Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide for C22 M3, C24 M3, C220 M3 and C240 M3 Servers, Release 3.0

First Published: 2016-12-13

Last Modified: 2017-04-19

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

CONTENTS

Preface

This preface includes the following sections:

Audience

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

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.

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

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

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

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

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

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 Cisco UCS Documentation

Documentation Roadmaps

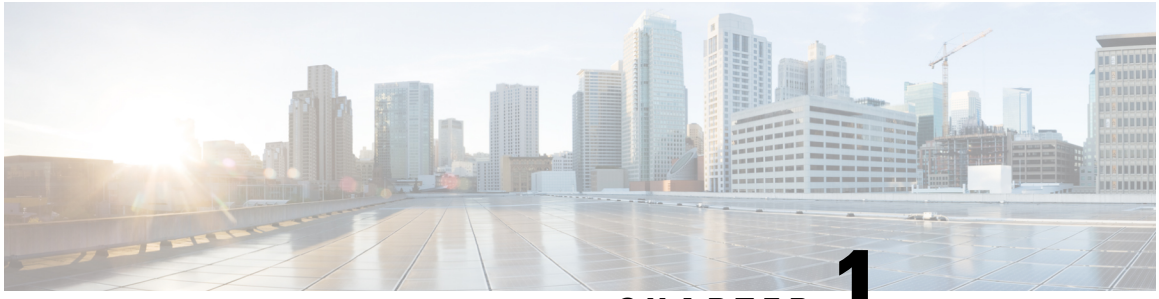
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.



CHAPTER 1

Overview

This chapter includes the following sections:

Overview of the Cisco UCS C-Series Rack-Mount Servers

The Cisco UCS C-Series rack-mount servers include the following models:

- Cisco UCS C22 M3 Rack-Mount Server
- Cisco UCS C24 M3 Rack-Mount Server
- Cisco UCS C220 M3 Rack-Mount Server
- Cisco UCS C240 M3 Rack-Mount Server

Note To determine which Cisco UCS C-Series rack-mount servers are supported by this firmware release, see the associated *Release Notes*. The C-Series release notes are available at the following URL: http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Overview of the Server Software

The Cisco UCS C-Series Rack-Mount Server ships with the Cisco IMC firmware.

Cisco IMC Firmware

Cisco IMC is a separate management module built into the motherboard. A dedicated ARM-based processor, separate from the main server CPU, runs the Cisco IMC firmware. The system ships with a running version of the Cisco IMC firmware. You can update the Cisco IMC firmware, but no initial installation is needed.

Server OS

The Cisco UCS C-Series rack servers support operating systems such as Windows, Linux, Oracle and so on. For more information on supported operating systems, see the *Hardware and Software Interoperability for Standalone C-series servers* at http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html. You can use Cisco IMC to install an OS on the server using the KVM console and vMedia.

Cisco Integrated Management Controller

The Cisco IMC is the management service for the C-Series servers. Cisco IMC runs within the server.

Note The Cisco IMC management service is used only when the server is operating in Standalone Mode. If your C-Series server is integrated into a UCS system, you must manage it using UCS Manager. For information about using UCS Manager, see the configuration guides listed in the *Cisco UCS B-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Management Interfaces

You can use a web-based GUI or SSH-based CLI or an XML-based API to access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in another. However, you cannot do the following:

- Use Cisco IMC GUI to invoke Cisco IMC CLI
- View a command that has been invoked through Cisco IMC CLI in Cisco IMC GUI
- Generate Cisco IMC CLI output from Cisco IMC GUI

Tasks You Can Perform in Cisco IMC

You can use Cisco IMC to perform the following server management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Toggle the locator LED
- Configuring BIOS settings
- Configure the server boot order
- View server properties and sensors
- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI Over LAN, and SNMP.
- Manage certificates
- Configure platform event filters

- Update Cisco IMC firmware
- Monitor faults, alarms, and server status
- Set time zone and view local time
- Install and activate Cisco IMC firmware
- Install and activate BIOS firmware

No Operating System or Application Provisioning or Management

Cisco IMC provisions servers, and as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on servers. For example, you cannot do the following:

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers
- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non-Cisco IMC user accounts
- Configure or manage external storage on the SAN or NAS storage

Overview of the Cisco IMC User Interface

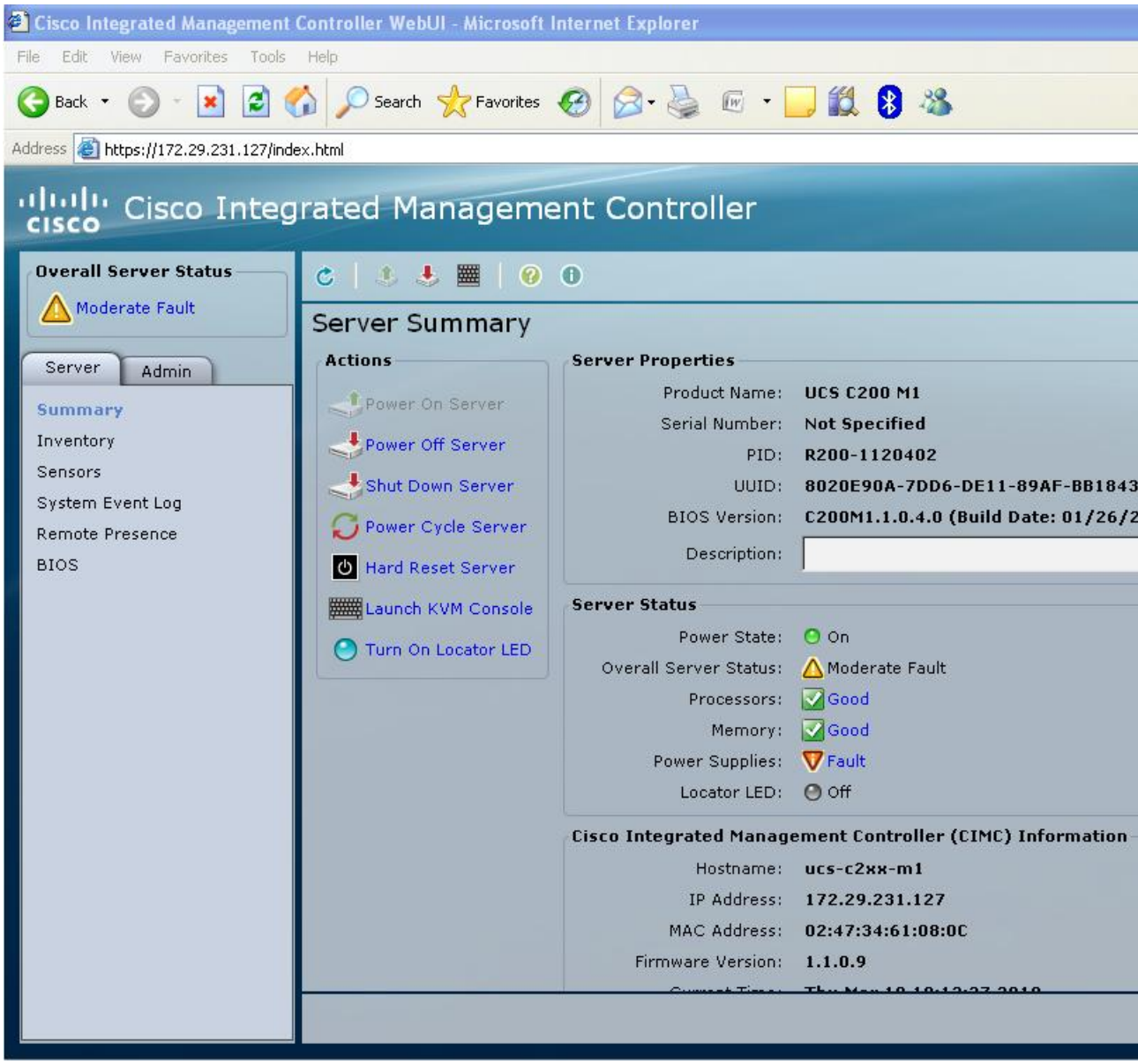
The Cisco IMC user interface is a web-based management interface for Cisco C-Series servers. You can launch the Cisco IMC user interface and manage the server from any remote host that meets the following minimum requirements:

- Sun JRE 1.8.0_ 45 to Sun JRE 1.8.0_ 60
- Microsoft Internet Explorer 6.0 or higher, Mozilla Firefox 3.0 or higher
- Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows Vista, Apple Mac OS X v10.6, Red Hat Enterprise Linux 5.0 or higher operating systems
- Transport Layer Security (TLS) version 1.2.

Note In case you lose or forget the password that you use to log in to Cisco IMC, see the password recovery instructions in the Cisco UCS C-Series server installation and service guide for your server. This guide is available from the *Cisco UCS C-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Cisco IMC Home Page

When you first log into Cisco IMC GUI, the user interface looks similar to the following illustration:



Navigation and Work Panes

The **Navigation** pane displays on the left side of the Cisco IMC GUI. Clicking links on the **Server**, **Admin**, or **Storage** tabs in the **Navigation** pane displays the associated tabs in the **Work** pane on the right.

The **Navigation** pane has the following areas:

- **Overall Server Status** area
- **Server** tab

- **Admin** tab
- **Storage** tab

Overall Server Status Area

The **Overall Server Status** area is above the **Server**, **Admin**, and **Storage** tabs. Click the link in area to refresh the **Server Summary** tab in the **Work** pane.

Note If a different tab is displayed in the **Work** pane, clicking this link redisplays the **Server Summary** tab with updated server information.

Server Tab

Each node in the **Server** tab leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

Server Tab Node Name	Work Pane Tabs Provide Information About...
Summary	Server properties, status, BIOS version, Cisco IMC firmware version, IP address, and MAC address.
Inventory	Installed CPUs, memory cards, power supplies, PCI adapters, Cisco VIC adapters, network adapters, storage adapters, TPM, SAS expander, and PID catalog.
Sensors	Power supply, fan, temperature, voltage, current, LEDs, and storage sensor readings.
Remote Presence	KVM, virtual media, and Serial over LAN settings.
BIOS	The installed BIOS firmware version and the server boot order.
Power Policies	Power policy settings.
Faults and Logs	Fault summary, fault history, system event log, Cisco IMC logs, and logging controls.
Troubleshooting	Bootstrap process recording, crash recording, and player.

Admin Tab

Each node in the **Admin** tab leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

Admin Tab Node Name	Work Pane Tabs Provide Information About...
User Management	Locally-defined user accounts, Active Directory settings, and current user session information.
Network	NIC, IPv4, VLAN, and LOM properties, along with network security settings.

Admin Tab Node Name	Work Pane Tabs Provide Information About...
Communication Services	HTTP, SSH, XML API, IPMI over LAN, and SNMP settings.
Certificate Management	Security certificate information and management.
Event Management	Platform event filters.
Firmware Management	Cisco IMC and BIOS firmware information and management.
Utilities	Technical support data collection, system configuration import and export options, and restore factory defaults settings.

Storage Tab

Each node in the **Storage** tab corresponds to the LSI MegaRAID controllers or Cisco FlexFlash controllers that are installed in theCisco UCS C-Series Rack-Mount Servers. Each node leads to one or more tabs that display in the **Work** pane and provide information about the installed controllers.

Storage Tab Node Name	Work Pane Tabs Provide Information About...
Controller Info	General information about the selected MegaRAID controller or Cisco Flexible Flash controller.
Physical Drive Info	General drive information, identification information, and drive statusl
Virtual Drive Info	General drive information, RAID information, and physical drive information.
Battery Backup Unit	Backup battery information for the selected MegaRAID controller.
Storage Log	Storage messages.

Toolbar

The toolbar displays above the **Work** pane.

Button Name	Description
Refresh	Refreshes the current page.
Power On Server	Powers on the server.
Power Off Server	Powers off the server.
Launch KVM Console	Launches the KVM console.
Ping	Launches the **Ping Details** pane.
Help	Displays the online help for the tab displayed in the **Work** pane.
Info	Displays Cisco IMC information.

Cisco Integrated Management Controller Online Help Overview

The GUI for the Cisco Integrated Management Controller (Cisco IMC) software is divided into two main sections, a **Navigation** pane on the left and a **Work** pane on the right.

This help system describes the fields on each Cisco IMC GUI page and in each dialog box.

To access the page help, do one of the following:

- In a particular tab in the Cisco IMC GUI, click the **Help** icon in the toolbar above the **Work** pane.
- In a dialog box, click the **Help** button in that dialog box.

Note 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.

Logging In to Cisco IMC

Before you begin

If not installed, install Adobe Flash Player 10 or later on your local machine.

Procedure

Step 1 In your web browser, type or select the web link for Cisco IMC.

Step 2 If a security dialog box displays, do the following:

a) (Optional) Check the check box to accept all content from Cisco.

b) Click **Yes** to accept the certificate and continue.

Step 3 In the log in window, enter your username and password.

Tip When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.

The following situations occur when you login to the Web UI for the first time:

- You cannot perform any operation until you change default admin credentials on the Cisco IMC Web UI.
- You cannot close or cancel the password change pop-up window and opening it in a tab or refreshing the browser page will continue to display the pop-up window. This pop-up window appears when you login after a factory reset or upgraded Cisco IMC from 1.5(x) or 2.0(1) version to the latest version.
- You cannot choose the word 'password' as your new password. If this creates problems for any scripts you may be running, you could change it to password by logging back into the user management options, but this is ENTIRELY at your own risk. It is not recommended by Cisco.

Step 4 Click **Log In**.

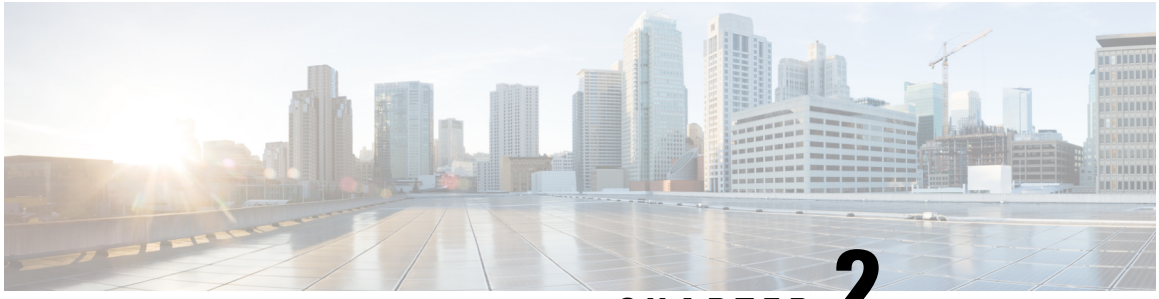
Logging Out of Cisco IMC

Procedure

Step 1 In the upper right of Cisco IMC, click **Log Out**.

Logging out returns you to the Cisco IMC log in page.

Step 2 (Optional) Log back in or close your web browser.



CHAPTER 2

Installing the Server OS

This chapter includes the following sections:

OS Installation Methods

C-Series servers support several operating systems. Regardless of the OS being installed, you can install it on your server using one of the following tools:

- KVM console
- PXE installation server

KVM Console

The KVM console is an interface accessible from Cisco IMC 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.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network
- USB flash drive on the network

You can use the KVM console to install an OS on the server.

Note When launching the KVM Console from Internet Explorer 6 SP1 on Windows Server 2003, the browser will report that it cannot download a required file. If this occurs, click the browser Tools menu and select Internet Options. Click the Advanced tab and, in the Security section, uncheck the checkbox for "Do not save encrypted pages to disk." Launch the KVM Console again.

Installing an OS Using the KVM Console

Note This procedure describes only the basic installation steps. Detailed guides for installing Linux, VMware, and Windows can be found at this URL: http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html.

Before you begin

- Locate the OS installation disk or disk image file.
- You must log in as a user with admin privileges to install an OS.

Procedure

Step 1 Load the OS installation disk into your CD/DVD drive, or copy the disk image files to your computer.

Step 2 If Cisco IMC is not open, log in.

Step 3 In the **Navigation** pane, click the **Server** tab.

Step 4 On the **Server** tab, click **Remote Presence**.

Step 5 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 6 In the **Actions** area, click **Launch KVM Console**.

The **KVM Console** opens in a separate window.

Step 7 From the KVM console, click the **VM** tab.

Step 8 In the **VM** tab, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the CD/DVD drive containing the OS installation disk.
- Click **Add Image**, navigate to and select the OS installation disk image, click **Open** to mount the disk image, and then check the **Mapped** check box for the mounted disk image.

Note You must keep the **VM** tab open during the OS installation process. Closing the tab unmaps all virtual media.

Step 9 Reboot the server and select the virtual CD/DVD drive as the boot device.

When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to do next

After the OS installation is complete, reset the LAN boot order to its original setting. Always follow your OS vendors recommended configuration, including software interoperability and driver compatibility. For more information on driver recommendations and installation, follow the Cisco UCS Hardware Compatibility list here:

https://ucshcltool.cloudapps.cisco.com/public/

PXE Installation Servers

A Preboot Execution Environment (PXE) installation server allows a client to boot and install an OS from a remote location. To use this method, a PXE environment must be configured and available on your VLAN, typically a dedicated provisioning VLAN. Additionally, the server must be set to boot from the network. When the server boots, it sends a PXE request across the network. The PXE installation server acknowledges the request, and starts a sequence of events that installs the OS on the server.

PXE servers can use installation disks, disk images, or scripts to install an OS. Proprietary disk images can also be used to install an OS, additional components, or applications.

Note PXE installation is an efficient method for installing an OS on a large number of servers. However, considering that this method requires setting up a PXE environment, it might be easier to use another installation method.

Installing an OS Using a PXE Installation Server

Before you begin

- Verify that the server can be reached over a VLAN.
- You must log in as a user with admin privileges to install an OS.

Procedure

Step 1 Set the boot order to **PXE** first.

Step 2 Reboot the server.

If a PXE install server is available on the VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to do next

After the OS installation is complete, reset the LAN boot order to its original setting. Always follow your OS vendors recommended configuration, including software interoperability and driver compatibility. For more information on driver recommendations and installation, follow the Cisco UCS Hardware Compatibility list here:

https://ucshcltool.cloudapps.cisco.com/public/

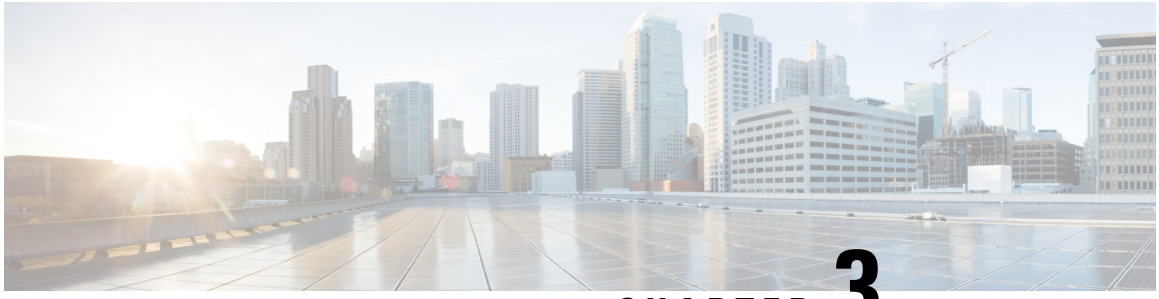
Booting an Operating System from a USB Port

All Cisco UCS C-series servers support booting an operating system from any USB port on the server. However, there are a few guidelines that you must keep in mind, prior to booting an OS from a USB port.

- To maintain the boot order configuration, it is recommended that you use an internal USB port for booting an OS.
- The USB port must be enabled prior to booting an OS from it.

  By default, the USB ports are enabled. If you have disabled a USB port, you must enable it prior to booting an OS from it. For information on enabling a disabled USB ports, see topic *Enabling or Disabling the Internal USB Port* in the server-specific installation and service guide available at the following link:

  http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.
- After you boot the OS from the USB port, you must set the second-level boot order so that the server boots from that USB source every time.



CHAPTER 3

Managing the Server

This chapter includes the following sections:

Viewing Overall Server Status

Procedure

Step 1 In the **Overall Server Status** area of the **Navigation** pane, click the blue health report link to refresh the **Server Summary** pane.

Step 2 (Optional) Review the following information in the **Server Status** area of the **Server Summary** pane:

Note The following list shows all possible status fields. The actual fields displayed depend on the type of C-Series server that you are using.

Name	Description
Power State field	The current power state.
Overall Server Status field	The overall status of the server. This can be one of the following: • **Memory Test In Progress**—The server is performing a self-test of the installed memory. This condition normally occurs during the boot process. • **Good** • **Moderate Fault** • **Severe Fault**
Temperature field	The temperature status. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view more temperature information.
Processors field	The overall status of the processors. This can be one of the following: • **Good** • **Fault** You can click the link in this field to view more information about the processors. **Note** This option is available only on some UCS C-Series servers.
Overall DIMM Status field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Power Supplies field	The overall status of the power supplies. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.

Name	Description
Fans field	The overall status of the power supplies. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
HDD field	The overall status of the hard drives. This can be one of the following: • **Good** • **Fault** You can click the link in this field to view detailed status information. **Note** This option is available only on some UCS C-Series servers.
Locator LED field	Whether the locator LEDs are on or off.
Front Locator LED field	Whether the front panel locator LED on the chassis is on or off. **Note** This option is available only on some UCS C-Series servers.
Overall Storage Status field	The overall status of all controllers. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault**

Viewing a Server Utilization

You can view a server utilization only on some UCS C-Series servers.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 Review the following information in the **Server Utilization** area of the **Server Summary** pane:

Name	Description
Overall Utilization (%) field	The overall realtime utilization of CPU, memory, and IO (input and output) of the system in percentage.
CPU Utilization (%) field	The CPU or computation utilization of the system on all the available CPUs in percentage.
Memory Utilization (%) field	The memory utilization of the system on all the available memory (DIMM) channels in percentage.
IO Utilization (%) field	The IO resource utilization of the system in percentage.

Note These utilization values are reported as a percentage of the total hardware bandwidth. These values may not match with the values being displayed by the host based resource monitoring software.

Toggling the Locator LED

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Turn On Locator LED**.

The LED indicator in the **Locator LED** field lights up and the physical locator LED on the server turns on and blinks.

Step 4 In the **Actions** area, click **Turn Off Locator LED**.

The locator LED turns off.

Toggling the Front Locator LED for the Chassis

This option is available only on some UCS C-Series servers.

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Turn On Front Locator LED** button.

The LED indicator in the Locator LED field lights up and the physical locator LED on the chassis turns on and blinks.

Step 4 In the **Actions** area, click **Turn Off Front Locator LED**.

The front locator LED turns off.

Toggling the Locator LED for a Hard Drive

This option is available only on some UCS C-Series servers.

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Storage** tab.

Step 4 In the **Storage** table, find the hard disk drive (HDD) whose locator LED you want to change.

Step 5 In the **LED Status** column for that HDD, select the desired locator LED state from the drop-down list.

If you select **Turn On**, the LED status indicator in this column lights up and the physical locator LED on the associated HDD turns on and blinks.

Selecting a Time Zone

Selecting a Time Zone

Selecting a time zone helps you choose a local time zone so that you can view the local time rather than the default machine time. Cisco IMC Web UI and the CLI provide you options to choose and set a time zone of your choice.

Setting the time zone to your local time will apply the time zone variable to all the services that utilize the system timing. This impacts the logging information and is utilized in the following applications of the Cisco IMC:

- Fault summary and fault history logs
- Cisco IMC log
- rsyslog

When you set a local time, the timestamp on the applications that you can view are updated with the local time that you have chosen.

Selecting a Time zone

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Cisco Integrated Management Controller (Cisco IMC) Information** area, click **Select Timezone**.

Select Timezone screen appears.

Step 4 In the **Select Timezone** pop-up screen, mouse over the map and click on the location to select your time zone or choose your time zone from the **Timezone** drop-down menu.

Step 5 Click **Save**.

Creating a Server Asset Tag

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Properties** area, update the **Asset Tag** field.

Step 4 Click **Save Changes**.

Managing the Server Boot Order

Server Boot Order

Using Cisco IMC, you can configure the order in which the server attempts to boot from available boot device types. In the legacy boot order configuration, Cisco IMC allows you to reorder the device types but not the devices within the device types. With the precision boot order configuration, you can have a linear ordering of the devices. In the web UI or CLI you can change the boot order and boot mode, add multiple devices under each device types, rearrange the boot order, set parameters for each device type.

When you change the boot order configuration, Cisco IMC sends the configured boot order to BIOS the next time that server is rebooted. To implement the new boot order, reboot the server after you make the configuration change. The new boot order takes effect on any subsequent reboot. The configured boot order remains until the configuration is changed again in Cisco IMC or in the BIOS setup.

Note The actual boot order differs from the configured boot order if either of the following conditions occur:

- BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through BIOS.
- BIOS appends devices that are seen by the host but are not configured from the user.

Note When you create a new policy using the configure boot order feature, BIOS tries to map this new policy to the devices in the system. It displays the actual device name and the policy name to which it is mapped in the **Actual Boot Order** area. If BIOS cannot map any device to a particular policy in Cisco IMC, the actual device name is stated as **NonPolicyTarget** in the **Actual Boot Order** area.

Note When you upgrade Cisco IMC to the latest version 2.0(x) for the first time, the legacy boot order is migrated to the precision boot order. During this process, previous boot order configuration is erased and all device types configured before updating to 2.0 version are converted to corresponding precision boot device types and some dummy devices are created for the same device types. you can view these devices in the **Configured Boot Order** area in the web UI. To view these devices in the CLI, enter **show boot-device** command. During this the server's actual boot order is retained and it can be viewed under actual boot order option in web UI and CLI.

When you downgrade Cisco IMC prior to 2.0(x) verison the server's last legacy boot order is retained, and the same can be viewed under **Actual Boot Order** area. For example:

- If you configured the server in a legacy boot order in 2.0(x) version, upon downgrade a legacy boot order configuration is retained.
- If you configured the server in a precision boot order in 2.0(x), upon downgrade the last configured legacy boot order is retained.

Important

- Boot order configuration prior to 2.0(x) is referred as legacy boot order. If your running version is 2.0(x), then you cannot configure legacy boot order through web UI, but you can configure through CLI and XML API. In the CLI, you can configure it by using **set boot-order HDD,PXE** command. Even though, you can configure legacy boot order through CLI or XML API, in the web UI this configured boot order is not displayed.
- Legacy and precision boot order features are mutually exclusive. You can configure either legacy or precision boot order. If you configure legacy boot order, it disables all the precision boot devices configured. If you configure precision boot order, then it erases legacy boot order configuration.

Configuring the Precision Boot Order

Before you begin

You must log in as a user with admin privileges to configure server the boot order.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

The BIOS page appears.

Step 3 In the **Actions** area, click **Configure Boot Order**.

A dialog box with boot order instructions appears.

Step 4 Review the instructions, and then click **OK**.

The **Configure Boot Order** dialog box is displayed.

Step 5 In the **Configure Boot Order** dialog box, update the following properties:

Name	Description
Add Boot Device table	The server boot options. You can add one or more of the following boot device and set parameters of the selected device: **Note** The following list shows all possible boot devices. The actual devices displayed depend on the type of C-Series server that you are using. • **Add Local HDD** • **Add PXE Boot** • **Add SAN Boot** • **Add iSCSI Boot** • **Add SD Card** **Note** This option is available only on some UCS C-Series servers. • **Add USB** • **Add Virtual Media** • **Add PCH Storage** • **Add UEFI SHELL** • **Add NVME** • **Add Local CDD**
Enable/Disable button	The visibility of a device by BIOS. The state can be one of the following: • **Enabled**— The device is visible to BIOS in a boot order configuration. • **Disabled**— The device is not visible to BIOS in a boot order configuration.
Modify button	Modifies the attributes of the selected devices.
Delete button	Deletes the selected bootable device from the **Boot Order** table.
Clone button	Copies an existing device setting to a new device.
Re-Apply button	Reapplies the boot order configuration to BIOS when the last configured boot order source displays as BIOS.
Move Up button	Moves the selected device type to a higher priority in the **Boot Order** table.
Move Down button	Moves the selected device type to a lower priority in the **Boot Order** table.

Name	Description
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot is attempted.
Save Changes button	Saves the changes to the configured boot order or reapplies a previously configured boot order. Cisco IMC sends the configured boot order to BIOS the next time that server is rebooted.
Reset Values button	Resets the values of the configured boot order.
Close button	Closes the dialog box without saving any changes or reapplying the existing configuration. If you choose this option, the actual boot order does not change the next time that server is rebooted.

Step 6 Click **Save**.

Additional device types might be appended to the actual boot order, depending on what devices you have connected to your server.

What to do next

Reboot the server to boot with your new boot order.

Managing a Boot Device

Before you begin

You must log in as a user with admin privileges to add device type to the server boot order.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Action** area, click **Configure Boot Order**.

A dialog box with boot order instructions appears.

Step 4 Review the instructions, and then click **OK**.

The **Configure Boot Order** dialog box is displayed.

Step 5 In the **Configure Boot Order** dialog box, from the **Add Boot Device** table, choose the device that you want add to the boot order.

To add the local HDD device, click **Add Local HDD**, and update the following parameters:

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. The range depends on the C-Series servers: • For C220 M4 and C240 M4 servers, enter HBA. • For C460 M4 servers, enter a value within the range 1 - 255, or SAS. • For the other C-Series servers, enter a value within the range 1 - 255, or M.
Add Device button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the PXE device, click **Add PXE**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.

Name	Description
Slot field	• For C220 M4 and C240 M4 servers, enter a number between 1 and 255, or L, or MLOM. • For C3160 servers, enter a value between 1 and 255. • For C460M4 servers, enter a value between 1 and 255, or L1, or L2. • For the other C-Series servers, enter a value between 0 and 255, or L.
MAC Address	MAC address of the server. **Note** This option is available only on some C-Series servers.
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255.

To add the SAN boot device, click **Add SAN**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. The range depends on the C-Series servers: • For C220 M4 and C240 M4 servers, enter a number between 1 and 255, or MLOM. • For C460M4 servers, enter a value between 1 and 255, or L1, or L2. • For the other C-Series servers, enter a value between 1 and 255.
LUN field	Logical unit in a slot where the device is present. Enter a number between 0 and 255.

Name	Description
Save Changes button	Adds the device to the **Boot Order** table, and saves the changes.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the iSCSI boot device, click **Add iSCSI**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. The range depends on the C-Series servers: • For C220 M4 and C240 M4 servers, enter a number between 1 and 255, or L, or MLOM. • For C3160 servers, enter a value between 1 and 255. • For C460M4 servers, enter a value between 1 and 255, or L1, or L2. • For the other C-Series servers, enter a value between 1 and 255, or L.
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255. **Note** In case of a VIC card, use a vNIC instance instead of the port number.
Save Changes button	Adds the device to the **Boot Order** table, and saves the changes.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the SD card, click **Add SD Card**, and update the following parameters:

Note This option is available only on some UCS C-Series servers.

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the USB device, click **Add USB**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Sub Type drop-down list	The subdevice type under a certain device type. This can be one of the following: • **CD** • **FDD** • **HDD**
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the virtual media, click **Virtual Media**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Sub Type drop-down list	The subdevice type under a certain device type. This could be any one of the following: • **KVM Mapped DVD** • **Cisco IMC Mapped DVD** • **KVM Mapped HDD** • **Cisco IMC Mapped HDD** • **KVM Mapped FDD**
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the PCH storage device, click **PCH Storage**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.

Name	Description
LUN field	Logical unit in a slot where the device is present. • Enter a number between 0 and 255 • SATA in AHCI mode—Enter a value between 1 and 10 • SATA in SWRAID mode—Enter 0 for SATA , and enter 1 for SATA **Note** SATA mode is available only on some UCS C-Series servers.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the UEFI shell device, click **Add UEFI Shell**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Add Device button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Overview to UEFI Secure Boot

You can use Unified Extensible Firmware Interface (UEFI) secure boot to ensure that all the EFI drivers, EFI applications, option ROM or operating systems prior to loading and execution are signed and verified for authenticity and integrity, before you load and execute the operating system. You can enable this option using either web UI or CLI. When you enable UEFI secure boot mode, the boot mode is set to UEFI mode and you cannot modify the configured boot mode until the UEFI boot mode is disabled.

Note If you enable UEFI secure boot on a nonsupported OS, on the next reboot, you cannot boot from that particular OS. If you try to boot from the previous OS, an error is reported and recorded the under system software event in the web UI. You must disable the UEFI secure boot option using Cisco IMC to boot from your previous OS.

Important Also, if you use an unsupported adapter, an error log event in Cisco IMC SEL is recorded. The error messages is displayed that says:

System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .

UEFI secure boot is supported on the following components:

Components	Types
Supported OS	• Windows Server 2012 • Windows Server 2012 R2
Broadcom PCI adapters	• 5709 dual and quad port adapters • 57712 10GBASE-T adapter • 57810 CNA • 57712 SFP port
Intel PCI adapters	• i350 quad port adapter • X520 adapter • X540 adapter • LOM
QLogic PCI adapters	• 8362 dual port adapter • 2672 dual port adapter
Fusion-io	

Components	Types
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro card

Enabling UEFI Secure Boot

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **BIOS Properties** area, check **UEFI Secure Boot** checkbox.

Note If checked, the boot mode is set to UEFI secure boot. You cannot modify the **Configure Boot Mode** until UEFI secure boot option is disabled.

If you enable UEFI secure boot on a nonsupported OS, on the next reboot, you cannot boot from that particular OS. If you try to boot from the previous OS, an error is reported and recorded under the system software event in the web UI. You must disable the UEFI secure boot option by using Cisco IMC to boot from your previous OS.

Step 4 Click **Save Changes**.

What to do next

Reboot the server to have your configuration boot mode settings take place.

Disabling UEFI Secure Boot

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **BIOS Properties** area, uncheck the **UEFI Secure Boot** check box.

Step 4 Click **Save Changes**.

What to do next

Reboot the server to have your configuration boot mode settings take place.

Viewing the Actual Server Boot Order

The actual server boot order is the boot order actually used by BIOS when the server last booted. The actual boot order can differ from the boot order configured in Cisco IMC.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

The **BIOS** page appears.

Step 3 In the **Actual Boot Order** area of **BIOS** page, review the list of boot devices in the order actually used by BIOS when the server last booted.

All devices present during the last boot are listed in a linear order. You can expand the device string name to view the attributes of that particular device.

Note BIOS discovers devices that do not match any configurations in a configured boot order, and lists them as NonPolicyTarget devices in a device list.

Configuring a Server to Boot with a One-time Boot Device

You can configure a server to boot from a particular device only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one time boot device, all its future reboots occur from the previously configured boot order.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **BIOS Properties** area, select an option from the **Configured One Time Boot Device** drop-down.

Note The host boots to the one time boot device even when configured with a disabled advanced boot device.

Resetting the Server

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Hard Reset Server**.

A dialog box with the message **Hard Reset the Server?** appears.

Step 4 Click **OK**.

Shutting Down the Server

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Shut Down Server**.

A dialog box with the message **Shut Down the Server?** appears.

Step 4 Click **OK**.

Managing Server Power

Powering On the Server

Note If the server was powered off by any means other than through Cisco IMC, it will not become active immediately when powered on. The server will remain in standby mode until Cisco IMC completes initialization.

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Power On Server**.

A dialog box with the message **Power on the server?** appears.

Step 4 Click **OK**.

Powering Off the Server

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Power Off Server**.

A dialog box with the message **There is an update available for Chassis Firmware, would you like to continue?** appears. Clicking **OK** powers off the server and updates the system firmware.

Step 4 Click **OK**.

Power Cycling the Server

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Power Cycle Server**.

A dialog box with the message **Power Cycle the Server?** appears.

Step 4 Click **OK**.

Configuring Power Policies

Configuring the Power Restore Policy

The power restore policy determines how power is restored to the server after a chassis power loss.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Navigation** pane, click the **Compute** menu.

Step 4 In the work pane, click the **Power Policies** tab.

Step 5 In the **Power Restore Policy** area, update the following fields:

Name	Description
Power Restore Policy drop-down list	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power Off**—The server remains off until it is manually restarted. • **Power On**—The server is allowed to boot up normally when power is restored. The server can restart immediately or, optionally, after a fixed or random delay. • **Restore Last State**—The server restarts and the system attempts to restore any processes that were running before power was lost.
Power Delay Type drop-down list	If the selected policy is **Power On**, the restart can be delayed with this option. This can be one of the following: • **fixed**—The server restarts after a fixed delay. • **random**—The server restarts after a random delay. **Note** This option is available only for some C-Series servers.
Power Delay Value field	If a fixed delay is selected, once chassis power is restored and the Cisco IMC has finished rebooting, the system waits for the specified number of seconds before restarting the server. Enter an integer between 0 and 240. **Note** This option is available only for some C-Series servers.

Step 6 Click **Save Changes**.

Configuring Fan Policies

Fan Control Policies

Fan Control Policies enable you to control the fan speed to bring down server power consumption and noise levels. Prior to these fan policies, the fan speed increased automatically when the temperature of any server component exceeded the set threshold. To ensure that the fan speeds were low, the threshold temperatures of components are usually set to high values. While this behavior suited most server configurations, it did not address the following situations:

- Maximum CPU performance

  For high performance, certain CPUs must be cooled substantially below the set threshold temperature. This required very high fan speeds which resulted in higher power consumption and increased noise levels.

- Low power consumption

To ensure the lowest power consumption, fans must run very slowly, and in some cases, stop completely on servers that support it. But slow fan speeds resulted in servers overheating. To avoid this situation, it is necessary to run fans at a speed that is moderately faster than the lowest possible speed.

With the introduction of fan policies, you can determine the right fan speed for the server, based on the components in the server. In addition, it allows you to configure the fan speed to address problems related to maximum CPU performance and low power consumption.

Following are the fan policies that you can choose from:

- **Balanced**

  This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards, since these cards overheat easily.

- **Performance**

  This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds will run at the same speed or higher speed than that of the Balanced fan policy.

  Note This option is available only on some C-Series servers.

- **Low Power**

  This is the default policy. This setting is ideal for minimal configuration servers that do not contain any PCIe cards.

- **High Power**

  This setting can be used for server configurations that require fan speeds ranging from 60 to 85%. This policy is ideal for servers that contain PCIe cards that easily overheat and have high temperatures.

- **Maximum Power**

  This setting can be used for server configurations that require extremely high fan speeds ranging between 70% to 100%. This policy is ideal for servers that contain PCIe cards that easily overheat and have extremely high temperatures.

- **Acoustic**

  This setting can be used for configuring the fan noise level, thereby enabling noise reduction in the servers. Application of this policy might result in performance throttling impacting system performance. If excessive thermal or performance events are recorded in the event logs, select a standard fan control policy like **Low Power**, which is a non-disruptive change.

  Note This option is available only on UCS C240 M5 servers.

Note Although you set a fan policy in Cisco IMC, the actual speed that the fan runs at is determined by the configuration requirements of the server. For example, if you set the fan policy to **Balanced**, but the server includes PCIe cards that overheat easily, then the speed of the fans on the server is adjusted automatically to the required minimum fan speed to prevent the overheating. If you have set a fan speed configuration higher than required, the system retains the selected fan speed. The **Applied Fan Policy** displays the actual fan speed that runs on the server.

The **Configuration Status** displays the status of the configured fan policy. This can be one of the following:

- SUCCESS —The selected fan policy matches the actual fan speed that runs on the server.
- PENDING —The configured fan policy is not in effect yet. This can be due to one of the following:
  - The server is powered off
  - The BIOS POST is not complete
- FAN POLICY OVERRIDE—Overrides the specified fan speed with the actual speed determined by the configuration requirements of the server.

Configuring the Fan Policy

You can determine the right fan policy based on the server configuration and server components.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Configured Fan Policy** area, select a fan policy from the drop-down list. It can be one of the following:

Name	Description
Fan Policy drop-down list	This can be one of the following: • **Balanced**—This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards as these cards overheat easily. • **Performance**—This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds run at the same speed or higher speed than that of the fan speed set with the Balanced fan policy. **Note** This option is available only on some C-Series servers. • **Low Power**—This is the default policy. This setting is ideal for minimal configuration servers that do not contain any PCIe cards. • **High Power**—This setting can be used for server configurations that require fan speeds ranging from 60% to 85%. This policy is ideal for servers that contain PCIe cards that overheat easily and have high temperatures. • **Maximum Power**—This setting can be used for server configurations that required extremely high fan speeds ranging from 70% to 100%. This policy is ideal for servers that contain PCIe cards that overheat easily and have very high temperatures. • **Acoustic**—This setting can be used for configuring the fan noise level, thereby enabling noise reduction in the servers. Application of this policy might result in performance throttling impacting system performance. If excessive thermal or performance events are recorded in the event logs, select a standard fan ontrol policy like **Low Power**, which is a non-disruptive change. **Note** This option is available only on UCS C240 M5 servers.

Name	Description
Applied Fan Policy field	The actual speed of the fan that runs on the server. When the configured fan policy is not in effect, it displays N/A. The configured fan policy takes effect when the server is powered on and the POST is complete.

Configuration Status field	The configuration status of the fan policy. This can be one of the following:
	• SUCCESS —The fan speed set by you matches the actual fan speed that runs on the server.
	• PENDING —The configured fan policy is not in effect yet. This can be due to one of the following:
	  • The server is powered off
	  • The BIOS POST is not complete
	• FAN POLICY OVERRIDE—Overrides the specified fan speed with the actual speed determined by the configuration requirements of the server.

Step 4 Click **Save Changes**.

PID Catalog Overview

Currently the product ID (PID) catalog on a standalone rack server is updated only with a new Cisco IMC image, or a new container. This means that even if a new device is added to the server, the PID catalog remains outdated until a new Cisco IMC image is produced.

Effective with this release, you can update just the PID catalog, independently, without having to update the Cisco IMC or container. You can download a signed PID update package using FTP, TFTP, SFTP, HTTP, and SCP. Once downloaded, the signed PID update package is verified, and a new 'pid-update-catalog.xml' is generated. This XML file replaces the existing catalog.xml when you use the **show* - pid** command.

The PID catalog update involves the following steps:

- Creation of PID update package
- Security and signing of the package
- Secure generic update of the catalog

Uploading a PID Catalog

Before you begin

You must log in as a user with admin privileges to upload a PID catalog.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PID Catalog** tab.

Step 4 In the **Actions** area, click the **Upload PID Catalog** link.

The **Upload PID Catalog** dialog box appears.

Depending on the location of the catalog file, choose one of the options.

Step 5 In the **Upload PID Catalog from Local File** dialog box, click **Browse** and use the **Choose File to Upload** dialog box to select the catalog file that you want to upload.

Name	Description
File field	The PID catalog file that you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate file.

Step 6 In the **Upload PID Catalog from Remote Server** dialog box, complete the following fields:

Name	Description
Upload PID Catalog from Remote Server drop-down list	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the PID catalog information is available. Depending on the setting in the Upload PID Catalog from drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the catalog file on the remote server.
Username field	Username of the remote server.

Name	Description
Password field	Password of the remote server.
Upload button	Uploads the selected PID catalog. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Cancel button	Closes the wizard without making any changes to the firmware versions stored on the server.

Activating a PID Catalog

Before you begin

- You must log in as a user with admin privileges to activate a PID catalog.
- The Upload Status of a PID catalog must be displayed as Yes.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PID Catalog** tab.

Step 4 In the **Actions** area, click the **Activate PID Catalog** link.

A confirmation box appears. Select Yes or No to activate the PID catalog or cancel activation.

Note The **Activate PID Catalog** link is greyed out when you log on to the system for the first time. It gets activated only after you upload a PID catalog to the server.

Managing the Flexible Flash Controller

Cisco Flexible Flash

On the M5 servers, Flexible Flash Controller is inserted into the mini storage module socket. The mini storage socket is inserted into the M.2 slot on the motherboard. M.2 slot also supports SATA M.2 SSD slots.

Note M.2 slot does not support NVMe in this release.

Some C-Series Rack-Mount Servers support an internal Secure Digital (SD) memory card for storage of server software tools and utilities. The SD card is hosted by the Cisco Flexible Flash storage adapter.

The SD storage is available to Cisco IMC as a single hypervisor (HV) partition configuration. Prior versions had four virtual USB drives. Three were preloaded with Cisco UCS Server Configuration Utility, Cisco drivers and Cisco Host Upgrade Utility, and the fourth as user-installed hypervisor. A single HV partition configuration is also created when you upgrade to the latest version of Cisco IMC or downgrade to the prior version, and reset the configuration.

For more information about installing and configuring the M.2 drives, see the **Storage Controller Considerations (Embbeded SATA RAID Requirements)** and **Replacing an M.2 SSD in a Mini-Storage Carrier For M.2** sections in the Cisco UCS Server Installation and Service Guide for the C240 M5 servers at this URL:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html

For information about the Cisco software utilities and packages, see the *Cisco UCS C-Series Servers Documentation Roadmap* at this URL:

http://www.cisco.com/go/unifiedcomputing/c-series-doc

Card Management Feature in the Cisco Flexible Flash Controller

The Cisco Flexible Flash controller supports management of both single and two SD cards as a RAID-1 pair. With the introduction of card management, you can perform the following tasks:

Note

- If you want to upgrade from version 1.4(5e) to 1.5(4) or higher versions, you must first upgrade to version1.5(2) and then upgrade to a higher version of Cisco IMC.
- Reset the Cisco Flexible Flash controller to load the latest Flex Flash firmware after every Cisco IMC firmware upgrade.

Action	Description
Reset Cisco Flex Flash	Allows you to reset the controller.
Reset Partition Defaults	Allows you to reset the configuration in the selected slot to the default configuration.

Action	Description
Synchronize Card Configuration	Allows you to retain the configuration for an SD card that supports firmware version 253 and later.
Configure Operational Profile	Allows you to configure the SD cards on the selected Cisco Flexible Flash controller.

RAID Partition Enumeration

Non-RAID partitions are always enumerated from the primary card and the enumeration does not depend on the status of the primary card.

Following is the behavior of the RAID partition enumeration when there are two cards in the Cisco Flexible Flash controller:

Scenario	Behavior
Single card	RAID partitions are enumerated if the card is healthy, and if the mode is either **Primary** or **Secondary-active**.
Dual paired cards	RAID partitions are enumerated if one of the cards is healthy. When only one card is healthy, all read/write operations occur on this healthy card. You must use UCS SCU to synchronize the two RAID partitions.
Dual unpaired cards	If this scenario is detected when the server is restarting, then neither one of the RAID partitions is enumerated. If this scenario is detected when the server is running, when a user connects a new SD card, then the cards are not managed by the Cisco Flexible Flash controller. This does not affect the host enumeration. You must pair the cards to manage them. You can pair the cards using the **Reset Partition Defaults** or **Synchronize Card Configuration** options.

Upgrading from Single Card to Dual Card Mirroring with FlexFlash

You can upgrade from a single card mirroring to dual card mirroring with FlexFlash in one of the following methods:

- Add an empty FlexFlash card to the server, and then upgrade its firmware to the latest version.
- Upgrade the FlexFlash firmware to the latest version and then add an empty card to the server.

Prior to using either of these methods, you must keep in mind the following guidelines:

- To create RAID1 mirroring, the empty card that you want to add to the server must be of the exact size of the card that is already in the server. Identical card size is a must to set up RAID1 mirroring.

- Ensure that the card with valid data in the Hypervisor partition is marked as the primary healthy card. You can determine this state either in the Cisco IMC GUI or from the Cisco IMC CLI. To mark the state of the card as primary healthy, you can either use the **Reset Configuration** option in the Cisco IMC GUI or run the **reset-config** command in the Cisco IMC CLI. When you reset the configuration of a particular card, the secondary card is marked as secondary active unhealthy.
- In a Degraded RAID health state all read-write transactions are done on the healthy card. In this scenario, data mirroring does not occur. Data mirroring occurs only in the Healthy RAID state.
- Data mirroring is only applicable to RAID partitions. In the C-series servers, only Hypervisor partitions operate in the RAID mode.
- If you have not configured SD cards for use with prior versions, then upgrading to the latest version loads the latest 253 firmware and enumerates all four partitions to the host.

While upgrading versions of the FlexFlash, you may see the following error message:

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE”
```

In addition, the card status may be shown as **missing**. This error occurs because you accidently switched to an alternate release or a prior version, such as 1.4(x). In this scenario, you can either revert to the latest version, or you can switch back to the FlexFlash 1.4(x) configuration. If you choose to revert to the latest Cisco IMC version, then the Cisco FlexFlash configuration remains intact. If you choose to switch back to the prior version configuration, you must reset the Flexflash configuration. In this scenario, you must be aware of the following:

- If multiple cards are present, and you revert to a prior version, then the second card cannot be discovered or managed.
- If the card type is SD253, then you must run the **reset-config** command twice from the Cisco IMC CLI - once to reload the old firmware on the controller and to migrate SD253 to SD247 type, and the second time to start the enumeration.

Configuring the Flexible Flash Controller Properties

After you upgrade to the latest verison of Cisco IMC or downgrade to a prior version, and reset the configuration, the server will access HV partition only.

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task

Configuring the Flexible Flash Controller Firmware Mode

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 In the **Actions** area, click **Configure Firmware Mode**.

Step 4 Click **OK** in the confirmation box.

Switches the controller firmware mode from the current firmware mode to the other.

Configuring the Flexible Flash Controller Cards

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 In the **Actions** area, click **Configure Cards**.
Configure Cards dialog box appears.

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

Name	Description
Mirror radio button	Enter the following: • **Mirror Partition Name** field—The name that you want to assign to the partition. • **Auto Sync** checkbox—If selected, data from the selected primary card will sync automatically with the secondary card. **Note** • There must be two cards for you to choose this option. • If this option is selected, data on the secondary card is erased and overwritten by the data on the primary card. • The status of this is displayed under the **Physical Driver Info** tab. • **Select Primary Card** drop-down—Slot that you want to set as the primary card. This can be one of the following: • **Slot1** • **Slot2**

Name	Description

Util radio button	Select this option to configure the card in **Util** mode. When you configure the cards in the Util mode, the following situations occur:
	• The card in the selected slot creates four partitions that has a partition each for the utilities: SCU, HUU, Drivers and one partition that can be used by the user and the card is marked healthy.
	• The card in the other slot, if it exists, creates a single partition and the card is marked healthy.
	• The card read/write error counts and read/write threshold are set to 0.
	• Host connectivity could be disrupted.
	• The configured cards will be paired.
	Enter the following:
	• **User Partition Name** field—The name that you want to assign to the fourth partition of the Util card.
	• **Non Util Card Partition Name** field—The name that you want to assign to the single partition on the second card, if it exists.
	• **Select Util Card** drop-down—Slot that you want to set for Util. This can be one of the following:
	  • **Slot1**
	  • **Slot2**
	  • **None**—Applicable only when the server has one SD card.

Step 5 Click **Save**.

The cards are configured in the chosen mode.

Booting from the Flexible Flash Card

You can specify a bootable virtual drive on the Cisco Flexible Flash card that overrides the default boot priority the next time that the server is restarted, regardless of the default boot order defined for the server. The specified boot device is used only once. After the server has rebooted, this setting is ignored. You can choose a bootable virtual drive only if a Cisco Flexible Flash card is available. Otherwise, the server uses a default boot order.

Note Before you reboot the server, ensure that the virtual drive that you select is enabled on the Cisco Flexible Flash card. Go to the **Storage** tab, choose the card, and then go to the **Virtual Drive Info** subtab.

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure Boot Override Priority**.

The **Boot Override Priority** dialog box appears.

Step 4 From the **Boot Override Priority** drop-down list, choose a virtual drive to boot from.

Step 5 Click **Apply**.

Resetting the Flexible Flash Controller

In normal operation, it should not be necessary to reset the Cisco Flexible Flash. We recommend that you perform this procedure only when explicitly directed to do so by a technical support representative.

Note This operation will disrupt traffic to the virtual drives on the Cisco Flexible Flash controller.

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Reset FlexFlash Controller**.

Step 4 Click **OK** to confirm.

Enabling Virtual Drives

Before you begin

- You must log in with admin privileges to perform this task.

- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, click **Enable/Disable Virtual Drive(s)**.

Step 5 In the **Enable/Disable VD(s)** dialog box, select the virtual drives that you want to enable.

Step 6 Click **Save**.
The selected virtual drives are enabled to the host.

Erasing Virtual Drives

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, click **Erase Virtual Drive(s)**.

Step 5 In the **Erase Virtual Drive(s)** dialog box, select the virtual drives that you want to erase.

Step 6 Click **Save**.
Data on the selected virtual drives is erased.

Syncing Virtual Drives

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- Cards must be in mirror mode.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, click **Sync Virtual Drive**.

Step 5 Click **OK** in the confirmation dialog box.
Syncs the virtual drive hypervisor with the primary card.

Adding an ISO Image Configuration

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- The cards must be configured in Util mode.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, select the virtual drive for which you want to add an image, click **Add Image**.

Step 5 In the **Add Image** dialog box, update the following fields:

Name	Description
Volume field	The identity of the image mounted for mapping. This can be one of the following: • **SCU** • **HUU** • **Drivers**
Mount Type drop-down list	The type of mapping. This can be one of the following: • **NFS**—Network File System. • **CIFS**—Common Internet File System.
Remote Share field	The URL of the image to be mapped. The format depends on the selected **Mount Type**: • **NFS**—Use `serverip:/share path`. • **CIFS**—Use `//serverip/share path`.
Remote File field	The name and location of the .iso file in the remote share. Following are the example of remote share files: • **NFS** — `/softwares/ucs-cxx-scu-3.1.9.iso` • **CIFS** — `/softwares/ucs-cxx-scu-3.1.9.iso`

Name	Description
Mount Options field	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • `ro` • `rw` • `nolock` • `noexec` • `soft` • `port=VALUE` • `timeo=VALUE` • `retry=VALUE` If you are using **CIFS**, leave the field blank or enter one or more of the following: • `soft` • `nounix` • `noserverino`
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 Click **Save**.

Updating an ISO Image

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- This task is available only when the cards are configured in **Util** mode.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, select the virtual drive on which you want to update the image, click **Update Image**.

Note SCU and HUU update may take up to an hour and the drivers update may take up to five hours.

Unmapping an ISO Image

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, select the virtual drive for which you want to un map the image, click **Unmap Image**.

Resetting the Cisco Flexible Flash Card Configuration

When you reset the configuration of the slots in the Cisco Flexible Flash card, the following situations occur:

- The card in the selected slot is marked as primary healthy.
- The card in the other slot is marked as secondary-active unhealthy.
- One RAID partition is created.
- The card read/write error counts and read/write threshold are set to 0.

- Host connectivity could be disrupted.

If you upgrade to the latest version and select reset configuration option, a single hypervisor (HV) partition is created, and the existing four partition configurations are erased. This may also result in data loss. You can retrieve the lost data only if you have not done any data writes into HV partition, and downgrade to prior version.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Reset Partition Defaults**.

Step 4 In the **Reset Partition Defaults** dialog box, update the following fields:

Name	Description
Slot radio button	Select the slot for which you want to mark the card as primary healthy. The card in the other slot, if any, is marked as secondary-active unhealthy.
Reset Partition Defaults button	Resets the configuration of the selected slot.
Cancel button	Closes the dialog box without making any changes.

Step 5 Click **Yes**.

Retaining Configuration of the Cisco Flexible Flash Cards

You can retain the configuration for an FlexFlash that supports firmware version 253 and later card in the following situations:

- There are two unpaired FlexFlash
- The server is operating from a single FlexFlash, and an unpaired FlexFlash is in the other slot.
- One FlexFlash supports firmware version 253, and the other FlexFlash is unpartitioned.

When you retain the configuration, the following situations occur:

- The configuration for the FlexFlash in the selected slot is copied to the other card.
- The card in the selected slot is marked as primary healthy.
- The card in the secondary slot is marked as secondary-active unhealthy.

Before you begin

- You must log in with admin privileges to perform this task.

Procedure

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Synchronize Card Configuration**.

Step 4 In the **Synchronize Card Configuration** dialog box, update the following fields:

Name	Description
Slot radio button	Select the slot for which you want the configuration retained. The configuration is copied from the selected slot to the card in the other slot, and the card in the selected slot is marked as primary healthy.
Synchronize Card Configuration button	Copies the configuration from the selected card only if the selected card is of type SD253 and has single HV configuration.
Cancel button	Closes the dialog box without making any changes.

Step 5 Click **Yes**.

Adding an SD Card and Upgrading the Firmware to 1.5(4) Version

Procedure

Step 1 Insert the empty SD card into SLOT-2 of the server.

Step 2 Upgrade the Cisco IMC software version to release 1.5(4) and reboot Cisco IMC.

Step 3 In the **Navigation** pane, click the **Storage** tab.

Step 4 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 5 In the **Controller Info** tab, determine the state displayed for the **Internal State** field.

The state should be displayed as **WAIT_ON_USER**.

Step 6 Click **Reset FlexFlash Controller**.

Important This option resets the partition enumeration to the host. Before you reset the FlexFlash controller, ensure that the SD card is not used from the host.

When you reset the FlexFlash controller, the card in SLOT-1 is automatically marked as primary healthy, and the empty card in SLOT-2 is marked as secondary active unhealthy card. RAID health is indicated as Degraded. In this situation, all data transactions are written on the healthy card and data mirroring does not occur

Step 7 (Optional) To change the RAID health to healthy, launch Cisco UCS Server Configuration Utility (Cisco UCS SCU) on the host, and click **Hypervisor Sync**.

This option mirrors data from the healthy card to the unhealthy card.

Upgrading Cisco IMC and SD Card Firmware Versions

SD storage is available to Cisco IMC version 1.5(4) as a single HV partition configuration, and it support firmware version 257. Prior releases had four-partition configuration, and supported firmware versions 247, 248, and 253. Cisco IMC version 1.5(4) supports all the SD card firmware versions prior to 257. For SD card with firmware version 253 and later, if you select **Reset FlexFlash Controller** option, the firmware version of these cards are upgraded to 257 automatically.

Upgrading from Cisco IMC Version 1.4(x) to 1.5(4)

The partition layout for the release 1.4(x) is significantly different from the release 1.5(4) so, automatic upgrades from Cisco IMC version 1.4(x) to 1.5(4) is not possible. If you upgrade Cisco IMC version 1.4(x) to 1.5(4) directly, then you are prompted to select **Reset Partition Default** option. If you select this option, a single HV partition configuration is created. This may result in data loss stored in the SD card. To retain the four partition configuration and the data stored on the SD card, Cisco recommends that you first upgrade the Cisco IMC version to 1.5(2) or 1.5(3) and then upgrade to 1.5(4) version. Select **Reset FlexFlash Controller** option.

Upgrading Cisco IMC, SD Card Firmware, and Adding a New SD Card

Before you begin

- The size of the empty card that you are adding should match the size of the existing card to successfully create a RAID1 mirror.
- Ensure that the SD card with the valid data in the HyperVisor partition is marked as a primary healthy card. To mark a specific SD card as healthy, you can click **Reset Partition Defaults**. This results in the other card being marked as secondary active unhealthy card.

Procedure

Step 1 Upgrade the Cisco IMC software version to release 1.5(4) and reboot Cisco IMC.

Step 2 In the **Navigation** pane, click the **Storage** tab.

Step 3 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 4 In the **Controller Info** tab, determine the state displayed for the **Internal State** field.

The state should be displayed as **WAIT_ON_USER**.

Step 5 Click **Reset FlexFlash Controller**.

Important This option resets the partition enumeration to the host. Before you reset the FlexFlash controller, ensure that the SD card is not used from the host.

When you reset the FlexFlash controller, the card in SLOT-1 is automatically marked as **primary healthy**, and the empty card in SLOT-2 is marked as **secondary active unhealthy** card. RAID health is indicated as

Degraded. In this situation, all data transactions are written on the healthy card and data mirroring does not occur

Step 6 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 7 In the **Controller Info** tab, click **Reset Partition Defaults**, and select **SLOT-1** are the primary slot.

The card in SLOT-1 is automatically marked as primary healthy, and the empty card in SLOT-2 is marked as secondary active unhealthy card. RAID health is indicated as Degraded

Step 8 (Optional) To change the RAID health to healthy, launch Cisco UCS Server Configuration Utility (Cisco UCS SCU) on the host, and click **Hypervisor Sync**.

This option mirrors data from the healthy card to the unhealthy card.

Configuring DIMM Blacklisting

DIMM Black Listing

In Cisco IMC, the state of the Dual In-line Memory Module (DIMM) is based on SEL event records. A DIMM is marked bad if the BIOS encounters a non-correctable memory error or correctable memory error with 16000 error counts during memory test execution during BIOS post. If a DIMM is marked bad, it is considered a non-functional device.

If you enable DIMM blacklisting, Cisco IMC monitors the memory test execution messages and blacklists any DIMM that encounters memory errors at any given point of time in the DIMM SPD data. This allows the host to map out those DIMMs.

DIMMs are mapped out or blacklisted only when Uncorrectable errors occur. When a DIMM gets blacklisted, other DIMMs in the same channel are ignored or disabled, which means that the DIMM is no longer considered bad.

Note DIMMs do not get mapped out or blacklisted for 16000 Correctable errors.

Enabling DIMM Black Listing

Before you begin

- You must be logged in as an administrator.

Procedure

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **Inventory** tab.

Step 4 In the **Memory** pane's **DIMM Black Listing** area, click the **Enable DIMM Black List** check box.

Configuring BIOS Settings

Configuring Main BIOS Settings

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS**.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Main** tab.

Step 5 Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Step 6 In the **Main** tab, update the BIOS settings fields.

The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see:

- BIOS Parameters by Server Model, on page 277

Step 7 (Optional) You can reset the parameters or restore the default values using the buttons at the bottom of the **Configure BIOS Parameters** dialog box.

The available options are:

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.

Name	Description
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Step 8 Click **Save Changes**.

Configuring Advanced BIOS Settings

Note Depending on your installed hardware, some configuration options described in this topic may not appear.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS**.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Advanced** tab.

Step 5 Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Step 6 In the **Advanced** tab, update the BIOS settings fields.

The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see:

- BIOS Parameters by Server Model, on page 277

Step 7 (Optional) You can reset the parameters or restore the default values using the buttons at the bottom of the **Configure BIOS Parameters** dialog box.

The available options are:

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Step 8 Click **Save Changes**.

Configuring Server Management BIOS Settings

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS**.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Server Management** tab.

Step 5 Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Step 6 In the **Server Management** tab, update the BIOS settings fields.

The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see:

- BIOS Parameters by Server Model, on page 277

Step 7 (Optional) You can reset the parameters or restore the default values using the buttons at the bottom of the **Configure BIOS Parameters** dialog box.

The available options are:

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Step 8 Click **Save Changes**.

Entering BIOS Setup

Before you begin

- The server must be powered on.
- You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Enter BIOS Setup**.

Step 4 Click **Enable**.
Enables enter BIOS setup. On restart, the server enters the BIOS setup.

Restoring BIOS Manufacturing Custom Defaults

In instances where the components of the BIOS no longer function as desired, you can restore the BIOS set up tokens and parameters to the customized manufacturing default values.

Note This action is only available for some C-Series servers.

Before you begin

- The server must be powered off.
- You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Restore Manufacturing Custom Defaults**.

Step 4 Click **OK**.

BIOS Profiles

On the Cisco UCS server, default token files are available for every server platform, and you can configure the value of these tokens using the Graphic User Interface (GUI), CLI interface, and the XML API interface. To optimize server performance, these token values must be configured in a specific combination.

Configuring a BIOS profile helps you to utilize pre-configured token files with the right combination of the token values. Some of the pre-configured profiles that are available are virtualization, high-performance, low power, and so on. You can download the various options of these pre-configured token files from the Cisco website and apply it on the servers through the BMC.

You can edit the downloaded profile to change the value of the tokens or add new tokens. This allows you to customize the profile to your requirements without having to wait for turnaround time.

Uploading a BIOS Profile

You can upload a BIOS profile either from a remote server location or through a browser client.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS Profile**.

Step 4 To upload the BIOS profile using a remote server location, in the **BIOS Profile** area, click the **Upload** button.

Step 5 In the **Upload BIOS Profile** dialog box, update the following fields:

Name	Description
Upload BIOS Profile from drop-down list	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the BIOS profile information is available. Depending on the setting in the Upload BIOS Profile from drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the BIOS profile on the remote server.
Username field	Username of the remote server.
Password field	Password of the remote server.
Upload button	Uploads the selected BIOS profile. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Cancel button	Closes the wizard without making any changes to the firmware versions stored on the server.

Step 6 To upload the BIOS profile using a browser client, in the **BIOS Profile** area, click the **Upload** button.

Step 7 In the **Upload BIOS Profile** dialog box, update the following fields:

Name	Description
File field	The BIOS profile that you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate file.

What to do next

Activate a BIOS profile.

Activating a BIOS Profile

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

The BIOS page appears.

Step 3 In the **Actions** area, click **Configure BIOS Profile**.

Step 4 In the **BIOS Profile** area click **Activate**.

Step 5 At the prompt, click **Yes** to activate the BIOS profile.

What to do next

Delete an existing BIOS profile.

Deleting a BIOS Profile

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

The BIOS page appears.

Step 3 In the **Actions** area, click **Configure BIOS Profile**.

Step 4 In the **BIOS Profile** area click **Delete**.

Step 5 At the prompt, click **OK** to delete the BIOS profile.

Backing up a BIOS Profile

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

The BIOS page appears.

Step 3 In the **Actions** area, click **Configure BIOS Profile**.

Step 4 In the **BIOS Profile** area click **Take Backup**.

Step 5 At the prompt, click **Yes** to take a backup of the BIOS profile.

What to do next

Activate a BIOS profile.

Viewing BIOS Profile Details

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

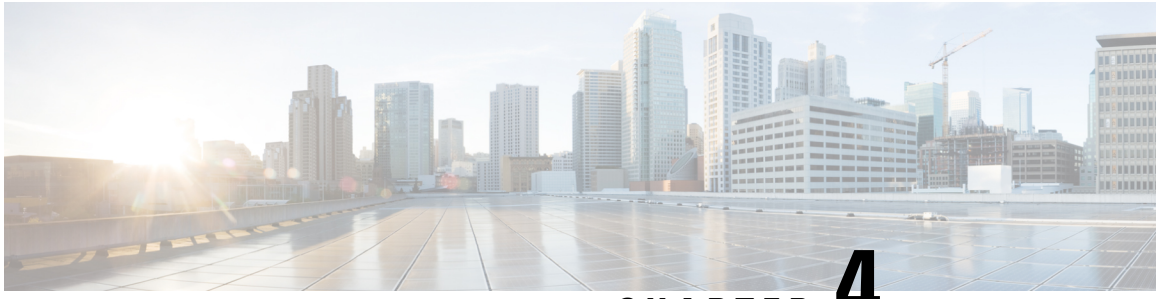
The BIOS page appears.

Step 3 In the **Actions** area, click **Configure BIOS Profile**.

Step 4 In the **BIOS Profile** area click **Details**.

Step 5 Review the following information in the **BIOS Profile Details** window:

Name	Description
Token Name column	Displays the token name of the BIOS profile.
Display Name column	Displays the user name of the BIOS profile.
Profile Value column	Displays the value that was provided in the uploaded file.
Actual Value column	Displays the value of the active BIOS configuration.



CHAPTER 4

Viewing Server Properties

This chapter includes the following sections:

Viewing Server Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Properties** area of the **Server Summary** pane, review the following information:

Name	Description
Product Name field	The model name of the server.
Serial Number field	The serial number for the server.
PID field	The product ID.
UUID field	The UUID assigned to the server.
BIOS Version field	The version of the BIOS running on the server.
Description field	A user-defined description for the server.

Name	Description
Asset Tag field	A user-defined tag for the server. By default, the asset tag for a new server displays **Unknown**.

Viewing Cisco IMC Information

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Cisco Integrated Management Controller (Cisco IMC) Information** area of the **Server Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the Cisco IMC. By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.
IP Address field	The IP address for the Cisco IMC.
MAC Address field	The MAC address assigned to the active network interface to the Cisco IMC.
Firmware Version field	The current Cisco IMC firmware version.
Current Time field	The current date and time according to the Cisco IMC clock. **Note** Cisco IMC gets the current date and time from the server BIOS when the NTP is disabled. When NTP is enabled, BIOS and Cisco IMC gets the current time and date from the NTP server. To change this information, reboot the server and press **F2** when prompted to access the BIOS configuration menu. Then change the date or time using the options on the main BIOS configuration tab.
Local Time field	The local time of the region according to the chosen time zone.
Timezone field	Allows you to select a time zone by clicking on the **Select Timezone** option. In the **Select Timezone** pop-up screen, mouse over the map and click on the location to select your time zone or choose your time zone from the **Timezone** drop-down menu.

Viewing CPU Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **CPUs** tab.

Step 4 Review the following information for each CPU:

Name	Description
Socket Name field	The socket in which the CPU is installed.
Vendor field	The vendor for the CPU.
Status field	The status of the CPU.
Family field	The family to which this CPU belongs.
Version field	The version information of the CPU.
Speed field	The CPU speed, in megahertz.
Number of Cores field	The number of cores in the CPU.
Signature field	The signature information for the CPU.
Number of Threads field	The maximum number of threads that the CPU can process concurrently.

Viewing Memory Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Memory** tab.

Step 4 In the **Memory Summary** area, review the following summary information about memory:

Name	Description
Memory Speed field	The memory speed, in megahertz.
Failed Memory field	The amount of memory that is currently failing, in megabytes.

Name	Description
Total Memory field	The total amount of memory available on the server if all DIMMs are fully functional.
Ignored Memory field	The amount of memory currently not available for use, in megabytes.
Effective Memory field	The actual amount of memory currently available to the server.
Number of Ignored DIMMs field	The number of DIMMs that the server cannot access.
Redundant Memory field	The amount of memory used for redundant storage.
Number of Failed DIMMs field	The number of DIMMs that have failed and cannot be used.
Memory RAS Possible field	Details about the RAS memory configuration that the server supports.
Memory Configuration field	The current memory configuration. This can be one of the following: • **Maximum Performance**—The system automatically optimizes the memory performance. • **Mirroring**—The server maintains two identical copies of the data in memory. This option effectively halves the available memory on the server, as one half is automatically reserved for mirrored copy. • **Lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance.
DIMM location diagram	Displays the DIMM or memory layout for the current server.

Step 5 In the **DIMM Black Listing** area, view the overall status of a DIMM and also enable DIMM black listing.

Name	Description
Overall DIMM Status field	The overall status of a DIMM. This can be one of the following: • **Good**—The DIMM status is available. • **Severe Fault**— The DIMM status when uncorrectable ECC errors are present.
Enable DIMM Black List checkbox	Check this option to enable DIMM black listing.

Step 6 In the **Memory Details** table, review the following detailed information about each DIMM:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
Name column	The name of the DIMM slot in which the memory module is installed.

Name	Description
Capacity column	The size of the DIMM.
Channel Speed column	The clock speed of the memory channel, in megahertz.
Channel Type column	The type of memory channel.
Memory Type Detail column	The type of memory used in the device.
Bank Locator column	The location of the DIMM within the memory bank.
Manufacturer column	The vendor ID of the manufacturer. This can be one of the following: • **0x2C00**—Micron Technology, Inc. • **0x5105**—Qimonda AG i. In. • **0x802C**—Micron Technology, Inc. • **0x80AD**—Hynix Semiconductor Inc. • **0x80CE**—Samsung Electronics, Inc. • **0x8551**—Qimonda AG i. In. • **0xAD00**—Hynix Semiconductor Inc. • **0xCE00**—Samsung Electronics, Inc.
Serial Number column	The serial number of the DIMM.
Asset Tag column	The asset tag associated with the DIMM, if any.
Part Number column	The part number for the DIMM assigned by the vendor.
Visibility column	Whether the DIMM is available to the server.
Operability column	Whether the DIMM is currently operating correctly.
Data Width column	The amount of data the DIMM supports, in bits.

Viewing Power Supply Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Power Supplies** tab.

Step 4 Review the following information for each power supply:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
Device ID column	The identifier for the power supply unit.
Input column	The input into the power supply, in watts. **Note** This option is available only on some C-Series servers.
Max Output column	The maximum output from the power supply, in watts. **Note** This option is available only on some C-Series servers.
FW Version column	The firmware version for the power supply.
Product ID column	The product identifier for the power supply assigned by the vendor.

Viewing PCI Adapter Properties

Before you begin

The server must be powered on, or the properties will not display.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PCI Adapters** tab.

Step 4 In the **PCI Adapters** area, review the following information for the installed PCI adapters:

Name	Description
Slot ID column	The slot in which the adapter resides.
Product Name column	The name of the adapter.
Option ROM Status column	Indicates the Option ROM status. This can be one of the following: • Loaded—Data is available in the card. • Unloaded—Data is not available in the card. • Load Error—Card is present and Option ROM is enabled. But Option ROM failed to load due to an error in the card. **Note** This field is available only on some C-Series servers.

Name	Description
Firmware Version column	The firmware versions of the adapters. **Note** The firmware versions are displayed only for adapters that provide versions through the standard UEFI interface. For example, Intel LOM and Emulex Adapters.
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Viewing Nvidia GPU Card Information

This information is not available on all Cisco UCS C-series servers.

Before you begin

The server must be powered to view information on the available Nvidia GPU cards.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PCI Adapters** tab.

Step 4 In the **PCI Adapters** area, review the following information for the installed PCI adapters:

Name	Description
Slot ID column	The slot in which the adapter resides.
Product Name column	The name of the adapter.
Option ROM Status column	Indicates the Option ROM status. This can be one of the following: • Loaded—Data is available in the card. • Unloaded—Data is not available in the card. • Load Error—Card is present and Option ROM is enabled. But Option ROM failed to load due to an error in the card. **Note** This field is available only on some C-Series servers.

Name	Description
Firmware Version column	The firmware versions of the adapters. **Note** The firmware versions are displayed only for adapters that provide versions through the standard UEFI interface. For example, Intel LOM and Emulex Adapters.
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Step 5 Click the **Slot ID** or the **Product Name** of the Nvidia GPU card.

Step 6 In the **GPU Inventory** dialog box, review the following information for the Nvidia GPU card:

Name	Description
GPU ID	ID of the GPU in the NVidia card.
Temperature	The temperature of the GPU card in Celsius.

Viewing TPM Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **TPM** tab

Step 4 Review the following information:

Name	Description
Version field	The TPM version. This field displays **NA** if the TPM version details are not available.
Presence field	Presence of the TPM module on the host server. • **Equipped**—The TPM is present on the host server. • **Empty**—The TPM does not exist on the host server.
Model field	The model number of the TPM. This field displays **NA** if the TPM does not exist on the host server.

Name	Description
Enabled Status field	Whether or not the TPM is enabled. • **Enabled**—The TPM is enabled. • **Disabled**—The TPM is disabled. • **Unknown**—The TPM does not exist on the host server.
Vendor field	The name of the TPM vendor. This field displays **NA** if the TPM does not exist on the host server.
Active Status field	Activation status of the TPM. • **Activated**—The TPM is activated. • **Deactivated**—The TPM is deactivated. • **Unknown**—The TPM does not exist on the host server. **Note** In some C-series servers that have installed TPM version 2.0, **Active Status** is displayed as **NA**.
Serial field	The serial number of the TPM. This field displays **NA** if the TPM does not exist on the host server.
Ownership field	The ownership status of TPM. • **Owned**—The TPM is owned. • **Unowned**—The TPM is unowned. • **Unknown**—The TPM does not exist on the host server. **Note** In some C-series servers that have installed TPM version 2.0, **Ownership** status is displayed as **NA**.
Revision field	Revision number of the TPM. This field displays **NA** if the TPM does not exist on the host server.

Viewing PID Catalog

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PID Catalog** tab.

Step 4 In the **Actions** area,

Step 5 In the **Summary** area, review the following summary information about the PID catalog:

Name	Description
Upload Status field	The download status of the PID catalog. It can be any of the following: • Download in Progress • Download Successful • Download Error - TFTP File Not Found • Download Error - Connection Failed • Download Error - Access Denied • Download Error - File Not Found • Download Error - Download Failed • Activation Successful • Error - Unknown • N/A
Activation Status field	The activation status of the PID catalog.
Current Activated version field	The activated version of the PID catalog.

Step 6 In the **CPU** table, review the following information about CPU:

Name	Description
Socket field	The socket in which the CPU is installed.
Product ID field	The product ID for the CPU.
Model field	The model number of the CPU

Step 7 In the **Memory** table, review the following information about memory:

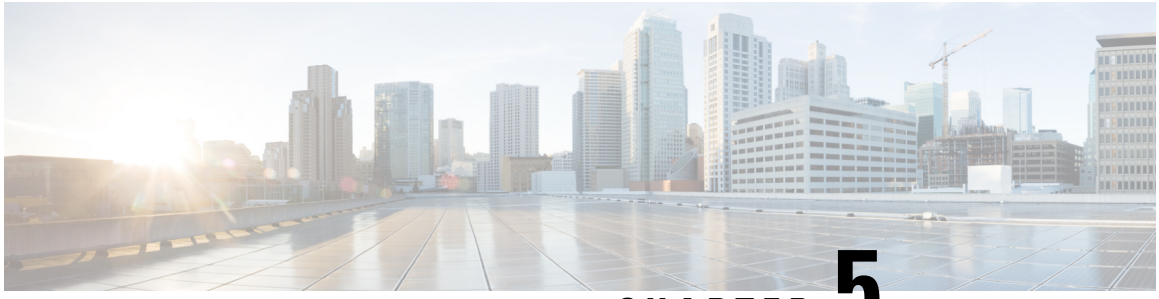
Name	Description
Name field	The name of the memory slot.
Product ID field	The product ID for the memory slot assigned by the vendor.
Vendor ID field	The ID assigned by the vendor.
Capacity field	The size of the memory.
Speed (MHz) field	The memory speed, in megahertz.

Step 8 In the **PCI Adapter** table, review the following information about PCI adapter:

Name	Description
Slot column	The slot in which the adapter resides.
Product ID column	The product ID for the adapter.
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Step 9 In the **HDD** table, review the following information about HDD:

Name	Description
Disk field	The disk of the hard drive.
Product ID field	The product ID for the hard drive.
Controller field	The system-defined name of the selected Cisco Flexible Flash controller. This name cannot be changed.
Vendor field	The vendor for the hard drive.
Model field	The model of the hard drive.



CHAPTER 5

Viewing Sensors

This chapter includes the following sections:

Viewing Power Supply Sensors

Tip Click a column header to sort the table rows according to the entries in that column.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Power Supply** tab.

Step 4 In the **Properties** area, the **Redundancy Status** field displays the status of the power supply redundancy of the server.

Step 5 In the **Discrete Sensors** area, you can view the following statistics for the server:

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The basic state of the sensor.

Step 6 In the **Threshold Sensors** area, you can view the following statistics for the server:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The current power usage, in watts.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Fan Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Fan** tab.

Step 4 View the following fan-related statistics for the server:

Tip Click a column header to sort the table rows according to the entries in that column.

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Speed column	The fan speed in RPM.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Temperature Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Temperature** tab.

Step 4 View the following temperature-related statistics for the server:

Tip Click a column header to sort the table rows according to the entries in that column.

Name	Description
Sensor Name column	The name of the sensor.
Sensor Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Temperature column	The current temperature, in Celsius and Fahrenheit.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Voltage Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Voltage** tab.

Step 4 View the following voltage-related statistics for the server:

Tip Click a column header to sort the table rows according to the entries in that column.

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Voltage column	The current voltage, in volts.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Current Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Current** tab.

Step 4 View the following current-related statistics on the **Current** tab:

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Current column	The current in amperes.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing LED Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **LEDs** tab.

Step 4 View the following LED-related statistics for the server:

Name	Description
Sensor Name column	The name of the sensor.
LED State column	Whether the LED is on, blinking, or off.
LED Color column	The current color of the LED. For details about what the colors mean, see the hardware installation guide for the type of server you are using.

Viewing Storage Sensors

Procedure

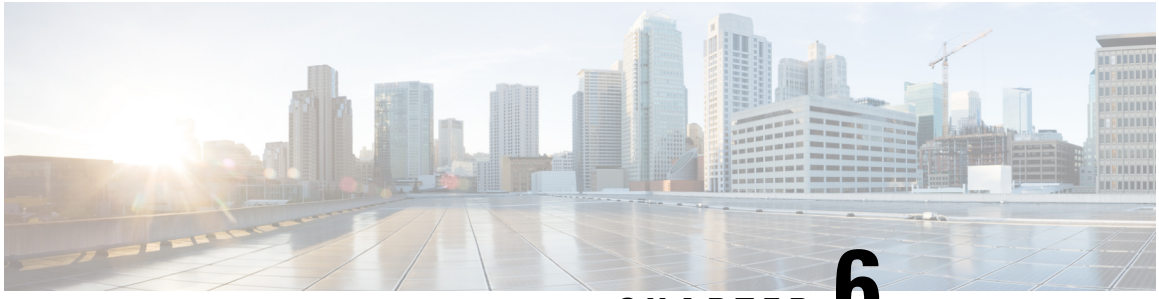
Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Storage** tab.

Step 4 View the following storage-related statistics for the server:

Name	Description
Name column	The name of the storage device.
Status column	A brief description of the storage device status.
LED Status column	The current LED color, if any. To make the physical LED on the storage device blink, select **Turn On** from the drop-down list. To let the storage device control whether the LED blinks, select **Turn Off**. **Note** This information is only available for some C-Series servers.



CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

Configuring Serial Over LAN

Serial over LAN enables the input and output of the serial port of a managed system to be redirected over IP. Configure and use serial over LAN on your server when you want to reach the host console with Cisco IMC.

Before you begin

You must log in as a user with admin privileges to configure serial over LAN.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Serial over LAN** tab.

Step 4 In the **Serial over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, Serial over LAN (SoL) is enabled on this server.

Name	Description
Baud Rate drop-down list	The baud rate the system uses for SoL communication. This can be one of the following: • **9600 bps** • **19.2 kbps** • **38.4 kbps** • **57.6 kbps** • **115.2 kbps**
Com Port drop-down list	The serial port through which the system routes SoL communication. **Note** This field is only available on some C-Series servers. If it is not available, the server always uses COM port 0 for SoL communication. You can select one of the following: • **com0**—SoL communication is routed through COM port 0, an externally accessible serial port that supports either a physical RJ45 connection to an external device or a virtual SoL connection to a network device. If you select this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device. • **com1**—SoL communication is routed through COM port 1, an internal port accessible only through SoL. If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0. **Note** Changing the Com Port setting disconnects any existing SoL sessions. **Note** This option is available only on some C-Series servers.
SSH Port filed	The port through which you can access Serial over LAN directly. The port enables you to by-pass the Cisco IMC shell to provide direct access to SoL. The valid range is 1024 to 65535. The default value is 2400. **Note** Changing the SSH Port setting disconnects any existing SSH sessions.

Step 5 Click **Save Changes**.

Configuring Virtual Media

Before you begin

You must log in as a user with admin privileges to configure virtual media.

Procedure

Step 1 In the **Navigation** pane, click the **Compute** tab.

Step 2 In the **Compute** tab, click the **Remote Management** tab.

Step 3 In the **Remote Management** tab, click the **Virtual Media** tab.

Step 4 In the **Virtual Media Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, virtual media is enabled. **Note** If you clear this check box, all virtual media devices are automatically detached from the host.
Active Sessions field	The number of virtual media sessions that are currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.
Low Power USB enabled check box	If checked, low power USB is enabled. If the low power USB is enabled, after mapping the ISO and rebooting the host, the virtual drives appear on the boot selection menu. But, while mapping an ISO to a server that has a UCS VIC P81E card and the NIC is in Cisco Card mode, this option must be disabled for the virtual drives to appear on the boot selection menu.

Step 5 Click **Save Changes**.

Creating a Cisco IMC-Mapped vMedia Volume

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **Cisco IMC-Mapped vMedia** area, click **Add New Mapping**.

Step 5 In the **Cisco IMC-Mapped vMedia** dialog box, update the following fields:

Name	Description
Volume field	The identity of the image mounted for mapping.
Mount Type drop-down list	The type of mapping. This can be one of the following: **Note** Ensure that the communication port of the mount type that you choose is enabled on the switch. For example, when you are using CIFS as your mount type, ensure port 445 (which is its communication port) is enabled on the switch. Similarly, enable ports 80 for HTTP, 443 for HTTPS and 2049 for NFS when you use them. • **NFS**—Network File System. • **CIFS**—Common Internet File System. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS-based system. **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server.
Remote Share field	The URL of the image to be mapped. The format depends on the selected **Mount Type**: • **NFS**—Use `serverip:/share`. • **CIFS**—Use `//serverip/share`. • **WWW(HTTP/HTTPS)**—Use `http[s]://serverip/share`.
Remote File field	The name and location of the .iso or .img file in the remote share.

Name	Description
Mount Options field	

Name	Description
	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • **`ro`** • **`rw`** **Note** The folder, which is shared, should have write permissions to use read-write option. Read-write option is available only for .img files. • **`nolock`** • **`noexec`** • **`soft`** • **`port=VALUE`** • **`timeo=VALUE`** • **`retry=VALUE`** If you are using **CIFS**, leave the field blank or enter one or more of the following: • **`soft`** • **`nounix`** • **`noserverino`** • **`guest`** • **`username=VALUE`**—ignored if **`guest`** is entered. • **`password=VALUE`**—ignored if **`guest`** is entered. • **`sec=VALUE`** The protocol to use for authentication when communicating with the remote server. Depending on the configuration of CIFS share, **VALUE** could be one of the following: • **None**—No authentication is used • **Ntlm**—NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **Ntlmi**—NTLMi security protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **Ntlmssp**—NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows

Name	Description
	2008 R2 and Windows 2012 R2. • **Ntlmsspi**—NTLMSSPi protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **Ntlmv2**—NTLMv2 security protocol. Use this option only with Samba Linux. • **Ntlmv2i**—NTLMv2i security protocol. Use this option only with Samba Linux. If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following: • `noauto` **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server. • `username=VALUE` • `password=VALUE`
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 Click **Save**.

Viewing Cisco IMC-Mapped vMedia Volume Properties

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **Cisco IMC-Mapped vMedia** area, select a row from the **Current Mappings** table.

Step 5 Click **Properties** and review the following information:

Name	Description
Volume field	The identity of the image mounted for mapping.

Name	Description
Mount Type drop-down list	The type of mapping. This can be one of the following: • **NFS**—Network File System. • **CIFS**—Common Internet File System. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS- based system. **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server.
Remote Share field	The URL of the image to be mapped.
Remote File field	The name and location of the .iso or .img file in the remote share.
Mount Options field	The selected mount options.
User Name field	The username, if any.
Password field	The password for the selected username, if any.

Removing a Cisco IMC-Mapped vMedia Volume

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **Cisco IMC-Mapped vMedia** area, click **Unmap**.

When you are prompted to save the mapping, click **Save**.

Remapping an Existing Cisco IMC vMedia Image

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.
Step 4 In the **Cisco IMC-Mapped vMedia** area, select a row from the **Current Mappings** table.
Step 5 Click **Remap**.

Deleting a Cisco IMC vMedia Image

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.
Step 4 In the **Cisco IMC-Mapped vMedia** area, select a row from the **Current Mappings** table.
Step 5 Click **Delete**.

KVM Console

The KVM console is an interface accessible from Cisco IMC 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.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network
- USB flash drive on the network

You can use the KVM console to install an OS on the server.

Note When launching the KVM Console from Internet Explorer 6 SP1 on Windows Server 2003, the browser will report that it cannot download a required file. If this occurs, click the browser Tools menu and select Internet Options. Click the Advanced tab and, in the Security section, uncheck the checkbox for "Do not save encrypted pages to disk." Launch the KVM Console again.

Configuring the Virtual KVM

Before you begin

You must log in as a user with admin privileges to configure the virtual KVM.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 On the **Virtual KVM** tab, complete the following fields:

Name	Description
Enabled check box	If checked, the virtual KVM is enabled. **Note** The virtual media viewer is accessed through the KVM. If you disable the KVM console, Cisco IMC also disables access to all virtual media devices attached to the host.
Max Sessions drop-down list	The maximum number of concurrent KVM sessions allowed. You can select any number between 1 and 4.
Active Sessions field	The number of KVM sessions running on the server.
Remote Port field	The port used for KVM communication.
Enable Video Encryption check box	If checked, the server encrypts all video information sent through the KVM.
Enable Local Server Video check box	If checked, the KVM session is also displayed on any monitor attached to the server.

Step 5 Click **Save Changes**.

Enabling the Virtual KVM

Before you begin

You must log in as a user with admin privileges to enable the virtual KVM.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 On the **Virtual KVM** tab, check the **Enabled** check box.

Step 5 Click **Save Changes**.

Disabling the Virtual KVM

Before you begin

You must log in as a user with admin privileges to disable the virtual KVM.

Procedure

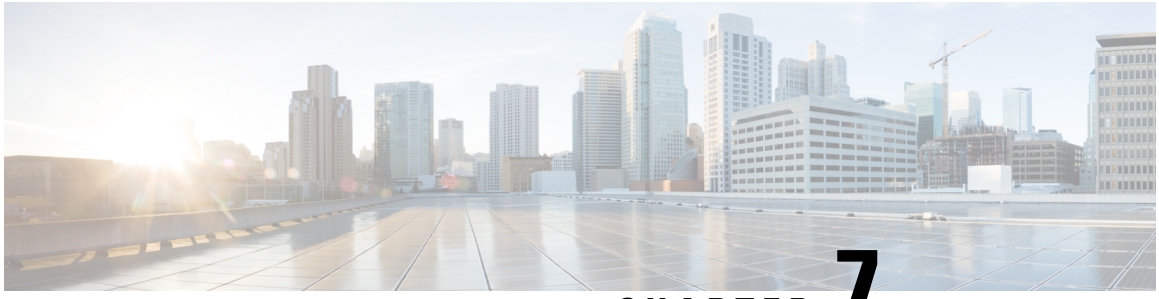
Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 On the **Virtual KVM** tab, uncheck the **Enabled** check box.

Step 5 Click **Save Changes**.



CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

Configuring Local Users

The Cisco IMC now implements a strong password policy wherein you are required to follow guidelines and set a strong password when you first log on to the server for the first time. The **Local User** tab displays a **Disable Strong Password** button which allows you to disable the strong password policy and set a password of your choice by ignoring the guidelines. Once you disable the strong password, an **Enable Strong Password** button is displayed. By default, the strong password policy is enabled.

Effective with Release 2.0(9f), you can choose to disable all local users and authenticate only using remote authentication including LDAP or Active Directory. To enable this, local user management supports the disabling of all Cisco IMC users including default admin user.

Warning If you choose to disable all Cisco IMC users and do not have an alternative method to log on to Cisco IMC, you may not be able access Cisco IMC. As a workaround, the Cisco IMC factory default is required, which then enables the default admin user credentials.

Before you begin

You must log in as a user with admin privileges to configure or modify local user accounts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 To configure or modify a local user account, click a row.

Step 5 In the **User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user.
Enabled check box	If checked, the user is enabled on the Cisco IMC.
Username field	The username for the user. Enter between 1 and 16 characters.

Role field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the KVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Change Password check box	If checked, when you save the changes the password for this user will be changed. You must check this box if this is a new user name.

Name	Description

New Password field	The password for this user name.
	Click the **Suggest** button to get a system generated password that you may want to use.
	When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed:
	• The password must have a minimum of 8 and a maximum of 20 characters.
	• The password must not contain the User's Name.
	• The password must contain characters from three of the following four categories:
	  • English uppercase characters (A through Z).
	  • English lowercase characters (a through z).
	  • Base 10 digits (0 through 9).
	  • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _,+ , =).
	These guidelines are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local User Management** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters.

Confirm New Password field	The password repeated for confirmation purposes.

Step 6 Click **Save Changes**.

LDAP Servers

Cisco IMC supports directory services that organize information in a directory, and manage access to this information. Cisco IMC supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, Cisco IMC supports Microsoft Active Directory (AD). Active Directory is a technology that provides a variety of network services including LDAP-like directory services, Kerberos-based authentication, and DNS-based naming. The Cisco IMC utilizes the Kerberos-based authentication service of LDAP.

When LDAP is enabled in the Cisco IMC, user authentication and role authorization is performed by the LDAP server for user accounts not found in the local user database. The LDAP user authentication format is username@domain.com.

By checking the Enable Encryption check box in the **LDAP Settings** area, you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The Cisco IMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.

Important For more information about altering the schema, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

Note This example creates a custom attribute named CiscoAVPair, but you can also use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales.

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

The following steps must be performed on the LDAP server.

Procedure

Step 1 Ensure that the LDAP schema snap-in is installed.

Step 2 Using the schema snap-in, add a new attribute with the following properties:

Properties	Value
Common Name	`CiscoAVPair`
LDAP Display Name	`CiscoAVPair`
Unique X500 Object ID	`1.3.6.1.4.1.9.287247.1`
Description	`CiscoAVPair`
Syntax	`Case Sensitive String`

Step 3 Add the CiscoAVPair attribute to the user class using the snap-in:

a) Expand the **Classes** node in the left pane and type `U` to select the user class.
b) Click the **Attributes** tab and click **Add**.
c) Type `C` to select the CiscoAVPair attribute.
d) Click **OK**.

Step 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to Cisco IMC:

Role	CiscoAVPair Attribute Value
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

Note For more information about adding values to attributes, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to do next

Use the Cisco IMC to configure the LDAP server.

Configuring LDAP Settings and Group Authorization in Cisco IMC

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **LDAP Settings** area, update the following properties:

Name	Description
Enable LDAP check box	If checked, user authentication and role authorization is performed first by the LDAP server, followed by user accounts that are not found in the local user database.
Base DN field	Base Distinguished Name. This field describes where to load users and groups from. It must be in the `dc=domain,dc=com` format for Active Directory servers.
Domain field	The IPv4 domain that all users must be in. This field is required unless you specify at least one Global Catalog server address.
Enable Encryption check box	If checked, the server encrypts all information it sends to the LDAP server.

Name	Description
Enable Binding CA Certificate check box	If checked, allows you to bind the LDAP CA certificate.
Timeout (0 - 180) seconds	The number of seconds the Cisco IMC waits until the LDAP search operation times out. If the search operation times out, Cisco IMC tries to connect to the next server listed on this tab, if one is available. **Note** The value you specify for this field could impact the overall time.
User Search Precedence	Allows you to specify the order of search between the local user database and LDAP user database. This can be one of the following: • **Local User Database** (Default setting) • **LDAP User Database**

Step 5 In the **Configure LDAP Servers** area, update the following properties:

Name	Description
Pre-Configure LDAP Servers radio button	If checked, the Active Directory uses the pre-configured LDAP servers.
LDAP Servers fields	
Server	The IP address of the 6 LDAP servers. If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers 4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers. **Note** You can provide the IP address of the host name as well.
Port	The port numbers for the servers. If you are using Active Directory for LDAP, then for servers 1, 2 and 3, which are domain controllers, the default port number is 389. For servers 4, 5 and 6, which are Global Catalogs, the default port number is 3268. LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port.

Name	Description
Use DNS to Configure LDAP Servers radio button	If checked, you can use DNS to configure access to the LDAP servers.
DNS Parameters fields	
Source	Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following: • **Extracted**—specifies using domain name extracted-domain from the login ID • **Configured**—specifies using the configured-search domain. • **Configured-Extracted**—specifies using the domain name extracted from the login ID than the configured-search domain.
Domain to Search	A configured domain name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.
Forest to Search	A configured forest name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.

Step 6 In the **Binding Parameters** area, update the following properties:

Name	Description
Method	It can be one of the following: • **Anonymous**—requires NULL username and password. If this option is selected and the LDAP server is configured for Anonymous logins, then the user can gain access. • **Configured Credentials**—requires a known set of credentials to be specified for the initial bind process. If the initial bind process succeeds, then the distinguished name (DN) of the user name is queried and re-used for the re-binding process. If the re-binding process fails, then the user is denied access. • **Login Credentials**—requires the user credentials. If the bind process fails, the user is denied access. By default, the **Login Credentials** option is selected.
Binding DN	The distinguished name (DN) of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.
Password	The password of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.

Step 7 In the **Search Parameters** area, update the following fields:

Name	Description
Filter Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **sAMAccountName**.
Group Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **memberOf**.

Name	Description
Attribute	An LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. The LDAP attribute can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, **CiscoAvPair**.
Nested Group Search Depth (1-128)	Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameter defines the depth of a nested group search.

Step 8 (Optional) In the **Group Authorization** area, update the following properties:

Name	Description
LDAP Group Authorization check box	If checked, user authentication is also done on the group level for LDAP users that are not found in the local user database. If you check this box, Cisco IMC enables the **Configure Group** button.
Nested Group Search Depth (1-128)	Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameter defines the depth of a nested group search.
Group Name column	The name of the group in the LDAP server database that is authorized to access the server.
Group Domain column	The LDAP server domain the group must reside in.

Role column	The role assigned to all users in this LDAP server group. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the KVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Name	Description
Configure button	Configures an active directory group.
Delete button	Deletes an existing LDAP group.

Step 9 Click **Save Changes**.

Setting User Search Precedence

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **LDAP Settings** area's **User Search Precedence** field, select **Local User Database** or **LDAP User Database**.

This field allows you to specify the order of search between the above options. **Local User Database** is the default option.

LDAP Certificates Overview

Cisco C-series servers allow an LDAP client to validate a directory server certificate against an installed CA certificate or chained CA certificate during an LDAP binding step. This feature is introduced in the event where anyone can duplicate a directory server for user authentication and cause a security breach due to the inability to enter a trusted point or chained certificate into the Cisco IMC for remote user authentication.

An LDAP client needs a new configuration option to validate the directory server certificate during the encrypted TLS/SSL communication.

Downloading an LDAP CA Certificate from Local Browser

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.

Note Only CA certificates or chained CA certificates must be used in Cisco IMC. By default, CA certificate is in .cer format. If it is a chained CA certificate, then it needs to be converted to .cer format before downloading it to Cisco IMC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **Certificate** area, click the **Download LDAP CA Certificate from Local Browser** link.

The **Download LDAP CA Certificate from Local Browser** dialog box appears.

Name	Description
File field	Using the **Browse** button, select an LDAP CA certificate stored on a drive that is local to the computer running the Cisco IMC GUI.
Download Certificate button	Allows you to download the certificate to the server.

Downloading an LDAP CA Certificate from Remote Server

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.

Note Only CA certificates or chained CA certificates must be used in Cisco IMC. By default, CA certificate is in .cer format. If it is a chained CA certificate, then it needs to be converted to .cer format before downloading it to Cisco IMC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **Certificate** area, click the **Download LDAP CA Certificate from Remote Server** link.

The **Download LDAP CA Certificate from Remote Server** dialog box appears.

Name	Description
Download LDAP CA Certificate from drop-down list	Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the LDAP CA certificate file should be stored. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the certificate from the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Download Certificate button	Allows you to download the certificate to the server.

Exporting an LDAP CA Certificate

Before you begin

You must log in as a user with admin privileges to perform this action.

You should have downloaded a signed LDAP CA Certificate before you can export it.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **Certificate** area, click the **Export LDAP CA Certificate** link.

The **Export LDAP CA Certificate** dialog box appears.

Name	Description
Export LDAP CA Certificate to Remote Server	Selecting this option allows you to choose the certificate from a remote server and export it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the LDAP CA certificate file should be exported. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the certificate from the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Export LDAP CA Certificate to Local File	Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.

Step 5 Click **Export**.

Pasting an LDAP CA Certificate

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.

Note Only CA certificates or chained CA certificates must be used in Cisco IMC. By default, CA certificate is in .cer format. If it is a chained CA certificate, then it needs to be converted to .cer format before downloading it to Cisco IMC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **Certificate** area, click the **Paste LDAP CA Certificate** link.

The **Paste LDAP CA Certificate** dialog box appears.

Name	Description
Certificate text field	Copy the entire content of the signed certificate and paste it here. **Note** Ensure the certificate is signed before downloading.

Step 5 Click **Save Certificate**.

Testing LDAP Binding

Before you begin

You must log in as a user with admin privileges to perform this action.

Note If you checked the **Enable Encryption** and the **Enable Binding CA Certificate** check boxes, enter the fully qualified domain name (FQDN) of the LDAP server in the LDAP Server field. To resolve the FQDN of the LDAP server, configure the preferred DNS of Cisco IMC network with the appropriate DNS IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **Certificate** area, click the **Test LDAP Binding** link.

The **Test LDAP CA Certificate Binding** dialog box appears.

Name	Description
Username field	Enter the user name.
Password field	Enter the corresponding password.

Step 5 Click **Test**.

Viewing User Sessions

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **User Management** pane, click the **Sessions** tab.

Step 4 View the following information about current user sessions:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
Session ID column	The unique identifier for the session.
User name column	The username for the user.
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**.
Type column	The type of session the user chose to access the server. This can be one of the following: • **webgui**— indicates the user is connected to the server using the web UI. • **CLI**— indicates the user is connected to the server using CLI. • **serial**— indicates the user is connected to the server using the serial port.

Name	Description
Action column	This column displays **N/A** when the SOL is enabled and **Terminate** when the SOL is disabled. You can terminate a session by clicking **Terminate** on the web UI.

Password Expiry

You can set a shelf life for a password, after which it expires. As an administrator, you can set this time in days. This configuration would be common to all users. Upon password expiry, the user is notified on login and would not be allowed to login unless the password is reset.

Note When you downgrade to an older database, existing users are deleted. The database returns to default settings. Previously configured users are cleared and the database is empty, that is, the database has the default username - 'admin' and password - 'password'. Since the server is left with the default user database, the change default credential feature is enabled. This means that when the 'admin' user logs on to the database for the first time after a downgrade, the user must mandatorily change the default credential.

Password Set Time

A 'Password set time' is configured for every existing user, to the time when the migration or upgrade occurred. For new users (users created after an upgrade), the Password Set time is configured to the time when the user was created, and the password is set. For users in general (new and existing), the Password Set Time is updated whenever the password is changed.

Configuring Password Expiry Duration

Before you begin

- You must enable password expiry.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **Local Users** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, update the following fields:

Name	Description
Enable Password Expiry check box	Checking this box allows you to configure the **Password Expiry Duration**. Uncheck the check box to disable it.

Name	Description
Password Expiry Duration field	The time period that you can set for the existing password to expire (from the time you set a new password or modify an existing one). The range is between 1 to 3650 days.
Password History field	The number of occurrences when a password was entered. When this is enabled, you cannot repeat a password. Enter a value between 0 to 5. Entering 0 disables this field.
Notification Period field	Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this field. **Note** The notification period time must be lesser than the password expiry duration.
Grace Period field	Time period till when the existing password can still be used, after it expires. Enter a value between 0 to 5 days. Entering 0 disables this field. **Note** The grace period time must be lesser than the password expiry duration.

Step 5 Click **Save Changes**.

Enabling Password Expiry

Before you begin

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

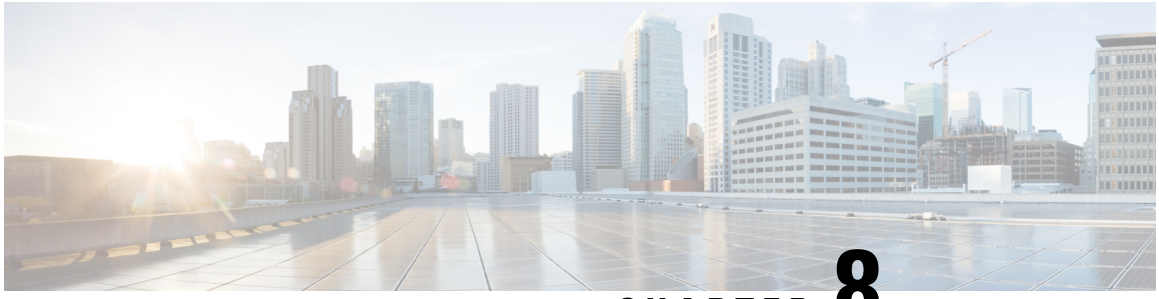
Step 3 In the **Local Users** area (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, check the **Enable Password Expiry** check box.

The **Password Expiry Duration** text field becomes editable and you can configure the duration by entering a number in days.

What to do next

Configure password expiry duration.



CHAPTER 8

Configuring Network-Related Settings

This chapter includes the following sections:

Server NIC Configuration

Server NICs

NIC Mode

The NIC mode setting determines which ports can reach the Cisco IMC. The following network mode options are available, depending on your platform:

- **Dedicated**—The management port that is used to access the Cisco IMC.
- **Shared LOM**—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC.
- **Shared LOM 10G**—Any 10G LOM port can be used to access the Cisco IMC.
- **Cisco Card**—Any port on the adapter card that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI).
- **Shared LOM Extended**—Any LOM port or Cisco adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support.

Note **Shared LOM Extended** and **Shared LOM 10G** are available only on some UCS C-Series servers.

NIC Redundancy

The following NIC redundancy options are available, depending on the selected NIC mode and your platform:

- **none**—Each port that is associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem.
- **active-active**—If supported, all ports that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to Cisco IMC.

  Note When using **active-active**, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using **active-standby**.

- **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode.

  Note If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same VLAN to ensure that traffic is secure regardless of which port is used.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the *Hardware Installation Guide* (HIG) for the type of server you are using. The C-Series HIGs are available at the following URL:
http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

Configuring Server NICs

Configure a server NIC when you want to set the NIC mode and NIC redundancy.

Before you begin

You must log in as a user with admin privileges to configure the NIC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **NIC Properties** area, update the following properties:

Name	Description Cisco IMC
NIC Mode drop-down list	The ports that can be used to access Cisco IMC. This can be one of the following: • **Dedicated**—The management port that is used to access the Cisco IMC. • **Shared LOM**—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC. • **Shared LOM 10G**—Any 10G LOM port can be used to access the Cisco IMC. • **Cisco Card**—Any port on the adapter card that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI). • **Shared LOM Extended**—Any LOM port or Cisco adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support. **Note** **Shared LOM Extended** and **Shared LOM 10G** are available only on some UCS C-Series servers. **Note** If you choose any of the shared LOM options, make sure that all host ports belong to the same subnet.

Name	Description Cisco IMC
VIC Slot drop-down list	The VIC slot that can be used for management functions in Cisco card mode. This can be one of the following: For C220 M4 servers, VIC slot options are as follows: • **Riser 1**—Slot 1 is selected. • **Riser 2**— Slot 2 is selected. • **FLEX LOM**—Slot 3 (MLOM) is selected. For C240 M4 servers, VIC slot options are as follows: • **Riser 1**—Slot 2 is the primary slot, but you can also use slot 1. • **Riser 2**— Slot 5 is the primary slot, but you can also use slot 4. • **FLEX LOM**—Slot 7 (MLOM) is selected. The following options are available only on some UCS C-Series servers: • **4** • **5** • **9** • **10** **Note** This option is available only on some UCS C-Series servers.
SIOC Slot drop-down list	Configures Cisco IMC network mode. Based on the card present in the System IO Controller (SIOC1), network mode can be changed to either Cisco card mode or Shared LOM mode. **Note** This option is available only on some UCS C-Series servers.

Name	Description Cisco IMC
NIC Redundancy drop-down list	The available NIC redundancy options depend on the selected NIC mode and the model of the server that you are using. If you do not see a particular option, it is not available for the selected mode or server model. This can be one of the following: • **none**—Each port that is associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem. • **active-active**—If supported, all ports that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to Cisco IMC. **Note** When using **active-active**, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using **active-standby**. • **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode. **Note** If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same VLAN to ensure that traffic is secure regardless of which port is used.
MAC Address field	The MAC address of the Cisco IMC network interface that is selected in the **NIC Mode** field.

Step 5 Click **Save Changes**.

Common Properties Configuration

Overview to Common Properties Configuration

Hostname

The Dynamic Host Configuration Protocol (DHCP) enhancement is available with the addition of the hostname to the DHCP packet, which can either be interpreted or displayed at the DHCP server side. The hostname, which is now added to the options field of the DHCP packet, sent in the DHCP DISCOVER packet that was initially sent to the DHCP server.

The default hostname of the server is changed from ucs-c2XX to CXXX-YYYYYY, where XXX is the model number and YYYYYY is the serial number of the server. This unique string acts as a client identifier, allows

you to track and map the IP addresses that are leased out to Cisco IMC from the DHCP server. The default serial number is provided by the manufacturer as a sticker or label on the server to help you identify the server.

Dynamic DNS

Dynamic DNS (DDNS) is used to add or update the resource records on the DNS server from Cisco IMC. You can enable Dynamic DNS by using either the web UI or CLI. When you enable the DDNS option, the DDNS service records the current hostname, domain name, and the management IP address and updates the resource records in the DNS server from Cisco IMC.

Note The DDNS server deletes the prior resource records (if any) and adds the new resource records to the DNS server if any one of the following DNS configuration is changed:

- Hostname
- Domain name in the LDAP settings
- When DDNS and DHCP are enabled, if the DHCP gets a new IP address or DNS IP or domain name due to a change in a network or a subnet.
- When DHCP is disabled and if you set the static IP address by using CLI or web UI.
- When you enter the **dns-use-dhcp** command.

Dynamic DNS Update Domain— You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of the Cisco IMC for the DDNS update.

Configuring Common Properties

Use common properties to describe your server.

Before you begin

You must log in as a user with admin privileges to configure common properties.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the Common Properties area, update the following properties:

a) In the **Hostname** field, enter the name of the host.

By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

Note If DHCP is enabled, the DHCP DISCOVER packet sent out will also carry the Cisco IMC hostname in it.

b) Check the **Dynamic DNS** check box.
c) In the **Dynamic DNS Update Domain** field, enter the domain name.

Step 5 Click **Save Changes**.

Configuring IPv4

Before you begin

You must log in as a user with admin privileges to configure IPv4.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **IPv4 Properties** area, update the following properties:

Name	Description
Enable IPv4 check box	If checked, IPv4 is enabled.
Use DHCP check box	If checked, Cisco IMC uses DHCP.
IP Address field	The IP address for Cisco IMC.
Subnet Mask field	The subnet mask for the IP address.
Gateway field	The gateway for the IP address.
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC retrieves the DNS server addresses from DHCP.
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.

Step 5 Click **Save Changes**.

Configuring IPv6

Before you begin

You must log in as a user with admin privileges to configure IPv6.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **IPv6 Properties** area, update the following properties:

Name	Description
Enable IPv6 check box	If checked, IPv6 is enabled.
Use DHCP check box	If checked, the Cisco IMC uses DHCP. **Note** Only stateful DHCP is supported.
IP Address field	The IPv6 address for the Cisco IMC. **Note** Only global unicast addresses are supported.
Prefix Length field	The prefix length for the IPv6 address. Enter a value within the range 1 to 127. The default value is 64.
Gateway field	The gateway for the IPv6 address. **Note** Only global unicast addresses are supported.
Obtain DNS Server Addresses from DHCP check box	If checked, the Cisco IMC retrieves the DNS server addresses from DHCP. **Note** You can use this option only when the **Use DHCP** option is enabled.
Preferred DNS Server field	The IPv6 address of the primary DNS server.
Alternate DNS Server field	The IPv6 address of the secondary DNS server.
Link Local Address field	The link local address for the IPv6 address.
Stateless Address Auto Configuration field	The Stateless Address Auto Configuration (SLAAC) depends on the Router Advertisement (RA) of the network.

Step 5 Click **Save Changes**.

Connecting to a VLAN

Before you begin

You must be logged in as admin to connect to a VLAN.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **VLAN Properties** area, update the following properties:

Name	Description
Enable VLAN check box	If checked, the Cisco IMC is connected to a virtual LAN. **Note** You can configure a VLAN or a port profile, but you cannot use both. If you want to use a port profile, make sure that this check box is not checked.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 5 Click **Save Changes**.

Connecting to a Port Profile

Note You can configure a port profile or a VLAN, but you cannot use both. If you want to use a port profile, make sure the **Enable VLAN** check box in the **VLAN Properties** area is not checked.

Before you begin

You must be logged in as admin to connect to a port profile.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **Port Profile** area, update the following properties:

Name	Description
Port Profile field	The port profile that Cisco IMC uses to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC 1225 Virtual Interface Card. Enter up to 80 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen. **Note** The port profile must be defined on the switch to which this server is connected.

Step 5 Click **Save Changes**.

Configuring Interface Properties

Overview to Network Interface Configuration

This support is added to configure network speed and duplex mode for the Cisco IMC management port. Auto Negotiation mode can be set for dedicated mode only. When auto negotiation is enabled the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. When auto negotiation is disabled, you can configure the network port speed (10 Mbps, 100 Mbps, or 1 Gbps) and set the duplex value at either full or half.

Port Properties can be managed in the following two modes:

- **Admin Mode**—You can configure the network speed and duplex values by disabling the **Auto Negotiation** option. The default value of the network speed in the admin mode is 100 Mbps and the duplex mode is set to Full. Before changing the network speed ensure that the switch you connected to has the same port speed.
- **Operation Mode**—Displays the operation network port speed and duplex values. If you enabled auto negotiation mode, the network port speed and duplex details of the switch are displayed. If unchecked, the network port speed and duplex values that you set at the **Admin Mode** are displayed.

When you reset Cisco IMC 1.5(x), 2.0(1), and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default.

For C3160 servers, if you reset to factory defaults, **Dedicated** mode is configured to **Full** duplex mode with 100 Mbps speed by default.

Configuring Interface Properties

The settings on the switch must match with the Cisco IMC settings to avoid any speed or duplex mismatch.

Important This action is available only on some UCS C-Series servers.

Procedure

Step 1 Log in to Cisco IMC Web UI.

Step 2 In the **Navigation** pane, click the **Admin** tab.

Step 3 On the **Admin** tab, click **Network**.

Step 4 In the **Network** pane, click the **Network Settings** tab.

Step 5 In the **NIC Properties** area, select **Dedicated** mode from the **NIC Mode** drop down list.

NIC mode must be in dedicated to set any network configuration like net speed and duplex.

Step 6 In the **Port Properties** area:

- If you check the **Auto Negotiation** check box, the setting for duplex will be ignored by the system. The Cisco IMC retains the speed at which the switch is configured.
- If you uncheck the **Auto Negotiation** check box, you can set duplex. Else, a default speed of 100 Mbps will be applied, and duplex will retain its previous value.

By default, the duplex mode is set to **Full**.

Step 7 Click **Save Changes**.

Network Security Configuration

Network Security

The Cisco IMC uses IP blocking as network security. IP blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers.

IP banning is commonly used to protect against denial of service (DoS) attacks. Cisco IMC bans IP addresses by setting up an IP blocking fail count.

Configuring Network Security

Configure network security if you want to set up an IP blocking fail count.

Before you begin

You must log in as a user with admin privileges to configure network security.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Security** tab.

Step 4 In the **IP Blocking Properties** area, update the following properties:

Name	Description
Enable IP Blocking check box	Check this box to enable IP blocking.
IP Blocking Fail Count field	The number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. The number of unsuccessful login attempts must occur within the time frame specified in the **IP Blocking Fail Window** field. Enter an integer between 3 and 10.
IP Blocking Fail Window field	The length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.
IP Blocking Penalty Time field	The number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.

Step 5 In the **IP Filtering** area, update the following properties:

Name	Description
Enable IP Filtering check box	Check this box to enable IP filtering.
IP Filter fields	To provide secure access to the server, you can now set a filter to allow only a selected set of IPs to access it. This option provides four slots for storing IP addresses (IP Filter 1, 2, 3, and 4). You can either assign a single IP address or a range of IP addresses while setting the IP filters. Once you set the IP filter, you would be unable to access the server using any other IP address.

Step 6 Click **Save Changes**.

Network Time Protocol Settings

Network Time Protocol Service Setting

By default, when Cisco IMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure Cisco IMC to synchronize the time with an NTP server. The NTP server does not run in Cisco IMC by default. 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 or time source servers. When you enable the NTP service, Cisco IMC synchronizes the time with the configured NTP server. The NTP service can be modified only through Cisco IMC.

Note To enable the NTP service, it is preferable to specify the IP address of a server rather than the DNS address.

Configuring Network Time Protocol Settings

Configuring NTP disables the IPMI **Set SEL time** command.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **NTP Settings** tab.

Step 4 In the **NTP Settings** area, update the following properties:

Name	Description
Enable NTP	Check this box to enable the NTP service.
Server 1	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 2	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 3	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 4	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Status message	Indicates whether or not the server is able to synchronize its time with the remote NTP server. This can be one of the following: • **synchronized to NTP server (RefID) at stratum 7**— When the NTP service is enabled and multiple or individual IPv4 or IPv6 based NTP servers are added. • **unsynchronized** — When the NTP service is enabled and an unknown or unreachable server is added. • **NTP service disabled** — When the NTP service is disabled.

Step 5 Click **Save Changes**.

Pinging an IP Address from the Web UI

Effective with this release, you can ping an IP address from the Cisco IMC web UI using a **Ping** button available on the toolbar. This would help validate the network connectivity to the IP address available in Cisco IMC. You can ping an IPv4, IPv6 or a host IP address using this button.

Before you begin

You must log in with user or admin privileges to perform this task.

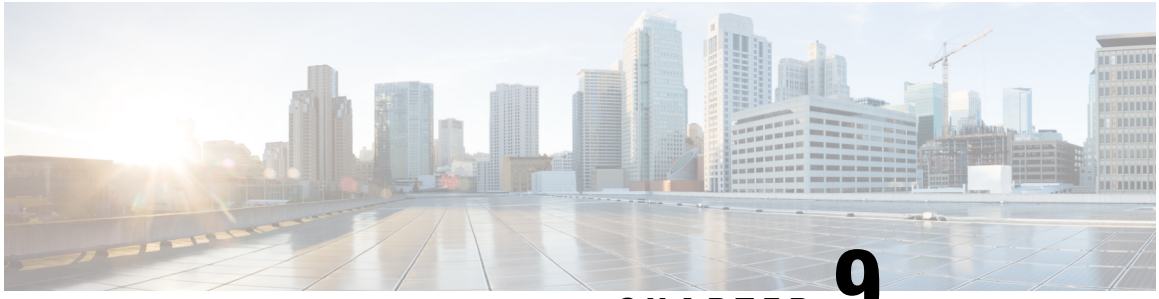
Procedure

Step 1 In the toolbar above the work pane, click the **Ping** icon.

Step 2 In the **Ping Details** dialog box, update the following fields:

Name	Description
Hostname/IP Address column	Hostname or IP address you want to reach out to.
Number of Retries column	The maximum number of retries allowed to ping the IP address. The default value is 3. The valid range is from 1 to 10.
Timeout column	The maximum response time for a pinging activity. The default value is 10 seconds. The valid range is from 1 to 20 seconds.
Ping Status area	Displays results of the pinging activity.

Step 3 Click **Ping**.



CHAPTER 9

Managing Network Adapters

This chapter includes the following sections:

Overview of the Cisco UCS C-Series Network Adapters

Note The procedures in this chapter are available only when a Cisco UCS C-Series network adapter is installed in the chassis.

A Cisco UCS C-Series network adapter can be installed to provide options for I/O consolidation and virtualization support. The following adapters are available:

- Cisco UCS VIC 1225 Virtual Interface Card
- Cisco UCS VIC 1227T Virtual Interface Card
- Cisco UCS VIC 1385 Virtual Interface Card
- Cisco UCS VIC 1387 Virtual Interface Card

Note You must have same generation VIC cards on a server. For example, you cannot have a combination of 3rd generation and 4th generation VIC cards on a single server.

The interactive *UCS Hardware and Software Interoperability Utility* lets you view the supported components and configurations for a selected server model and software release. The utility is available at the following URL: http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

Cisco UCS VIC 1225 Virtual Interface Card

The Cisco UCS VIC 1225 Virtual Interface Card is a high-performance, converged network adapter that provides acceleration for the various new operational modes introduced by server virtualization. It brings superior flexibility, performance, and bandwidth to the new generation of Cisco UCS C-Series Rack-Mount Servers.

The Cisco UCS VIC 1225 implements the Cisco Virtual Machine Fabric Extender (VM-FEX), which unifies virtual and physical networking into a single infrastructure. It provides virtual-machine visibility from the physical network and a consistent network operations model for physical and virtual servers. In virtualized environments, this highly configurable and self-virtualized adapter provides integrated, modular LAN interfaces on Cisco UCS C-Series Rack-Mount Servers. Additional features and capabilities include:

- Supports up to 256 PCIe virtual devices, either virtual network interface cards (vNICs) or virtual host bus adapters (vHBAs), with high I/O operations per second (IOPS), support for lossless Ethernet, and 20 Gbps to servers.
- PCIe Gen2 x16 helps assure optimal bandwidth to the host for network-intensive applications with a redundant path to the fabric interconnect.
- Half-height design reserves full-height slots in servers for Cisco certified third-party adapters.
- Centrally managed by Cisco UCS Manager with support for Microsoft Windows, Red Hat Enterprise Linux, SUSE Linux, VMware vSphere, and Citrix XenServer.

Cisco UCS VIC 1385 Virtual Interface Card

The Cisco UCS VIC 1385 Virtual Interface Cardis a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable half-height PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers. It incorporates Cisco's next-generation converged network adapter (CNA) technology, with a comprehensive feature set, providing investment protection for future feature software releases. The card enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1385 card supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure. Additional features and capabilities include:

- Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect
- The Cisco UCS VIC 1385 Virtual Interface Card provides high network performance and low latency for the most demanding applications such as SMB-Direct, VMQ, DPDK, and Cisco NetFlow

Cisco UCS VIC 1227T Virtual Interface Card

The Cisco UCS VIC 1227T Virtual Interface Card is a dual-port 10GBASE-T (RJ-45) 10-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)–capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter designed exclusively for Cisco UCS C-Series Rack Servers. New to Cisco rack servers, the mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing Fibre Channel connectivity over low-cost twisted pair cabling with a bit error rate (BER) of 10 to 15 up to 30 meters and investment protection for future feature releases. The mLOM card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1227T Virtual Interface Card supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment. Additional features and capabilities include:

- Stateless and agile design - The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure.
- Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect.
- Cisco SingleConnect technology provides an exceptionally easy, intelligent, and efficient way to connect and manage computing in the data center. Cisco SingleConnect technology dramatically simplifies the way that data centers connect to rack and blade servers, physical servers, virtual machines, LANs, SANs, and management networks.

Cisco UCS VIC 1387 Virtual Interface Card

The Cisco UCS VIC 1387 Virtual Interface Card is a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable half-height PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers. It incorporates Cisco's next-generation converged network adapter (CNA) technology, with a comprehensive feature set, providing investment protection for future feature software releases. The card enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1387 card supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure. Additional features and capabilities include:

- Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect
- The Cisco UCS VIC 1387 Virtual Interface Card provides high network performance and low latency for the most demanding applications such as SMB-Direct, VMQ, DPDK, and Cisco NetFlow

Viewing Network Adapter Properties

Before you begin

- The server must be powered on, or the properties will not display.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Network Adapters** tab.

Step 4 In the **Network Adapters** area, review the following information:

Name	Description
Slot column	The slot in which the adapter is installed.
Product Name column	The product name for the adapter.
Number of Interfaces column	The number of interfaces for the adapter.
External Ethernet Interfaces	**ID**—The ID for the external ethernet interface. **MAC Address**—The MAC address for the external ethernet interface.

Step 5 In the **Adapter Card** area, review the following information:

Name	Description
Slot column	The slot in which the network adapter resides.
Product Name column	The product name of the network adapter.
Number of Interfaces column	The number of interfaces for the network adapter.
External Ethernet Interfaces column	
ID column	The ID number of the external ethernet interface.
MAC Address column	The MAC address of the external ethernet interface.

Viewing VIC Adapter Properties

Before you begin

- The server must be powered on, or the properties will not display.

- A supported Virtual Interface Card (VIC) must be installed in the chassis and the server must be powered on.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, click an adapter in the table to display its properties.

The resources of the selected adapter appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the **Adapter Cards** area, review the following information for the installed adapters:

Name	Description
PCI Slot column	The PCI slot in which the adapter is installed.
Product Name column	The product name for the adapter.
Serial Number column	The serial number for the adapter.
Product ID column	The product ID for the adapter.
Vendor column	The vendor for the adapter.
Cisco IMC Management Enabled column	Whether the adapter is able to manage Cisco IMC. This functionality depends on the type of adapter installed and how it is configured. For details, see the hardware installation guide for the type of server you are using.

Step 6 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 7 In the **Adapter Card Properties** area, review the following information for the adapter:

Name	Description
PCI Slot field	The PCI slot in which the adapter is installed. **Note** For the C220 M4 and C240 M4 servers, PCI slot could also display as **MLOM**.
Vendor field	The vendor for the adapter.
Product Name field	The product name for the adapter.
Product ID field	The product ID for the adapter.
Serial Number field	The serial number for the adapter.
Version ID field	The version ID for the adapter.
Hardware Revision field	The hardware revision for the adapter.

Name	Description
Cisco IMC Management Enabled field	If this field displays **yes**, then the adapter is functioning in Cisco Card Mode and passing Cisco IMC management traffic through to the server Cisco IMC.
Configuration Pending field	If this field displays **yes**, the adapter configuration has changed in Cisco IMC but these changes have not been communicated to the host operating system. To activate the changes, an administrator must reboot the adapter.
Description field	The user-defined description for the adapter, if any.
FIP Mode field	Whether FCoE Initialization Protocol (FIP) mode is enabled. FIP mode ensures that the adapter is compatible with current FCoE standards.
LLDP field	Whether the LLDP option is enabled for this VIC card. **Note** This option is available only on some UCS C-Series servers.
VNTAG Mode field	Whether virtual network tag (VNTAG) is enabled. If VNTAG mode is enabled: • vNICs and vHBAs can be assigned to a specific channel • vNICs and vHBAs can be associated with a port profile • vNICs can fail over to another vNIC if there are communication problems
ISCSI Boot Capable field	Whether iSCSI boot is supported on the adapter.
usNIC Capable field	Whether the adapter and the firmware running on the adapter support the usNIC.

Step 8 In the **External Ethernet Interfaces** area, review the following information for the adapter:

Name	Description
ID column	The uplink port ID.
MAC Address column	The MAC address of the uplink port.

Name	Description
Link State column	The current operational state of the uplink port. This can be one of the following: • **Fault** • **Link Up** • **Link Down** • **SFP ID Error** • **SFP Not Installed** • **SFP Security Check Failed** • **Unsupported SFP**
Encap column	The mode in which adapter operates. This can be one of the following: • **CE**—Classical Ethernet mode. • **NIV**—Network Interface Virtualization mode.
Admin Speed column	The data transfer rate for the port. This can be one of the following: • **Auto** • **1 Gpbs** • **10 Gpbs** • **40 Gpbs** **Note** This option is only available for some adapter cards.
Operating Speed column	The operating rate for the port. This can be one of the following: • **Auto** • **1 Gpbs** • **10 Gpbs** • **40 Gpbs** **Note** This option is only available for some adapter cards.
Training Link column	Indicates if link training is enabled on the port.

Name	Description
Connector Present column	Indicated whether or not the connector is present. This can be one of the following: • **Yes**—Connector is present. • **No**—Connector not present. **Note** This option is only available for some adapter cards.
Connector Supported column	Indicates whether or not the connector is supported by Cisco. This can be one of the following: • **Yes**—The connector is supported by Cisco. • **No**—The connector is not supported by Cisco. If the connector is not supported then the link will not be up. **Note** This option is only available for some adapter cards.
Connector Type column	The type of the connector. **Note** This option is only available for some adapter cards.
Connector Vendor column	The vendor for the connector. **Note** This option is only available for some adapter cards.
Connector Part Number column	The part number of the connector. **Note** This option is only available for some adapter cards.
Connector Part Revision column	The part revision number of the connector. **Note** This option is only available for some adapter cards.

Step 9 In the **Firmware** area, review the following information for the adapter:

Name	Description
Running Version field	The firmware version that is currently active.
Backup Version field	The alternate firmware version installed on the adapter, if any. The backup version is not currently running. To activate it, administrators can click **Activate Firmware** in the **Actions** area. **Note** When you install new firmware on the adapter, any existing backup version is deleted and the new firmware becomes the backup version. You must manually activate the new firmware if you want the adapter to run the new version.
Startup Version field	The firmware version that will become active the next time the adapter is rebooted.

Name	Description
Bootloader Version field	The bootloader version associated with the adapter card.
Status field	The status of the last firmware activation that was performed on this adapter. **Note** The status is reset each time the adapter is rebooted.

What to do next

To view the properties of virtual NICs and virtual HBAs, see the following sections:

- Viewing vNIC Properties, on page 154
- Viewing vHBA Properties, on page 140

Viewing Storage Adapter Properties

Before you begin

- The server must be powered on.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click **Storage Adapters** tab and review the following information:

Name	Description
Controller field	The type of controller.
PCI Slot field	The PCI slot in which the adapter is installed.
Product Name field	The product name for the adapter.
Serial Number field	The serial number for the adapter.
Firmware Package Build field	The installed firmware package for the adapter.
Product ID field	The product ID for the adapter.
Battery Status field	The vendor for the adapter.
Cache Memory Size field	The size of the cache memory, in megabytes.

Name	Description
Health field	The health of the adapter. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault** • **N/A**
Details link	Click the **Details** link to view the **Storage** tab.

Managing vHBAs

Guidelines for Managing vHBAs

When managing vHBAs, consider the following guidelines and restrictions:

- The Cisco UCS Virtual Interface Cards provide two vHBAs and two vNICs by default. You can create up to 14 additional vHBAs or vNICs on these adapter cards.

  The Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. You can create up to 10 additional vHBAs or vNICs on these adapter cards.

  Note If Network Interface Virtualization (NIV) mode is enabled for the adapter, you must assign a channel number to a vHBA when you create it.

- When using the Cisco UCS Virtual Interface Cards in an FCoE application, you must associate the vHBA with the FCoE VLAN. Follow the instructions in the **Modifying vHBA Properties** section to assign the VLAN.
- After making configuration changes, you must reboot the host for settings to take effect.

Viewing vHBA Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Properties** to open the **vHBA Properties** dialog box.

Step 8 In the **General** area, review the information in the following fields:

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
Target WWNN field	The WWNN associated with the vHBA. To let the system generate the WWNN, select **AUTO**. To specify a WWNN, click the second radio button and enter the WWNN in the corresponding field.
Target WWPN field	The WWPN associated with the vHBA. To let the system generate the WWPN, select **AUTO**. To specify a WWPN, click the second radio button and enter the WWPN in the corresponding field.
FC SAN Boot check box	If checked, the vHBA can be used to perform a SAN boot.
Enable Persistent LUN Binding check box	If checked, any LUN ID associations are retained in memory until they are manually cleared.
Uplink Port field	The uplink port associated with the vHBA. **Note** This value cannot be changed for the system-defined vHBAs fc0 and fc1.
MAC Address field	The MAC address associated with the vHBA. To let the system generate the MAC address, select **AUTO**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Default VLAN field	If there is no default VLAN for this vHBA, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field.
Class of Service drop-down list	The CoS for the vHBA. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.

Name	Description
Rate Limit field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
PCIe Device Order field	The order in which this vHBA will be used. To let the system set the order, select **ANY**. To specify an order, select the second radio button and enter an integer between 0 and 17.
EDTOV field	The error detect timeout value (EDTOV), which is the number of milliseconds to wait before the system assumes that an error has occurred. Enter an integer between 1,000 and 100,000. The default is 2,000 milliseconds.
RATOV field	The resource allocation timeout value (RATOV), which is the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000 milliseconds.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112.
Channel Number field	The channel number that will be assigned to this vHBA. Enter an integer between 1 and 1,000. **Note** VNTAG mode is required for this option.
Port Profile drop-down list	The port profile that should be associated with the vHBA, if any. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.

Step 9 In the **Error Recovery** area, review the information in the following fields:

Name	Description
Enable FCP Error Recovery check box	If checked, the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE).

Name	Description
Link Down Timeout field	The number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240,000.
Port Down I/O Retries field	The number of times an I/O request to a port is returned because the port is busy before the system decides the port is unavailable. Enter an integer between 0 and 255.
I/O Timeout Retry field	The time period till which the system waits for timeout before retrying. When a disk does not respond for I/O within the defined timeout period, the driver aborts the pending command, and resends the same I/O after the timer expires. Enter an integer between 1 and 59.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240,000.

Step 10 In the **Fibre Channel Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSIx**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 11 In the **Fibre Channel Port** area, review the information in the following fields:

Name	Description
I/O Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1,024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 1,024. The recommended value is 1024.
LUN Queue Depth field	The number of commands that the HBA can send or receive in a single chunk per LUN. This parameter adjusts the initial queue depth for all LUNs on the adapter. Default value is 20 for physical miniports and 250 for virtual miniports.

Step 12 In the **Fibre Channel Port FLOGI** area, review the information in the following fields:

Name	Description
FLOGI Retries field	The number of times that the system tries to log in to the fabric after the first failure. To specify an unlimited number of retries, select the **INFINITE** radio button. Otherwise select the second radio button and enter an integer into the corresponding field.
FLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 13 In the **Fibre Channel Port PLOGI** area, review the information in the following fields:

Name	Description
PLOGI Retries field	The number of times that the system tries to log in to a port after the first failure. Enter an integer between 0 and 255.
PLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 14 In the **SCSI I/O** area, review the information in the following fields:

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. Enter an integer between 1 and 8.
CDB Transmit Queue Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 15 In the **Receive/Transmit Queues** area, review the information in the following fields:

Name	Description
FC Work Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.
FC Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 128.

Modifying vHBA Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Properties** to open the **vHBA Properties** dialog box.

Step 8 In the **General** area, update the following fields:

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
Target WWNN field	The WWNN associated with the vHBA. To let the system generate the WWNN, select **AUTO**. To specify a WWNN, click the second radio button and enter the WWNN in the corresponding field.
Target WWPN field	The WWPN associated with the vHBA. To let the system generate the WWPN, select **AUTO**. To specify a WWPN, click the second radio button and enter the WWPN in the corresponding field.
FC SAN Boot check box	If checked, the vHBA can be used to perform a SAN boot.
Enable Persistent LUN Binding check box	If checked, any LUN ID associations are retained in memory until they are manually cleared.
Uplink Port field	The uplink port associated with the vHBA. **Note** This value cannot be changed for the system-defined vHBAs fc0 and fc1.
MAC Address field	The MAC address associated with the vHBA. To let the system generate the MAC address, select **AUTO**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.

Name	Description
Default VLAN field	If there is no default VLAN for this vHBA, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field.
Class of Service drop-down list	The CoS for the vHBA. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
PCIe Device Order field	The order in which this vHBA will be used. To let the system set the order, select **ANY**. To specify an order, select the second radio button and enter an integer between 0 and 17.
EDTOV field	The error detect timeout value (EDTOV), which is the number of milliseconds to wait before the system assumes that an error has occurred. Enter an integer between 1,000 and 100,000. The default is 2,000 milliseconds.
RATOV field	The resource allocation timeout value (RATOV), which is the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000 milliseconds.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112.
Channel Number field	The channel number that will be assigned to this vHBA. Enter an integer between 1 and 1,000. **Note** VNTAG mode is required for this option.
Port Profile drop-down list	The port profile that should be associated with the vHBA, if any. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.

Step 9 In the **Error Recovery** area, update the following fields:

Name	Description
Enable FCP Error Recovery check box	If checked, the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE).
Link Down Timeout field	The number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240,000.
Port Down I/O Retries field	The number of times an I/O request to a port is returned because the port is busy before the system decides the port is unavailable. Enter an integer between 0 and 255.
I/O Timeout Retry field	The time period till which the system waits for timeout before retrying. When a disk does not respond for I/O within the defined timeout period, the driver aborts the pending command, and resends the same I/O after the timer expires. Enter an integer between 1 and 59.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240,000.

Step 10 In the **Fibre Channel Interrupt** area, update the following fields:

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSIx**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 11 In the **Fibre Channel Port** area, update the following fields:

Name	Description
I/O Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1,024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 1,024. The recommended value is 1024.

Name	Description
LUN Queue Depth field	The number of commands that the HBA can send or receive in a single chunk per LUN. This parameter adjusts the initial queue depth for all LUNs on the adapter. Default value is 20 for physical miniports and 250 for virtual miniports.

Step 12 In the **Fibre Channel Port FLOGI** area, update the following fields:

Name	Description
FLOGI Retries field	The number of times that the system tries to log in to the fabric after the first failure. To specify an unlimited number of retries, select the **INFINITE** radio button. Otherwise select the second radio button and enter an integer into the corresponding field.
FLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 13 In the **Fibre Channel Port PLOGI** area, update the following fields:

Name	Description
PLOGI Retries field	The number of times that the system tries to log in to a port after the first failure. Enter an integer between 0 and 255.
PLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 14 In the **SCSI I/O** area, update the following fields:

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. Enter an integer between 1 and 8.
CDB Transmit Queue Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 15 In the **Receive/Transmit Queues** area, update the following fields:

Name	Description
FC Work Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.

Name	Description
FC Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 128.

Step 16 Click **Save Changes**.

Creating a vHBA

The adapter provides two permanent vHBAs. If NIV mode is enabled, you can create up to 16 additional vHBAs.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, choose one of these actions:

- To create a vHBA using default configuration settings, click **Add**.
- To create a vHBA using the same configuration settings as an existing vHBA, select that vHBA and click **Clone**.

The **Add vHBA** dialog box appears.

Step 7 In the **Add vHBA** dialog box, enter a name for the vHBA in the **Name** entry box.

Step 8 Click **Add vHBA**.

What to do next

- Reboot the server to create the vHBA.
- If configuration changes are required, configure the new vHBA as described in Modifying vHBA Properties, on page 145.

Deleting a vHBA

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Note You cannot delete either of the two default vHBAs, **fc0** or **fc1**.

Step 7 Click **Delete** and click **OK** to confirm.

vHBA Boot Table

In the vHBA boot table, you can specify up to four LUNs from which the server can boot.

Creating a Boot Table Entry

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Boot Table** to open the **Boot Table** dialog box for the selected vHBA.

Step 8 In the **Boot Table** dialog box, click **Add** to open the **Add Boot Entry** dialog box.

Step 9 In the **Add Boot Entry** dialog box, update the following fields:

Name	Description
Target WWPN field	The World Wide Port Name (WWPN) that corresponds to the location of the boot image. Enter the WWPN in the format **`hh:hh:hh:hh:hh:hh:hh:hh`**.
LUN ID field	The LUN ID that corresponds to the location of the boot image. Enter an ID between 0 and 255.
Add Boot Entry button	Adds the specified location to the boot table.
Reset Values button	Clears the values currently entered in the fields.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 10 Click **Add Boot Entry**.

Deleting a Boot Table Entry

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Boot Table** to open the **Boot Table** dialog box for the selected vHBA.

Step 8 In the **Boot Table** dialog box, click the entry to be deleted.

Step 9 Click **Delete** and click **OK** to confirm.

vHBA Persistent Binding

Persistent binding ensures that the system-assigned mapping of Fibre Channel targets is maintained after a reboot.

Viewing Persistent Bindings

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Persistent Bindings** to open the **Persistent Bindings** dialog box for the selected vHBA.

Step 8 In the **Persistent Bindings** dialog box for the selected vHBA, review the following information:

Name	Description
Index column	The unique identifier for the binding.
Target WWPN column	The target World Wide Port Name with which the binding is associated.
Host WWPN column	The host World Wide Port Name with which the binding is associated.
Bus ID column	The bus ID with which the binding is associated.
Target ID column	The target ID on the host system with which the binding is associated.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.
Close button	Closes the dialog box and saves your changes.

Step 9 Click **Close**.

Rebuilding Persistent Bindings

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Persistent Bindings** to open the **Persistent Bindings** dialog box for the selected vHBA.

Step 8 In the **Persistent Bindings** dialog box for the selected vHBA, click **Rebuild Persistent Bindings**.

Step 9 Click **Close**.

Managing vNICs

Guidelines for Managing vNICs

When managing vNICs, consider the following guidelines and restrictions:

- The Cisco UCS Virtual Interface Cards provide two vHBAs and two vNICs by default. You can create up to 14 additional vHBAs or vNICs on these adapter cards.

  The Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. You can create up to 10 additional vHBAs or vNICs on these adapter cards.

  Note If Network Interface Virtualization (NIV) mode is enabled for the adapter, you must assign a channel number to a vNIC when you create it.

- After making configuration changes, you must reboot the host for settings to take effect.

Cisco C-series servers use Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) for packet transfers. RoCE defines the mechanism of performing RDMA over ethernet, based on the similar mechanism of RDMA over Infiniband. However, RoCE, with its performance oriented characteristics, delivers a superior performance compared to traditional network socket implementation because of the lower latency, lower CPU utilization and higher utilization of network bandwidth. RoCE meets the requirement of moving large amount of data across networks very efficiently.

The RoCE firmware requires the following configuration parameters provided by Cisco UCS Manager for better vNIC performance:

- Queue Pairs
- Memory Regions
- Resource Groups

Guidelines and Limitations for SMB Direct with RoCE

- Microsoft SMB Direct with RoCE is supported:
  - On Windows 2012 R2.

- On Windows 2016.

- Cisco UCS C-Series server does not support more than 4 RoCE-enabled vNICs per adapter.
- Cisco UCS C-Series server does not support RoCE with NVGRE, VXLAN, VMQ, or usNIC.
- Maximum number of queue pairs per adapter is 8192.
- Maximum number of memory regions per adapter is 524288.
- RoCE configuration is supported between Cisco adapters. Interoperability between Cisco adapters and third party adapters is not supported.

Important It is required to configure the no-drop QOS policy settings at the switches in the RDMA traffic path.

Viewing vNIC Properties

Procedure

Step 1 In the **Navigation** pane, click the **Networking** menu.

Step 2 In the **Adapter Card** pane, click the **vNICs** tab.

Step 3 In the **vNICs** pane, click **eth0** or **eth1**.

Step 4 In the **Ethernet Interfaces** pane's **vNIC Properties** area, review the information in the following fields:

Name	Description
Name field	The name for the virtual NIC. This name cannot be changed after the vNIC has been created.
CDN field	The Consistent Device Name (CDN) that you can assign to the ethernet vNICs on the VIC cards. Assigning a specific CDN to a device helps in identifying it on the host OS. **Note** This feature works only when the **CDN Support for VIC** token is enabled in the BIOS.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
MAC Address field	The MAC address associated with the vNIC. To let the adapter select an available MAC address from its internal pool, select **Auto**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.

Name	Description
Class of Service drop-down list	The class of service to associate with traffic from this vNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
PCI Order field	The order in which this vNIC will be used. To specify an order, enter an integer within the displayed range.
Default VLAN field	If there is no default VLAN for this vNIC, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field. **Note** This option cannot be used in VNTAG mode.
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	If you want this vNIC to have an unlimited data rate, select OFF. Otherwise, click the second radio button and enter a rate limit in the associated field. Enter an integer between 1 and 10,000 Mbps. For VIC 13xx controllers, you can enter an integer between 1 and 40,000 Mbps. For VIC 1455 and 1457 controllers: • If the adapter is connected to 25 Gbps link on a Switch, then you can enter an integer between 1 to 25,000 Mbps for the **Rate Limit** field. • If the adapter is connected to 10 Gbps link on a Switch, then you can enter an integer between 1 to 10,000 Mbps for the **Rate Limit** field. For VIC 1495 and 1497 controllers: • If the adapter is connected to 40 Gbps link on a switch, then you can enter an integer between 1 to 40,000 Mbps for the **Rate Limit** field. • If the adapter is connected to 100 Gbps link on a switch, then you can enter an integer between 1 to 100,000 Mbps for the **Rate Limit** field. **Note** This option cannot be used in VNTAG mode.

Name	Description
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Channel Number field	Select the channel number that will be assigned to this vNIC. **Note** VNTAG mode is required for this option.
PCI Link field	The link through which vNICs can be connected. These are the following values: • **0** - The first cross-edged link where the vNIC is placed. • **1** - The second cross-edged link where the vNIC is placed. **Note** • This option is available only on some Cisco UCS C-Series servers.
Port Profile drop-down list	Select the port profile that should be associated with the vNIC. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.
Enable Uplink Failover check box	Check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems. **Note** VNTAG mode is required for this option.
Enable VMQ check box	Check this box to enable Virtual Machine Queue (VMQ). **Note** Ensure that VMQ is not enabled when SR-IOV or netflow option is enabled on the adapter. This option is available only on some Cisco UCS C-Series servers.
Enable aRFS check box	Check this box to enable Accelerated Receive Flow steering (aRFS). This option is available only on some Cisco UCS C-Series servers.
Enable NVGRE check box	Check this box to enable Network Virtualization using Generic Routing Encapsulation. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 cards.
Enable VXLAN check box	Check this box to enable Virtual Extensible LAN. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 and VIC 14xx cards.

Name	Description
Advanced Filter check box	Check this box to enable advanced filter options in vNICs.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600. **Note** VNTAG mode is required for this option.

Step 5 In the **Ethernet Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Coalescing Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 6 In the **Ethernet Receive Queue** area, review the information in the following fields:

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.

Step 7 In the **Ethernet Transmit Queue** area, review the information in the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.

Step 8 In the **Completion Queue** area, review the information in the following fields:

Name	Description
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Completion Queue Ring Size field	The number of descriptors in each completion queue. This value cannot be changed.

Step 9 In the **TCP Offload** area, review the information in the following fields:

Name	Description
Enable TCP Segmentation Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Enable TCP Rx Offload Checksum Validation check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.
Enable TCP Tx Offload Checksum Generation check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
Enable Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.

Step 10 In the **Receive Side Scaling** area, review the information in the following fields:

Name	Description
Enable TCP Receive Side Scaling check box	Receive Side Scaling (RSS) distributes network receive processing across multiple CPUs in multiprocessor systems. If checked, network receive processing is shared across processors whenever possible. If cleared, network receive processing is always handled by a single processor even if additional processors are available.
Enable IPv4 RSS check box	If checked, RSS is enabled on IPv4 networks.
Enable TCP-IPv4 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv4 networks.
Enable IPv6 RSS check box	If checked, RSS is enabled on IPv6 networks.
Enable TCP-IPv6 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.
Enable IPv6 Extension RSS check box	If checked, RSS is enabled for IPv6 extensions.
Enable TCP-IPv6 Extension RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.

Modifying vNIC Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Step 7 Click **Properties** to open the **vNIC Properties** dialog box.

Step 8 In the **General** area, update the following fields:

Name	Description
Name field	The name for the virtual NIC. This name cannot be changed after the vNIC has been created.

Name	Description
CDN field	The Consistent Device Name (CDN) that you can assign to the ethernet vNICs on the VIC cards. Assigning a specific CDN to a device helps in identifying it on the host OS. **Note** This feature works only when the **CDN Support for VIC** token is enabled in the BIOS.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
MAC Address field	The MAC address associated with the vNIC. To let the adapter select an available MAC address from its internal pool, select **Auto**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Class of Service drop-down list	The class of service to associate with traffic from this vNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
PCI Link field	The link through which vNICs can be connected. These are the following values: • **0** - The first cross-edged link where the vNIC is placed. • **1** - The second cross-edged link where the vNIC is placed. **Note** • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 cards.
PCI Order field	The order in which this vNIC will be used. To let the system set the order, select **Any**. To specify an order, select the second radio button and enter an integer between 0 and 17.
Default VLAN field	If there is no default VLAN for this vNIC, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field. **Note** This option cannot be used in VNTAG mode.

Name	Description
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**. When the VLAN is set to **ACCESS** mode, any frame received from the specified default VLAN (1-4094) that is received from the switch with a TAG removes that TAG when it is sent to the host OS through the vNIC. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	If you want this vNIC to have an unlimited data rate, select OFF. Otherwise, click the second radio button and enter a rate limit in the associated field. Enter an integer between 1 and 10,000 Mbps or 40,000 Mbps depending on the adapter card you choose. **Note** This option cannot be used in VNTAG mode.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Channel Number field	Select the channel number that will be assigned to this vNIC. **Note** VNTAG mode is required for this option.
Port Profile drop-down list	Select the port profile that should be associated with the vNIC. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.
Enable Uplink Failover check box	Check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems. **Note** VNTAG mode is required for this option.
Enable VMQ check box	Check this box to enable Virtual Machine Queue (VMQ). **Note** Ensure that VMQ is not enabled when SR-IOV or netflow option is enabled on the adapter.
Enable aRFS check box	Check this box to enable Accelerated Receive Flow steering (aRFS). This option is available only on some Cisco UCS C-Series servers.
Enable NVGRE check box	Check this box to enable Network Virtualization using Generic Routing Encapsulation. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 cards.

Name	Description
Enable VXLAN check box	Check this box to enable Virtual Extensible LAN. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 cards.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600. **Note** VNTAG mode is required for this option.

Step 9 In the **Ethernet Interrupt** area, update the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Coalescing Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 10 In the **Ethernet Receive Queue** area, update the following fields:

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.

Name	Description
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.

Step 11 In the **Ethernet Transmit Queue** area, update the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.

Step 12 In the **Completion Queue** area, update the following fields:

Name	Description
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Completion Queue Ring Size field	The number of descriptors in each completion queue. This value cannot be changed.

Step 13 In the **RoCE Properties** area, update the following fields:

Name	Description
RoCE checkbox	Check the check box to change the RoCE Properties.
Queue Pairs (1 - 8192) field	The number of queue pairs per adapter. Enter an integer between 1 and 8192. We recommend that this number be an integer power of 2. The recommended value for queue pairs per vNIC is 2048. This allows four vNICs to be created per adapter. Windows driver reserves two queue pairs for internal use, so a valid range of values would be 4 to 8192 queue pairs per vNIC.
Memory Regions (1 - 524288) field	The number of memory regions per adapter. Enter an integer between 1 and 524288. We recommend that this number be an integer power of 2. The recommended value is 131072. The number of memory regions supported should be enough to meet application requirements as the regions are primarily used to send operation channel semantics.

Name	Description
Resource Groups (1 - 128) field	The number of resource groups per adapter. Enter an integer between 1 and 128. We recommend that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance. Recommended value is 32. The resource group defines the total number of hardware resources such as WQ, RQ, CQ, and interrupts required to support the RDMA functionality, and is based on the total number of processor cores available with the host. The host chooses to dedicate a particular resource group to a core to maximize performance and get a better non-uniform memory access.

Step 14 In the **TCP Offload** area, update the following fields:

Name	Description
Enable TCP Segmentation Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Enable TCP Rx Offload Checksum Validation check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.
Enable TCP Tx Offload Checksum Generation check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
Enable Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.

Step 15 In the **Receive Side Scaling** area, update the following fields:

Name	Description
Enable TCP Receive Side Scaling check box	Receive Side Scaling (RSS) distributes network receive processing across multiple CPUs in multiprocessor systems. If checked, network receive processing is shared across processors whenever possible. If cleared, network receive processing is always handled by a single processor even if additional processors are available.
Enable IPv4 RSS check box	If checked, RSS is enabled on IPv4 networks.

Name	Description
Enable TCP-IPv4 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv4 networks.
Enable IPv6 RSS check box	If checked, RSS is enabled on IPv6 networks.
Enable TCP-IPv6 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.
Enable IPv6 Extension RSS check box	If checked, RSS is enabled for IPv6 extensions.
Enable TCP-IPv6 Extension RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.

Step 16 Click **Save Changes**.

Creating a vNIC

The adapter provides two permanent vNICs. You can create up to 16 additional vNICs.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, choose one of these actions:

- To create a vNIC using default configuration settings, click **Add**.
- To create a vNIC using the same configuration settings as an existing vNIC, select that vNIC and click **Clone**.

The **Add vNIC** dialog box appears.

Step 7 In the **Add vNIC** dialog box, enter a name for the vNIC in the **Name** entry box.

Step 8 (Optional) In the **Add vNIC** dialog box, enter a channel number for the vNIC in the **Channel Number** entry box.

Note If NIV is enabled on the adapter, you must assign a channel number for the vNIC when you create it.

Step 9 Click **Add vNIC**.

What to do next

If configuration changes are required, configure the new vNIC as described in Modifying vNIC Properties, on page 159.

Deleting a vNIC

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Note You cannot delete either of the two default vNICs, **eth0** or **eth1**.

Step 7 Click **Delete** and click **OK** to confirm.

Managing Cisco usNIC

Overview of Cisco usNIC

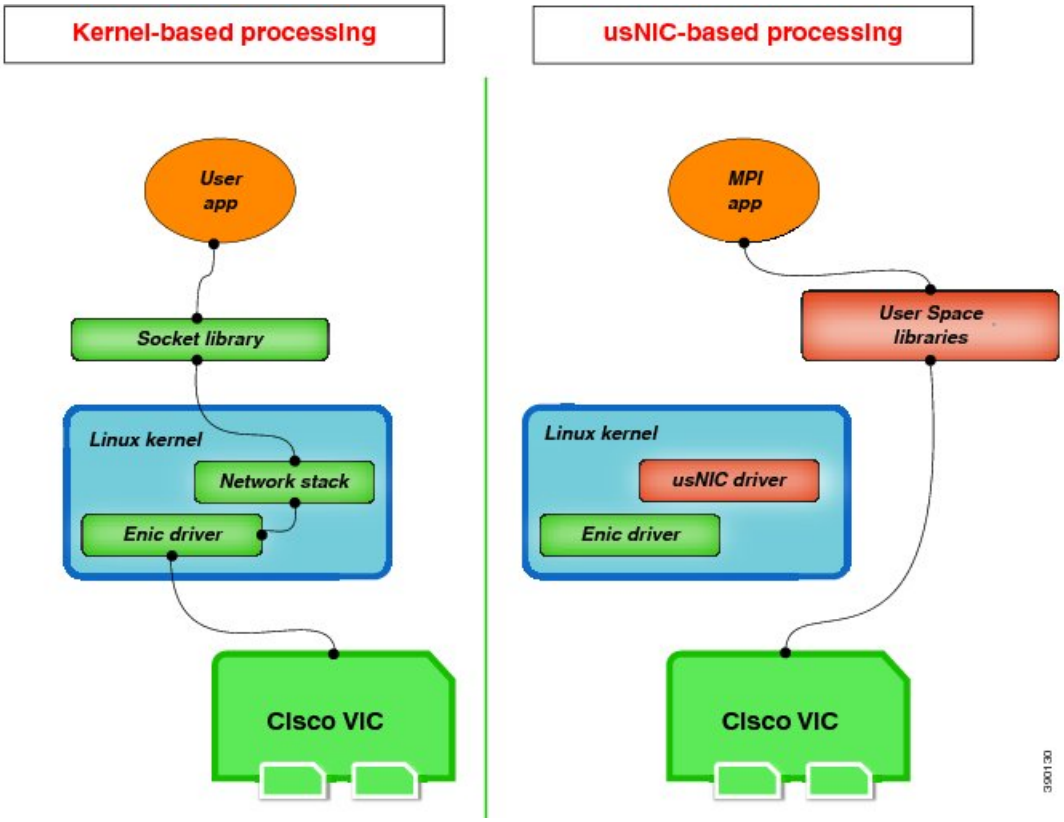
The Cisco user-space NIC (Cisco usNIC) feature improves the performance of software applications that run on the Cisco UCS servers in your data center by bypassing the kernel when sending and receiving networking packets. The applications interact directly with a Cisco UCS VIC second generation or later generation adapter, such as the , which improves the networking performance of your high-performance computing cluster. To benefit from Cisco usNIC, your applications must use the Message Passing Interface (MPI) instead of sockets or other communication APIs.

Cisco usNIC offers the following benefits for your MPI applications:

- Provides a low-latency and high-throughput communication transport.
- Employs the standard and application-independent Ethernet protocol.
- Takes advantage of lowlatency forwarding, Unified Fabric, and integrated management support in the following Cisco data center platforms:
  - Cisco UCS server
  - Cisco UCS VIC second generation or later generation adapter
  - 10 or 40GbE networks

Standard Ethernet applications use user-space socket libraries, which invoke the networking stack in the Linux kernel. The networking stack then uses the Cisco eNIC driver to communicate with the Cisco VIC hardware. The following figure shows the contrast between a regular software application and an MPI application that uses Cisco usNIC.

Figure 1: Kernel-Based Network Communication versus Cisco usNIC-Based Communication



Configuring Cisco usNIC Using the Cisco IMC GUI

Note Even though several properties are listed for Cisco usNIC in the usNIC properties dialog box, you must configure only the following properties because the other properties are not currently being used.

- **cq-count**
- **rq-count**
- **tq-count**
- **usnic-count**

Before you begin

You must log in to the Cisco IMC GUI with administrator privileges to perform this task. Click Play on this video to watch how to configure Cisco usNIC in CIMC.

Procedure

Step 1 Log into the Cisco IMC GUI.

For more information about how to log into Cisco IMC, see Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Step 2 In the **Navigation** pane, click the **Server** tab.

Step 3 On the **Server** tab, click **Inventory**.

Step 4 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 5 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 6 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 7 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Note For each vNIC that you want to configure as a usNIC, select the vNIC entry from the table and specify its properties as explained in steps 9 through step 18.

Step 8 Click **usNIC** to open the **usNIC Properties** dialog box.

Step 9 In the **usNICs** property, specify the number of Cisco usNICs that you want to create.

Each MPI process that is running on the server requires a dedicated usNIC. You might need to create up to 64 usNICs to sustain 64 MPI processes running simultaneously. We recommend that you create at least as many usNICs, per usNIC-enabled vNIC, as the number of physical cores on your server. For example, if you have 8 physical cores on your server, create 8 usNICs.

Step 10 In the **Properties** area, update the following fields:

Field Name	Description
Transmit Queue Count	The number of transmit queue resources to allocate. Cisco recommends setting this value to 6.
Receive Queue Count	The number of receive queue resources to allocate. Cisco recommends setting this value to 6.
Completion Queue Count	The number of completion queue resources to allocate. Cisco recommends setting this value to 6.

Step 11 Click **Apply**.

Step 12 In the **Navigation** pane, click the **Server** tab.

Step 13 On the **Server** tab, click **BIOS**.

Step 14 In the **Actions** area, click **Configure BIOS**.

Step 15 In the **Configure BIOS Parameters** dialog box, click the **Advanced** tab.

Step 16 In the **Processor Configuration** area, set the following properties to `Enabled`:

- **Intel(R) VT-d**

- **Intel(R) VT-d ATS support**
- **Intel(R) VT-d Coherency Support**

Step 17 Click **Save Changes**.

The changes take effect upon the next server reboot.

Viewing usNIC Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interface** area, select the usNIC that is assigned to vNIC, to open the **usNIC properties** dialog box.

Step 7 In the **usNIC** area, review or update the information in the following fields:

Name	Description
Name	The name for the vNIC that is the parent of the usNIC. **Note** This field is read-only.
usNIC field	The number of usNICs assigned to the specific vNIC. Enter an integer between 0 and 225. To assign additional usNICs to a specified vNIC, enter value higher than the existing value. To delete usNICs from a specified vNIC, enter value smaller than the existing value. To delete all the usNICs assigned to a vNIC, enter zero.

Step 8 In the **Properties** area, review or update the information in the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Interrupt Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Coalescing Timer Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Class of Service field	The class of service to associate with traffic from this usNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.

Name	Description
TCP Segment Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.
TCP Tx Checksum check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
TCP Rx Checksum check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.

Name	Description
Apply button	Applies changes to all the usNICs associated with the vNIC device.
Reset values button	Restores the values for the usNIC to the settings that were in effect when this dialog box was first opened.
Cancel button	Closes the dialog box without making any changes.

Configuring iSCSI Boot Capability

Configuring iSCSI Boot Capability for vNICs

When the rack-servers are configured in a standalone mode, and when the VIC adapters are directly attached to the Nexus 5000 family of switches, you can configure these VIC adapters to boot the servers remotely from iSCSI storage targets. You can configure Ethernet vNICs to enable a rack server to load the host OS image from remote iSCSI target devices.

To configure the iSCSI boot capability on a vNIC:

- You must log in with admin privileges to perform this task.

- To configure a vNIC to boot a server remotely from an iSCSI storage target, you must enable the PXE boot option on the vNIC.

Note You can configure a maximum of 2 iSCSI vNICs for each host.

Configuring iSCSI Boot Capability on a vNIC

You can configure a maximum of 2 iSCSI vNICs for each host.

Before you begin

- To configure a vNIC to boot a server remotely from an iSCSI storage target, you must enable the PXE boot option on the vNIC.
- You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the Inventory pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table, and click **iSCSI Boot**.

Step 7 In the **General Area**, update the following fields:

Name	Description
Name field	The name of the vNIC.
DHCP Network check box	Whether DHCP Network is enabled for the vNIC. If enabled, the initiator network configuration is obtained from the DHCP server.
DHCP iSCSI check box	Whether DHCP iSCSI is enabled for the vNIC. If enabled and the DHCP ID is set, the initiator IQN and target information are obtained from the DHCP server. **Note** If DHCP iSCSI is enabled without a DHCP ID, only the target information is obtained.

Name	Description
DHCP ID field	The vendor identifier string used by the adapter to obtain the initiator IQN and target information from the DHCP server. Enter a string up to 64 characters.
DHCP Timeout field	The number of seconds to wait before the initiator assumes that the DHCP server is unavailable. Enter an integer between 60 and 300 (default: 60 seconds)
Link Timeout field	The number of seconds to wait before the initiator assumes that the link is unavailable. Enter an integer between 0 and 255 (default: 15 seconds)
LUN Busy Retry Count field	The number of times to retry the connection in case of a failure during iSCSI LUN discovery. Enter an integer between 0 and 255. The default is 15.
IP Version field	The IP version to use during iSCSI boot.

Step 8 In the **Initiator Area**, update the following fields:

Name	Description
Name field	A regular expression that defines the name of the iSCSI initiator. You can enter any alphanumeric string as well as the following special characters: • . (period) • : (colon) • - (dash) **Note** The name is in the IQN format.
IP Address field	The IP address of the iSCSI initiator.
Subnet Mask field	The subnet mask for the iSCSI initiator.
Gateway field	The default gateway.
Primary DNS field	The primary DNS server address.
Secondary DNS field	The secondary DNS server address.
TCP Timeout field	The number of seconds to wait before the initiator assumes that TCP is unavailable. Enter an integer between 0 and 255 (default: 15 seconds)
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.

Name	Description
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Step 9 In the **Primary Target Area**, update the following fields:

Name	Description
Name field	The name of the primary target in the IQN format.
IP Address field	The IP address of the target.
TCP Port field	The TCP port associated with the target.
Boot LUN field	The Boot LUN associated with the target.
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Step 10 In the **Secondary Target Area**, update the following fields:

Name	Description
Name field	The name of the secondary target in the IQN format.
IP Address field	The IP address of the target.
TCP Port field	The TCP port associated with the target.
Boot LUN field	The Boot LUN associated with the target.
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Name	Description
Configure ISCSI button	Configures iSCSI boot on the selected vNIC.
Unconfigure ISCSI button	Removes the configuration from the selected vNIC.
Reset Values button	Restores the values for the vNIC to the settings that were in effect when this dialog box was first opened.
Cancel button	Closes the dialog box without making any changes.

Step 11 Click **Configure ISCSI**.

Removing iSCSI Boot Configuration from a vNIC

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the Inventory pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table, and click **iSCSI Boot**.

Step 7 In the dialog box that appears, click **Unconfigure ISCSI**.

Configuring Virtual Machine Queues on a vNIC

Before you begin

You must log in to the Cisco IMC GUI with administrator privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Networking** menu.

Step 2 In the **Adapter Card** pane, click the **vNICs** tab.

Step 3 In the **Ethernet Interfaces** pane's **vNIC Properties** area, check the **Enable VMQ** checkbox.

Step 4 In the **Ethernet Transmit Queue** area, enter an integer in the **Transmit Queue Count** field. This number should be greater than 1.

Step 5 In the **Ethernet Receive Queue** area, enter an integer in the **Receive Queue Count** field. This number should be equal to the number of transmit queues.

Step 6 In the **Ethernet Interrupt** area, enter an integer in the **Interrupt Count** field. This should be equal to the number of logical processors, or completion queues.

What to do next

- Reboot the server.
- Create a logical switch on the NIC.

Backing Up and Restoring the Adapter Configuration

Exporting the Adapter Configuration

The adapter configuration can be exported as an XML file to a remote server which can be one of the following:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

Before you begin

Obtain the remote server IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Export Configuration**.

The **Export Adapter Configuration** dialog box opens.

Step 7 In the **Export Adapter Configuration** dialog box, update the following fields:

Name	Description
Export to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server to which the adapter configuration file will be exported. Depending on the setting in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 8 Click **Export Configuration**.

Importing the Adapter Configuration

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Import Configuration**.

The **Import Adapter Configuration** dialog box opens.

Step 7 In the **Import Adapter Configuration** dialog box, update the following fields:

Name	Description
Import from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server on which the adapter configuration file resides. Depending on the setting in the **Import from** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 8 Click **Import Configuration**.

The adapter downloads the configuration file from the specified path on the TFTP server at the specified IP address. The configuration will be installed during the next server reboot.

What to do next

Reboot the server to apply the imported configuration.

Restoring Adapter Defaults

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Reset To Defaults** and click **OK** to confirm.

Managing Adapter Firmware

Adapter Firmware

A Cisco UCS C-Series network adapter contains the following firmware components:

- Adapter firmware —The main operating firmware, consisting of an active and a backup image, can be installed from the Cisco IMC GUI or CLI interface or from the Host Upgrade Utility (HUU). You can upload a firmware image from either a local file system or a TFTP server.
- Bootloader firmware—The bootloader firmware cannot be installed from the Cisco IMC. You can install this firmware using the Host Upgrade Utility.

Installing Adapter Firmware From a Local File

Before you begin

Store the adapter firmware file in the file system of the managing computer.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Install Firmware** to open the **Install Adapter Firmware** dialog box.

Step 7 In the **Install Adapter Firmware** dialog box, select **Install from local file**, then click **Next**.

Step 8 Click **Browse...** and locate the adapter firmware file.

Step 9 Click **Install Firmware**.

What to do next

To activate the new firmware, see *Activating Adapter Firmware*.

Installing Adapter Firmware From a Remote Server

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Install Firmware** to open the **Install Adapter Firmware** dialog box.

Step 7 In the **Install Adapter Firmware** dialog box, select **Install from Remote Server**, then click **Next**.

Step 8 In the **Install Adapter Firmware** dialog box, update the following fields:

Name	Description
Install from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IP address or hostname of the server on which the adapter configuration file resides. Depending on the setting in the **Install from** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Back button	Click this button if you want to specify a local path for the firmware package.
Install Firmware button	Click this button to install the selected firmware package in the adapter's backup memory slot.
Close button	Click this button to close the wizard without making any changes to the firmware versions stored on the server.

Step 9 Click **Install Firmware**.

What to do next

To activate the new firmware, see *Activating Adapter Firmware*.

Activating Adapter Firmware

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Activate Firmware** to open the **Activate Adapter Firmware** dialog box.

Step 7 In the **Activate Adapter Firmware** dialog box, select the image to run the next time the firmware starts up.

Step 8 Click **Activate Adapter Firmware**.

Resetting the Adapter

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Reset** and click **Yes** to confirm.

Note Resetting the adapter also resets the host.

CHAPTER 10

Managing Storage Adapters

This chapter includes the following sections:

Self Encrypting Drives (Full Disk Encryption)

Cisco IMC supports self encrypting drives (SED). A special hardware in the drives encrypts incoming data and decrypts outgoing data in real-time. This feature is also called Full Disk Encryption (FDE).

The data on the drive is encrypted on its way into the drive and decrypted on its way out. However, if you lock the drive, no security key is required to retrieve the data.

When a drive is locked, an encryption key is created and stored internally. All data stored on this drive is encrypted using that key, and stored in encrypted form. Once you store the data in this manner, a security key is required in order to un-encrypt and fetch the data from the drive. Unlocking a drive deletes that encryption key and renders the stored data unusable. This is called a Secure Erase. The FDE comprises a key ID and a security key.

The FDE feature supports the following operations:

- Enable and disable security on a controller
- Create a secure virtual drive
- Secure a non-secure drive group
- Unlock foreign configuration drives
- Enable security on a physical drive (JBOD)
- Clear secure SED drives
- Clear secure foreign configuration

Scenarios to consider While Configuring Controller Security in a Dual or Multiple Controllers Environment

Note Dual or Multiple controllers connectivity is available only on some servers.

Controller security can be enabled, disabled, or modified independently. However, local and remote key management applies to all the controllers on the server. Therefore security action involving switching the key management modes must be performed with caution. In a scenario where both controllers are secure, and you decide to move one of the controllers to a different mode, you need to perform the same operation on the other controller as well.

Consider the following two scenarios:

- Scenario 1—Key management is set to remote; both controllers are secure and use remote key management. If you now wish to switch to local key management, switch the key management for each controller and disable remote key management.

- Scenario 2—Key management is set to local; both controllers are secure and use local key management. If you now wish to switch to remote key management, enable remote key management and switch the key management for each controller.

If you do not modify the controller security method on any one of the controllers, it renders the secure key management in an unsupported configuration state.

Create Virtual Drive from Unused Physical Drives

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Actions** area, click **Create Virtual Drive from Unused Physical Drives**.

The **Create Virtual Drive from Unused Physical Drives** dialog box displays.

Step 5 In the **Create Virtual Drive from Unused Physical Drives** dialog box, select the RAID level for the new virtual drives:

This can be one of the following:

- **Raid 0**—Simple striping.
- **Raid 1**—Simple mirroring.
- **Raid 5**—Striping with parity.
- **Raid 6**—Striping with two parity drives.
- **Raid 10**—Spanned mirroring.
- **Raid 50**—Spanned striping with parity.
- **Raid 60**—Spanned striping with two parity drives.

Note You must have multiple drive groups available to create virtual drives for certain RAID levels. While creating drives for these RAID levels, the create drive option is available only if the required number of drives are selected.

Step 6 Optionally, select the **Enable Full Disk Encryption** checkbox.

This enables disk encryption on the drive group and allows you to secure it.

Step 7 In the **Create Drive Groups** area, choose one or more physical drives to include in the group.

Use the >> button to add the drives to the **Drive Groups** table. Use the << button to remove physical drives from the drive group.

Note The size of the smallest physical drive in the drive group defines the maximum size used for all the physical drives. To ensure maximum use of space for all physical drives, it is recommended that the size of all the drives in the drive group are similar.

Step 8 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 9 Click **Create Virtual Drive**.

Create Virtual Drive from an Existing Drive Group

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Create Virtual Drive from an Existing Virtual Drive Group**.

The **Create Virtual Drive from an Existing Virtual Drive Group** dialog box displays.

Step 5 In the **Create Virtual Drive from an Existing Virtual Drive Group** dialog box, select the virtual drive whose drive group you want to use to create a new virtual drive.

Step 6 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.

Name	Description
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 7 Click **Create Virtual Drive**.

Setting a Virtual Drive to Transport Ready State

You can move a virtual drive from one MegaRAID controller to another using the **Set Transport Ready** feature. This allows all the pending IOs of the virtual drive to complete their activities, hide the virtual drive from the operating system, flush cache, pause all the background operations, and save the current progress in disk data format, allowing you to move the drive. When you move a virtual drive, all other drives belonging to the same drive group inherit the same change as the moved drive.

When the last configured physical drive on the group is removed from the current controller, the drive group becomes foreign and all foreign configuration rules apply to the group. However, the Transport Ready feature does not change any foreign configuration behavior.

You can also clear a virtual drive from the Transport Ready state. This makes the virtual drive available to the operating systems.

Following restrictions apply to a transport ready virtual drive:

- Only a maximum of 16 transport ready drive groups are currently supported.
- This feature is not supported on high availability.
- A virtual drive cannot be set as transport ready under these conditions:
  - When a virtual drive of a drive group is being reconstructed
  - When a virtual drive of a drive group contains a pinned cache

- When a virtual drive of a drive group is marked as cacheable or associated with a cachecade virtual drive
- If a virtual drive is a cachecade virtual drive
- If a virtual drive is offline
- If a virtual drive is a bootable virtual drive

Setting a Virtual Drive as Transport Ready

Before you begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be in optimal state to enable transport ready.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA Controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want set as transport ready.

Step 5 In the **Actions** area, click **Set Transport Ready**.

The **Set Transport Ready** dialog box displays.

Step 6 Update the following properties in the dialog box:

Name	Description
Initialize Type drop-down list	Allows you to select the initialization type using which you can set the selected virtual drive as transport ready. This can be one of the following: • **Exlude All**— Excludes all the dedicated hot spare drives. • **Include All**— Includes any exclusively available or shared dedicated hot spare drives. • **Include Dedicated Hot Spare Drive**— Includes exclusive dedicated hot spare drives.
Set Transport Ready button	Sets the selected virtual drive as transport ready.
Cancel button	Cancels the action.

Note When you set a virtual drive to transport ready all the physical drives associated with it are displayed as **Ready to Remove**.

Clearing a Virtual Drive from Transport Ready State

Before you begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be transport ready.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive to set as transport ready.

Step 5 In the **Actions** area, click **Clear Transport Ready**.

This reverts the selected transport ready virtual drive to its original optimal state.

Importing Foreign Configuration

When a set of physical drives hosting a secured drive group are inserted into a different server or controller (or the same controller but whose security-key has been changed while they were not present), they become foreign configurations. Since they are secured, these foreign configurations must be unlocked by verifying their security key information before they can be imported.

Complete the following steps to verify the security key for a foreign configuration and import the configuration:

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Import Foreign Config**.

This action opens the **Secure Key Verification** dialog box. Review the following information before proceeding:

Table 1: Secure Key Verification Area

Name	Description
Security Key field	Unique key ID assigned to a controller.
Verify button	Verifies if the key you entered matches the stored key information. If the secure key is verified to be correct, the requested action is completed.
Cancel button	Cancels the action.

Step 5 Click **OK** to confirm.

Clearing Foreign Configuration

Important This task clears all foreign configuration on the controller. Also, all configuration information from all physical drives hosting foreign configuration is deleted. This action cannot be reverted.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Clear Foreign Config**.

Step 5 Click **OK** to confirm.

Clearing a Boot Drive

Important This task clears the boot drive configuration on the controller. This action cannot be reverted.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Controller Info** tab.
Step 4 In the **Actions** area, click **Clear Boot Drive**.
Step 5 Click **OK** to confirm.

Enabling a JBOD

Note You can enable Just a Bunch Of Disks (JBOD) only on some UCS C-Series servers.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage Adapters** pane, click the appropriate **MegaRAID** controller.
Step 3 On the **Work** pane, click **Controller Info** tab.
Step 4 In the **Actions** area, click **Enable JBOD**.
Step 5 Click **Ok** to confirm.

Disabling a JBOD

Note This option is available only on some UCS C-Series servers.

Before you begin

JBOD option must be enabled for the selected controller.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage Adapters** pane, click the appropriate **MegaRAID** controller.
Step 3 On the **Work** pane, click **Controller Info** tab.

Step 4 In the **Actions** area, click **Disable JBOD**.

Step 5 Click **Ok** to confirm.

Preparing a Drive for Removal

Note You can perform this task only on physical drives that display the **Unconfigured Good** status.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the drive you want to remove.

Step 5 In the **Actions** area, click **Prepare for Removal**.

Step 6 Click **OK** to confirm.

Retrieving TTY Logs for a Controller

This task retrieves the TTY logs for the controller and places it in the `/var/log` location. This ensures that this log data is available when Technical Support Data is requested.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Get TTY Log**.

Step 5 Click **OK** to confirm.

Important Retrieving TTY logs for a controller could take up to 2-4 minutes. Until this process is complete, do not initiate exporting technical support data.

Modifying Controller Security

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Modify Drive Security**.

The **Modify Drive Security** dialog box appears.

Step 5 In the **Modify Drive Security** dialog box, review the following information:

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **Enabled**— Controller security is enabled. • **Disabled**— Controller security is disabled.
Security Key Identifier field	The current key ID.
Security Key field	Security key used to enable controller security. If you wish to change the current security key, enter the new key here. **Note** Once you change the security key, a **Secure Key Verification** pop-up window appears where you need to enter the current security key to verify it.
Confirm Security Key field	Re-enter the security key.
Modify Security Key check box	**Note** This option appears only for remote key management. If you select this option the security key on the KMIP server is modified.
Suggest button	Suggests the security key or key ID that can be assigned.
Save button	Saves the data.

Name	Description
Cancel button	Cancels the action.

Disabling Controller Security

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Disable Drive Security**.

Click **Yes** or **No** at the prompt.

Enabling Controller Security

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Enable Drive Security**.

The **Enable Drive Security** dialog box appears.

Step 5 In the **Enable Drive Security** dialog box, review the following information:

Table 2: Secure Key Configuration Area

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **True**— Controller security is enabled. • **False**— Controller security is disabled.
Security Key Identifier field	The current key ID.
Security Key field	Security key used to enable controller security. If you wish to change the current security key, enter the new key here. **Note** Once you change the security key, a **Secure Key Verification** pop-up window appears where you need to enter the current security key to verify it.
Confirm Security Key field	Re-enter the security key.
Suggest button	Suggests the security key or key ID that can be used.
Save button	Saves the data.
Cancel button	Cancels the action.

What to do next

Undo Preparing a Drive for Removal

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.

Step 3 On the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select a drive with a status of **Ready to Remove**.

Step 5 In the **Actions** area, click **Undo Prepare for Removal**.

Step 6 Click **OK** to confirm.

Making a Dedicated Hot Spare

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the physical drive you want to make a dedicated hot spare.

Step 5 In the **Actions** area, click **Make Dedicated Hot Spare**.

The **Make Dedicated Hot Spare** dialog box displays.

Step 6 In the **Virtual Drive Details** area, update the following properties:

Name	Description
Virtual Drive Number drop-down list	Select the virtual drive to which you want to dedicate the physical drive as hot spare.
Virtual Drive Name field	The name of the selected virtual drive.
Physical Drive Number field	The number of the physical drive.

Step 7 Click **Make Dedicated Hot Spare** to confirm.

Making a Global Hot Spare

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the physical drive you want to make a global hot spare.

Step 5 In the **Actions** area, click **Make Global Hot Spare**.

Removing a Drive from Hot Spare Pools

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the global or dedicated hot spare you want to remove from the hot spare pools.

Step 5 In the **Actions** area, click **Remove From Hot Spare Pools**.

Toggling Physical Drive Status

Before you begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the drive you want to set as unconfigured good.

Step 5 In the **Actions** area, click **Set State as Unconfigured Good**.

Step 6 Click **OK** to confirm that the JBOD mode be disabled.

The **Set State as JBOD** option is enabled.

Step 7 To enable the JBOD mode for the physical drive, click **Set State as JBOD**.

Step 8 Click **OK** to confirm.

The **Set State as Unconfigured Good** option is enabled.

Setting a Physical Drive as a Controller Boot Drive

Before you begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to set as boot drive for the controller.
Step 5 In the **Actions** area, click **Set as Boot Drive**.
Step 6 Click **OK** to confirm.

Enabling Full Disk Encryption on a Physical Drive

Before you begin

- You must log in with admin privileges to perform this task.
- The physical drive must be a JBOD.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Enable Full Disk Encryption**.

Clearing a Secure Physical Drive

Before you begin

- You must log in with admin privileges to perform this task.

- You must enable full disk encryption on a physical drive.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Clear Secure Drive**.

Clearing Secure Foreign Configuration Drive

If the security key used to lock a foreign configuration is lost, the data cannot be retrieved. You then have the option of either discarding the HDD or clearing the foreign configuration.

Note Clearing a foreign configuration erases all data from the drive.

Before you begin

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Clear Secure Foreign Config Drive**.

Initializing a Virtual Drive

All data on a virtual drive is lost when you initialize the drive. Before you run an initialization, back up any data on the virtual drive that you want to save.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want to initialize.

Step 5 In the **Actions** area, click **Initialize**.

The **Initialize Virtual Drive** dialog box displays.

Step 6 Choose the type of initialization you want to use for the virtual drive.

This can be one of the following:

- **Fast Initialize**—This option allows you to start writing data to the virtual drive immediately.
- **Full Initialize**—A complete initialization is done on the new configuration. You cannot write data to the new virtual drive until the initialization is complete.

Step 7 Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.

Step 8 To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.

The following details are displayed:

Name	Description
Operation	Name of the operation that is in progress on the drive.
Progress in %	Progress of the operation, in percentage complete.
Elapsed Time in secs	The number of seconds that have elapsed since the operation began.

Set as Boot Drive

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive from which the controller must boot.

Step 5 In the **Actions** area, click **Set as Boot Drive**.

Step 6 Click **OK** to confirm.

Editing a Virtual Drive

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage Adapters pane**, click **LSI MegaRAID SAS 9266-8i**.

Step 3 On the **Work** pane, click **Virtual Drive Info** tab.

Step 4 In the **Actions** area, click **Edit Virtual Drive**.

Step 5 Review the instructions, and then click **OK**.
The Edit Virtual Drive dialog box displays.

Step 6 From the **Select RAID Level to migrate** drop-down list, choose a RAID level.

See the following table for RAID migration criteria:

Name	Description
Select RAID Level to migrate drop-down list	Select the RAID level to which you want to migrate. Migrations are allowed for the following RAID levels: • **RAID 0** to **RAID 1** • **RAID 0** to **RAID 5** • **RAID 0** to **RAID 6** • **RAID 1** to **RAID 0** • **RAID 1** to **RAID 5** • **RAID 1** to **RAID 6** • **RAID 5** to **RAID 0** • **RAID 6** to **RAID 0** • **RAID 6** to **RAID 5** When you are migrating from one raid level to another, the data arms of the new RAID level should be equal to or greater than the existing one. In case of RAID 6, the data arms will be number of drives minus two, as RAID 6 has double distributed parity. For example, when you create RAID 6 with eight drives, the number of data arms will be 8 – 2 = 6. In this case, if you are migrating from RAID 6 to RAID 0, RAID 0 must have a minimum of six drives. If you select lesser number of drives then **Edit** or **Save** button will be disabled. If you are adding, you can migrate to RAID 0 as you will not be deleting any drives. **Note** RAID level migration is not supported in the following cases: • When there are multiple virtual drives in a RAID group. • With a combination of SSD/HDD RAID groups.

Step 7 From the **Write Policy** drop-down list in the **Virtual Drive Properties** area, choose one of the following:

- **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache.
- **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure.
- **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.

Step 8 Click **Save Changes**.

Securing a Virtual Drive

You can secure a virtual drive only after enabling full disk encryption on that drive. You can complete this action while creating a virtual drive from an unused physical drive. Since it is a physical drive that performs encryption, when a virtual drive in the drive group is secured, all the virtual drives in the drive group are secured. Virtual drives inherit the security setting of the drive group.

Before you begin

- You must log in with admin privileges to perform this task.
- You must enable full disk encryption on a virtual drive.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, select the drive you want to secure.

Step 5 In the **Actions** area, click **Secure Virtual Drive**.

Deleting a Virtual Drive

Important This task deletes a virtual drive, including the drives that run the booted operating system. So back up any data that you want to retain before you delete a virtual drive.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, select the virtual drive you want to delete.

Step 5 In the **Actions** area, click **Delete Virtual Drive**.

Step 6 Click **OK** to confirm.

Enabling Auto Learn Cycle for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.

Step 4 From the **Actions** pane, click **Enable Auto Learn Mode**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Disabling Auto Learn Cycle for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.

Step 4 From the **Actions** pane, click **Disable Auto Learn Mode**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Starting Learn Cycles for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.

Step 4 From the **Actions** pane, click **Start Learn Cycle**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Toggling Locator LED for a Physical Drive

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 From the **Status** area, select **Turn On** or **Turn Off** radio button for the **Locator LED** field.

Viewing Storage Controller Logs

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click **Storage Log** tab and review the following information:

Name	Description
Time column	The date and time the event occurred.

Name	Description
Severity column	The event severity. This can be one of the following: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Description column	A description of the event.

Viewing SSD Smart Information for MegaRAID Controllers

You can view smart information for a solid state drive. Complete these steps:

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Smart Information** area, review the following information:

Name	Description
Power Cycle Count field	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours field	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left field	The number of write cycles remaining in a solid state drive (SSD). For instance, if an SSD is capable of 100 write cycles during its life time, and it has completed 15 writes, then the percentage of life left in the drive is 85%.

Name	Description
Wear Status in Days field	The number of days an SSD has gone through with the write cycles. SSD vendors provide a finite number of writes per day on the SSD, based on which, you can calculate the total number of years the SSD would continue to work.
Operating Temperature field	The current temperature of the drive at which the selected SSD operates at the time of selection.

CHAPTER 11

Configuring Communication Services

This chapter includes the following sections:

Configuring HTTP

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **HTTP Properties** area, update the following properties:

Name	Description
HTTP/S Enabled check box	Whether HTTP and HTTPS are enabled on the Cisco IMC.
Redirect HTTP to HTTPS Enabled check box	If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. We strongly recommend that you enable this option if you enable HTTP.
HTTP Port field	The port to use for HTTP communication. The default is 80.
HTTPS Port field	The port to use for HTTPS communication. The default is 443

Name	Description
Session Timeout field	The number of seconds to wait between HTTP requests before the Cisco IMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the Cisco IMC.

Step 5 Click **Save Changes**.

Configuring SSH

Before you begin

You must log in as a user with admin privileges to configure SSH.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **SSH Properties** area, update the following properties:

Name	Description
SSH Enabled check box	Whether SSH is enabled on the Cisco IMC.
SSH Port field	The port to use for secure shell access. The default is 22.
SSH Timeout field	The number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent SSH sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of SSH sessions currently running on the Cisco IMC.

Step 5 Click **Save Changes**.

Configuring XML API

XML API for Cisco IMC

The Cisco Cisco IMC XML application programming interface (API) is a programmatic interface to Cisco IMC for a C-Series Rack-Mount Server. The API accepts XML documents through HTTP or HTTPS.

For detailed information about the XML API, see *Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer's Guide*.

Enabling the XML API

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **XML API Properties** area, update the following properties:

Name	Description
XML API Enabled check box	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the Cisco IMC.

Step 5 Click **Save Changes**.

Configuring IPMI

IPMI Over LAN

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the Cisco IMC with IPMI messages.

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **IPMI over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.

Name	Description
Privilege Level Limit drop-down list	The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following: • **read-only**—IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges. • **user**—IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server. • **admin**—IPMI users can perform all available actions. If you select this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.
Encryption Key field	The IPMI encryption key to use for IPMI communications.
Randomize button	Enables you to change the IPMI encryption key to a random value.

Step 5 Click **Save Changes**.

Configuring SNMP

SNMP

The Cisco UCS C-Series Rack-Mount Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps. For information on Management Information Base (MIB) files supported by Cisco IMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html.

Configuring SNMP Properties

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **SNMP Properties** area, update the following properties:

Name	Description
SNMP Enabled check box	Whether this server sends SNMP traps to the designated host. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
SNMP Port field	The port on which Cisco IMC SNMP agent runs. Enter an SNMP port number within the range 1 to 65535. The default port number is 161. **Note** The port numbers that are reserved for system calls, such as 22,23,80,123,443,623,389,636,3268,3269 and 2068, cannot be used as an SNMP port.
Access Community String field	The default SNMP v1 or v2c community name Cisco IMC includes on any SNMP get operations. Enter a string up to 18 characters.
SNMP Community Access drop-down list	This can be one of the following: • **Disabled** — This option blocks access to the information in the inventory tables. • **Limited** — This option provides partial access to read the information in the inventory tables. • **Full** — This option provides full access to read the information in the inventory tables. **Note** SNMP Community Access is applicable only for SNMP v1 and v2c users.
Trap Community String field	The name of the SNMP community group used for sending SNMP trap to other devices. Enter a string up to 18 characters. **Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 users need to use SNMP v3 credentials.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 64 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter a string up to 64 characters.
SNMP Input Engine ID field	User-defined unique identification of the static engine.

Name	Description
SNMP Engine ID field	Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the BMC serial number.

Step 5 Click **Save Changes**.

What to do next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings, on page 215.

Configuring SNMP Trap Settings

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 Click on **Trap Destinations** tab.

Step 5 In the **Trap Destinations** area, you can perform one of the following:

- Select an existing user from the table and click **Modify**.
- Click **Add** to create a new user.

Note If the fields are not highlighted, select **Enabled**.

Step 6 In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID field	The trap destination ID. This value cannot be modified.
Enabled check box	If checked, then this trap is active on the server.
Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V2** • **V3**

Name	Description
Trap Type radio button	The type of trap to send. This can be one of the following: • **Trap**: If this option is chosen, the trap will be sent to the destination but you do not receive any notifications. • **Inform**: You can choose this option only for V2 users. If chosen, you will receive a notification when a trap is received at the destination.
User drop-down list	The drop-down list displays all available users, select a user from the list.
Trap Destination Address field	Address to which the SNMP trap information is sent. You can set an IPv4 or IPv6 address or a domain name as the trap destination.
Port	The port the server uses to communicate with the trap destination. Enter a trap destination port number within the range 1 to 65535.

Step 7 Click **Save Changes**.

Step 8 If you want to delete a trap destination, select the row and click **Delete**.

Click **OK** in the delete confirmation prompt.

Sending a Test SNMP Trap Message

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 Click the **SNMP** tab, and then click on the **Trap Destinations** tab.

Step 4 In the **Trap Destinations** area, select the row of the desired SNMP trap destination.

Step 5 Click **Send SNMP Test Trap**.

An SNMP test trap message is sent to the trap destination.

Note The trap must be configured and enabled in order to send a test message.

Managing SNMPv3 Users

Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **SNMPV3 Users** area, update the following properties:

Name	Description
Add button	Click an available row in the table then click this button to add a new SNMP user.
Modify button	Select the user you want to change in the table then click this button to modify the selected SNMP user.
Delete button	Select the user you want to delete in the table then click this button to delete the selected SNMP user.
ID column	The system-assigned identifier for the SNMP user.
Name column	The SNMP user name.
Auth Type column	The user authentication type.
Privacy Type column	The user privacy type.

Step 5 Click **Save Changes**.

Configuring SNMPv3 Users

Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **Users** area, perform one of the following actions:

- Select an existing user from the table and click **Modify**.
- Select a row in the **Users** area and click **Add** to create a new user.

Step 5 In the **SNMP User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user. This field cannot be changed.
Name field	The SNMP username. Enter between 1 and 31 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **MD5** • **SHA**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type drop-down	The privacy type. This can be one of the following: • **DES** • **AES**
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.

Name	Description
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Step 6 Click **Save Changes**.

Step 7 If you want to delete a user, select the user and click **Delete**.

Click **OK** in the delete confirmation prompt.

CHAPTER 12

Managing Certificates and Server Security

This chapter includes the following sections:

Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the Cisco IMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority. The generated certificate key length is 2048 bits.

Note Before performing any of the following tasks in this chapter, ensure that the Cisco IMC time is set to the current time.

Procedure

Step 1 Generate the CSR from the Cisco IMC.

Step 2 Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.

Step 3 Upload the new certificate to the Cisco IMC.

Note The uploaded certificate must be created from a CSR generated by the Cisco IMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

Note Do not use special characters (For example ampersand (**&**)) in the **Common Name** or **Organization Unit** field.

Before you begin

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click the **Generate New Certificate Signing Request** link.

The **Generate New Certificate Signing Request** dialog box appears.

Step 4 In the **Generate New Certificate Signing Request** dialog box, update the following properties:

Name	Description
Common Name field	The fully qualified name of the Cisco IMC. By default the CN of the servers appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server. When you upgrade to latest version, CN is retained as is.
Subject Alternate Name (SAN)	You can now provide additional input parameter for Subject Alternate Name. This allows various values to be associated using the subject field of the certificate. The various options of SAN includes: • Email • DNS name • IP address • Uniform Resource Identifier (URI) **Note** This field is optional. You can configure any number of SAN instances of each type, but all together the instances count must not exceed 10.
Organization Name field	The organization requesting the certificate.

Name	Description
Organization Unit field	The organizational unit.
Locality field	The city or town in which the company requesting the certificate is headquartered.
State Name field	The state or province in which the company requesting the certificate is headquartered.
Country Code drop-down list	The country in which the company resides.
Email field	The email contact at the company.
Signature Algorithm	Allows you to select the signature algorithm for generating certificate signing request. This can be one of the following: • SHA384 • SHA1 • SHA256 • SHA512 The default signature algorithm selected for generating certificate signing request is SHA384.
Self Signed Certificate check box	Generates a Self Signed Certificate. **Warning** After successful certificate generation, the Cisco IMC Web GUI restarts. Communication with the management controller may be lost momentarily and you will need to re-login. **Note** If enabled, CSR is generated, signed and uploaded automatically.

Note If Self-signed certificate is enabled, ignore steps 5 and 6.

Step 5 Click **Generate CSR**.

The **Opening csr.txt** dialog box appears.

Step 6 Perform any one of the following steps to manage the CSR file, csr.txt:

a) Click **Open With** to view csr.txt.
b) Click **Save File** and then click **OK** to save csr.txt to your local machine.

What to do next

- Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.
- Ensure that the certificate is of type **Server**.

Creating an Untrusted CA-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see http://www.openssl.org.

Note These commands are to be entered on a Linux server with the OpenSSL package, not in the Cisco IMC.

Before you begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out ca.key 2048`	This command generates an RSA private key that will be used by the CA. **Note** To allow the CA to access the key without user input, do not use the -des3 option for this command. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* **Example:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	**echo "nsCertType = server" > openssl.conf** **Example:** `# echo "nsCertType = server" > openssl.conf`	This command adds a line to the OpenSSL configuration file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server".
Step 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial**	This command directs the CA to use your CSR file to generate a server certificate.

	Command or Action	Purpose
	04 -CAkey *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** **Example:** `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	Your server certificate is contained in the output file.
Step 5	**openssl x509 -noout -text -purpose -in <cert file>** **Example:** `openssl x509 -noout -text -purpose -in <cert file>`	Verifies if the generated certificate is of type **Server**. **Note** If the values of the fields **Server SSL** and **Netscape SSL** server are not yes, ensure that openssl.conf is configured to generate certificates of type server.
Step 6	(Optional) If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5.	Certificate with the correct validity dates is created.

Example

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
# /usr/bin/openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01
-CAkey ca.key -out server.crt -extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
```

```
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

What to do next

Upload the new certificate to the Cisco IMC.

Creating a Self-Signed Certificate Using Windows

Before you begin

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

Step 1 Open **IIS Manager** and navigate to the level you want to manage.

Step 2 In the **Features** area, double-click **Server Certificate**.

Step 3 In the **Action** pane, click **Create Self-Signed Certificate**.

Step 4 On the **Create Self-Signed Certificate** window, enter name for the certificate in the **Specify a friendly name for the certificate** field.

Step 5 Click **Ok**.

Step 6 (Optional) If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5.
Certificate with the correct validity dates is created.

Uploading a Server Certificate

Before you begin

- You must log in as a user with admin privileges to upload a certificate.
- The certificate file to be uploaded must reside on a locally accessible file system.
- Ensure that the generated certificate is of type server.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Note You must first generate a CSR using the Cisco IMC Certificate Management menu, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Upload Server Certificate**.

The **Upload Certificate** dialog box appears.

Step 4 In the **Upload Certificate** dialog box, update the following properties:

Name	Description
File field	The certificate file you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate certificate file.
Upload Certificate button	Allows you to upload the certificate.

Step 5 Click **Upload Certificate**.

Pasting Server Certificate Content

As an alternative to uploading the server certificate from a local file system, you can also upload a new server certificate by pasting the content of the certificate in a text field.

Before you begin

- You must log in as a user with admin privileges to upload a certificate.
- The certificate file to be uploaded must reside on a locally accessible file system.
- Ensure that the generated certificate is of type server.
- Ensure that the certificate you upload is signed.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Paste Server Certificate**.

The **Paste Server Certificate** dialog box appears.

Step 4 In the **Paste Server Certificate** dialog box, paste the server certificate content in the **Certificate** text field and click **Save**.

This uploads the certificate to the server.

Troubleshooting a New Certificate

Occasionally, a new certificate might not be displayed in the system. In this scenario, you need to complete the following troubleshooting steps and reboot Cisco IMC.

Before you begin

- You must log in as a user with admin privileges to upload a certificate.
- You must have uploaded a new certificate.

Procedure

Step 1 Start a new secure shell session on the Cisco IMC server.

Step 2 Run the commands **scope certificate** and **show detail** respectively to verify that the certificate displayed is the one you uploaded.

Step 3 Exit the secure shell command line interface.

Step 4 Log on to Cisco IMC web interface.

Step 5 In the **Navigation** pane, click the **Admin** tab.

Step 6 On the **Admin** tab, click **Utilities**.

Step 7 In the **Actions** area of the **Utilities** pane, click **Reboot Cisco IMC**.

Step 8 Click **OK**.

Step 9 Clear your web browser's history.

Step 10 Log out of Cisco IMC and log on again to verify that the new certificate is in use.

CHAPTER 13

Configuring Platform Event Filters

This chapter includes the following sections:

Platform Event Filters

A platform event filter (PEF) can trigger an action. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs.

Configuring Platform Event Filters

Before you begin

You must log in as a user with admin privileges to configure platform event filters.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Event Management**.

Step 3 In the **Platform Event Filters** area, complete the following fields for each event:

Name	Description
ID column	The unique filter ID.
Event column	The name of the event filter.

Name	Description
Action column	For each filter, select the desired action from the scrolling list box. This can be one of the following: • **None**—No action is taken. • **Reboot**—The server is rebooted. • **Power Cycle**—The server is power cycled. • **Power Off**—The server is powered off.

Step 4 Click **Save Changes**.

Resetting Platform Event Filters

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Event Management**.

Step 3 In the **Platform Event Filters** area, click **Reset Event Filters**.
Resets the event filters and displays the latest event filters.

CHAPTER 14

Cisco IMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use Cisco-certified firmware that is specific to the C-Series server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.

Caution When you install the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, Cisco IMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

If you want to update the firmware manually, you must update the Cisco IMC firmware first. The Cisco IMC firmware update process is divided into the following stages to minimize the amount of time that the server is offline:

- Installation—During this stage, Cisco IMC installs the selected Cisco IMC firmware in the nonactive, or backup, slot on the server.
- Activation—During this stage, Cisco IMC sets the nonactive firmware version as active, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the Cisco IMC firmware, you can update the BIOS firmware. You must power off server during the entire BIOS update process, so the process is not divided into stages. Instead, you only need to enter one command and Cisco IMC installs and updates the BIOS firmware as quickly as possible. After the Cisco IMC finishes rebooting, the server can be powered on and returned to service.

Note

- You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.
- This procedure only applies to the Cisco UCS C-Series server running on Stand-Alone mode. Contact Cisco Technical Assistance Center to upgrade firmware for UCS C-Series running on Cisco UCS Manager integrated mode.

Cisco IMC in a secure mode ensures that all the firmware images prior to loading and execution are digitally signed and are verified for authenticity and integrity to protect the device from running tampered software.

Obtaining Firmware from Cisco

Procedure

Step 1 Navigate to http://www.cisco.com.

Step 2 If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.

Step 3 In the menu bar at the top, click **Support**.

Step 4 Click **All Downloads** in the roll down menu.

Step 5 If your server model is listed in the **Recently Used Products** list, click the server name. Otherwise, do the following:

a) In the left-hand box, click **Products**.
b) In the center box, click **Unified Computing and Servers**.
c) In the right-hand box, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.
d) In the right-hand box, click the server model whose software you want to download.

Step 6 Click the **Unified Computing System (UCS) Server Firmware** link.

Step 7 (Optional) Select a prior release from the menu bar on the left-hand side of the page.

Step 8 Click the **Download** button associated with the Cisco Host Upgrade Utility ISO for the selected release.

Step 9 Click **Accept License Agreement**.

Step 10 Save the ISO file to a local drive.

We recommend you upgrade the Cisco IMC and BIOS firmware on your server using this ISO file, which contains the Cisco Host Upgrade Utility. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Step 11 (Optional) If you plan to upgrade the Cisco IMC and BIOS firmware manually, do the following:

Beginning with Release 3.0, the BIOS and Cisco IMC firmware files are no longer embedded inside the HUU as a standalone .zip file. BIOS and Cisco IMC firmware must now be extracted using the **getfw** utility, which is available in the GETFW folder of the HUU. Perform the following steps to extract the BIOS or Cisco IMC firmware files:

Note To perform this:

- Openssl must be installed in the target system.
- Squashfs kernel module must be loaded in the target system.

Viewing the GETFW help menu:

```
[root@RHEL65-***** tmp]# cd GETFW/
[root@RHEL65-***** GETFW]# ./getfw -h
Help:
  Usage: getfw {-b -c -C -H -S -V -h} [-s SRC] [-d DEST]
    -b      : Get BIOS Firmware
    -c      : Get CIMC Firmware
    -C      : Get CMC Firmware
    -H      : Get HDD Firmware
    -S      : Get SAS Firmware
    -V      : Get VIC Firmware
    -h      : Display Help
    -s SRC  : Source of HUU ISO image
    -d DEST : Destination to keep Firmware/s
  Note : Default BIOS & CIMC get extracted
```

Extracting the BIOS firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d /tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd bios/
[root@RHEL65-***** bios]# ls
bios.cap
[root@RHEL65-***** bios]#
```

Extracting the CIMC firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d /tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd cimc/
[root@RHEL65-***** cimc]# ls
```

```
cimc.cap
[root@RHEL65-***** cimc]#
```

Step 12 (Optional) If you plan to install the firmware from a remote server, copy the BIOS installation CAP file and the Cisco IMC installation BIN file to the remote server you want to use.

The remote server can be one of the following:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

The server must have read permission for the destination folder on the remote server.

Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.

If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.

The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

What to do next

Use the Cisco Host Upgrade Utility to upgrade all firmware on the server or manually install the Cisco IMC firmware on the server.

Introduction to Cisco IMC Secure Boot

About Cisco IMC Secure Mode

Note Cisco IMC secure boot mode is enabled by default only on some Cisco UCS C-Series servers.

You can update Cisco IMC to the latest version using Host Upgrade Utility (HUU), web UI, or CLI. If you use HUU to upgrade Cisco IMC, you are prompted to enable secure boot mode. If you choose **Yes**, the system enters a secure mode and install the firmware twice. If you choose **No**, it enters a nonsecure mode. If you use either the web UI or CLI to upgrade Cisco IMC, you must upgrade to version 2.0(x). After you boot the system with version 2.0(x), it boots in a nonsecure mode by default. You must enable secure mode. when you enable secure mode, you are automatically reinstalling the firmware. In the web UI, the secure mode option is available

as a checkbox within the Cisco IMC firmware update page. In the CLI, you can enable the secure mode by using the **update-secure** command.

During the first upgrade to Cisco IMC version 2.0, a warning message might display stating that some of the features and applications are not installed correctly and a second upgrade is required. We recommend that you perform the second upgrade with or without the secure boot option enabled to correctly install the Cisco IMC firmware version 2.0(x) in a secure mode. After the installation is complete, you must activate the image. After you boot your system with the secure boot option enabled, Cisco IMC remains in secure mode and you cannot disable it later on. If you do not activate the image and reinstall any other firmware images, Cisco IMC may become unresponsive.

Warning After you install the firmware with the secure boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive.

The secure boot is enabled only when the firmware installation is complete and you have activated the image.

Note When Cisco IMC is in a secure mode, it means the following:

- Only signed Cisco IMC firmware images can be installed and booted on the device.
- Secure Cisco IMC mode cannot be disabled later on.
- Any Cisco IMC versions can be upgraded to the latest version directly.
- Cisco IMC firmware versions cannot be installed or booted prior to version 1.5(3x).
- Cisco IMC version 2.0 cannot be downgraded to version 1.4(x), 1.5, 1.5(2x), or 1.5(1), 1.5(2) or to any nonsecure firmware version.

Supported Cisco IMC Version When Downgrading from the Latest Version

The following table lists the Cisco IMC versions in a secure mode that can be downgraded to prior versions.

From Cisco IMC Version	To Cisco IMC Version	Possibility
2.0(x)	Prior to 1.5(1)	Not possible
2.0(x)	1.5(3x) or later	Possible
2.0(x)	Prior to 1.5(3x)	Not possible

Note When the Cisco IMC verison you are using is in a nonsecure mode, you can downgrade Cisco IMC to any prior version.

Note If you use HUU to downgrade Cisco IMC versions prior to 1.5(4), you must first downgrade Cisco IMC and then downgrade other firmware. Activate the firmware and then downgrade the BIOS firmware.

Number of Updates Required for Cisco IMC Version 2.0(1)

Important This section is valid for Cisco IMC version 2.0(1) and prior releases.

Supported Cisco IMC Version When Upgrading to the Latest Version

The following table lists the number of updates required for Cisco IMC to correctly install all the applications of the latest version.

From Cisco IMC Version	To a Nonsecure Cisco IMC Version 2.0(x)	To a Secure Cisco IMC Version 2.0(x)
Prior to 1.5(2)	Double update	Double update
1.5(2)	Single update	Double update
1.5(3)	Single update	Double update
1.5(3x) or Later	Single update	Double update

Updating Cisco IMC in a Nonsecure Mode

Important This section is valid for Cisco IMC version 2.0(1) and prior releases.

You can upgrade Cisco IMC to the latest version in a nonsecure mode with all the latest feature and applications installed correctly. When you upgrade Cisco IMC to the latest version using the web UI or CLI, you might need to update the firmware twice manually depending upon the version you are using. See, Supported Cisco IMC Version when Upgrading to the Latest Version. If you use HUU to upgrade the Cisco IMC verison, it gets upgraded to the latest verison automatically.

Note If you are installing from a Cisco IMC version prior to 1.5(2x), the following message is displayed:

Warning "Some of the Cisco IMC firmware components are not installed properly! Please reinstall Cisco IMC firmware version 2.0(1) or higher to recover".

Note If you are in the middle of (HUU) update, we recommend that you reconnect any KVM sessio current status of the update.

When Cisco IMC runs in a nonsecure mode, it implies the following:

- Any signed or unsigned Cisco firmware images can be installed on the device.
- Any Cisco IMC versions can be upgraded to the latest version directly.
- Cisco IMC firmware versions can be installed or booted to any prior versions.

Installing the Cisco IMC Firmware from a Remote Server

Before you begin

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in Obtaining Firmware from Cisco, on page 232.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install Cisco IMC Firmware from Remote Server**.

Step 4 In the **Install Cisco IMC Firmware** dialog box, complete the following fields:

Name	Description
Install Cisco IMC Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**

Name	Description
TFTP Server IP/Hostname field	The IP address or hostname of the server on which the Cisco IMC firmware installation file resides. Depending on the setting in the **Install Cisco IMC Firmware from** drop-down list, the name of the field might vary.
Image Path and Filename field	The path and filename of the Cisco IMC firmware installation file on the remote server.
Install Firmware button	Reinstalls Cisco IMC firmware with the latest updates. If you install the firmware with Cisco IMC secure boot enabled, you must activate the firmware image. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. **Note** After installing the firmware with the Secure Boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive. The secure boot is enabled only when the firmware installation is complete and you have activated the image.
Close button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 5 Click **Install Firmware**.

What to do next

Activate the Cisco IMC firmware Immediately.

Installing the Cisco IMC Firmware Through the Browser

Before you begin

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in Obtaining Firmware from Cisco, on page 232.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install Cisco IMC Firmware through Browser Client**.

Step 4 In the **Install Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the .bin file that you want to install.

Step 5 (Optional) Check the **Enable Cisco IMC Secure Boot** check box to enable secure mode for Cisco IMC.

Note This option is available for Cisco IMC version 2.0(1) only. For later versions, it is enabled by default.

If checked, a confirmation dialog box appears with a message that if secure boot is enabled, you can install only signed Cisco IMC firmware images on the device. Also, any unsigned Cisco IMC firmware images or images of Cisco IMC versions prior to 1.5(3x) are not supported. If you want to continue Cisco IMC in a secure boot, choose **OK**. If you do not want to continue Cisco IMC in a secure boot, choose **Cancel**.

Important After you enable secure boot, you cannot disable it later, and Cisco IMC continues to be in secure mode.

Step 6 Click **Install Firmware**.

Note After installing the firmware with the secure boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive.

For Cisco IMC version 2.0(1), the secure boot is enabled only when the firmware installation is complete and you have activated the image.

What to do next

Activate the Cisco IMC firmware immediately.

Activating Installed Cisco IMC Firmware

Before you begin

Install the Cisco IMC firmware on the server.

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset Cisco IMC.
- Activate any other firmware.
- Export technical support or configuration data.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Activate Cisco IMC Firmware**.

The **Activate Firmware** dialog box appears.

Step 4 In the **Activate Firmware** dialog box, choose the firmware image to activate.

Step 5 Click **Activate Firmware**.

Installing BIOS Firmware from a Remote Server

Note This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before you begin

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in Activating Installed Cisco IMC Firmware, on page 239.
- Power off the server.

Note For C220 M4, C240 M4 and C3160, you do not have to power off the server.

Caution When you install the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, Cisco IMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Status** area, verify that the **Power State** field says "Off". If it says "On", click **Power Off Server** in the **Actions** area and wait for the server to power off before continuing.

Step 4 In the **Navigation** pane, click the **Admin** tab.

Step 5 On the **Admin** tab, click **Firmware Management**.

Step 6 In the **Cisco IMC Firmware** area, make sure the firmware version shown in the **Running Version** field matches the BIOS firmware version you are installing.

Important If the Cisco IMC firmware version does not match, activate the Cisco IMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed Cisco IMC Firmware, on page 239.

Step 7 In the **Actions** area, click **Install BIOS Firmware from Remote Server**.

Step 8 In the **Install BIOS Firmware** dialog box, complete the following fields:

Name	Description
Install BIOS Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

Name	Description
Server IP/Hostname field	The IP address or hostname of the server on which the BIOS firmware installation file resides. Depending on the setting in the **Install BIOS Firmware from** drop-down list, the name of the field may vary.
Image Path and Filename field	The path and filename of the BIOS firmware installation file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 9 Click **Install Firmware**.

Step 10 Watch the messages in the **Status** field in the **Last BIOS Firmware Install** area until the status changes to "Completed Successfully".

Step 11 Power on the server to complete the BIOS upgrade.

Installing BIOS Firmware Through the Browser

Note This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before you begin

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in Activating Installed Cisco IMC Firmware, on page 239.
- Power off the server.

Note For C220 M4, C240 M4 and C3160, you do not have to power off the server.

Caution When you install the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, Cisco IMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Status** area, verify that the **Power State** field says "Off". If it says "On", click **Power Off Server** in the **Actions** area and wait for the server to power off before continuing.

Step 4 In the **Navigation** pane, click the **Admin** tab.

Step 5 On the **Admin** tab, click **Firmware Management**.

Step 6 In the **Cisco IMC Firmware** area, make sure the firmware version shown in the **Running Version** field matches the BIOS firmware version you are installing.

Important If the Cisco IMC firmware version does not match, activate the Cisco IMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed Cisco IMC Firmware, on page 239.

Step 7 In the **Actions** area, click **Install BIOS Firmware through Browser Client**.

Step 8 In the **Install BIOS Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the CAP file you want to install.

Step 9 Click **Install Firmware**.

Step 10 Watch the messages in the **Status** field in the **Last BIOS Firmware Install** area until the status changes to "Completed Successfully".

Step 11 Power on the server to complete the BIOS upgrade.

Activating Installed BIOS Firmware

Note The **Activate BIOS Firmware** option is available only for some C-Series servers. For the servers that do not have this option, you can activate the installed BIOS firmware by rebooting the server.

Before you begin

- Install the BIOS firmware on the server.
- Power off the host.

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset Cisco IMC.
- Activate any other firmware.
- Export technical support or configuration data.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Activate BIOS Firmware.**.

The **Activate Firmware** dialog box appears.

Step 4 In the **Activate Firmware** dialog box, choose the firmware image to activate.

Step 5 Click **Activate Firmware**.

Installing the CMC Firmware Through the Browser

Before you begin

Note This option is available only on some UCS C-Series servers.

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in Obtaining Firmware from Cisco, on page 232.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install CMC Firmware through Browser Client**.

Step 4 In the **Install Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the .bin file that you want to install.

Step 5 From the **CMC** drop-down menu, choose **CMC-1** or **CMC-2**.

Step 6 Click **Install Firmware**.

What to do next

Activate the CMC firmware immediately.

Installing the CMC Firmware from a Remote Server

Before you begin

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in Obtaining Firmware from Cisco, on page 232.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install CMC Firmware from Remote Server**.

Step 4 In the **Install CMC Firmware** dialog box, complete the following fields:

Name	Description
CMC drop-down list	Allows you to choose the CMC on SIOC controller 1 or 2. This can be one of the following: • **CMC-1** • **CMC-2**

Name	Description
Install CMC Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
TFTP Server IP/Hostname field	The IP address or hostname of the server on which the CMC firmware installation file resides. Depending on the setting in the **Install CMC Firmware from** drop-down list, the name of the field might vary.
Image Path and Filename field	The path and filename of the CMC firmware installation file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Install Firmware button	Reinstalls CMC firmware with the latest updates.
Close button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 5 Click **Install Firmware**.

What to do next

Activate the CMC firmware Immediately.

Activating Installed CMC Firmware

Before you begin

Install the CMC firmware on the server.

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset Cisco IMC.
- Activate any other firmware.
- Export technical support or configuration data.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Activate CMC Firmware**.

The **Activate Firmware** dialog box appears.

Step 4 In the **Activate Firmware** dialog box, choose the firmware image to activate.

Step 5 Click **Activate Firmware**.

Installing SAS Expander Firmware Through the Browser

Before you begin

- You must log in with admin privileges to perform this task.
- Power on the server.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install SAS Expander Firmware through Browser Client**.

Step 4 In the **Install SAS Expander Firmware** dialog box, click the **Choose File** button to select the firmware image you want to install.

Step 5 Select the SAS Expander from the **SAS Expander** drop-down list.

Step 6 Click **Install Firmware**.

Step 7 Power on the server to complete the upgrade.

Installing SAS Expander Firmware Through the Remote Server

Before you begin

- You must log in with admin privileges to perform this task.
- Power on the server.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install SAS Expander Firmware from Remote Server**.

Step 4 In the **Install SAS Expander Firmware** dialog box, complete the following fields:

Name	Description
SAS Expander drop-down list	Allows you to choose the SAS expander for which you to install the firmware. **Note** For some servers only one SAS expander is available.
Install SAS Expander Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

Name	Description
Server IP/Hostname field	The IP address or hostname of the server on which the SAS expander firmware installation file resides. Depending on the setting in the **Install SAS Expander Firmware from** drop-down list, the name of the field may vary.
Image Path and Filename field	The path and filename of the SAS expander firmware installation file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Install Firmware**.

Step 6 Power on the server to complete the upgrade.

Activating SAS Expander Firmware

Before you begin

- Install the SAS expander firmware on the server.
- Power on the host.

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset Cisco IMC.
- Activate any other firmware.
- Export technical support or configuration data.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Activate SAS Expander Firmware.**.

The **Activate SAS Expander Firmware** dialog box appears.

Step 4 In the **Activate SAS Expander Firmware** dialog box, choose the expander from the **SAS Expander** drop-down list.

Step 5 Choose the SAS Expander firmware version from the radio button.

Step 6 Click **Activate Firmware**.

Activating an SAS expander firmware makes it the running version.

CHAPTER 15

Viewing Faults and Logs

This chapter includes the following sections:

Faults Summary

Viewing the Fault Summary

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Fault Summary** tab, review the following information:

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Critical** • **Informational** • **Major** • **Minor** • **Warning**
Code	The unique identifier assigned to the fault.

Name	Description
DN	The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

Fault History

Viewing the Fault History

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Fault History** tab, review the following information:

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source	The software module that logged the event.
Probable Cause	The unique identifier associated with the event that caused the fault.

Name	Description
Description	More information about the fault. It also includes a proposed solution.

Cisco IMC Log

Viewing the Cisco IMC Log

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** window, click **Cisco IMC Log**.

Step 4 Review the following information for each Cisco IMC event in the log.

Name	Description
Time column	The date and time the event occurred.
Severity column	The event severity. This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source column	The software module that logged the event.
Description column	A description of the event.
Clear Log button	Clears all events from the log file. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.

Step 5 From the **Entries Per Page** drop-down list, select the number of Cisco IMC events to display on each page.

Step 6 Click **<Newer** and **Older>** to move backward and forward through the pages of Cisco IMC events, or click **<<Newest** to move to the top of the list.

By default, the newest Cisco IMC events are displayed at the top if the list.

Clearing the Cisco IMC Log

Before you begin

You must log in as a user with user privileges to clear the Cisco IMC log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click **Cisco IMC Log**.

Step 4 In the **Cisco IMC Log** pane, click **Clear Log**.

Step 5 In the dialog box that appears, click **OK**.

System Event Log

Viewing the System Event Log

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** window, click **System Event Log**.

Step 4 Above the log table, view the percentage bar, which indicates how full the log buffer is.

Step 5 Review the following information for each system event in the log:

Name	Description
Time column	The date and time the event occurred.
Severity column	The severity field includes both text and a color-coded icon. For the icon, green indicates normal operation, yellow is informational, and warning, critical, and non-recoverable errors are shown in shades of red.
Description column	A description of the event.

Name	Description
Clear Log button	Clears all events from the log file. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.

Step 6 Required: From the **Entries Per Page** drop-down list, select the number of system events to display on each page.

Step 7 Required: Click **<Newer** and **Older>** to move backward and forward through the pages of system events, or click **<<Newest** to move to the top of the list.

By default, the newest system events are displayed at the top if the list.

Clearing the System Event Log

Before you begin

You must log in as a user with user privileges to clear the system event log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** window, click **System Event Log**.

Step 4 In the **System Event Log** pane, click **Clear Log**.

Step 5 In the dialog box that appears, click **OK**.

Logging Controls

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive Cisco IMC log entries.

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In either of the **Remote Syslog Server** areas, complete the following fields:

Name	Description
Enabled check box	If checked, Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. You can set an IPv4 or IPv6 address or a domain name as the remote system address.
Port field	Enter a destination port number of the Syslog server within the range 1 to 65535. The default port number is 514.

Step 5 (Optional) In the **Minimum Severity to Report** drop-down list, specify the lowest level of messages that will be included in the remote logs.

You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the Cisco IMC remote log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Step 6 Click **Save Changes**.

Configuring the Cisco IMC Log Threshold

You can specify the lowest level of messages that will be included in the Cisco IMC log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 Required: In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages that will be included in the Cisco IMC log.

You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note Cisco IMC does not log any messages with a severity below the selected severity. For example, if you select **Error**, then the Cisco IMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Sending a Test Cisco IMC Log to a Remote Server

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In the **Action** area, click **Send Test Syslog**.

A test Cisco IMC log is sent to the configured remote servers.

CHAPTER 16

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Exporting Technical Support Data to a Remote Server

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Technical Support Data to Remote Server**.

Step 4 In the **Export Technical Support Data** dialog box, complete the following fields:

Name	Description
Export Technical Support Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
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 **Export Technical Support Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server. **Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

What to do next

Provide the generated report file to Cisco TAC.

Downloading Technical Support Data to a Local File

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate Technical Support Data for Local Download**.

Step 4 In the **Download Technical Support Data to Local File** dialog box, complete the following fields:

Name	Description
Generate Technical Support Data radio button	Cisco IMC disables this radio button when there is no technical support data file to download. Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Regenerate Technical Support Data radio button	Cisco IMC displays this radio button when a technical support data file is available to download. To replace the existing support data file with a new one, select this option and click **Regenerate**. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Download to local file radio button	Cisco IMC enables this radio button when a technical support data file is available to download. To download the existing file, select this option and click **Download**. **Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card.
Generate button	Allows you to generate the technical support data file.
Download button	Allows you to download the technical support data file after it is generated.

What to do next

Provide the generated report file to Cisco TAC.

Rebooting Cisco IMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the Cisco IMC. This procedure is not part of the normal maintenance of a server. After you reboot the Cisco IMC, you are logged off and the Cisco IMC will be unavailable for a few minutes.

Note If you reboot the Cisco IMC while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the Cisco IMC reboot is complete.

Before you begin

You must log in as a user with admin privileges to reboot the Cisco IMC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Reboot Cisco IMC**.

Step 4 Click **OK**.

Recovering from a Corrupted BIOS

Note This procedure is not available in some server models.

In addition to this procedure, there are three other methods for recovering from a corrupted BIOS:

- Use the Cisco Host Upgrade Utility (HUU). This is the recommended method.
- Use the Cisco IMC CLI interface.
- If your server model supports it, use the BIOS recovery function of the hardware jumper on the server motherboard. For instructions, see the Cisco UCS Server Installation and Service Guide for your server model.

Before you begin

- You must be logged in as admin to recover corrupt BIOS.
- Have the BIOS recovery ISO image ready. You will find the BIOS recovery ISO image under the **Recovery** folder of the firmware distribution package.
- Schedule some down time for the server because it will be powered cycled at the end of the recovery procedure.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the server tab, click **BIOS**.

The BIOS page appears.

Step 3 In the **Actions** area, click **Recover Corrupt BIOS**.

The **Recover Corrupt BIOS** wizard appears.

Step 4 Use the **Recover Corrupt BIOS** wizard to recover your corrupt BIOS.

Resetting Cisco IMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the Cisco IMC to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the Cisco IMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

When you upgrade from version 1.5(1) to version 1.5(2), the hostname in the Cisco IMC interface is retained as is. However, after upgrading to version 1.5(2), if you do a factory reset, the hostname changes to CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

When you downgrade from version 1.5(2) to version 1.5(1), the hostname is retained as is. However, if you do a factory reset, the hostname changes to ucs-cxx-mx format.

Note If you reset Cisco IMC 1.5(x), 2.0, and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default. For C3160 servers, if you reset Cisco IMC to factory defaults, **Dedicated** mode is configured to **Full** duplex with 100 Mbps speed by default.

Before you begin

You must log in as a user with admin privileges to reset the Cisco IMC to factory defaults.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Reset Cisco IMC to Factory Default Configuration**.

Step 4 Click **OK**.

A reboot of Cisco IMC while the host is performing BIOS POST (Power on Self Test) or is in EFI shell will turn off the host for a short amount of time. Cisco IMC will power on when it is ready.

Exporting and Importing the Cisco IMC Configuration

Exporting and Importing the Cisco IMC Configuration

To perform a backup of the Cisco IMC configuration, you take a snapshot of the system configuration and export the resulting Cisco IMC configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported Cisco IMC configuration file to the same system or you can import it to another Cisco IMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The Cisco IMC configuration file is an XML text file whose structure and elements correspond to the Cisco IMC command modes.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

You can perform an import or an export operation on the following features:

- Cisco IMC version

  Note You can only export this information.

- Network settings
- Technical support
- Logging control for local and remote logs
- Power policies
- BIOS - BIOS Parameters

  Note Precision boot is not supported.

- Communication services
- Remote presence
- User management - LDAP
- Event management
- SNMP

Exporting the Cisco IMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Before you begin

Obtain the backup remote server IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Cisco IMC Configuration**.

Step 4 In the **Export Cisco IMC Configuration** dialog box, complete the following fields:

Name	Description
Export To drop-down list	The location where you want to save the XML configuration file. This can be one of the following: • **Local**: Select this option and click **Export** to save the XML configuration file to a drive that is local to the computer running the Cisco IMC GUI.. When you select this option, Cisco IMC GUI displays a **File Download** dialog box that lets you navigate to the location to which the configuration file should be saved. • **Remote Server**: Select this option to import the XML configuration file from a remote server. When you select this option, Cisco IMC GUI displays the remote server fields.

Name	Description
Export To drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server to which the configuration file will be exported. Depending on the remote server type selected in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the exported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )"

Step 5 Click **Export**.

Importing a Cisco IMC Configuration

Before you begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, Cisco IMC does not overwrite the current values with those saved in the configuration file.

In the XML file that contains the Cisco IMC configuration, the network settings information will be commented out. You must un-comment it if you want to import the IP settings information. To un-comment the network settings, delete the following text in the XML file:

```
“□!- -Kindly Update and uncomment below settings for
network configurations “ and ”- -□”
```

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Import Cisco IMC Configuration**.

Step 4 In the **Import Cisco IMC Configuration** dialog box, complete the following fields:

Name	Description
Import From drop-down list	The location of the XML configuration file. This can be one of the following: • **Local**: Select this option to import the XML configuration file to a drive that is local to the computer running Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import. • **Remote Server**: Select this option to import the XML configuration file from a remote server. When you select this option, Cisco IMC GUI displays the remote server fields.

Name	Description
Import From drop-down list	**Note** These options are available only when you choose **Remote**. The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server on which the configuration file resides. Depending on the remote server type selected in the **Import From** drop-down list, the name of the field might vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the imported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" **Note** If you edit the encrypted sections in the configuration file and try to import it, the edits will be ignored and the import operation displays a partially successful message.

Step 5 Click **Import**.

Generating Non Maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the OS.

Before you begin

- You must log in as a user with admin privileges.
- The server must be powered on.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate NMI to host**.

This action sends an NMI signal to the host, which might restart the OS.

Step 4 Click **OK**.

Adding or Updating the Cisco IMC Banner

You can modify copyright information or messages that you want to display on the login screen using this feature. Complete the following steps:

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Add/Update Cisco IMC Banner**.

The **Add/Update Cisco IMC Banner** pop-up window appears.

Step 4 In the **Banner** area, review the following information:

Name	Description
Banner (80 Chars per line. Max 2K Chars.) field	Enter copyright information or messages that you want to display on the login screen, before logging on to the Web UI or the command line interface.

Name	Description
Restart SSH checkbox	When checked, the active SSH sessions are terminated after you click the **Save Banner** button.

What to do next

Viewing Cisco IMC Last Reset Reason

You can view the reason for why a component was last reset by the user using this feature.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Cisco IMC Last Reset** area of the **Utilities** pane, review the following information.

Name	Description
Status field	The reason why the component was last reset. This can be one of the following: • **watchdog-reset**—The watchdog-timer resets when the Cisco IMC memory reaches full capacity. • **ac-cycle**— PSU power cables are removed (no power input). • **graceful-reboot**— Cisco IMC reboot occurs.

Enabling Secure Adapter Update

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Secure Adapter Update** area, check the **Secure Adapter Update** check box to enable the secure adapter update.

Note If you wish to disable the update, uncheck the **Secure Adapter Update** check box.

Downloading Hardware Inventory to a Local File

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Download Hardware Inventory Data to Local Download**.

Step 4 In the **Download Inventory Data to Local File** dialog box, complete the following fields:

Name	Description
Generate Inventory Data radio button	Cisco IMC displays this radio button when there is no hardware inventory data file to download.
Download to local file radio button	Cisco IMC enables this radio button when a inventory data file is available to download. To download the existing file, select this option and click **Download**.

Step 5 Click **Generate** to create the data file. When data collection is complete, select the **Download Inventory Data to Local File** radio button and click **Download** to download the file locally.

Exporting Inventory Hardware Data to a Remote Server

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Inventory Hardware Data to Remote Server** .

Step 4 In the **Export Hardware Inventory Data** dialog box, complete the following fields:

Name	Description
Export Hardware Inventory Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IP address or hostname of the server on which the data file should be stored. Depending on the setting in the **Export Hardware Inventory Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

CHAPTER 17

Troubleshooting

This chapter includes the following sections:

Recording the Last Boot Process

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Troubleshooting**.

Step 3 In the **Bootstrap Process Recording** area of the **Troubleshooting** tab, check **Enable Recording** check-box.

By default, this option is enabled.

Caution This task is for troubleshooting purpose, and might impact Cisco IMC performance if it is enabled all the time.

Step 4 (Optional) If you want to record the boot process until BIOS POST, then check **Stop On BIOS POST** check-box.

Step 5 Click **Save Changes**

Step 6 On the tool bar above the **Work** pane, click **Power On Server**.

Step 7 In the **Actions** area, of the **Bootstrap Process Recording** pane, click **Play Recording**.

A confirmation dialog box with instructions on supported Java version appears.

Step 8 Review the instructions and click **Ok**.

The **DVR Player Controls** dialog box opens. This dialog box plays the recording of the last boot process. If you have enabled **Stop On BIOS POST** option then the system plays the recording process only till BIOS POST.

This recording can be reviewed to analyze the factors that caused the system to reboot.

Step 9 In the **Actions** area of the **Bootstrap Process Recording** area, click **Download Recording**.

Follow the instructions to download.

Note The file is saved in a `.dvc` format to a local drive. You can view this recording using KVM player or an offline player. Every time you choose **Download Recording** option, the last boot process is recorded, it autogenerate the file name, and save it in the path specified earlier.

Step 10 Once the download is complete, you can select the file that you want play the video of the recording, and click **Open**.
A **DVR Player Controls** window opens and plays the video of the selected file.

Recording Last Crash Capture

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Troubleshooting**.

Step 3 In the **Crash Recording** area of the **Troubleshooting** tab, check **Enable Recording** check-box.

Caution This task is for troubleshooting purpose, and might impact Cisco IMC performance if it is enabled all the time.

Step 4 Click **Save Changes**.
Capture Recording button in the **Actions** area is enabled.

Step 5 (Optional) In the **Actions** area, click **Capture Recording**, to capture the recording of the system that crashed automatically.

Note If you choose this option, it overwrites the existing crash records file. Click **OK** to continue.

Step 6 Click **Play Recording** in the **Actions** area to view the recording of the operations that ran on the server.

A confirmation dialog box with instructions on supported Java version appears.

Step 7 Review the instructions and click **Ok**.

The **DVR Player Controls** dialog box appears. This dialog box plays the recording of the operations that ran on the server in the last few minutes. This recording can be reviewed to analyze the factors that caused system to crash.

Step 8 In the **Actions** area of the **Crash Recording** area, click **Download Recording**.

Follow the instructions to download.

Note The file is saved in a `.dvc` format to a local drive. You can view this recording using KVM player or an offline player. Every time you choose **Download Recording** option, the last crash process is recorded, it autogenerate the file name, and save it in the path specified earlier.

Step 9 Once the download is complete, you can select the file that you want play the video of the recording, and click **Open**.
A **DVR Player Controls** window opens and plays the video of the selected file.

Downloading a DVR Player

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Troubleshooting**.

Step 3 In the **Player** area of the **Troubleshooting** tab, click **Download Player**.

Step 4 Follow the instructions to download. These files are saved to your local drive as a zipped file in a .tgz file format.

The offline player is stored for Windows, Linux, and MAC.

Step 5 Extract the zip file. The zip file generally gets saved below the bootstrap file, and its name follows the format `offline.tgz`

Step 6 Open the script file that you want to review the video recording.

Note If you want to play the recording for Windows, then ensure that the Java version running on your system and in the script file are the same. If the Windows script file fails to play the recording, then follow these steps:

a) Extract the Windows script file to your desktop.
b) Open the file using notepad.
c) Search for jre, and replace the Java version to match the version running on your system. By default, the Java version is set to jre7.
d) Save the file.

After you update the Java version, you can delete the extracted files from your desktop.

Note Verification of Java version is required only for Windows OS. For Linux and MAC, the Java version is picked automatically.

Step 7 Navigate to the folder in which these files are downloaded and open the script file that you want to play the video recording.
The DVR player is launched, playing the video of the operations that ran on the server.

Playing a Recorded Video Using the DVR Player on the KVM Console

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 In the **Actions** area of the **Virtual KVM** tab, click **Launch KVM Console**.

Note You can also launch KVM console by clicking **Launch KVM Console** button on the toolbar displayed above the **Work** pane.

The **KVM Console** opens in a separate window.

Step 5 On the **KVM Console** window, choose **Tools** > **Recorder /Playback Controls**.
A DVR Player Controls window opens.

Step 6 On the **DVR Player Controls** window, click **Open** button.

Step 7 Choose the file that you want to play the recording, and click **Open**.
The DVR player is launched, playing the video of the operations that ran on the server.

APPENDIX A

BIOS Parameters by Server Model

This appendix contains the following sections:

C22 and C24 Servers

Main BIOS Parameters for C22 and C24 Servers

Name	Description
TPM Support	TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Advanced BIOS Parameters for C22 and C24 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All**—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n***—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel VT	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.

Name	Description
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise**—All options are enabled. • **High Throughput**—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC**—All options are enabled. This setting is also known as high performance computing. • **Custom**—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled**—The processor only fetches the required line. • **Enabled**— The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled**—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled**—Data from I/O devices is not placed directly into the processor cache. • **Enabled**—Data from I/O devices is placed directly into the processor cache.
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom**—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled**—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient**—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.

Name	Description
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled**—The BIOS does not send the C6 report. • **Enabled**—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled**—The CPU continues to run at its maximum frequency in C1 state. • **Enabled**—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled**— The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled**— The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL**—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance**—System performance is optimized. • **Mirroring**—System reliability is optimized by using half the system memory as backup. • **Lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced**— DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance**—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **Energy Efficient**—DRAM clock throttling is increased to improve energy efficiency.

Name	Description
NUMA	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **Disabled**—The BIOS does not support NUMA. • **Enabled**—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Power Saving Mode**—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **Performance Mode**—The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x**—DRAM cells are refreshed every 64ms. • **2x**—DRAM cells are refreshed every 32ms. • **3x**—DRAM cells are refreshed every 21ms. • **4x**—DRAM cells are refreshed every 16ms. • **Auto**—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way**—The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way**—The maximum amount of rank interleaving is used.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled**— Single bit memory errors are not corrected. • **Enabled**— Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

Name	Description
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **Auto**—The CPU determines the physical elevation. • **300 M**—The server is approximately 300 meters above sea level. • **900 M**—The server is approximately 900 meters above sea level. • **1500 M**—The server is approximately 1500 meters above sea level. • **3000 M**—The server is approximately 3000 meters above sea level.

QPI Configuration Parameters

Name	Description
QPI Link Frequency Select	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto**—The CPU determines the QPI link frequency. • **6.4 GT/s** • **7.2 GT/s** • **8.0 GT/s**

Name	Description
QPI Snoop Mode	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Auto**—The CPU automatically recognizes this as Early Snoop mode. • **Early Snoop**— The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized. • **Home Snoop**— The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Home Directory Snoop**— The home directory is an optional enabled feature that is implemented at both the HA and iMC logic in the processor. The goal of the directory is to filter snoops to the remote sockets and a node controller in scalable platforms and 2S and 4S configurations. • **Home Directory Snoop with OSB**— In the Opportunistic Snoop Broadcast (OSB) directory mode, the HA could choose to do speculative home snoop broadcast under very lightly loaded conditions even before the directory information has been collected and checked.

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **Disabled**—The software RAID controller is not available. • **Enabled**—The software RAID controller is available.

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled**—All USB devices are disabled. • **Enabled**—All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Front	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Internal	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: KVM	Whether the KVM ports are enabled or disabled. This can be one of the following: • **Disabled**—Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled**—Enables the KVM keyboard and/or mouse devices.
USB Port: vMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
MMIO Above 4GB	Whether to enable or disable MMIO above 4GB or not. This can be one of the following: • **Disabled**—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled**—The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Disabled**—ASPM support is disabled in the BIOS. • **Force L0s**—Force all links to L0 standby (L0s) state. • **Auto**—The CPU determines the power state.

Name	Description
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **Onboard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled**—Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled**—No console redirection occurs during POST. • **Enabled**—Enables console redirection on serial port A during POST.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI**—The PC-ANSI terminal font is used. • **VT100**—A supported vt100 video terminal and its character set are used. • **VT100+**—A supported vt100-plus video terminal and its character set are used. • **VT-UTF8**—A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600**—A 9,600 BAUD rate is used. • **19200**—A 19,200 BAUD rate is used. • **38400**—A 38,400 BAUD rate is used. • **57600**—A 57,600 BAUD rate is used. • **115200**—A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None**—No flow control is used. • **Hardware RTS/CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100**—The function keys generate **`ESC OP`** through **`ESC O[.`** • **LINUX**—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate **`ESC [[A`** through **`ESC [[E`**. • **XTERMR6**—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO**—The function keys F1 to F12 generate **`ESC [M`** through **`ESC [X`**. The function and shift keys generate **`ESC [Y`** through **`ESC [j`**. The control and function keys generate **`ESC [k`** through **`ESC [v`**. The shift, control and function keys generate **`ESC [w`** through **`ESC [{`**. • **ESCN**—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as **`ESC [11~`** and **`ESC [12~`**. • **VT400**—The function keys behave like the default mode. The top row of the numeric keypad generates **`ESC OP`** through **`ESC OS`**.
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable**—BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader**—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.
Out-of-Band Mgmt Port	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: • **Disabled**—Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • **Enabled**—Configures the COM port 0 as a remote management port for Windows Emergency Management services.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled**—All LOM ports are disabled. • **Enabled**—All LOM ports are enabled.
LOM Port *n* OptionROM	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled**—Option ROM is not available on LOM port ***n***. • **Enabled**—Option ROM is available on LOM port ***n***. • **UEFI Only**—The expansion slot ***n*** is available for UEFI only. • **Legacy Only**—The expansion slot ***n*** is available for legacy only.
All PCIe Slots OptionROM	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for all PCIe slots are not available. • **Enabled**—The Option ROMs for all the PCIe slots are available. • **UEFI Only**—The Opiton ROMs for slot ***n*** are available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** are available for legacy only.
PCIe Slot:*n* OptionROM	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.

Name	Description
PCIe Slot:*n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **Disabled**—The maximum speed is not restricted. For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to **GEN2**. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.
CDN Support for LOM	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. By default, CDN option is disabled. • **LOMS Only**— OS Ethernet Network identifier is named in a consistent device naming (CDN) according to the physical LAN on Motherboard(LOM) port numbering; LOM Port 0, LOM Port 1 and so on. **Note** CDN is enabled for LOM ports and works with Windows 2012 or the latest OS only.
CDN Support for VIC	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— CDN support for VIC cards is disabled. • **Enabled**— CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.

Server Management BIOS Parameters for C22 and C24 Servers

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled**—The FRB2 timer is not used. • **Enabled**—The FRB2 timer is started during POST and used to recover the system if necessary.
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled**—The watchdog timer is not used to track how long the server takes to boot. • **Enabled**—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the Cisco IMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Watchdog Timer Timeout	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5 Minutes**—The OS watchdog timer expires 5 minutes after it begins to boot. • **10 Minutes**—The OS watchdog timer expires 10 minutes after it begins to boot. • **15 Minutes**—The OS watchdog timer expires 15 minutes after it begins to boot. • **20 Minutes**—The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing**—The server takes no action if the watchdog timer expires during OS boot. • **Power Down**—The server is powered off if the watchdog timer expires during OS boot. • **Reset**—The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

C220 and C240 Servers

Main BIOS Parameters for C220 and C240 Servers

Name	Description
TPM Support	TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Advanced BIOS Parameters for C220 and C240 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All**—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n***—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel VT	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.

Name	Description
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise**—All options are enabled. • **High Throughput**—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC**—All options are enabled. This setting is also known as high performance computing. • **Custom**—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled**—The processor only fetches the required line. • **Enabled**— The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled**—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled**—Data from I/O devices is not placed directly into the processor cache. • **Enabled**—Data from I/O devices is placed directly into the processor cache.
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom**—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled**—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient**—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.

Name	Description
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled**—The BIOS does not send the C6 report. • **Enabled**—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled**—The CPU continues to run at its maximum frequency in C1 state. • **Enabled**—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled**— The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled**— The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL**—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance**—System performance is optimized. • **Mirroring**—System reliability is optimized by using half the system memory as backup. • **Lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced**— DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance**—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **Energy Efficient**—DRAM clock throttling is increased to improve energy efficiency.

Name	Description
NUMA	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **Disabled**—The BIOS does not support NUMA. • **Enabled**—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Power Saving Mode**—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **Performance Mode**—The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x**—DRAM cells are refreshed every 64ms. • **2x**—DRAM cells are refreshed every 32ms. • **3x**—DRAM cells are refreshed every 21ms. • **4x**—DRAM cells are refreshed every 16ms. • **Auto**—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way**—The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way**—The maximum amount of rank interleaving is used.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled**— Single bit memory errors are not corrected. • **Enabled**— Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

Name	Description
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **Auto**—The CPU determines the physical elevation. • **300 M**—The server is approximately 300 meters above sea level. • **900 M**—The server is approximately 900 meters above sea level. • **1500 M**—The server is approximately 1500 meters above sea level. • **3000 M**—The server is approximately 3000 meters above sea level.

QPI Configuration Parameters

Name	Description
QPI Link Frequency Select	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto**—The CPU determines the QPI link frequency. • **6.4 GT/s** • **7.2 GT/s** • **8.0 GT/s**

Name	Description
QPI Snoop Mode	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Auto**—The CPU automatically recognizes this as Early Snoop mode. • **Early Snoop**— The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized. • **Home Snoop**— The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Home Directory Snoop**— The home directory is an optional enabled feature that is implemented at both the HA and iMC logic in the processor. The goal of the directory is to filter snoops to the remote sockets and a node controller in scalable platforms and 2S and 4S configurations. • **Home Directory Snoop with OSB**— In the Opportunistic Snoop Broadcast (OSB) directory mode, the HA could choose to do speculative home snoop broadcast under very lightly loaded conditions even before the directory information has been collected and checked.

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **Disabled**—The software RAID controller is not available. • **Enabled**—The software RAID controller is available.
Onboard SCU Storage SW Stack	Allows you to choose a pre-boot software stack for an onboard SCU storage controller. This can be one of the following: • **Intel RSTe(1)** • **LSI SW RAID (0)** **Note** This configuration parameter is valid only for the C220 servers.

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled**—All USB devices are disabled. • **Enabled**—All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Front	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Internal	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: KVM	Whether the KVM ports are enabled or disabled. This can be one of the following: • **Disabled**—Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled**—Enables the KVM keyboard and/or mouse devices.
USB Port: vMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.
USB Port: SD Card	Whether the SD card drives are enabled or disabled. This can be one of the following: • **Disabled**—Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • **Enabled**—Enables the SD card drives.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB	Whether to enable or disable MMIO above 4GB or not. This can be one of the following: • **Disabled**—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled**—The server maps I/O of 64-bit PCI devices to 4GB or greater address space. **Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.

Name	Description
MMCFG BASE	Sets the low base address for PCIe adapters within 4GB. This can be one of the following: • **1 GB** • **2 GB** • **2.5 GB** • **3 GB** • **Auto**— Automatically sets the low base address for PCIe adapters. **Note** This is valid for C240 servers only.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Disabled**—ASPM support is disabled in the BIOS. • **Force L0s**—Force all links to L0 standby (L0s) state. • **Auto**—The CPU determines the power state.
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **Onboard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled**—Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
Out-of-Band Mgmt Port	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: • **Disabled**—Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • **Enabled**—Configures the COM port 0 as a remote management port for Windows Emergency Management services.
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled**—No console redirection occurs during POST. • **COM 0**—Enables console redirection on COM port 0 during POST. • **COM 1**—Enables console redirection on COM port 1 during POST.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI**—The PC-ANSI terminal font is used. • **VT100**—A supported vt100 video terminal and its character set are used. • **VT100+**—A supported vt100-plus video terminal and its character set are used. • **VT-UTF8**—A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
Bits per second	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600**—A 9,600 BAUD rate is used. • **19200**—A 19,200 BAUD rate is used. • **38400**—A 38,400 BAUD rate is used. • **57600**—A 57,600 BAUD rate is used. • **115200**—A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None**—No flow control is used. • **Hardware RTS/CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100**—The function keys generate **`ESC OP`** through **`ESC O[.`** • **LINUX**—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate **`ESC [[A`** through **`ESC [[E`**. • **XTERMR6**—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO**—The function keys F1 to F12 generate **`ESC [M`** through **`ESC [X`**. The function and shift keys generate **`ESC [Y`** through **`ESC [j`**. The control and function keys generate **`ESC [k`** through **`ESC [v`**. The shift, control and function keys generate **`ESC [w`** through **`ESC [{`**. • **ESCN**—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as **`ESC [11~`** and **`ESC [12~`**. • **VT400**—The function keys behave like the default mode. The top row of the numeric keypad generates **`ESC OP`** through **`ESC OS`**.
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable**—BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader**—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

LOM and PCIe Slots Configuration Parameters

Name	Description
CDN Support for LOM	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. By default, CDN option is disabled. • **LOMS Only**— OS Ethernet Network identifier is named in a consistent device naming (CDN) according to the physical LAN on Motherboard(LOM) port numbering; LOM Port 0, LOM Port 1 and so on. **Note** CDN is enabled for LOM ports and works with Windows 2012 or the latest OS only.
CDN Support for VIC	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— CDN support for VIC cards is disabled. • **Enabled**— CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.
All Onboard LOM Ports	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled**—All LOM ports are disabled. • **Enabled**—All LOM ports are enabled.
LOM Port *n* OptionROM	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.

Name	Description
All PCIe Slots OptionROM	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Slot:*n* OptionROM	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Mezzanine OptionROM	Whether the PCIe mezzanine slot expansion ROM is available to the server. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.

Name	Description
PCIe Slot:*n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **Disabled**—The maximum speed is not restricted. For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to **GEN2**. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.

Server Management BIOS Parameters for C220 and C240 Servers

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled**—The FRB2 timer is not used. • **Enabled**—The FRB2 timer is started during POST and used to recover the system if necessary.
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled**—The watchdog timer is not used to track how long the server takes to boot. • **Enabled**—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the Cisco IMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.

Name	Description
OS Watchdog Timer Timeout	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5 Minutes**—The OS watchdog timer expires 5 minutes after it begins to boot. • **10 Minutes**—The OS watchdog timer expires 10 minutes after it begins to boot. • **15 Minutes**—The OS watchdog timer expires 15 minutes after it begins to boot. • **20 Minutes**—The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing**—The server takes no action if the watchdog timer expires during OS boot. • **Power Down**—The server is powered off if the watchdog timer expires during OS boot. • **Reset**—The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

APPENDIX B

BIOS Token Name Comparison for Multiple Interfaces

This appendix contains the following section:

BIOS Token Name Comparison for Multiple Interfaces

The following table lists the BIOS token names used in the XML, CLI and Web GUI interfaces. You can use this list to map the names across these interfaces.

Note The parameters that are available depend on the type of Cisco UCS server you are using.

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
Main	TPM Support	biosVfTPMSupport/ vpTPMSupport	TPMAdminCtrl
Process Configuration	Intel(R) Hyper-Threading Technology	biosVfIntelHyperThreadingTech/ vpIntelHyperThreadingTech	IntelHyperThread
	Number of Enable Cores	biosVfCoreMultiProcessing/ vpCoreMultiProcessing	CoreMultiProcessing
	Execute Disable	biosVfExecuteDisableBit/ vpExecuteDisableBit	ExecuteDisable
	Intel(R) VT	biosVfIntelVirtualizationTechnology/ vpIntelVirtualizationTechnology	IntelVT

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Intel(R) VT-d	biosVfIntelVTForDirectedIO/ vpIntelVTForDirectedIO	IntelVTD
	Intel(R) VT-d Coherency Support	biosVfIntelVTForDirectedIO/ vpIntelVTDCoherencySupport	CoherencySupport
	Intel(R) VT-d ATS Support	biosVfIntelVTForDirectedIO/ vpIntelVTDATSSupport	ATS
	CPU Performance	biosVfCPUPerformance/ vpCPUPerformance	CpuPerformanceProfile
	Hardware Prefetcher	biosVfHardwarePrefetch/ vpHardwarePrefetch	HardwarePrefetch
	Adjacent Cache Line Prefetcher	biosVfAdjacentCacheLinePrefetch/ vpAdjacentCacheLinePrefetch	AdjacentCacheLinePrefetch
	DCU Streamer Prefetch	biosVfDCUPrefetch/ vvpStreamerPrefetch	DcuStreamerPrefetch
	DCU IP Prefetcher	biosVfDCUPrefetch/ vpIPPrefetch	DcuIpPrefetch
	Direct Cache Access Support	biosVfDirectCacheAccess/ vpDirectCacheAccess	DirectCacheAccess
	Power Technology	biosVfCPUPowerManagement/ vpCPUPowerManagement	CPUPowerManagement
	Enhanced Intel Speedstep(R) Technology	biosVfEnhancedIntelSpeedStepTech/ vpEnhancedIntelSpeedStepTech	EnhancedIntelSpeedStep
	Intel(R) Turbo Boost Technology	biosVfIntelTurboBoostTech/ vpIntelTurboBoostTech	IntelTurboBoostTech
	Processor Power state C6	biosVfProcessorCState/ vpProcessorCState	ProcessorC6Report
	Processor Power state C1 Enhanced	biosVfProcessorC1E/ vpProcessorC1E	ProcessorC1E

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Frequency Floor Override	biosVfCPUFrequencyFloor/ vpCPUFrequencyFloor	CpuFreqFloor
	P-STATE Coordination	biosVfPStateCoordType/ vpPStateCoordType	PsdCoordType
	Energy Performance	biosVfCPUEnergyPerformance/ vpCPUEnergyPerformance	CpuEngPerfBias
Memory Configuration	Select Memory RAS	biosVfSelectMemoryRASConfiguration/ vpSelectMemoryRASConfiguration	SelectMemoryRAS
	DRAM Clock Throttling	biosVfDRAMClockThrottling/ vpDRAMClockThrottling	DRAMClockThrottling
	NUMA	biosVfNUMAOptimized/ vpNUMAOptimized	NUMAOptimize
	Low Voltage DDR Mode	biosVfLvDIMMSupport/ vpNUMAOptimized	LvDDRMode
	DRAM Refresh rate	biosVfDramRefreshRate/ vpDramRefreshRate	DramRefreshRate
	Channel Interleaving	biosVfMemoryInterleave/ vpChannelInterLeave	ChannelInterLeave
	Rank Interleaving	biosVfMemoryInterleave/ vpRankInterLeave	RankInterLeave
	Patrol Scrub	biosVfPatrolScrub/ vpPatrolScrub	PatrolScrub
	Demand Scrub	biosVfDemandScrub/ vpDemandScrub	DemandScrub
	Altitude	biosVfAltitude/ vpAltitude	Altitude
QPI Configuration	QPI Link Frequency Select	biosVfQPIConfig/ vpQPILinkFrequency	QPILinkFrequency
	Cluster on Die	biosVfCODEnable/ vpCODEnable	CODEnable

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Snoop Mode	biosVfEarlySnoop/ vpEarlySnoop	EarlySnoop
SATA Configuration	SATA Mode	Not supported	SATAMode
Onboard Storage	Onboard SCU Storage Support	biosVfOnboardStorage/ vpOnboardSCUStorageSupport	DisableSCU
	Onboard SCU Storage SW Stack	biosVfOnboardStorageSWStack vpOnboardSCUStorageSWStack	PchScuOromSelect
USB Configuration	Legacy USB Support	biosVfLegacyUSBSupport/ vpLegacyUSBSupport	LegacyUSBSupport
	Port 60/64 Emulation	biosVfUSBEmulation/ vpUSBEmul6064	UsbEmul6064
	All USB Devices	biosVfUSBPortsConfig/ vpAllUsbDevices	AllUsbDevices
	USB Port:Rear	biosVfUSBPortsConfig/ vpUsbPortRear	UsbPortRear
	USB Port:Front	biosVfUSBPortsConfig/ vpUsbPortFront	UsbPortFront
	USB Port:Internal	biosVfUSBPortsConfig/ vpUsbPortInternal	UsbPortInt
	USB Port:KVM	biosVfUSBPortsConfig/ vpUsbPortKVM	UsbPortKVM
	USB Port:Vmedia	biosVfUSBPortsConfig/ vpUsbPortVMedia	UsbPortVMedia
	USB Port:SD Card	biosVfUSBPortsConfig/ vpUsbPortSDCard	UsbPortSdCard
	xHCI Mode	biosVfPchUsb30Mode/ vpPchUsb30Mode	PchUsb30Mode
PCI Configuration	PCI ROM CLP	Not Supported	PciRomClp

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	MMIO above 4GB	biosVfMemoryMappedIOAbove4GB/ vpMemoryMappedIOAbove4GB	MemoryMappedIOAbove4GB
	ASPM Support	biosVfASPMSupport/ vpASPMSupport	ASPMSupport
	VGA Priority	biosVfVgaPriority/ vpVgaPriority	VgaPriority
Serial Configuration	Console Redirection	biosVfConsoleRedirection/ vpConsoleRedirection	ConsoleRedir
	Terminal Type	biosVfConsoleRedirection/ vpTerminalType	TerminalType
	Bits per second	biosVfConsoleRedirection/ vpBaudRate	BaudRate
	Flow Control	biosVfConsoleRedirection/ vpFlowControl	FlowCtrl
	Putty KeyPad	biosVfConsoleRedirection/ vpPuttyKeyPad	PuttyFunctionKeyPad
	Redirection After BIOS POST	biosVfConsoleRedirection/ vpLegacyOSRedirection	RedirectionAfterPOST
LOM and PCIe Slots Configuration	PCH SATA Mode	biosVfSataModeSelect/ vpSataModeSelect	SataModeSelect
	All Onboard LOM Ports	biosVfSataModeSelect/ vpSataModeSelect	AllLomPortControl
	LOM Port 0 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort0State	LomOpromControlPort0
	LOM Port 1 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort1State	LomOpromControlPort1
	All PCIe Slots OptionROM	biosVfPCIOptionROMs/ vpPCIOptionROMs	PcieOptionROMs

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	PCIe Slot:*n* OptionROM	biosVfPCISlotOptionROMEnable/ vpSlot*n*State	PcieSlot*n*OptionROM
	PCIe Mezzanine OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMezzState	PcieMezzOptionROM
	PCIe Slot:1 Link Speed or SIOC1 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot1LinkSpeed	PcieSlot1LinkSpeed
	PCIe Slot:2 Link Speed or SIOC2 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot2LinkSpeed	PcieSlot2LinkSpeed
	PCIe Slot:MLOM OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMLOMState	PcieSlotMLOMOptionROM
	PCIe Slot:HBA OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotHBAState	PcieSlotHBAOptionROM
	PCIe Slot:N1 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN1State	PcieSlotN1OptionROM
	PCIe Slot:N2 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN2State	PcieSlotN2OptionROM
Server Management	FRB-2 Timer	biosVfFRB2Enable/ vpFRB2Enable	FRB-2
	OS Watchdog Timer	biosVfOSBootWatchdogTimer/ vpOSBootWatchdogTimer	OSBootWatchdogTimer
	OS Watchdog Timer Timeout	biosVfOSBootWatchdogTimerPolicy/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerTimeout
	OS Watchdog Timer Policy	biosVfOSBootWatchdogTimerTimeOut/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerPolicy

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Boot Order Rules	biosVfUCSMBootOrderRuleControl/ vpUCSMBootOrderRule	UCSMBootOrderRule

BIOS Token Name Comparison for Multiple Interfaces

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X