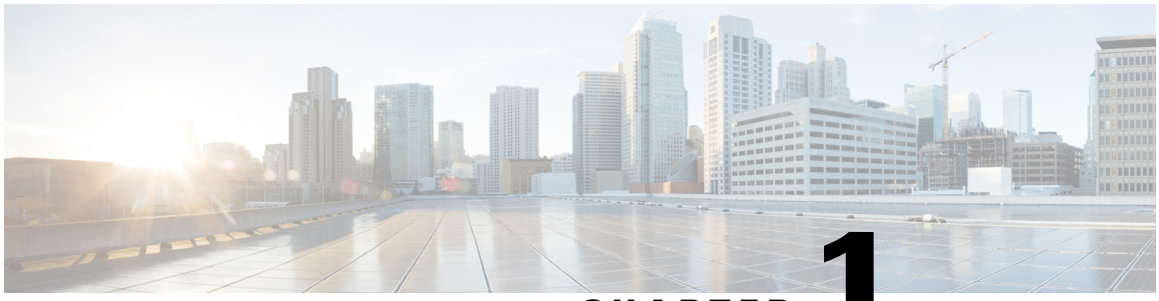
Documentation Feedback

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.



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following section:

New and Changed Information for this Release

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

Table 1: New Features and Changed Behavior in Cisco IMC Supervisor, Release 1.1.0.1

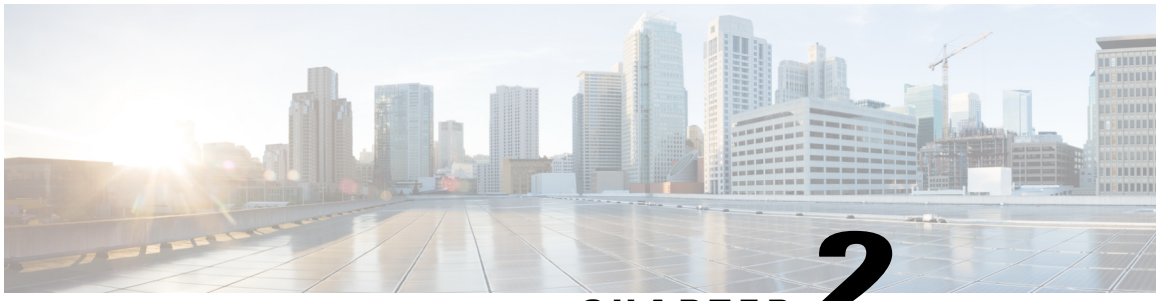
Feature	Description	Where Documented
Support for Selecting Multiple Servers	You can select multiple rack servers and perform various actions such as powering on/off, hard reset, power cycle and so on.	For the various actions, see sections under Inventory and Fault Status for Rack Groups, on page 11
Managing Tags for All Rack Groups	You can select the top level rack groups, select multiple servers and manage tags for all the selected servers.	Managing Tags for a Rack Mount Server, on page 19
Collecting Inventory for Multiple Rack Accounts or Rack Groups	You can manage your rack accounts or servers better by collecting inventory for one or more rack accounts or rack groups.	Collecting Inventory for Multiple Rack Accounts or Rack Groups, on page 28
Assigning Rack Accounts to a Rack Group	You can assign a server or multiple servers to a rack group from the Systems menu.	Assigning Rack Accounts to a Rack Group, on page 28

Feature	Description	Where Documented
Support for HTTP(S) Based Network Images for Firmware Upgrade	You can download and add a firmware image from a network server using the HTTP/S server type option available in the Firmware Management Menu.	Adding Images from a Network Server, on page 35

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 2: New Features and Changed Behavior in Cisco IMC Supervisor, Release 1.1

Feature	Description	Where Documented
FlexFlash Inventory	You can view the details of FlexFlash adapters used in the server such as Controller Info, Physical Drives and so on.	Viewing a Rack Mount Server Details, on page 12
Enhancement to Managing Firmware	New UI enhancements are available for Firmware download and upgrade and you can view the images hosted in IMCSupervisor and on the network separately from the UI. It now supports downloading local images for new M4 models and E-Series.	Firmware Management Menu, on page 33
Managing Policies and Profiles	Support for managing policies and profiles has been introduced in this release. You can now create hardware policies by configuring various properties such as BIOS, LDAP, Users and so on. A combination of existing set of hardware policies make up a profile. You can now apply configuration details of a rack server profile for example, to multiple rack-mount servers. You can also associate this hardware profile to specific rack-mount servers. You can perform various management tasks such as adding, editing, and deleting hardware policies and profiles.	Managing Policies, on page 37
Email Alerts	You can create, update, or delete multiple email alerts. Alert levels are introduced for each email alert sent.	System Menu, on page 70



CHAPTER 2

Overview

This chapter contains the following topics:

About Cisco IMC Supervisor

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

You can use Cisco IMC Supervisor to perform the following tasks for a rack mount server:

- Support for logical grouping of servers and summary views per group
- Collect inventory for the servers
- Provide monitoring capabilities for servers and groups
- Firmware management including firmware download, upgrade, and activation
- Manage standalone server actions including power control, LED control, log collection, KVM launch, CIMC UI launch and e-mail alerts
- Role Based Access Control (RBAC) to restrict access
- Email alerts
- Configure server properties using Policies and Profiles

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 (60 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.

The process for obtaining and installing the licenses is the same.

You must obtain a license to use Cisco IMC Supervisor, as follows:

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 4.
3. After you install Cisco IMC Supervisor, update the license in Cisco IMC Supervisor as described in Updating the License, on page 7.
4. After the license has been validated, you can start to use Cisco IMC Supervisor.

Fulfilling the Product Access Key

Before You Begin

You need the PAK number.

Procedure

Step 1 Navigate to the Cisco Software License website.

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

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

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

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

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

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

Step 7 Click **Issue Key**.
The features for your license appear, and an email with the Digital License Agreement and a zipped license file is sent to the email address you provided.

Common Terms in Cisco IMC Supervisor User Interface

Rack Groups

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

Note There is a **Default Group** already included in Cisco IMC Supervisor. You cannot delete or modify the **Default Group**. You may add new Rack Accounts in the **Default Group** or create a new Rack Group as per your requirement.

Rack Account

Rack Account is a stand alone 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.

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

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

Procedure

Step 1 Update the value for the redirectPort parameter to **443** in the `server.xml` file.
This file is located in the `/opt/infra/web_cloudmgr/apache-tomcat/conf/` directory.

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

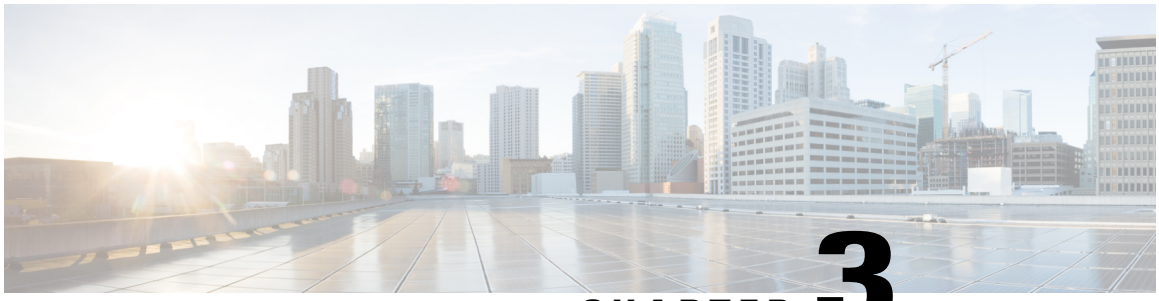
Step 2 Uncomment the following lines in the `web.xml` file:

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

You can add these lines anywhere in the file.

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

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



CHAPTER 3

Getting Started

This chapter contains the following topics:

Launching Cisco IMC Supervisor

Perform this procedure to log in to Cisco IMC Supervisor.

Before You Begin

- Cisco IMC Supervisor is installed successfully.
- 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

Updating the License

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 From the menu bar, choose **Administration** > **License**.

Step 2 Select the **License Keys** tab.

Step 3 Click **Update License**.

Step 4 In the **Update License** dialog box, 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.

Adding a Rack Group

Perform this procedure when you want to add a new Rack Group in Cisco IMC Supervisor.

Before You Begin

If you have logged in for the first time, ensure that the license are updated for Cisco IMC Supervisor. Refer Updating the License, on page 7 to update licenses.

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.
By default, **Rack Group** tab is selected.

Step 2 Click **Create**.

Step 3 In the **Create Rack Group** dialog box, complete the following fields:

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

Step 4 Click **Create**.

Step 5 In the **Submit Result** dialog box, click **OK**.

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 Rack Group to the Cisco IMC Supervisor. Once 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 mount server to an existing Rack Group.

Before You Begin

- If you have logged in for the first time, ensure that the license are updated for Cisco IMC Supervisor. Refer Updating the License, on page 7 to update licenses.
- You have already created a Rack Group.

Note You may still add a Rack Account under **Default Group** without creating a new Rack Group.

- In Cisco IMC, XML API must be enabled so that you can add/manage the rack server from Cisco IMC Supervisor.

Procedure

Step 1 From the menu bar, choose **System** > **Physical Accounts**.

Step 2 Click the **Rack Accounts** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Create Account** dialog box, complete the following fields:

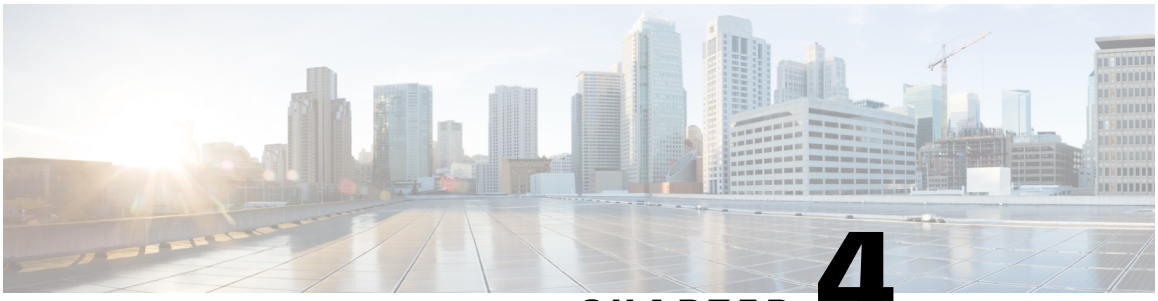
Field	Description
Account Name field	A descriptive name for the Rack Account.
Server IP field	The IP address of the rack mount server.
Description field	(Optional) A description of the Rack Account.
Use Credential Policy check box	(Optional) If you have already created credential policies, then check this 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	

Field	Description
User Name field	Login ID for the rack mount server.
Password field	Password for the login ID for the rack mount server.
Protocol drop-down list	Choose https or http from the list.
Port field	The port number associated with the selected protocol.
Rack Group drop-down list	Choose a rack group from the list.
Contact field	(Optional) The contact email address for the account.
Location field	(Optional) The location of the account.

Step 5 Click **Submit**.

What to Do Next

Test the rack server connection. Refer Testing Account Connection, on page 27.



CHAPTER 4

Managing Servers Using Systems Menu

This chapter contains the following topics:

Inventory and Fault Status for Rack Groups

Systems menu contains **Inventory and Fault Status** and **Physical Accounts** menu options. **Inventory and Fault Status for Rack Groups** page is divided vertically into two sections. Left pane contains the list of the Rack Groups. If the list is collapsed, click the down arrow beside **Rack Groups** to expand the view. You will see the default and all the user defined Rack Groups. You can manage and monitor all C-series and E-series servers using this option.

Note If you are logging in for the first time, then **Default Group** is the only Rack Group available. Refer Adding a Rack Group, on page 8 to add more Rack Groups.

When **Rack Groups** heading is selected in the left pane, the following tabs are available in the right pane:

Tab	Description
Summary	You can add summary reports to the Summary page for quick view. Refer Adding Summary Reports to Dashboard, on page 98 to add summary reports.
Rack Servers	Rack Servers tab provides the details of the rack mount servers added to all the Rack Groups.
Faults	Faults tab provides the details for all the faults logged in Cisco IMC Supervisor.
More Reports	More Reports tab provides additional reports in the form of pie chart for faults, server health, firmware versions, server models, and power state.

When any Rack Group is selected in the left pane (including **Default Group**), the following tabs are available in the right pane:

Tab	Description
Summary	You can add summary reports of the selected group to the Summary page for quick view. Refer Adding Summary Reports to Dashboard, on page 98 to add summary reports.
Rack Servers	Rack Servers tab provides the details of the rack mount servers added to the selected Rack Group.
Faults	**Faults** tab provides the details for all the faults logged in the selected Rack Group for the rack mount servers.
More Reports	More Reports tab provides additional reports in the form of pie chart for faults, server health, firmware versions, server models, and power state.

Server Task Under Inventory and Fault Status Tab

Viewing a Rack Mount Server Details

Perform this procedure when you want to view the details of a rack mount server.

Note You can also perform this procedure by clicking **Rack Groups** in the left pane.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

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

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

The following details are available for a rack mount server:

Tab	Description
Summary	Provides an overview of the Rack Account.
CPUs	Provides the details of the CPU used in the server.

Tab	Description
Memory	Provides the details of the memory used in the server.
PSUs	Provides the details of the power supply unit used in the server.
PCI Adapters	Provides the details of the PCI adapters used in the server.
VIC Adapters	Provides 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**, **VM FEXs** and so on.
Network Adapters	Provides the details of the network adapters used in the server. Select any of the Network Adapters listed and click **View Details** to view information on **External Ethernet Interfaces**.
Storage Adapters	Provides the details of the storage adapters used in the server. Select any of the Storage Adapters listed and click **View Details** to view information such as **Controller Info**, **Physical Drives** and so on.
FlexFlash Adapters	Provides 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**, **Physical Drives** and so on. If you are upgrading Cisco IMC Supervisor from a previous version, you must run the inventory by going to **Systems** > **Physical Accounts** > **Rack Accounts** > **Inventory** or wait for the periodic inventory to run for the flexflash details to appear in the report.
Communication	Provides the details of HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.
Remote Presence	Provides the details of vKVM, Serial Over LAN, and vMedia.
Faults	Provides the details of the faults logged in the server.
Users	Provides the details of users.
Cisco IMC Log	Provides the details of the Cisco IMC logs for the server.
System Event Log	Provides the details of the server logs.
TPM	Provides information on the TPM inventory.
BIOS	Provides 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	Provides historical information on the faults that occurred on the server.

Tab	Description
Tech Support	Provides an option to export the tech-support log files to a remote server using one of the following protocols: • FTP • TFTP • SFTP • SCP **Note** Currently, downloading the tech-support log file to a local system is not supported.
Associated Hardware Profiles	Provides details of policies that are associated to a hardware profile.

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

Viewing a Rack Mount Server Fault Details

Perform this procedure when you want to view the fault details of a rack mount server.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Faults** tab.

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

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

The following details are available for a rack mount server:

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

Step 5 Click **Close** in the **Fault Details** window to go to the previous window.

Powering On/Off a Rack Mount Server

Perform this procedure when you want to power on or off 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 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

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

Step 5 Click **Power ON** or **Power OFF** or right-click and choose the options.

Note You cannot see **Power ON** and **Power OFF** buttons till you select the server from the list.

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

Note A message that the servers were powered on or 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.

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 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **Shut Down** or right-click and choose the option.

Note You cannot see the **Shut Down** button till you select the server from the list. You can also click the down arrow on the far right and choose the option.

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

Performing a Hard Reset on Rack Mount Server

Perform this procedure when you want to hard reset 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 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **Hard Reset**.

Note You cannot see the **Hard Reset** button till you select the server from the list. You can also click the down arrow on the far right and choose the option.

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

Performing a Power Cycle on Rack Mount Server

Perform this procedure when you want to do a power cycle on 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 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **Power Cycle**.

Note You cannot see **Power Cycle** button till you select the server from the list. You can also click the down arrow on the far right and choose the option.

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

Launching KVM Console for a Rack Mount Server

Perform this procedure when you want to launch KVM console for a rack mount server.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **KVM Console**.

Note You cannot see **KVM Console** button till you select the server from the list.

Step 6 Click **Submit**.
Cisco IMC Supervisor downloads the *kvm.jnlp* file.

Step 7 Double-click on the *kvm.jnlp* file in your downloads folder.
The KVM Console opens in a separate window.

If you do not have the required Java Runtime Environment (JRE) installed, click **More Info** in the dialog box and follow the instructions to download and install the JRE.

Launching GUI for a Rack Mount Server

Perform this procedure when you want to launch GUI for a rack mount server.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **Launch GUI**.

Note You cannot see the **Launch GUI** button till you select the server from the list.

Step 6 In the **Launch GUI** dialog box, click **Submit**.
The GUI for the server is launched in a separate browser.

Setting Locator LED for a Rack Mount Server

Perform this procedure when you want to set locator LED for 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 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **Locator LED**.

Note You cannot see **Locator LED** button till you select a server from the list.

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

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Setting Label for a Rack Mount Server

Perform this procedure when you want to set label for a rack mount server.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Select the sever from the list.

Step 5 Click **Set Label**.

Note You cannot see **Set Label** button till you select the server from the list.

Step 6 Enter a new label.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Managing Tags for a Rack Mount Server

Before You Begin

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

Perform this procedure when you want to manage tags for a rack mount server.

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, expand **Rack Groups** and select the Rack Group which contains the server

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Click **Manage Tags**.

Note You cannot see **Manage Tags** button till you select the server from the list.

Step 5 Click on the plus icon to add a new tag. In the **Add Entry to Tag** dialog box, complete the following:

Field	Description
Tag Name	Select the tag name from the drop-down list and click **Submit** or create a new tag. **1** Click the + icon. **2** In the **Create Tag** window, do the following: **a** In the **Name** field, enter a descriptive name for the tag. **b** In the **Description** field, enter a description of the tag. **c** In the **Type** field, select String or Integer from the drop-down list. **d** In the **Possible Tag Values** field, enter a possible value for the tag. **e** Click **Next**. **f** Click the + icon to add a new category. **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. **4** Choose the taggable entities from the table. **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**.
Tag Value	Select the tag value from the drop-down list.

Step 6 Click **Submit**.
Step 7 In the **Submit Result** dialog box, click **OK**.
Step 8 Select a tag in the **Manage Tags** dialog box and click on the Edit icon to edit a tag.
Step 9 Choose the Tag Name and Tag Value to modify the tags
Step 10 Click **Submit**
Step 11 In the **Submit Result** dialog box, click **OK**.
Step 12 Select a tag in the **Manage Tags** dialog box and click on the Delete icon to delete a tag.
Step 13 Click Submit if you are sure you want to delete the tag.
Step 14 In the **Submit Result** dialog box, click **OK**.

Adding Tags for a Rack Mount Server

Before You Begin

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

Perform this procedure when you want to add tags for a rack mount server.

Note You can also select multiple rack servers.

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.
Step 2 In the left pane, expand **Rack Groups** and select the Rack Group which contains the server.
Step 3 In the right pane, select the **Rack Servers** tab.
Step 4 Click **Add Tags**.
Note You cannot see **Add Tags** button till you select the server from the list.
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 19 to create tags.

Deleting Tags for a Rack Mount Server

Before You Begin

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

Perform this procedure when you want to add tags for a rack mount server.

Note You can also select multiple rack servers.

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

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

Step 3 In the right pane, select the **Rack Servers** tab.

Step 4 Click **Delete Tags**.

Note You cannot see **Delete Tags** button till you select the server from the list.

Step 5 Check the check box against the tag name that you want to delete or check the check box against **Tag Name** to delete all the available tags.

Step 6 Click **Submit**.

Exporting Technical Support Data to a Remote Server

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

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

Step 5 Click the **Tech Support** tab.

Step 6 Click **Upload Logs**.

Step 7 In the **Upload Technical Logs** dialog box, complete the following fields:

Name	Description
Network Type drop-down list	The network type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP**

Name	Description
Server IP/Hostname field	The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Network Type** drop-down list, the name of this field will vary.
Path and Filename field	The path and filename that must be used when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the network type is TFTP.
Password	The password for the remote server username. This field does not apply if the network type is TFTP.

Step 8 Click **Submit**.

Clearing SEL

Procedure

Step 1 From the menu bar, choose **Systems** > **Inventory and Fault Status**.

Step 2 In the left pane, select **Rack Groups** or expand **Rack Groups** and select the Rack Group which contains the server.

Step 3 In the right pane, select the **Rack Servers** tab.

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

Step 5 Click the **System Event Log** tab.

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

Step 7 (Optional) In the **Clear IMC SEL Logs** dialog box, 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**.

Physical Accounts Menu

Physical Accounts menu displays the following tabs:

Tab	Description
Rack Groups	This tab displays all the rack groups in Cisco IMC Supervisor.
Rack Accounts	This tab displays all the rack accounts in Cisco IMC Supervisor. You can also use this tab to create, edit, delete, and test rack accounts.
Discovered Devices	This tab displays all the devices which are in the configured subnet. You can also configure and delete a profile in this tab.

Managing Physical Servers

Managing Rack Groups

Adding a Rack Group

Refer Adding a Rack Group, on page 8 to create rack groups.

Editing a Rack Group

Perform this procedure when you want to edit a rack group.

Before You Begin

The rack group has already been created under Rack Groups.

Note You cannot edit the Default Rack Group.

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.

Step 2 From the list of groups, select the group you want to edit.

Step 3 Click **Modify**.

Note You cannot see the **Modify** button till you select the rack group from the list.

Step 4 In the **Modify Rack Group** dialog box, complete the following fields:

Field	Description
New Group Name field	A descriptive name for the Rack Group.
New Description field	(Optional) A description of the Rack Group.

Step 5 Click **Modify**.

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

Deleting a Rack Group

Perform this procedure when you want to delete a rack group.

Before You Begin

The rack group has already been created under Rack Groups.

Note You cannot delete the Default Rack Group.

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.

Step 2 From the list of groups, select the group you want to delete.

Step 3 Click **Delete**.

Note You cannot see the **Delete** button till you select the rack group from the list.

Step 4 (Optional) If you want to delete the rack accounts associate with the rack group you want delete, then check the **Delete rack accounts within rack group (rack group name)** checkbox.

Note If you leave **Delete rack accounts within rack group (rack group name)** unchecked, the associated rack accounts are moved to **Default Group**.

Step 5 Click **Delete**.

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

Managing Rack Accounts

Adding a Rack Account

Refer Adding a Rack Account, on page 9 to create rack accounts.

Note You can create a rack account again immediately without having to wait for the previous command of creating a rack account to complete.

Editing a Rack Account

Perform this procedure when you want to edit a rack account.

Before You Begin

The rack account has already been created under Rack Accounts.

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.

Step 2 Click the **Rack Accounts** tab.

Step 3 From the list of accounts, select the account you want to edit.

Step 4 Click **Modify**.

Note You cannot see the **Modify** button till you select the rack account from the list.

Step 5 In the **Modify Account** dialog box, complete the following fields:

Field	Description
Description field	(Optional) A description of the Rack Account.
Use Credential Policy checkbox	(Optional) If you have already created credential policies, then check this box to select the policy from the drop-down list.
If you check **Use Credential Policy** checkbox	
Credential Policy drop-down list	Choose a policy from the drop-down list.
If you uncheck **Use Credential Policy** checkbox	
User Name field	Login ID for the rack mount server.
Password field	Password for the login ID for the rack mount server.
Protocol drop-down list	Choose https or http from the list.
Port field	The port number associated with the selected protocol.
Rack Group drop-down list	Choose a rack group from the list.
Contact field	(Optional) The contact email address for the account.
Location field	(Optional) The location of the account.

Step 6 Click **Modify**.

Step 7 Click **OK**.

Testing Account Connection

Perform this procedure when you want to test a rack account connection. We recommend you to perform this procedure for every new account added in Cisco IMC Supervisor.

Before You Begin

The rack account has already been created under Rack Accounts.

Procedure

Step 1 From the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Click the **Rack Accounts** tab.

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

Step 4 Click **Test Connection**.

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

Step 5 In the **Test Connection** dialog box, click **Submit**.
Testing the connection may take several minutes.

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

Deleting a Rack Account

Perform this procedure when you want to delete a rack account.

Before You Begin

The rack account has already been created under Rack Accounts.

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.

Step 2 Click the **Rack Accounts** tab.

Step 3 From the list of rack accounts, select the account you want to delete.

Step 4 Click **Delete**.

Step 5 In the **Delete Rack Server Accounts** dialog box, click **Select** and check the check boxes of the rack accounts you want to delete.

Step 6 Click **Select**.

Step 7 Click **Submit**.

Step 8 In the confirmation dialog box, click **OK**.

Collecting Inventory for Multiple Rack Accounts or Rack Groups

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

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.

Step 2 Click the **Rack Accounts** tab.

Step 3 A list of rack accounts is displayed.

Step 4 Click **Inventory**.

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

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

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

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

Step 8 Click **Submit**.

Step 9 In the confirmation dialog box, click **OK**.

Assigning Rack Accounts to a Rack Group

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

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.

Step 2 Click the **Rack Accounts** tab.

Step 3 A list of servers is displayed.

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

Step 5 In the **Assign Rack Groups** dialog box, select the rack group you want to assign the servers to.

Step 6 Click **Submit**.

Step 7 In the confirmation dialog box, click **OK**.

Managing Server Discovery

Discovering and Importing a Server

Perform this procedure when you want to auto discover and import a server.

Procedure

	Command or Action	Purpose
Step 1	Configure a discovery profile.	Refer Configuring Auto Discovery Profile, on page 29.
Step 2	Discover a server.	Refer Performing Auto Discovery, on page 30.
Step 3	Import a Server.	Refer Importing a Server, on page 31.
Step 4	Delete a discovery profile.	(Optional) Refer Deleting Auto Discovery Profile, on page 32.
Step 5	Clear a server from the auto discovered list.	(Optional) Refer Clearing Auto Discovery List, on page 32.

Configuring Auto Discovery Profile

You should configure the 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 a auto discovery profile.

Procedure

Step 1 From the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Click the **Discovered Devices** tab.

Step 3 Click **Configure**.

Step 4 In the **Discovery Configuration Criteria** dialog box you can either create a new profile or edit an existing profile.
To create a new profile, complete the following:

Field	Description
Select Profile drop-down list	Select **<New>** from the drop-down list.
Profile Name Field	A descriptive name for the profile.
Search Criteria drop-down list	Select **IP Address Range**, **Subnet Mask Range**, **IP Address CSV File**, or **IP Address List** from the drop-down list.

Field	Description
If you select **IP Address Range**	
Starting IP Field	Valid IP address
Ending IP Field	Valid IP address
If you select **Subnet Mask Range**	
Network Address Field	Valid IP address
Subnet Mask drop-down list	Select a value from the drop-down list.
If you select **IP Address CSV File**	
Select a file for upload field	Click **Browse** and navigate to a .csv file which contains the IP addresses.
If you select **IP Address List**	
IP Addresses field	Enter multiple IP addresses separated by comma.
Use Credential Policy checkbox	If you have already created credential policies, then check this box to select the policy from the drop-down list.
If you check **Use Credential Policy** checkbox	
Credential Policy drop-down list	Choose a policy from the drop-down list or click the + icon and create new policy. Refer Creating a Credential Policy, on page 38 to create a new policy.
If you uncheck **Use Credential Policy** checkbox	
User Name field	The server login name.
Password field	The server login password
Protocol drop-down list	Choose https or http from the list.
Port field	Enter a port number.

Step 5 Click **Submit**.

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

Performing Auto Discovery

Perform this procedure when you want to perform auto discovery.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Administration** > **Physical Accounts**.
Step 2 Click the **Discovered Devices** tab.
Step 3 Click **Discover**.
Step 4 In the **Discover Devices** dialog box, select a profile from the **Select Profile** drop-down list.
Step 5 Click **Submit**.
Step 6 In the confirmation dialog box, click **OK**.

Importing a Server

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

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Physical Accounts**.
Step 2 Click the **Discovered Devices** tab.
Step 3 Click **Import**.
Step 4 In the **Import Discovered Devices** dialog box, complete the following: click **Select** button.

Field	Description
Select Device(s) field	Click **Select** to choose the devices to import. Check the check boxes of all the servers you want to import. **Note** For a server, if the **Account Exists** column is marked with **Yes**, then it implies that this account is currently being managed by Cisco IMC Supervisor. You must select accounts that are marked with **No** to proceed without any errors.
Select Rack Group drop-down list	Choose the rack group.

Step 5 Click **Submit**.

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

Note You can import discovered devices again without having to wait for the previous import to complete.

Deleting Auto Discovery Profile

Perform this procedure when you want to delete a auto discovery profile.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Click the **Discovered Devices** tab.

Step 3 Click **Delete Profile**.

Step 4 In the **Delete Profile** dialog box, select a profile from the **Select Profile** drop-down list.

Step 5 Click **Submit**.

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

Clearing Auto Discovery List

Perform this procedure when you want to delete a server or all the servers from the auto discovered list.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Click the **Discovered Devices** tab.

Step 3 Click **Clear**.

Step 4 In the **Clear Devices** dialog box, click **Select** button.

Step 5 In the **Select** dialog box, check the check box of the server you want to delete.

Note To select all the servers, check the topmost check box.

Step 6 Click **Select**.

Step 7 In the **Clear Devices** dialog box, click **Submit**.

Step 8 In the confirmation dialog box, click **OK**.

Firmware Management Menu

Firmware Management menu displays the following tabs:

Tab	Description
Images - Local	This tab displays the firmware image details that you downloaded to the appliance from cisco.com. The firmware image details are listed against the configured profile associated with the image. You can also use this tab to refresh the report data, add report as a favorite, view profile configuration details, add, modify and delete a firmware image.
Images - Network	This tab displays the firmware image details that reside in a network share such as the Network File System (NFS), Common Internet File System (CIFS), or HTTP(s) system. A rack server CIMC picks up these images during upgrade. You can now manage these network locations that contain images using Cisco IMC Supervisor. You can also use this tab to refresh the report data, add report as a favorite, view profile configuration details, add, modify and delete a firmware image.
Firmware Upgrades	This tab allows you to create firmware upgrade profiles and upgrade the devices.

Managing Firmware

Adding Images to a Local Server

Procedure

Step 1 From the menu bar, choose **Systems** > **Firmware Management**.

Step 2 Click **Images - Local** tab and click + to add an image.

Step 3 In the **Add Firmware Image - Local** dialog box, complete the following:

Field	Description
Profile Name field	Enter a descriptive and unique profile name.
User Name (cisco.com) field	Enter your Cisco login user name.

Field	Description
Password (cisco.com) field	Enter your Cisco login password.
Enable Proxy Configuration check box	(Optional) Check this checkbox to enable proxy configuration and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.
Enable Proxy Authentication check box	(Optional) Check this checkbox to enable proxy authentication and complete the following: • **Proxy User Name** field - Enter a proxy user name for the proxy authentication. • **Proxy Password** field - Enter the password for the proxy user name.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server is listed here.
Available Image drop-down list	Choose the .iso image from the drop-down list.
Download Now check box	Check this check box to download the .iso image immediately after adding a profile. If not, you can click on **Download Image** to download the image later.
Accept License Agreement	Check this check box to accept the license agreement. Click on the Terms and Conditions link to read the End User License Agreement. **Note** You cannot create a firmware profile without accepting the license agreement even if you want to download the image later.

Step 4 Click **Submit**.

Step 5 In the **Submit Result** dialog box, click **OK**.

Note
- You can click **View Location Details** to view profile configuration details, click **Modify** to modify the firmware image details, and click **Delete Profile** to delete the image profile. You can select multiple profiles concurrently and delete them.
- The profile name must be unique across both Local and Network image profiles.
- For downloading the E-Series firmware images you must associate a contract access to the cisco.com account.

Adding Images from a Network Server

Procedure

Step 1 From the menu bar, choose **Systems** > **Firmware Management**.

Step 2 Click **Images - Network** tab and click + to add an image.

Step 3 In the **Add Firmware Image - Network** dialog box, complete the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server is listed here.
Server Type drop-down list	Choose either Network File System (NFS), Common Internet File System (CIFS) or HTTP/S server types.
Remote IP field (only for NFS and CIFS server types)	Enter remote IP address.
Remote Share field (only for NFS and CIFS server types)	Enter remote share path.
Remote File Name field (only for NFS and CIFS server types)	Enter a remote filename. **Note** The remote filename is the Unified Computing System (UCS) Server Configuration Utility ISO file.
Location Link field (only for HTTP server type)	Enter a valid http/https URL link for the image location.
User Name field	Enter a network path user name.
Password field	Enter a network path password.
Mount Options drop-down list (only for CIFS server type)	Select valid mount options from the **Mount Options** drop-down list. **Note** **Mount Options** drop-down list is applicable only for servers running Cisco IMC 2.0(8) and later.

Step 4 Click **Submit**.

Step 5 In the **Submit Result** dialog box, click **OK**.

Note
- You can click **View Location Details** to view profile configuration details, click **Modify** to modify the firmware image details, and click **Delete Profile** to delete the image profile. You can select multiple profiles concurrently and delete them.
- The profile name must be unique across both Local and Network image profiles.

Upgrading Firmware

Perform this procedure when you want to upgrade firmware.

Before You Begin

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

Procedure

Step 1 From the menu bar, choose **Systems** > **Firmware Management**.

Step 2 Click the **Firmware Upgrades** tab.

Step 3 Click **Run Upgrade**.
A warning message that running upgrade on the selected servers will cause the host to reboot into the firmware update tool and on completing the firmware update, the servers will reboot back to the host OS is displayed.

Step 4 Click **OK** to confirm.

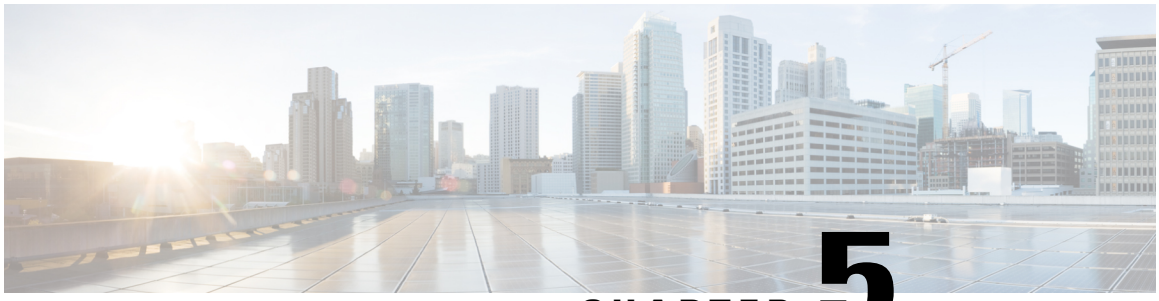
Step 5 In the **Upgrade Firmware** dialog box complete the following:

Field	Description
Select Profile drop-down list	Choose a profile from the drop-down list.
Select Server	Choose the servers from the list and click **Select**. The list displays only those servers whose platform matches the one configured in the selected profile.

Step 6 In the **Upgrade Firmware** dialog box, click **Submit**.

Step 7 Click **OK**.

Note You can click **View Upgrade Details** to view firmware upgrade details and click **Delete Upgrade Status** to delete the status records for the specified upgrade operation.



CHAPTER 5

Policies Menu

This chapter contains the following topics:

Policies Menu Options

The **Policies** menu contains the following menu options:

- Manage Policies and Profiles
- Tag Library

Managing Policies

The **Manage Policies and Profiles** menu displays the following tabs:

Tab	Description
Credential Policies	You can create a credential policy specifying a user name, password, protocol, and port. You can reuse the credentials specified in this policy for example, while creating a rack account. You can perform various tasks such as adding, editing, and deleting credential policies from this page. For information on performing these tasks, see Creating a Credential Policy.

Tab	Description
Manage Hardware Policies	A policy helps in categorically grouping and classifying the various characteristics of a server. You can create hardware policies by configuring various properties such as BIOS, LDAP, Users and so on. These policies can then be applied to a server or server groups. You can perform various tasks such as adding, editing, and deleting hardware policies from this page. For information on performing these tasks, see Hardware Policies.
Manage Hardware Profiles	A combination of existing set of policies make up a profile. You can apply configuration details of a rack hardware profile for example, to multiple servers. You can associate this hardware profile to specific servers. You can perform various tasks such as adding, editing, and deleting hardware profiles from this page. For information on performing these tasks, see Creating a Hardware Profile.

Tag Library

Tagging is when you assign a label to an object. As an administrator, you can decide to tag objects such as resource groups and user groups in Cisco IMC Supervisor. You can assign tags to a category such as a rack account. You can also apply a tag to a specific type of account in the selected category.

Tag Library has only one tab which displays the following details:

Field	Description
Name	User defined name of the tag library.
Description	User defined brief description of the tag library.
Type	String or an integer.
Possible Tag Values	User defined tag values.
Applies To	Rack mount servers or users.

Credential Policies

Creating a Credential Policy

Perform this procedure when you want to create a credential policy.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 Click **Add**.

Step 3 In the **Add Credential Policy** dialog box, complete the following fields:

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

Step 4 Click **Submit**.

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

Note You can also perform the following policy tasks:

- Click **Edit** and modify a selected credential policy you created.
- Click **Clone** to copy the details of a selected credential policy to a new policy.
- Click **Delete** to delete a selected policy.
- Click **View** to view the credential policy details of a selected policy.
- Click **Apply** to apply a policy on a server or server group.
- Click **View Server Mappings** to see the list of the servers that the policy is associated to.

Editing a Credential Policy

Perform this procedure when you want to edit a credential policy.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to edit.

Step 3 Click **Edit**.

Note You cannot see the **Edit** button till you select the policy from the list.

Step 4 In the **Modify Credential Policy** dialog box, edit the following fields:

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

Note You cannot change the name of the policy.

Step 5 Click **Submit**.

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

Cloning a Credential Policy

Perform this procedure when you want to create a new credential policy based on another policy.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to clone.

Step 3 Click **Clone**.

Note You cannot see the **Clone** button till you select the policy from the list.

Step 4 In the **Clone Credential Policy** dialog box, complete the following fields:

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

Step 5 Click **Submit**.

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

Deleting a Credential Policy

Perform this procedure when you want to delete a credential policy.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to delete.

Step 3 Click **Delete**.

Note You cannot see the **Delete** button till you select the policy from the list.

Step 4 In the **Delete Credential Policy** dialog box, click **Delete**.

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

Viewing a Credential Policy Details

Perform this procedure when you want to view a credential policy details.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to view.

Step 3 Click **View**.

Note You cannot see the **View** button till you select the policy from the list.

Step 4 You can view the details in the **Credential Policy Details** dialog box.

Step 5 Click **Close** to go back to the previous screen.

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.

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 43.
   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 57.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Policy, on page 57.
3. Perform any of the following optional tasks on the policy:
   a. Edit
   b. Delete
   c. Clone

   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 58.

   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 61.

Creating Hardware Policies

Perform this procedure when you want to create a new hardware policy.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

Step 2 Choose **Manage Hardware Policies** tab.

Step 3 Click **Add**.

Step 4 In the **Add Policy** dialog box, 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.

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
BIOS Policy, on page 44	*Configuring BIOS Settings*
Disk Group Policy, on page 45	*Managing Storage Adapters*
IPMI Over LAN Policy, on page 45	*Configuring IPMI*
LDAP Policy, on page 46	*Configuring the LDAP Server*
Legacy Boot Order Policy, on page 47	*Server Boot Order*
Network Security Policy, on page 48	*Network Security Configuration*
NTP Policy, on page 49	*Configuring Network Time Protocol Settings*
Precision Boot Order Policy, on page 49	*Configuring the Precision Boot Order*
RAID Policy, on page 50	*Managing Storage Adapters*
Serial Over LAN Policy, on page 51	*Configuring Serial Over LAN*
SNMP Policy, on page 52	*Configuring SNMP*
SSH Policy, on page 53	*Configuring SSH*
User Policy, on page 53	*Configuring Local Users*
VIC Adapter Policy, on page 55	*Viewing VIC Adapter Properties*
Virtual KVM Policy, on page 55	*Configuring the Virtual KVM*

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
vMedia Policy, on page 56	*Configuring Virtual Media*

What to Do Next

Apply the policy to a server. For more information about applying a policy, see Applying a Policy, on page 57.

BIOS Policy

A BIOS policy automates the configuration of BIOS settings on servers. You can create one or more BIOS policies which contain a specific grouping of BIOS settings that match 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 remain as they are, either a default set of values for a brand new bare metal server or a set of values which were configured using Cisco IMC. If a BIOS policy is specified, the values specified in the policy replace any previously configured values on the server.

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

Perform the following procedure to create a BIOS policy.

Procedure

Step 1 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **BIOS 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Note If some properties or attributes in Cisco IMC Supervisor are not applicable to a server running a specific Cisco IMC version, they are not applied. If the properties are not available on the Cisco IMC server, they are displayed as **Platform-Default** in the property fields.

Step 4 In the **Main** dialog box, select values for the main BIOS properties such as **Boot Option Retry**, **Post Error Pause**, and **TPM Support** drop-down lists.

Step 5 In the **Advanced** dialog box, choose the BIOS property values from the drop-down lists and click **Next**.

Step 6 In the **Server Management** dialog box, choose the server property values from the drop-down lists and click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.

Disk Group Policy

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

A disk group policy defines how a disk group is created and configured. The policy specifies the RAID level to be used for the virtual drive. You can use a disk group policy to manage multiple disk groups. A single Disk Group policy can be associated with multiple virtual drives. If so, the virtual drives share the same Virtual Drive group space. Disk Group policies associated with different virtual drives in a RAID policy do not have any physical disk repeated across different Disk Group policies. For more information about RAID policy, see RAID Policy, on page 50.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, 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 In the **Virtual Drive Configuration** dialog box, choose the virtual drive properties and click **Next**.

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

Step 6 In the **Submit Result** dialog box, click **OK**.

Step 7 Click **Submit** in the **Main** dialog box.

Step 8 In the **Submit Result** dialog box, click **OK**.

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.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, complete the following fields.

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

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

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

LDAP Policy

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

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

Perform the following procedure to create a LDAP policy.

Procedure

Step 1 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **LDAP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, fill in the LDAP properties.

Step 5 Click **Next**.

Step 6 In the **LDAP Servers** dialog box, fill in the LDAP server details.

Step 7 Click **Next**.

Step 8 In the **Group Authorization** dialog box, fill in the group authorization details and click + to add an LDAP group entry to the table.

Step 9 In the **Add Entry to LDAP Groups** dialog box, fill in the group details.

Step 10 Click **Submit**.

Step 11 In the **Submit Result** dialog box, click **OK**.

Step 12 Click **Submit** in the **Group Authorization** dialog box.

Step 13 In the **Submit Result** dialog box, click **OK**.

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. removed and replaced with whatever role groups are configured in the policy. If you have not added any role groups into the policy, then the existing role groups on the server are removed, but not replaced.
- **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. For more information about precision boot order, see Precision Boot Order Policy, on page 49.

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.

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

Procedure

Step 1 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, 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** dialog box.

Step 6 In the **Submit Result** dialog box, click **OK**.

Step 7 Click **Submit** in the **Main** dialog box.

Step 8 In the **Submit Result** dialog box, click **OK**.

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 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.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **Network Security** 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, check **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **NTP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, check **Enable NTP** check box to enable alternate servers and specify up to 4 NTP servers.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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

Precision Boot Order Policy

Configuring the precision boot order allows linear ordering of the devices. In Cisco IMC Supervisor you can change the boot order and boot mode, add multiple devices under each device types, 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

Step 1 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **Precision 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, check UEFI Secure Boot check box or select the boot mode from the **Configure Boot Mode** drop-down list.

Step 5 Click + and select or enter device details. The table lists the devices you have added.
You can also select an existing device in the **Select Devices** table and click **x** to delete or click edit icon to edit a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

Step 6 Click **Submit** in the **Add Entry to Select Devices** dialog box.

Step 7 In the **Submit Result** dialog box, click **OK**.

Step 8 Click **Submit** in the **Main** dialog box.

Step 9 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **RAID 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, click + to add virtual drives that you want to configure on the server to the **Virtual Drives** list.

Step 5 In the **Add Entry to Virtual Drives** dialog box, enter or select the virtual drive details.
You can either select an existing Disk Group policy from the drop-down list and edit or add a new Disk Group policy to specify local disks. To create a Disk Group policy, refer Disk Group Policy, on page 45.

Note If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.

Step 6 Click **Submit** in the **Add Entry** dialog box.

Step 7 In the **Submit Result** dialog box, click **OK**.

Step 8 Check the **Erase 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 results in loss of existing data.

Step 9 Check the **Configure remaining disks as JBOD** check box to configure the remaining disks as JBOD.
This option is applicable only on storage controllers that support JBOD. The disks that are not used for virtual drives or hotspares are configured as JBOD.

Step 10 Click **Submit** in the **Main** dialog box.

Step 11 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **Serial 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, 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 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **SNMP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **SNMP Users** dialog box, 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 5 Click **Next**.

Step 6 In the **SNMP Traps** dialog box, 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 7 Click **Next**.

Step 8 In the **SNMP Settings** dialog box, configure the SNMP properties.

Step 9 Click **Submit**.

Step 10 In the **Submit Result** dialog box, click **OK**.

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

SSH Policy

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

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

Perform the following procedure to create an SSH policy.

Procedure

Step 1 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **SSH 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, check **Enable SSH** check box, and enter SSH properties or use the existing properties.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **User 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, you can add users that need to be configured on the server to the **Users** list.

Step 5 Click + to add a user.

Step 6 In the **Add Entry to Users** dialog box, complete the following fields:

Option	Description
Username	Enter a name for the user in the field.
Role	Choose a role for the user such as read-only, admin and so on from the drop-down list.
Enabled	Check this check box to activate the user.
NewPassword	Enter a password associated with the username.
Confirm New Password	Repeat the password from the previous field.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.
You can also select an existing user from the **Users** table in the **Main** dialog box 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.
- When you apply a user policy, the user entries in Cisco IMC Supervisor are replaced with the user entries you created. Blank entries in Cisco IMC are replaced with default users from Cisco IMC Supervisor. The default user role is always read-only and the user is disabled.
- Ensure that the account used to manage the Cisco IMC Supervisor is not deleted from the user list in the policy. If deleted, the Cisco IMC Supervisor will lose 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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **Virtual KVM 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 Check the **Enable vKVM** check box.

Step 5 Choose or enter the virtual server properties or use the existing properties.

Step 6 Click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.

VIC Adapter Policy

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

Perform the following procedure to create a VIC Adapter policy.

Procedure

Step 1 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **VIC Adapter 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, click + to add a VIC adapter entry in the table.

Step 5 In the **Add Entry to VIC Adapters** dialog box and enter 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 6 Click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.

Step 8 Click **Submit** in the **Main** dialog box.

Step 9 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

Step 2 In the **Add** dialog box, choose **vMedia 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 57.

Step 4 In the **Main** dialog box, check the **Enable vMedia** check box to enable vMedia and check the **Enable Virtual Media Encryption** for enabling vMedia encryption.

Step 5 Click **Next**.

Step 6 Check the **Add CDD vMedia Mapping** check box and complete the CDD mapping details.

Step 7 Click **Next**.

Step 8 Check the Add **HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 9 Click **Submit**.

Step 10 In the **Submit Result** dialog box, click **OK**.

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.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 43.

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:

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.

b) Click **Select** and choose a server from where you can retrieve the configurations.

Step 4 Click **Next**.
You will go to the **Main** dialog box. Continue creating a policy.

Applying a Policy

Perform this procedure when you want to apply an existing policy to a server.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies**.

Step 2 Choose the **Manage Hardware Policies** tab.

Step 3 Select a policy you want to apply from the left pane.

Step 4 Click **Apply** from the options available at the top.

Step 5 In the **Apply Policy** dialog box, choose the server or server group from the drop-down list based on whether you want to apply the policy to individual servers or an entire rack server group.

Step 6 Click **Select** to select the server groups or servers to which you want to apply the policy.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.
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 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

Step 2 Choose the **Manage Hardware Policies** tab.

Step 3 Expand a policy from the left pane and select a policy in the **Manage 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 only if you have not associated the policy with a server. If you have associated a policy to a server, re-associate the server with a different policy or the same policy after modifying it.

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 Policy, on page 57.

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 policy 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 59.
   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 60.
2. Apply the profile on a server. For more information about applying a profile, see Applying a Hardware Profile, on page 61.
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 61.

Creating a Hardware Profile

Perform this procedure when you want to create a hardware profile.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

Step 2 Choose the **Manage Hardware Profiles** tab.

Step 3 Click **Add**.

Step 4 In the **Create Hardware Profile** dialog box, enter a name for the profile you want to create in the **Profile Name** field.

Step 5 Click **Next** or check **Create profile from current configuration of the server** check box and click **Next**.
To perform the tasks in the Server Details window, see Creating a Profile from an Existing Configuration.

Step 6 In the **Profile Entities** dialog box, click + to add a profile entry.
You can also click the edit and delete icons to edit and delete the existing entries.

Step 7 In the **Add Entry to Profile Name** dialog box, choose the **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 have selected earlier. For more information about creating policies, see Creating Hardware Policies, on page 43

Step 9 Click **Submit**.

Step 10 In the **Submit Result** confirmation dialog box, click **OK**.

Step 11 Click **Submit** in the **Profile Entities** dialog box.

Step 12 In the **Submit Result** confirmation dialog box, click **OK**.

What to Do Next

You can also edit, delete, clone a profile and also view the server mapped to a selected profile. For performing these tasks, see General Tasks Under Hardware Profiles, on page 61

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 current configuration of a server.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

Step 2 Choose the **Manage Hardware Profiles** tab.

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:

a) Check the **Enter Server Details Manually** check box and fill in the following fields:

1. Enter the IP address in the **Server IP** field.
2. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy in the **Credential Policy Add Form** dialog box.
3. Enter the server login name in the **User Name** field.
4. Enter the server login password in the **Password** field.
5. Select http or https from the **Protocol** drop-down list.

6 Enter the port number associated with the selected protocol in the **Port** field.

7 Click **Select**, select the policies, and click **Select**.

b) Click **Select** and choose a server from where you can retrieve the configurations.
c) Click **Select**, choose the policies, and click **Select**.

Step 6 Click **Next**.

Step 7 In the **Profile Entities** dialog box, click **+** to add an entry to the profile name.
Click **x** to delete an existing entry from the **Profile Name** table.

Step 8 Click **Submit**.

Step 9 In the **Submit Result** dialog box, click **OK**.

Applying a Hardware Profile

Perform this procedure when you want to apply a hardware profile to a rack server.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

Step 2 Choose the **Manage Hardware Profiles** tab.

Step 3 Select an existing hardware profile and click **Apply** from the options listed above.

Step 4 In the **Apply Profile** dialog box, choose the server or server group from the drop-down list, based on whether you want to apply the profile to individual servers or an entire rack server group.

Step 5 Click **Select** to select the server groups or servers to which you want to apply the profile.

Step 6 Click **Submit**.

Step 7 In the **Submit Result** confirmation dialog box, click **OK**.
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 server(s) 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 From the menu bar, choose **Policies** > **Manage Policies and Profiles** > **Manage Hardware Profiles**.

Step 2 Expand the Hardware Profile in the left pane and select a profile in the **Manage Hardware Profiles** page.
Perform the following optional tasks:

a) (Optional) To delete a profile, click **Delete**. Click **Select** in the **Delete Profile** dialog box, select one or more profiles and click **Select**. Click **Submit** to delete a profile.
You cannot delete a profile which is associated to a server. You must associate a different profile to the server before deleting it.

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**. For more information about applying a profile, see Applying a Hardware Profile, on page 61.

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 3 Click **Submit** and/or **Close** if applicable.

Tagging Task Under Tag Library

Creating a Tag Library

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

Before You Begin

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 Click **Create**.

Step 3 In the **Create Tag** dialog box, complete the following fields for **Tag Details**:

Field	Description
Name field	A descriptive name for the tag.
Description field	(Optional) A description of the tag.
Type drop-down list	Select String or Integer.
Possible Tag Values field	The possible values for the tag.

Step 4 Click **Next**.

Step 5 In the **Applicability Rules** screen, complete the following:

Name	Description
Taggable Entities field	Choose the entities on which the tag needs to be applied. To add an entity, do the following: 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**. **Note** The tags are displayed under the respective category according to the set taggable entities.

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

Step 7 In the **Create Tag** dialog box, click **Submit**.

Step 8 Click **OK**.

Cloning a Tag Library

Perform this procedure when you want to create a new tag library based on another tag library.

Before You Begin

The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to clone.

Step 3 Click **Clone**.

Note You cannot see the **Clone** button till you select the tag library from the list.

Step 4 In the **Clone Tag** dialog box, complete the following fields for **Tag Details**:

Field	Description
Name field	A descriptive name for the tag.

Field	Description
Description field	(Optional) A description of the tag.
Type drop-down list	Select String or Integer.
Possible Tag Values field	The possible values for the tag.

Step 5 Click **Next**.

Step 6 In the **Applicability Rules** screen, complete the following:

Name	Description
Taggable Entities field	Choose the entities on which the tag needs to be applied. To add an entity, do the following: **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**. **Note** The tags are displayed under the respective category according to the set taggable entities.

Step 7 In the confirmation dialog box, click **OK**.

Step 8 Click **Submit**.

Step 9 Click **OK**.

Editing a Tag Library

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

Before You Begin

The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to edit.

Step 3 Click **Edit**.
You cannot see the **Edit** button till you select the tag library from the list.

Step 4 In the **Edit Tag** dialog box, complete the following fields for **Tag Details**:

Field	Description
Name field	A descriptive name for the tag.
Description field	(Optional) A description of the tag.
Type drop-down list	Select String or Integer.
Possible Tag Values field	The possible values for the tag.

Step 5 Click **Next**.

Step 6 In the **Applicability Rules** screen, complete the following:

Name	Description
Taggable Entities field	Choose the entities on which the tag needs to be applied. To add an entity, do the following: **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**. **Note** The tags are displayed under the respective category according to the set taggable entities.

Step 7 In the confirmation dialog box, click **OK**.

Step 8 Click **Submit**.

Step 9 Click **OK**.

Deleting a Tag Library

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

Before You Begin

The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to delete.

Step 3 Click **Delete**.

Note You cannot see the **Delete** button till you select the tag library from the list.

Step 4 In the **Tag** dialog box, click **Delete**.

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

Viewing a Tag Details

Perform this procedure when you want to view a tag library details.

Before You Begin

- The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to view.

Step 3 Click **View**.

Note You cannot see the **View** button till you select the tag library from the list.

Step 4 You can view the details in the **Tag Details** dialog box.

Step 5 Click **Close** to go back to previous screen.

Viewing a Tag Association Details

Perform this procedure when you want to view a tag library association details.

Before You Begin

The tag library has already been created under **Tag Library** and has been associated with an entity.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to view.

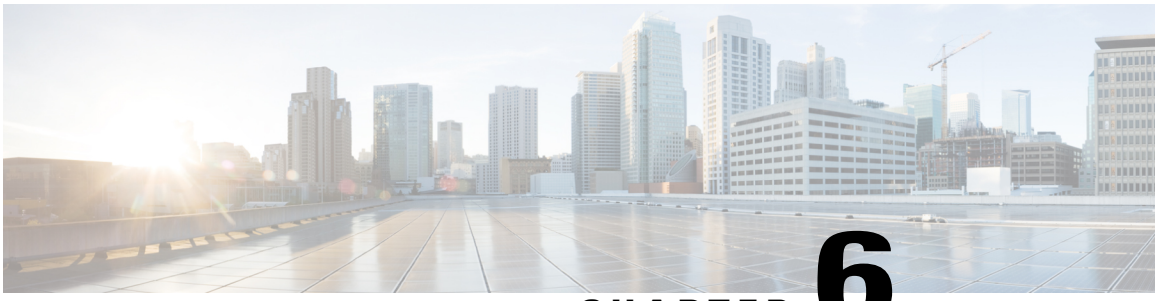
Step 3 Double-click the tag library from the list or click the tag library from the list and click **View Details**.

Note You cannot see the **View Details** button till you select the tag library from the list.

You can view the following details in the **Tag Association** page:

Field	Description
Tag Name	The descriptive name for the tag.
Associated Resource Entity	The value of the entity.
Resource Entity Type	The resource type of the entity.
Tag Value	The value of the tag.

Step 4 Click **Close** to go back to previous screen.



CHAPTER 6

Cisco IMC Supervisor Administration

This chapter contains the following topics:

License Menu

The **License** menu displays the following tabs:

Tab	Description
License Keys	This tab displays the details of the license used in Cisco IMC Supervisor. You can also use this tab to update and upgrade the license.
License Utilization	This tab shows the licenses in use and details about each license, including license limit, available quantity, status, and remarks. License audits can also be run from this page.
Resource Usage Data	This tabs displays the details of the various resources used.

System Menu

The **System** menu displays the following tabs:

Tab	Description
System Information	Basic system information includes the system details such as name, IP address, uptime and so on. It also includes service status, database node information, memory capacity and usage, disk information and so on.
Mail Setup	You can use this tab to set up SMTP configuration.
System Tasks	This tabs displays all the system tasks. You can use this tab to manage any system task.
User Roles	This tabs displays all Cisco IMC Supervisor users and their roles . You can use this tab to manage any user. **Note** This is not a login user. Here the user is defined as an admin with all privileges or a end user with defined privileges. Login users can then be configured under any of these user roles.
Email Alert Rules	Use this tab to set rules for email alerts from the system. You can set email alerts for faults of any severity.

Users Menu

The **Users** menu displays the following tabs:

Tab	Description
Login Users	This tab displays all the user who can log in Cisco IMC Supervisor. You can also use this tab to create new users.
Currently Online Users	This tab displays all the users who are currently logged in Cisco IMC Supervisor.
Login Page Branding	This tab displays the customized login page for Cisco IMC Supervisor. You can also use this tab to create new login page with a domain and logo.
Authentication Preferences	You can use this tab to configure the authentication preference as Local Authentication, Local first, LDAP first, or VeriSign Identity Protection.
LDAP Integration	You can use this tab to view and configure LDAP settings.

Tab	Description
Password Policy	You can use this tab to change the password policy for users.

Integration Menu

Integration menu displays the following tabs:

Tab	Description
CMDB Integration Setup	You can use this tab to configure the FTP settings.
Change Records	This tab displays the time stamp for the changes made in Cisco IMC Supervisor.

User Interface Settings

User Interface Settings menu displays the following Fields:

Fields	Description
Product Name field	You can configure this field to change the title text at the far left corner of the header bar.
Product Name 2nd Line field	You can configure this field to change the text below the title at the far left corner of the header bar.
Enable About Dialog checkbox	You can configure this option to enable or disable **About** on the header bar.
Administrator Portal	
Custom Link 1 Lable field	You can configure this field to change the text on header bar.
Custom Link 1 URL field	You can configure the URL for the **Custom Link 1 Lable**
Custom Link 2 Lable field	You can configure this field to change the text on header bar.
Custom Link 2 URL field	You can configure the URL for the **Custom Link 2 Lable**
End-user Portal	
Custom Link 1 Lable field	You can configure this field to change the text on header bar.
Custom Link 1 URL field	You can configure the URL for the **Custom Link 1 Lable**
Custom Link 2 Lable field	You can configure this field to change the text on header bar.

Fields	Description
Custom Link 2 URL field	You can configure the URL for the **Custom Link 2 Lable**

Support Information

You can use the Support Information menu to configure the type of support information displayed in Cisco IMC Supervisor.

Managing Licensing Information

Applying Upgrade License

You want to upgrade Cisco IMC Supervisor license.

Procedure

Step 1 From the menu bar, choose **Administration** > **License**.

Step 2 Click the **License Keys** tab.

Step 3 Click **Update License**.

Step 4 In the **Update License** dialog box, complete the following:

Field	Description
Select File to Upload field	Click **Browse** to locate and select a license file. After selecting the file, click **Upload**.
Enter License Text check box	Check this check box to copy and paste the license text.

Step 5 Click **Submit**.

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

Running License Audit

Perform this procedure when you want to audit the license.

Before You Begin

The license should be updated. To update the license, refer Updating the License, on page 7.

Procedure

Step 1 From the menu bar, choose **Administration** > **License**.
Step 2 Click the **License Utilization** tab.
Step 3 Click **Run License Audit**.
Step 4 In the **Run License Audit** dialog box, click **Submit**.
Auditing starts and may take some time to complete.
Step 5 In the confirmation dialog box, click **OK**.

Managing System Information

Configuring Mail Setup

All outgoing emails from Cisco IMC Supervisor require an SMTP server.

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.
Step 2 Click the **Mail Setup** tab.
Step 3 In the **Mail Setup** pane, complete the following fields:

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

Step 4 Click **Save**.

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

Managing System Tasks

Perform this procedure when you want to manage system task.

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

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.

Step 2 Click the **System Tasks** tab.

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

Step 4 In the **Manage Task** dialog box, complete the following:

Field	Description
Task Execution drop-down list	(Optional) Choose enable or disable from the drop-down list.
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 from the drop-down list.
Minutes drop-down list	Choose a number to indicate the frequency from the drop-down list. **Note** This drop-down list appears only for specific system tasks.

Step 5 Click **Submit**.

Step 6 Click **OK**.

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 From the menu bar, choose **Administration** > **System**.
Step 2 Click the **System Tasks** tab.
Step 3 Choose a system task from the table.
Step 4 Click **Run Now**.
Step 5 Click **Submit**.
Step 6 Click **OK**.

Adding Email Alert Rules

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.

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.
Step 2 Click the **Email Alert Rules** tab.
Step 3 Click **Add**.
Step 4 In the **Add Email Alert Rule** dialog box, complete the following:

Field	Description
Name	Enter a unique name for the rule.
Alert Scope	Choose **System** for receiving all system level alerts for new faults discovered on any server. Choose **ServerGroup** for receiving email alerts for new faults discovered on a server which is part of the specified Rack Group.

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.
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 **Modify** and **Delete** options are visible only when you select a rule. Click **Modify** 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.

Managing User Roles

Adding a User Role

By default, an operator role and an administrator role is available in Cisco IMC Supervisor. Perform this procedure when you want to add a new user role.

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.

Step 2 Click the **User Roles** tab.

Step 3 Click **Add**.

Step 4 In the **Add User Role** dialog box, complete the following for **User Role** pane:

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

Step 5 Click **Next**.

Step 6 In the**Menu Settings** pane, choose the required menu options. To choose the menu option, check the checkbox against the menu setting field.

Step 7 Click **Next**.

Step 8 In the**User Permissions** pane, choose the required operations. To choose the operation, check the checkbox against the operation.

Step 9 Click **Submit**.

Step 10 In the confirmation dialog box, click **OK**.

Editing a User Role

Perform this procedure to edit an existing user role.

Before You Begin

You should have an existing user role.

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.

Step 2 Click the **User Roles** tab.

Step 3 From the list of user roles, select the user role you want to edit.

Step 4 Click **Edit**.

Note You cannot see the **Edit** button till you select the user role from the list.

Step 5 Click **Next**.

Note You cannot edit the **User Role**, **Role Type** or the **Description**.

Step 6 Click **Next**.

Step 7 In the**Menu Settings** pane, check or uncheck the checkbox against the menu setting field as per requirement.

Step 8 Click **Next**.

Step 9 In the**User Permissions** pane, check or uncheck the checkbox against the operation field as per requirement.

Step 10 Click **Submit**.

Step 11 In the confirmation dialog box, click **OK**.

Cloning a User Role

Perform this procedure to clone an existing user role.

Before You Begin

You should have an existing user role.

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.

Step 2 Click the **User Roles** tab.

Step 3 From the list of user roles, select the user role you want to clone.

Step 4 Click **Clone**.

Note You cannot see the **Clone** button till you select the user role from the list.

Step 5 In the **Clone User Role** dialog box, complete the following for **User Role** pane:

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

Step 6 Click **Next**.
Step 7 In the**Menu Settings** pane, check or uncheck the checkbox against the menu setting field as per requirement.
Step 8 Click **Next**.
Step 9 In the**User Permissions** pane, check or uncheck the checkbox against the operation field as per requirement.
Step 10 Click **Submit**.
Step 11 In the confirmation dialog box, click **OK**.

Deleting a User Role

Perform this procedure to delete an existing user role.

Before You Begin

You should have an existing user role.

Procedure

Step 1 From the menu bar, choose **Administration** > **System**.
Step 2 Click the **User Roles** tab.
Step 3 From the list of user roles, select the user role you want to delete.
Step 4 Click **Delete**.
Note You cannot see the **Delete** button till you select the user role from the list.
Step 5 In the **Delete User Role** dialog box, click **Submit**.
Step 6 In the confirmation dialog box, click **OK**.

Managing Users

Managing Login Users

Adding a Login User

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

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **Login Users** tab.

Step 3 Click **Add**.

Step 4 In the **Add User** dialog box, complete the following:

Field	Description
User Role drop-down list	Choose **Operator** or **System Admin**.
Login Name field	The login name for the user.
Password field	The password for the user. If the Lightweight Directory Access Protocol (LDAP) authentication is configured to the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	Repeat the password from the previous field.
User Contact Email field	The email address.
First Name field	(Optional) The first name of the user.
Last Name field	(Optional) The last name of the user.
Phone field	(Optional) The phone number of the user.
Address field	(Optional) The postal address of the user.

Step 5 Click **Add**.

Step 6 Click **OK**.

Editing Login User

Perform this procedure when you want to edit a login user.

Before You Begin

The login user group has already been created under Login Users.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.
Step 2 Click the **Login Users** tab.
Step 3 From the list of login users, select the user you want to edit.
Step 4 Click **Edit**.
Step 5 In the **Edit User** dialog box, complete the following:

Field	Description
User Contact Email field	The email address.
First Name field	(Optional) The first name of the user.
Last Name field	(Optional) The last name of the user.
Phone field	(Optional) The phone number of the user.
Address field	(Optional) The postal address of the user.

Note You cannot edit the **User Role** and **Login Name** details of the user.

Step 6 Click **Save**.
Step 7 Click **OK**.

Deleting a Login User

Perform this procedure when you want to delete a login user.

Before You Begin

The login user group has already been created under Login Users.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.
Step 2 Click the **Login Users** tab.
Step 3 From the list of login users, select the user you want to delete.
Step 4 Click **Delete**.
Step 5 In the **Delete User** dialog box, click **Delete**.
Step 6 In the confirmation dialog box, click **OK**.

Changing User Password

Perform this procedure when you want to change the password for a login user.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.
Step 2 Click the **Login Users** tab.
Step 3 From the list of user, select the user role for which you want to change the password.
Step 4 Click **Change Password**.
Step 5 In the **Change Password** dialog box, complete the following:

Field	Description
New Password field	Enter a new password.
Confirm Password field	Repeat the new password.

Step 6 Click **Save**.
Step 7 Click **OK**.

Managing Branding Page

Adding New Login Branding

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

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.
Step 2 Click the **Login Page Branding** tab.
Step 3 Click **Add**.
Step 4 In the **Domain Branding** dialog box, complete the following:

Field	Description
Domain Name drop-down list	A descriptive name for the domain.

Field	Description
Custom Domain Logo checkbox	(Optional) If you want to add a logo, check this checkbox and do the following: **1** Click **Browse**. **2** Navigate to a logo and choose the file. **3** Click **Open**.

Step 5 Click **Submit**.

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

Editing a Branding Page

Perform this procedure when you want to edit the logo of a branding page. You cannot change the name of a branding page.

Before You Begin

You should have a user defined branding page already created.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **Login Page Branding** tab.

Step 3 From the list of branding pages, select the page you want to edit.

Step 4 Click **Edit**.

Note You cannot see the **Edit** button till you select the page from the list.

Step 5 In the **Domain Branding** dialog box, complete the following:

1. Check **Custom Domain Logo** checkbox.
2. Click **Browse**.
3. Navigate to a logo and choose the file.
4. Click **Open**.

Step 6 Click **Submit**.

Step 7 In the confirmation dialog box, click **OK**.

Cloning a Branding Page

Perform this procedure when you want to clone a branding page.

Before You Begin

You should have a user defined branding page already created.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **Login Page Branding** tab.

Step 3 From the list of branding pages, select the page you want to clone.

Step 4 Click **Clone**.

Note You cannot see the **Clone** button till you select the page from the list.

Step 5 In the **Domain Branding** dialog box, complete the following:

Field	Description
Domain Name drop-down list	A descriptive name for the domain.
Custom Domain Logo checkbox	(Optional) If you want to add a logo, check this checkbox and do the following: **1** Click **Browse**. **2** Navigate to a logo and choose the file. **3** Click **Open**.

Step 6 Click **Submit**.

Step 7 In the confirmation dialog box, click **OK**.

Managing Authentication Preference

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

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 From the **Authentication Preferences** drop-down list choose the authentication type.
The following options are available:

- **Local Authentication—**With this authentication preference, LDAP users cannot login to Cisco IMC Supervisor. Continue to Step Step 4.
- **Local First, fallback to LDAP—** If you select this option, then you must configure the LDAP integration. Refer x. Continue to Step Step 4.
- **LDAP First, fallback to local—** If you select this option, then you must configure the LDAP integration. Refer x. Continue to Step Step 4.
- **Verisign Identity Protection—** If you select this option, continue to Step Step 3.

Step 3 If you select Verisign Identity Protection, complete the following steps:

1. Click **Browse** to upload a VIP certificate. Locate and select the certificate, and click **Upload**.
2. Enter the password.

Step 4 Click **Save**.

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. In addition, LDAP synchronization is also available as a 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.

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

LDAP Integration Rules and Limitations

User Synchronization Rules

- 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.

User Synchronization Limitations

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

Note Be sure that the user is assigned to the correct group after the LDAP synchronization process.

Adding LDAP Configurations

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Choose the **LDAP Integration** tab.

Step 3 Click + to add LDAP configurations.

Step 4 In the **Add LDAP Configurations** dialog box, complete the following fields:

Field	Description
Account Name field	An LDAP account name.
Server Type drop-down list	Choose either Microsoft Active Directory or Open LDAP.
Server field	Host name or the IP address of the server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name for the LDAP user.
Username field	Enter a name for the LDAP user.
Password field	Enter a password associated with the username.

Step 5 Click **Next**.

Step 6 In the **LDAP Search Base** dialog box, 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 88.

Step 7 Click **Select** in the **Select** dialog box.
The search criteria you have selected is displayed next to the **Search Base** field.

Step 8 Click **Next** in the **LDAP Search Base** dialog box.

Step 9 Click + to add entry to user role filters table in the **LDAP User Role Filter** dialog box.

Step 10 Enter the user role details in the **Add Entry to User Role Filters** dialog box.

Step 11 Click **Submit**.

Step 12 In the **Submit Result** dialog box, click **OK**.
You can edit or delete these filters. You can also use the up or down arrows to move the filters to set priority.

Step 13 Click **Submit** in the **LDAP User Role Filter** dialog box.

Step 14 In the **Submit Result** dialog box, click **OK**.

Viewing LDAP Server Summary Information

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Choose the **LDAP Integration** tab.

Step 3 Choose an LDAP account name from the table.

Step 4 Click **View**.
The **View LDAP Account Information** dialog box displays summary information of the LDAP account.

Step 5 Click **Close**.

Testing LDAP Server Connectivity

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Choose the **LDAP Integration** tab.

Step 3 Choose an LDAP account name from the table.

Step 4 Click **Test Connection**.
The status of the connection is displayed.

Step 5 Click **Close** in the **Test LDAP Connectivity** dialog box.

Searching BaseDN

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **LDAP Integration** tab and select an LDAP account.

Step 3 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 4 Click **Select** in the **LDAP Search Base** dialog box.

Step 5 Choose one or more users and click **Select** in the **Select** dialog box.

Step 6 Click **Submit** in the **LDAP Search Base** dialog box.

Step 7 In the **Submit Result** dialog box, click **OK**.

Requesting Manual LDAP Sync

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **LDAP Integration** tab and select an LDAP account.

Step 3 Click **Request Manual LDAP Sync**.

Step 4 In the **Manual LDAP Sync** dialog box, choose **Advanced Search** check box.
Ignore the **Basic Search** check box.

Step 5 Click + to add an entry for user filters.

Step 6 In the **Add Entry to User Filters** dialog box, complete the attribute details.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.
You can also edit or delete entries, or use the up or down arrows to move the entries in the table.

Note Ignore the **Group Filters** table.

Step 9 Click **Next**.

Step 10 In the **Select Users and Groups** dialog box, click **Select** next to **LDAP Users** field.

Note Ignore the **LDAP Groups** field.

Step 11 In the **Select** dialog box, check the usernames and click **Select**.

Step 12 Click **Submit**.

Step 13 In the **Submit Result** dialog box, click **OK**.
From the menu bar, choose **Administration** > **Users** and click **Login Users** tab to see the synced users. Note that the access level of the user will be **Operator** and the user group is **Default Group**.

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
- Search BaseDN selections

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **LDAP Integration** tab and select an LDAP account.

Step 3 Click **Modify**.

Step 4 In the **Modify LDAP Server Configuration** dialog box, edit the following fields:

Name	Description
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
User Name field	The user name. If you selected **OpenLDAP** as the LDAP Directory Type, then specify the user names in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where **ou** specified is the one all the other users are placed in the directory hierarchy.
Password field	The user password.

Step 5 Click **Next**.

Step 6 In the **LDAP Search Base** dialog box, click **Select** to specify LDAP search base entries and click **Select**.

Step 7 Click **Next**.

Step 8 In the **LDAP User Role Filter** dialog box, click add, edit, delete, or move table entries using up and down arrows.

Step 9 Click Submit in the respective dialog boxes.

Step 10 In the **Submit Result** dialog box, click **OK**.

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

Step 12 In the **Submit Result** dialog box, click **OK**.

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.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Choose the **LDAP Integration** tab.

Step 3 Choose an LDAP account name from the table.

Step 4 Click **Delete**.

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

Step 6 Click **OK**.
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.

Managing Users Password Policy

Perform this procedure when you want to change the users password policy.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users**.

Step 2 Click the **Password Policy** tab.

Step 3 For the **Minimum Password Length**, choose a value from the drop-down list.

Step 4 For the **Maximum Password Length**, choose a value from the drop-down list.

Step 5 For the **Minimum Character Classes**, choose a value from the drop-down list.

Step 6 (Optional) If checked, **Disallow Login in Password** checkbox will not allow users to use the login text as password.

Step 7 (Optional) If checked, **Disallow Previouis Password** checkbox will not allow users to use the same password again while changing the password.

Step 8 (Optional) For **Disallow Password that match Regular Expression**, enter common expressions which you do not want users to choose as password. Prefix each expression with #.

Step 9 Click **Submit**.

Step 10 In the confirmation dialog box, click **OK**.

Managing Integration

Configuring CMDB Integration Setup

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.

Perform this procedure when you want to configure or change CMDB integration settings.

Procedure

Step 1 From the menu bar, choose **Administration** > **Integration**.

Step 2 Choose the **CMDB Integration Setup** tab and complete the following fields:

Field	Description
Export to FTP Server checkbox	Check the check box to export change records to an FTP server.
Export Format drop-down list	Choose CSV or XML from the list.
FTP Server field	FTP server IP address.
FTP Port field	(Optional) FTP server port number.
FTP User field	(Optional) FTP server user name.
FTP Server field	FTP server user password.

Field	Description
FTP Export Frequency drop-down list	Choose the frequency from the drop-down list.
FTP File Name field	FTP server user password.
Test FTP checkbox	Check the check box to test FTP settings.

Step 3 Click **Save**.

Viewing Audit Logs

Cisco IMC Supervisor can store up to 10000 audit logs. If the number of logs exceed 10000 logs, then the**CMDB 10K Records Purge Task**, which runs every 24 hours, purges the old logs.

Perform this procedure when you want to view audit logs.

Procedure

Step 1 From the menu bar, choose **Administration** > **Integration**.

Step 2 Choose the **Change Records** tab.
The following records are available:

Field	Description
ID	Serial number of the log.
Change Time	System time when the change was done.
Change Type	Type of change (ADD, MODIFY, or DELETE)
Resource Type	Type of the resource.
Change by User	Login user name.
Resource Name	IP address or name of the resource.
Description	Description of the log.
Additional Details	Additional details for the log.

Note You may customize the number of records to display on one page. Click the drop-down list at the far right bottom corner of the page and choose the number of records from the list to display on one page.

Configuring User Interface Settings

You can use this procedure to update the header title and other header options on the Cisco IMC Supervisor.

Procedure

Step 1 From the menu bar, choose **Administration** > **User Interface Settings**.

Step 2 In the **User Interface Settings** window, complete the following:

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

Step 3 Click **Save**.

Step 4 In the confirmation dialog box, click **OK**.

Viewing Support Information

You can use this procedure to view the support information for Cisco IMC Supervisor.

Before You Begin

Ensure that the pop-up blocker is disabled for your web browser.

Procedure

Step 1 From the menu bar, choose **Administration** > **Support Information**.

Step 2 In the **Support Information** window, you can view:

Table 3: System information (basic)

Field	Description
Support Information drop-down list	Choose **System Information (Basic)** and click **Submit** to view basic information.

Table 4: System information (advanced)

Field	Description
Support Information drop-down list	Choose **System Information (Advanced)** and click **Submit** to view advanced information such as processor, memory, disk information and so on.

Table 5: View Logs

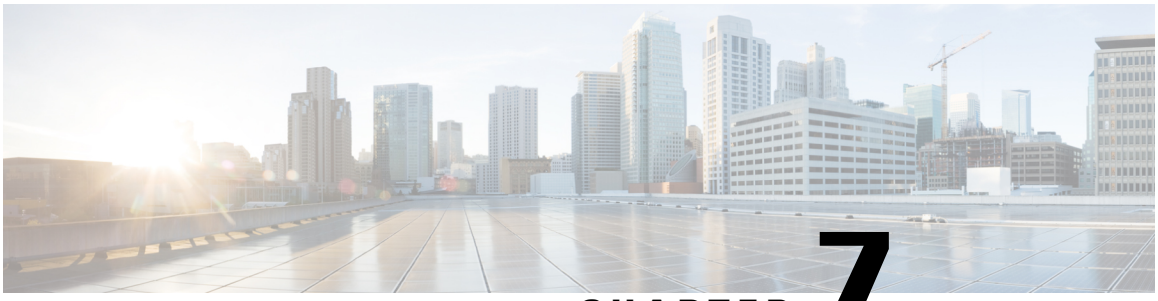
Field	Description
Support Information drop-down list	Choose **Show log**.
Show Log drop-down list	Choose the log type you want to view and click **Show Logs**.

Table 6: Download All Logs

Field	Description
Support Information drop-down list	Choose **Download All Logs** and click **Download**.

Table 7: Download Debug Logging

Field	Description
Support Information drop-down list	1 Choose **Debug Logging** and click **Start Debug Logging**. 2 To stop and download log data, click **Stop Debug Logging** and click the download debug link.



CHAPTER 7

Frequently Performed Tasks and Procedures

This chapter contains the following topics:

Frequently Performed Procedures

This section provides a quick access to frequently performed procedures in Cisco IMC Supervisor. The reference directs you to the section of the document where the detailed procedures has already been described.

Procedure	Reference
How to log in Cisco IMC Supervisor	Launching Cisco IMC Supervisor, on page 7
How to update license	Updating the License, on page 7
How to add login users in Cisco IMC Supervisor	Adding a Login User, on page 79
How to add a rack group	Adding a Rack Group, on page 8
How to create a rack account	Adding a Rack Account, on page 9

Miscellaneous Procedures

Enabling Dashboard Auto Refresh

Perform this procedure to enable auto refreshing for the reports added on the dashboard. You can also define the refresh rate.

Procedure

Step 1 From the menu bar, choose **Dashboard**.

Step 2 In the **Dashboard** panel, beside the **Automatic Refresh** option, click **OFF**.
Automatic Refresh option changes to **ON** and **Interval** slide bar is visible.

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

Note You can set the refresh rate in multiples of 5 minutes up to a maximum of 60 minutes.

Adding Summary Reports to Dashboard

Perform this procedure to add a summary report to dashboard for quick access.

Note Only summary reports can be added to dashboard.

Procedure

Step 1 Browse to the summary report you want to add to the dashboard.

Step 2 Click the down arrow on the right upper corner of the report panel.

Step 3 Click **Add to Dashboard**.

Note **Add to Dashboard** option is available only if the summary report supports dashboard view.

Step 4 From the menu bar, choose **Dashboard** and verify that the report appears on the dashboard.

Adding a Menu or Tab to Favorites

Perform this procedure to add a menu option or tab to **Favorites** menu.

Procedure

Step 1 Browse to the menu or tab you want to add to **Favorites** menu.

Step 2 Click **Favorite**.

Note You can see the **Favorite** button only if the menu or tab supports it.

Step 3 In the **Favorite Report** dialog box, you may edit the **Menu Label** field.

Step 4 Click **Save**.

Step 5 From the menu bar, choose **Favorites** and verify the new menu is visible.

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**.