Cisco UCS Director Management Guide for Rack Servers, Release 6.7

First Published: 2019-01-09

Last Modified: 2020-06-18

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

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

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

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

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

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

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

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

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

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

© 2019–2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface contains the following sections:

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director 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`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
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

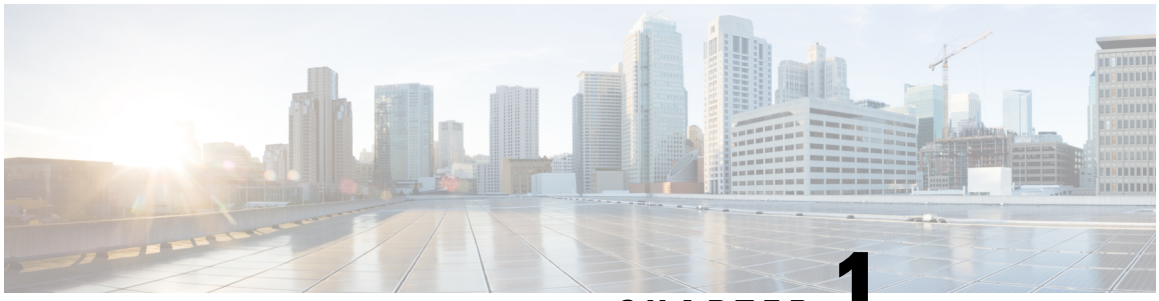
Documentation Feedback

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

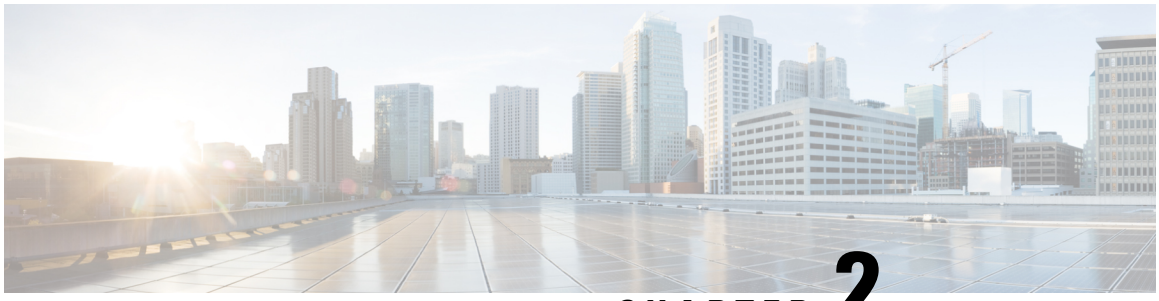
The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New and Changed Features in Release 6.7.4.1

Feature	Description	Where Documented
Introduction of SFTP User Configuration	With this release, you must configure a password for an SFTP user in Cisco UCS Director. This user configuration is used in server diagnostics and tech support processes to transfer files to Cisco UCS Director using SFTP. This SFTP user configuration replaces the previously available SCP user configuration functionality. After installing or upgrading to this release, you must configure the password for the SFTP user. If you upgrade to version 6.7.4.1 of the Cisco UCS Director Base Platform Connector Pack, then you must also upgrade to version 6.7.4.1 of the Cisco UCS Director IMC Connector Pack to use the Server Diagnostics and Tech Support features with the SFTP user configuration.	The procedure to configure the password for an SCP user has been removed from this guide. It has been replaced with a procedure to configure the password for an SFTP user. Configuring SFTP User Password, on page 113

Table 2: New and Changed Features in Release 6.7

Feature	Description	Where Documented
Support for upgrading firmware from MicroSD cards or FlexFlash cards	Starting with this release, you can upgrade firmware on rack servers using ISO images from MicroSD cards (for M5 servers) or FlexFlash cards (for M4 servers). MicroSD card is not supported on Cisco UCS S3260 servers. This feature is only supported on Cisco UCS M5 or higher servers running Cisco IMC version 3.1(3a) or higher and on Cisco UCS M4 servers running Cisco IMC version 4.0(2) or higher.	Firmware Upgrades From SD Cards, on page 103 Downloading Firmware Image to an SD Card, on page 103 Running Firmware Upgrade from an SD Card, on page 104
Support for scheduling the **Apply Profile** process, and **Run Upgrade** process for a Host Image Profile.	Starting with this release, new scheduling options have been introduced in the **Run Upgrade** and **Apply Profile** screens for host image profile procedures. Using these options, you can schedule these processes to run at a later point in time.	Running a Host Image Upgrade Manually, on page 88 Applying a Host Image Profile, on page 87
Enhancements to email alert on faults	Starting with this release, you can configure the system to send email alerts for all open faults, based on the configured email alert rule, irrespective of whether you have been notified previously for a fault or not. A new option **Send alert for all faults every 24 hours** has been introduced in the **Add Email Alert Rule** screen. If you select this option, the system will send out email alerts every 24 hours for all open faults that match the specified alert rule.	Configuring Email Alert Rules, on page 110
Introduction of the Power Restore policy for Cisco UCS C-series servers.	Starting with this release, you can configure a power restore policy for Cisco UCS C-series servers.	Power Restore Policy, on page 60



CHAPTER 2

Overview

About Standalone Rack-Mount Server Management Through Cisco UCS Director

Cisco UCS Director is not a replacement for the management of rack servers (Cisco UCS C-Series Rack-Mount Servers and Cisco UCS E-series servers) through Cisco Integrated Management Controller (Cisco IMC). Rather, Cisco UCS Director enables you to orchestrate and automate some of the steps required to configure and maintain a rack-mount server. In this way, Cisco UCS Director provides a statistical analysis of data and a converged view of each pod.

You must add these rack servers as a Rack account to Cisco UCS Director, after which Cisco UCS Director provides you with complete visibility into the rack server configuration. In addition, you can use Cisco UCS Director to manage and configure the rack-mount server.

Important Support for rack server management through the legacy Cisco Rack Server (CIMC) accounts is not available from release version 5.4 onwards. After you upgrade to Cisco UCS Director Release 5.4, the connection status of account type Cisco Rack Server (CIMC) from the **Physical Accounts** tab is displayed as Failed. You must create new accounts from the **Rack Accounts** tab for the CIMC servers, and manually delete the accounts displayed from the **Physical Accounts** tab.

You can only manage rack servers that are running Cisco Integrated Management Controller (Cisco IMC) version 1.5 and higher on C-series servers, and version 2.3.1 and higher on E-series servers. For information on how to add and manage rack servers in Cisco UCS Director, see Adding a Rack Group, on page 5 and Discovering and Importing Rack Servers, on page 9.

Cisco IMC Tasks You Can Perform in Cisco UCS Director

You can use Cisco UCS Director to perform Cisco IMC management, monitoring, and reporting tasks for physical and virtual devices on a rack-mount server.

Configuration and Administration

You can create, configure, and administer the following hardware and software components for standalone rack-mount servers in Cisco UCS Director:

- Rack server profiles
- Network and storage adapters

You can also perform firmware upgrades of these components.

Monitoring and Reporting

You can also use Cisco UCS Director to monitor and report on standalone rack-mount servers and their components including:

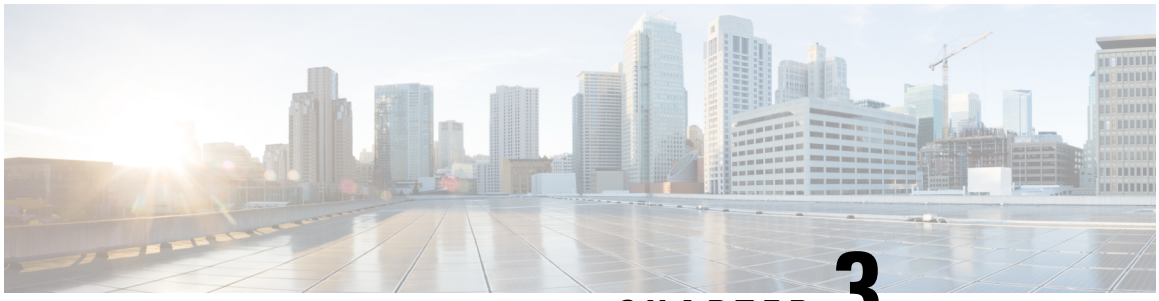
- Power consumption
- Temperature
- Rack server profile association

Cisco IMC Tasks You Cannot Perform in Cisco UCS Director

You cannot use Cisco UCS Director to perform certain Cisco IMC system management tasks on a rack-mount server, such as the following:

- Virtual machine management

Some server management tasks that you cannot perform in Cisco UCS Director can be automated through orchestration workflows, such as associating a VIC policy, RAID policy or a boot policy.



CHAPTER 3

Configuring Rack Accounts and Rack Groups

This chapter contains the following topics:

Adding a Rack Group

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

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Groups**.

Step 3 Click **Add**.

Step 4 In the **Add Rack Group** screen, complete the required fields, including the following:

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

Step 5 Click **Create**.

What to do next

Add one or more rack accounts to this rack group.

Adding a Rack Account

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

Procedure

Step 1 On the menu bar, choose **Administration** > **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	IP address of the rack mount server.
Description field	(Optional) A description of the rack group.
Use Credential Policy check box	**Note** If you have logged in Cisco UCS Director for the first time, then do not check this checkbox. If you have already created credential policies, then check this check box to select a policy from the drop-down list.
Credential Policy drop-down list	Choose a policy from the drop-down list. This field is visible when you check the **Use Credential Policy** check box.
User Name field	Log in ID for the rack mount server.
Password field	Password for the log in ID for the rack mount server.
Protocol drop-down list	Choose HTTPS or HTTP from the list.
Port field	The port number associated with the selected protocol.
Rack Group drop-down list	Choose a rack group within which you want this rack account created.
Contact field	(Optional) The contact email address for the account.
Location field	(Optional) The location of the account.

Step 5 Click **Submit**.

Testing the Connection to a Rack Account

You can test the connection at any time after you add an account.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Accounts**.

Step 3 In the table, select the row of the account for which you want to test the connection.

Step 4 Click **Test Connection**.

Step 5 In the **Test Connection** screen, click **Submit**.

The **Physical Accounts** page will display the results of the test in the **Connection Status** and **Connection Message** columns.

What to do next

If the connection fails, verify the configuration of the account, including the username and password. If the username and password are correct, determine whether there is a network connectivity problem.

Assigning Rack Groups to a Pod

You can assign a rack group to a pod for easy management.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Groups**.

Step 3 In the table, select the row of the account for which you want to assign to a pod.

Step 4 Click **Assign Pod**.

Step 5 In the **Assign Pod** screen, choose a pod from the drop-down list.

Step 6 Click **Submit**.

What to do next

You can manage the rack group through the pod.

Running a Rack Account Inventory Process

When the rack account is added to a rack group, the inventory process is automatically initiated. If you want to review the changes in configuration that occurred in the rack account at a later point in time, you can use the **Inventory** option.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Accounts**.

Step 3 In the table, click the row of the account for which you want to run the inventory.

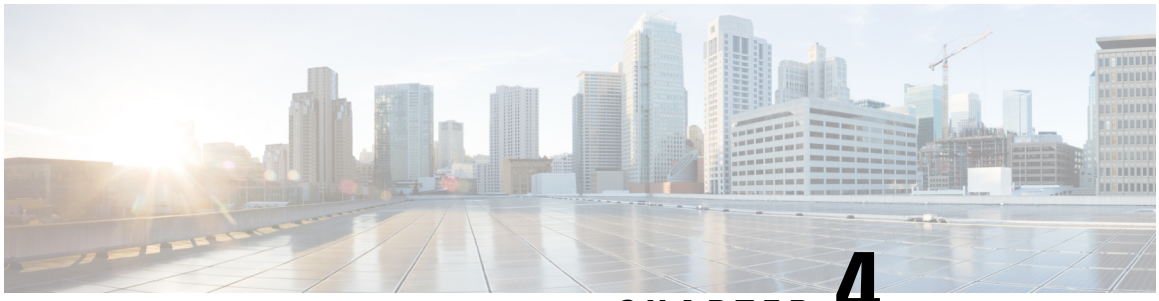
Step 4 Click **Inventory**.

Step 5 In the **Collect Inventory for Account(s)** screen, complete the required field, including the following:

Name	Description
Choose drop-down list	Choose if you want to run an inventory process on a rack group or a rack account.
Rack Group list	Expand the list to check the check boxes of the rack groups that you want to run an inventory collection process for. **Note** This field is visible only when you select **Rack Group** in the drop-down list.
Rack Account list	Expand the list to check the check boxes of the rack accounts that you want to run an inventory collection process for. **Note** This field is visible only when you select **Rack Account** in the drop-down list.

Step 6 Click **Submit**.

The **Physical Accounts** page will display the results of the inventory collection in the **Last Inventory Updated** and **Inventory Message** columns.



CHAPTER 4

Managing Rack Server Discovery

This chapter discusses the following topics:

Discovering and Importing Rack Servers

To discover rack servers in Cisco UCS Director, you can specify configuration criteria and save it as a rack server discovery profile. Using this profile, you can discover multiple rack servers simultaneously and import them into Cisco UCS Director.

With a discovery profile, you can choose to discover rack servers with one of the following options:

- IP address range—Discovers all rack servers with IP addresses within the specified range.
- Subnet range—Discovers all rack servers within the specified subnet range.
- IP Address CSV file—Discovers rack servers with IP addresses that match those specified in the uploaded CSV file.
- Specific IP addresses—Discovers rack servers with IP addresses that match the IP addresses you specify.

Perform this procedure when you want to discover and import rack servers.

Procedure

	Command or Action	Purpose
Step 1	Configure a rack server discovery profile.	Refer Configuring a Rack Discovery Profile, on page 10.
Step 2	Discover servers using the profile.	Refer Performing Auto Discovery, on page 12.

	Command or Action	Purpose
Step 3	Import the servers.	Refer Importing One or More Rack Servers, on page 12.
Step 4	(Optional) Delete a discovery profile.	Refer Deleting Auto Discovery Profile, on page 14.
Step 5	(Optional) Clear a server from the auto discovered list.	Refer Clearing Auto Discovery List, on page 14.

Configuring a Rack Discovery Profile

You can configure a rack discovery profile using which the system can automatically discover rack mount servers. Perform this procedure when you want to add a rack discovery profile.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Server Discovery Profiles**.

Step 3 Click **Add**.

Step 4 In the **Add Discovery Profile** screen, complete the required fields, including 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.
If you select **IP Address Range**	
Starting IP field	Valid IP address
Ending IP field	Valid IP address
If you select **Subnet Mask Range**	
Network Address field	Valid IP address
Subnet Mask drop-down list	Select a value from the drop-down list. This drop-down list shows the available subnets in the network.
If you select **IP Address CSV File**	
Select a file for upload field	Click **Select a File** and navigate to a .csv file which contains the IP addresses.
Sample CSV File field	Click **File Template** to download a sample CSV file.
If you select **IP Address List**	

Field	Description
IP Addresses field	Enter multiple IP addresses separated by comma.
Use Credential Policy check box	If you have already created credential policies, then check this box to select the policy from the drop-down list.
If you check **Use Credential Policy** check box	
Credential Policy drop-down list	Choose a policy from the drop-down list or click the + icon to create a new policy.
Description field	Enter a description for the server.
Contact field	Enter the contact details of the server administrator.
Location field	Enter the geographic location of the server.
Rack Group drop-down list	Choose a rack group or create a new rack group.
If you uncheck **Use Credential Policy** check box	
User Name field	The login name.
Password field	The login password
Protocol drop-down list	Choose https or http from the list.
Port field	Enter a port number.

Note If you choose **IP Address CSV File**, you can specify additional fields such as IP, description, location, contact, rack group and tags in the CSV file in the following format:

- **<ip>**
- (optional) **<description>**
- (optional) **<location>**
- (optional) **<contact>**
- (optional) **<rack group>**
- (optional) **<tag name:tag value>;<tag name:tag value>**

You can specify either an existing value or a new value for the Rack Group field and the Tags field. Specifying a value for these fields is optional. If you do not specify a value for the Rack Group field in the CSV file, then the Default Group is used.

When you upgrade to the current Cisco UCS Director version, replace the existing CSV file with the CSV file you have created in the new format using the **Select a File** option.

The tag type will only be of type **STRING**.

Step 5 Click **Submit**.

What to do next

Click **Discover** to select a profile, and discover devices that match the profile.

Performing Auto Discovery

Perform this procedure when you want to perform auto discovery.

Before you begin

You should configure a profile based on which Cisco UCS Director can discover the rack servers.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Server Discovered Devices**.

Step 3 Click **Discover**.

Step 4 In the **Discover Devices** screen, expand the **Select Profile** list and check the check boxes of the profiles.

Step 5 (Optional) You can choose to schedule this task to run at a later point in time by checking the **Schedule Later** check box.

If you check this check box, then you can either select a schedule that you previously created or create a new schedule. For information on creating a new schedule, see Creating Schedules, on page 31.

Step 6 Click **Submit**.

Importing One or More Rack Servers

Perform this procedure when you want to import one or more rack servers that were discovered using the discovery profile.

Important You cannot perform multiple account-related tasks, such as adding, modifying or importing accounts, simultaneously in Cisco UCS Director. We recommend that you wait for one task to complete, before initiating another task. For example, while importing discovered devices into a rack group, we recommend that you let you this task complete before you edit any other rack groups or rack accounts.

Before you begin

- You should configure a profile based on which Cisco UCS Director can discover the devices.
- You have already discovered rack servers using the discovery profile.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Server Discovered Devices**.

Step 3 Click **Import**.

Step 4 In the **Import Discovered Devices** screen, complete the required fields, including the following:

Field	Description
Select Device(s) list	Expand the list of devices that have been discovered. Check the check boxes of all the servers you want to import.
User Prefix field	Enter a prefix for the user.

Step 5 Click **Submit**.

Setting Properties for Discovered Devices

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

Before you begin

You should have configured a discovery profile based on which devices can be discovered.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Rack Server Discovered Devices**.

Step 3 Select a device and choose **Set Properties**.

Step 4 In the **Set Properties** screen, complete the required fields, including the following:

Field	Description
Description field	Enter a description of the server.
Contact field	Enter the contact number of a person who can attend to the issues on the server.
Location field	Enter the address of the server.
Select Rack Group drop-down list	Choose a rack group from the list or create a new rack group.

Step 5 Click **Submit**.

Clearing Auto Discovery List

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

Before you begin

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

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Rack Server Discovered Devices**.
Step 3 Click **Clear**.
Step 4 In the **Clear Devices** screen, click **Delete**.

Deleting Auto Discovery Profile

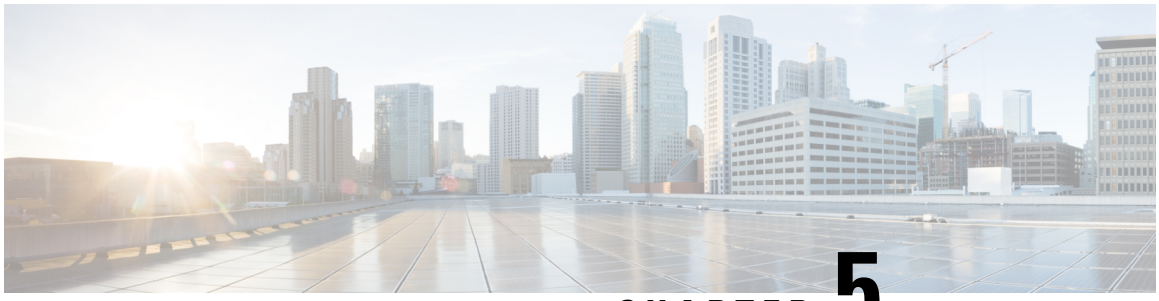
Perform this procedure when you want to delete an automatic discovery profile.

Before you begin

You should configure a profile based on which Cisco UCS Director can discover the devices.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Rack Server Discovery Profiles**.
Step 3 Select a profile from the table, and click **Delete**.
Step 4 In the **Delete Discovery Profile** screen, click **Submit**.



CHAPTER 5

Managing Rack Servers

This chapter discusses the following topics:

Viewing Rack Server Details

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

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Rack Servers**.

Step 4 Select a server from the list.

Step 5 From the **More Actions** drop-down list, choose **View Details** or double-click the sever from the list.

Note The **More Actions** drop-down list is visible only after you select a server from the list.

The following details are available for a rack mount server:

Tab	Description
Summary	Displays an overview of the rack server.
CPUs	Displays the details of the CPUs in the server.
Memory	Displays details of the memory cards used in the server.
PSUs	Displays details of the power supply units in the server.
PCI Adapters	Displays details of the PCI adapters in the server.
VIC Adapters	Displays details of the VIC adapters in the server.
Network Adapters	Displays details of the network adapters in the server.
Storage Adapters	Displays details of the storage adapters in the server.
FlexFlash Adapters	Displays details of the Cisco FlexFlash adapters in the server.
Communication	Displays all the communication protocols that are configured in the server.
Remote Presence	Displays information on vKVM, vMedia and Serial over LAN (SOL) for the server.
Faults	Displays the details of the faults logged in the server. • Severity • DN • Description • Code - Error code for the fault. • Created - Date and time the fault was logged. • Cause - Reason for the fault.
Hardware Compatibility Report	Displays the status against the current software version or a target software version.
Users	Displays the list of users for the server.
Cisco IMC Log	Displays the details of the Cisco IMC logs for the server. You can also clear the Cisco IMC logs.
System Event Log	Displays the details of the server logs.

Tab	Description
TPM	Displays information on the TPM inventory.
BIOS	Displays BIOS-related information of the server.
Fault History	Displays historical information on the faults that occurred on the server.
Tech Support	Provides an option to upload tech-support log files to a remote server or to a local server.
Host Images	Details of an image such as name, size, MD5 checksum, last modified time, and if the image is mapped are displayed. You can select an image and click Map Image,Unmap Image, and Delete Image to perform the various actions. **Note** Host image mapping is applicable only for E-series servers.
Associated Hardware Profiles	Displays the server profiles that are associated with the server.

Viewing Fault Details of a Rack Server

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

Before you begin

The server is added as a rack account within a rack group.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Faults**.

Step 4 Select a server from the list.

Step 5 Choose **View Details**.

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 6 Click **Close** to return to the previous screen.

Setting a Label for a Rack Server

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

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Servers**.
Step 4 Select the server from the list.
Step 5 From the **More Actions** drop-down list, choose **Set Label**.
Step 6 Enter a new label.
Step 7 Click **Submit**.

Managing Tags for a Rack-Mount Server

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

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Servers**.
Step 4 Select a server from the list
Step 5 From the **More Actions** drop-down list, choose **Manage Tags**.
Step 6 In the **Manage Tags** screen, click **+** to add an entry to the **Manage Tags** table.
Step 7 In the **Add Entry to Tag** screen, complete the required fields, including the following:

Field	Description
Tag Name	Select the tag name from the drop-down list and click **Submit** or create a new tag. **a.** Click the + icon. **b.** In the **Create Tag** window, do the following: **1.** In the **Name** field, enter a descriptive name for the tag. **2.** In the **Description** field, enter a description of the tag. **3.** In the **Type** field, select String or Integer from the drop-down list. **4.** In the **Possible Tag Values** field, enter a possible value for the tag. **5.** Click **Next**. **6.** Click the + icon to add a new category. **c.** In the **Add Entry to Entities** window, from the **Category** drop-down list, choose the category. It can be one of the following: • **Physical_Compute** category creates tag entities for a Rack Server. • **Administration** category creates tag entities for users. **Note** You can also add tags for a chassis. For more information about adding tags for a chassis, see Tagging Assets for a Cisco UCS S3260 Server, on page 34. **d.** Check the **Rack Servers** or **Chassis** check box. **e.** Click **Submit**. **Note** The tags are displayed under the respective category according to the set taggable entities. **f.** In the confirmation dialog box, click **OK**.
Tag Value	Select the tag value from the drop-down list.

Step 8 Click **Submit**.

Step 9 Select a tag in the **Manage Tags** screen and click Edit to edit a tag.

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

Step 11 Click **Submit**.

Adding Tags for a Rack-Mount Server

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

Before you begin

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

Note You can also select multiple rack servers.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Rack Servers**.

Step 4 Select a server from the list

Step 5 Click **Add Tags**.

Note The **Add Tags** option is visible only after you select a server from the list.

Step 6 In the **Add Tags** screen, complete the required fields, including the following:

Name	Description
Tag Name drop-down list	Choose a name from the drop-down list or you can create a new tag. Click the plus icon to create a new tag. See Managing Tags for a Rack-Mount Server, on page 18 to create tags.
Tag Value drop-down list	Choose a tag value from the drop-down list.

Step 7 Click **Submit**.

Setting Locator LED for a Rack Server

Perform this procedure when you want to set locator LED for a rack server.

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Servers**.
Step 4 Select a sever from the list.
Step 5 Click **Locator LED**.

Note The **Locator LED** option is visible only after you select a server from the list.

Step 6 From the **Turn the Locater LED for selected servers on/off** drop-down list, choose **ON** or **OFF**.
Step 7 Click **Submit**.

Performing a Power Cycle on a Rack Server

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

Before you begin

The server is added as a rack account within a rack group.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Server**.
Step 4 Choose the server that you want to perform a power cycle.

You can select multiple servers.

Step 5 Click **Power Cycle**.
Step 6 In the **Server Power Cycle** page, click **Submit**.

Powering On a Rack Server

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Server**.
Step 4 Choose the server that you want to power on.
Step 5 Click **Power ON**.
Step 6 Click **Submit**.

Powering Off a Rack Server

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Server**.
Step 4 Choose the server that you want to power off.
Step 5 Click **Power OFF**.
Step 6 Click **Submit**.

Performing a Hard Reset on a Rack Server

Perform this procedure when you want to hard reset a rack server.

Before you begin

The server is already added as an account within a rack group.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Servers**.
Step 4 Select a sever from the list.

Step 5 Click **Hard Reset**.

Rebooting a Server

Perform this procedure when you want to reboot the BMC on a rack server.

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Server**.
Step 4 Choose the server that you want to reboot.
Step 5 Click **Reboot**.
Step 6 On the **Server Reboot BMC** page, click **Submit**.

Shutting Down a Rack Server

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

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Servers**.
Step 4 Select the sever from the list.
Step 5 Click **Shut Down**.
Step 6 In the confirmation dialog box, click **OK**.

Tagging Assets for a Rack Server

An asset tag is a user-defined label for a rack server. Using the **Asset Tag** option you can set a user-defined label for a rack server or for a chassis. For information on adding an asset tag to a chassis, see Tagging Assets for a Cisco UCS S3260 Server, on page 34.

Important Asset tagging is supported on C-series and S-series servers that are running firmware versions of 3.0(1c) and above. For E-series and ENCS servers, asset tagging is supported on servers running firmware versions 3.2.1 and above.

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Server**.
Step 4 Choose the server that you want to set a tag to.
Step 5 From the **More Actions** drop-down list, choose **Asset Tag**.
Step 6 In the **Set Asset Tag** page, enter the name of the asset tag in the **Asset Tag** field.
Step 7 Click **Submit**.

Launching the KVM Console for a Rack Server

Before you begin

You must have Java Run-Time Environment (JRE) installed on your system.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the account under **Pods**.
Step 3 Click **Rack Server**.
Step 4 Choose the server for which you want to start the KVM console.
Step 5 From the **More Actions** drop-down list, click **KVM Console**.
Step 6 In the **Launch KVM Console** screen, click **Submit**.

Step 7 If the Cisco IMC version installed on the server is prior to version 4.1(1c), then a `kvm.jnlp` file is downloaded to your system. Double-click the `kvm.jnlp` file in your Downloads folder.

The KVM Console opens in a separate window.

Step 8 If the Cisco IMC version installed on the server is version 4.1(1c) and above, then clicking **Submit** in the **Launch KVM Console** screen displays a new tab with a link. Click this link to enter the KVM console credentials and login.

For more information about using the KVM Console, see the Cisco UCS C-Series Servers Integrated Management Controller Configuration Guides.

Launching the Cisco IMC GUI for a Rack Server

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

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Rack Servers**.

Step 4 Select the sever from the list.

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

Step 6 In the **Launch GUI** screen, click **Submit**.

The GUI for the server is launched in a separate browser.

Assign User Groups to a Rack Server

Perform this procedure when you want to assign a user group to the rack server.

Before you begin

The server is added as a rack account within a rack group.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Rack Server**.

Step 4 Choose the server that you want to assign a user group to.

Step 5 From the **More Actions** drop-down list, choose **Assign Group**.

Step 6 In the **Assign User Group - Rack Server** screen, complete the required fields, including the following:

Field	Description
Assign to Users check box	Check this check box to allow resource assignment to users.
User list	Expand this list, and check the names of the users. **Note** This field is displayed only if you have checked the **Assign to Users** check box.
Group list	Expand this list to check the names of the groups. **Note** This field is displayed only if you have not checked the **Assign to Users** check box.
Label field	Enter any comments, if required.

Step 7 Click **Submit**.

What to do next

At a later point in time, if you want to remove this user group from the rack server, you can return to this page, select the server, and choose **Unassign Group**.

Viewing Smart Information for Solid State Drives

Before you begin

The server is added as a Rack Account under a Rack Groups.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Rack Servers**.

Step 4 Select the sever from the list that contains the solid state drive (SSD).

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

Step 6 Double-click the solid state drive, and choose **Controller Info**.

The following settings are available:

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

Step 7 Double-click the solid state drive, and choose **Physical Drives**.

Step 8 Double-click a physical drive, and choose **View Smart Information**.

The following information is displayed:

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

Step 9 Click **Close**.

On the **Storage Adapter** page, choose **Controller Info** to view the controller settings such as **Percentage Life Left**, **Enable Copy back on SMART**, and **Enable Copy back to SSD on SMART Error**.

What to do next

Controller Drive Security

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

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

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

Viewing Controller Drive Security Information

Controller Driver Security information is displayed in the following tabs for a rack server:

- **Controller Info**
- **Physical Drives**
- **Virtual Drives**

Before you begin

The M4 rack-mount server or the Cisco UCS S3260 storage server must have Self Encrypting Drives (SED) connected in it.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Rack Servers**.

Step 4 Select a sever from the list.

Step 5 From the **More Actions** drop-down list, choose **View Details**.

Step 6 On the **Rack Server** page, choose **Storage Adapters**.

Step 7 Select the adapter from the list and choose **View Details**.

Step 8 On the **Storage Adapters** page, choose **Controller Info**.

The following details are available for a SSD drive:

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

Step 9 On the **Storage Adapter** page, choose **Physical Drives**.

Details such as the controller name, physical drive number, status, health, serial number, firmware, FDE capable, FDE enabled, Secured, Locked, Foreign Locked and so on are displayed.

Step 10 On the **Storage Adapter** page, choose **Virtual Drives**.

Details such as the virtual drive number, name, status, health, size, RAID level, Boot drive, FDE capable, FDE enabled and so on are displayed.

Step 11 Click the rack server name on the top right corner of the page to return to the page listing the rack servers.

Managing System Tasks for Rack Servers

System tasks are available for single node and multi node systems. For more information about how to manage system tasks, including the system task policy, see the Cisco UCS Director Administration Guide.

Procedure

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

Step 2 On the **System** page, click **System Tasks**.

Step 3 To access the system tasks you can use for rack servers, expand the following folders:

- **Rack Server Tasks**—System tasks that are specific to rack servers, such as monitoring and inventory tasks.
- **General**—System tasks that are available for all implementations, such as data purge, data aggregation, and deleted account clean-up tasks.

Step 4 After you choose a rack server task in the table, you can perform one or more of the following actions:

Name	Description
Manage Task	In the **Manage Task** screen, complete the required fields, including the following: **a.** From the **Task Execution** drop-down list, choose **Enable** or **Disable**. **b.** From the **System Task Policy** drop-down list, choose **default-system-task-policy** or **local-run-policy**. **c.** To set the frequency at which the task needs to be executed, choose the number of hours from the **Hours** drop-down list and number of minutes from the **Minutes** drop-down list. **d.** Click .

Step 5 Click **Submit**.

Managing Schedules for Rack Servers

Overview of Managing Schedules

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

Creating Schedules

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Schedules**.

Step 3 Click **Add**.

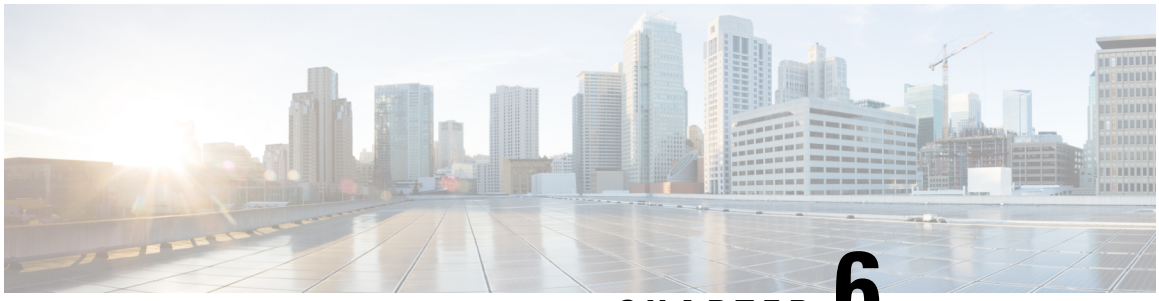
Step 4 In the **Create Schedule** screen, complete the required fields, including the following:

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 drop-down list	Select a one time schedule or recurring schedule frequency. If you choose a **One Time** schedule, select the date, time, and AM or PM radio buttons. **Note** The schedule time is based on the time on the appliance. However, the time zone is of the local client browser. If you choose a **Recurring** schedule, select the days (0 to 30 days), hours and minutes from the drop-down lists.
Schedule Time field	Specify a date using the calendar, and specify a time using the drop-down list. This field is visible only if you selected **One Time** option in the **Scheduler Type** drop-down list.
Days drop-down list	Select the number of days on which this task must be scheduled for.
Hours drop-down list	Select the number of hours.
Minutes drop-down list	Select the number of minutes.

Step 5 Click **Submit**.

What to do next

- You can select an existing schedule and modify, delete, or view scheduled tasks. **View Scheduled Tasks** displays a report which allows you to view the status of the upgrade firmware, auto discovery, apply policy and profile tasks you associated with the schedule while Upgrading the Firmware Image, 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 6

Managing Cisco UCS S3260 Servers

About Cisco UCS S3260 Dense Storage Rack Server

The Cisco UCS S3260 is a dense storage rack server that supports dual server nodes. It can also have one optimized for large datasets used in environments such as Big data, cloud, object storage, and content delivery. It belongs to the Cisco UCS C-Series rack-mount servers product family.

The Cisco UCS S3260 Dense Storage Rack Server is designed to operate in a standalone environment and as part of the Cisco Unified Computing System with Cisco UCS Director integration. The Cisco UCS S3260 Dense Storage Rack Server includes the following features:

- Enterprise-class redundancy with full featured Redundant Array of Independent Disks (RAID) plus Just a Bunch of Disks (JBOD)
- Standalone management interface (Cisco Integrated Management Controller)
- No data migration required when replacing or upgrading server nodes
- No need for extended depth racks

For more information about Cisco UCS S3260 dense storage rack server, see Cisco UCS S3260 Rack Server.

Cisco UCS S3260 Server Management in Cisco UCS Director

Managing Cisco UCS S3260 servers using Cisco UCS Director is largely the same as managing other rack-mount servers. Several of the features and tasks that are supported on other c-series servers are applicable to UCS S3260 servers as well. However, there are a few minor differences while performing these tasks. These include:

- While adding a rack account, you can specify a virtual management IP address and not a Chassis Management Controller (CMC) IP address. If you specify a CMC IP address, an error message appears. For more information, see Adding a Rack Account, on page 6.

  After the inventory collection task, you can view the servers managed by the Cisco UCS S3260 Rack Server from the Rack Servers tab.

- While adding or applying a policy, you can now specify if the policy is specifically for Cisco UCS S3260 servers. Also, you can now create a Zoning policy which is applicable only for this server.

  Legacy Boot Order and Flex Flash policies are not available for Cisco UCS S3260 Rack Server.

- You can perform a firmware upgrade at the server level. But during a server upgrade, the chassis components and the disk drive components associated with the server are also upgraded. For more information, see Upgrading the Firmware Image, on page 101.

Managing a Chassis

Tagging Assets for a Cisco UCS S3260 Server

An asset tag is a user-defined label for a rack server. Using the **Asset Tag** option you can set a user-defined label for a chassis or a rack-server. For information on adding a asset tag to a rack server, see Tagging Assets for a Rack Server, on page 24.

Important Asset tagging is supported on C-series and S-series servers that are running firmware versions of 3.0(1c) and above. For E-series and ENCS servers, asset tagging is supported on servers running firmware versions 3.2.1 and above.

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Click **Chassis**.

Step 4 Choose the chassis that you want to set a tag to.

Step 5 From the **More Actions** drop-down list, choose **Asset Tag**.

Step 6 In the **Set Asset Tag** page, enter the name of the asset tag in the **Asset Tag** field.

Step 7 Click **Submit**.

Rebooting a Chassis

Perform this procedure when you want to restart a chassis.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the pod.
Step 3 On the **Compute** page, choose the account under **Pods**.
Step 4 Click **Chassis**.
Step 5 From the list, choose a chassis and click **Reboot CMC**.
Step 6 In the **Reboot Chassis Management Controller** screen, select either **CMC1** or **CMC2**.
Step 7 Click **Submit**.

Managing Tags for a Chassis

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 for a chassis. For adding tags for a rack-mount server, see Adding Tags for a Rack-Mount Server, on page 20.

Before you begin

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

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the pod.
Step 3 On the **Compute** page, choose the account under **Pods**.
Step 4 Click **Chassis**.
Step 5 From the list, choose a chassis and click **Manage Tags**.

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

Step 6 Click **+** to add an entry to the **Manage Tags** table.
Step 7 In the **Add Entry to Tag** screen, complete the following:

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

Step 8 Click **Submit**.

Step 9 Select a tag in the **Manage Tags** screen and click Edit.

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

Step 11 Click **Submit**.

Adding Tags for a Chassis

Tagging is used to assign a label to an object, such as a resource group or a rack server. Tags can be used to provide information such as rack locations, responsible support groups, purpose, or Operating System. Perform this procedure to add tags to a Cisco UCS S3260 Rack Server.

Before you begin

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

Note You can also select multiple rack servers.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

Step 3 On the **Compute** page, choose the account under **Pods**.

Step 4 Click **Chassis**.

Step 5 From the list, choose a chassis and click **Add Tags**.

Note The **Add Tags** option is displayed only after you select the server from the list.

Step 6 Choose a name from the **Tag Name** drop-down list.

If there are no tags available, you can create a new tag at this point.

Step 7 Choose a value for the tag from the **Tag Value**drop-down list.

Step 8 Click **Submit**.

Setting Front Locator LED

A server locator LED helps you to identify a specific server among many servers in a data center. Perform this procedure when you want to turn on or turn off the front locator LED for a selected chassis.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

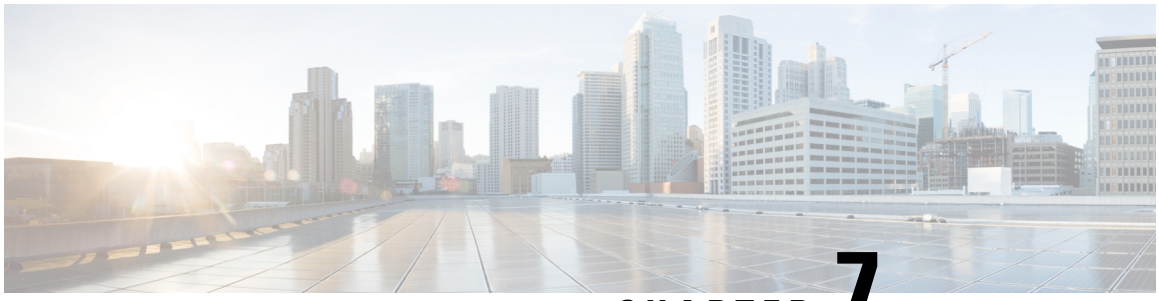
Step 3 On the **Compute** page, choose the account under **Pods**.

Step 4 Click **Chassis**.

Step 5 From the list, choose a chassis and click **Front Locator LED**.

Step 6 From the **Turn the Front Locator LED for selected chassis on/off** drop-down list, choose **ON** or **OFF**.

Step 7 Click **Submit**.



CHAPTER 7

Managing Rack Server Policies and Profiles

This chapter contains the following topics:

Rack Server Policies

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

The following workflow indicates how you can work with server policies in Cisco UCS Director:

1. Create a server 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 Server Policies, on page 40.
   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 41.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Policy, on page 74.
3. Perform any of the following optional tasks on the policy:
   a. View the list of servers that are mapped to a specific policy. For more information on performing these tasks, see Common Tasks for Server Policies, on page 42.
   b. Edit a policy to modify values.
   c. Delete a policy when it is no longer needed
   d. Clone a policy to use similar values
   e. Group multiple policies into a server profile. For more information about applying profiles, see Applying a Policy, on page 74.

Creating Server Policies

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

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

Policy	Procedure Documented in this Guide	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
BIOS Policy	Creating a BIOS Policy, on page 43	*Configuring BIOS Settings*
Disk Group Policy	Creating a Disk Group Policy, on page 44	*Managing Storage Adapters*
FlexFlash Policy	FlexFlash Policy, on page 45	*Managing the Flexible Flash Controller*
IPMI over LAN Policy	Creating an IPMI Over LAN Policy, on page 49	*Configuring IPMI*
LDAP Policy	Creating an LDAP Policy, on page 50	*Configuring the LDAP Server*
Legacy Boot Order Policy	Creating a Legacy Boot Order Policy, on page 52	*Server Boot Order*
Network Configuration Policy	Creating a Network Configuration Policy, on page 54	*Configuring Network-Related Settings*
Network Security Policy	Creating a Network Security Policy, on page 56	*Network Security Configuration*
Network Time Protocol Policy	Creating an NTP Policy, on page 57	*Configuring Network Time Protocol Settings*
Password Expiration Policy	Creating a Password Expiration Policy, on page 58	*Password Expiry*
Precision Boot Order Policy	Creating a Precision Boot Order Policy, on page 59	*Configuring the Precision Boot Order*
Power Restore Policy	Power Restore Policy, on page 60	*Configuring the Power Restore Policy*

Policy	Procedure Documented in this Guide	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
RAID Policy	Creating a RAID Policy, on page 61	*Managing Storage Adapters*
Serial Over LAN Policy	Creating a Serial Over LAN Policy, on page 64	*Configuring Serial Over LAN*
SNMP Policy	Creating an SNMP Policy, on page 64	*Configuring SNMP*
SSH Policy	Creating an SSH Policy, on page 66	*Configuring SSH*
User Policy	Creating a User Policy, on page 67	*Configuring Local Users*
VIC Adapter Policy	Creating a VIC Adapter Policy, on page 68	*Viewing VIC Adapter Properties*
Virtual KVM Policy	Creating a Virtual KVM Policy, on page 70	*Configuring the Virtual KVM*
vMedia Policy	Creating a vMedia Policy, on page 71	*Configuring Virtual Media*
Zoning Policy	Creating a Zoning Policy, on page 73	*Dynamic Storage* in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers.

Step 5 Click **Submit**.

What to do next

Apply the policy to a server. For more information about applying a policy, see Applying a Policy, on page 74.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

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

Step 4 In the **Add** screen, choose a policy from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Server Details** pane, you can use the server details in the following two methods:

a) Check **Enter Server Details Manually** and complete the required fields, including the following:

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 8 Click **Next**.

You will return to the **Main** pane for creating the policy. Continue with creating a policy using the prompts in the wizard. The fields for each policy vary depending on the policy you are creating in the system.

Step 9 Click **Submit**.

Common Tasks for Server Policies

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Expand a policy folder and select a policy.

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 74.

Step 5 (Optional) Click **View Apply Status** to view the details of a selected policy such as the status of the policy you have applied, the server details to which you have applied the policy and so on. If the policy is not successfully applied for example, an error message is displayed in the **Status Message** column.

Step 6 (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.

Step 7 (Optional) To clone a policy, click **Clone** to copy the details of a selected policy to a new policy.

Step 8 (Optional) To delete a policy, click **Delete**. In the **Delete Policy** screen, expand **Select Policy(s)** and check the policies you want to delete, and click **Submit**.

You can delete one or more selected policies even if you have associated the policy with a server. If you try to delete a policy which is associated to a profile, an error occurs.

Step 9 Click **Submit**.

Creating a 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **BIOS Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Note If some properties or attributes in Cisco UCS Director 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 6 Click **Next**.

Step 7 In the **Main** pane, select values for the main BIOS properties such as **CDN Control**, **POST Error Pause**, and **TPM Support** drop-down lists.

Step 8 Click **Next**.

Step 9 In the **Advanced** pane, choose the BIOS property values from the drop-down lists and click **Next**.

Step 10 In the **Boot Options** pane, choose the appropriate setting for the drop-down lists.

The **Power ON Password Support** drop-down list allows you to enable or disable power on password support. You can also choose the default platform setting. Enabling this option prevents you from making any changes to the server, including configuration changes and entering the BIOS setup. Prior to enabling this option, ensure that a BIOS password is set in the BIOS Configuration screen using the Cisco IMC user interface.

Step 11 In the **Server Management** pane, choose the server property values from the drop-down lists.

Step 12 Click **Submit**.

Creating a 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 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 Creating a RAID Policy, on page 61.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Disk Group Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create Disk Group Policy** screen, enter a name in the **Policy Name** field and click **Next**.

Step 6 In the **Virtual Drive Configuration** pane, choose the RAID level and click **Next**.

Step 7 In the **Local Disk Configuration** pane, click **+** to add an entry to reference a local disk configuration.

Step 8 In the **Add Entry to Local Disk Configuration Reference** pane, complete the required fields, including the following:

Name	Description
Slot Number field	Enter the slot number of the disk.
Role drop-down list	Choose a role. It be can one of the following: • Normal • Dedicated Hot Spare • Global Hot Spare

Step 9 Click **Submit**.

Step 10 In the **Local Disk Configuration** pane, select a local disk from the table and click **Submit**.

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

FlexFlash Policy

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

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

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

You cannot create a FlexFlash policy for Cisco UCS S3260 rack servers.

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **FlexFlash Policy** from the drop-down list and click **Submit**.

Step 5 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** pane. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 41.

Step 6 In the **Configure Cards** pane, complete the required fields, including the following:

Field	Description
Firmware Mode options	Choose any of the following firmware operating modes: • **Mirror** - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers. • **Util** - 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. This mode is available only for C220 M3, C240 M3, C22, C24, and C460 M4 servers.
Mirror radio button	Check **Enable Virtual Drive** to enable the Hypervisor virtual drive or **check Erase Virtual Drive** to erase it.
Util radio button	Check **Enable Virtual Drive** to enable virtual drives such as SCU, Hypervisor, Drivers, HUU, and User Partition or check **Erase Virtual Drive** to erase them. **Note** You can select multiple virtual drives.

Field	Description
Not Applicable radio button	Check **Enable Virtual Drive** to enable virtual drives such as SCU, HV, Drivers, and HUU. **Note** You can select multiple virtual drives. The **Erase Virtual Drive** check box is not available.
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).
Slot-1 Write Error Threshold field	The number of write errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

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

Step 7 If you selected **Not Applicable** as the firmware mode, complete the required fields, including the following:

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

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

Step 8 Click **Submit**.

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

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

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

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

Creating an IPMI Over LAN Policy

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **IPMI Over LAN Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create IPMI Over LAN Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.

Name	Description
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, see Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** page, complete the required fields, including the following:

Field	Description
Enable IPMI Over LAN check box	Check this check box to configure the IPMI properties.
Privilege Level Limitdrop-down list	Choose a privilege level from the drop-down list.
Encryption Key field	Enter a key in the field. 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 automatically added with zeros to the length of 40.

Step 8 Click **Next**.

Step 9 In the **Confirm** page, click **Submit**.

Creating an LDAP Policy

Cisco UCS Director 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **LDAP Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create LDAP Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, see Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the required fields, including the following:

Name	Description
Enable LDAP check box	Check the check box to enable LDAP on the server.
Base DN field	The Base DN for the server. The Base DN refers to the point from where the server begins the search for users.
Domain field	The LDAP domain name.
Timeout drop-down list	Choose a timeout interval.
Enable Encryption check box	Check this check box to enable encryption.
Binding Parameters	
Method drop-down list	Choose a binding method from the drop-down list.
Binding DN field	Specify the binding DN for the LDAP server. The Binding DN consists of the user and the location of the user in the LDAP tree.
Password field	The password.
Search Parameters	
Filter Attribute field	Specify the filtering attribute.

Name	Description
Group Attribute field	Specify the group attribute.
Attribute field	Specify the attribute.

Step 8 Click **Next**.

Step 9 In the **Configure LDAP Servers** pane, complete the required fields, including the following:

Name	Description
Use DNS to Configure LDAP Servers check box	Check this check box to specify DNS parameters.
Source drop-down list	Choose a source method for DNS. It can be Extracted, Configured or Configured-Extracted. If you select Extracted, then the remaining DNS parameters are not displayed.
Domain to Search field	Specify the domains that must be searched.
Forest to Search field	Specify the forests that must be searched.
Server 1 field	The IP address or the host name of the LDAP server.
Port field	The port number. You can enter details for about 6 servers. **Note** These fields are not displayed if you have enabled DNS to configure LDAP servers.

Step 10 Click **Next**.

Step 11 In the **Group Authorization** pane, fill in the group authorization details and click + to add an LDAP group entry to the table.

Step 12 In the **Add Entry to LDAP Groups** screen, fill in the group details.

Step 13 Click **Submit**.

Note
- Any existing LDAP Role Groups configured previously on the rack server are removed and replaced with the role groups that you 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).

Creating a Legacy Boot Order Policy

A Legacy Boot Order Policy automates the configuration of boot order settings of a rack server. 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 UCS Director, you can configure the order in which the rack 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 Creating a Precision Boot Order Policy, on page 59.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Legacy Boot Order Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers. For this policy, this check box is disabled.

Step 6 In the **Main** pane, click **+** to create a device type entry to the table. and select the device type from the drop-down list. The table lists the devices you have added.

Step 7 In the **Add Entry to Select Devices** pane, choose a device type, and click **Submit**.

You cannot add a device type multiple times.

In the **Device Type** table, select an existing device and use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

Step 8 Click **Submit**.

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. For servers running versions higher than 2.0, you must use the Precision Boot Order policy instead.

Creating a Network Configuration Policy

With a Network Configuration policy, you can specify the following network settings on a server:

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

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

Perform the following procedure to create a Network Configuration policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Network Configuration Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, see Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the following fields:

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

Step 8 If you checked the **Cisco UCS S3260** check box in the **General** pane, then you must complete the following steps:

a) In the **CMC Settings** pane, specify the hostname and IPv4 address, and click **Next**.
b) In the **BMC Settings** pane, specify the hostname and IPv4 address, and click **Next**.

Step 9 In the **Confirm** pane, click **Submit**.

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

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

Creating a Network Security Policy

Cisco UCS Director 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Network Security** from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **IP Blocking** pane, check the **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 8 Click **Next**.

Step 9 In the **IP Filtering** pane, check the **Enable IP Filtering** checkbox to enter IP addresses or a range of IP addresses.

Step 10 Click **Submit**.

Creating an NTP Policy

With an NTP service, you can configure a server managed by Cisco UCS Director to synchronize the time with an NTP server. By default, the NTP server does not run in Cisco UCS Director. 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 UCS Director 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **NTP Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the required fields, including the following:

Name	Description
Enable NTP check box	Check this check box to enable NTP and to configure a maximum of 4 servers.
NTP Server 1 field	Enter the IP address of the NTP server. You can enter the IP addresses of a maximum of 4 servers.

Step 8 Click **Submit**.

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

Creating a Password Expiration Policy

You can set a shelf life for a password, after which the password expires and is no longer valid for use. As an administrator, you can set this time in days. This configuration is common to all users. Users can set and derive the configuration as part of the user policy and create a password expiration policy.

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Password Expiration Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** page, enter a name for the policy and click **Next**.

Step 6 In the **Main** page, complete the required fields, including the following:

Field	Description
Enable Password Expiry check box	Check this check box to enable a specified password expiry duration. You must set the number of days after which the password will expire. Choose a number from the **Password Expiry Duration** drop-down list.
Password History field	Set the number of occurrences that will be displayed when you view the password history.
Notification Period field	Set the number of days before which you will be notified about the password expiry.
Grace Period field	Set the grace period after which the password will expire.

Step 7 Click **Submit**.

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

Creating a Precision Boot Order Policy

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

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

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

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Precision Boot Order Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create Precision Boot Order Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 In the **Main** pane, complete the required fields, including the following:

Name	Description
UEFI Secure Boot check box	Check the check box to enable UEFI secure boot. If you check this check box, then you cannot configure a boot mode.
Configure Boot Mode drop-down list	Choose a boot mode from the drop-down list. You can choose a boot mode only if you have not checked **UEFI Secure Boot**.
Select Devices list	Expand the list, and click + and select or enter device details. To enter the device details, you must specify the following fields: • Device Type • Device Name • State • Slot

Step 7 In the **Add Entry to Select Devices** screen, click **Submit**.

The devices that you have added are listed in the table. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

Step 8 Click **Submit**.

Step 9 Check **Configure One Time Boot Device** to set the device from which the server must boot once.

Important This check box is not applicable for Cisco IMC versions older than 3.0(1c).

Step 10 Select the device from the **One Time Boot Device** drop-down list.

Step 11 Check **Reboot On Update** to reboot the selected server after the one time boot device has been updated in the server.

Step 12 Click **Submit**.

Power Restore Policy

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

Note You cannot create this policy for ENCS servers.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 On the **Add** screen, choose **Power Restore Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field.

You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** screen. See Creating a Policy from an Existing Configuration, on page 41.

Step 6 Choose a setting from the **Power Restore Policy** drop-down list.

It can be one of the following options:

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

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

Step 7 Choose a value in the **Power Delay Type** drop-down list.

It can be one of the following:

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

Step 8 Specify a value between 0 and 240 seconds in the **Power Delay Type** field.

Step 9 Click **Submit**.

What to do next

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

Creating a 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **RAID Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create RAID Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, click + to add virtual drives that you want to configure on the server to the **Virtual Drives** list.

Step 8 In the **Add Entry to Virtual Drives** screen, complete the required fields, including the following:

Name	Description
Virtual Drive Name field	Enter a unique name for the virtual drive.
Virtual Drive Size (MB) field	The size of the virtual drive.

Name	Description
Disk Group Policy drop-down list	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, see Creating a Disk Group Policy, on page 44. **Note** If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.
Access Policy drop-down list	Choose an access policy for the virtual drive.
Read Policy drop-down list	Choose a read policy for the virtual drive.
Write Policy drop-down list	Choose a Write for the virtual drive.
IO Policy drop-down list	Choose an IO for the virtual drive.
Drive Cache drop-down list	Select the status of the drive cache.
Expand to available check box	Check the check box to expand the virtual drive.
Boot drive check box	Check the check box to indicate this virtual drive as a boot drive.
Set disks in JBOD state to Unconifigured Good check box	Disks which are in JBOD state will be set to Unconfigured Good state before being used for the Virtual Drive creation

Step 9 In the **Add Entry to Virtual Drives** screen, click **Submit**.

Step 10 Check **Delete existing Virtual Drives** 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 11 Check **Configure Unused Disks** to configure the remaining disks.

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.

a) Check either of the following options:

- **Unconfigured Good**
- **JBOD**

Step 12 Click **Submit**.

Creating a 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 UCS Director. 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Serial Over LAN Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create SoL Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, 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 8 Click **Submit**.

Creating an SNMP Policy

Cisco UCS Director 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **SNMP Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create SNMP Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **SNMP Users** pane, 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 8 Click **Next**.

Step 9 In the **SNMP Traps** pane, 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 10 Click **Next**.

Step 11 In the **SNMP Settings** pane, configure the SNMP properties.

Step 12 Click **Submit**.

Note

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

Creating an SSH Policy

The SSH server enables an 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **SSH Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create SSH Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the required fields, including the following:

Name	Description
Enable SSH check box	Check the check box to enable SSH and configure the SSH properties.
SSH Port field	By default, the port number of 22 is displayed. Use the arrows to increase or decrease the number.
SSH Session Timeout (seconds) field	The idle time, in seconds, after which an SSH session is timed out. By default, it is set to 60 seconds. Use the arrows to increase or decrease the number.

Step 8 Click **Submit**.

Creating a 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **User Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create User Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, check **Enforce Strong Password**.

Checking this check box implies that users selected for this policy must create a strong password.

Step 8 Click **+** to add users that need to be configured on the server to the **Users** list.

You can also select an existing user from the **Users** table and click **Edit** or **Delete** icons to edit or delete a user.

Step 9 In the **Add Entry to Users** screen, complete the required fields, including the following:

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

Step 10 Click **Submit**.

Step 11 In the **Main** pane, check **Add Password Expiration Policy**, and you can either choose a password expiration policy that you have previously created, or you can create a new policy.

To use a password expiration policy, Cisco IMC version 3.0(1c) or later is required.

Step 12 Click **Submit**.

Note
- The first user in the **Users** table is the admin user. You cannot delete this admin user but you can change the password.
- When you apply a user policy, the user entries in Cisco UCS Director are replaced with the user entries you created. Blank entries in Cisco UCS Director are replaced with default users from Cisco UCS Director. The default user role is always read-only and the user is disabled.
- Ensure that the account used to manage the Cisco UCS Director is not deleted from the user list in the policy. If deleted, the Cisco UCS Director will lose connection to the server being managed.

Creating a 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **VIC Adapter Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create VIC Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, click **+** to add a VIC adapter entry in the table.

Step 8 In the **Add Entry to VIC Adapters** screen, enter or select the adapter details.

- **PCI Slot Selection**—Specifies if the adapter is installed in any available PCI Slot or in a specific PCI slot. If you choose Any, then the **PCI Slot** field is not displayed.
- **PCI Slot**—The PCI slot in which the adapter is installed.
- **Description**—Description of the adapter.
- **FIP Mode**—Specifies if FCoE Initialization Protocol (FIP) mode is enabled or disabled.
- **Configure LLDP**—If checked, then Link Layer Discovery Protocol (LLDP) enables all the Data Center Bridging Capability Exchange protocol (DCBX) functionality, which includes FCoE, and priority based flow control.
- **VNTAG Mode**—Specifies if VNTAG mode is enabled or disabled.
- **Port Channel**—Sets the port channel to **Enabled**, **Disabled**, or **Not Applicable** state. For Cisco VIC 1455 and 1457 adapters, the port channel is set to **Enabled** by default. For adapters that do not support port channel configuration, this field is set to **Not Applicable**. vNICs and vHBAs are configured, by default, based on the port channel state selected in this field. The existing configuration is overwritten with the latest configuration when you change the port channel state. When the **Port Channel** field is set to **Enabled** or **Not Applicable**, a minimum of two vNIC(s) (eth0 and eth1) and two vHBA(s) (fc0 and fc1) are configured, by default. If the **Port Channel** field is set to **Disabled**, then a minimum of four

vNIC(s) (eth0, eth1, eth2, and eth3) and four vHBA(s) (fc0, fc1, fc2, and fc3) are configured, by default. However, you can create additional vHBAs or vNICs on these adapters.

- **External Ethernet Interface**—Configures the Admin Forward Error Correction (FEC) mode for Cisco VIC 1455, Cisco VIC 1457, Cisco VIC 1495, and Cisco VIC 1497 adapters. By default, four ports are available and you cannot delete them. However, the number of ports configured with the Admin FEC mode is based on the adapter model selected. For example, in a Cisco VIC 1497 adapter, only two ports are available. So, the Admin FEC mode is configured only on the first two ports (port 0 and port1), ignoring the remaining ports (port 2 and port 3).

  For existing policies, this field is set to **Auto**. But you can change this value to **cl91**, **cl74**, and **Off**. If the adapter model does not support Admin FEC mode, then these values would be ignored.

  Note The **cl74** option is not supported for Cisco VIC 1495 and Cisco VIC 1497 adapters.

- **vNIC**—Default properties are eth0 and eth1. You can only edit these properties and cannot delete them. These properties are also available for usNIC properties. When the **Port Channel** field is set to **Enabled** or **Not Applicable**, a minimum of two vNIC(s) (eth0 and eth1) are configured, by default, with an uplink port as 0 and 1. If the **Port Channel** field is set to **Disabled**, then a minimum of four vNIC(s), eth0, eth1, eth2, and eth3, are configured, by default, with an uplink port from 0 to 3. However, you can create additional vNICs on these adapters.

- **vHBA**—Default properties are fc0 and fc1. You can only edit these properties and cannot delete them. When the **Port Channel** field is set to **Enabled** or **Not Applicable**, a minimum of two vHBA(s) (fc0 and fc1) are configured, by default. If the **Port Channel** field is set to **Disabled**, then a minimum of four vHBA(s), fc0, fc1, fc2, and fc3, are configured by default. However, you can create additional vHBAs on these adapters.

Step 9 Click **Submit**.

Step 10 In the **Main** pane, click **Submit**.

Creating a Virtual KVM Policy

The KVM console is an interface accessible from Cisco UCS Director 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Virtual KVM Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create vKVM Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 Check **Enable vKVM**.

Step 8 In the **Max Sessions** drop-down list, choose a number to indicate the maximum number of KVM sessions.

Step 9 In the **Remote Port** field, specify the port number.

Step 10 Check the **Enable Video Encryption** check box.

Step 11 Check the **Enable Local Server Video** check box.

Step 12 Click **Submit**.

Creating a vMedia Policy

You can use Cisco UCS Director 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 UCS Director - 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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **vMedia Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create vMedia Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** screen, complete the required fields, including the following:

Name	Description
Enable vMedia check box	Check the check box to enable vMedia.
Enable Virtual Media Encryption check box	Check the check box for enabling vMedia encryption. This field is editable only after you check **Enable vMedia**.
Enable Low Power USB check box	Check this check box to enable low power USB on the server.
Maximum Sessions drop-down list	Select the maximum number of sessions allowed on the server.

Step 8 Click **Next**.

Step 9 Check **Add CDD vMedia Mapping** and complete the CDD mapping details.

Step 10 Click **Next**.

Step 11 Check **Add HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 12 Click **Submit**.

Note
- **Low Power USB State** cannot be configured currently in Cisco UCS Director.
- 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 Zoning Policy

A Zoning policy is used to assign physical drives to server. The Cisco UCS C-Series rack-mount servers support dynamic storage of Serial Attached SCSI (SAS) drives in the Cisco Management Controller (CMC). This dynamic storage support is provided by the SAS fabric manager located in the CMC. Dynamic storage supports the following options:

- Assigning physical disks to server 1 and server 2
- Chassis Wide Hot Spare (supported only on RAID controllers)
- Shared mode (supported only in HBAs)
- Un-assigning physical disks
- Viewing SAS expander properties
- Assigning physical drives to servers
- Moving physical drives as Chassis Wide Hot Spare
- Un-assigning physical drives

For details about configuring the various disk group properties, see section *Dynamic Storage* in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers.

Perform the following procedure to create a Zoning policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Zoning Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create Zoning Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 41.
Cisco UCS S3260 check box	A Zoning Policy is only applicable to Cisco UCS S3260 Rack Server. So, the **Cisco UCS S3260** check box is checked by default.

Step 6 Click **Next**.

Step 7 In the **Zoning** screen, click + to add local disks that you want to configure on the server.

Step 8 In the **Add Entry to Local Disks** screen, enter the **Slot Number** where the local disk is present.

Step 9 Select the local disk details such as the **Ownership** assigning the ownership of the local disk.

Step 10 Check **Force** when assigning disks owned by one server to another server.

Step 11 Click **Submit**.

Step 12 Check **Modify Physical Drive Power Policy** to set the policy.

Step 13 Select the power state from the **Physical Drive Power State** drop-down list.

Step 14 Click **Submit**.

Applying a Policy

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Expand the folders, and select a policy you want to apply.

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

Step 5 In the **Apply Policy** screen, choose the servers on which you want to apply this policy.

Step 6 Check **Schedule Later** to apply the policy at a later time.

You will have to select a schedule from the **Schedule** drop-down list, or create a new schedule.

Step 7 Click **Submit**.

The process of applying the policy to the specified set of servers is initiated. This process can take a few minutes depending on the policy type and network connectivity to servers to which the policy is being applied.

What to do next

You can also perform the following policy-related tasks:

- Click **Clone** to copy the details of a selected policy to a new policy.
- Click **View Apply Status** to see the list of the servers that the policy is associated to.
- Click **Delete** to delete policies from the system.

Deleting a Policy

You cannot delete a policy if it is mapped to a hardware profile.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Delete**.

Step 4 In the **Delete Policy** screen, check the check boxes of the policies you want to delete.

Step 5 Click **Submit**.

Rack Server Profiles

Multiple policies combined together form a server profile. For example, you can apply configuration details of a rack server profile to multiple rack-mount servers. You can associate this server 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 server profile in Cisco UCS Director:

1. Create a server profile. You can create a policy in one of the following methods:
   a. Create a new profile. For more information about creating a new profile, see Creating a Server Profile, on page 75.
   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 76.
2. Apply the profile on a server. For more information about applying a profile, see Applying a Server Profile, on page 78.
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 Common Tasks Under Server Profiles, on page 77.

Creating a Server Profile

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

Step 3 Click **Add**.

Step 4 In the **Create Hardware Profile** screen, in the **General** pane, 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** pane, see Creating a Profile from an Existing Configuration, on page 76.

Step 6 In the **Profile Entities** screen, 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** screen, 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 Server Policies, on page 40.

Step 9 Click **Submit**.

Step 10 In the **Profile Entities** screen, click **Submit**.

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 Common Tasks Under Server Profiles, on page 77

Creating a Profile from an Existing Configuration

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

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

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

Step 3 Click **Add**.

Step 4 Enter a name for the profile in the **Profile Name** field.

Step 5 Check **Create profile from current configuration of the server**. 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** screen, 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**.

Common Tasks Under Server Profiles

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

Step 3 Expand the list of hardware profiles and select a profile.

Step 4 (Optional) To delete a profile, click **Delete** and complete the following steps:

a) Click **Select** in the **Delete Profile** screen.

b) Select one or more profiles.

c) Click **Select**.

d) Click **Submit**.

You cannot delete a profile which is associated to a server. You must associate a different profile to the server before deleting it.

Step 5 (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.

Step 6 (Optional) To copy the details of an existing profile to a new profile, click **Clone**.

Step 7 (Optional) To apply a profile to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Server Profile, on page 78.

Step 8 Click **View Details** to view the details of a selected profile such as the status of the profile you have applied, the server details to which you have applied the profile and so on. If the profile is not successfully applied for example, an error message is displayed in the **Status Message** column.

Step 9 Click **Submit** or **Close** if applicable.

Applying a Server Profile

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

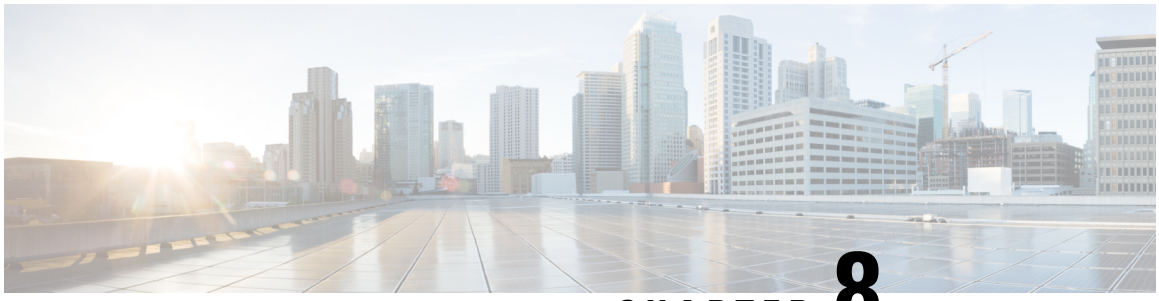
Step 3 Select an existing server profile and click **Apply**.

Step 4 In the **Apply Profile** screen, 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**.

The process of applying a profile to the specified set of servers is initiated. This process can take a few minutes depending on the profile type and network connectivity to server(s) to which the profile is being applied.



CHAPTER 8

Host Image Mapping for E-series Servers

Host Image Mapping

Host Image Mapping is a commonly used feature for the E-Series servers which allows you to download a firmware file to Cisco IMC, and upgrade the firmware. Using Cisco UCS Director, you can create a host image mapping profile to download and upgrade either one of the following:

- ISO firmware image
- CIMC image or
- BIOS image

You can download the firmware image on Cisco IMC in one of the following methods:

- Provide a location on the network (an FTP, FTPS, HTTP or HTTPS server) where the firmware file is currently available.

  For more information, see Adding a Network Host Image Mapping Profile, on page 80

- Choose the firmware file from a location on your system.

  For more information, see Creating an Upload Profile for Host Image Mapping, on page 82

- Download the firmware image from www.cisco.com.

  For more information, see Creating a Cisco.com Profile for Host Image Mapping, on page 84

Important To perform these tasks, Cisco IMC version 3.2.4 must be installed on the E-series servers. This feature does not work with prior versions of Cisco IMC.

For information on creating a profile to upgrade the firmware, see Adding a Network Host Image Mapping Profile, on page 80.

Adding a Network Host Image Mapping Profile

Before you begin

You should have created rack accounts for UCS E-series servers in the system.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Choose **Network Profile**.

Click this button if you have downloaded the firmware image from a location on the network.

Step 4 On the **Create Host Image Mapping Profile - Network** screen, complete the required fields, including the following:

Field	Description
Profile Name field	A descriptive name for the profile.
Platform drop-down list	Choose a server platform. While applying this profile, the list of available servers is populated based on the platform you select in this drop-down list. **Attention** This drop-down list is populated by the rack accounts that you have created for UCS E-series servers.
Download Image From drop-down list	Select the type of server where the firmware image is available. It can be one of the following: • FTP Server • FTPS Server • HTTP Server • HTTPS Server
Server IP Address field	IP address of the server.

File Path field	The path to the location where the fimware file is available.
File Type drop-down list	Choose the file type of the image. It can be one of the following: • **ISO** • **CIMC** • **BIOS**
File Name field	Enter the name of the file.
User name field	The user name. **Note** This field is only displayed when you select **FTP Server** or **FTPS Server** in the **Download Image From** drop-down list.
Password field	The user password. **Note** This field is only displayed when you select **FTP Server** or **FTPS Server** in the **Download Image From** drop-down list.
Map After Download check box	Maps the downloaded image. **Important** This check box is displayed only if you selected **ISO** in the **File Type** drop-down list. You can map the image while creating the profile, or you can map the image at a later point in time. Mapping an ISO image is mandatory for initiating an upgrade on the server. If you have not mapped the image on the server, and attempt to upgrade the firmware, an error message stating that the image is not mapped is displayed.For information on mapping an image in this scenario, see Mapping and Unmapping a Host Image, on page 89.
Delete All Existing Images check box	Deletes all the currently downloaded images available in Cisco IMC of the server chosen for the firmware upgrade.

Run Upgrade After Download check box	Check this check box if you want to initiate the upgrade process immediately after the firmware file is downloaded. If you prefer to initiate the upgrade process manually at a later time, then do not check this check box. To run this process at a later time, see Running a Host Image Upgrade Manually, on page 88. **Important** If you chose **ISO** in the **File Type** drop-down list, and if you check this check box, then you must also check the **Map After Download** check box to proceed. By checking both these check boxes, the firmware file is downloaded and mapped to Cisco IMC.

Step 5 Click **Submit**.

What to do next

After creating a profile, you must select a server on which this profile must run on. For more information, see Applying a Host Image Profile, on page 87.

Following are some of the other actions you can perform after creating a profile:

- Edit or delete a profile
- View status information for a profile
- Initiate the upgrade process if not previously indicated while creating the profile.

Creating an Upload Profile for Host Image Mapping

Follow this procedure to upload a firmware file from your system to Cisco IMC.

Before you begin

You should have created rack accounts for UCS E-series servers in the system.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Choose **Upload Profile**.

Step 4 In the **Create Host Image Mapping Profile – Upload** screen, complete the required fields including the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile. The profile name must be unique.
Platform drop-down list	Choose a platform from the drop-down list. While applying this profile, the list of available servers is populated based on the platform you select in this drop-down list **Attention** This drop-down list is populated by the rack accounts that you have created for UCS E-series servers.
File Type drop-down list	Choose the file type of the image. It can be one of the following: • ISO • CIMC • BIOS
File Name field	Click **Select a File** to browse for and select a file from your system.
Map After Download check box	Maps the downloaded image. **Important** This check box is displayed only if you selected **ISO** in the **File Type** drop-down list. You can map the image while creating the profile, or you can map the image at a later point in time. Mapping an ISO image is mandatory for initiating an upgrade on the server. If you have not mapped the image on the server, and attempt to upgrade the firmware, an error message stating that the image is not mapped is displayed.For information on mapping an image in this scenario, see Mapping and Unmapping a Host Image, on page 89.
Delete All Existing Images check box	Deletes all the currently downloaded images available in Cisco IMC of the server chosen for the firmware upgrade.

Field	Description
Run Upgrade After Download check box	Check this check box if you want to initiate the upgrade process immediately after the firmware file is downloaded. If you prefer to initiate the upgrade process manually at a later time, then do not check this check box. To run this process at a later time, see Running a Host Image Upgrade Manually, on page 88. **Important** If you chose **ISO** in the **File Type** drop-down list, and if you check this check box, then you must also check the **Map After Download** check box to proceed. By checking both these check boxes, the firmware file is downloaded and mapped to Cisco IMC.

Step 5 Click **Submit**.

What to do next

After creating a profile, you must select a server on which this profile must run on. For more information, see Applying a Host Image Profile, on page 87.

Following are some of the other actions you can perform after creating a profile:

- Edit or delete a profile
- View status information for a profile
- Initiate the upgrade process if not previously indicated while creating the profile.

Creating a Cisco.com Profile for Host Image Mapping

Complete this procedure to create a profile to download an image from www.cisco.com.

Before you begin

- You should have configured the Cisco.com user credentials. For more information, see Configuring Your Cisco User Account, on page 94
- You should enabled proxy configuration on the system. For more information, see Configuring Proxy Settings, on page 91

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Choose **CCO Profile**.

Step 4 In the **Create Host Image Mapping Profile - CCO** screen, complete the required fields, including the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile. The profile name must be unique.
Proxy Configuration check box	Indicates if the proxy settings have been configured or not. If the check box is checked, it implies that the proxy settings have been configured.
Platform drop-down list	Choose a platform from the drop-down list. While applying this profile, the list of available servers is populated based on the platform you select in this drop-down list **Attention** This drop-down list is populated by the rack accounts that you have created for UCS E-series servers.
Download Now check box	Check this check box to initiate the download of the firmware image immediately after you create the profile. If you do not check this check box now, you can download the image at a later point in time. To do so, choose the profile name in the **Host Image Mapping** screen, and from the **More Actions** drop-down list, choose **Download Image**. After the image is downloaded, you must apply the profile. For more information, see Applying a Host Image Profile, on page 87.
Available Image drop-down list	Choose the image from the drop-down list. This list is populated with images relevant to the server platform you chose in the **Platform** drop-down list.

Field	Description
Map After Download check box	Maps the downloaded image. **Important** This check box is displayed only if you selected **ISO** in the **File Type** drop-down list. You can map the image while creating the profile, or you can map the image at a later point in time. Mapping an ISO image is mandatory for initiating an upgrade on the server. If you have not mapped the image on the server, and attempt to upgrade the firmware, an error message stating that the image is not mapped is displayed.For information on mapping an image in this scenario, see Mapping and Unmapping a Host Image, on page 89.
Delete All Existing Images check box	Deletes all the currently downloaded images available in Cisco IMC of the server chosen for the firmware upgrade.
Run Upgrade After Download check box	Check this check box if you want to initiate the upgrade process immediately after the firmware file is downloaded. If you prefer to initiate the upgrade process manually at a later time, then do not check this check box. To run this process at a later time, see Running a Host Image Upgrade Manually, on page 88. **Important** If you chose **ISO** in the **File Type** drop-down list, and if you check this check box, then you must also check the **Map After Download** check box to proceed. By checking both these check boxes, the firmware file is downloaded and mapped to Cisco IMC.

Step 5 Click **Submit**.

What to do next

After creating a profile, you must select a server on which this profile must run on. For more information, see Applying a Host Image Profile, on page 87.

Following are some of the other actions you can perform after creating a profile:

- Edit or delete a profile
- View status information for a profile
- Initiate the upgrade process if not previously indicated while creating the profile.

- Download an image if not previously downloaded while creating the profile.
- Delete a downloaded image.

Applying a Host Image Profile

After creating a host image mapping profile, you can select a server on which:

- A profile can be run to download the image to Cisco IMC or
- firmware upgrade must be initiated immediately, provided you selected the **Run Upgrade After Download** check box while creating the profile.

Note If you do not apply a host image profile, then blank reports are generated when you choose the **View Status** option. Also, you cannot initiate a firmware upgrade without applying a profile, or when the Apply Host Image Profile action is in progress.

Before you begin

You should have created a host image mapping profile in the system.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Select a profile from the table and click **Apply**.

Alternatively, you can select and profile, and choose **Apply** from the **More Actions** drop-down list.

Step 4 In the **Apply Profile** screen, click **Select** to select the servers on which this firmware image must be applied on.

You can select multiple servers. The list of servers is populated based on the server platforms you selected while creating the profile.

Step 5 Click Select to return to the **Apply Profile** screen.

Step 6 Click **Submit**.

Downloading a Firmware Image

Complete this procedure to download a firmware image on the Cisco IMC of the server.

Before you begin

- You have created a Cisco.com profile for downloading the firmware image.

- While creating the profile, you have not checked the Download Now check box.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Choose a CCO profile from the list of profiles.

Step 4 From the **More Actions** drop-down list, choose **Download Image**.

Step 5 In the **Download Image** screen, review the information displayed and click **Download**.

The firmware image specified in the profile is downloaded from Cisco.com using the Cisco.com credentials that you configured.

What to do next

At a later point in time, you can delete the image that you have downloaded. For more information, see Deleting a Downloaded Image, on page 89.

Running a Host Image Upgrade Manually

While creating a host image mapping profile, if you did not check the Run Upgrade After Download check box, then you manually initiate the upgrade process by completing the following procedure.

Before you begin

You should have created a host image mapping profile in the system.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Choose **Run Upgrade**.

Step 4 In the **Upgrade Host Image** screen, complete the required fields, including the following:

Field	Description
Select Profile drop-down list	Choose a profile. After you choose a profile, the details of the profile are displayed on the screen.
Servers field	Click **Select** to choose the servers on which the upgrade must be run.

Field	Description
Schedule Later check box	Check this check box and select an existing schedule to upgrade the server at a later time, or click + to create a new schedule. For information on creating a new schedule, see Creating Schedules.

Step 5 Click **Submit**.

Deleting a Downloaded Image

While creating a Cisco.com profile, you can choose to download the firmware image immediately after creating the profile, or you can download it at a later point in time. After an image is downloaded, you can delete it from the Cisco UCS Director. This option is only available for images downloaded with the Cisco.com profile.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.
Step 3 Choose the CCO profile from the list of created profiles.
Step 4 From the **More Actions** drop-down list, choose **Delete Image**.
Step 5 In the **Delete Image(s)** screen, click **Delete**.

Mapping and Unmapping a Host Image

Complete this procedure to map or unmap a host image on a specific Cisco IMC server. You can map and unmap only an ISO host image. For other host images such as BIOS and CIMC, you can only delete them from this screen.

Before you begin

You should have created a host image mapping profile in the system.

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, choose the pod.
Step 3 Choose the **Rack Servers** tab.

Step 4 Double-click the server in the list to view the details, or select **View Details** from the **More Actions** drop-down list.

Step 5 Choose the **Host Images** tab.

The screen lists all the images that are available on the Cisco IMC server.

Step 6 Choose an ISO host image and select **Map Image** or **Unmap Image** or **Delete Image**.

From this screen, you can only select **Delete Image** for BIOS and CIMC images.

Viewing Status Details of a Host Image Profile

Before you begin

You should have created a host image mapping profile in the system.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Select a profile from the table and choose **View Status Details** from the **More Actions** drop-down list.

You can also select a profile from the table and right-click to choose **View Status Details**.

The **View Host Image Mapping Profile Status** screen displays the following information:

- Profile name
- Server IP address
- Download status
- Upgrade status

  The status information is displayed for an upload profile and for a Cisco.com profile.

Note If you chose a BIOS file to upgrade the firmware, then you must wait for about 3-4 minutes for the changes to reflect in the Cisco IMC of that server.

Deleting a Host Image Mapping Profile

Procedure

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

Step 2 On the **Physical Accounts** page, click **Host Image Mapping**.

Step 3 Select a profile from the table and click **Delete Profile**.

Step 4 In the **Delete Profile** screen, click **Delete**.

The profile is deleted from the system.

Configuring Proxy Settings

Perform this procedure when you want to configure proxy settings.

Procedure

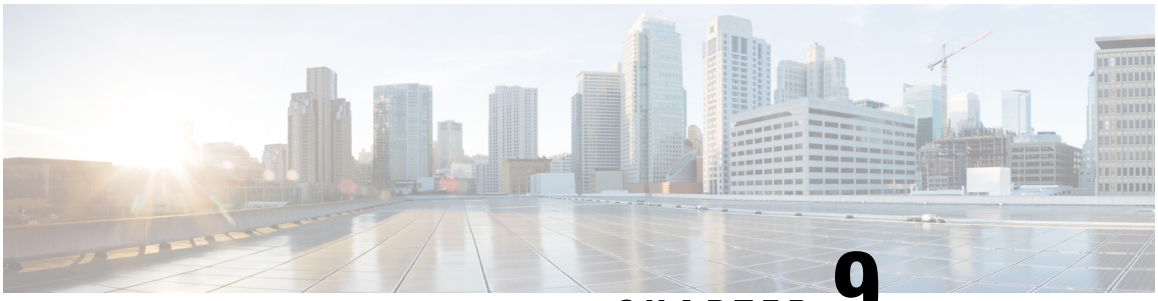
Step 1 Choose **Administration** > **System**.

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

Step 3 Complete the required fields, including the following, to configure proxy on the system:

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

Step 4 Click **Save**.



CHAPTER 9

Managing Cisco UCS Hardware Compatibility Reports

Hardware Compatibility Reports

Cisco UCS Hardware Compatibility Report allows you to check interoperability information for Cisco UCS components and configurations that have been tested and verified by Cisco, Cisco partners, or both. You can run reports and check the status against your current software version or a target software version. The hardware compatibility report checks the compatibility of the operating systems on servers, and then checks the adapter drivers associated with that operating system.

Cisco UCS Director integrates with the Cisco UCS Hardware Compatibility Report tool to provide information on whether the server, firmware and related components (Storage, Network Adapters, VIC adapters) are supported for a given server model, OS Vendor, Version and processor combination.

Important Cisco UCS Hardware Compatibility Report tool is available only for Cisco C-Series/S-Series servers.

An independent version of this tool is available at https://ucshcltool.cloudapps.cisco.com/public. Cisco UCS Director leverages the REST APIs exposed by this tool to obtain the compatibility report.

To use the Cisco UCS Hardware Compatibility Report tool, you must ensure the following:

- The DNS is properly configured and the url https://ucshcltool.cloudapps.cisco.com is reachable from the system.
- You have specified cisco.com credentials. See Configuring Your Cisco User Account, on page 94.

Configuring Your Cisco User Account

Complete this procedure to configure your Cisco-provided credentials in the system. If you configure these details, you can use the hardware compatibility report tool in Cisco UCS Director.

Procedure

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

Step 2 On the **Sytems** page, choose **Cisco.com User Configuration**.

Step 3 Complete the required fields, including the following:

Field	Description
Username field	Your Cisco login user name.
Password field	Your Cisco login password.

Step 4 Click **Save**.

Tagging OS Vendor and OS Version

To be able to use the hardware compatibility report tool in Cisco UCS Director, you must tag the rack servers with an operating system vendor name and operation system version.

You can select the servers at the system, rack groups or at a rack server level and tag them by performing the following procedure.

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the account under **Pods**.

Step 3 Choose a rack server from the list.

Step 4 From the **More Actions** drop-down list, choose **Manage OS Tag for HCR**.

Note This option is not available for E-series servers.

Step 5 In the **Manage OS Tag for Hardware Compatibility Report** page, complete the required fields, including the following:

Field	Description
Operating System drop-down list	Choose an operating system from the list.
Operating System Version drop-down list	Choose an operating system version from the list.

Note If the operating systems and the related versions are not listed in the drop-down lists, then verify that the DNS is properly configured and the url https://ucshcltool.cloudapps.cisco.com/ is reachable from the Cisco UCS Director appliance. Also, manually run the Synchronize Hardware Compatibility Reports system task available from the **Administration** > **System** > **System Task** screen.

Step 6 Click **Submit**.

What to do next

When you no longer need this tag, you can select the rack server, and choose **Delete OS Tag for HCR** from the **More Actions** drop-down list.

Creating Hardware Compatibility Reports

Before you begin

- You have configured your Cisco.com account details. For more information, see Configuring Your Cisco User Account, on page 94
- You have tagged the servers with operating system vendors and operating system versions. For more information, see Tagging OS Vendor and OS Version, on page 94.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Compatibility Report**.

Step 3 Click **Add**.

Step 4 In the **Create Hardware Compatibility Report** page, complete the required fields, including the following:

Field	Description
Profile Name field	Enter a name for the hardware compatibility report profile.
Servers list	Expand the list to check the checkboxes of servers that you want to retrieve configurations for.

Step 5 Click **Validate**.

Step 6 Click **Submit**.

The **Hardware Compatibility Report** page lists the profiles that you have created. You can choose a profile from this list, and click **View Status Details**. You can also view the reports by selecting a rack group or rack server and choosing **Hardware Compatibility Reports**.

What to do next

You can select the report you have created and Delete, Edit, Synchronize HCL Report and or View Status Details. The report determines if the server is supported and if it is compliant. Compliance can be in any of the following states:

- **Fully Compliant**—If the server OS Vendor, version or processor and its related components are fully supported.
- **Partially Compliant**—If a few of the components are found to be unsupported.
- **Not Compliant**—If there is a compliance error or if the given combination of server or related components are invalid.
- **Error or Cannot Determine**—If the given server is not tagged or if there is an error while trying to retrieve the response from the backend.

Synchronizing Hardware Compatibility Reports

The **Synchronize Hardware Compatibility Reports** system task runs every week to synchronize the Hardware Compatibility Reports with the backend periodically. Perform this procedure to synchronize the reports manually.

Before you begin

- Configure the URL https://ucshcltool.cloudapps.cisco.com.
- You have configured your Cisco.com account details. For more information, see Configuring Your Cisco User Account, on page 94

Procedure

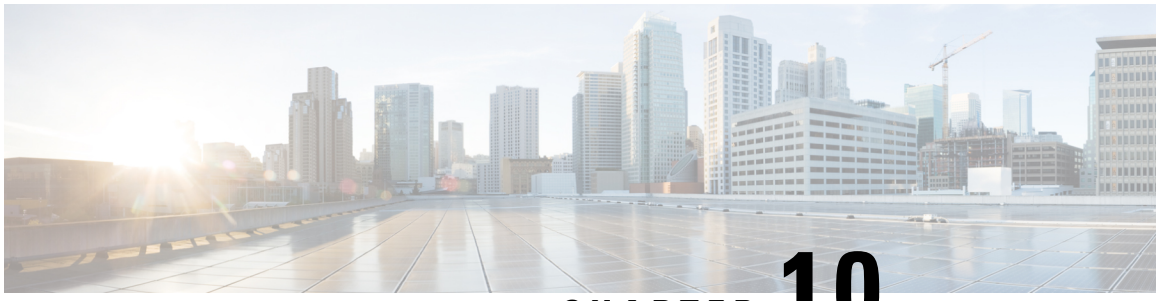
Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Expand **Rack Server Tasks**.and choose **Synchronize Hardware Compatibility Reports**.

Step 4 Click **Run Now**.

Step 5 Click **Submit**.



CHAPTER 10

Managing Firmware Upgrades

This chapter discusses the following topics:

About Upgrading Firmware on Rack Servers

In Cisco UCS Director, you can create firmware upgrade profiles and then use these profiles to upgrade the firmware on rack servers. You can create the following types of firmware upgrade profiles:

- Profile for locally stored firmware images.

  For more information on creating this profile, see Adding Images to a Local Cisco UCS Director System, on page 97

- Profile for firmware images stored on the network.

  For more information on creating this profile, see Adding Images from a Network Server, on page 100

Adding Images to a Local Cisco UCS Director System

Procedure

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

Step 2 On the **Physical Accounts** page, click **Images - Local**.

Step 3 Click **Add**.

Step 4 In the **Add Firmware Image - Local** screen, complete the required fields, including the following:

Field	Description
Profile Name field	Enter a descriptive and unique profile name. The profile name must be unique across both Local and Network image profiles.
Proxy Configuration check box	(Optional) Check this check box to enable proxy configuration and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.
Platform drop-down list	Choose a platform from the drop-down list. This list displays only those platforms that have at least one server being managed.
Available Image drop-down list	Choose the .iso image from the drop-down list.
Download Now check box	Check this check box to download the .iso image immediately after adding a profile.
Graceful Timeout check box	Check this check box to specify a time period within which the host system must shutdown to initiate the firmware upgrade process. **Note** You can configure graceful timeout for systems running Cisco IMC 3.1(3a) or higher. If you do not provide a timeout period, then the system is forcibly shut down after 120 seconds.
Timeout (in mins) field	Specify a time period, in minutes, within which the host system must shutdown to initiate the firmware upgrade process. You can specify a value between 0 and 60.
Force Shutdown Server check box	Check this check box to forcibly shut down the host system if it did not shut down within the time specified in the **Graceful Timeout (in mins)** field. This option is enabled by default.
Accept License Agreement check box	Check this check box to accept the license agreement. Click on the **Terms and Conditions** link to read the End User License Agreement. **Note** You must accept the license agreement to create a firmware profile, irrespective of the time you choose to download the image.

Step 5 Click **Submit**.

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

Uploading Images from a Local File System

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

Procedure

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

Step 2 On the **Physical Accounts** page, click **Images - Local**.

Step 3 Click **Upload** to add an image.

Step 4 In the **Upload Firmware Image - Local** screen, complete the required fields, including 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 5 Click **Upload**.

Step 6 Click **OK** in the **File Upload** confirmation screen, once the upload is complete.

Step 7 Click **Close**.

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 system.

Adding Images from a Network Server

Procedure

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

Step 2 On the **Physical Accounts** page, click **Images - Network**.

Step 3 Click **Add**.

Step 4 In the **Add Firmware Image - Network** screen, complete the required fields, including the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile. The profile name must be unique across both Local and Network image profiles.
Platform drop-down list	Choose a platform from the drop-down list.
Mount Type drop-down list	Choose either Network File System (NFS) or Common Internet File System (CIFS) server types.
Remote IP field	Enter remote IP address.
Remote Share field	Enter remote share path.
Remote File Name field	Enter a remote filename. **Note** The remote filename is the Unified Computing System (UCS) Server Configuration Utility ISO file.
User Name field	Enter a network path user name.
Password field	Enter a network path password.
Graceful Timeout check box	Check this check box to specify a time period within which the host system must shutdown to initiate the firmware upgrade process.
Timeout (in mins) field	Specify a time period, in minutes, within which the host system must shutdown to initiate the firmware upgrade process.
Force Shutdown Server check box	Check this check box to forcibly shut down the host system if it did not shut down within the time specified in the **Graceful Timeout (in mins)** field. This option is enabled by default.

Step 5 Click **Submit**.

Note You can click **View Location Details** to view profile configuration details, click **Modify** to modify the firmware image details, and click **Delete Profile** to delete the image profile. You can also select multiple profiles concurrently and delete them.

Upgrading the Firmware Image

Perform this procedure when you want to upgrade firmware on a rack server.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Firmware Upgrades**.

Step 3 Click **Run Upgrade**.

A warning message stating that the firmware upgrade process will result in downtime of the hosts is displayed.

Step 4 Click **OK** to confirm.

Step 5 In the **Upgrade Firmware** screen, complete the following:

Field	Description
Select Profile drop-down list	Choose a profile from the drop-down list.
Server(s) list	Check the check boxes of the servers. 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 31. You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to verify the scheduled task and its progress. You can also select a scheduled task and click **Remove Scheduled Tasks** to remove the associated scheduled task.

Step 6 Click **Submit**.

Deleting the Firmware Image

Perform this procedure when you want to delete only the firmware image and not the profile using which the firmware image was downloaded.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Images - Local**.

Step 3 Select a profile from the table.

Step 4 Click **Delete Image**.

Step 5 In the **Delete Image(s)** screen, click **Delete**.

The firmware image is deleted from the system. You can download this firmware image from later on by using the **Download Image** option.

Deleting a Profile Created for Firmware Upgrade

Perform this procedure when you want to delete a profile created for firmware upgrade.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Images - Local** or **Images - Network**.

Step 3 Select a profile from the table.

Step 4 Click **Delete Profile**.

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

Clearing Firmware Upgrade Status Messages

Perform this procedure to clear all firmware-related status messages recorded in the Cisco UCS Director system.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Firmware Upgrades**.

Step 3 Click **Delete Upgrade Status**.

Step 4 Click **Submit**.

Firmware Upgrades From SD Cards

As an administrator, you can now perform firmware upgrades on rack servers by downloading ISO images to Miscro SD cards or FlexFlash cards. The user interface provides you with the following options to perform these firmware upgrades:

- **Download Image**—Use this option to download a firmware image for specific servers. You can also choose to initiate the firmware upgrade immediately after the image is downloaded. See Downloading Firmware Image to an SD Card, on page 103.
- **Run Upgrade**—Use this option to initiate a firmware upgrade at a later point in time after the image is downloaded. See Running Firmware Upgrade from an SD Card, on page 104.
- Delete Status Messages—Use this option to delete all firmware upgrade-related status messages from the user interface. See Deleting Image Download Messages, on page 105.

To use these options, you must first create rack accounts in the system, and then create either local image profiles or network image profiles in the system. For more information on creating these profiles, see Adding Images to a Local Cisco UCS Director System, on page 97 and Adding Images from a Network Server, on page 100.

Downloading Firmware Image to an SD Card

Before you begin

- Racks accounts are added in the system.
- Local and network image profiles are created in the system.
- On Cisco UCS M4 servers, ensure that the FlexFlash controller is configured in the Util mode and not the mirror mode. If the controller is configured in the mirror mode, you cannot download the ISO file to the SD card. Use the FlexFlash policy to configure the controller in the Util mode.

Procedure

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

Step 2 Choose **Firmware Upgrades - SD**.

Step 3 Choose **Download Image**.

Step 4 In the **Download Image** screen, complete the required fields, including the following:

Field Name	Description
Download Image From drop-down list	Choose if you want to use a local profile or a network profile to download the image.
Select Profile drop-down list	Choose a profile from the list. This drop-down list displays profiles for only M4 and M5 servers.

Field Name	Description
Run Upgrade After Download check box	Check this check box if the firmware upgrade process must be initiated immediately after the image is downloaded. By default, this check box is not checked.
Servers field	Click **Select** to check the check boxes of the servers on which you want the firmware upgrade process to run on. Click **Select** to return to the **Download Image** screen.

Step 5 Click **Submit**.

The firmware image is downloaded to the servers that you selected.

What to do next

Initiate the firmware upgrade on the servers. See Running Firmware Upgrade from an SD Card, on page 104.

Running Firmware Upgrade from an SD Card

Before you begin

You have downloaded the firmware image using the **Download Image** option. See Downloading Firmware Image to an SD Card, on page 103.

Procedure

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

Step 2 Choose **Firmware Upgrades - SD**.

Step 3 Click **Run Upgrade**.

Step 4 Click **Select** to check the check boxes of the servers on which you want the firmware upgrade process to run on.

Step 5 Click **Select**.

Step 6 Click **Submit**.

The firmware upgrade process is initiated on the selected servers. You can review the progress of the upgrade from the **Images -SD** screen. The status is displayed in the **Upgrade Status** column.

Deleting Image Download Messages

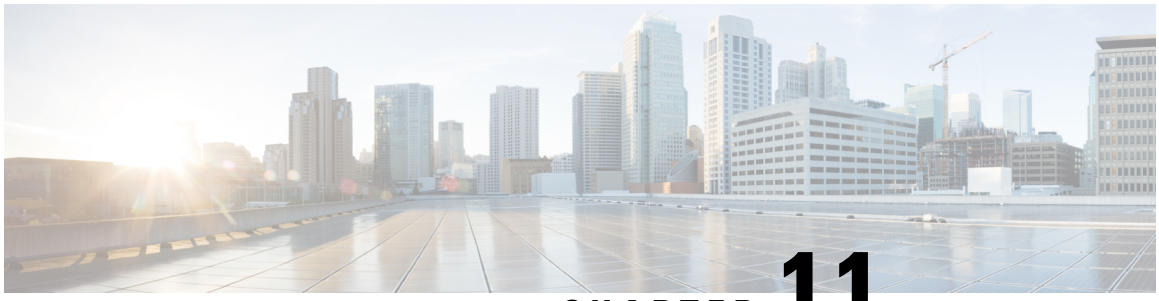
Procedure

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

Step 2 Choose **Firmware Upgrades - SD**.

Step 3 Choose a profile from the list and click **Delete Status**.

Step 4 In the **Delete Image Download Messages** screen, click **Delete**.



CHAPTER 11

Monitoring and Reporting

About Monitoring and Reporting

Cisco UCS Director displays all managed components in each rack-mount server that has been added to a rack group. These components can be hardware or software.

Information You Can View

You can view and monitor details about each component, including the following:

- License status
- Summary of the current status

Components You Can Monitor

You can monitor specific components or view reports for each of the components, including the following:

- vNICs and vHBAs
- Adapters, such as network and PCI
- Hardware components, such as CPUs, interface cards, and memory

Email Alerts

You can configure rules in Cisco UCS Director so that an email message is triggered when faults of a certain severity occur on rack servers or rack server groups. When fault conditions specified in the rule occur, an

email message is triggered and sent to the recipients you have specified. For information on configuring these email alert rules, see Configuring Email Alert Rules, on page 110.

Monitoring a Rack Server and Its Components

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

Step 3 On the **Compute** page, choose the account under **Pods**.

Step 4 Click **Rack Servers**.

Step 5 Choose the row of the server that you want to monitor.

Step 6 Click **View Details**.

By default, the **Summary** tab is displayed.

Step 7 Click on one of the tabs to view the status of the licenses, the server, or a specific component in the server.

Additional information may be available if you click **View Details** on one or more of the individual components.

Viewing Reports About a Rack Server

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

Step 3 On the **Compute** page, choose the account under **Pods**.

Step 4 Click **Rack Servers**.

Step 5 Choose the row of the server for which you want to view reports.

Step 6 In the right pane, click **Summary** to view a wide array of tabular, graphical, and map reports that provide a view of trending data for the account.

Step 7 For some reports, you can click the icons on the table bar to customize the table columns, filter the results, or export a report of the current table contents.

For more information, see the Cisco UCS Director Administration Guide.

Clearing SEL

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

Step 3 On the **Compute** page, choose the account under **Pods**.

Step 4 Click **Rack Servers**.

Step 5 Double-click the sever from the list to view the details or click the sever from the list and from the **More Actions** drop-down menu, choose **View Details**.

Step 6 Click **System Event Log**.

Step 7 Click **Clear IMC SEL Log**.

Step 8 (Optional) In the **Clear IMC SEL Logs** screen, check **Delete historical logs from Cisco UCS Director**.

Selecting this option clears the system event logs from the Cisco UCS Director GUI.

Step 9 Click **Submit**.

Uploading Technical Support Data to a Server

Procedure

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the pod.

Step 3 On the **Compute** page, choose the account under **Pods**.

Step 4 Click **Rack Servers**.

Step 5 Double-click the sever from the list to view the details or click the sever from the list and from the **More Actions** drop-down menu, choose **View Details**.

Step 6 Click **Tech Support**.

Step 7 Click **Create Tech Support**.

Step 8 In the **Create Tech Support** screen, complete the required fields, including the following:

Name	Description
Destination Type drop-down list	Select a destination for the support data. It can be one of the following: • Remote—Implies an external server • Local—Implies the current system.

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 uploading 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 9 Click **Submit**.

Configuring Email Alert Rules

Procedure

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

Step 2 On the **System** page, click **Email Alert Rules**.

Step 3 Click **Add**.

Step 4 In the **Add Email Alert Rule** screen, complete the required fields, including the following:

Field	Description
Name field	A unique name for the email alert rule.
Alert Scope drop-down list	Choose if the alert rule applies to a system, server groups or servers.
Server Groups field	Click **Select** to check the check boxes of the server groups that email alerts should be sent for. This field is displayed only when **Server Group** is selected in the **Alert Scope** drop-down list.

Field	Description
Servers field	Click **Select** to check the check boxes of the servers that email alerts should be sent for. This field is displayed only when **Server** is selected in the **Alert Scope** drop-down list.
Email Addresses field	The email address of the recipients of the email. You can enter multiple email addresses, separated by commas.
Severity field	Click **Select** to check the check boxes of the severity levels for which the email alert must be triggered.
Enable Alert check box	Check this check box to enable the alert rule immediately.
Send alert for all faults every 24 hours check box	Check this check box to send email alerts once every 24 hours. This email alert will contain all active and open faults based on the configured email alert rule.

Step 5 Click **Submit**.

Server Diagnostics

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 SFTP user password to run server diagnostics. To configure the SFTP user password, see Configuring SFTP User Password, on page 113.

Configuring Server Configuration Utility Image Location

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

Procedure

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

Step 2 On the **Physical Accounts** page, click **SCU Images Profiles**.

Step 3 Click **Add**.

Step 4 In the **Configure SCU Image Location** screen, complete the required fields, including the following:

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

Step 5 Click **Save**.

Running Diagnostics

Perform this procedure when you want to run diagnostics for servers or server groups. Running diagnostics on servers will result in the selected servers being restarted.

Procedure

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

Step 2 On the **Physical Accounts** page, click **Server Diagnostics**.

Step 3 Click **Run Diagnostics**.

Step 4 In the **Run Diagnostics** screen, complete the required fields, including the following:

Field	Description
Select Profile drop-down list	Choose a diagnostics profile from the list.
Server(s) drop-down list	Click **Select** to check the check boxes of the server groups for which you want to run the diagnostics.

Step 5 Click **Submit**.

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

- Select a server and click **View Report** to view reports.
- Select a server or multiple servers and click **Delete Report** to delete reports.
- Select a server or multiple servers and click **Download Report** to download reports. When you select multiple servers to download diagnostics reports, a zip file containing all the reports are downloaded.

You cannot choose a server which is already running a diagnostics operation. Wait for the diagnostics operation to complete before triggering another diagnostics on this server.

Diagnostics may take around 40 minutes to complete. This varies depending on the number of components present in the server.

Configuring SFTP User Password

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

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

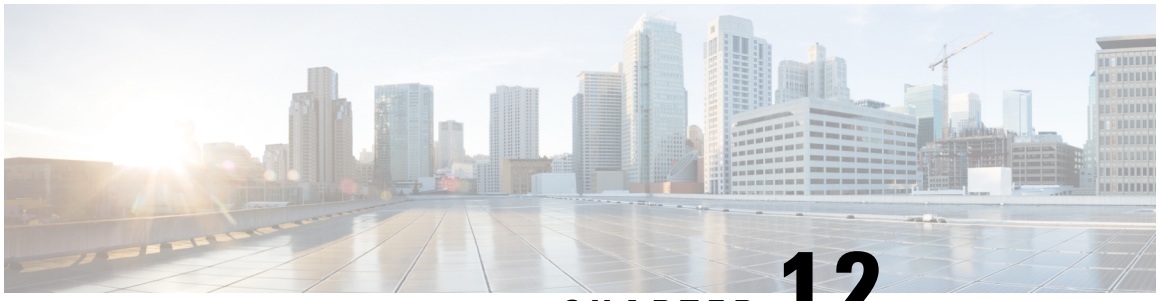
Procedure

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

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

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

Step 4 Click **Submit**.



CHAPTER 12

Using Orchestration Workflows

Orchestration Workflows for Rack Servers

Cisco UCS Director includes orchestration features that allow you to create workflows to automate the configuration and management of tasks that are typically managed by Cisco Integrated Management Controller (Cisco IMC). Some tasks, such as associating a rack server profile with a rack server or adding a vNIC or a vHBA to a rack-mount server, can only be done through a workflow.

For an example of a workflow for a rack server, see Sample Workflow: Power Cycling a Rack Server, on page 116. For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

Orchestration Tasks for Rack Servers

Cisco UCS Director provides some orchestration tasks in the Task Library that you can include in workflows.

Location of Orchestration Tasks

A complete list of the Cisco IMC orchestration tasks is available in the Workflow Designer and the Task Library. The Task Library includes a description of the orchestration tasks. It can be accessed from the following locations in Cisco UCS Director:

- **Policies** > **Orchestration** > **Workflows**
- `http://IP_address/app/cloudmgr/onlinedocs/cloupiaTaskLib.html` where *IP_address* is the IP address of Cisco UCS Director.

In the Workflow Designer, you can access these tasks to add them to a workflow from the **Available Tasks** pane through **Physical Compute Tasks** > **Rack Server Tasks**.

Types of Orchestration Tasks

The Cisco IMC orchestration tasks include tasks to configure and manage the following:

- Power On/Power Off CIMC Server
- Configure Rack Server
- Unconfigure Rack Server
- Select Rack Server

Note These Cisco IMC orchestration tasks are currently not supported on Cisco UCS S3260 servers.

Sample Workflow: Power Cycling a Rack Server

You can create workflows to automate many configuration and management tasks for rack servers. The following sample workflow power cycles a rack-mount server. You can find detailed information about each workflow task in the Task Library.

Workflow Task	Inputs	Outputs
Power On/Off CIMC Server	User input: • **Manage Workflow User Inputs**—Add **CIMC Server Identity** as a user input. • **CIMC Server**—Check the **Map to User Input** check box and choose the label you assigned to **CIMC Server Identity** to enable the user to choose a server. Task input—Choose **Power Off**, **Power On** or **Reset** to perform respective power operation on the selected server.	Server identity, including information about the MAC address, VLAN, and WWPN of the vHBA.

Workflow Task	Inputs	Outputs
Configure Rack Server	User inputs: • **Manage Workflow User Inputs**—Add **CIMC Rack Server Profile Selector** and **CIMC Server Identity** as user input. • Check the **Map to User Input** check box and choose the label you assigned to **Rack Server Profile Selector** to enable the user to choose the rack server profile to be associated with the server. • **Select Rack Server**—Check the **Map to User Input** check box and choose the label you assigned to **CIMC Server Identity** to enable the user to choose a server. Task inputs: • **Policy Type**— Choose the type of policy to be applied to the server from the profile. • **Rack Server Profile**—Choose the rack server profile that includes the policy type that you selected. • **Select Rack Server**— Choose the rack server to which the policy type must be applied. The selected policy type from the profile is applied on the rack server.	Server identity, including information on the server profile identity, MAC address, VLAN and WWPN of the vHBA.
Unconfigure Rack Server	User input: • **Select Rack Server**—Check the **Map to User Input** check box and choose the label you assigned to **Rack Server Identity** to enable the user to choose a server. Task input—None.	Server identity.