Cisco UCS Director Management Guide for Rack Servers, Release 5.5

First Published: June 14, 2016

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

CONTENTS

Preface

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`.

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

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

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

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

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

Warning

IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

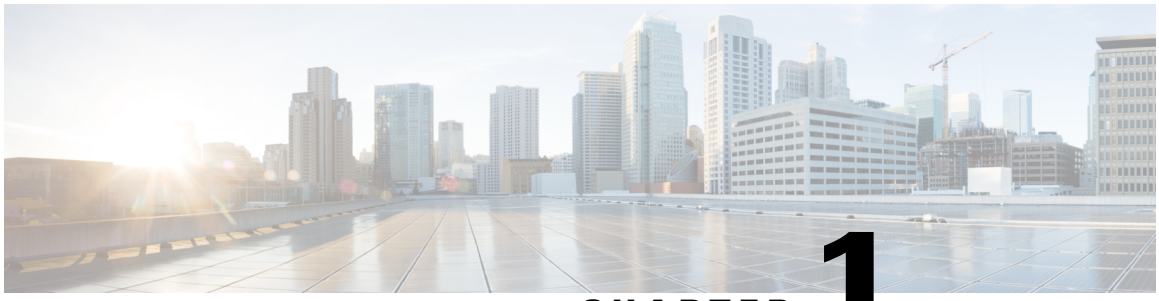
Documentation Feedback

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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following section:

New and Changed Information for this Release

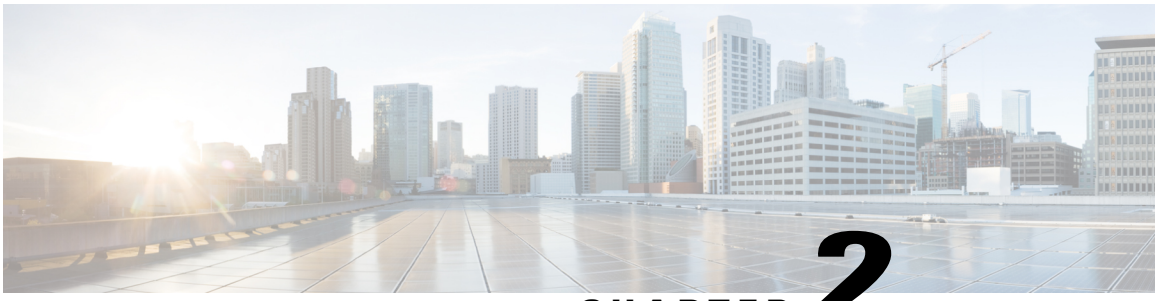
The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco UCS Director, Release 5.5

Feature	Description	Where Documented
Support for creating schedules	Defining a schedule allows you to defer certain tasks to occur at a different time. Tasks such as firmware updates or server discovery can be scheduled to run at a pre-defined time or at a pre-defined interval.	Overview of Managing Schedules, on page 22 Performing Auto Discovery, on page 11
Support for creating a FlexFlash Policy	This policy allows you to configure and enable the SD card on a rack server.	FlexFlash Policy, on page 31
Support for Server Diagnostics	Server diagnostics is available through UCS Server Configuration Utility (UCS-SCU). You can use diagnostics tools to diagnose hardware problems with your Cisco servers and run tests on various server components to find out hardware issues along with analysis of the test results in a tabular format.	Overview of Server Diagnostics, on page 63

New and Changed Information for this Release

Feature	Description	Where Documented
Support for uploading firmware images	You can upload a firmware image from your local file system to the Cisco UCS Director system.	Uploading Images from a Local File System, on page 53
Support for uploading tech support logs to a server	You can upload tech support logs to a local server or to a remote server.	Uploading Technical Support Data to a Server, on page 61
Configuring email alerts for faults	You can create email alert rules in the system for faults on the rack servers.	Configuring Email Alert Rules, on page 62



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:

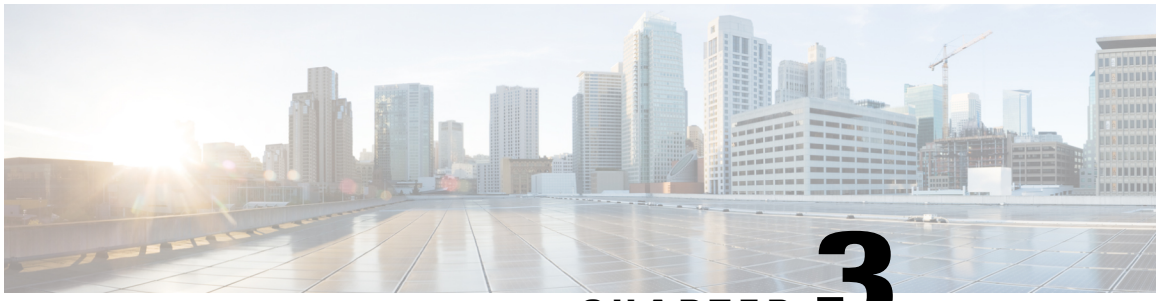
- Power consumption
- Temperature
- Rack server profile association

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 On the menu bar, choose **Administration** > **Physical Accounts**.

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

Step 3 Click **Create**.

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

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

Step 5 Click **Create**.

Step 6 Click **OK**.

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 On the menu bar, choose **Administration** > **Physical Accounts**.
Step 2 Click the **Rack Accounts** tab.
Step 3 In the table, click the row of the account for which you want to test the connection.
Step 4 Click **Test Connection**.
Step 5 In the **Test Connection** dialog box, click **Submit**.
Step 6 When the connection test has completed, click **Close**.

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 On the menu bar, choose **Administration** > **Physical Accounts**.
Step 2 Click the **Rack Groups** tab.
Step 3 In the table, click the row of the group that you want to assign to a pod.
Step 4 Click **Assign Pod**.
Step 5 In the **Assign Pod** dialog box, 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 On the menu bar, choose **Administration** > **Physical Accounts**.

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

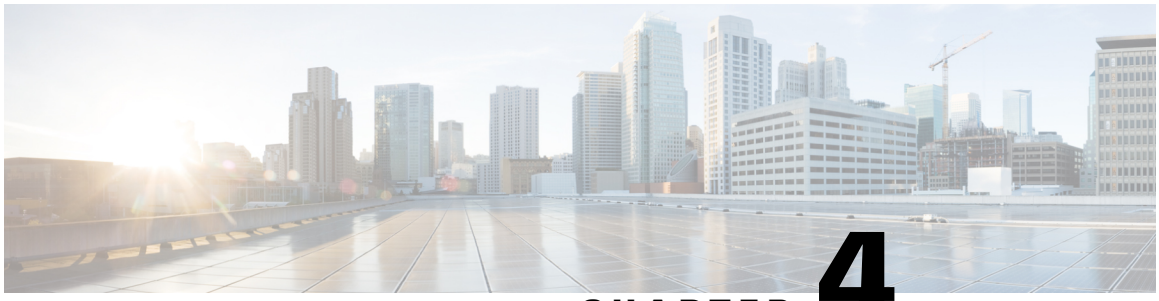
Step 3 In the table, click the row of the account for which you want to run the inventory.

Step 4 Click **Inventory**.

Step 5 In the **Inventory** dialog box, click **Inventory**.

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

Step 7 When the connection test has completed, click **Close**.



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 11.
Step 3	Import the servers.	Refer Importing One or More Rack Servers, on page 12.
Step 4	Delete a discovery profile.	(Optional) Refer Deleting Auto Discovery Profile, on page 13.
Step 5	Clear a server from the auto discovered list.	(Optional) Refer Clearing Auto Discovery List, on page 13.

Configuring a Rack Discovery Profile

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

Procedure

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

Step 2 Click the **Rack Server Discovery Profile** tab.

Step 3 Click **Add**.

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

Field	Description
Profile Name field	A descriptive name for the profile.
Search Criteria drop-down list	Select **IP Address Range**, **Subnet Mask Range**, **IP Address CSV File** or **IP Address List** from the drop-down list.
If you select **IP Address Range**	
Starting IP field	Valid IP address
Ending IP field	Valid IP address
If you select **Subnet Mask Range**	

Field	Description
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 **Browse** and navigate to a .csv file which contains the IP addresses.
If you select **IP Address List**	
IP Addresses field	Enter multiple IP addresses separated by comma.
Use Credential Policy checkbox	If you have already created credential policies, then check this box to select the policy from the drop-down list.
If you check **Use Credential Policy** checkbox	
Credential Policy drop-down list	Choose a policy from the drop-down list or click the + icon and create new policy.
If you uncheck **Use Credential Policy** checkbox	
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.

Step 5 Click **Submit**.

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

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

Step 2 Click the **Rack Server Discovery** tab.

Step 3 Click **Discover**.

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

Step 5 (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 23.

Step 6 Click **Submit**.

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

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

Step 2 Click the **Rack Server Discovery** tab.

Step 3 Click **Import**.

Step 4 In the **Import Discovered Devices** dialog box, complete the following:

Field	Description
Select Device(s) field	Click **Select** to choose the devices to import. Check the check boxes of all the servers you want to import.
User Prefix field	Enter a prefix for the user.

Field	Description
Description field	Enter a description for the user.
Contact field	Enter the contact details for the user.
Location field	Enter the location details for the user.
Select Rack Group drop-down list	Choose from the list of existing rack groups or create a new rack group.

Step 5 Click **Submit**.

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

Clearing Auto Discovery List

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

Before You Begin

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

Procedure

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

Step 2 Click the **Rack Server Discovery** tab.

Step 3 Click **Clear**.

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

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

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

Step 6 Click **Select**.

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

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

Deleting Auto Discovery Profile

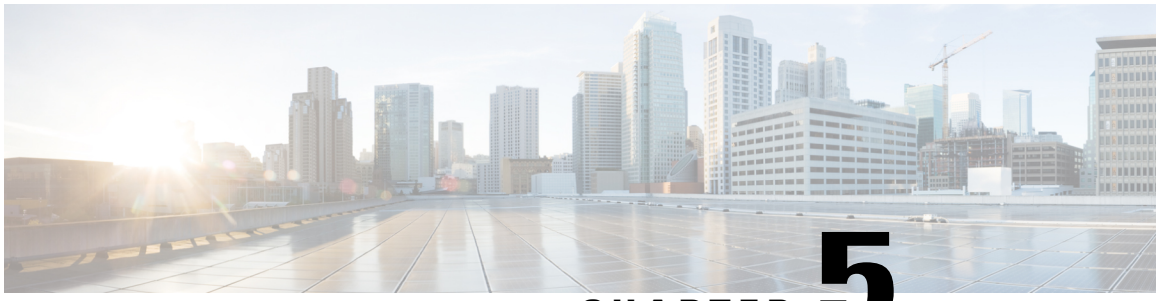
Perform this procedure when you want to delete an automatic discovery profile.

Before You Begin

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

Procedure

Step 1 On the menu bar, choose **Administration** > **Physical Accounts**.
Step 2 Click the **Rack Server Discovery Profile** tab.
Step 3 Select a profile.
Step 4 In the **Delete Discovery Profile** dialog box, click **Submit**.
Step 5 In the confirmation dialog box, click **OK**.



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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

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

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

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

The following details are available for a rack mount server:

Tab	Description
Summary	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.
Users	Displays the list of users for the server.

Tab	Description
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.
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.
Associated Hardware Profiles	Displays the server profiles that are associated with the server.

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

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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

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

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

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

The following details are available for a rack mount server:

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

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

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 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.
Step 3 In the right pane, click the **Rack Servers** tab.
Step 4 Select the server from the list.
Step 5 Click **Set Label**.
Note You cannot see **Set Label** button till you select the server from the list.
Step 6 Enter a new label.
Step 7 Click **Submit**.
Step 8 In the **Submit Result** dialog box, click **OK**.

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 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.
Step 3 In the right pane, click the **Rack Servers** tab.
Step 4 Select the sever from the list.
Step 5 Click **Locator LED**.

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

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

Step 7 Click **Submit**.

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

Powering On a Rack Server

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of 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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of 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 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.
Step 3 In the right pane, click the **Rack Servers** tab.
Step 4 Select the sever from the list.
Step 5 Click **Hard Reset**.
Note You cannot see the **Hard Reset** button till you select the server from the list.
Step 6 In the confirmation dialog box, click **OK**.

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 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.
Step 3 In the right pane, click the **Rack Servers** tab.
Step 4 Select the sever from the list.
Step 5 Click **Shut Down**.
Note You cannot see **Shut Down** button till you select the server from the list.
Step 6 In the confirmation dialog box, click **OK**.

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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of the server for which you want to start the KVM console.

Step 5 Click **KVM Console**.

Step 6 Click **Submit**.
Cisco UCS Director downloads the `kvm.jlp` file to your system.

Step 7 Double-click the `kvm.jlp` file in your Downloads folder.
The KVM Console opens in a separate window.

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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

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

Step 4 Select the sever from the list.

Step 5 Click **Launch GUI**.

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

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

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 On the menu bar, choose **Adminstration** > **System**.

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

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

- **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** dialog box, do the following: **1** From the **Task Execution** drop-down list, choose **Enable** or **Disable**. **2** From the **System Task Policy** drop-down list, choose **default-system-task-policy** or **local-run-policy**. **3** To set the frequency at which the task needs to be executed, choose the number of hours from the **Hours** drop-down list. **4** Click **Submit**.
Run Now	Runs the task.
View Details	Displays the history for the system task.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Schedules** tab.

Step 3 Click **Add**.

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

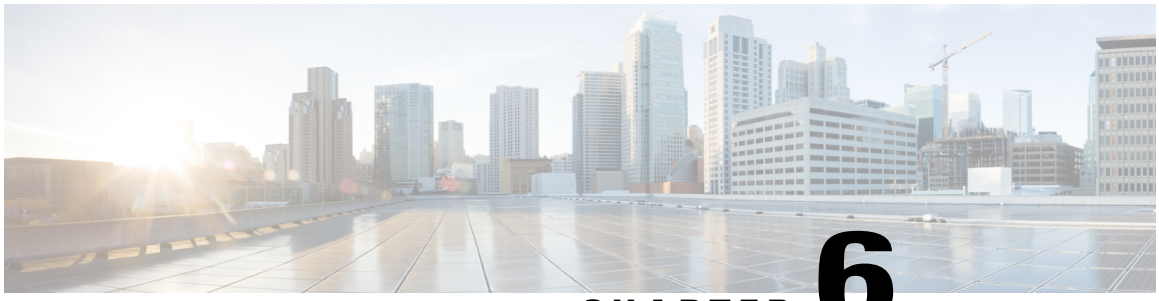
Field	Description
Schedule Name field	Enter a name for the schedule task.
Enable Schedule check box	Check this check box to enable a schedule. By enabling or disabling a schedule (using the **Enable** or **Disable** options), you can enable or disable the tasks associated with the schedule from running.
Scheduler Type radio button	Select a one time schedule or recurring schedule frequency. If you choose a **One Time** schedule, select the date, time, and AM or PM radio buttons. **Note** The schedule time is based on the time on the appliance. However, the time zone is of the local client browser. If you choose a **Recurring** schedule, select the days (0 to 30 days), hours and minutes from the drop-down lists.

Step 5 Click **Submit**.

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

What to Do Next

- You can select an existing schedule and modify, delete, or view scheduled tasks. **View Scheduled Tasks** displays a report which allows you to view the status of the upgrade firmware, 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 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 26.
   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 27.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Policy, on page 45.
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 28.
   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 45.

Creating Server Policies

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

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add**.

Step 4 In the **Add Policy** dialog box, choose a policy type from the drop-down list.
For more information about creating a policy based on the policy type, select the policy type listed in the table below. The various properties required to configure these policies are available in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide. The respective sections in this guide are listed against each policy type.

Policy	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 29	*Configuring BIOS Settings*
Disk Group Policy	Creating a Disk Group Policy, on page 30	*Managing Storage Adapters*
FlexFlash Policy	FlexFlash Policy, on page 31	*Managing the Flexible Flash Controller*
IPMI over LAN Policy	Creating an IPMI Over LAN Policy, on page 34	*Configuring IPMI*
LDAP Policy	Creating an LDAP Policy, on page 35	*Configuring the LDAP Server*
Legacy Boot Order Policy	Creating a Legacy Boot Order Policy, on page 36	*Server Boot Order*
Network Security Policy	Creating a Network Security Policy, on page 36	*Network Security Configuration*
Network Time Protocol Policy	Creating an NTP Policy, on page 37	*Configuring Network Time Protocol Settings*
Precision Boot Order Policy	Creating a Precision Boot Order Policy, on page 38	*Configuring the Precision Boot Order*

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 39	*Managing Storage Adapters*
Serial Over LAN Policy	Creating a Serial Over LAN Policy, on page 40	*Configuring Serial Over LAN*
SNMP Policy	Creating an SNMP Policy, on page 40	*Configuring SNMP*
SSH Policy	Creating an SSH Policy, on page 41	*Configuring SSH*
User Policy	Creating a User Policy, on page 42	*Configuring Local Users*
VIC Adapter Policy	Creating a VIC Adapter Policy, on page 43	*Viewing VIC Adapter Properties*
Virtual KVM Policy	Creating a Virtual KVM Policy, on page 44	*Configuring the Virtual KVM*
vMedia Policy	Creating a vMedia Policy, on page 45	*Configuring Virtual Media*

What to Do Next

Apply the policy to a server. For more information about applying a policy, see Applying a Policy, on page 45.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

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

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

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

Step 5 In the dialog box that appears, check the **Create policy from current configuration of the server** check box and click **Next**.

Step 6 In the **Server Details** dialog box, check the **Create policy from current configuration of the server** check box. You can use the server details in the following two methods:

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

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

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

Step 7 Click **Next**.
You will return to the **Main** dialog box. Continue with creating a policy following the prompts in the wizard. The fields for each policy vary depending on the policy you are creating in the system.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

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

Step 3 Expand a policy from the left pane 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 45.

Step 5 (Optional) Click **View Details** 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** dialog box, click **Select** and select the policies you want to delete. Click **Select** and **Submit**.
You can delete one or more selected policies even if you have associated the policy with a server. If you try to delete a policy which is associated to a profile, an error occurs.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **BIOS 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

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

Step 7 In the **Advanced** dialog box, choose the BIOS property values from the drop-down lists and click **Next**.

Step 8 In the **Server Management** dialog box, choose the server property values from the drop-down lists and click **Submit**.

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

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 39.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

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

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

Step 6 In the **Virtual Drive Configuration** dialog box, choose the virtual drive properties and click **Next**.

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

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

Step 9 Click **Submit** in the **Main** dialog box.

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

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

FlexFlash Policy

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

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

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

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 In the **Add** dialog box, choose **FlexFlash Policy** from the drop-down list and click **Submit**.

Step 4 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 5 In the **Configure Cards** dialog box, complete the following fields:

Field	Description
Firmware Mode pane	Choose any of the following firmware operating modes: • **Mirror Mode** - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers. • **Util Mode** - In this mode one card with four partitions and one card with a single partition is created. This mode is available only for C220 M4 and C240 M4 servers. • **Not Applicable** - No firmware operating modes are selected. Go to step 5 if you select **Not Applicable**. This mode is available only for C220 M3, C240 M3, C22, C24, and C460 M4 servers.
Partition Name field	The name of the partition.

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

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

Step 6 If you selected **Not Applicable** in the **Details** pane in step 4, complete the following fields:

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

Step 8 In the **Submit Result** dialog box, click **OK**.
You can also select an existing FlexFlash policy from the **Hardware Policies** table and delete, edit, clone, apply or view the apply status by selecting the respective options in the user interface.

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

1. The settings on the server will be set to default.
2. The new settings on the policy will be applied. 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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **IPMI Over LAN 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, complete the following fields.

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.

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

Step 7 Click **Submit**.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **LDAP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, fill in the LDAP properties.

Step 7 Click **Next**.

Step 8 In the **LDAP Servers** dialog box, fill in the LDAP server details.

Step 9 Click **Next**.

Step 10 In the **Group Authorization** dialog box, fill in the group authorization details and click + to add an LDAP group entry to the table.

Step 11 In the **Add Entry to LDAP Groups** dialog box, fill in the group details.

Step 12 Click **Submit**.

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

Step 14 Click **Submit** in the **Group Authorization** dialog box.

Step 15 In the **Submit Result** dialog box, click **OK**.

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 38.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **Legacy Boot Order 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, click + and select the device type from the drop-down list. The table lists the devices you have added.
In the **Select Devices** table, select an existing device and click **x** to delete a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

You cannot add the same device type again.

Step 7 Click **Submit** in the **Add Entry to Select Devices** dialog box.

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

Step 9 Click **Submit** in the **Main** dialog box.

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

Note This policy is applicable only for Cisco IMC versions prior to 2.0. An error message is displayed if the policy is applied to a server running higher Cisco IMC versions. For servers running versions higher than 2.0, you must use the Precision Boot Order policy instead.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **Network Security** 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, check **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 7 Click **Submit**.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **NTP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, check **Enable NTP** check box to enable alternate servers and specify up to 4 NTP servers.

Step 7 Click **Submit**.

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

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **Precision Boot Order 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, check the **UEFI Secure Boot** check box or select the boot mode from the **Configure Boot Mode** drop-down list.

Step 7 Click + and select or enter device details. The table lists the devices you have added.
You can also select an existing device in the **Select Devices** table and click **x** to delete or click edit icon to edit a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

Step 8 Click **Submit** in the **Add Entry to Select Devices** dialog box.

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

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

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **RAID 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, click + to add virtual drives that you want to configure on the server to the **Virtual Drives** list.

Step 7 In the **Add Entry to Virtual Drives** dialog box, enter or select the virtual drive details.
You can either select an existing Disk Group policy from the drop-down list and edit or add a new Disk Group policy to specify local disks. To create a Disk Group policy, refer Disk Group Policy.

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

Step 8 Click **Submit** in the **Add Entry** dialog box.

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

Step 10 Check the **Erase existing Virtual Drives** check box to delete all existing virtual drives on the server.
If you select this check box, all existing virtual drives on the server will be deleted when the policy is applied. This results in loss of existing data.

Step 11 Check the **Configure remaining disks as JBOD** check box to configure the remaining disks as JBOD.
This option is applicable only on storage controllers that support JBOD. The disks that are not used for virtual drives or hotspares are configured as JBOD.

Step 12 Click **Submit** in the **Main** dialog box.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **Serial Over LAN 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, check the **Enable SoL** check box and select the **CoM Port** and **Baud Rate** values from the drop-down list or use the existing values.

Step 7 Click **Submit**.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **SNMP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **SNMP Users** dialog box, click + to add a SNMP user and fill in the user details. You can use the + icon to add up to 15 SNMP Users.
Select an existing SNMP entry to edit or delete an entry from the table.

Step 7 Click **Next**.

Step 8 In the **SNMP Traps** dialog box, click + to add a SNMP trap and fill in the trap details. You can use the + icon to add up to 15 SNMP Traps.
Select an existing SNMP entry to edit or delete an entry from the table.

Step 9 Click **Next**.

Step 10 In the **SNMP Settings** dialog box, configure the SNMP properties.

Step 11 Click **Submit**.

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

Note
- Any existing **SNMP Users** or **SNMP Traps** configured previously on the server are removed and replaced with users or traps that you configured in the policy. If you have not added any users or traps into the policy, the existing users or traps on the server are removed but not replaced.
- The **SNMP Port** cannot be configured on a 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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **SSH 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, check the **Enable SSH** check box, and enter SSH properties or use the existing properties.

Step 7 Click **Submit**.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **User 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, you can add users that need to be configured on the server to the **Users** list.

Step 7 Click + to add a user.

Step 8 In the **Add Entry to Users** dialog box, complete the following fields:

Field	Description
Username field	Enter a name for the user in the field.

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

Step 9 Click **Submit**.

Step 10 In the **Submit Result** dialog box, click **OK**.
You can also select an existing user from the **Users** table in the **Main** dialog box and click **Edit** or **Delete** icons to edit or delete a user.

Note
- The first user in the **Users** table is the admin user. You cannot delete this admin user but 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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **VIC Adapter 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, click + to add a VIC adapter entry in the table.

Step 7 In the **Add Entry to VIC Adapters** dialog box, enter or select the adapter details.

- **vNIC** - default properties are eth0 and eth1. You can only edit these properties and cannot delete them. These properties are also available for usNIC properties.
- **vHBA** - default properties are fc0 and fc1. You can only edit these properties and cannot delete them.

Step 8 Click **Submit**.

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

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

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **Virtual KVM 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 Check the **Enable vKVM** check box.

Step 7 In the **Max Sessions** drop-down list, choose a number to indicate the maximum number of KVM sessions.

Step 8 In the **Remote Port** field, specify the port number.

Step 9 Check the **Enable Video Encryption** check box.

Step 10 Check the **Enable Local Server Video** check box.

Step 11 Click **Submit**.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

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

Step 4 In the **Add** dialog box, choose **vMedia 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 27.

Step 6 In the **Main** dialog box, check the **Enable vMedia** check box to enable vMedia and check the **Enable Virtual Media Encryption** for enabling vMedia encryption.

Step 7 Click **Next**.

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

Step 9 Click **Next**.

Step 10 Check the Add **HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 11 Click **Submit**.

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

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.

Applying a Policy

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

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 Choose the **Hardware Policies** tab.
Step 3 Select a policy you want to apply from the left pane.
Step 4 Click **Apply** from the options available at the top.
Step 5 In the **Apply Policy** dialog box, choose the server or server group from the drop-down list based on whether you want to apply the policy to individual servers or an entire rack server group.
Step 6 Click **Select** to select the server groups or servers to which you want to apply the policy.
Step 7 Click **Submit**.
Step 8 In the **Submit Result** dialog box, click **OK**.
The process of applying the policy to the specified set of servers begins. This process can take a few minutes depending on the policy type and network connectivity to 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 associated with or applied to a server.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 Choose the **Hardware Policies** tab.
Step 3 Click **Delete**.
Step 4 In the **Delete Policy** dialog box, click **Select** to 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 47.

   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 48.

2 Apply the profile on a server. For more information about applying a profile, see Applying a Server Profile, on page 49.

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 49.

Creating a Server Profile

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

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

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

Step 3 Click **Add**.

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

Step 5 Click **Next** or check **Create profile from current configuration of the server** check box and click **Next**. To perform the tasks in the **Server Details** pane, see Creating a Profile from an Existing Configuration, on page 48.

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

Step 7 In the **Add Entry to Profile Name** dialog box, choose the **Policy Type**.

Step 8 Select the policy name from the **Policy Name** drop-down list which lists the names of policies you have already created.
You can click the + next to **Policy Name** to create a new policy based on the policy type you have selected earlier. For more information about creating policies, see Creating Server Policies, on page 26.

Step 9 Click **Submit**.

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

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

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

What to Do Next

You can also edit, delete, clone a profile and also view the server mapped to a selected profile. For performing these tasks, see Common Tasks Under Server Profiles, on page 49

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

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

Step 3 Click **Add**.

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

Step 5 Check the **Create profile from current configuration of the server** check box. You can use the server details in the following methods:

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

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

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

c) Click **Select**, choose the policies, and click **Select**.

Step 6 Click **Next**.

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

Step 8 Click **Submit**.

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

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

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

Step 3 Expand the Hardware Profile in the left pane 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** dialog box.
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 49.

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 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

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

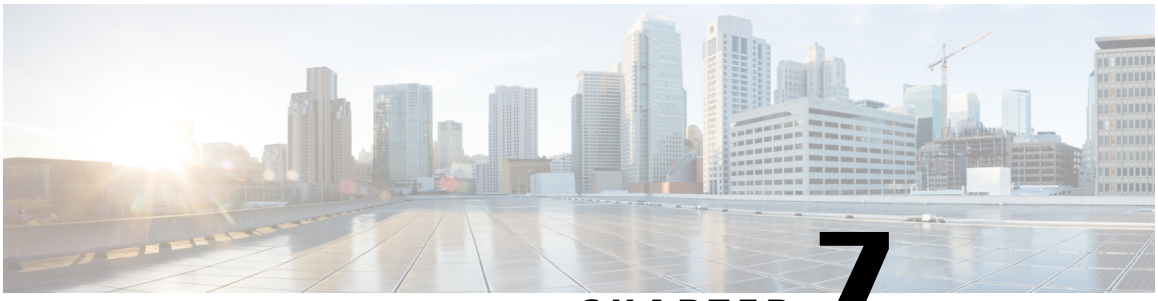
Step 3 Select an existing server profile and click **Apply**.

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

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

Step 6 Click **Submit**.

Step 7 In the **Submit Result** confirmation dialog box, click **OK**.
The process of applying a profile to the specified set of servers begins. This process can take a few minutes depending on the profile type and network connectivity to server(s) to which the profile is being applied.



CHAPTER 7

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 Server, on page 52

- Profile for firmware images stored on the network.

  For more information on creating this profile, see Adding Images from a Network Server, on page 54

Adding Images to a Local Server

Procedure

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

Step 2 Choose the **Images - Local** tab.

Step 3 Click **Add**.

Step 4 In the **Add Firmware Image - Local** dialog box, complete the following fields:

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.
User Name (cisco.com) field	Enter your Cisco login user name.
Password (cisco.com) field	Enter your Cisco login password.
Enable Proxy Configuration check box	(Optional) Check this check box to enable proxy configuration and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.
Enable Proxy Authentication check box	(Optional) Check this check box to enable proxy authentication and complete the following: • **Proxy User Name** field - Enter a proxy user name for the proxy authentication. • **Proxy Password** field - Enter the password for the proxy user name.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server is listed here.
Available Image drop-down list	Choose the .iso image from the drop-down list.
Download Now check box	Check this check box to download the .iso image immediately after adding a profile. If not, you can click on **Download Image** to download the image later.

Field	Description
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**.

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

Note
- You can click **View Location Details** to view profile configuration details, click **Modify** to modify the firmware image details, and click **Delete Profile** to delete the image profile. You can select multiple profiles concurrently and delete them.
- 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 From the menu bar, choose **Systems** > **Firmware Management**.

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

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

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

Step 4 Click **Upload**.

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

Step 6 Click **Submit**.

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

Adding Images from a Network Server

Procedure

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

Step 2 Choose the **Images - Network** tab.

Step 3 Click **Add**.

Step 4 In the **Add Firmware Image - Network** dialog box, complete the following:

Field	Description
Profile Name field	A descriptive and unique name for the profile. The profile name must be unique across both Local and Network image profiles.
Platform drop-down list	Choose a platform from the drop-down list. Only platforms that manage at least one server is listed here.
Server Type drop-down list	Choose either Network File System (NFS) 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.

Step 5 Click **Submit**.

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

Note You can click **View Location Details** to view profile configuration details, click **Modify** to modify the firmware image details, and click **Delete Profile** to delete the image profile. You can 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 On the menu bar, choose **Administration** > **Physical Accounts**.

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

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

Step 4 Click **OK** to confirm.

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

Field	Description
Select Profile drop-down list	Choose a profile from the drop-down list.
Server(s) button	Click **Select** and choose the servers from the list. The list displays only those servers whose platform matches the one configured in the selected profile.
Schedule later check box	Check this check box and select an existing schedule to run an upgrade. You can also click on + icon to create a new schedule. For more information on creating schedules, see Creating Schedules, on page 23. You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to verify the scheduled task and its progress. You can also select a scheduled task and click **Remove Scheduled Tasks** to remove the associated scheduled task.

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

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

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 On the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Choose the **Images - Local** tab.

Step 3 Select a profile from the table.

Step 4 Click **Delete Image**.

Step 5 In the **Delete Image(s)** dialog box, 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 On the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Choose the **Images - Local** tab or the **Images - Network** tab.

Step 3 Select a profile from the table.

Step 4 Click **Delete Profile**.

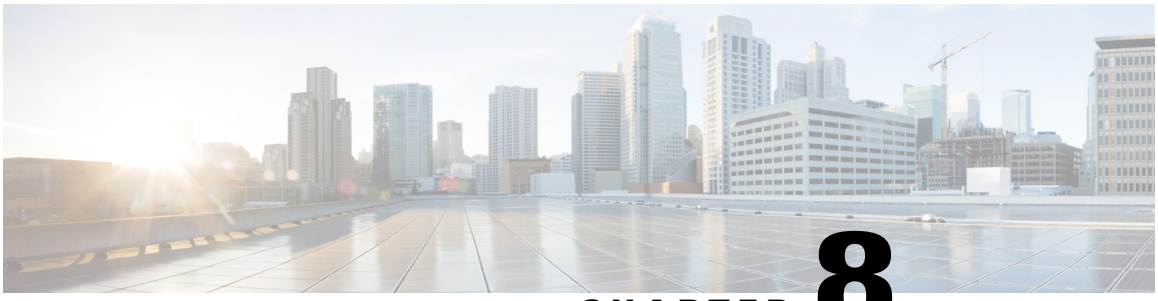
Step 5 In the confirmation dialog box, click **Delete**.

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 On the menu bar, choose **Administration** > **Physical Accounts**.
Step 2 Click the **Firmware Upgrades** tab.
Step 3 Click **Delete Upgrade Status**.
Step 4 Click **Submit**.
Step 5 Click **OK**.



CHAPTER 8

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 62.

Monitoring a Rack Server and Its Components

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of the server that you want to monitor.

Step 5 Click **View Details**.
By default, the **Summary** tab is displayed.

Step 6 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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of the server for which you want to view reports.

Step 5 In the right pane, click the **Summary** tab to view a wide array of tabular, graphical, and map reports that provide a view of trending data for the account.

Step 6 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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

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

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

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

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

Step 7 (Optional) In the **Clear IMC SEL Logs** dialog box, check the **Delete historical logs from Cisco UCS Director** check box.
Selecting this option clears the system event logs from the Cisco UCS Director GUI.

Step 8 Click **Submit**.

Uploading Technical Support Data to a Server

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

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

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

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

Step 6 Click **Create Tech Support**.

Step 7 In the **Create Tech Support** dialog box, complete the following fields:

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 8 Click **Submit**.

Configuring Email Alert Rules

Procedure

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

Step 2 Choose the **Email Alert Rules** tab.

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

Step 4 In the **Add Email Alert Rule** dialog box, complete the following fields:

Field	Description
Name field	A unique name for the email alert rule.
Alert Level drop-down list	Choose if the alert rule applies to a system or a server group.

Field	Description
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 Level** drop-down list.
Email Address 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.

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 scpuser password to run server diagnostics. To configure the scpuser password, see Configuring an SCP User Password, on page 65.

Configuring Server Configuration Utility Image Location

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

Procedure

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

Step 2 Choose the **Server Diagnostics** tab.

Step 3 Click **Configure SCU Image Location**.

Step 4 In the **Configure SCU Image Location** dialog box complete the following:

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

Step 5 Click **Save**.

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

Running Diagnostics

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

Procedure

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

Step 2 Choose the **Server Diagnostics** tab.

Step 3 Click **Run Diagnostics**.

Step 4 In the **Run Diagnostics** dialog box, complete the following:

Field	Description
Choose drop-down list	Choose whether you want to run diagnostics on a server or server group from the drop-down list.

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

Step 5 Click **Select** and select the servers or server groups from the **Select** dialog-box.

Step 6 Click **Select**.
The selected servers or server groups are displayed next to the **Server(s)** or **Server Group(s)** field.

Step 7 Click **Submit**.

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

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

- Select a server and click **View Report** to view reports.
- Select a server or multiple servers and click **Delete Report** to delete reports.
- Select a server or multiple servers and click **Download Report** to download reports. When you select multiple servers to download diagnostics reports, a zip file containing all the reports are downloaded.

You cannot choose a server which is already running a diagnostics operation. Wait for the diagnostics operation to complete before triggering another diagnostics on this server.

Diagnostics may take around 40 minutes to complete. This varies depending on the number of components present in the server.

Configuring an SCP User Password

An SCP user is used by server diagnostics and tech support upload operations for transferring files to the Cisco IMC Supervisor appliance using the SCP protocol. An scp user account cannot be used to login to the Cisco IMC Supervisor UI or the shelladmin. You must create an SCP user using Putty, and then log in to the user interface to set a password.

Complete this procedure to configure a password for an SCP user.

Procedure

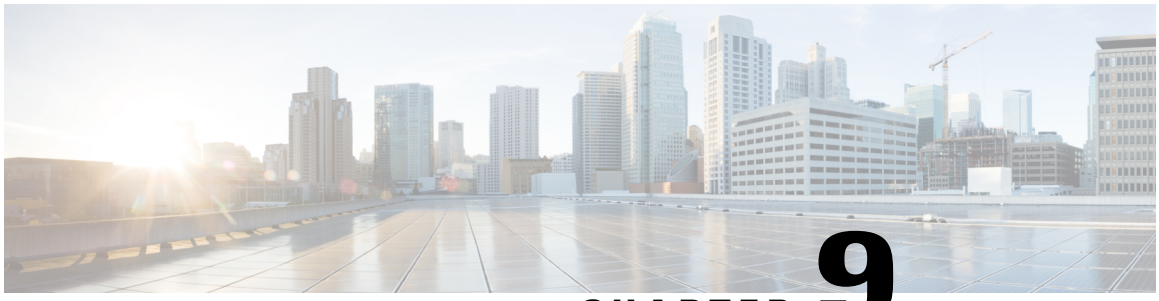
Step 1 From the menu bar, choose **Administration** > **Users and Groups**.

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

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

Step 4 Click **Submit**.

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



CHAPTER 9

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 68. 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

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.

Workflow Task	Inputs	Outputs
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.