Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.0

First Published: March 18, 2016

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.

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

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

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

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 2.0

Feature	Description	Where Documented
Support for Scheduling Tasks	Defining a schedule allows you to defer certain tasks to occur at a different time. Tasks such as firmware updates or server discovery can be scheduled to run at a pre-defined time or at a pre-defined frequency. You could schedule tasks during off-peak hours where the workloads on servers are low.	Overview of Managing Schedules, on page 103.
Introduction of FlexFlash Policy	A FlexFlash policy allows you to configure and enable the SD card.	FlexFlash Policy, on page 72.

Feature	Description	Where Documented
Support Smart Call Home	Cisco Smart Call Home is an automated support capability that provides continuous monitoring, proactive diagnostics, alerts, and remediation recommendations on select Cisco devices. Cisco IMC Supervisor managed server tasks such as Group Rack Server Inventory, Rack Server Fault, and Health System are run at periodic intervals and send relevant information to the Smart Call Home backend. The backend processes this data and if issues are identified, it will automatically raise cases with the TAC for resolution of issues.	Overview of Smart Call Home, on page 109.
Running Server Diagnostics	Server diagnostics is available through UCS Server Configuration Utility (UCS-SCU). You can use diagnostics tools to diagnose hardware problems with your Cisco servers and run tests on various server components to find out hardware issues along with analysis of the test results in a tabular format.	Overview of Server Diagnostics, on page 105.
Automated Notifications on Patch Releases	Cisco IMC Supervisor periodically (every 14 days) checks for any new patch releases that are made available on Cisco.com. If you have configured the settings, you will be notified if there is a new version. If a higher version is available, the Diagnostic System Messages dialog box displays a message that a newer version of Cisco IMC Supervisor is found. If you have not configured the update settings, you will find a notification bubble next to your login name on the top right corner. The Diagnostic System Messages dialog box displays a message that settings are not configured.	Overview of Updating Cisco IMC Supervisor Patches, on page 101.

Feature	Description	Where Documented
Support for Creating a Group Share Policy	You can now share a policy you have created with a user group.	Adding Group Share Policy, on page 36.

New and Changed Information for this Release

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:

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

- Defining schedules to defer tasks such as firmware updates or server discovery
- Diagnosing server hardware issues using UCS Server Configuration Utility
- Cisco Smart Call Home provides proactive diagnostics, alerts, and remediation recommendations

About Licenses

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

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

Important If you are using an evaluation license for Cisco IMC Supervisor, note that when this license expires (90 days from the date the license is generated), retrieving inventory and system health information, such as faults, will not work. You will not be able to refresh system data, or even add new accounts. At that point, you must install a perpetual license to use all features of Cisco IMC Supervisor.

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

1. Before you install Cisco IMC Supervisor, generate the Cisco IMC Supervisor license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in Fulfilling the Product Access Key, on page 6.
3. After you install Cisco IMC Supervisor, update the license as described in Updating the License, on page 15.
4. After the license has been validated, you can start to use Cisco IMC Supervisor.

For various other licensing tasks you can perform, see Licensing Tasks, on page 14.

Fulfilling the Product Access Key

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

Before You Begin

You need the PAK number.

Procedure

Step 1 Navigate to the Cisco Software License website.

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

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

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

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

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

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

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

Common Terms in the Cisco IMC Supervisor User Interface

Rack Groups

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

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

Rack Account

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

Policies

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

Profiles

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

Common User Interface Options

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

Icon	Label	Description
	**Refresh**	Refreshes the reported data on the page.
	**Favorite**	Adds a page to the **Favorites** menu. You can use this option to view frequently accessed pages more quickly.
	**Add**	Brings up the **Add** dialog box, from which you can add a new resource.

Icon	Label	Description
	Edit	Brings up the **Edit** dialog box, from which you can edit a resource.
	Customize Table	Brings up the **Customize Report Table** dialog box, in which you choose what columns you want to include on the screen.
	Export Report	Brings up the **Export Report** dialog box, from which you download a report to your system. You can generate a report in one of the following formats: • PDF • CSV • XLS
	Expand	Expands all the folders that are displayed on the page.
	Collapse	Collapses all the folders that are displayed on the page.
	Add Advanced Filter	Adds additional filtering parameters on the page.
	Search Field	Accepts a keyword to filter for specific records on the page.

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

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

Procedure

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

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

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

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

You can add these lines anywhere in the file.

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

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

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

Procedure

Step 1 Log in as root.

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

a) Comment out the existing port 8080 Connector tag

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

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

```
<Connector port="8080" protocol="HTTP/1.1"
```

```
maxThreads="150" minSpareThreads="4"
connectionTimeout="20000"
URIEncoding = "UTF-8" />
```

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

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

Step 4 Restart the services.

Step 5 Launch the user interface and log in to the system.
You can now log into the system in the non-secure mode using the following URL format:

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

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

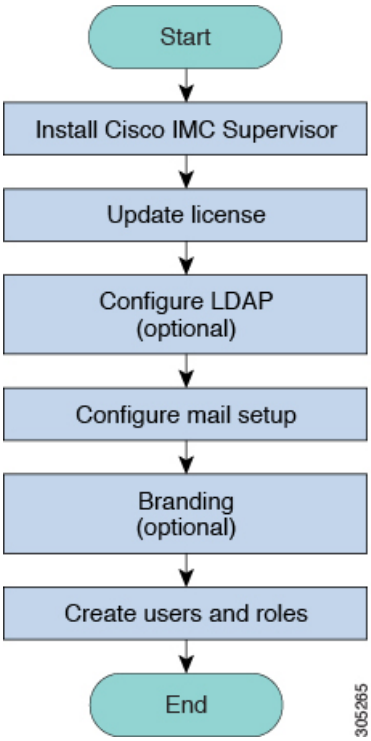
CHAPTER 3

Getting Started

This chapter contains the following topics:

Overview

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



Launching Cisco IMC Supervisor

Perform this procedure to log in to Cisco IMC Supervisor.

Before You Begin

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

Procedure

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

- User Name - admin
- Password - admin

Licensing Tasks

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

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

Updating the License

You must perform the following procedure to update the license before you start using Cisco IMC Supervisor. For the list of valid licenses, see About Licenses, on page 6. You must generate a license key, claim and register the Product Access Key. After installing Cisco IMC Supervisor, the license is validated and you can start using Cisco IMC Supervisor.

Before You Begin

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

Procedure

Step 1 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.

Running License Audit

Perform this procedure when you want run license audits.

Before You Begin

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

Procedure

Step 1 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**.
This process takes some time to complete.

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

Authentication and LDAP Integration

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

Name	Description
Local First, fallback to LDAP	Authentication is done first at the local server (Cisco IMC Supervisor). If the user is unavailable at the local server, the LDAP server is checked.
Verisign Identity Protection	VIP Authentication Service (two-factor authentication) is enabled.

Configuring Authentication Preferences

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

Procedure

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

Step 2 Choose the **Authentication Preferences** tab

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

- **Local First, fallback to LDAP**

  If you select this option, then you must configure LDAP servers. For more information, see Configuring LDAP Servers, on page 19.

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

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

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

b) Enter the **Password.**

Step 5 Click **Save**.

Configuring LDAP

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

LDAP Integration 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 Ensure that the user is assigned to the correct group after the LDAP synchronization process.

Adding LDAP Configurations

Perform this procedure to add LDAP configurations.

Procedure

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

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

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 23.

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**.

Configuring LDAP Servers

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

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

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

Before You Begin

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

Procedure

Step 1 On the menu bar, choose **Administration** > **Users and Groups**.

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

Step 3 Click **Add**.

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

Name	Description
Account Name field	The name of the account. This name must be unique.

Name	Description
Server Type field	The type of LDAP server. It can be one of the following: • OpenLDAP • MSAD - Microsoft Active Directory
Server field	The IP address or the host name of the LDAP server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name. If you selected **OpenLDAP** as the LDAP Directory Type, then this domain name must match the domain specified with the user name. **Important** You must specify the complete domain name. For example, vxedomain.com.
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.
Synchronization Frequency drop-down list	Select the frequency (hours) at which the LDAP server must be synchronized. It can be one of the following: • 1 • 4 • 12 • 24

Step 5 Click **Next**.

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

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

Step 7 Click **Next**.

Step 8 In the **Configure User and Group Filters** pane, complete the following fields:

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

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

Step 9 Click **Next**.

Step 10 In the **LDAP User Role Filter** pane, click the + sign to add a user role filter.

Step 11 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**

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

Step 12 Click **Submit**.

Step 13 Click **OK**.
The user role filters are added to the **User Role Filters** table.

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

If you manually update the user role for a user from the **Login Users** tab, then the user role that you mapped the group is no longer applied on the user.

What to Do Next

If you have not set the authentication preference to LDAP, then you are prompted to modify the authentication preference. For more information on changing the authentication preference, see Configuring Authentication Preferences, on page 16.

Viewing LDAP Server Summary Information

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

Procedure

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

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

Perform this procedure to text the LDAP connection.

Procedure

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

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

Perform this procedure to search the BaseDN.

Procedure

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

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

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

Procedure

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

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, complete the following fields:

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

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

Step 5 For basic search, click **Select** to specify the search base.

Step 6 Choose the search base DN, and click **Select** and continue to Step 9.

Step 7 For advanced search, in the **Advanced Filtering Options** pane, add or edit attribute names for **User Filters** and **Group Filters**.

Step 8 Click **Next**.

Step 9 In the **Select Users and Groups** dialog box, complete the following fields:

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

Step 10 Click **Submit**.

Step 11 In the **Submit Result** dialog box, click **OK** to synchronize the LDAP server.
From the menu bar, choose **Administration** > **Users and Groups** and click **Users** tab to see the synchronized users.

Viewing LDAP Synchronized Results

Perform this procedure to view the LDAP synchronized results.

Procedure

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

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

Step 3 Click **Results**.

Step 4 Click the **License Status** tab to view the validity of the Cisco IMC Supervisor license.

Step 5 Click the **LDAP Integration** tab to view the details such as the start and end time of LDAP synchronization, status of synchronization and a detailed message of the status.

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

Perform the following procedure to modify the LDAP server details.

Procedure

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

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.

Name	Description
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 **Configure User and Group Filters** pane, select and edit the required attributes in the **User Filters** and **Group Filters** table.

Step 9 Click **Next**.

Step 10 In the **LDAP User Role Filter** dialog box, click add, edit, delete, or move table entries using up and down arrows.

Step 11 Click Submit in the respective dialog boxes.

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

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

Step 14 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. Perform this procedure to delete the LDAP server information.

Procedure

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

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.

Configuring a SCP User

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

Procedure

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

Step 2 Click the **SCP User Configuration** tab.

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

Step 4 Click **Submit**.

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

Configuring Mail Setup

All outgoing emails from Cisco IMC Supervisor require an SMTP server. Cisco IMC Supervisor generated emails such as alerts for faults and so on are sent to the mail setup you have configured using the following procedure. For more information about adding email alert rules, see Adding Email Alert Rules for Server Faults, on page 50.

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.

Field	Description
Send Test Email checkbox	Check this check box to send a test email to the configured address.

Step 4 Click **Save**.

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

Branding

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

Adding New Login Branding Page

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

Procedure

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

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

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

Configuring User Interface Settings

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

Procedure

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

Step 3 Click **Save**.

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

CHAPTER 4

Creating Users and User Roles

This chapter contains the following topics:

Overview

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

- **System Admin —** A user with the privilege of adding users. As an administrator in Cisco IMC Supervisor, you can assign users to system-provided user roles or to custom-defined user roles. In addition, at a later point in time, you can view information on the role that a user is assigned to. You can perform the following tasks with user roles:
  - Create a custom user role in the system, and create users with this role or assign the role to existing users.

    When you create a new user role, you can specify if the role is that of an administrator or an operator. For more information about creating users, see Creating a User, on page 32 and for create user roles, see Adding a User Role, on page 33.
  - Modify existing user roles, including default roles, to change menu settings and read/write permissions for users associated with that role.

    The procedure to modify menu settings and permissions for a role is the same as the procedure followed while creating a user role.
- **Group Admin —** A system-defined user group **Default Group** is available by default in Cisco IMC Supervisor. As a group administrator, you can create and assign users to this group or you can assign

them to the groups you have created. A user can be part of multiple user groups. However, the group that the user was most recently added to is set as the default primary group for the user.

- **Operator —** As the system administrator's role type is admin, you can modify the existing Operator role as required with any combination of access restrictions (menu settings and user permissions).

Creating a User

Perform this procedure when you want to create a new user.

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

Procedure

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

Step 2 Click the **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 **Group Admin**, **Operator**, or **System Admin**.
User Group drop-down list	Select the group that the user will have access to. You can either select a group already available, or you can add a new group. **Note** This field is visible only when you select **Group Admin** as the user role.
Login Name field	The login name for the user.
Password field	The password for the user. If the Lightweight Directory Access Protocol (LDAP) authentication is configured to the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	Repeat the password from the previous field.
User Contact Email field	The email address.
First Name field	(Optional) The first name of the user.
Last Name field	(Optional) The last name of the user.
Phone field	(Optional) The phone number of the user.
Address field	(Optional) The postal address of the user.

Step 5 Click **Add**.

Step 6 Click **OK**.

Viewing Online Users

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

Procedure

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

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

Adding a User Role

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

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**.
Description field	(Optional) A description of the user role.

Step 5 Click **Next**.

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

Step 7 Click **Next**.

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

Step 9 Click **Submit**.

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

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

Adding a User Group

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

Procedure

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

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

Step 3 Click **Add**.

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

Field	Description
Name field	A name of the user group.
Description field	(Optional) A description of the user group.
Code field	(Optional) A shorter name or code name for the group.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals if necessary.
First Name field	(Optional) The contact's first name.
Last Name field	(Optional) The contact's last name.
Phone field	(Optional) The contact's phone number.
Address field	(Optional) The contact's address.
Group Share Policy drop-down list	(Optional) Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies.

Field	Description
Allow Resource Assignment To Users checkbox	(Optional) If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

Step 6 Click **OK**.

Note You can select these user groups and manage them by viewing, editing, deleting, enabling, and disabling them. You can also manage tags from the **User Groups** tab.

Branding a User Group

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

Procedure

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

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

Step 3 Select a user group.

Step 4 Click **Branding**.

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

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

Step 6 Click **Submit**.

Step 7 Click **OK** in the **Submit Result** dialog box.

Group Share Policy

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

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

Adding Group Share Policy

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

Procedure

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

Step 2 Click the **Group Share Policy** tab.

Step 3 Click **Add**.

Step 4 In the **Add Group Share Policy** dialog box, complete the following fields:

Field	Description
Policy Name field	The name of the group share policy.
Policy Description field	The description of the policy.
Select Groups drop-down list	Choose the groups to share the policy you have created.

Step 5 Click **Submit**.

Step 6 Click **OK** in the **Submit Result** dialog box.

Note You can also select an existing policy to view, edit, delete, and clone them.

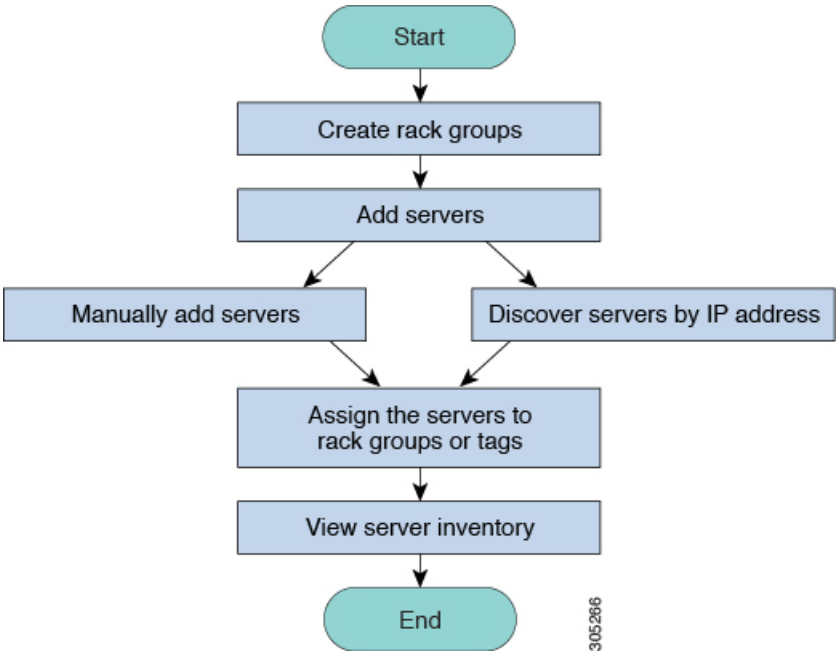
CHAPTER 5

Managing Server Discovery, Rack Groups, and Rack Accounts

This chapter contains the following topics:

Overview

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



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

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

Discovering and Importing a Server

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

Configuring Auto Discovery Profile

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

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

Procedure

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

Step 2 Click the **Discovery Profiles** tab.

Step 3 Click **Add**.

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

Field	Description
Profile Name Field	A descriptive name for the profile.
Search Criteria drop-down list	Select **IP Address Range**, **Subnet Mask Range**, **IP Address CSV File**, or **IP Address List** from the drop-down list.
Starting IP Field	Valid IP address
Ending IP Field	Valid IP address
If you check **Use Credential Policy** checkbox	
Credential Policy drop-down list	Choose a policy from the drop-down list or click the + icon and create new policy. Refer Creating a Credential Policy, on page 68 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**.

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

Performing Auto Discovery

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

Before You Begin

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

Procedure

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

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

Step 3 Click **Discover**.

Step 4 In the **Discover Devices** dialog box, complete the following fields: select a profile from the **Select Profile** drop-down list.

Field	Description
Select Profile drop-down list	Click **Select** to choose the profiles to discover. Check the check boxes of all the profiles you want to discover.
Schedule Later check box	Check this check box and select an existing schedule to auto discover servers at a later time or click on + to create a new schedule. For more information on creating schedules, see Creating Schedules, on page 103. You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to view the scheduled task or click **Remove Scheduled Tasks** to delete scheduled tasks.
Schedule(s) drop-down list	If you have chosen the **Schedule Later** check box, this schedule(s) select a schedule you have created from the list. **Note** You can also create a new schedule from this dialog box.

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:

Field	Description
Select Device(s) field	Click **Select** to choose the devices to import. Check the check boxes of all the servers you want to import. **Note** If the **Import Status** of a particular rack account is imported then the status will be imported and will not show that rack account for import.
User Prefix	Enter a prefix for the user.
Description	Enter a description for the user.
Contact	Enter the contact details of the user.
Location	Enter the address of the user.
Select Rack Group drop-down list or + icon	Choose a rack group or create a rack group.

Step 5 Click **Submit** if you have selected a rack group or **Create** if you have chosen to create a rack group.

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

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

Adding a Rack Group

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

Before You Begin

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

Procedure

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

By default, **Rack Group** tab is selected.

Step 2 Click **Add**.

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 froup.

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 rackmount server to any of the Rack Group to the Cisco IMC Supervisor. After the account is added, you can use Cisco IMC Supervisor to manage the server.

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

Before You Begin

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

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

- Ensure that you have enabled XML API in Cisco IMC Supervisor. This ensures that you can add and manage the rackmount servers 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 rackmount 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 check box to select the policy from the drop-down list.
If you check **Use Credential Policy** check box	
Credential Policy drop-down list	Choose a policy from the drop-down list.
If you uncheck **Use Credential Policy** check box	
User Name field	Login ID for the rackmount server.
Password field	Password for the login ID for the rackmount 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 or + icon	Choose a rack group from the list or click + to create a rack group. For more information on creating a rack group, see Adding a Rack Group, on page 41.
Contact field	(Optional) The contact email address for the account.
Location field	(Optional) The location of the account.

Step 5 Click **Submit**.

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

What to Do Next

Test the rack server connection. Refer Testing an Account Connection, on page 45.

Collecting Inventory for Rack Accounts or Rack Groups

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

Before You Begin

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

Procedure

Step 1 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.

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

Step 6 Click **Submit**.

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

Testing an 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.

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

CHAPTER 6

Viewing Inventory Data and Faults

This chapter contains the following topics:

Viewing Rack Mount Server Details

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

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 a server from the list.

The following details are available for a rackmount server:

Tab	Description
Summary	An overview of the rack account.
CPUs	The details of the CPU used in the server.
Memory	The details of the memory used in the server.
PSUs	The details of the power supply unit used in the server.
PCI Adapters	The details of the PCI adapters used in the server.
VIC Adapters	The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click **View Details** to view information such as **External Ethernet Interfaces**, **VM FEXs** and so on.
Network Adapters	The details of the network adapters used in the server. Select any of the Network Adapters listed and click **View Details** to view information on **External Ethernet Interfaces**.
Storage Adapters	The details of the storage adapters used in the server. Select any of the Storage Adapters listed and click **View Details** to view information such as **Controller Info**, **Physical Drives** and so on.
FlexFlash Adapters	The details of the FlexFlash adapters used in the server. Select any of the FlexFlash Adapters listed and click **View Details** to view information such as **Controller Info**, **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	The information on the protocol such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.
Remote Presence	The details of vKVM, Serial Over LAN, and vMedia.
Faults	The details of the faults logged in the server.
Users	The details of users.
Cisco IMC Log	The details of the Cisco IMC logs for the server.
System Event Log	the details of the server logs.
TPM	Information on the TPM inventory.

Tab	Description
BIOS	Details about the BIOS settings and Boot Order for the server. Select the server and click on **View BIOS Settings**, **View Boot Settings**, or **View Boot Order**.
Fault History	Historical information on the faults that occurred on the server.
Tech Support	Details about the tech-support log files such as the file name, destination type, status of the upload and so on are displayed in the **Tech Support** table. An option to export the tech-support log files to a remote server or on the Cisco IMC Supervisor appliance, in a local directory is available. For more information about exporting, see Exporting Technical Support Data to a Remote Server, on page 63.
Associated Hardware Profiles	Details of policies that are associated to a hardware profile.

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

Viewing Fault Details for a Rack Mount Server

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

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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.

Summary Reports for a Rack Group

The Inventory and Fault Status for Rack Groups page is divided vertically into two sections. Left pane contains the list of the Rack Groups. When the Rack Groups heading is selected in the left pane including Default Group, a Summary report is available in the right pane which displays the following reports:

- **Faults—**represents the overall fault count for selected rack groups. The fault counts are categorized based on their severity such as Critical, Major, Warnings, Minor, and Info.
- **Server Health—**represents the overall health status of the server. The overall server health status can be in any of the states such as Good, Memory Test In Progress, Moderate Fault, and Severe Fault.

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

- **Firmware Versions—**represents the overall server count of the firmware versions that are managed for the selected rack groups.
- **Server Models—**represents the overall server count of the models that are managed for the selected rack groups.
- **Power State—**represents the overall server count of the power state which is managed for the selected rack groups. The power states can either be On or Off.
- **Server Connection Status—**represents the overall server count of the connection status of servers for the selected rack groups. The connection status can either be Success or Failed.

Adding Email Alert Rules for Server Faults

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

Procedure

Step 1 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.
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 **Edit** and **Delete** options are visible only when you select a rule. Click **Edit** and modify the required fields displayed or click **Delete** and confirm deletion.
- You can select multiple rules concurrently and click **Delete** to delete them.
- The number of email alerts sent are based on the number of rules you have created.
- If you have a system level rule present in 1.0 or 1.0.0.1, when you upgrade to 1.1, you can see that the name of the rule by default is added as **system-default**. You cannot modify the **Alert Level** field for this group, but you can delete this system level rule.

CHAPTER 7

Managing Rack Servers

This chapter contains the following topics:

Viewing Rack Mount Server Details

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

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 a server from the list.

The following details are available for a rackmount server:

Tab	Description
Summary	An overview of the rack account.
CPUs	The details of the CPU used in the server.
Memory	The details of the memory used in the server.
PSUs	The details of the power supply unit used in the server.
PCI Adapters	The details of the PCI adapters used in the server.
VIC Adapters	The details of the VIC adapters used in the server. Select any of the VIC Adapters listed and click **View Details** to view information such as **External Ethernet Interfaces**, **VM FEXs** and so on.
Network Adapters	The details of the network adapters used in the server. Select any of the Network Adapters listed and click **View Details** to view information on **External Ethernet Interfaces**.
Storage Adapters	The details of the storage adapters used in the server. Select any of the Storage Adapters listed and click **View Details** to view information such as **Controller Info**, **Physical Drives** and so on.
FlexFlash Adapters	The details of the FlexFlash adapters used in the server. Select any of the FlexFlash Adapters listed and click **View Details** to view information such as **Controller Info**, **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	The information on the protocol such as HTTP, HTTPS, SSH, IPMI Over LAN, NTP, and SNMP.

Tab	Description
Remote Presence	The details of vKVM, Serial Over LAN, and vMedia.
Faults	The details of the faults logged in the server.
Users	The details of users.
Cisco IMC Log	The details of the Cisco IMC logs for the server.
System Event Log	the details of the server logs.
TPM	Information on the TPM inventory.
BIOS	Details about the BIOS settings and Boot Order for the server. Select the server and click on **View BIOS Settings**, **View Boot Settings**, or **View Boot Order**.
Fault History	Historical information on the faults that occurred on the server.
Tech Support	Details about the tech-support log files such as the file name, destination type, status of the upload and so on are displayed in the **Tech Support** table. An option to export the tech-support log files to a remote server or on the Cisco IMC Supervisor appliance, in a local directory is available. For more information about exporting, see Exporting Technical Support Data to a Remote Server, on page 63.
Associated Hardware Profiles	Details of policies that are associated to a hardware profile.

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

Viewing Fault Details for a Rack Mount Server

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

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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 and Off a Rack Mount Server

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

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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.

Note You can also select multiple rack servers.

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

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**.

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 to reset the server.

Note You can also select multiple rack servers.

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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 a Rack Mount Server

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

Note You can also select multiple rack servers.

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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

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**.

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

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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

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

Note You can also select multiple rack servers.

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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

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

Before You Begin

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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

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

Before You Begin

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

Procedure

Step 1 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.

Step 6 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 7 Click **Submit**.

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

Step 9 Select a tag in the **Manage Tags** dialog box and click on the Edit icon to edit a tag.

Step 10 Choose the Tag Name and Tag Value to modify the tags

Step 11 Click **Submit**

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

Adding Tags for a Rack-Mount Server

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

Before You Begin

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

Note You can also select multiple rack servers.

Procedure

Step 1 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 61 to create tags.

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

Exporting Technical Support Data to a Remote Server

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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**
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**.

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

Clearing SEL

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

Procedure

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

Step 2 In the left pane, select **Rack Groups**.

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**.

Managing System Tasks

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

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

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

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

Procedure

Step 1 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.
System Task Policy drop-down list	Choose one of the following options: • **default-system-task-policy** • **local-run-policy**
Hours drop-down list	Choose the hourly frequency to run the task.

Step 5 Click **Submit**.

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**.

CHAPTER 8

Managing Policies and Profiles

This chapter contains the following topics:

Credential Policies

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

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

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

You can perform various tasks such as adding, editing, and deleting policies from this page. For information about creating a credential policy, see Creating a Credential Policy, on page 68.

Creating a Credential Policy

Perform this procedure 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**.
You can edit, clone, delete, view, apply and view server mappings of the credential policy you have created.

Hardware Policies

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

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

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

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

1. Create a hardware policy such as BIOS policy or an NTP policy. You can create a policy in one of the following methods:
   a. Create a new policy. For more information about the various policy types and creating a new policy, see Creating Hardware Policies, on page 69.
   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 86.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Policy, on page 87.
3. Perform any of the following optional tasks on the policy:
   a. Edit
   b. Delete
   c. Clone
   d. You can also view the list of servers that are mapped to a specific policy. For more information on performing these tasks, see General Tasks Under Hardware Policies, on page 88.
   e. You can apply profiles to servers after creating various policies and grouping them into profiles. For more information about applying profiles, see Applying a Hardware Profile, on page 91.

Creating Hardware Policies

Perform this procedure to create hardware policies.

Procedure

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

Step 2 Choose the **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 70	*Configuring BIOS Settings*

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
Disk Group Policy, on page 71	*Managing Storage Adapters*
FlexFlash Policy, on page 72	*Managing the Flexible Flash Controller*
IPMI Over LAN Policy, on page 75	*Configuring IPMI*
LDAP Policy, on page 76	*Configuring the LDAP Server*
Legacy Boot Order Policy, on page 77	*Server Boot Order*
Network Security Policy, on page 78	*Network Security Configuration*
NTP Policy, on page 79	*Configuring Network Time Protocol Settings*
Precision Boot Order Policy, on page 79	*Configuring the Precision Boot Order*
RAID Policy, on page 80	*Managing Storage Adapters*
Serial Over LAN Policy, on page 81	*Configuring Serial Over LAN*
SNMP Policy, on page 82	*Configuring SNMP*
SSH Policy, on page 83	*Configuring SSH*
User Policy, on page 83	*Configuring Local Users*
VIC Adapter Policy, on page 85	*Viewing VIC Adapter Properties*
Virtual KVM Policy, on page 84	*Configuring the Virtual KVM*
vMedia Policy, on page 86	*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 87.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 80.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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.

FlexFlash Policy

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

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

Note The minimum Cisco Integrated Management Controller firmware version for FlexFlash support is 2.0(2c).

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 Click **Add** in the **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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

Step 3 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 86.

Step 4 In the **Configure Cards** dialog box, complete the following fields:

Field	Description
Firmware Mode pane	Choose any of the following firmware operating modes: • **Mirror Mode** - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers. • **Util Mode** - In this mode one card with four partitions and one card with a single partition is created. This mode is available only for C220 M4 and C240 M4 servers. • **Not Applicable** - No firmware operating modes are selected. Go to step 5 if you select **Not Applicable**. This mode is available only for C220 M3, C240 M3, C22, C24, and C460 M4 servers.
Partition Name field	The name of the partition.
Non Util Card Partition Name field	The name that you want to assign to the single partition on the second card, if it exists. **Note** This option is available only for util mode.
Select Primary Card (available for mirror mode) or **Select Util Card** (available for Util mode) drop-down list	Select the slots **Slot 1** or **Slot 2** where the SD cards are present or select **None** if only one SD card is present on the server. **Note** **None** is available only for **Select Util Card** option.
Auto Sync check box	Automatically synchronizes the SD card available in the selected slot. **Note** This option is available only for mirror mode.
Slot-1 Read Error Threshold field	The number of read errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

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

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

Field	Description
Virtual Drive Enable drop-down list	The virtual drives that can be made available to the server as a USB-style drive.
RAID Primary Member drop-down list	The slot in which the primary RAID member resides.
RAID Secondary Role drop-down list	The role of the secondary RAID.

Field	Description
I/O Read Error Threshold field	The number of read errors that are permitted while accessing the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
I/O Write Error Threshold field	The number of write errors that are permitted while accessing the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy The number of write errors that are permitted while accessing the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy.
Clear Errors check box	If checked, the read/write errors are cleared when you click **Submit**.

Step 6 Click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.
You can also select an existing FlexFlash policy from the **Hardware Policies** table and delete, edit, clone, apply or view the apply status by selecting the respective options in the user interface.

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

1. The settings on the server will be set to default.
2. The new settings on the policy will be applied. Hence, if there is any failure in this step, you will lose the existing settings prior to applying the policy.

IPMI Over LAN Policy

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

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

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

Procedure

Step 1 Click **Add** in the **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 79.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 71.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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:

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

Step 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 Cisco IMC Supervisor is not deleted from the user list in the policy. If deleted, Cisco IMC Supervisor loses connection to the server being managed.

Virtual KVM Policy

The KVM console is an interface accessible from Cisco IMC Supervisor that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location. You can create one or more KVM policies which contain a specific grouping of virtual KVM properties that match the needs of a server or a set of servers.

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

Perform this procedure when you want to create a Virtual KVM policy.

Procedure

Step 1 Click **Add** in the **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 86.

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 **Hardware Policies** page.
For more information about how to go to this page, see Creating Hardware Policies, on page 69.

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 **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 **Hardware Policies** tab.

Step 3 Expand a policy from the left pane and select a policy in the **Hardware Policies** page. Perform the following optional steps:

a) (Optional) To delete a policy, click **Delete**. In the **Delete Policy** dialog box, click **Select** and select the policies you want to delete. Click **Select** and **Submit**.
You can delete one or more selected policies even if you have associated the policy to a server. If you try to delete a policy which is associated to a profile, an error occurs.

b) (Optional) To modify a policy click **Properties** and modify the required properties.
When you modify a policy name, ensure that you do not specify a name which already exists.

c) (Optional) To clone a policy, click **Clone** to copy the details of a selected policy to a new policy.

d) (Optional) Click **View Details** to view the status of the policy you have applied and the server IP address to which you have applied the policy. If the policy is not successfully applied an error message is displayed in the **Status Message** column.

Step 4 To apply a policy to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Policy, on page 87.

Step 5 Click **Submit** and/or **Close** if applicable.

Hardware Profiles

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

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

1 Create a hardware profile. You can create a profile in one of the following methods:

   a Create a new profile. For more information about creating a new profile, see Creating a Hardware Profile, on page 89.

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 90.

2 Apply the profile on a server. For more information about applying a profile, see Applying a Hardware Profile, on page 91.

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 91.

Creating a Hardware Profile

Perform this procedure to create a hardware profile.

Procedure

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

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

Step 3 Click **Add**.

Step 4 In the **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 69

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 91

Creating a Profile from an Existing Configuration

You can choose to create a profile using a server that you have previously configured. By re-using the existing configuration on a server, you can reduce the time and effort involved in creating similar configurations.

Note When you create a profile from current configuration of a server, the password fields are not retrieved from the server.

Perform the following procedure when you want to create a profile from the current configuration of a server.

Procedure

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

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

Step 3 Select an existing hardware profile and click **Apply**.

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 servers to which the profile is being applied.

General Tasks Under Hardware Profiles

Perform the following procedure when you want to edit, delete, clone, or view server mapping details of an existing profile.

Procedure

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

Step 2 Expand the Hardware Profile in the left pane and select a profile in the **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 can delete a profile even if it is associated to a server.

b) (Optional) To modify a profile, select a profile, click **Edit** and modify the required properties.
When you modify a profile name, ensure that you do not specify a name which already exists.

c) (Optional) To copy the details of an existing profile to a new profile, click **Clone**.

d) (Optional) To apply a profile to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Hardware Profile, on page 91.

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.

Tag Library

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

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

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

Creating a Tag Library

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

Procedure

Step 1 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** pane, complete the following:

Name	Description
Taggable Entities field	Choose the entities on which the tag needs to be applied. To add an entity, do the following: **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**.

Note You can perform various tasks such as cloning, editing, deleting, viewing tag and tag association details by clicking on the available options.

CHAPTER 9

Firmware Profiles

This chapter contains the following topics:

Firmware Management Menu

Firmware images may either be uploaded from a local or a network server. The profile name must be unique across both local and network image profiles

Cisco delivers firmware updates in a single bundle to upgrade all Cisco IMC Supervisor components. Firmware updates can be downloaded from cisco.com. You cannot upgrade if a server is not managed in Cisco IMC Supervisor. For downloading the E-Series firmware images you must associate a contract access to the cisco.com account.

Adding Images to a Local Server

Perform this procedure when you want to add a firmware image from your local machine.

Procedure

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.
Password (cisco.com) field	Enter your Cisco login password.

Field	Description
Enable Proxy Configuration check box	(Optional) Check this check box to enable proxy configuration and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.
Enable Proxy Authentication check box	(Optional) Check this check box to enable proxy authentication and complete the following: • **Proxy User Name** field - Enter a proxy user name for the proxy authentication. • **Proxy Password** field - Enter the password for the proxy user name.
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 view profile configuration details, modify the firmware image details, and delete the image profile. You can also select multiple profiles concurrently and delete them.
- Cisco IMC Supervisor appliance should be able to remotely map to these images.
- You can select an image from the **Images-Local** window and download the image from cisco.com. For firmware profiles that require images to be downloaded, you can defer and initiate the download process later using the **Download Image** option. You can also delete an image downloaded from cisco.com using the **Delete Image** option.

Uploading Images from a Local File System

Perform this procedure to upload iso images from your local file system to the Cisco IMC Supervisor system.

Procedure

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

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

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

Field	Description
Profile Name field	Enter a descriptive and unique profile name.
Platform drop-down list	Select the C-Series or E-Series platform.
File Name field	Choose **Browse** to search and select a file to upload on your local file system.

Step 4 Click **Upload**.

Step 5 Click **OK** in the **File Upload** confirmation box, once the upload is complete.

Step 6 Click **Submit**.

Note
- You can view profile configuration details, modify the firmware image details, and delete the image profile. You can also select multiple profiles concurrently and delete them.
- The **Delete Profile** option removes the image associated with the profile. If you uploaded a wrong image or if a file is no longer associated with a profile, a purge system task which runs periodically (once a month) will delete the files from the Cisco IMC Supervisor appliance.

Adding Images from a Network Server

Perform this procedure to add firmware images from a network server by providing the profile name, remote IP, remote filename and so on.

Procedure

Step 1 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. The profile name must be unique.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server are listed here.
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 Host Upgrade Utility ISO file.
Location Link field (only for HTTP server type)	Enter a valid http/https URL link for the image location.
User Name field	Enter a network path user name.
Password field	Enter a network path password.
Mount Options drop-down list (only for CIFS server type)	Select valid mount options from the **Mount Options** drop-down list. **Note** You can select a mount option for servers that are running Cisco IMC version 2.0(8) and later.

Step 4 Click **Submit**.

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

Note
- You can view profile configuration details, modify the firmware image details, and delete the image profile. You can also select multiple profiles concurrently and delete them.
- Cisco IMC Supervisor appliance should be able to remotely map to these images.

Upgrading Firmware

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.
Server(s) button	Click **Select** and choose the servers from the list. The list displays only those servers whose platform matches the one configured in the selected profile.
Schedule later check box	Check this check box and select an existing schedule to run an upgrade. You can also click on + icon to create a new schedule. For more information on creating schedules, see Creating Schedules, on page 103. You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to verify the scheduled task and its progress. You can also select a scheduled task and click **Remove Scheduled Tasks** to remove the associated scheduled task.

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

Step 7 Click **OK**.

Note You can also view firmware upgrade details and delete the status records for the specified upgrade operation.

CHAPTER 10

Updating Cisco IMC Supervisor

This chapter contains the following topics:

Overview of Updating Cisco IMC Supervisor Patches

Automated patch update notifications is available in Cisco IMC Supervisor. Cisco IMC Supervisor periodically (every 14 days) checks for any new patch updates that are available in cisco.com using the Cisco Automated Software Distribution (ASD) service. If there are any patch updates later than the current release, the Cisco IMC Supervisor update manager will download the patch into a location within Cisco IMC Supervisor. You can then go to the Shell Admin and apply the patch. For more information about applying a patch, see section *Applying a Patch to Cisco IMC Supervisor* in the *Cisco IMC Supervisor Shell Guide*. You can also manually check for availability of any new versions using the **Check for Updates Now** option.

Note You will be notified only for new patch updates for the current release. The Cisco IMC Supervisor based update is not applicable for OVF files.

Configuring Update Settings

For Cisco IMC Supervisor to run periodic checks (once in 14 days) for new patch updates, you must provide your support credentials and other details. These details will be used by Cisco IMC Supervisor to communicate with the Cisco ASD backend service to query for any new updates. Any new versions of the patch will automatically be downloaded into the Cisco IMC Supervisor appliance. You must configure the settings so that you will be notified when there is a new version of Cisco IMC Supervisor. If a higher version is available, the **Diagnostic System Messages** dialog box displays a message that a newer version of Cisco IMC Supervisor is found. Perform this procedure to configure the update settings.

Note If you have not configured the update settings, you will find a notification bubble next to your login name on the top right corner. The **Diagnostic System Messages** dialog box displays a message that settings are not configured.

Procedure

Step 1 From the menu bar, choose **Administration** > **Update IMCS**.
The **IMCS Update Report** displays the current version, available upgrade version, upgrade status, the location where the file is downloaded and so on.

Step 2 Click **Configure Update Settings**.

Step 3 In the **Manage Update Settings** dialog box, complete the following:

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

Step 4 Click **Submit**.

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

Note Ensure that the URL https\cloudsso.cisco.com.null and https://api.cisco.com/ is reachable from the Cisco IMC Supervisor appliance.

CHAPTER 11

Managing Schedules

This chapter contains the following topics:

Overview of Managing Schedules

Defining a schedule allows you to defer certain tasks to occur at a different time. For example, tasks such as firmware updates or server discovery can be scheduled to run at a pre-defined time or at a pre-defined frequency. You could schedule tasks during off-peak hours where the workloads on servers are low.

Creating Schedules

Perform this procedure when you want to create a new schedule.

Procedure

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

Step 2 Click **Add**.

Step 3 In the **Create Schedule** dialog box, complete the following:

Field	Description
Schedule Name field	Enter a name for the schedule task.
Enable Schedule check box	Check this check box to enable a schedule. By enabling or disabling a schedule (using the **Enable** or **Disable** options), you can enable or disable the tasks associated with the schedule from running.
Scheduler Type radio button	Select this radio button to choose a one time or recurring schedule frequency.

Field	Description
Schedule Time field	Select the day from the calendar, hours and minutes from the drop-down lists, and AM or PM radio buttons. **Note** The schedule time is based on the time on the appliance. However, the time zone is of the local client browser.

Step 4 Click **Submit**.

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

What to Do Next

- You can select an existing schedule and modify, delete, or view scheduled tasks. **View Scheduled Tasks** displays a report which allows you to view the status of the upgrade firmware and auto discovery tasks you associated with the schedule while Upgrading Firmware or Performing Auto Discovery.
- You can select one or more tasks associated with the schedule and disassociate them from the schedule using the **Remove Scheduled Tasks** option.

CHAPTER 12

Running Server Diagnostics

This chapter contains the following topics:

Overview of Server Diagnostics

Server diagnostics is available through UCS Server Configuration Utility (UCS-SCU). You can use diagnostics tools to diagnose hardware problems with your Cisco servers and run tests on various server components to find out hardware issues along with analysis of the test results in a tabular format.

You must download, configure, and save the UCS-SCU image to a remote location.

Note Running a diagnostic test using the UCS-SCU image results in the server being temporarily unavailable as the server reboots with the UCS-SCU image.

When you run diagnostics on any rack server, it reboots with the UCS-SCU image hosted on the location you have configured. The diagnostics tabular report displays the status of diagnostics for each server on which you have run diagnostics. Also, details of the server, the date and time the report was generated, diagnostics status and so on are displayed. You can delete or download diagnostic reports for a single or for multiple servers.

Note You must configure the scpuser password to run server diagnostics. To configure the scpuser password, see Configuring a SCP User, on page 27.

Configuring Server Configuration Utility Image Location

Perform this procedure to configure and save the location of the UCS-SCU image.

Procedure

Step 1 From the menu bar, choose **Systems** > **Server Diagnostics**.

Step 2 Click **Configure SCU Image Location**.

Step 3 In the **Configure SCU Image Location** dialog box complete the following:

Field	Description
ISO Share IP field	Enter the ISO share IP address.
ISO Share Path field	Enter the ISO share path.
ISO Share Type drop-down list	Choose either Network File System (NFS), Common Internet File System (CIFS), or World Wide Web (WWW) share types.
Username field	Enter your ISO share login user name.
Password field	Enter your ISO share login password.

Step 4 Click **Save**.

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

Running Diagnostics

Perform this procedure when you want to run diagnostics for servers or server groups.

Procedure

Step 1 From the menu bar, choose **Systems** > **Server Diagnostics**.

Step 2 Click **Run Diagnostics**.

Step 3 In the **Run Diagnostics** dialog box, complete the following:

Field	Description
Choose drop-down list	Choose whether you want to run the diagnostics on a server or server group from the drop-down list.
Server(s) or **Server Group(s)** drop-down list	Choose the server(s) or server group(s) for which you want to run the diagnostics.

Step 4 Click **Select** and select the server(s) or server group(s) from the **Select** dialog-box.

Step 5 Click **Select**.

The selected server(s) or server group(s) are displayed next to the **Server(s)** or **Server Group(s)** field.

Step 6 Click **Submit**.

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

Note You can perform the following actions on a server or multiple servers:

- Select a server and click **View Report** to view reports.
- Select a server or multiple servers and click **Delete Report** to delete reports.
- Select a server or multiple servers and click **Download Report** to download reports. When you select multiple servers to download diagnostics reports, a zip file containing all the reports are downloaded.
- You cannot choose a server which is already running a diagnostics operation. Wait for the diagnostics operation to complete before triggering another diagnostics on this server.
- Diagnostics may take around 40 minutes to complete. This varies depending on the number of components present in the server.

CHAPTER 13

Smart Call Home for Cisco IMC Supervisor

This chapter contains the following topics:

Overview of Smart Call Home

Cisco Smart Call Home is an automated support capability that provides continuous monitoring, proactive diagnostics, alerts, and remediation recommendations on select Cisco devices. Smart Call Home can help identify and resolve issues quickly to achieve higher availability and increased operational efficiency. This capability is available with an active support contract for hardware managed by Cisco IMC Supervisor. When enabled, Smart Call Home looks for a specific set of faults that Cisco has identified through interaction with Cisco Technical Assistance Center (TAC) engineers, the Cisco support community, and developers. Instead of waiting for a user to notice a problem or a fault to escalate and be reported, Smart Call Home proactively identifies and diagnoses faults.

Cisco IMC Supervisor managed server tasks such as **Group Rack Server Inventory**, **Rack Server Fault**, and **Health System** are run at periodic intervals and send relevant information to the Smart Call Home backend. The backend processes this data and if issues are identified, it will automatically raise cases with the TAC for resolution of issues.

You can configure Smart Call Home using the Cisco IMC Supervisor user interface. For more information, see Configuring Smart Call Home, on page 109.

Configuring Smart Call Home

Perform this procedure to configure Smart Call Home.

Procedure

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

Step 2 Check the **Enable Smart Call Home** check box so that collected faults are forwarded to the Smart Call Home backend.

Note By default Smart Call Home is disabled.

Step 3 Enter **Contact Email** address.

Note You can enter only one contact email at a time in this field.

Step 4 The **Destination URL** of the Smart Call Home backend is set by default.

Note We recommend that you must not change the default URL.

Step 5 (Optional) Check the **Enable Proxy** check box and complete the following:

a) **Protocol** drop-down list - Choose https or http from the list.

b) **Host Name or IP Address** field - Enter a host name or IP address of the proxy server.

c) **Port** field - Enter the port for the proxy configuration.

Step 6 (Optional) Check the **Send Group Inventory Now** check box to send inventory details of the servers. One inventory message per managed server is sent to the Smart Call Home backend. This can be used as additional information for resolving issues by the TAC team.

Step 7 Click **Save**.

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

Note
- Any faults that occur on the managed servers are sent to the backend. For information about the various fault codes and its severity, see Fault Codes, on page 110. For more information about logging in to Smart Call Home and performing various tasks, see https://supportforums.cisco.com/community/4816/smart-call-home and for viewing messages received at the Smart Call Home backend see http://tools.cisco.com/sch/.
- Ensure that the URL https://tools.cisco.com/its/service/oddce/services/DDCEService is reachable from the Cisco IMC Supervisor appliance .

Fault Codes

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

Fault Code	Fault Name	Message	Severity
F0868	fltComputeBoardPowerFail	Motherboard of [serverid] power: [power]	critical
F0424	fltComputeBoardCmosVoltageThresholdCritical	CMOS battery voltage on [serverid] is [cmosVoltage]	major

Fault Code	Fault Name	Message	Severity
F0425	fltComputeBoardCmosVoltageThresholdNonRecoverable	CMOS battery voltage on [serverid] is [cmosVoltage]	critical
F0177	fltProcessorUnitThermalThresholdNonRecoverable	Processor [id] on [serverid] temperature:[thermal]	critical
F0379	fltEquipmentIOCardThermalProblem	IOCard [location] on server [id] operState: [operState]	major
F1004	fltStorageControllerInoperable	Storage Controller [id] operability: [operability]	critical
F0181	fltStorageLocalDiskInoperable	Local disk [id] on [serverid] operability: [operability]	major| warning
F1007	fltStorageVirtualDriveInoperable	Virtual drive [id] on [serverid] operability: [operability]	critical
F0531	fltStorageRaidBatteryInoperable	RAID Battery on [serverid] operability: [operability]	major
F0997	fltStorageRaidBatteryDegraded	Raid battery [id] on [serverid] operability: [operability]	major
F0185	fltMemoryUnitInoperable	DIMM [location] on [serverid] operability: [operability]	major
F0188	fltMemoryUnitThermalThresholdNonRecoverable	DIMM [location] on [serverid] temperature: [thermal]	critical
F0385	fltEquipmentPsuThermalThresholdNonRecoverable	Power supply [id] in [serverid] temperature: [thermal]	critical
F0389	fltEquipmentPsuVoltageThresholdCritical	Power supply [id] in [serverid] voltage: [voltage]	major

Fault Code	Fault Name	Message	Severity
F0391	fltEquipmentPsuVoltageThresholdNonRecoverable	Power supply [id] in [serverid] voltage: [voltage]	critical
F0407	fltEquipmentPsuIdentity	Power supply [id] on [serverid] has a malformed FRU	critical
F0411	fltEquipmentChassisThermalThresholdNonRecoverable	Thermal condition on [serverid] cause: [thermalStateQualifier]	critical
F0174	fltProcessorUnitInoperable	Processor [id] on [serverId] operability: [operability]	critical|major

CHAPTER 14

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 14
How to upgrade license	Updating the License, on page 15
How to add login users in Cisco IMC Supervisor	Creating a User, on page 32
How to add a rack group	Adding a Rack Group, on page 41
How to create a rack account	Adding a Rack Account, on page 42

Miscellaneous Procedures

The following sections include miscellaneous procedures that you would perform using Cisco IMC Supervisor.

Enabling Dashboard View

Perform this procedure to enable the dashboard view in the Cisco IMC Supervisor menu bar.

Procedure

Step 1 Click the username with which you logged in to the application. The username is on the far right of the application header.

Step 2 In the **User Information** window, click **Dashboard**.

Step 3 Check the **Enable Dashboard (in the top level menu)** check box to enable the dashboard.

Step 4 Click **Apply** and close the window.

Note You can see the **Dashboard** tab in the menu bar.

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**.