GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release 1.0

First Published: September 07, 2012

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

Text Part Number: OL-26445-01

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

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Describes the Cisco UCS E-Series Servers and the CIMC GUI.
Chapter 2	Installing the Server Operating System	Describes how to configure an operating system (OS) on the server.

Chapter	Title	Description
Chapter 3	Managing the Server	Describes how to configure the server boot device order, how to manage the server power, how to configure power policies, how to configure and manage RAID, and how to configure BIOS settings.
Chapter 4	Viewing Server Properties	Describes how to view the CPU, memory, power supply, storage, and PCI adapter properties of the server.
Chapter 5	Viewing Server Sensors	Describes how to view the fault, temperature, voltage, and storage sensors.
Chapter 6	Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Chapter 7	Managing User Accounts	Describes how to add or modify user accounts, how to configure Active Directory to authenticate users, and how to manage user sessions.
Chapter 8	Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, and network security.
Chapter 9	Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, IPMI, and SNMP.
Chapter 10	Managing Certificates	Describes how to generate, upload, and manage server certificates.
Chapter 11	Configuring Platform Event Filters	Describes how to configure and manage platform event filters.
Chapter 12	CIMC Firmware Management	Describes how to obtain, install, and activate firmware images.
Chapter 13	Viewing Logs	Describes how to view, export, and clear CIMC and system event log messages.
Chapter 14	Server Utilities	Describes how to export support data, how to export and import the server configuration, how to reset the server configuration to factory defaults, and how to reboot the management interface.
Chapter 15	Diagnostic Tests	Describes how to run diagnostic tests.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`courier` font	Terminal sessions and information that the system displays appear in `courier` font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

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

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

Warning Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

- Documentation Guide for Cisco UCS E-Series Servers—Provides links to all E-Series Server documentation
- *Release Notes for Cisco UCS E-Series Servers, Release 1.0*
- *Getting Started Guide for Cisco UCS E-Series Servers, Release 1.0*
- *Hardware Installation Guide for Cisco UCS E-Series Servers*
- *Cisco Network Modules, Server Modules, and Interface Cards Regulatory Compliance and Safety Information*
- *GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0*
- *CLI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0*
- *Troubleshooting Guide for Cisco UCS E-Series Servers*
- *Open Source Used in Cisco UCS E-Series Servers, Release 1.0*

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.

CHAPTER 1

Overview

This chapter includes the following sections:

Cisco UCS E-Series Servers Overview

The Cisco UCS E-Series Servers (E-Series Servers) are the next generation of Cisco UCS Express servers. E-Series Servers are a family of size, weight, and power efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (ISR G2). These servers provide a general purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Microsoft Windows or Linux; or as virtual machines on hypervisors, such as VMware vSphere Hypervisor™, Microsoft Hyper-V, or Citrix XenServer.

E-Series Servers reside in the Cisco 2900 series or 3900 series ISR G2. The following E-Series Servers are supported:

- UCS-E140S—Single-wide E-Series Server
- UCS-E140D—Double-wide E-Series Server, 4 core CPU
- UCS-E160D—Double-wide E-Series Server, 6 core CPU
- UCS-E140DP—Double-wide E-Series Server, 4 core CPU, with PCIe
- UCS-E160DP—Double-wide E-Series Server, 6 core CPU, with PCIe

Note For information about the maximum number of E-Series Servers that can be installed per ISR G2, see the "Server Hardware" section in the *Getting Started Guide for Cisco UCS E-Series Servers*.

Server Software

E-Series Servers require three major software systems:

- CIMC Firmware
- BIOS Firmware
- Operating System or Hypervisor

CIMC Firmware

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

CIMC is the management service for the E-Series Servers. You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server.

BIOS Firmware

BIOS initializes the hardware in the system, discovers bootable devices, and boots them in the provided sequence. It boots the operating system and configures the hardware for the operating system to use. BIOS manageability features allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, manage firmware, and create BIOS error reports.

The system ships with a running version of the BIOS firmware. You can update the BIOS firmware, but no initial installation is needed.

Operating System or Hypervisor

The main server CPU runs on an operating system, such as Microsoft Windows or Linux; or on a Hypervisor. You can purchase an E-Series Server with pre-installed Microsoft Windows Server or VMware vSphere Hypervisor™, or you can install your own platform.

The following platforms have been tested on the E-Series Servers:

- Microsoft Windows:
  - Windows Server 2008 R2 Standard 64-bit
  - Windows Server 2008 R2 Enterprise 64-bit
- Linux:
  - Red Hat Enterprise Linux 6.2
  - SUSE Linux Enterprise 11, service pack 2
  - Oracle Enterprise Linux 6.0, update 2
- Hypervisor:
  - VMware vSphere Hypervisor™ 5.0, update 1
  - Hyper-V (Windows 2008 R2)

◦ Citrix XenServer 6.0

CIMC Overview

The Cisco Integrated Management Controller (CIMC) is the management service for the E-Series Servers. CIMC runs within the server. You can use a web-based GUI or the SSH-based CLI to access, configure, administer, and monitor the server.

You can use CIMC to perform the following server management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Configure the server boot order
- Manage RAID levels
- View server properties and sensors
- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through the 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 CIMC firmware
- Update BIOS firmware
- Install the host image from an internal repository
- Monitor faults, alarms, and server status
- Collect technical support data in the event of server failure

Almost all tasks can be performed in either the GUI interface or CLI interface, and the results of tasks performed in one interface are displayed in another. However, you cannot do the following:

- Cannot use the CIMC GUI to invoke the CIMC CLI
- Cannot view a command that has been invoked through CIMC CLI in the CIMC GUI
- Cannot generate CIMC CLI output from the CIMC GUI

CIMC GUI

The CIMC GUI is a web-based management interface for E-Series Servers. You can launch the CIMC GUI and manage the server from any remote host that meets the following minimum requirements:

- Java 1.6 or later

- HTTP and HTTPS enabled
- Adobe Flash Player 10 or later

Logging Into the CIMC GUI

Before You Begin

- Make sure that you have configured the IP address to access CIMC. See the *Configuring CIMC Access* chapter in the *Getting Started Guide for Cisco UCS E-Series Server Modules*.
- If not installed, install Adobe Flash Player 10 or later on your local machine.

Procedure

Step 1 In your web browser, enter the IP address that you configured to access CIMC during initial setup.

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.

Step 4 Click **Log In**.

The **Change Password** dialog box appears.

Note The **Change Password** dialog box only appears the first time you log into CIMC. It does not appear for subsequent reboots.

Step 5 In the **New Password** field, enter your new password.

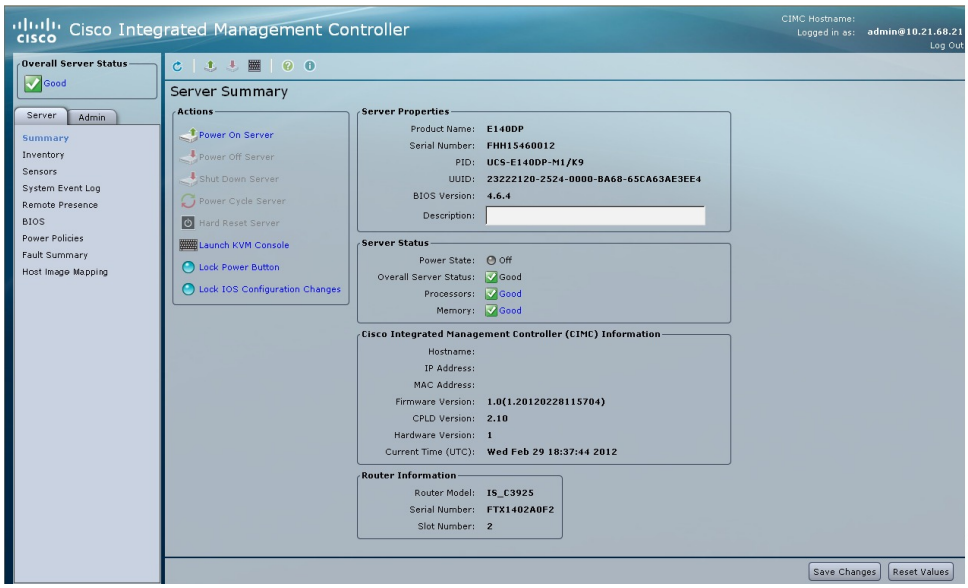
Step 6 In the **Confirm Password** field, enter the password again to confirm it.

Step 7 Click **Save Changes**.

The **Server Summary** page appears, which is the CIMC home page. See CIMC Home Page.

CIMC Home Page

The following figure shows the CIMC home page.



Navigation Pane

The Navigation pane displays on the left side in the CIMC user interface. Clicking links on the **Server** or **Admin** tabs in the **Navigation** pane displays the selected pages in the **Work** pane on the right side of the CIMC user interface.

The following table describes the elements in the **Navigation** pane:

Element Name	Description
Overall Server Status area	The **Overall Server Status** area is found above the **Server** and **Admin** tabs. Click this area to refresh the **Server Summary** page.
Server tab	The **Server** tab is found in the **Navigation** pane. It contains links to the following pages: • **Summary** • **Inventory** • **Sensors** • **System Event Log** • **Remote Presence** • **BIOS** • **Power Policies** • **Faults Summary** • **Host Image Mapping**

Admin tab	The **Admin** tab is found in the **Navigation** pane. It contains links to the following pages: • **User Management** • **Network** • **Communications Services** • **Certificate Management** • **CIMC Log** • **Event Management** • **Firmware Management** • **Utilities**

Work Pane

The **Work** pane displays on the right side of the UI. Different pages appear in the **Work** pane, depending on what link you click on the **Server** or **Admin** tab.

The following table describes the elements and pages in the **Work** pane.

Page or Element Name	Description
Summary	There are four areas on this page: • **Actions**—Use this area to control server power, reset the server, launch the KVM console, or control the locator LED. • **Server Properties**—Use this area to view the general server properties and assign a server description. • **Server Status**—Use this area to view the overall status of the major server subsystems. • **CIMC Information**—Use this area to view the server management name, network addresses, firmware version, and current date and time. • **Router Information**—Use this area to view the model and serial number of the router, and the slot number of the router in which the server is installed.

Inventory	There are five tabs on the page: • **CPUs**—Use this tab to view information about the CPU. • **Memory**—Use this tab to view information about memory. • **Power Supplies**—Use this tab to view information about power supplies. • **Storage**—Use this tab to view information about storage and to configure, modify, and clear RAID configuration. • **PCI Adapters**—Use this tab to view information about PCI adapters.
Sensors	There are six tabs on the page: • **Temperature**—Use this tab to view the temperature sensor. • **Voltage**—Use this tab to view the voltage sensor. • **LEDs**—Use this tab to view the state and color of the LEDs. • **Storage**—Use this tab to view the state of the storage devices.
System Event Log	Use this page to view the system event log.
Remote Presence	There are three tabs on the page: • **Virtual KVM**—Use this tab to set vKVM properties. • **Virtual Media**—Use this tab to set virtual media properties. • **Serial over LAN**—Use this tab to set serial over LAN properties.
BIOS	There are three areas on this page: • **Actions**—Use this area to configure BIOS, configure the server boot order, clear the BIOS CMOS, clear the BIOS password, and activate the backup BIOS. • **Firmware Actions**—Use this area to install the BIOS firmware from a client browser or TFTP server. • **Last Firmware Install**—Use this area to view the status of the last firmware installation. • **BIOS Properties**—Use this area to view the running version of the BIOS. • **Boot Order**—Use this area to view the configured and actual boot order.
Power Policies	Use this page to view power statistics.

Fault Summary	There are two areas on this page: • **Discrete Sensors**—Use this area to view the state of discrete sensors. • **Threshold Sensors**—Use this area to view the state of threshold sensors.
Host Image Mapping	There are three areas on this page: • **Existing Image Info**—Use this area to view information about the installed image. • **Install Pane**—Use this area to download, map, unmap, or delete a host or diagnostic image. • **Host Image Update**—Use this area to view the status of the last image that was mounted on the server and the type of boot device.
Network	There are two tabs on the page: • **Network Settings**—Use this tab to set network properties. • **Network Security**—Use this tab to set up network security.
Communications Services	There are two tabs on the page: • **Communications Services**—Use this area to set HTTP, SSH, and IPMI over LAN properties. • **SNMP**—Use this area to set SNMP properties and SNMP Trap Settings.
Certificate Management	There are two areas on the page: • **Actions**—Use this area to generate and upload a certificate. • **Current Certificate**—Use this area to view the current certificate for the server.
CIMC Log	There are two tabs on the page: • **CIMC Log**—Use this tab to view the CIMC Log. • **Remote Logging**—Use this tab to configure the sending of log messages to remote syslog servers.
Event Management	There is one tab on the page: • **Platform Event Filters**—Use this tab to set up platform event filters.

Firmware Management	There are three areas on this page: • **Actions**—Use this area to install CIMC firmware from a client browser or TFTP server, or to activate installed CIMC firmware. • **CIMC Firmware**—Use this area to view the status of the running, backup, and boot-loader versions of the firmware. • **Last Firmware Install**—Use this area to view information about the last firmware update.
Utilities	There are three areas on this page: • **Actions**—Use this area to export technical support data, export or import the CIMC configuration, reset the CIMC to factory default, and reboot the CIMC. • **Last Technical Support Data Export**—Use this area to view information about the last technical support data export. • **CIMC Configuration Import/Export**—Use this area to view the action type and its status.

Toolbar

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

Element 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.
Help	Launches help.
Info	Displays CIMC information.

CIMC Online Help

The CIMC user interface is divided into two main sections, a **Navigation** pane on the left and a **Work** pane on the right. To access online help for a page, do the following:

- In a particular tab in the user interface, click the **?** icon. The **?** icon is located on the toolbar above the **Work** pane.

- In a dialog box, click the **?** icon in that dialog box.

Logging Out of CIMC GUI

Procedure

Step 1 In the upper right of CIMC, click **Log Out**.
Logging out returns you to the CIMC log in page.

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

CHAPTER 2

Installing the Server Operating System or Hypervisor

This chapter includes the following sections:

Operating System or Hypervisor Installation Methods

E-Series Servers support several operating systems and hypervisors. Regardless of the platform being installed, you can install it on your server using one of the following tools:

- KVM console
- PXE installation server
- Host image mapping

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse 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

You can use the KVM console to install an operating system or hypervisor on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.
- Access the WebBIOS to configure RAID, by pressing the **Ctrl** and **H** keys during bootup.

Installing an Operating System or Hypervisor Using the KVM Console

Before You Begin

- Locate the operating system or hypervisor installation disk or disk image file.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image .

Procedure

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

Step 2 If CIMC is not open, log into the CIMC GUI.

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

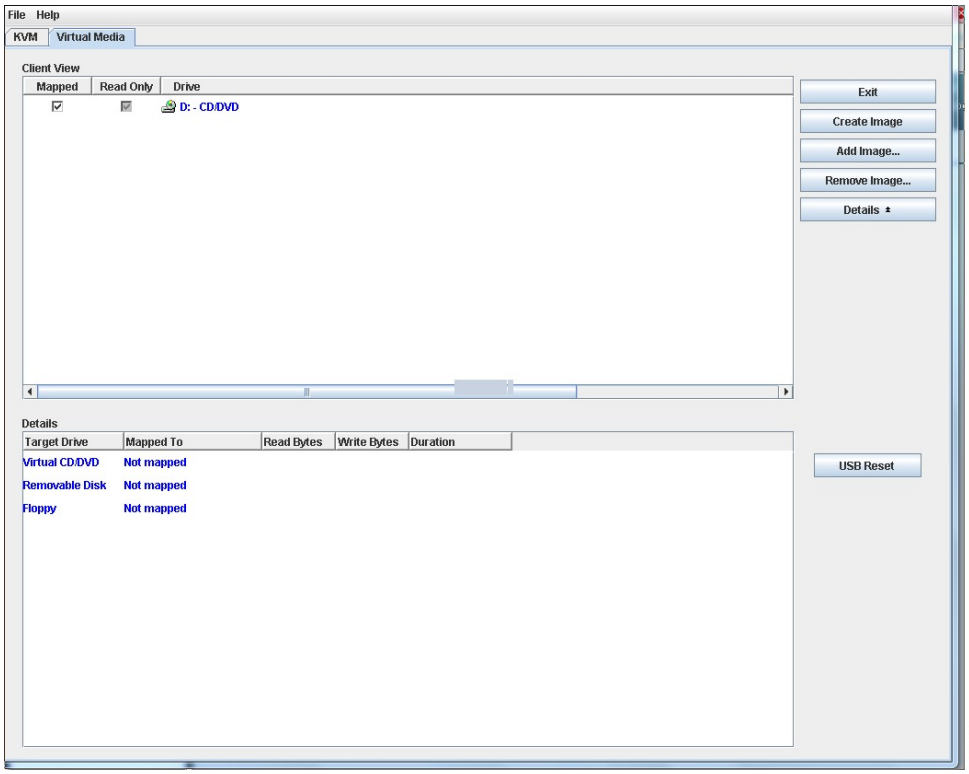
Step 4 On the **Server** tab, click **Summary**.

Step 5 From the **Actions** area, click **Launch KVM Console**.

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

Step 6 From the KVM console, click the **Virtual Media** tab.

Figure 1:



Step 7 In the **Virtual Media** tab, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the CD/DVD drive containing the operating system or hypervisor installation disk.
- Click **Add Image**, navigate to and select the operating system or hypervisor 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 **Virtual Media** tab open during the installation process. Closing the tab unmaps all virtual media.

Step 8 Set the boot order to make the virtual CD/DVD drive as the boot device.
To set the boot order, see Configuring the Server Boot Order.

Step 9 Reboot the server.
When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the installation guide for the platform being installed to guide you through the rest of the installation process.

Step 10 If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See the appropriate operating system or hypervisor documentation for instructions on how to install drivers.

For instructions on how to install drivers on a Microsoft Windows operating system, see Installing Drivers for the Microsoft Windows Server.

What to Do Next

After the installation is complete, reset the virtual media boot order to its original setting.

PXE Installation Servers

A Preboot Execution Environment (PXE) installation server allows a client to boot and install an operating system or hypervisor from a remote location. To use this method, a PXE environment must be configured and available on your LAN, typically a dedicated provisioning LAN. In addition, 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 operating system or hypervisor on the server.

PXE servers can use installation disks, disk images, or scripts to install the operating system or hypervisor. Proprietary disk images can also be used to install the platform, additional components, or applications.

Note PXE installation is an efficient method for installing a platform 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 Operating System or Hypervisor Using a PXE Installation Server

Before You Begin

- Verify that the server can be reached over a VLAN.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image .

Procedure

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

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 operating system or hypervisor being installed to guide you through the rest of the installation process.

What to Do Next

After the installation is complete, reset the LAN boot order to its original setting.

Host Image Mapping

The Host Image Mapping feature allows you to download, map, unmap, or delete a host image. Download a host image, such as a Microsoft Windows, Linux, or VMware from a remote FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository, then map the image onto the virtual drive of a USB controller in the E-Series Server. After you map the image, set the boot order to make the virtual drive, in which the image is mounted, as the first boot device, and then reboot the server. The host image must have .iso as the file extension.

The Host Image Mapping feature also allows you to download and mount a diagnostics image. The diagnostics image must have .diag as the file extension.

Mapping the Host Image

Before You Begin

- Log into CIMC as a user with admin privileges.
- Obtain the host image file from the appropriate third-party.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image .

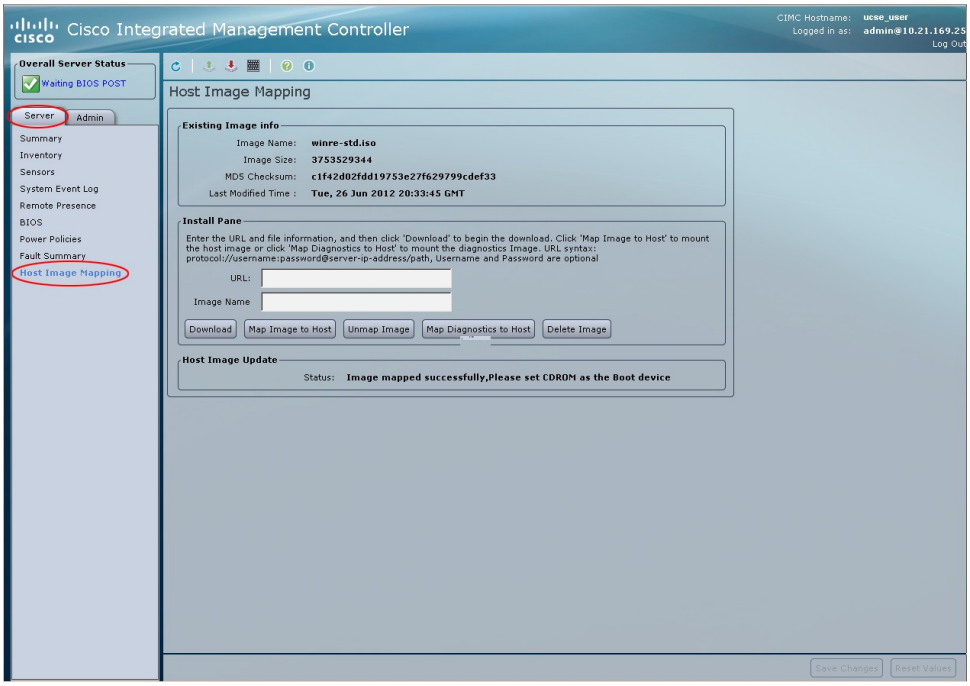
Note If you start an image update while an update is already in process, both updates will fail.

Procedure

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

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 2: Host Image Mapping



Step 3 In the **Install Pane**, complete the following fields:

Name	Description
URL field	The URL of the remote server on which the image is located. If the remote server requires user authentication, you must add the username and password of the remote server in the URL. The remote server can be an FTP, FTPS, HTTP, or HTTPS server. The URL syntax must be: *protocol://username:password@server-ip-address/path/filename*
Image Name field	The name of the image. • If you are installing a host image, that image must have .iso as the file extension. • If you are installing a diagnostics image, that image must have .diag as the file extension.

Step 4 Click **Download**.
The image file is downloaded from the specified FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository.

Step 5 Click **Map Image to Host**.
The image is mounted on the virtual drive of a USB controller. The virtual drive can be one of the following:

- HDD—Hard disk drive
- FDD—Floppy disk drive
- CDROM—Bootable CD-ROM

Step 6 Set the boot order to make the virtual drive in which the image is mounted as the first boot device.
To set the boot order, see Configuring the Server Boot Order.

Tip To determine in which virtual drive the image is mounted, see the **Host Image Update** area in the **Host Image Mapping** page.

Step 7 Reboot the server.

Step 8 If the image contains an answer file, the operating system or hypervisor installation is automated and the image is installed. Otherwise, the installation wizard is displayed. Follow the wizard steps to install the image.

Step 9 If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See the appropriate operating system or hypervisor documentation for instructions on how to install drivers. For instructions on how to install drivers on a Microsoft Windows operating system, see Installing Drivers for the Microsoft Windows Server.

What to Do Next

- After the installation is complete, reset the virtual media boot order to its original setting.
- Unmap the host image. See Unmapping the Host Image.

Installing Drivers for the Microsoft Windows Server

Note If you purchased E-Series Server Option 1 (E-Series Server without preinstalled operating system or hypervisor), and you installed your own version of the Microsoft Windows Server, you must install drivers.

Microsoft Windows operating system requires that you install three drivers:

- On-Board Network Drivers for Windows 2008 R2
- LSI Drivers (On-Board Hardware RAID Controller) for Windows 2008 R2
- Intel Drivers for Windows 2008 R2

If you have purchased a 10 Gigabit add-on card, you must also install the 10G PCIe Network Drivers for Windows 2008 R2.

Procedure

Step 1 Download the drivers from Cisco.com. See Obtaining Software from Cisco Systems.

Step 2 Copy the driver files into an USB flash drive.

Step 3 Install your own version of Microsoft Windows Server.
During the installation process, you will be prompted for the LSI Drivers.

Step 4 Plug the USB flash drive into the USB slot in the E-Series Server, and then install the LSI Drivers.

Step 5 After the Microsoft Windows Server installation is complete, install the On-Board Network Drivers (Broadcom) and the Intel Drivers.

Unmapping the Host Image

Before You Begin

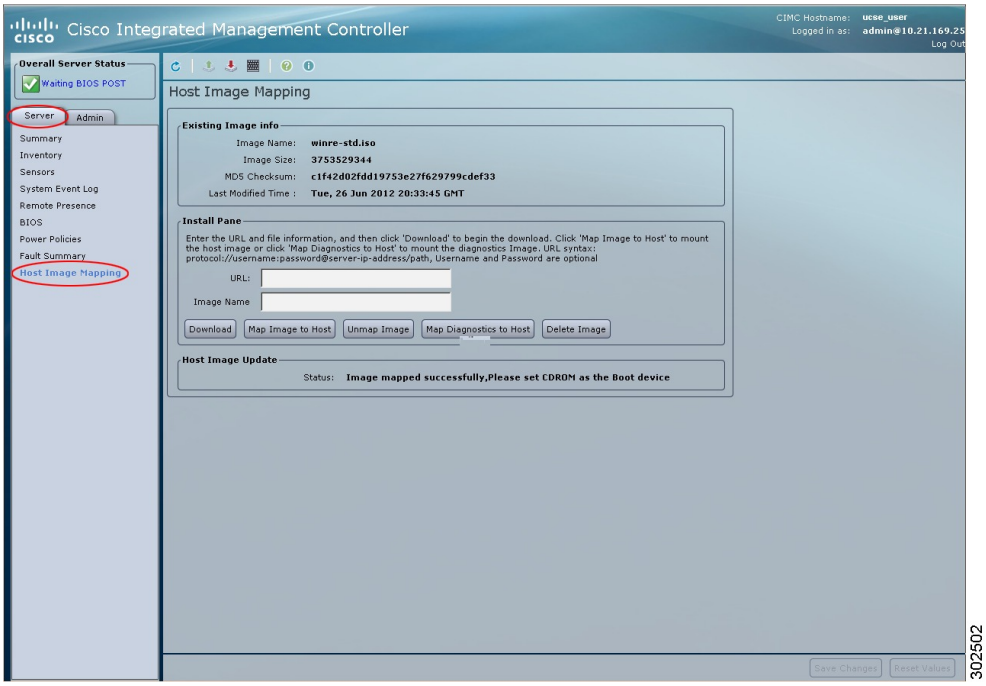
- Log into CIMC as a user with admin privileges.

Procedure

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

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 3: Host Image Mapping



Step 3 Click **Unmap Image**.
The image is unmounted from the virtual drive of the USB controller.

Deleting the Host Image

Before You Begin

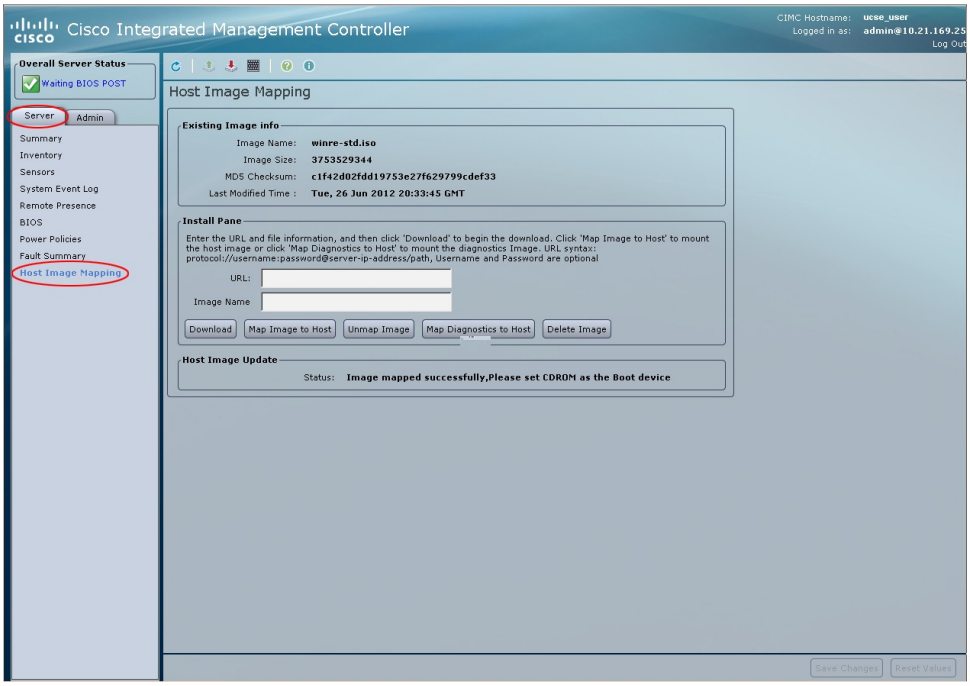
- Log into CIMC as a user with admin privileges.

Procedure

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

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 4: Host Image Mapping



Step 3 Click **Delete Image**.
The image is removed from the SD card.

Note After the image is removed from the SD card, the information that was originally displayed in the **Existing Image Information** area and the **Host Image Update** area is erased.

Downloading the Customized VMware vSphere Hypervisor Image

Use this procedure to download the customized VMware vSpere Hypervisor™ image.

Procedure

Step 1 Navigate to https://my.vmware.com/web/vmware/login.
The VMware login page appears.

Step 2 Enter your VMware credentials, and then click **Log In**.

If you do not have an account with VMware, click **Register** to create a free account.

Step 3 Under the **Support Requests** pane, click **Knowledge Base**.

Step 4 In the **Search** field located on the top right corner, enter **ESXi-5.0.0-623860-custom-Cisco-2.0.1.6.iso**, and then click **Search**.

Step 5 From the **Search Results**, click **Download VMware View 5.1** to download the customized VMware vSpere Hypervisor™ image.

What to Do Next

Install the VMware vSpere Hypervisor™ image. For installation instructions, see Mapping the Host Image.

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 E-Series Server that you are using.

Name	Description
Power State field	The current power state.

Name	Description
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**
Processors field	The overall status of the processors. This can be one of the following: • **Good** • **Fault** Click the link in this field to view more information about the processors.
Memory field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** Click the link in this field to view detailed status information.

Configuring the Server Boot Order Using the CIMC GUI

Before You Begin

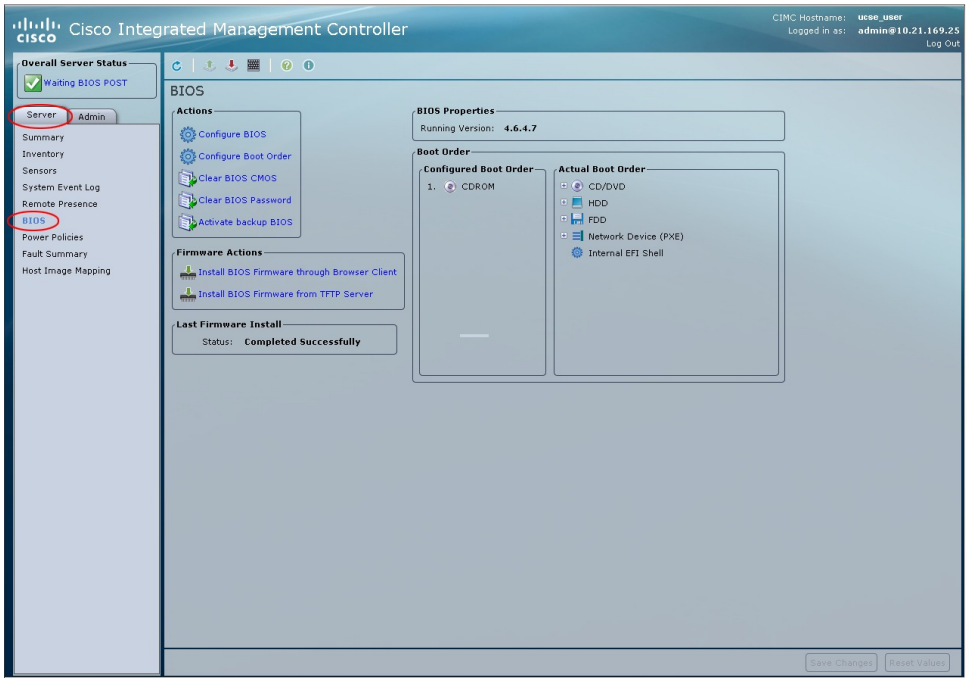
Log into CIMC as a user with admin privileges.

Procedure

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

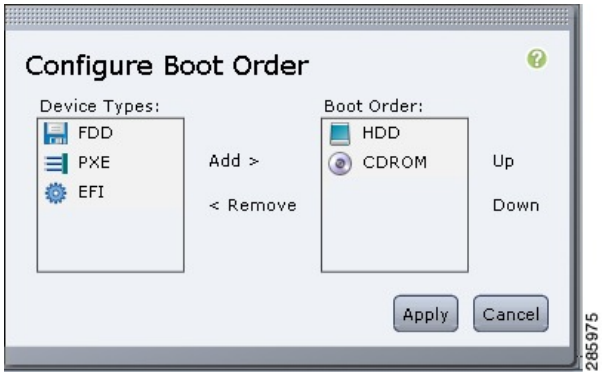
Step 2 On the **Server** tab, click **BIOS**.

Figure 5: BIOS



Step 3 In the **Actions** area, click **Configure Boot Order**.
The **Configure Boot Order** dialog box appears.

Figure 6: Configure Boot Order Dialog Box



Step 4 In the **Configure Boot Order** dialog box, complete the following fields as appropriate:

Name	Description
Device Types table	The server boot options. You can select one or more of the following: • **HDD**—Hard disk drive • **FDD**—Floppy disk drive • **CDROM**—Bootable CD-ROM • **PXE**—PXE boot • **EFI**—Extensible Firmware Interface **Note** You cannot configure second-level boot order from the **Configure Boot Order** dialog box. For example, within the HDD category, you cannot select SD Card or Hard Drive. You can configure second-level boot order from the BIOS setup menu. See Configuring the Boot Order Using the BIOS Setup Menu.
Add >	Moves the selected device type to the **Boot Order** table.
< Remove	Removes the selected device type from the **Boot Order** table.
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot will be attempted.
Up	Moves the selected device type to a higher priority in the **Boot Order** table.
Down	Moves the selected device type to a lower priority in the **Boot Order** table.

Step 5 Click **Apply**.
Additional device types may 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.
- If you want the server to boot from an external bootable device, such as an USB or an external CD ROM drive, which is directly connected to the E-Series Server, you must change the boot order priority. See Configuring the Boot Order Using the BIOS Setup Menu.

Configuring the Boot Order Using the BIOS Setup Menu

Use this procedure if you want the server to boot from an external bootable device, such as an USB or an external CD ROM drive that is directly connected to the E-Series Server.

Procedure

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

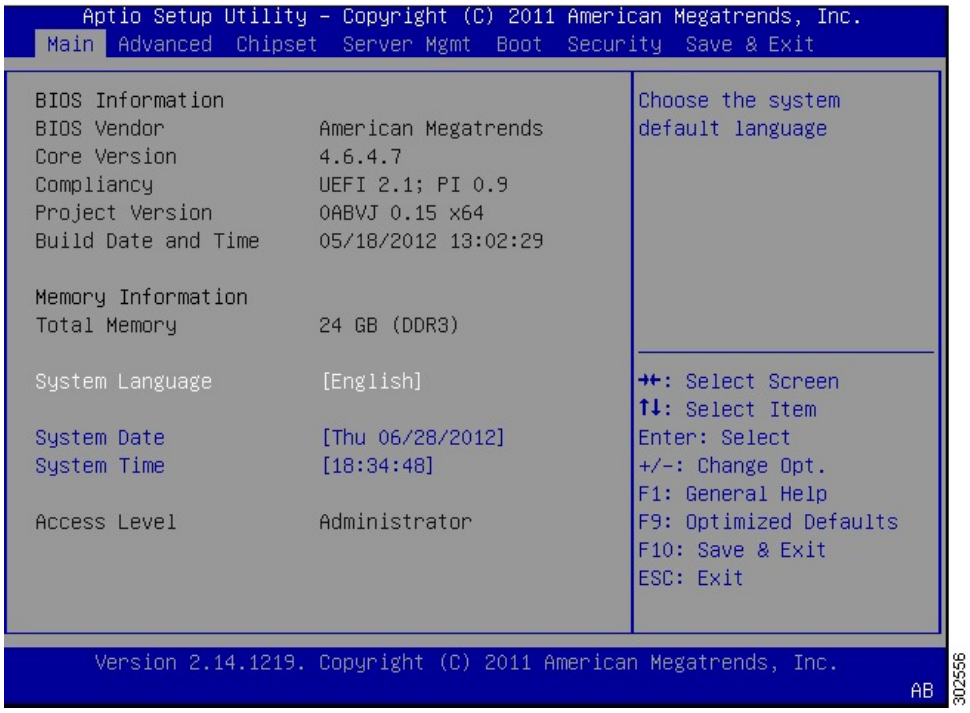
Step 2 On the **Server** tab, click **Summary**.

Step 3 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 4 From the **Server Summary** page, click **Power Cycle Server** to reboot the server.

Step 5 When prompted, press **F2** during bootup to access the BIOS setup menu.
The **Aptio Setup Utility** appears, which provides the BIOS setup menu options.

Figure 7: BIOS Setup Menu



Step 6 Click the **Boot** tab.

Step 7 Scroll down to the bottom of the page below the **Boot Options Priority** area. The following boot option priorities are listed:

- Floppy Drive BBS Priorities
- Network Device BBS Priorities

- Hard Drive BBS Priorities
- CD/DVD ROM Drive BBS Priorities

Step 8 Use the **Up** or **Down arrow keys** on your keyboard to highlight the appropriate option.

Step 9 Press **Enter** to select the highlighted field.

Step 10 Choose the appropriate device as Boot Option 1.

Step 11 Press **F4** to save changes and exit.
The **Main** tab of the BIOS setup displays the device that you configured as Boot Option 1.

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.

Note The Citrix XenServer does not gracefully shutdown when you click **Shut Down Server** or when you press the power button on the front panel of the E-Series Server.

Step 4 Click **OK**.

Managing Server Power

Powering On the Server

Note If the server was powered off by any means other than through CIMC, it will not become active immediately when powered on. The server will remain in standby mode until CIMC 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 **Power Off the Server?** appears.

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**.

Managing RAID

RAID Options

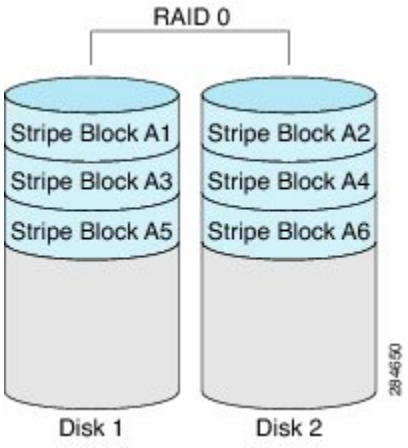
You can choose to store the E-Series Server data files on local Redundant Array of Inexpensive Disks (RAID). The following RAID levels are supported:

- Single-wide E-Series Server supports RAID 0 and RAID 1 levels.
- Double-wide E-Series Server supports RAID 0, RAID 1, and RAID 5 levels.
- Double-wide E-Series Server with PCIe option supports RAID 0 and RAID 1 levels.

RAID 0

With RAID 0, the data is stored evenly in stripe blocks across one or more disk drives without redundancy (mirroring). The data in all of the disk drives is different.

Figure 8: RAID 0



Compared to RAID 1, RAID 0 provides additional storage because both disk drives are used to store data. The performance is improved because the read and write operation occurs in parallel within the two disk drives.

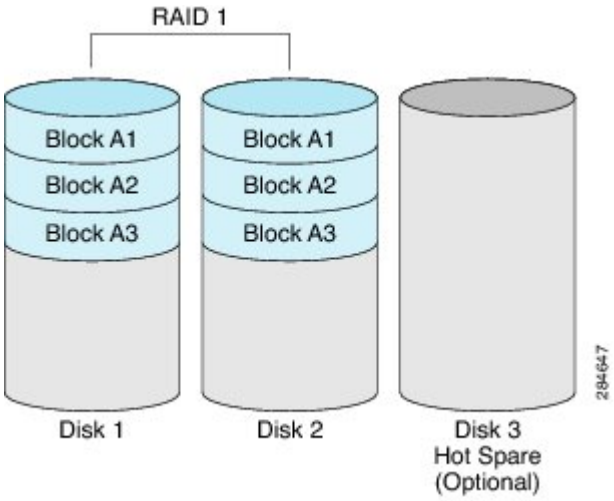
However, there is no fault tolerance, error checking, hot spare, or hot-swapping. If one disk drive fails, the data in the entire array is destroyed. Because there is no error checking or hot-swapping, the array is susceptible to unrecoverable errors.

RAID 1

RAID 1 creates a mirrored set of disk drives, where the data in both the disk drives is identical providing redundancy and high availability. If one disk drive fails, the other disk drive takes over, preserving the data.

RAID 1 also allows you to use a hot spare disk drive. The hot spare drive is always active and is held in readiness as a hot standby drive during a failover.

Figure 9: RAID 1



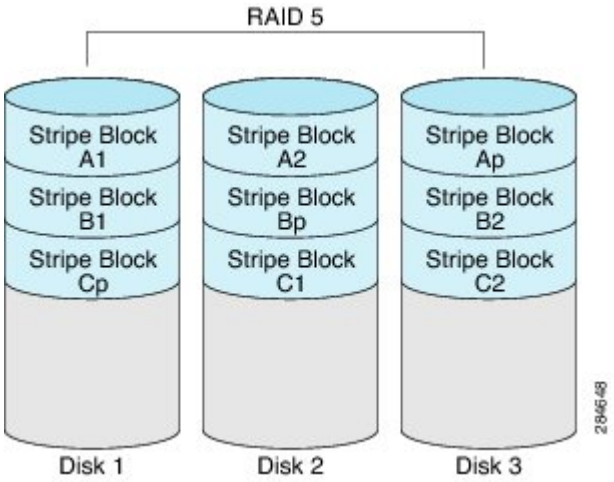
RAID 1 supports fault tolerance and hot-swapping. When one disk drive fails, you can remove the faulty disk drive and replace it with a new disk drive.

However, compared to RAID 0, there is less storage space because only half of the total potential disk space is available for storage and there is an impact on performance.

RAID 5

With RAID 5, the data is stored in stripe blocks with parity data staggered across all disk drives providing redundancy at a low cost.

Figure 10: RAID 5



RAID 5 provides more data storage capacity than RAID 1 and better data protection than RAID 0. It also supports hot swapping; however, RAID 1 offers better performance.

NON-RAID

When the disk drives of a computer are not configured as RAID, the computer is in non-RAID mode. Non-RAID mode is also referred to as Just a Bunch of Disks or Just a Bunch of Drives (JBOD). Non-RAID mode does not support fault tolerance, error checking, hot-swapping, hot spare, or redundancy.

Summary of RAID Options

RAID Options	Description	Advantages	Disadvantages
RAID 0	Data stored evenly in stripe blocks without redundancy	• Better storage • Improved performance	• No error checking • No fault tolerance • No hot-swapping • No redundancy • No hot spare
RAID 1	Mirrored set of disk drives and an optional hot spare disk drive	• High availability • Fault tolerance • Hot spare • Hot-swapping	• Less storage • Performance impact
RAID 5	Data stored in stripe blocks with parity data staggered across all disk drives	• Better storage efficiency than RAID 1 • Better fault tolerance than RAID 0 • Low cost of redundancy • Hot-swapping	• Slow performance
Non-RAID	Disk drives not configured for RAID Also referred to as JBOD	• Portable	• No error checking • No fault tolerance • No hot-swapping • No redundancy • No hot spare

Configuring RAID Using the CIMC GUI

Use this procedure to configure the RAID level, strip size, host access privileges, drive caching, and initialization parameters on a virtual drive. You can also use this procedure to designate the drive as a hot spare drive and to make the drive bootable.

Procedure

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

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

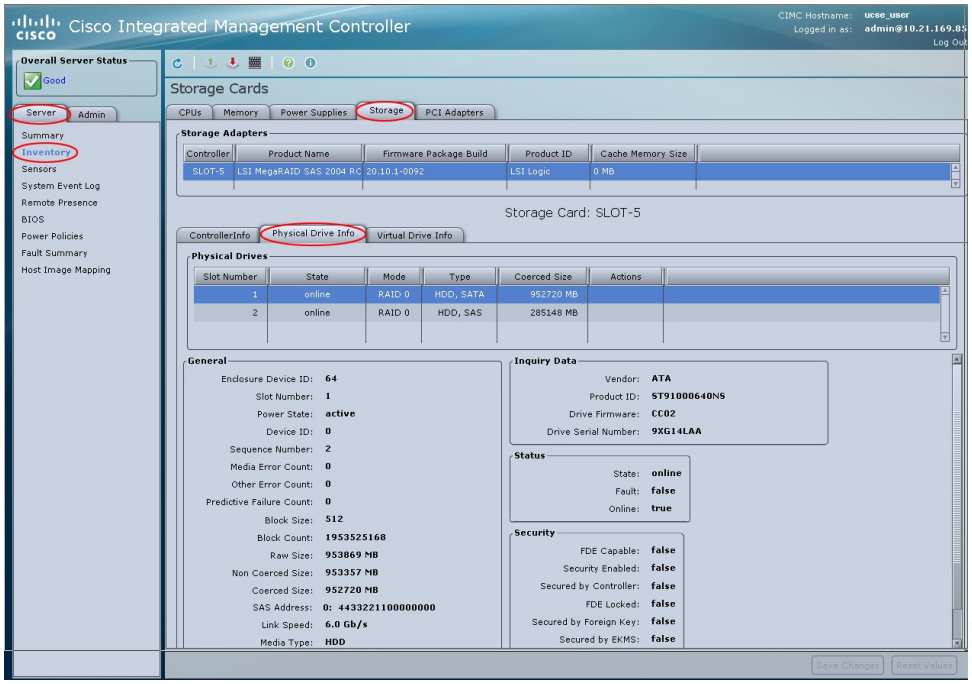
Step 3 In the **Inventory** pane, click the **Storage** tab.

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 To configure RAID, make sure that the status of each of the physical drives that you want to configure as RAID is **unconfigured good**. To change the physical drive status, do the following:

a) In the tabbed menu of the **Storage Card** area, click the **Physical Drive Info** tab.

Figure 11: Physical Drive Info Tab

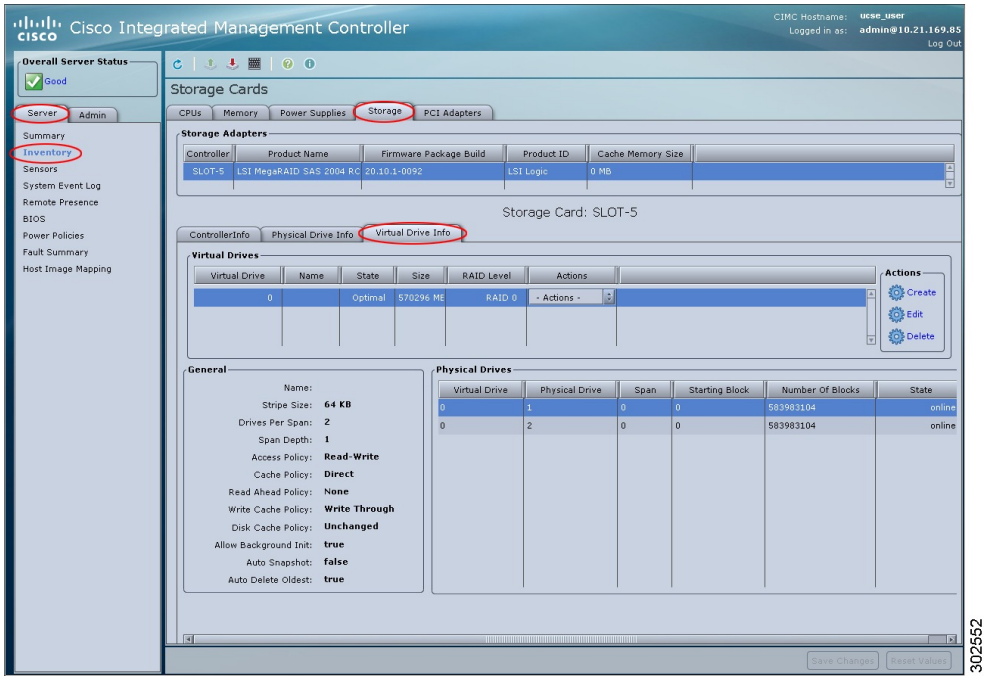


b) From the **Actions** column in the **Physical Drives** pane, choose **Set State** from the drop-down list.
The **Change Physical Drive State** dialog box appears.

c) From the **Change Physical Drive State to** drop-down list, choose **unconfigured good**, and then click **Confirm**.

Step 6 In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 12: Virtual Drive Info Tab



Step 7 In the **Actions** area of the **Virtual Drive Info** tab, click **Create**.
The **Configure Virtual Drive** dialog box appears. Complete the following fields as appropriate:

Name	Description
RAID Level drop-down list	The RAID level options. This can be one of the following: • **RAID 0**—Block striping. • **RAID 1**—Mirroring. • **RAID 5**—Block striping with parity. **Note** The single-wide E-Series Server supports RAID 0 and RAID 1 levels. The double-wide E-Series Server supports RAID 0, RAID 1, and RAID 5 levels. The double-wide E-Series Server with PCIe option supports RAID 0 and RAID 1 levels.
Unconfigured Drives table	Displays the drives that are unconfigured and available for RAID configuration.
Add >	Moves the selected drives from the **Unconfigured Drives** table to the **Selected Drives** table.

Name	Description
< Remove	Removes the selected drives from the **Selected Drives** table.
Selected Drives table	Displays the drives that are selected for RAID configuration.

Step 8 Click **Next**.
The **Configure RAID Parameters** dialog box appears. Complete the following fields as appropriate:

Name	Description
Strip Size drop-down list	The strip size options. This can be one of the following: • **64 KB** • **32 KB** • **16 KB** • **8 KB** **Caution** The smaller strip sizes have a known problem with VMware vSphere Hypervisor™ installation; therefore, if you are installing the vSphere platform, we recommend that you select the **64 KB** strip size option.
Access Policy drop-down list	Configures host access privileges. This can be one of the following: • **Read-Write**—The host has full access to the drive. • **Read Only**—The host can only read data from the drive. • **Blocked**—The host cannot access the drive.
Drive Cache drop-down list	How the controller handles drive caching. This can be one of the following: • **Unchanged**—The controller uses the caching policy specified on the drive. • **Enable**—Caching is enabled on the drives. • **Disable**—Caching is disabled on the drives.
Initialization drop-down list	How the controller initializes the drives. This can be one of the following: • **Quick**—Controller initializes the drive quickly. • **Full**—Controller does a complete initialization of the new configuration. • **None**—Controller does not initialize the drives.

Name	Description
HSP check-box	Designates the drive as a hot spare drive. **Note** Applicable for RAID 1 only.
Set Bootable check-box	How the controller boots the drive. This can be one of the following: • **Enable**—Makes this drive bootable. • **Disable**—This drive is not bootable. **Note** If you plan to install an operating system or Hypervisor into the RAID array, we recommend that you check this check-box.

Step 9 Click **Next**.
The **Confirm RAID Configuration** dialog box appears.

Step 10 Review the RAID configuration, and then click **Submit** to accept the changes.

Modifying RAID Configuration

Use this procedure to enable or disable auto rebuild on the storage controller, to verify disk drives for consistency, and to reconstruct a virtual drive.

Procedure

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

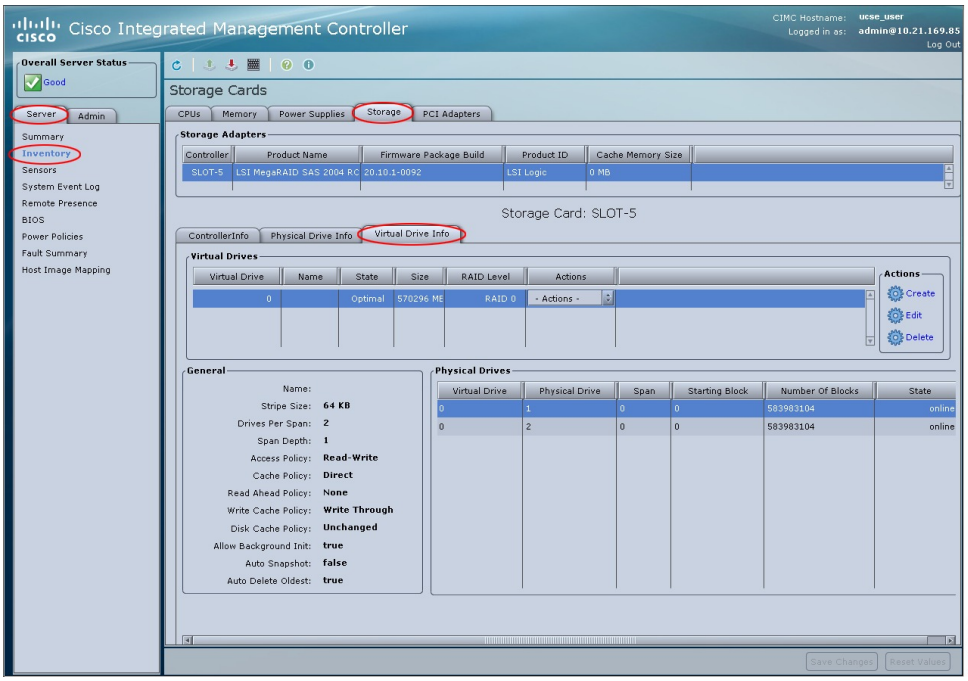
Step 2 On the **Server** tab, click **Inventory**.

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

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 13: Virtual Drive Info Tab



Step 6 In the **Actions** area of the **Virtual Drive Info** tab, click **Edit**.
The **Modify RAID Configuration** dialog box appears. Do the following as appropriate:

Name	Description
Unconfigured Drives table	Displays the drives that are unconfigured and are available for RAID configuration.
Hot Spares table	Displays the drive that is designated as a spare drive. **Note** Applicable for RAID 1 only.
Enable or Disable Auto Rebuild button	Whether the rebuild process starts on the new drive automatically when a virtual drive gets degraded. This can be one of the following: • **Enabled**—If a drive gets degraded and a new drive is plugged in, the rebuild process on the new drive starts automatically. **Note** The rebuild process overwrites all existing data; therefore, make sure that the drive that is plugged in does not contain important data. • **Disabled**—If a drive gets degraded and a new drive is plugged in, the new drive is ignored. You must manually start the rebuild process on the new drive.

Name	Description
Reconstruct Virtual Drive button	Opens the **Reconstruct Virtual Drive** dialog box, which allows you to add or delete physical drives as needed to migrate the virtual drive to the specified new RAID level. **Note** You can retain or increase the size of the virtual drive but you cannot decrease its size. For information about the supported options to migrate the virtual drive to the specified new RAID level, see Reconstructing the Virtual Drive Options.
Cancel button	Closes the dialog box without making any changes.

Reconstructing the Virtual Drive Options

To migrate (reconstruct) the virtual drive to a new RAID level, you must add or remove physical drives. When you add or remove the physical drives, the size of the virtual drive is either retained or increased.

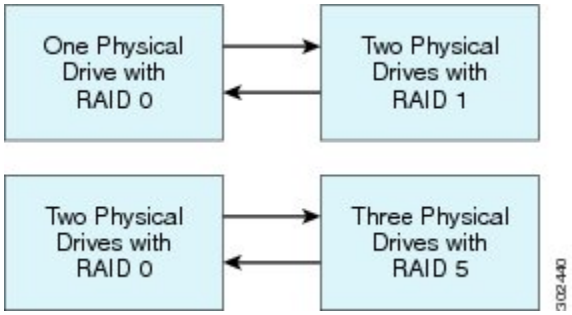
You can retain or increase the size of the virtual drive but you cannot decrease its size. For example, if you have two physical drives with RAID 0, you cannot migrate to RAID 1 with the same number of drives. Because RAID 1 creates a mirrored set of disk drives, the RAID 0 to RAID 1 migration would cause the size of the virtual drive to decrease, which is not supported.

Caution The virtual drive reconstruction process might take several hours to complete. You can continue to use the system during the reconstruction process.

Retaining the Size of the Virtual Drive Options

See the following figure and the table that follows for options that retain the size of the virtual drive when you migrate the virtual drive to a new RAID level.

Figure 14: Retaining the Virtual Drive Size Options



The following table lists the options that retain the size of the virtual drive and provides information about how many physical drives you must add or remove to migrate the virtual drive to a specific RAID level.

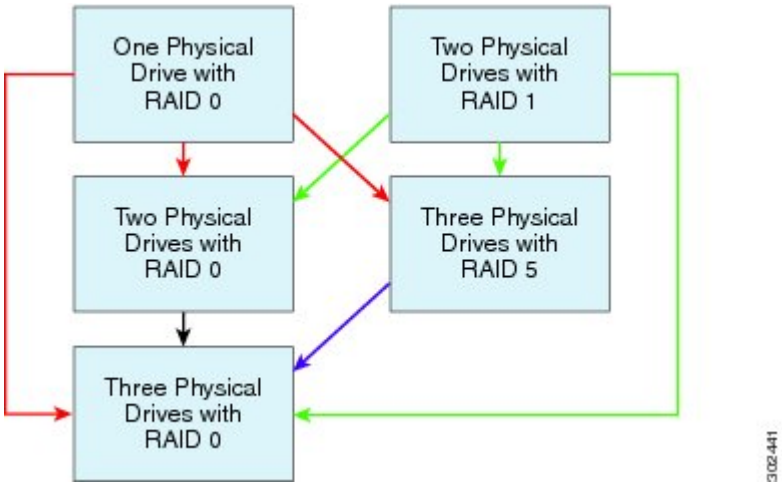
Table 1: Retaining the Virtual Drive Size

From:	Migrate to:	Add or Remove Disks
One physical drive with RAID 0	Two physical drives with RAID 1	Add one disk.
Two physical drives with RAID 1	One physical drive with RAID 0	Remove one disk.
Two physical drives with RAID 0	Three physical drives with RAID 5	Add one disk.
Three physical drives with RAID 5	Two physical drives with RAID 0	Remove one disk.

Increasing the Size of the Virtual Drive Options

See the following figure and the table that follows for options that increase the size of the virtual drive when you migrate the virtual drive to a new RAID level.

Figure 15: Increasing the Virtual Drive Size Options



The following table lists the options that increase the size of the virtual drive and provides information about how many physical drives you must add or remove to migrate the virtual drive to a specific RAID level.

Table 2: Increasing the Virtual Drive Size

From:	Migrate to:	Add or Remove Disks
One physical drive with RAID 0 See the **Red** arrows in the figure.	Two physical drives with RAID 0	Add one disk.
	Three physical drives with RAID 5	Add two disks.
	Three physical drives with RAID 0	Add two disks.

From:	Migrate to:	Add or Remove Disks
Two physical drives with RAID 1 See the **Green** arrows in the figure.	Two physical drives with RAID 0	—
	Three physical drives with RAID 5	Add one disk.
	Three physical drives with RAID 0	Add one disk.
Two physical drives with RAID 0 See the **Black** arrow in the figure.	Three physical drives with RAID 0	Add one disk.
Three physical drives with RAID 5 See the **Purple** arrow in the figure.	Three physical drives with RAID 0	—

Reconstructing the Virtual Drive

Use this procedure to migrate (reconstruct) the virtual drive to a new RAID level.

Before You Begin

See Reconstructing the Virtual Drive Options.

Procedure

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

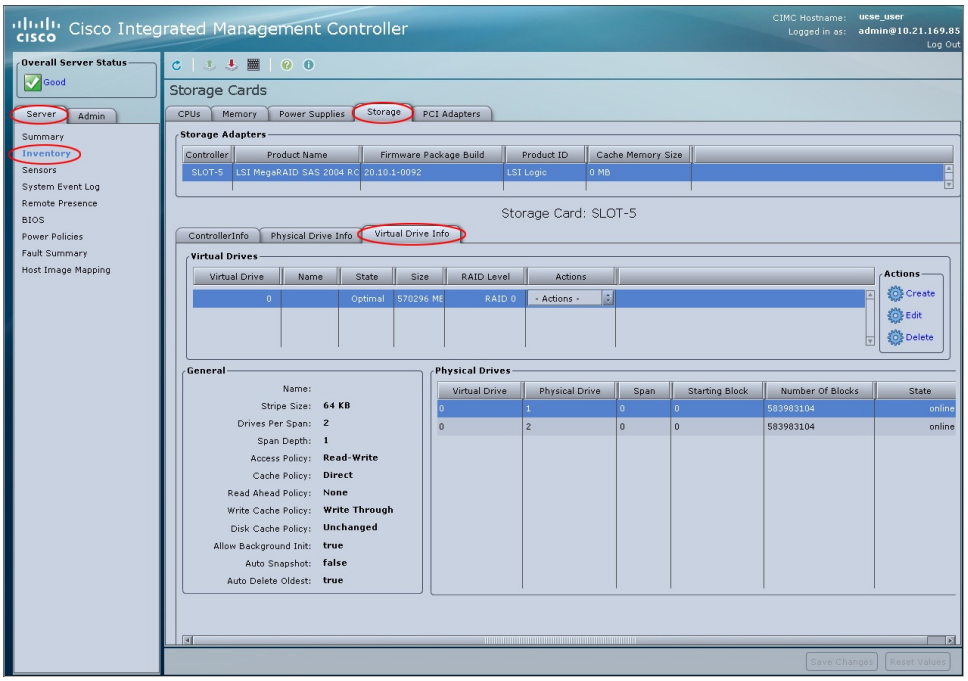
Step 2 On the **Server** tab, click **Inventory**.

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

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 16: Virtual Drive Info Tab



Step 6 In the **Actions** area of the **Virtual Drive Info** tab, click **Edit**.
The **Modify RAID Configuration** dialog box opens.

Step 7 Click the **Reconstruct Virtual Drive** button.
The **Reconstruct Virtual Drive** dialog box appears. Complete the following as appropriate:

Name	Description
Add Drive table	Adds the physical drives to migrate the virtual drive to the specified new RAID level. **Note** To select a single drive, click the drive. To select multiple drives or to unselect a drive, press the **Ctrl** key, and then click the **left mouse** button.
Remove Drive table	Removes the physical drives to migrate the virtual drive to the specified new RAID level. **Note** To select a single drive, click the drive. To select multiple drives or to unselect a drive, press the **Ctrl** key, and then click the **left mouse** button.
Current RAID Level drop-down list	The current RAD level configured on the drives.

Name	Description
New RAID Level drop-down list	The new RAID level to which you want to migrate the drives. Starts the reconstruction process after you click **Confirm**. **Note** You can retain or increase the size of the virtual drive but you cannot decrease its size. See Reconstructing the Virtual Drive Options.
Confirm button	Starts the reconstruction process on the virtual drives.
Cancel button	Closes the dialog box without making any changes.

Deleting RAID Configuration

Use this procedure to clear all RAID or foreign configurations.

Procedure

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

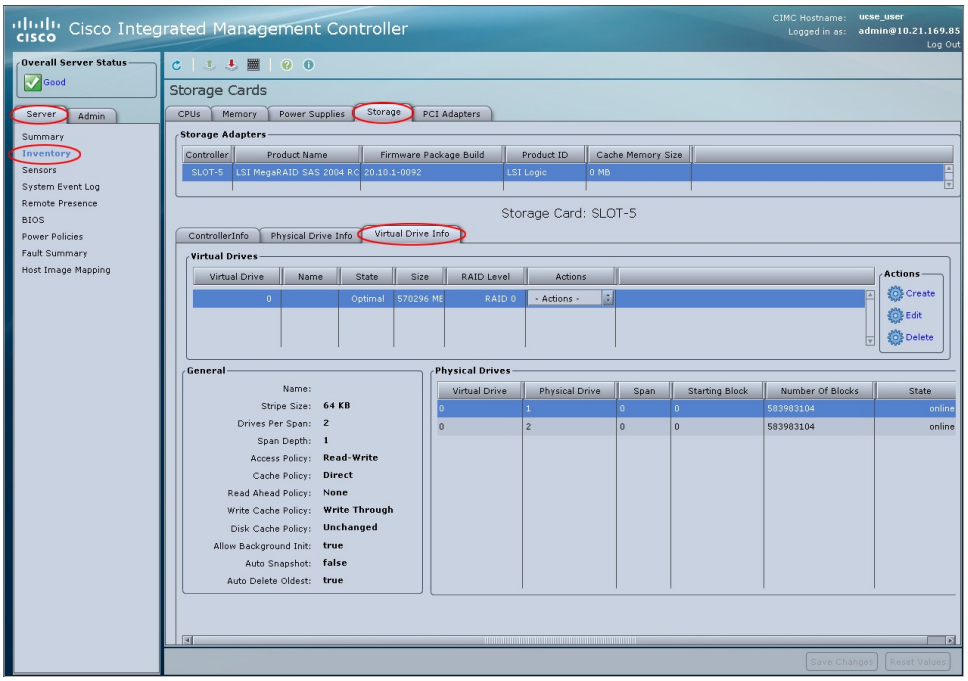
Step 2 On the **Server** tab, click **Inventory**.

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

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 17: Virtual Drive Info Tab



Step 6 In the **Actions** area of the **Virtual Drive Info** tab, click **Delete**.
The **Clear Configurations** dialog box appears. Do the following as appropriate:

Name	Description
Clear All RAID Config radio button	Deletes all RAID configuration. **Caution** When you click this radio button, all existing data in the drives is deleted.
Clear Foreign Config radio button	Deletes all foreign configuration. If you plug-in a drive from another E-Series Server, you must clear its foreign configuration to make it usable. **Note** When you click this radio button, only the configuration in the new plugged-in drive is deleted, while the configuration in the existing drives stay untouched.
Proceed button	Continues with the delete operation.

Changing the Physical Drive State

Use this procedure to change the state of the physical drive. Options are: hotspare, jbod, or unconfigured good.

Procedure

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

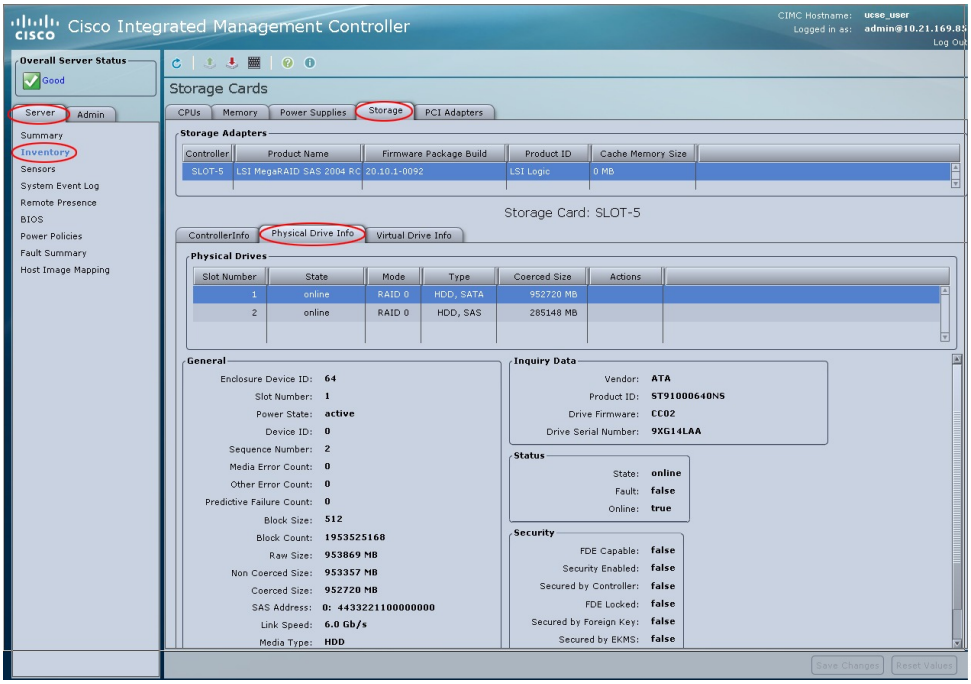
Step 2 On the **Server** tab, click **Inventory**.

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

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Physical Drive Info** tab.

Figure 18: Physical Drive Info Tab



Step 6 From the **Actions** column in the **Physical Drives** pane, choose **Set State** from the drop-down list.
The **Change Physical Drive State** dialog box appears.

Step 7 From the **Change Physical Drive State to** drop-down list, choose one of the following:

- **hotspare**—The drive is designated as a spare drive.
- **jbod**—The drive is not configured as RAID.

- **unconfigured good**—The drive is ready to be assigned to a drive group or hot spare pool.

Step 8 Click **Confirm**.

Enabling Auto Rebuild on the Storage Controller

Use this procedure to rebuild a disk drive automatically. If one of the disk drives that is configured with RAID gets degraded, and a new drive is plugged it, the rebuild process on the new drive starts automatically.

Procedure

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

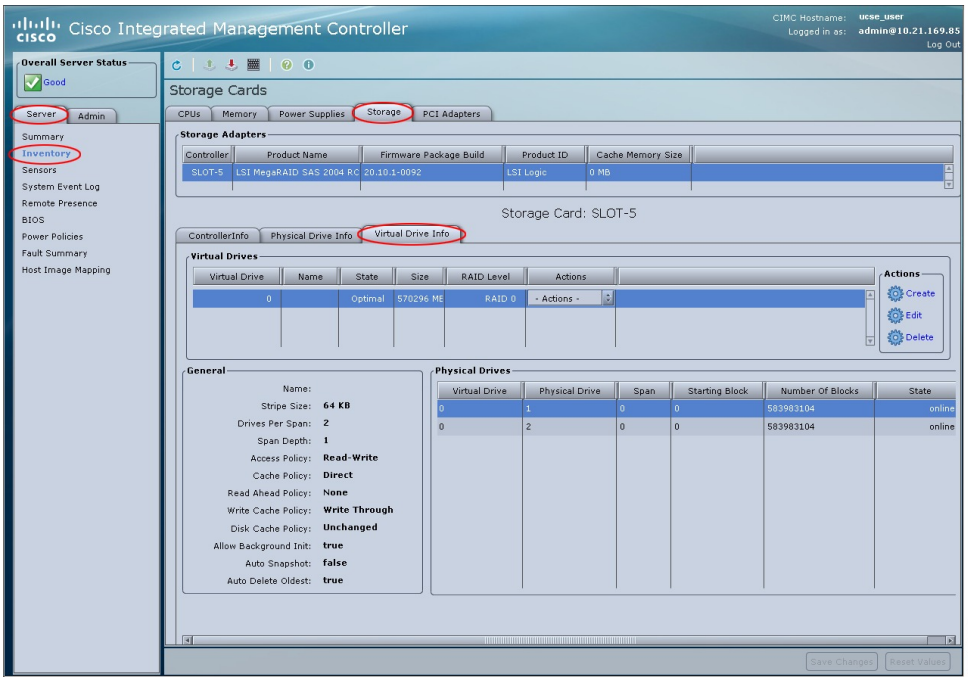
Step 2 On the **Server** tab, click **Inventory**.

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

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 19: Virtual Drive Info Tab



Step 6 In the **Actions** area of the **Virtual Drive Info** tab, click **Edit**.

The **Modify RAID Configuration** dialog box appears.

Step 7 Make sure the **Enable Auto Rebuild** button appears, otherwise, click the **Disable Auto Rebuild** to enable it.

Caution The rebuild process overwrites all existing data; therefore, make sure that the drive that is plugged in does not contain important data.

Rebuilding the Physical Drive

Use this procedure to manually start the rebuild process on the physical drive.

Procedure

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

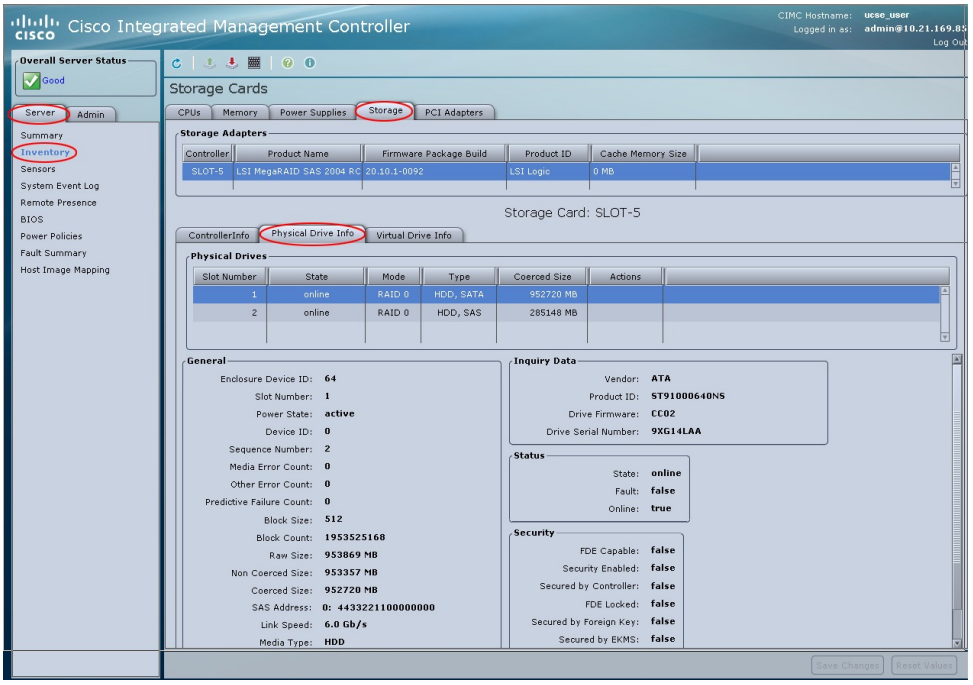
Step 2 On the **Server** tab, click **Inventory**.

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

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 In the tabbed menu of the **Storage Card** area, click the **Physical Drive Info** tab.

Figure 20: Physical Drive Info Tab



Step 6 From the **Actions** column in the **Physical Drives** pane, choose **Rebuild Physical Drive** from the drop-down list.
The **Rebuild Physical Drive** dialog box appears.

Step 7 In the **Rebuild Physical Drive** dialog box, click **Confirm**.

Making the Disk Drive Bootable

When you configure RAID, the RAID configuration wizard has a check box that allows you to make the disk drive bootable. If for some reason you did not check the **Set Bootable** checkbox during the RAID configuration process, you can use this procedure to make the disk drive bootable.

Procedure

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

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

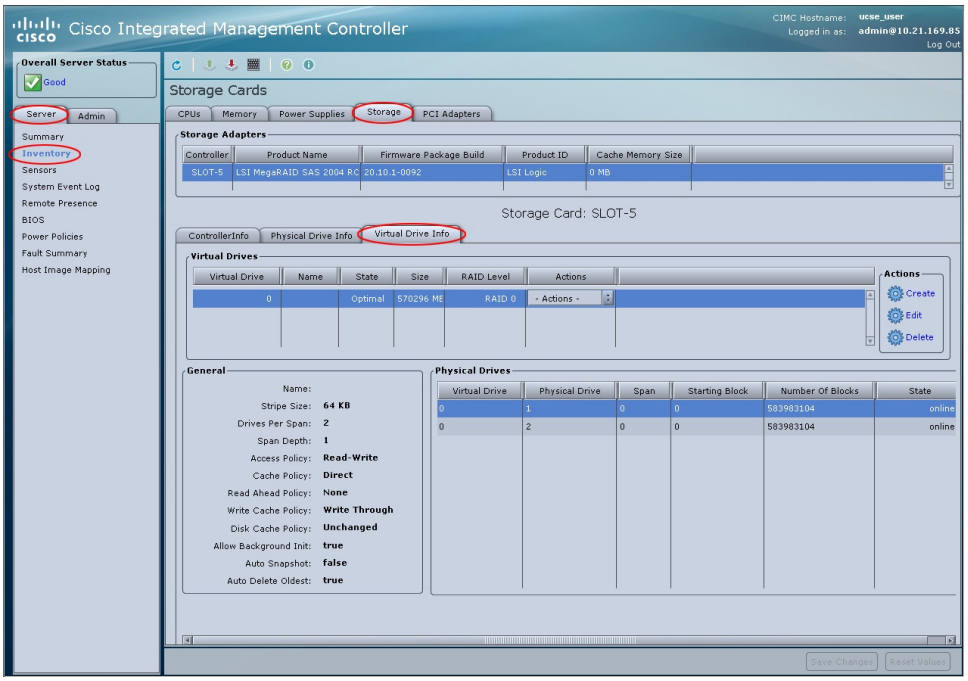
Step 3 In the **Inventory** pane, click the **Storage** tab.

Step 4 In the **Storage Adapters** area, select the storage card.
If the server is powered on, the resources of the selected storage adapter appear in the tabbed menu in the **Storage Card** area.

Step 5 To make a virtual drive bootable, do the following:

a) In the tabbed menu of the **Storage Card** area, click the **Virtual Drive Info** tab.

Figure 21: Virtual Drive Info Tab



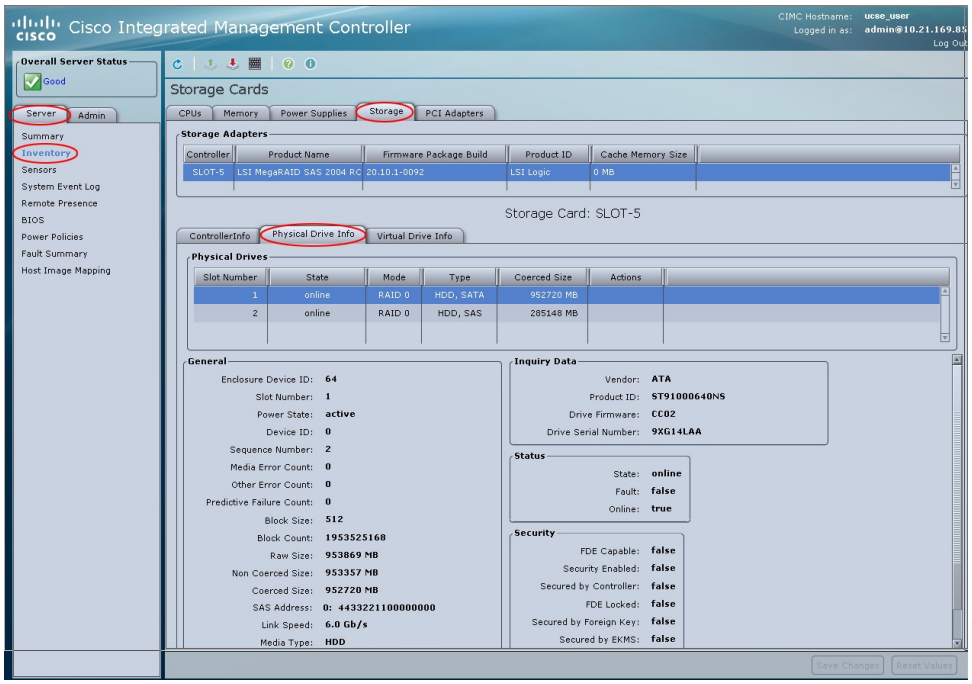
b) From the **Actions** column of the appropriate virtual drive, choose **Set Bootable** from the drop-down list. The **Change Boot Drive** dialog box appears.

c) Click **Confirm** to change the boot drive to this virtual drive.

Step 6 To make a physical drive bootable, do the following:

a) In the tabbed menu of the **Storage Card** area, click the **Physical Drive Info** tab.

Figure 22: Physical Drive Info Tab



b) From the **Actions** column of the appropriate physical drive, choose **Set Bootable** from the drop-down list. The **Change Boot Drive** dialog box appears.

c) Click **Confirm** to change the boot drive to this physical drive.

Note The physical drive must be in non-RAID mode to be bootable.

Step 7 To verify which drive is bootable, click the **Controller Info** tab, and see the **Current Boot Drive** information in the **Settings** area.

Configuring BIOS Settings

Installing BIOS Firmware Through the Browser

Before You Begin

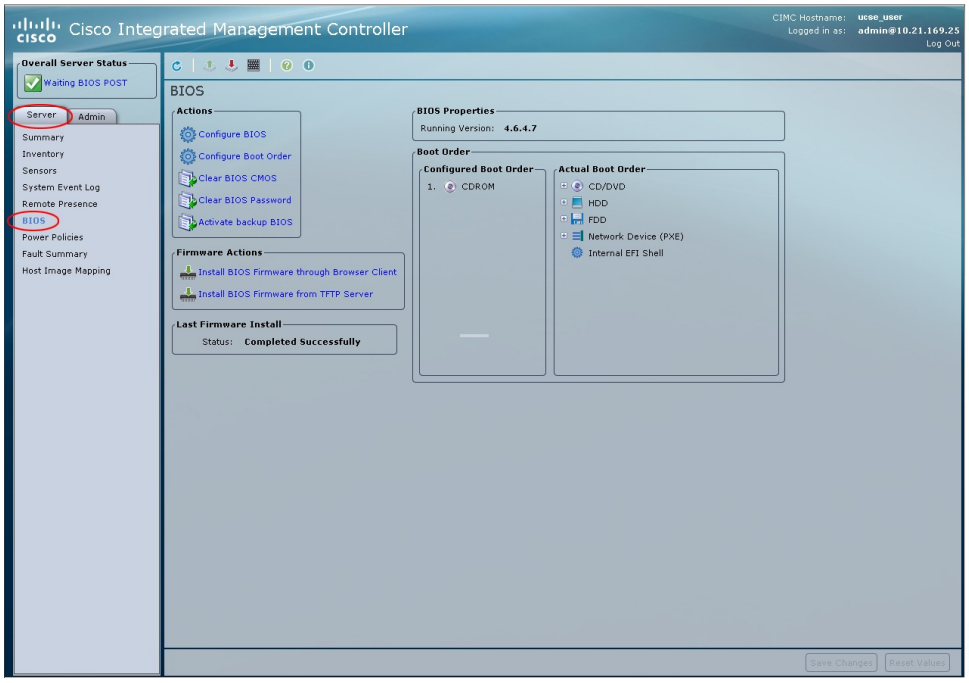
- Log into CIMC as a user with admin privileges.
- Obtain the BIOS firmware file from Cisco Systems. See Obtaining Software from Cisco Systems.
- Unzip the proper upgrade file to your local machine.

Procedure

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

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

Figure 23: BIOS



Step 3 In the **Firmware Actions** area, click **Install BIOS Firmware through Browser Client**.

Step 4 In the **Install BIOS Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the file to install.

Step 5 Click **Install Firmware**.
The BIOS is downloaded, the host is powered off, the BIOS is upgraded, and then the host is powered on.

Installing the BIOS Firmware From a TFTP Server

Before You Begin

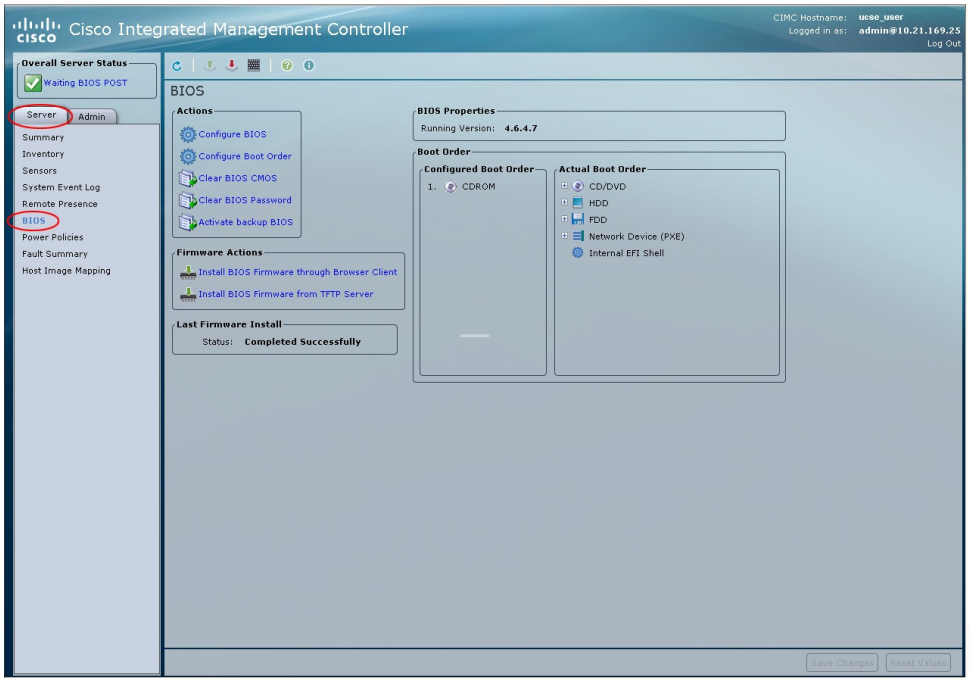
- Log into CIMC as a user with admin privileges.
- Obtain the BIOS firmware file from Cisco Systems. See Obtaining Software from Cisco Systems.
- Unzip the proper upgrade file on your TFTP server.

Procedure

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

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

Figure 24: BIOS



Step 3 In the **Firmware Actions** area, click **Install BIOS Firmware from TFTP Server**.

Step 4 In the **Install BIOS Firmware** dialog box, complete the following fields:

Name	Description
TFTP Server IP Address field	The IP address of the TFTP server on which the firmware image resides.
Image Path and Filename field	The firmware image filename on the server. When you enter this name, include the relative path for the image file from the top of the TFTP tree to the file location.

Step 5 Click **Install Firmware**.
The BIOS is downloaded, the host is powered off, the BIOS is upgraded, and then the host is powered on.

Activating the Backup BIOS

On rare occasions, the BIOS image might get corrupted. To recover from a corrupt BIOS image, activate the backup BIOS to boot the system.

Note The backup BIOS image is factory installed. It cannot be upgraded.

Before You Begin

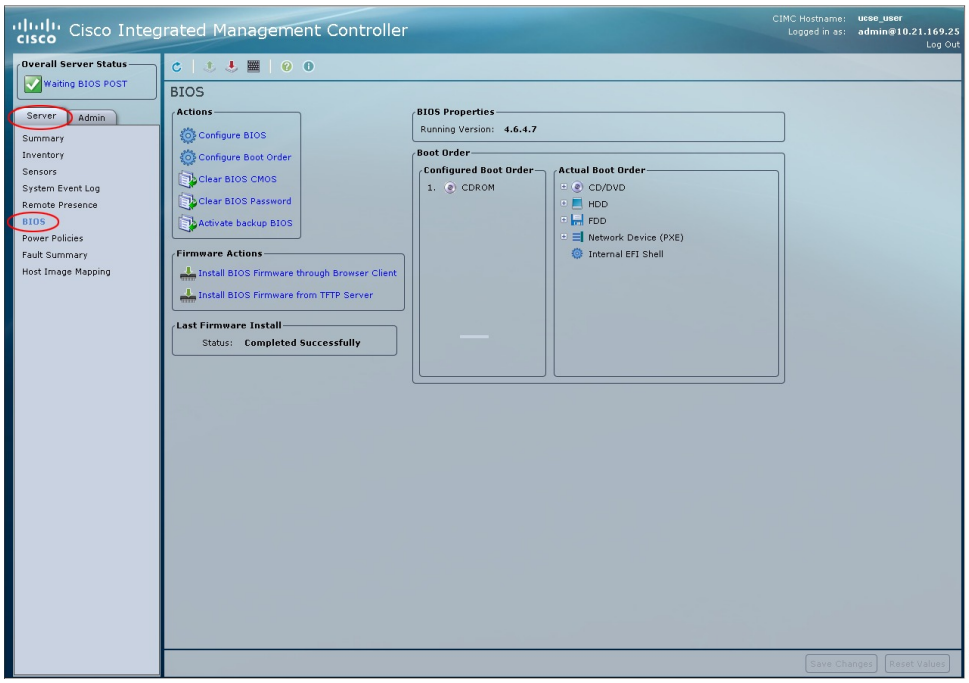
- Log into CIMC as a user with admin privileges.

Procedure

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

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

Figure 25: BIOS



Step 3 In the **Actions** area, click **Activate Backup BIOS**.

Step 4 In the confirmation window, click **OK**.

Configuring Advanced BIOS Settings

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

Before You Begin

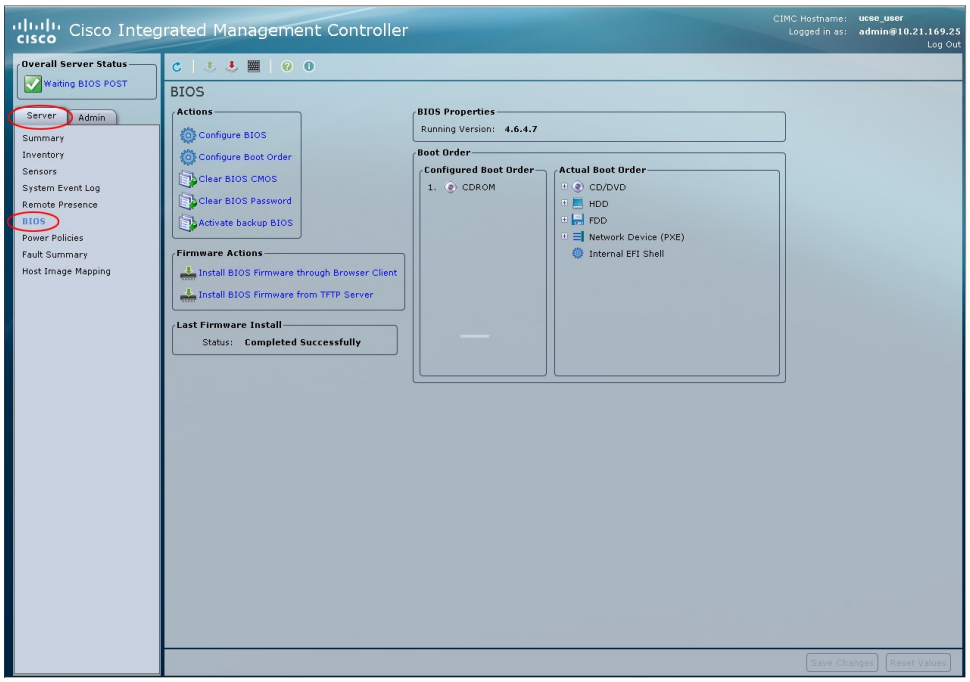
You must log in with admin privileges to perform this task.

Procedure

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

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

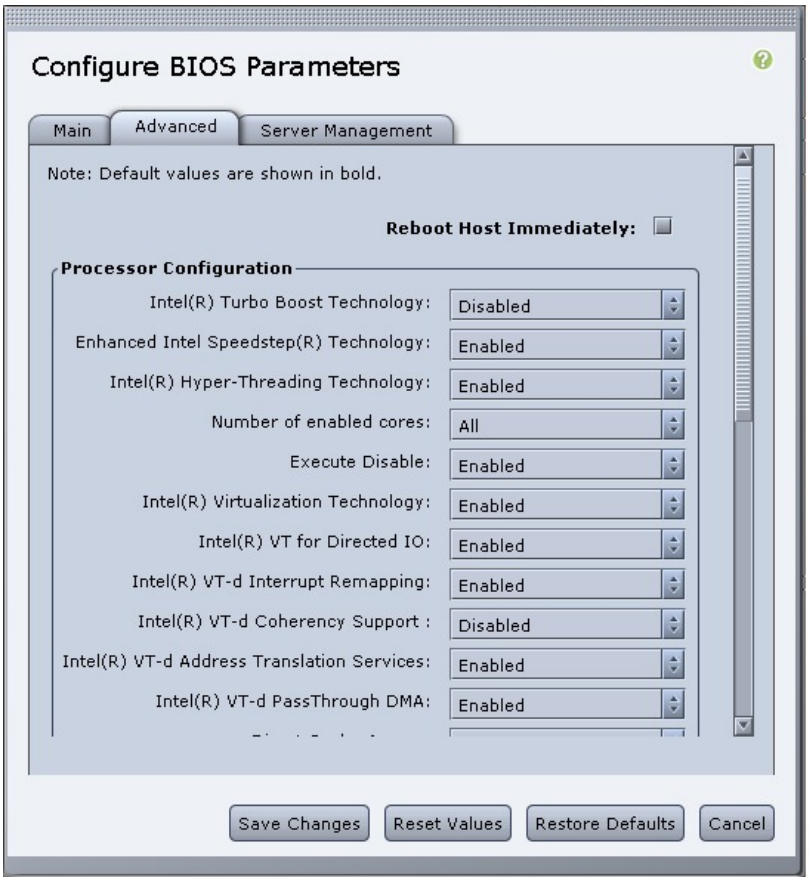
Figure 26: BIOS



Step 3 In the **Actions** area, click **Configure BIOS**.
The **Configure BIOS Parameters** dialog box appears.

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

Figure 27: Advanced Tab



Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Step 6 In the **Advanced** tab, update the BIOS settings fields.
For descriptions and information about the options for each BIOS setting, see the following topics:

- Advanced: Processor BIOS Settings, on page 60
- Advanced: Memory BIOS Settings, on page 65
- Advanced: Serial Port BIOS Settings, on page 65
- Advanced: USB BIOS Settings, on page 66

Step 7 Click **Save Changes**.

Configuring Server Management BIOS Settings

Before You Begin

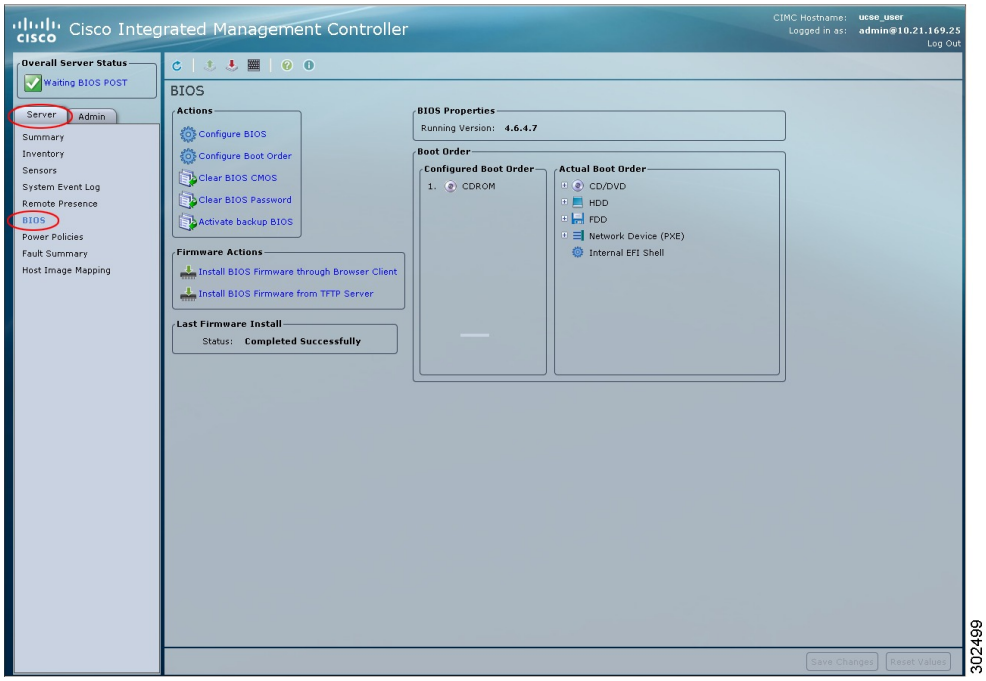
You must log in with admin privileges to perform this task.

Procedure

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

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

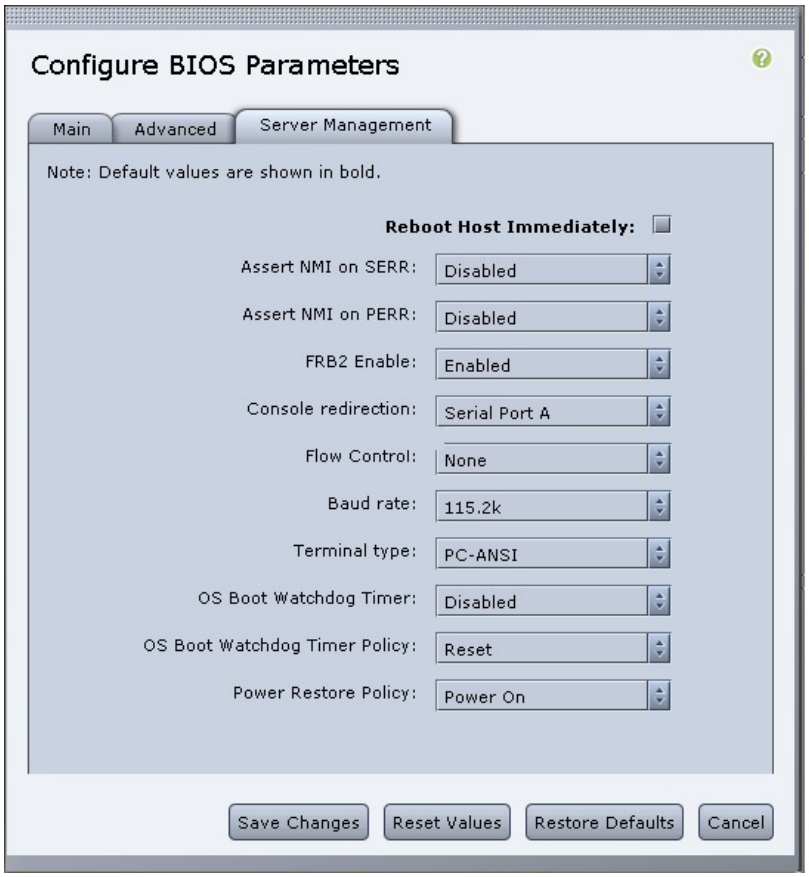
Figure 28: BIOS



Step 3 In the **Actions** area, click **Configure BIOS**.
The **Configure BIOS Parameters** dialog box appears.

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

Figure 29: Server Management Tab



Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Step 6 In the **Server Management** tab, update the BIOS settings fields.
For descriptions and information about the options for each BIOS setting, see the following topic:

- Server Management BIOS Settings, on page 66

Step 7 Click **Save Changes**.

Clearing the BIOS CMOS

Note On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

Before You Begin

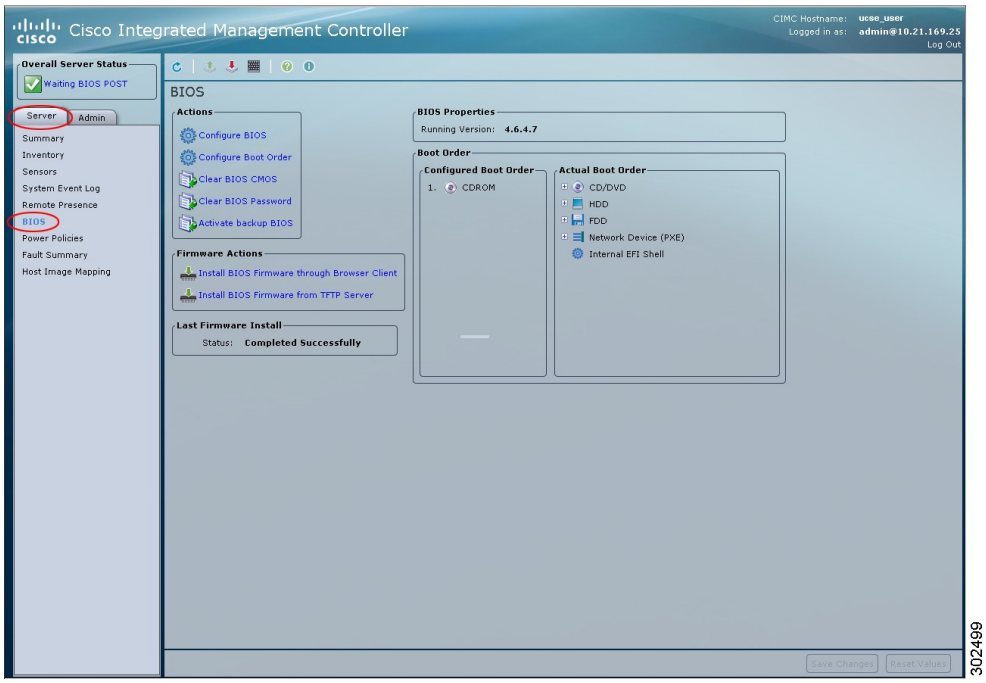
- Log into CIMC as a user with admin privileges.
- Power off the server.

Procedure

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

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

Figure 30: BIOS



Step 3 In the **Actions** area, click **Clear BIOS CMOS**.

Step 4 In the confirmation window, click **OK**.

Clearing the BIOS Password

Before You Begin

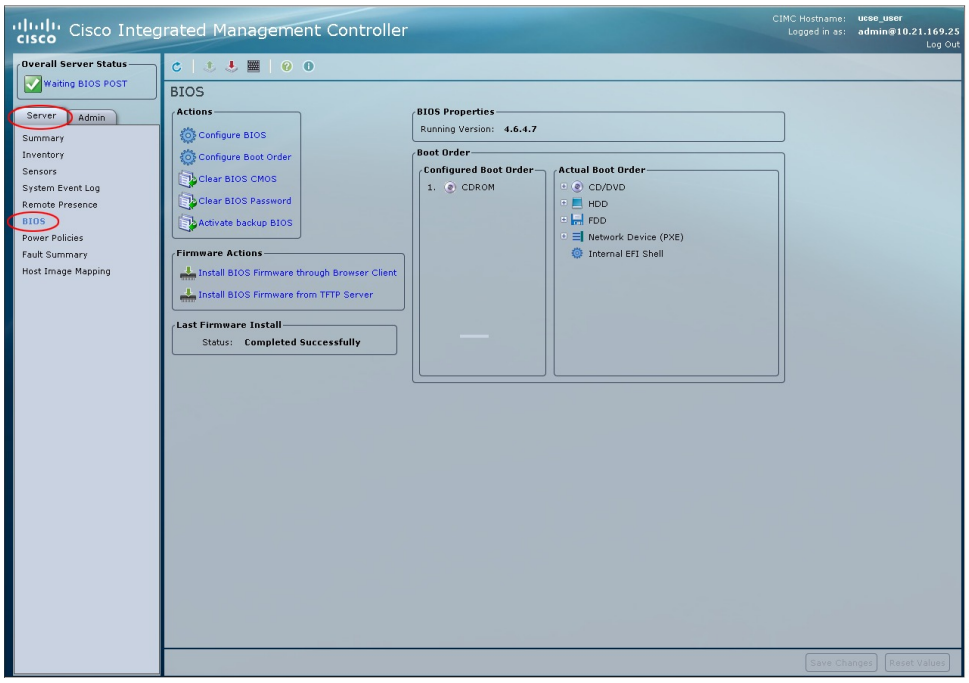
- Log into CIMC as a user with admin privileges.

Procedure

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

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

Figure 31: BIOS



Step 3 In the **Actions** area, click **Clear BIOS Password**.

Step 4 In the confirmation window, click **OK**.

What to Do Next

Reboot the server for the clear password operation to take effect. You are prompted to create a new password when the server reboots.

Server BIOS Settings

The tables in the following sections list the server BIOS settings that you can view and configure.

Note We recommend that you verify the support for BIOS settings in your server. Depending on your installed hardware, some settings may not be supported.

Main BIOS Settings

Name	Description
Reboot Host Immediately	If checked, the server is rebooted immediately after you click **Save Changes**. To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Advanced: Processor BIOS Settings

Name	Description
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.
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.

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	Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following: • **All**—Enables multi processing on all logical processor cores. • **1** through *n*—Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. 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 Virtualization Technology	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 for Directed IO	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 Interrupt Remapping	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled**—The processor does not support remapping. • **Enabled**—The processor uses VT-d Interrupt Remapping as required.
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 Address Translation Services	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.
Intel VT-d PassThrough DMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled**—The processor does not support pass-through DMA. • **Enabled**—The processor uses VT-d Pass-through DMA as required.

Name	Description
Direct Cache Access	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.
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C3 report. • **ACPI C2**—The processor sends the C3 report using the ACPI C2 format. • **ACPI C3**—The processor sends the C3 report using the ACPI C3 format.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C6 report. • **Enabled**—The processor sends the C6 report.
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. **Note** You must select **Custom** in the **CPU Performance** drop-down list to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.

Name	Description
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • **C0 state**—The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • **C2 state**— System level coordination is in progress resulting in high power consumption. There might be performance issues until the coordination is complete. • **C6 state**—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0 or C2, but there might be performance issues until the server returns to full power. • **C7 state**—When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • **No Limit**—The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.
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 allows you to perform a memory scrub on demand. This can be one of the following: • **Disabled**—The system does not allow you to perform a memory scrub on demand. • **Enabled**—The system allows you to perform a memory scrub on demand. If errors are found, the system attempts to fix them or marks the location as unreadable. This process allows the system to run faster and with fewer data processing errors.

Name	Description
Device Tagging	Whether the system allows you to group devices and interfaces based on a variety of information, including descriptions, addresses, and names. This can be one of the following: • **Disabled**—The system does not allow you to group devices and interfaces. • **Enabled**—The system allows you to group devices and interfaces based on a variety of information, including descriptions, addresses, and names.

Advanced: Memory BIOS Settings

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. • **Sparing**—System reliability is enhanced with a degree of memory redundancy while making more memory available to the operating system than mirroring.

Advanced: Serial Port BIOS Settings

Name	Description
Serial A Enable	Whether serial port A is enabled or disabled. This can be one of the following: • **Disabled**—The serial port is disabled. • **Enabled**—The serial port is enabled.

Advanced: USB BIOS Settings

Name	Description
USB Port 0	Whether the processor uses USB port 0. This can be one of the following: • **Disabled**—The server does not use the USB port 0. • **Enabled**—The processor uses the USB port 0.
USB Port 1	Whether the processor uses USB port 1. This can be one of the following: • **Disabled**—The server does not use the USB port 1. • **Enabled**—The processor uses the USB port 1.

Server Management BIOS Settings

Name	Description
Reboot Host Immediately	If checked, the server is rebooted immediately after you click **Save Changes**. To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **Disabled**—The BIOS does not generate an NMI or log an error when a SERR occurs. • **Enabled**—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert NMI on PERR**.
Assert NMI on PERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **Disabled**—The BIOS does not generate an NMI or log an error when a PERR occurs. • **Enabled**—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert NMI on SERR** to use this setting.

Name	Description
FRB2 Enable	Whether the FRB2 timer is used by CIMC 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.
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. • **Serial Port A**—Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
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. • **RTS-CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Baud Rate	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: • **9.6k**—A 9600 BAUD rate is used. • **19.2k**—A 19200 BAUD rate is used. • **38.4k**—A 38400 BAUD rate is used. • **57.6k**—A 57600 BAUD rate is used. • **115.2k**—A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
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-PLUS**—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.
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. 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 CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Boot Watchdog Timer Policy	The action the system takes when the watchdog timer expires. This can be one of the following: • **Do Nothing**—The state of the server power does not change when 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.
Power Restore Policy	The action the system takes when the AC power is restored. This can be one of the following: • **Power Off**—The server is powered off. • **Power On**—The server is powered on. • **Power Last State**—The server power is restored to its last state.

Common Controls

The buttons described in the following table are available in all **Configure BIOS Parameters** tabs.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the wizard. 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.

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.

Name	Description
BIOS Version field	The version of the BIOS running on the server.
Description field	A user-defined description for the server.

Viewing Router Information

Procedure

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

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

Step 3 In the **Router Information** area of the **Server Summary** tab, view the following information:

Name	Description
Router Model field	The model number of the router.
Serial Number field	The serial number of the router.
Slot Number field	The slot number of the router in which the server is installed.

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.

Name	Description
Status field	The status of the CPU.
Family field	The family to which this CPU belongs.
Speed field	The CPU speed, in megahertz.
Version field	The CPU version.
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.
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.

Name	Description
Memory RAS Possible field	Details about the memory configuration the server supports. This can be one of the following: • **Memory configuration can support mirroring** • **Memory configuration can support sparing** • **Memory configuration can support either mirroring or sparing** • **Memory configuration can support lockstep** • **Memory configuration cannot support RAS**
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, because one half is automatically reserved for mirrored copy. • **Sparing**—The system reserves some memory for use in the event a DIMM fails. If that happens, the server takes the DIMM offline and replaces it with the reserved memory. This option provides less redundancy than mirroring, but it leaves more of the memory available for programs running on the server. • **Lockstep**—The system uses two memory channels at a time and provides a higher level of protection. This option is most reliable, but it reduces the total memory capacity by one-third.

Step 5 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.
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.

Name	Description
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.

Name	Description
Input column	The input into the power supply, in watts.
Max Output column	The maximum output from the power supply, in watts.
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 Storage 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 **Storage** tab.

Step 4 In the **Storage Adapters** area, review the information about the available adapter cards.
This area contains a table listing all RAID controllers on the server that can be managed through CIMC. To view details about a particular storage device, select it in the table and view the information in the tabs below.

If a particular storage device does not appear on this tab, it cannot be managed through CIMC. To view the status of an unsupported device, see the documentation for that device.

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

Step 5 In the **Storage Adapters** area, click a row to view the detailed properties of that adapter.
The properties of the selected storage adapter appear in the tabbed menu below the **Storage Adapters** area.

Step 6 Select the **Controller Info** tab and review the information.
If a MegaRAID controller is selected in the **Storage Adapters** table, this tab shows the following information.

- Firmware versions
- PCI information
- Running firmware image information
- Virtual and physical drive counts
- General settings
- Capabilities
- Hardware configuration
- Error counters

Step 7 Select the **Physical Drive Info** tab and review the information.
This tab shows the following information for the controller selected in the **Storage Adapters** table.

- General drive information
- Identification information
- Drive status
- Security information

Step 8 Select the **Virtual Drive Info** tab and review the information.
This tab shows the following information for the controller selected in the **Storage Adapters** table.

- General drive information
- Physical drive information
- RAID information
- Allows you to create, edit, and clear RAID configuration

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.
Vendor ID column	The adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.

Viewing Power Statistics

Procedure

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

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

Step 3 In the **Power Statistics** area, review the information in the following fields:

Name	Description
Current Consumption field	The power currently being used by the server, in watts.
Maximum Consumption field	The maximum number of watts consumed by the server since the last time it was rebooted.
Minimum Consumption field	The minimum number of watts consumed by the server since the last time it was rebooted.

CHAPTER 5

Viewing Server Sensors

This chapter includes the following sections:

Viewing the Fault Summary

Procedure

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

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

Step 3 In the **Discrete Sensors** area, review the following information:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Critical** • **Non-Recoverable** • **Warning**
Reading column	This can be one of the following: • **absent** • **present**

Step 4 In the **Threshold Sensors** area, review the following information:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Critical** • **Non-Recoverable** • **Warning**
Reading column	The value reported by the sensor.
Units column	The units in which the sensor data is reported.
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. This can be one of the following: • **TEMP_AMB_***X*— Ambient temperature, obtained from sensors located inside the module. • **P1_TEMP_SENS**—Processor core temperature. • **DDR3_P1_***X***0_TMP**—Memory module temperature.
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.
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.
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 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. This can be one of the following: • **LED_HLTH_STATUS**—Overall system health status. • **LED_SYS_ACT**—System activity, indicates if the system is powered on and has finished booting.

Name	Description
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. This can be: **HDD***X*_**PRS**—Indicates the presence or absence of each hard drive.
Status column	A brief description of the status of the storage device.

CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

Managing the Virtual KVM

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse 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

You can use the KVM console to install an operating system or hypervisor on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.
- Access the WebBIOS to configure RAID, by pressing the **Ctrl** and **H** keys during bootup.

Configuring the Virtual KVM

Before You Begin

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

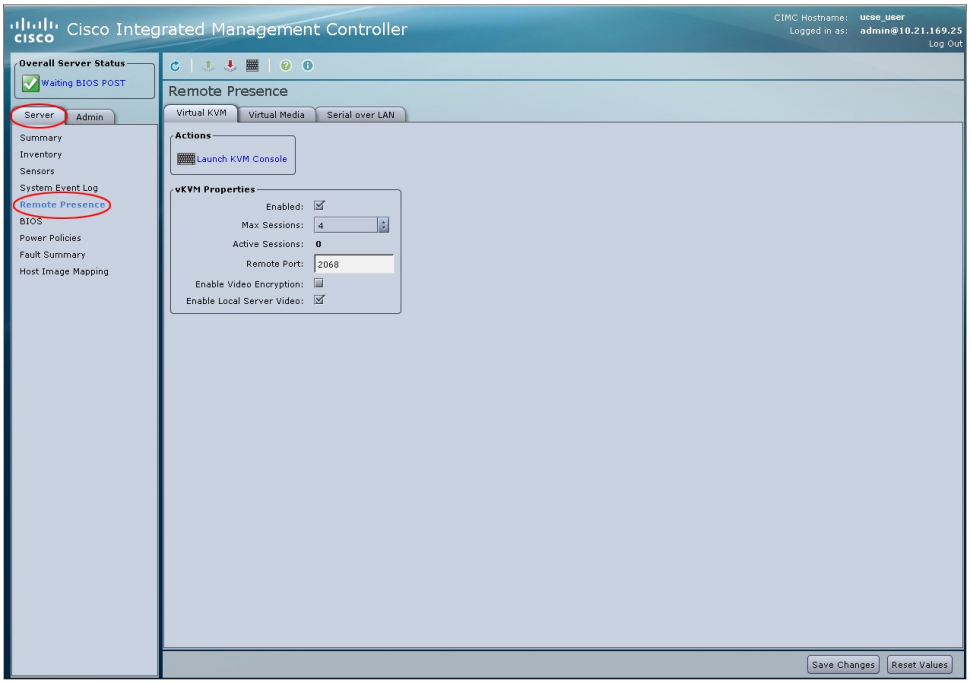
Procedure

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.

Figure 32: Virtual KVM Tab



Step 4 In the **vKVM Properties** area, 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, CIMC 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.

Name	Description
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.

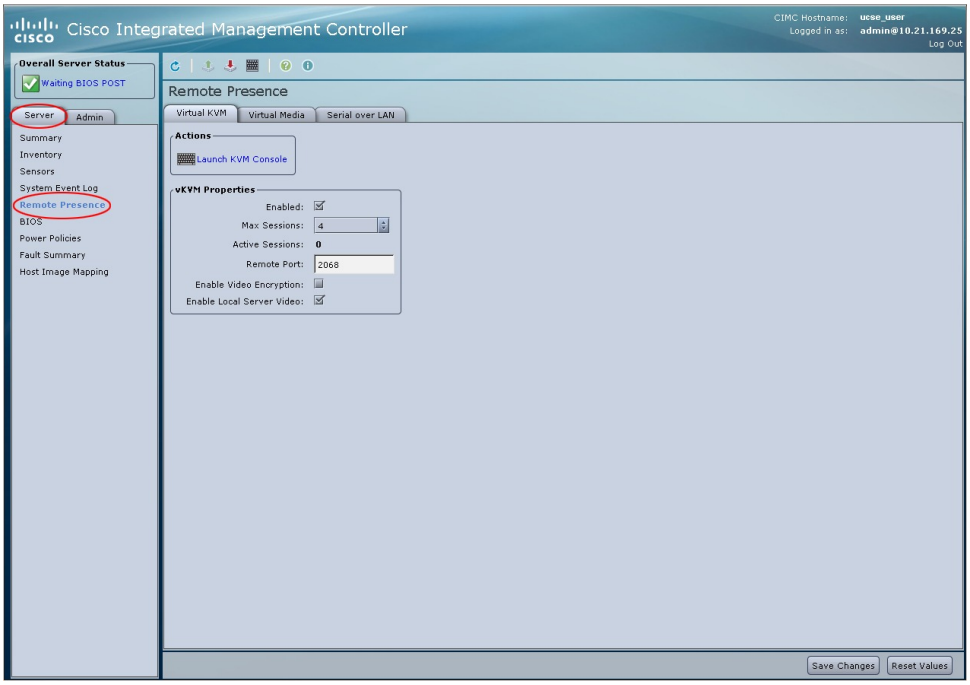
Procedure

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.

Figure 33: Virtual KVM Tab



Step 4 In the **vKVM Properties** area, 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.

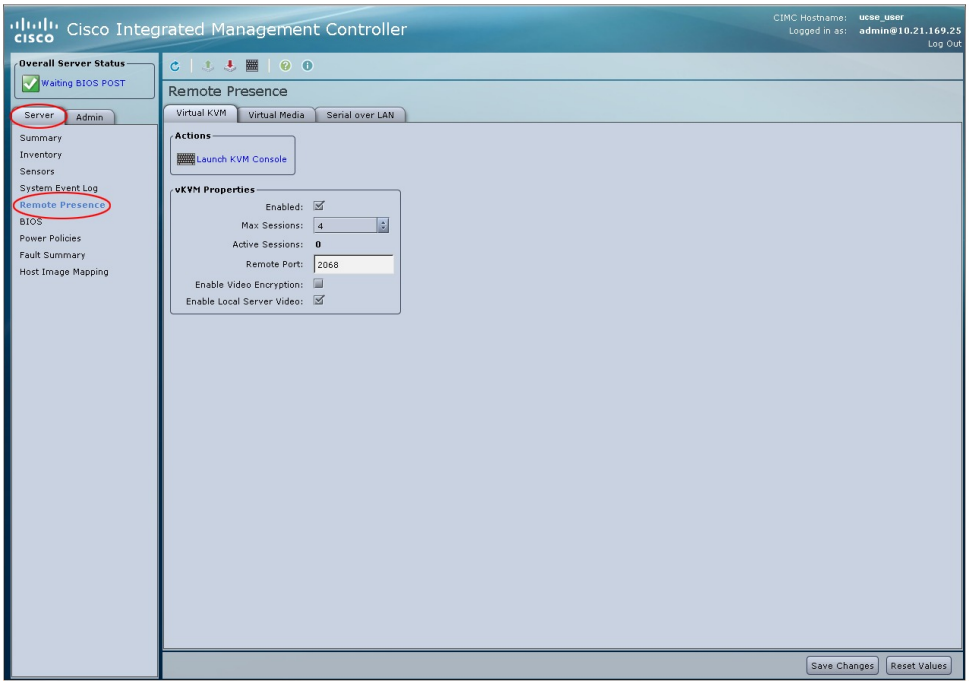
Procedure

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.

Figure 34: Virtual KVM Tab



Step 4 In the **vKVM Properties** area, uncheck the **Enabled** check box.

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.

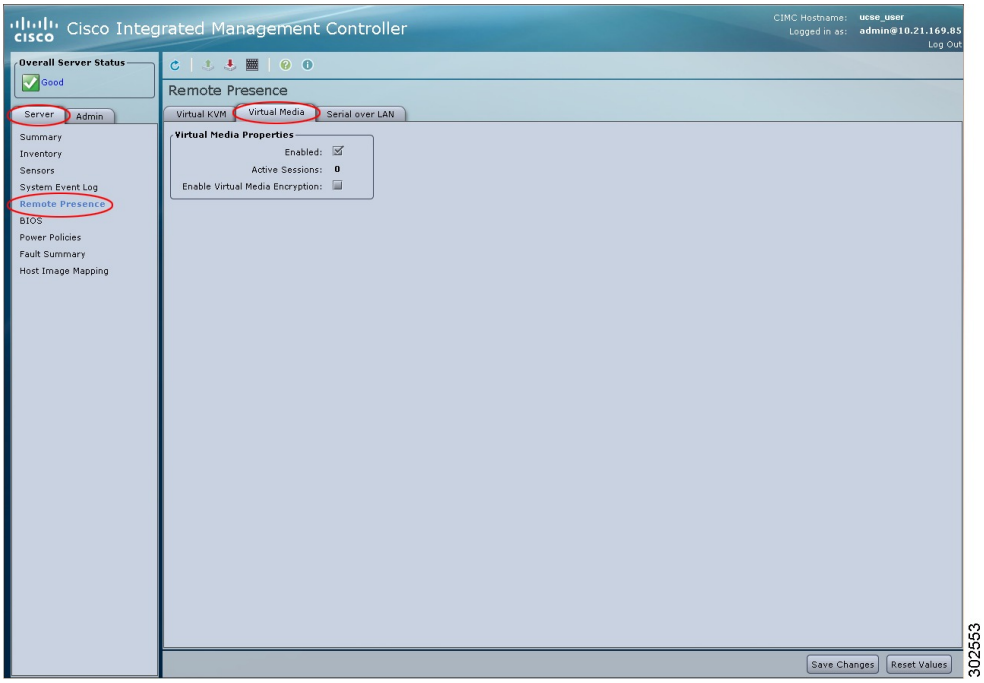
Procedure

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

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

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

Figure 35: 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 currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.

Step 5 Click **Save Changes**.

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 CIMC.

Note Some operating systems, such as Red Hat Enterprise Linux, require extra configuration to redirect the serial console.

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 is enabled on this server.
Baud Rate drop-down list	The baud rate the system uses for Serial over LAN communication. You can select one of the following: • 9600 bps • 19.2 kbps • 38.4 kbps • 57.6 kbps • 115.2 kbps

Step 5 Click **Save Changes**.

CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

Configuring Local Users

Before You Begin

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

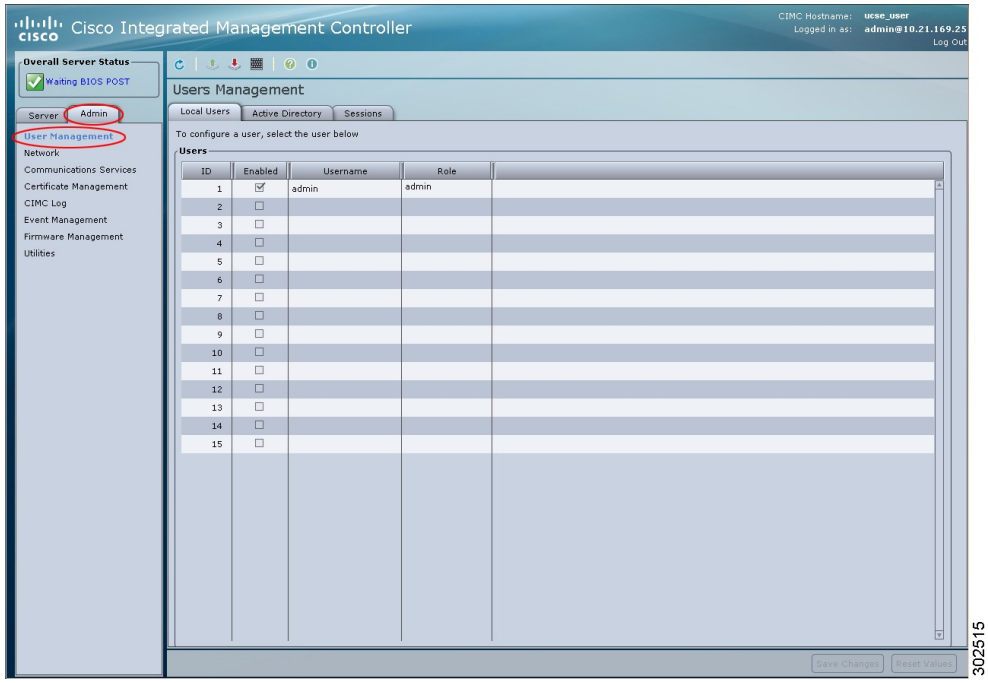
Procedure

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** tab.

Figure 36: Local Users 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 column	The unique identifier for the user.
Enabled check box	If checked, the user is enabled on the CIMC.
Username column	The username for the user.

Name	Description
Role column	The role assigned to the user. This can be one of the following: • **read-only**—This user can view information but cannot make changes. • **user**—This user can: ◦ 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 ◦ Toggle the locator LED • **admin**—This user can perform all actions available through the GUI, CLI, and IPMI.

Step 6 Enter password information.

Step 7 Click **Save Changes**.

Active Directory

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 CIMC utilizes the Kerberos-based authentication service of Active Directory.

When Active Directory is enabled in the CIMC, user authentication and role authorization is performed by Active Directory for user accounts not found in the local user database.

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

Configuring the Active Directory Server

The CIMC can be configured to use Active Directory for user authentication and authorization. To use Active Directory, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can modify the Active Directory 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. For more information about altering the Active Directory schema, see http://technet.microsoft.com/en-us/library/bb727064.aspx.

Use this procedure to create a custom attribute on the Active Directory server.

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

Procedure

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

Step 2 Using the Active Directory 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 Active Directory 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 CIMC:

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 http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to Do Next

Use the CIMC to configure Active Directory.

Configuring Active Directory in CIMC

Before You Begin

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

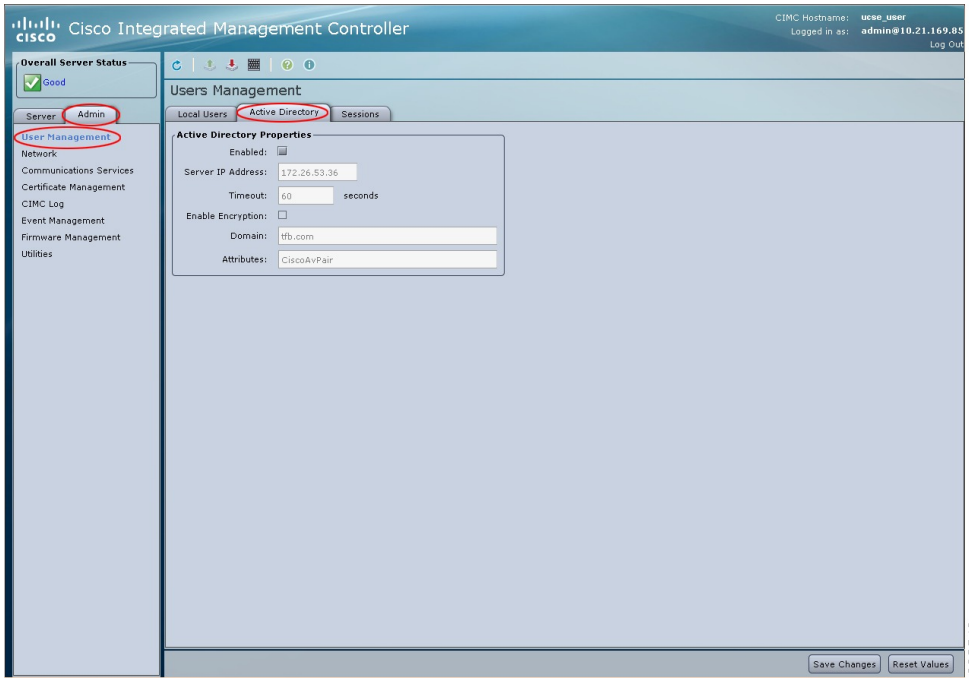
Procedure

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 **Active Directory** tab.

Figure 37: Active Directory Tab



Step 4 In the **Active Directory Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, user authentication and role authorization is performed by Active Directory for user accounts not found in the local user database. If you check this box, CIMC enables the rest of the fields in this section.
Server IP Address field	The Active Directory server IP address.

Name	Description
Timeout field	The number of seconds the CIMC waits until the LDAP search operation times out. If the search operation times out, CIMC tries to connect to the next domain controller or global catalog listed on this tab, if one is available.
Enable Encryption check box	If checked, the server encrypts all information it sends to Active Directory.
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.
Attributes field	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 must have the following attribute ID: 1.3.6.1.4.1.9.287247.1 **Note** If you do not specify this property, user access is restricted to read-only.

Step 5 Click **Save Changes**.

Step 6 To log into the Active Directory server, enter the domain name, back slash (\), and the Active Directory username.
For example, if the domain name is **mydomain.com** and the Active Directory username is **admin**, then the login name would be **mydomain.com\admin**.

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.

Name	Description
Username column	The username for the user.
IP Address column	The IP address from which the user accessed the server.
Type column	The method by which the user accessed the server. For example, CLI, vKVM, and so on.
Action column	If your user account is assigned the **admin** user role, this column displays **Terminate** if you can force the associated user session to end. Otherwise it displays **N/A**. **Note** You cannot terminate your current session from this tab.

CHAPTER 8

Configuring Network-Related Settings

This chapter includes the following sections:

CIMC NIC Configuration

CIMC NICs

Two NIC modes are available for connection to the CIMC.

NIC Mode

The **NIC Mode** drop-down list in the **NIC Properties** area determines which ports can reach the CIMC. The following mode options are available, depending on your platform:

- Dedicated—A connection to the CIMC is available through the management Ethernet port or ports.
- Shared LOM—A connection to the CIMC is available through the LAN On Motherboard (LOM) Ethernet host ports and through the router's PCIe and MGF interfaces.

Note In shared LOM mode, all host ports must belong to the same subnet.

NIC Redundancy

The **NIC Redundancy** drop-down list in the **NIC Properties** area determines how NIC redundancy is handled:

- None—Redundancy is not available.

- Active-Standby—One port fails over to the other.

The available redundancy modes vary depending on the selected network mode and your platform.

Configuring CIMC NICs

Use this procedure 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.

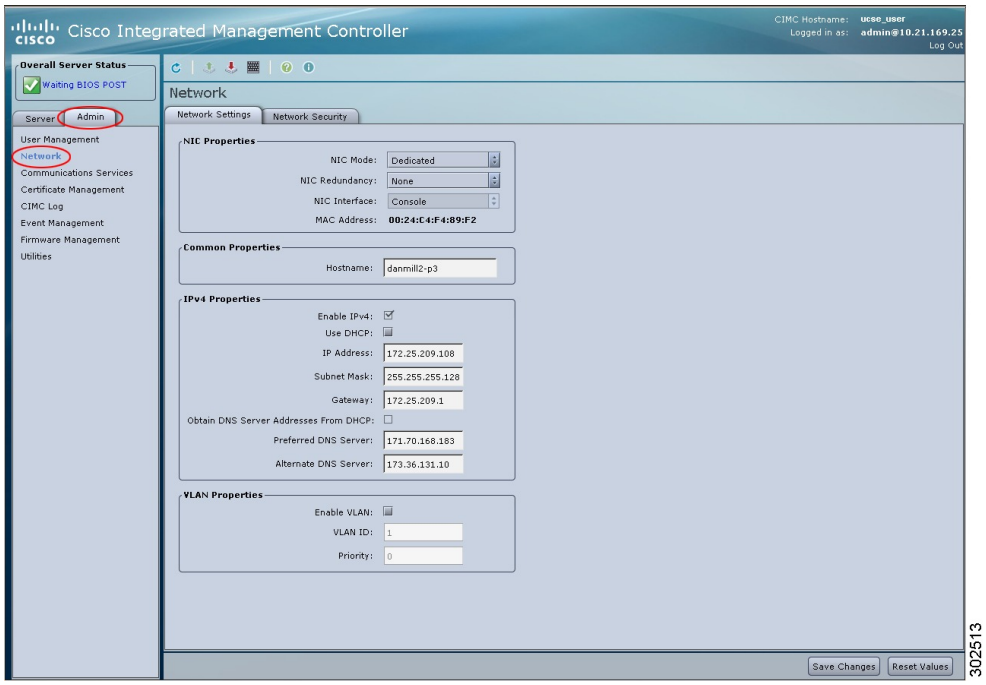
Procedure

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.

Figure 38: Network Settings Tab



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

Name	Description
NIC Mode drop-down list	The NIC mode. This can be one of the following: • **Dedicated**—The management port is used to access the CIMC. • **Shared LOM**—The LOM (LAN On Motherboard) ports are used to access the CIMC.
NIC Redundancy drop-down list	The NIC redundancy options depend on the mode chosen in the **NIC Mode** drop-down list and the model of the server that you are using. If you do not see a particular option, then it is not available for the selected mode or server model. The available options are: • **none**—Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem. • **active-standby**—If a port associated with the configured NIC mode fails, traffic will fail over to one of the other ports associated with the NIC mode. **Note** If you select this option, make sure all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.
NIC Interface field	The interface used by the NIC.
MAC Address field	The MAC address of the CIMC network interface selected in the **NIC Mode** field.

Note The available NIC mode options may vary depending on your platform.

If you select Shared LOM, make sure that all host ports belong to the same subnet.

Step 5 Click **Save Changes**.

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.

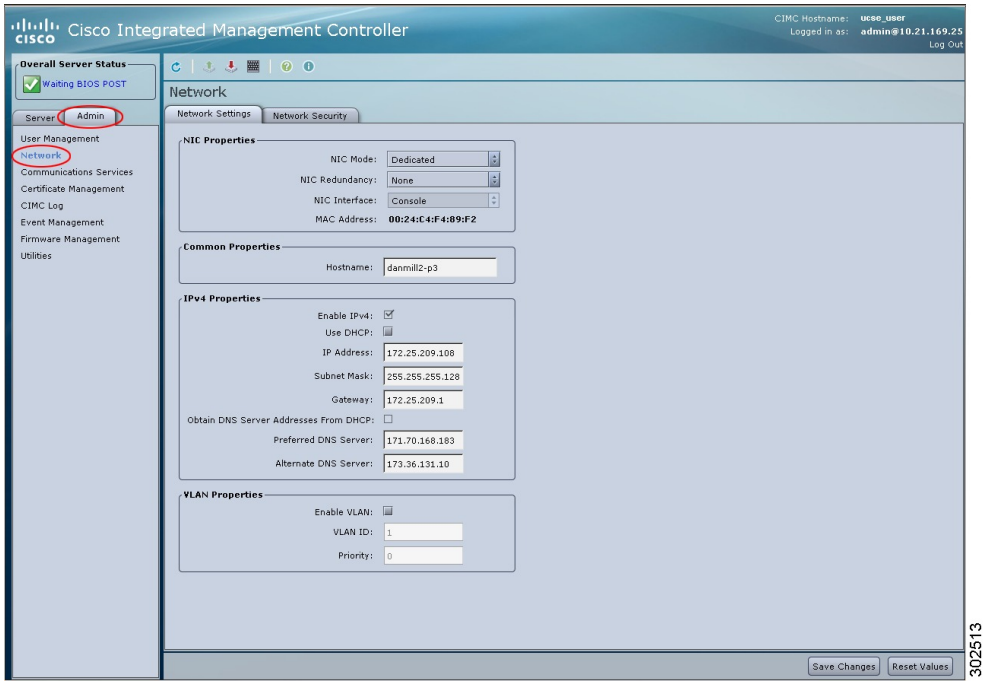
Procedure

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.

Figure 39: Network Settings Tab



Step 4 In the **Hostname** field, enter the name of the host.

Step 5 Click **Save Changes**.

Configuring IPv4

Before You Begin

You must log in as a user with admin privileges to configure IPv4.

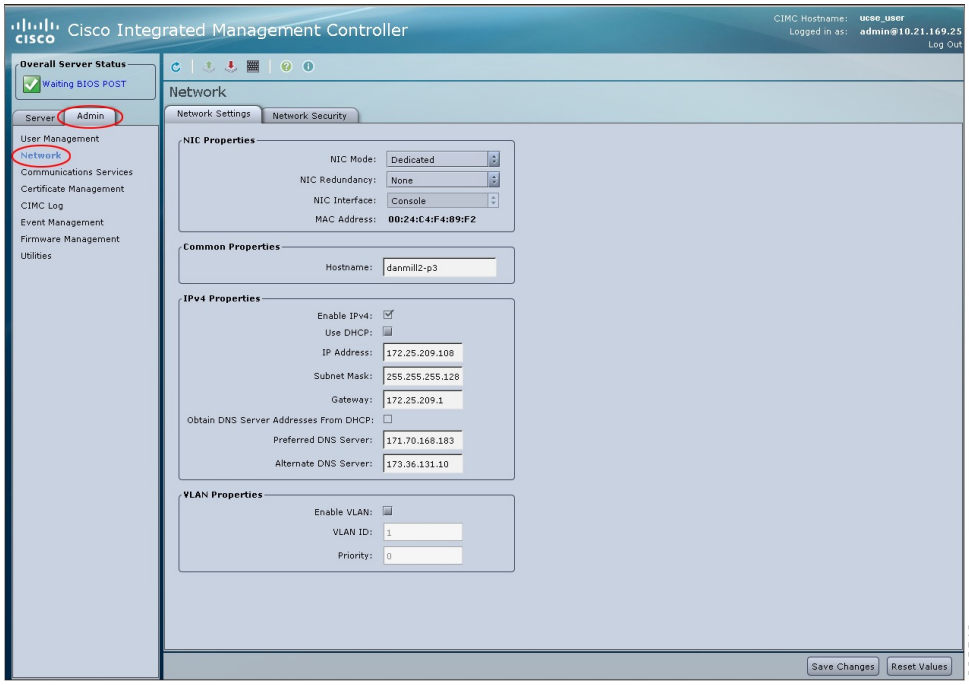
Procedure

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.

Figure 40: 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, the CIMC uses DHCP.
IP Address field	The IP address for the CIMC.
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, the CIMC retrieves the DNS server addresses from DHCP.
Preferred DNS Server field	The IP address of the primary DNS server.

Name	Description
Alternate DNS Server field	The IP address of the secondary DNS server.

Step 5 Click **Save Changes**.

Connecting to a VLAN

Before You Begin

You must be logged in as admin to connect to a VLAN.

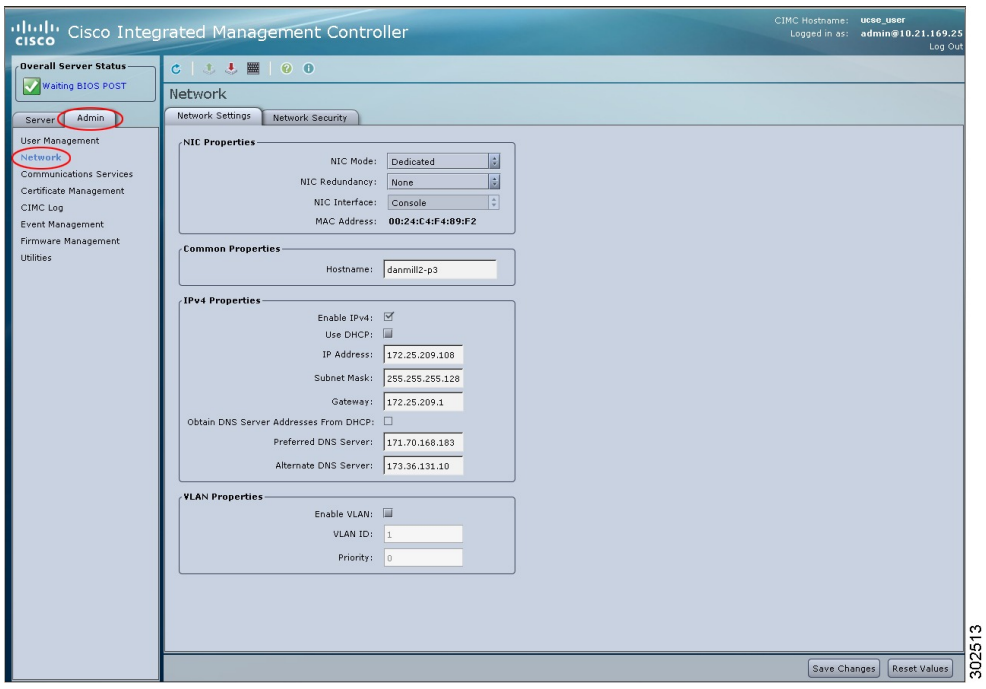
Procedure

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.

Figure 41: Network Settings Tab



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

Name	Description
Enable VLAN check box	If checked, the CIMC is connected to a virtual LAN.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 5 Click **Save Changes**.

Network Security Configuration

Network Security

The CIMC 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. CIMC 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.

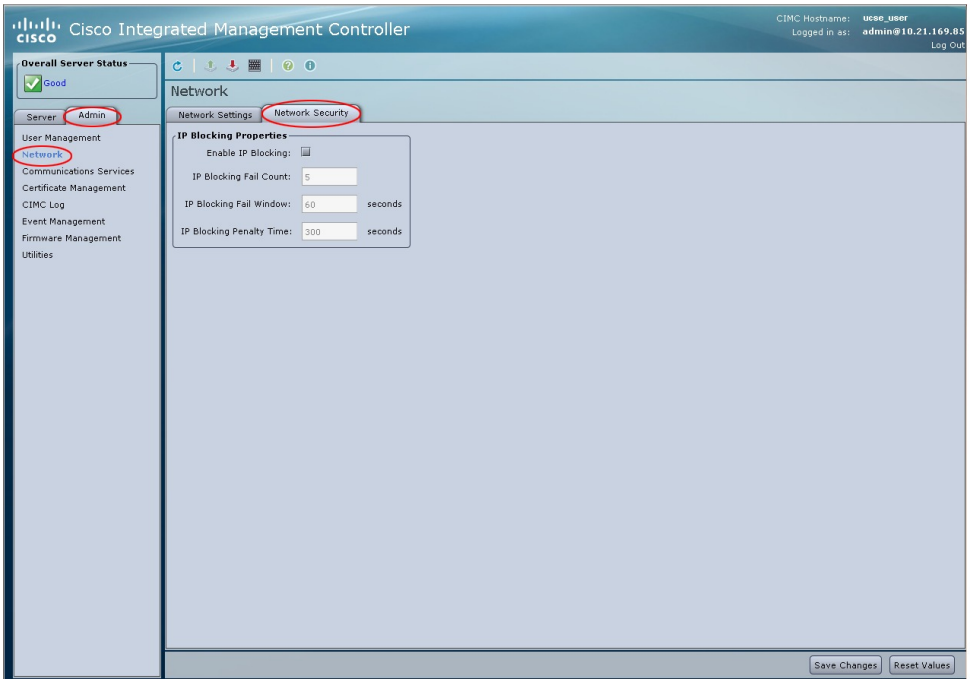
Procedure

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.

Figure 42: 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.

Name	Description
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 Click **Save Changes**.

CHAPTER 9

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.

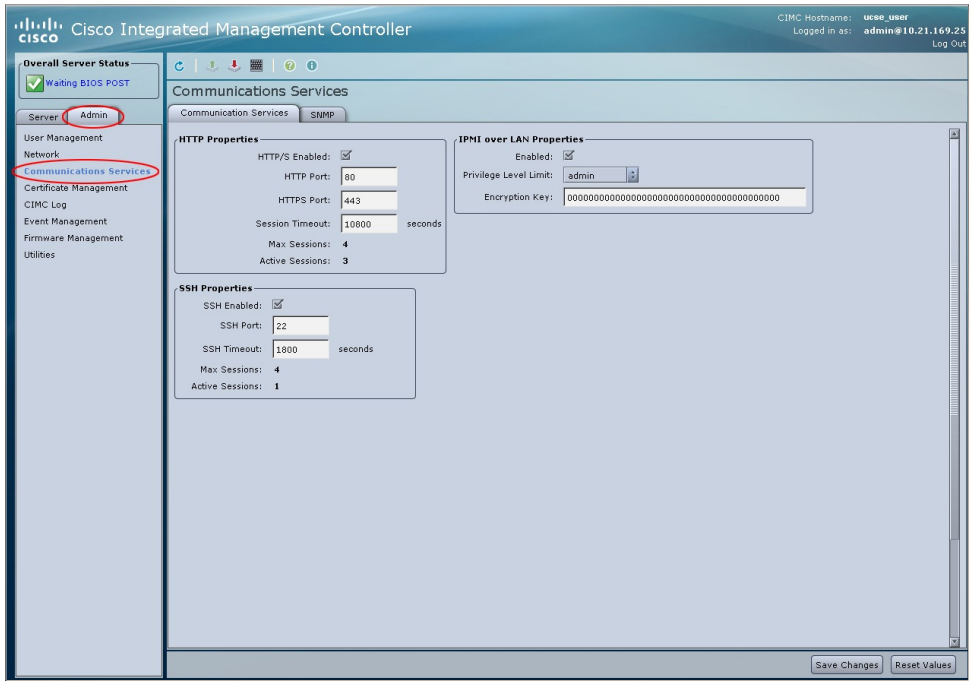
Procedure

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.

Figure 43: 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 CIMC.
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
Session Timeout field	The number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC. This value may not be changed.

Name	Description
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the CIMC.

Step 5 Click **Save Changes**.

Configuring SSH

Before You Begin

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

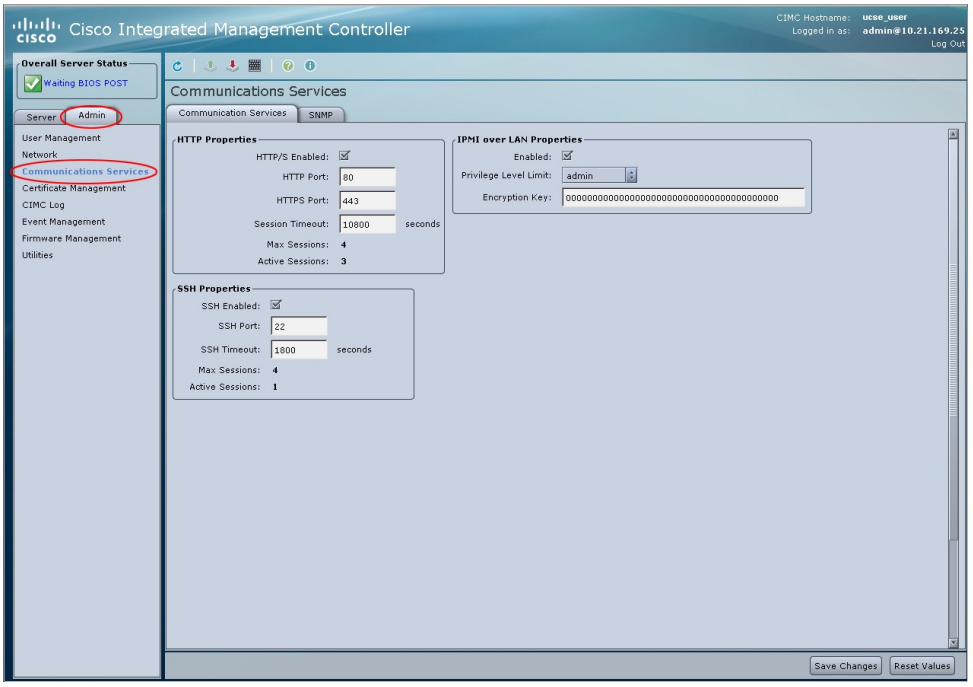
Procedure

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.

Figure 44: 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 CIMC.
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 CIMC. This value may not be changed.
Active Sessions field	The number of SSH sessions currently running on the CIMC.

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 the 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 CIMC with IPMI messages.

Before You Begin

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

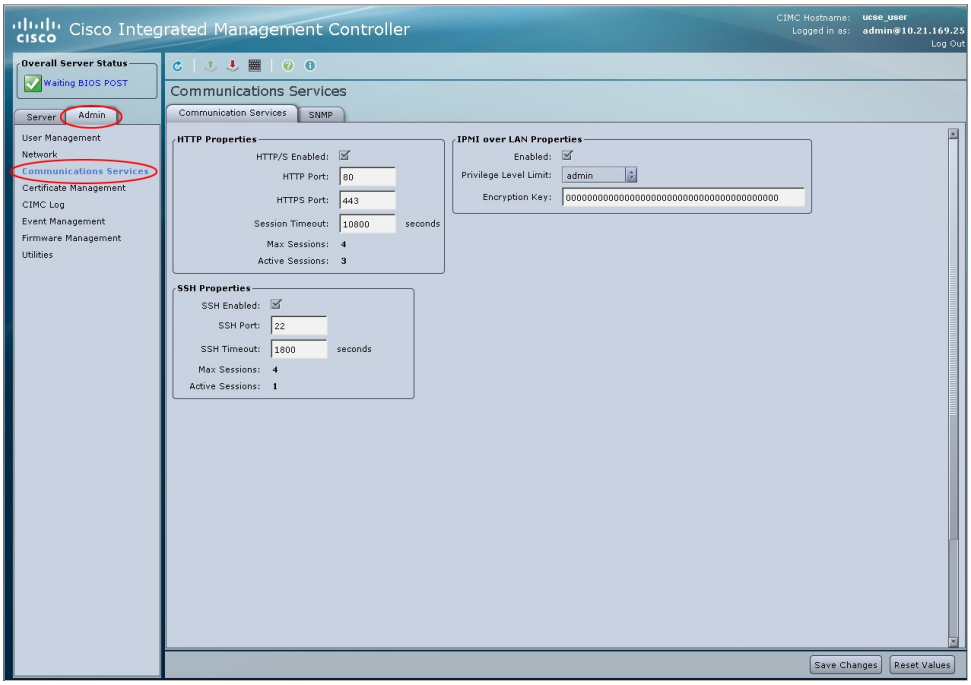
Procedure

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.

Figure 45: 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.

Step 5 Click **Save Changes**.

Configuring SNMP

SNMP

The Cisco UCS E-Series Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps.

Configuring SNMP Properties

Before You Begin

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

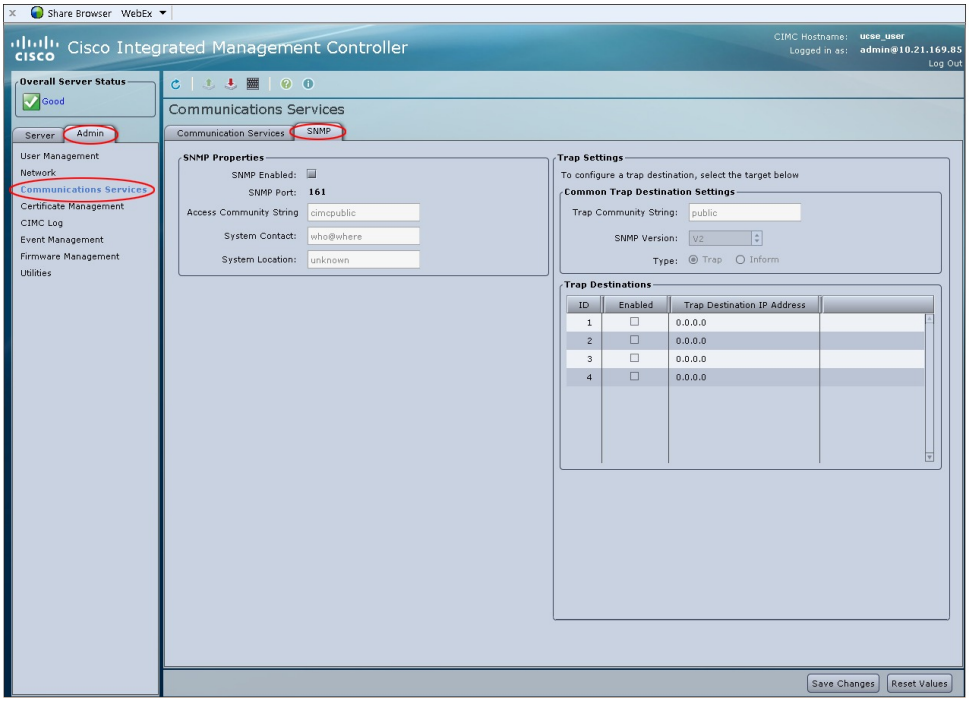
Procedure

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.

Figure 46: 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.
SNMP Port field	The port the server uses to communicate with the SNMP host. This value cannot be changed.
Access Community String field	The default SNMP v1 or v2c community name. Enter a string up to 18 characters.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 254 characters, such as an email address or a name and telephone number.

Name	Description
System Location field	The location of the host on which the SNMP agent (server) runs. Enter a string up to 254 characters.

Step 5 Click **Save Changes**.

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings.

Configuring SNMP Trap Settings

Before You Begin

You must log in as a user with admin privileges to disable platform event alerts.

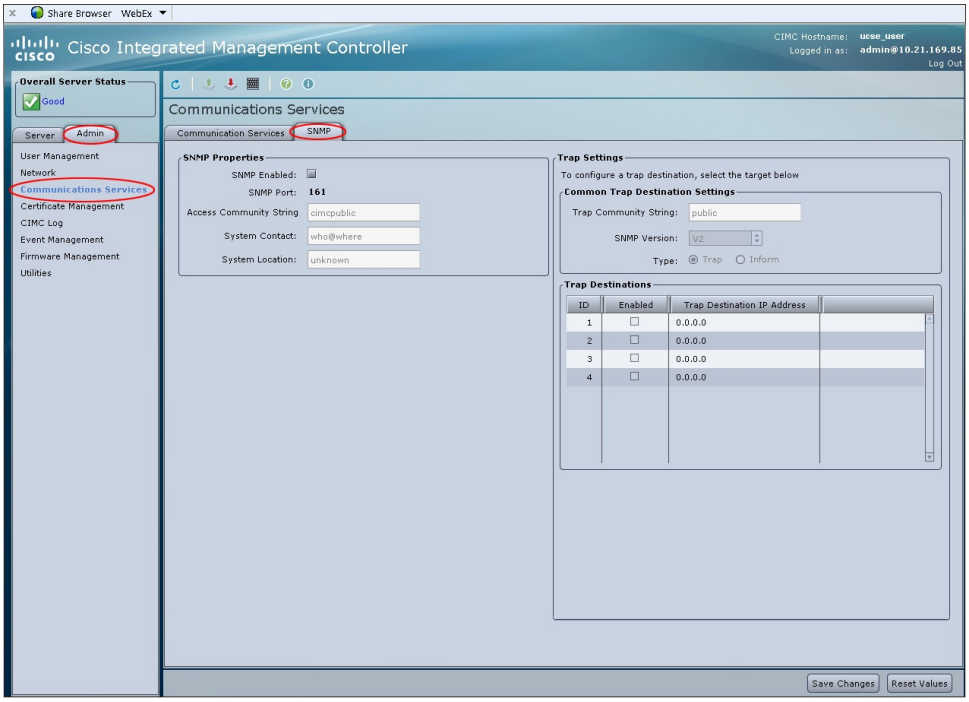
Procedure

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.

Figure 47: SNMP Tab



Step 4 In the **Trap Community String** text box in the **Common Trap Destination Settings** area, enter the name of the SNMP community to which trap information should be sent.

Step 5 In the **Trap Destinations** area, click the row of the desired SNMP trap destination.
The **Traps Details** dialog box opens.

Step 6 In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID column	The trap destination ID. This value cannot be modified.
Enabled column	For each SNMP trap destination that you want to use, check the associated check box in this column.
Trap Destination IP Address column	The IP address to which SNMP trap information is sent.

Step 7 Click **Save Changes**.

Sending a Test SNMP Trap Message

Before You Begin

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

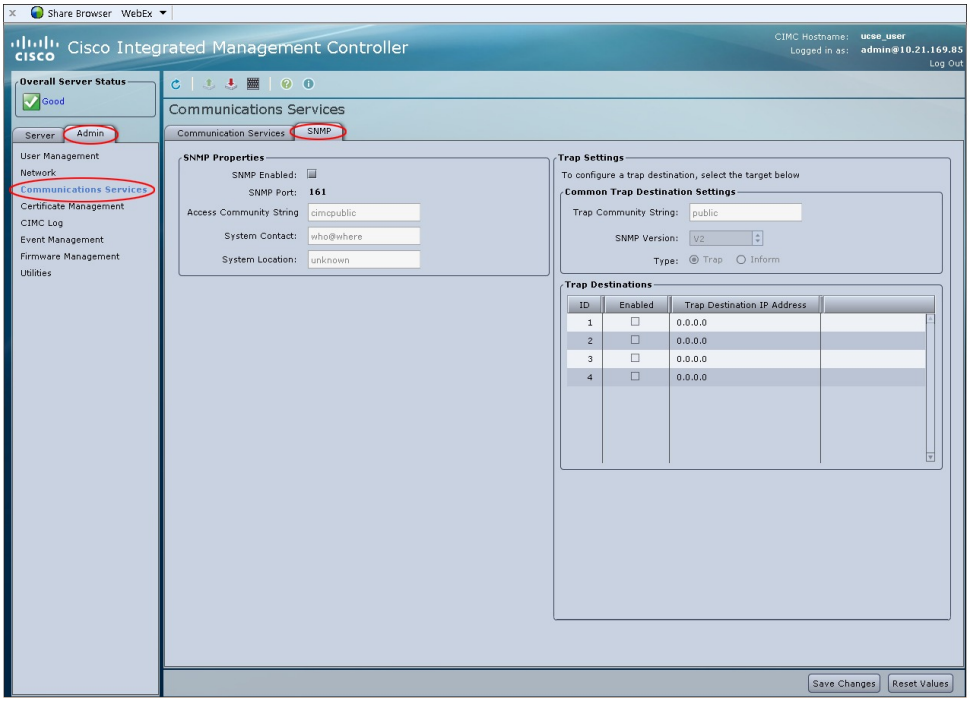
Procedure

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

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Figure 48: SNMP Tab



Step 4 In the **Trap Destinations** area, click the row of the desired SNMP trap destination.
The **Traps Details** dialog box opens.

Step 5 Click **Send SNMP trap**.
An SNMPv1 test trap message is sent to the trap destination.

Note The trap must be configured and enabled in order to send a test message.

CHAPTER 10

Managing Certificates

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 CIMC 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.

Procedure

Step 1 Generate the CSR from the CIMC.

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 CIMC.

Note The uploaded certificate must be created from a CSR generated by the CIMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

Before You Begin

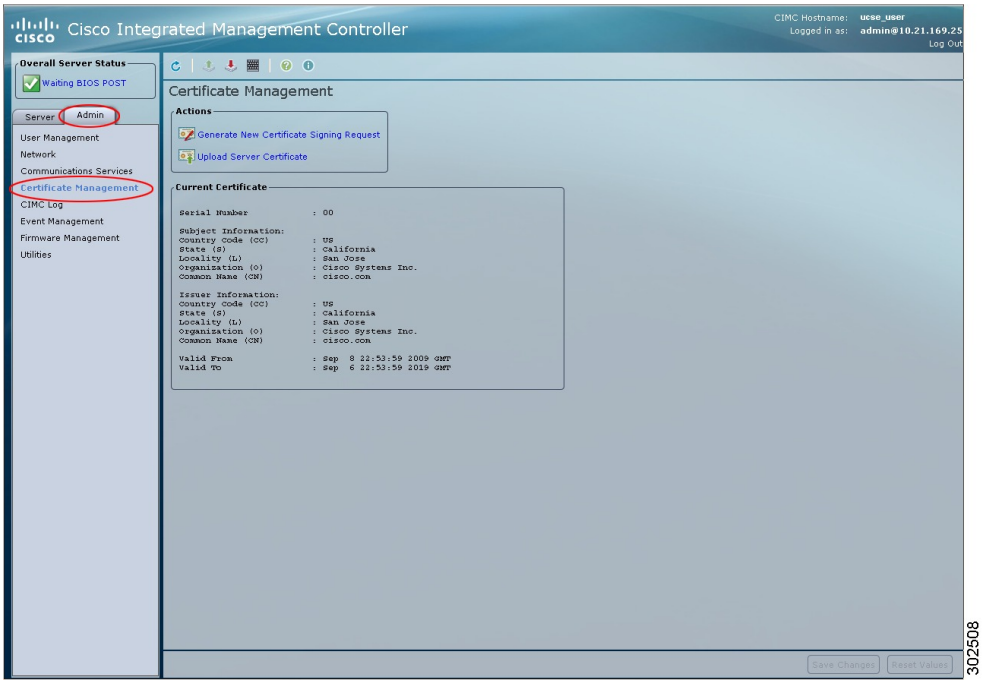
You must log in as a user with admin privileges to configure certificates.

Procedure

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

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

Figure 49: 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 hostname of the CIMC.
Organization Name field	The organization requesting the certificate.
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.

Name	Description
Email field	The e-mail contact at the company.

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.

Creating a Self-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 CIMC CLI.

Before You Begin

Obtain and install a certificate server software package on a server within your organization.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out ca.key 1024`	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*	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.

	Command or Action	Purpose
	Example: `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	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 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`	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

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 1024
Generating RSA private key, 1024 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 CIMC.

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.

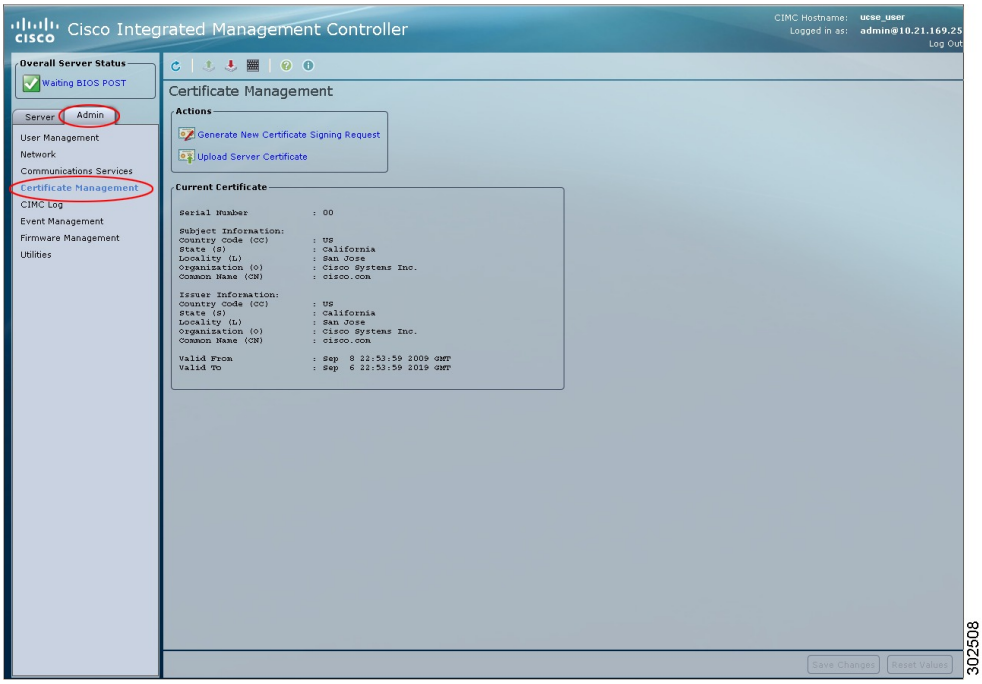
Note You must first generate a CSR using the CIMC Certificate Management menu, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

Procedure

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

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

Figure 50: 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. **Caution** After you select the certificate file using the **Browse** button, do not edit the certificate file name using the **Backspace** button on your keyboard. If you do, you will be logged out of CIMC.

Step 5 Click **Upload Certificate**.

CHAPTER 11

Configuring Platform Event Filters

This chapter includes the following sections:

Platform Event Filters

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs. You can also choose to generate and send an alert when a platform event occurs. Alerts are sent as an SNMP trap, so you must configure an SNMP trap destination before the alerts can be sent.

You can globally enable or disable the generation of platform event alerts. When disabled, alerts are not sent even if PEFs are configured to send them.

Enabling Platform Event Alerts

Before You Begin

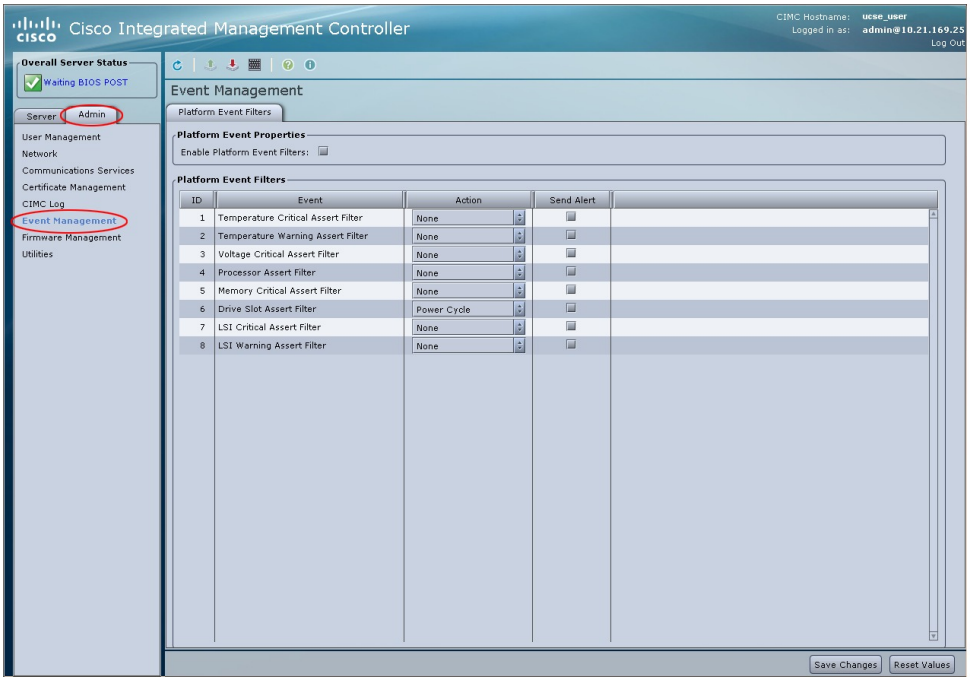
You must log in as a user with admin privileges to enable platform event alerts.

Procedure

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

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

Figure 51: Event Management



Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.

Step 4 In the **Platform Event Alerts** area, check the **Enable Platform Event Alerts** check box.

Step 5 Click **Save Changes**.

Disabling Platform Event Alerts

Before You Begin

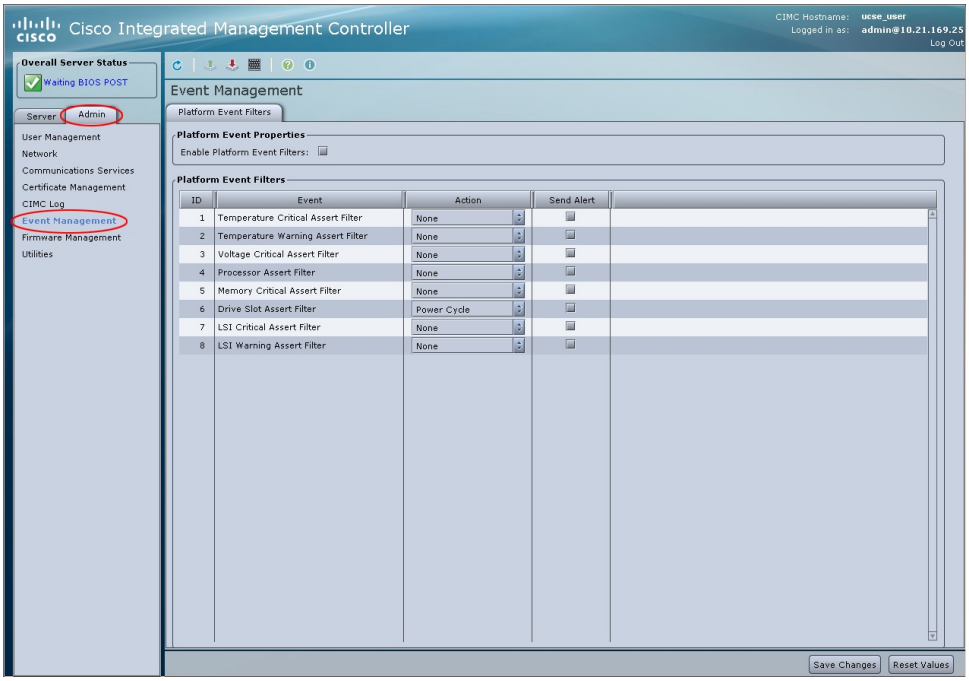
You must log in as a user with admin privileges to disable platform event alerts.

Procedure

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

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

Figure 52: Event Management



Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.

Step 4 In the **Platform Event Alerts** area, uncheck the **Enable Platform Event Alerts** check box.

Step 5 Click **Save Changes**.

Configuring Platform Event Filters

Before You Begin

You must log in as a user with admin privileges to configure platform event filters.

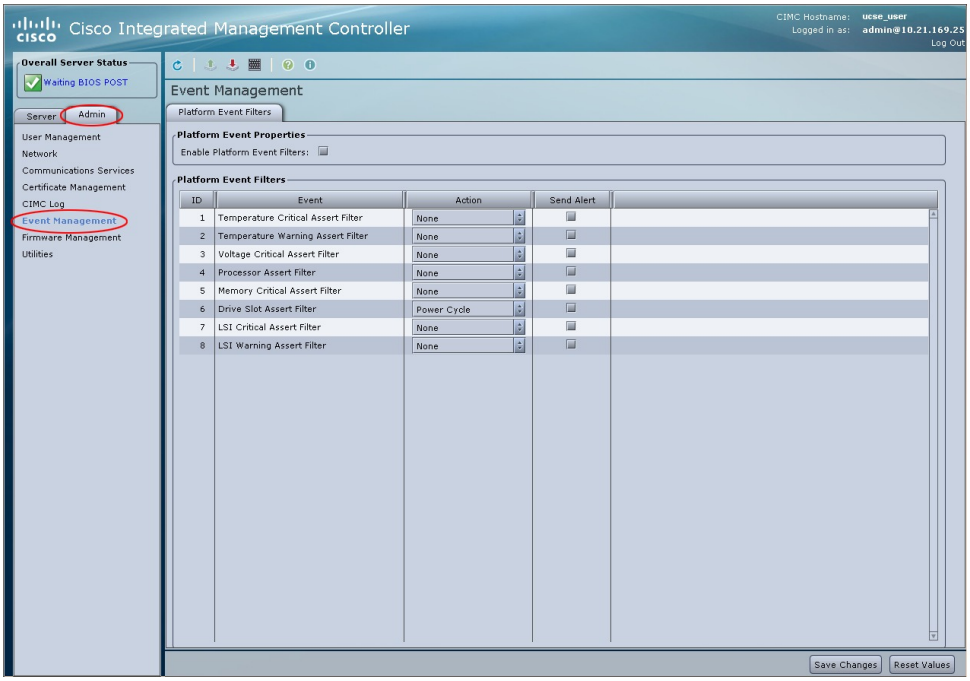
Configuring Platform Event Filters

Procedure

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

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

Figure 53: Event Management



Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.

Step 4 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.
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.

Name	Description
Send Alert column	For each filter that you want to send an alert, check the associated check box in this column. **Note** In order to send an alert, the filter trap settings must be configured properly and the **Enable Platform Event Filters** check box must also be checked.

Step 5 Click **Save Changes**.

What to Do Next

If you configure any PEFs to send an alert, complete the following tasks:

- Enabling Platform Event Alerts, on page 129
- Configuring SNMP Trap Settings

Interpreting Platform Event Traps

A CIMC platform event alert sent as an SNMP trap contains an enterprise object identifier (OID) in the form `1.3.6.1.4.1.3183.1.1.0.event`. The first ten fields of the OID represent the following information: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`, indicating an IPMI platform event trap (PET) version 1.0 message. The last field is an event number, indicating the specific condition or alert being notified.

Platform Event Trap Descriptions

The following table provides a description of the event being notified in a platform event trap message, based on the event number in the trap OID.

Event Number	Platform Event Description
0	Test Trap
131330	Under Voltage
131337	Voltage Critical
196871	Current Warning
262402	Fan Critical
459776	Processor related (IOH-Thermalert/Caterr sensor) predictive failure deasserted
459777	Processor related (IOH-Thermalert/Caterr sensor) predictive failure asserted
460032	Power Warning
460033	Power Warning
524533	Power Supply Critical

Event Number	Platform Event Description
524551	Power Supply Warning
525313	Discrete Power Supply Warning
527105	Power Supply Redundancy Lost
527106	Power Supply Redundancy Lost
552704	Power Supply Inserted
552705	PSU Failure
552707	Power Supply AC Lost
65799	Temperature Warning
65801	Temperature Critical
786433	Memory Warning
786439	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM)
818945	Memory Warning
818951	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM)
851968	Related to HDD sensor
851972	Related to HDD sensor
854016	HDD Absent
854017	HDD Present
880384	HDD Present, no fault indicated
880385	HDD Fault
880512	HDD Not Present
880513	HDD is deasserted but not in a fault state
884480	Drive Present
884481	Drive Slot Warning
884485	Drive in Critical Array
884488	Drive Rebuild/Remap Aborted
884489	Drive Slot Warning

CHAPTER 12

CIMC Firmware Management

This chapter includes the following sections:

Overview of CIMC Firmware

E-Series Servers use firmware downloaded from cisco.com. This firmware is certified by Cisco to upgrade on a E-Series Server.

The CIMC firmware you download is packaged in a .zip file. After you have downloaded a firmware .zip from Cisco, you can use it to update the firmware on your server. Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Caution Do not use the .zip file to update your server.

You use a .bin file to reimage. You must extract the proper .bin upgrade file from this .zip file. You can extract this .bin to a TFTP server or your local machine. You can update using a TFTP server or a browser on your local machine.

Note When you update the firmware, you can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

The CIMC separates the firmware update process into stages to ensure that you can install the firmware to a component while the server is running without affecting its uptime. Because you do not need to reboot the

server until after you activate, you can perform that task overnight or during other maintenance periods. When you update firmware, the following stages occur:

Install

During this stage, the CIMC transfers the selected firmware version to the server. The install process always overwrites the firmware in the non-active slot on the server. You can install the firmware using either of the following methods:

- Through a browser client—This method allows you to browse for a firmware image on your computer and install it on the server.
- From a TFTP server—This method allows you to install a firmware image residing on a TFTP server.

Activate

During this stage, the CIMC sets the non-active firmware version as active and reboots the server. When the server reboots, the non-active slot becomes the active slot, and the active slot becomes the non-active slot. The firmware in the new active slot becomes the running version.

Obtaining Software from Cisco Systems

Use this procedure to download drivers, BIOS and CIMC firmware, and the diagnostics image.

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**.
A roll-down menu appears.

Step 4 From the Downloads (center) pane, click **All Downloads** (located at the bottom right corner).
The **Download Software** page appears.

Step 5 From the left pane, click **Products**.

Step 6 From the center pane, click **Unified Computing and Servers**.

Step 7 From the right pane, click **Cisco UCS E-Series Software**.

Step 8 From the right pane, click the name of the server model for which you want to download the software.
The **Download Software** page appears with the following list of software categories that you can download:

- **Unified Computing System (UCSE) Server Drivers**—Contains the following drivers:
  - On-Board Network Drivers for Windows 2008 R2
  - 10G PCIe Network Drivers for Windows 2008 R2 and Linux
  - LSI Drivers (On-Board Hardware RAID Controller) for Windows 2008 R2
  - Intel Drivers for Windows 2008 R2

- **Unified Computing System (UCSE) Server Firmware**—Contains the following BIOS and CIMC firmware images:
  - Double-Wide BIOS
  - Single-Wide BIOS
  - BMC/CIMC Image
- **Unified Computing System (UCSE) Utilites**—Contains the following diagnostics image:
  - On-Board Diag Image

Step 9 Click the appropriate software category link.

Step 10 Click the **Download** button associated with software image that you want to download.
The **End User License Agreement** dialog box appears.

Step 11 (Optional) To download multiple software images, do the following:

a) Click the **Add to cart** button associated with the software images that you want to download.

b) Click the **Download Cart** button located on the top right .
All the images that you added to the cart display.

c) Click the **Download All** button located at the bottom right corner to download all the images.
The **End User License Agreement** dialog box appears.

Step 12 Click **Accept License Agreement**.

Step 13 Do one of the following as appropriate:

- Save the software image file to a local drive.
- If you plan to install the software image from a TFTP server, copy the file to the TFTP server that you want to use.

  The server must have read permission for the destination folder on the TFTP server.

What to Do Next

Install the software image.

Installing CIMC Firmware from the TFTP Server

Before You Begin

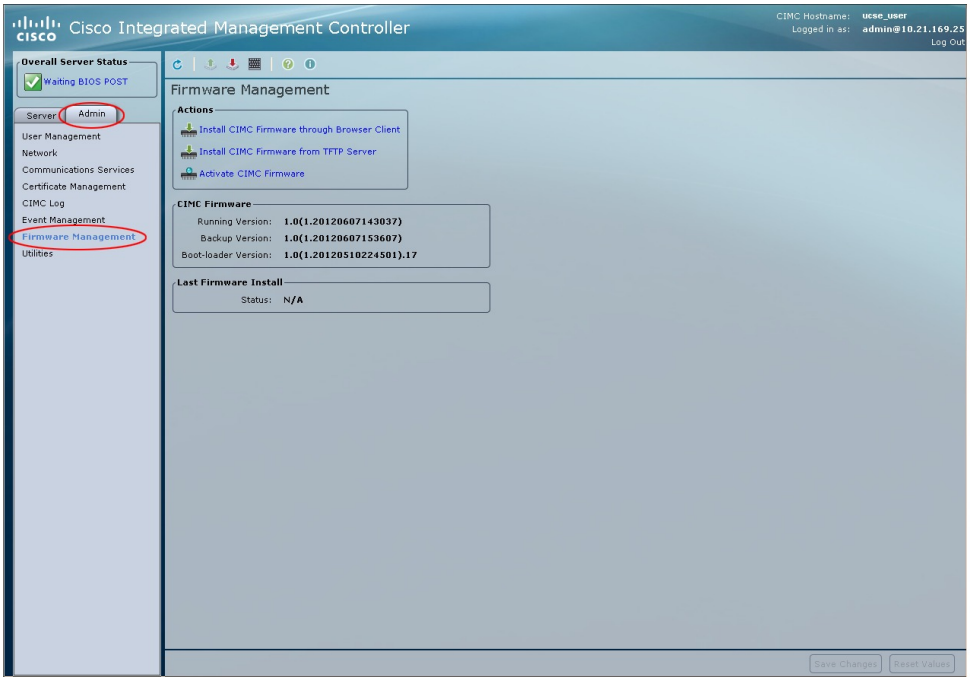
- You must log in as a user with admin privileges to install CIMC firmware through the browser.
- Obtain the CIMC firmware file from Cisco Systems. See Obtaining Software from Cisco Systems.
- Unzip the proper .bin upgrade file on your TFTP server.

Procedure

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

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

Figure 54: Firmware Management



Step 3 In the **Actions** area, click **Install CIMC Firmware from TFTP Server**.

Step 4 In the **Install Firmware** dialog box, complete the following fields:

Name	Description
TFTP Server IP Address field	The IP address of the TFTP server on which the firmware image resides.
Image Path and Filename field	The firmware image filename on the server. When you enter this name, include the relative path for the image file from the top of the TFTP tree to the file location.

Step 5 Click **Install Firmware**.

What to Do Next

Activate the CIMC firmware.

Installing CIMC Firmware Through the Browser

Before You Begin

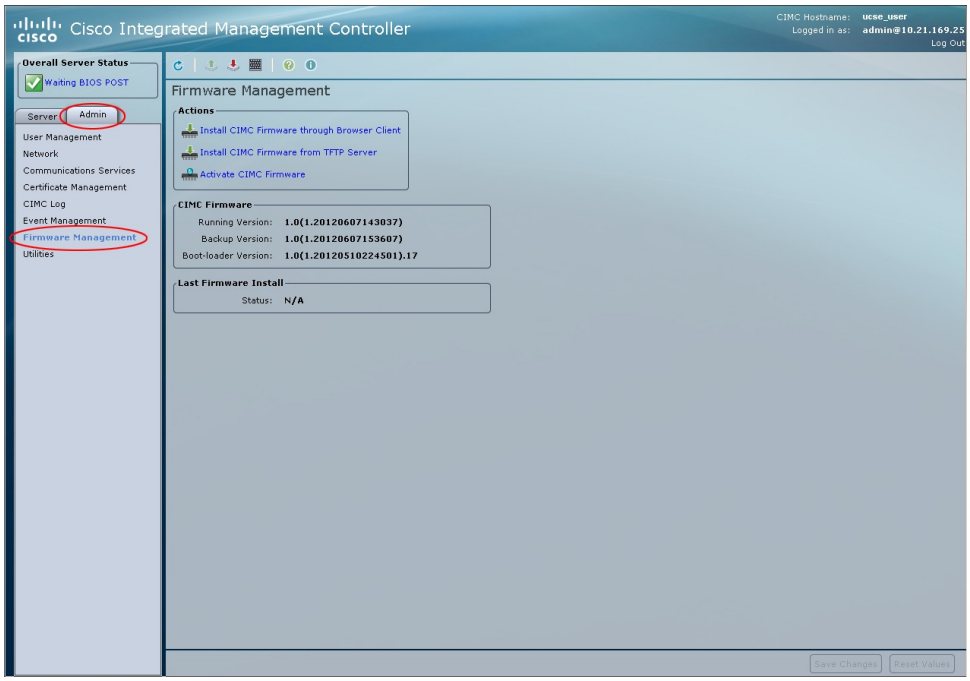
- You must log in as a user with admin privileges to install the CIMC firmware through the browser.
- Obtain the CIMC firmware file from Cisco Systems. See Obtaining Software from Cisco Systems.
- Unzip the proper .bin upgrade file to your local machine.

Procedure

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

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

Figure 55: Firmware Management



Step 3 In the **Actions** area, click **Install CIMC Firmware through Browser Client**.

Step 4 In the **Install CIMC Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the .bin file you want to install.

Step 5 Click **Install Firmware**.

What to Do Next

Activate the CIMC firmware.

Activating Installed CIMC Firmware

Before You Begin

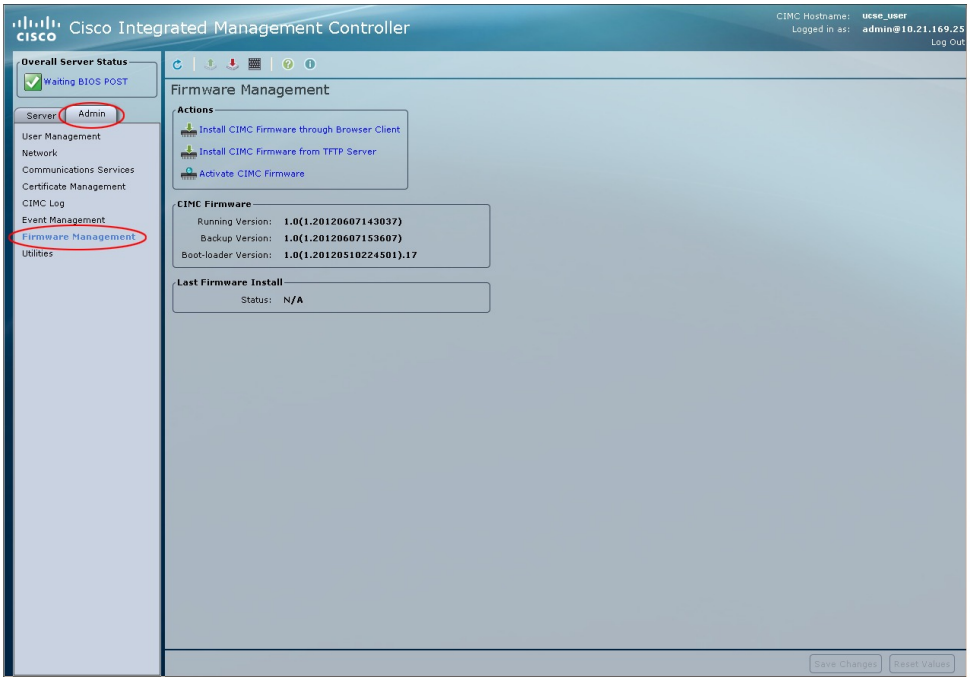
- You must log in as a user with admin privileges to activate firmware.
- Install CIMC firmware on the server.

Procedure

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

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

Figure 56: Firmware Management



Step 3 In the **Actions** area, click **Activate CIMC 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**.

Viewing CIMC 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 (CIMC) Information** area of the **Server Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the CIMC.
IP Address field	The IP address for the CIMC.
MAC Address field	The MAC address assigned to the active network interface to the CIMC.
Firmware Version field	The current CIMC firmware version.
CPLD Version field	The programable hardware logic version.
Hardware Version field	The printed circuit board version.
Current Time field	The current date and time according to the CIMC clock.

CHAPTER 13

Viewing Logs

This chapter includes the following sections:

CIMC Log

Viewing the CIMC Log

Procedure

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

Step 2 On the **Admin** tab, click **CIMC Log**.

Step 3 Review the following information for each CIMC event in the log.

Name	Description
Timestamp column	The date and time the event occurred.
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** role.

Step 4 From the **Entries Per Page** drop-down list, select the number of CIMC events to display on each page.

Step 5 Click **<Newer** and **Older>** to move backward and forward through the pages of CIMC events, or click **<<Newest** to move to the top of the list.

By default, the newest CIMC events are displayed at the top if the list.

Clearing the CIMC Log

Before You Begin

You must log in as a user with user privileges to clear the CIMC log.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **CIMC Log**.
Step 3 In the **CIMC Log** pane, click **Clear Log**.
Step 4 In the dialog box that appears, click **OK**.

Sending the CIMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive CIMC log entries.

Before You Begin

You can configure profiles for one or two remote servers to receive CIMC log entries.

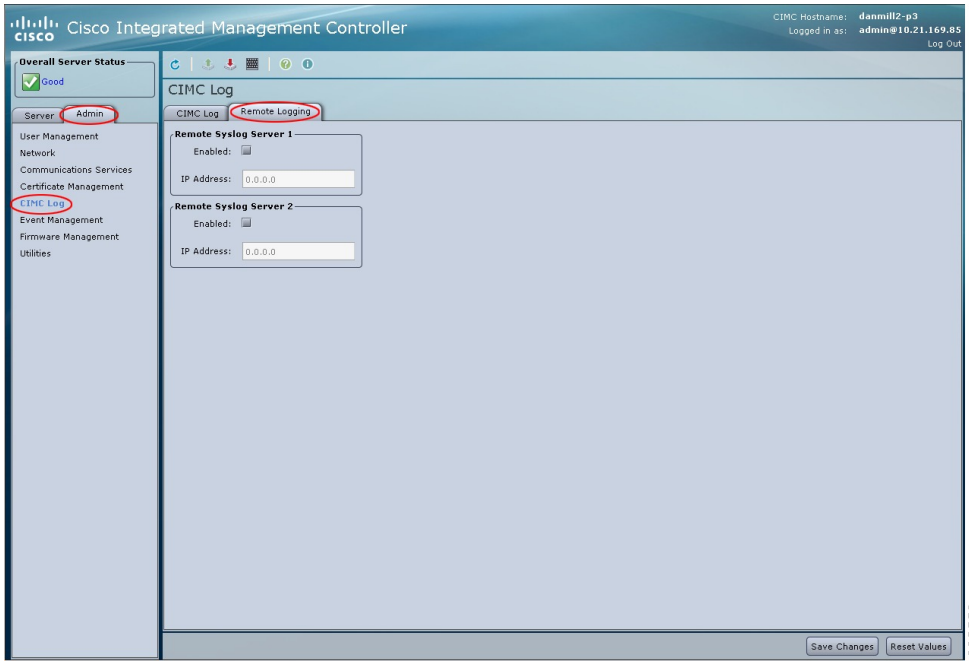
Procedure

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

Step 2 On the **Admin** tab, click **CIMC Log**.

Step 3 In the **CIMC Log** pane, click the **Remote Logging** tab.

Figure 57: Remote Logging Tab



Step 4 In either of the **Remote Syslog Server** dialog boxes, complete the following fields:

Name	Description
Enabled check box	If checked, CIMC sends log messages to the Syslog server named in the **IP Address** field.
IP Address field	The IP address of the Syslog server on which the CIMC log should be stored.

Step 5 Click **Save Changes**.

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 **System Event Log**.

Step 3 Review the following information for each system event in the log:

Name	Description
Time column	The time the event occurred.
Severity column	The event severity. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable** **Tip** The severity field includes both text and a color-coded icon. Green indicates normal operation. Yellow is informational. Warning, critical, and non-recoverable errors are displayed in shades of red.
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** role.

Step 4 From the **Entries Per Page** drop-down list, select the number of system events to display on each page.

Step 5 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 **System Event Log**.
Step 3 In the **System Event Log** pane, click **Clear Log**.
Step 4 In the dialog box that appears, click **OK**.

CHAPTER 14

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

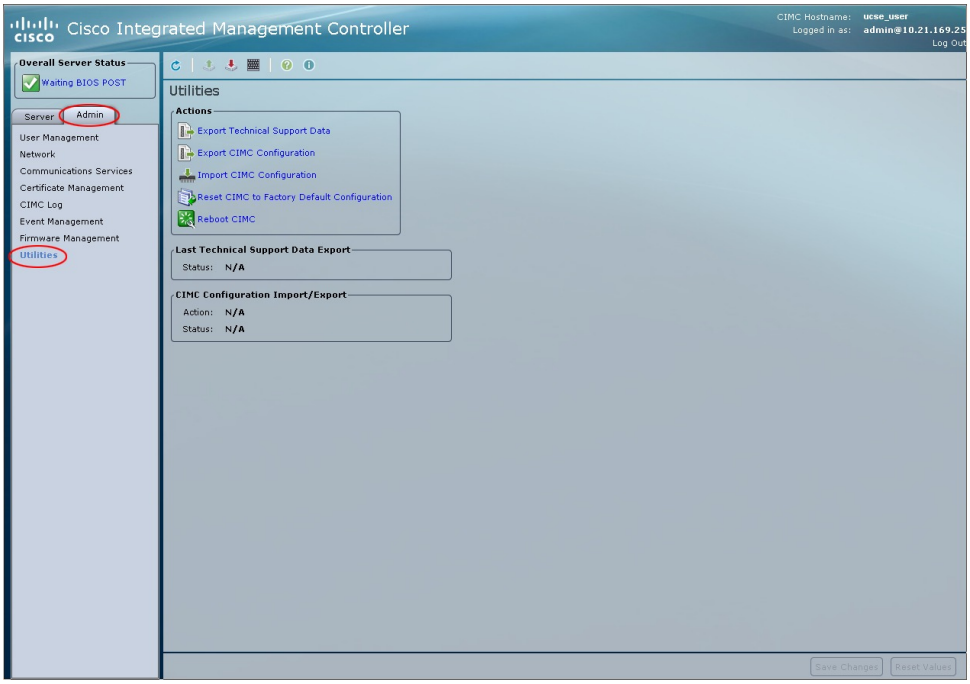
Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Procedure

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

Step 2 On the **Admin** tab, click **Utilities**.

Figure 58: Utilities



Step 3 In the **Actions** area of the **Utilities** pane, click **Export Technical Support Data**.

Step 4 In the **Export Technical Support Data** dialog box, complete the following fields:

Name	Description
Export to a local file radio button	Select this option and click **Export** to start the support data collection and export process. When the support data collection is complete, a **Download** button appears. Click **Download** to save the file to a drive that is local to the computer running the CIMC GUI.
Export to TFTP server radio button	Select this option to save the support data file to a TFTP server. When you select this option, CIMC GUI displays the following fields: • **TFTP Server IP Address**—The IP address of the TFTP server on which the support data file should be stored. • **Path and Filename**—The name of the file in which the support data should be stored on the server. When you enter this name, include the relative path for the file from the top of the TFTP tree to the desired location.

Step 5 Click **Export**.

What to Do Next

Provide the generated report file to Cisco TAC.

Rebooting CIMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the CIMC. This procedure is not part of the normal maintenance of a server. After you reboot the CIMC, you are logged off and the CIMC will be unavailable for a few minutes.

Note If you reboot the CIMC 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 CIMC reboot is complete.

Before You Begin

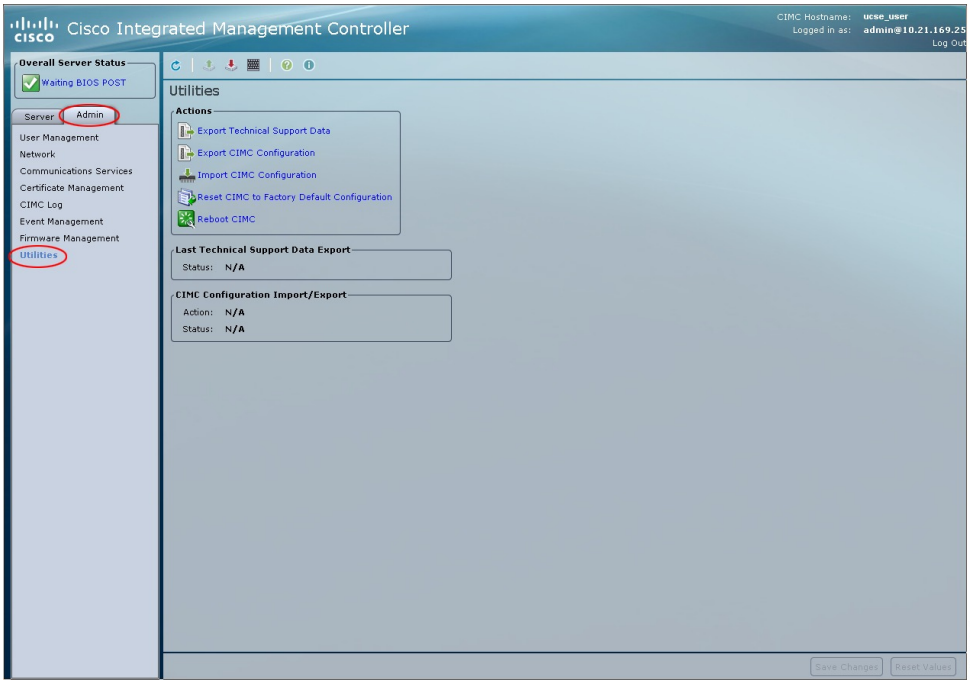
You must log in as a user with admin privileges to reboot the CIMC.

Procedure

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

Step 2 On the **Admin** tab, click **Utilities**.

Figure 59: Utilities



Step 3 In the **Actions** area of the **Utilities** pane, click **Reboot CIMC**.

Step 4 Click **OK**.

Resetting CIMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC 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 CIMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

Before You Begin

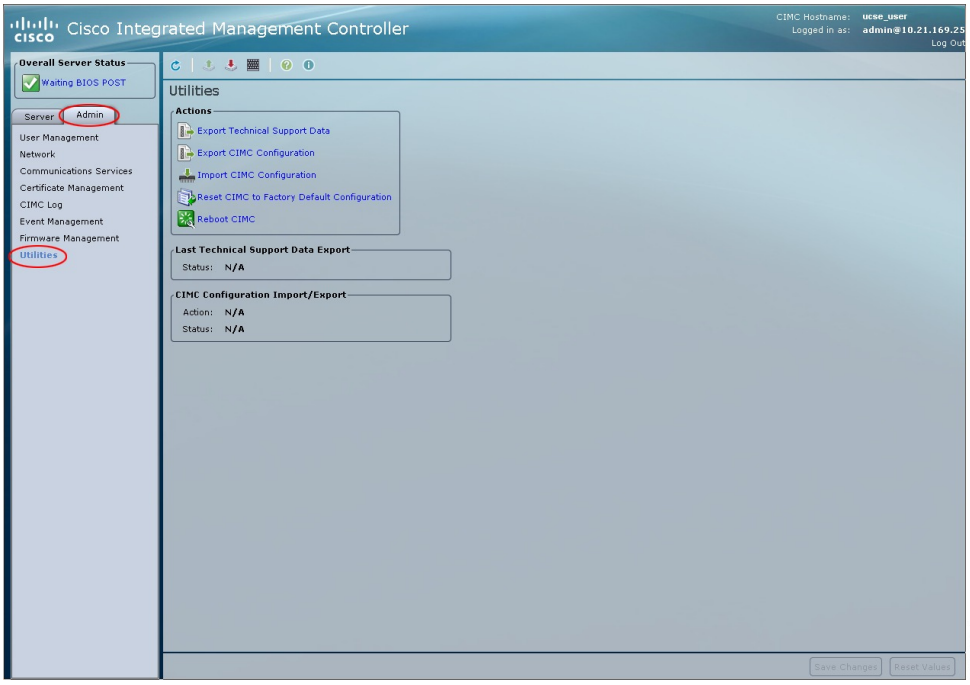
You must log in as a user with admin privileges to reset the CIMC to factory defaults.

Procedure

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

Step 2 On the **Admin** tab, click **Utilities**.

Figure 60: Utilities



Step 3 In the **Actions** area of the **Utilities** pane, click **Reset CIMC to Factory Default Configuration**.

Step 4 Click **OK**.

A reboot of CIMC 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. CIMC will power on when it is ready.

Exporting and Importing the CIMC Configuration

Exporting and Importing the CIMC Configuration

To perform a backup of the CIMC configuration, you take a snapshot of the system configuration and export the resulting CIMC 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 CIMC configuration file to the same system or you can import it to another CIMC 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 CIMC configuration file is an XML text file whose structure and elements correspond to the CIMC 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.

Exporting the CIMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Before You Begin

Obtain the backup TFTP server IP address.

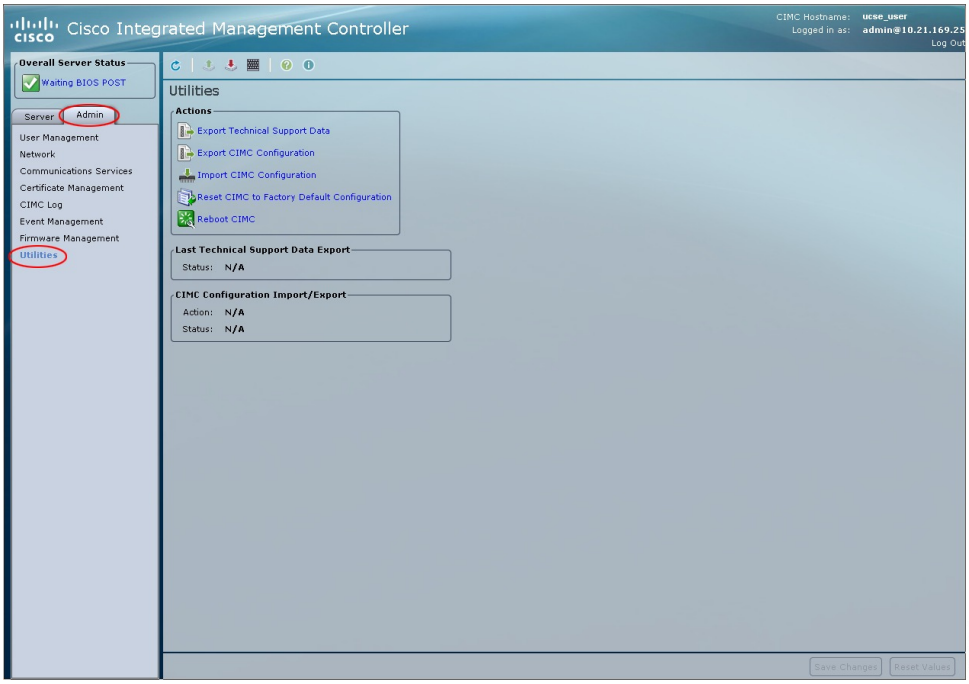
If you want the option to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is enabled on this server before you create the configuration file. If SNMP is disabled when you export the configuration, CIMC will not apply the SNMP values when the file is imported.

Procedure

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

Step 2 On the **Admin** tab, click **Utilities**.

Figure 61: Utilities



Step 3 In the **Actions** area of the **Utilities** pane, click **Export CIMC Configuration**.

Step 4 In the **Export CIMC Configuration** dialog box, complete the following fields:

Name	Description
Export to a local file radio button	Select this option and click **Export** to save the XML configuration file to a drive that is local to the computer running the CIMC GUI. When you select this option, CIMC GUI displays a **Browse** dialog box that lets you navigate to the location to which the configuration file should be saved.
Export to TFTP server radio button	Select this option to save the XML configuration file to a TFTP server. When you select this option, CIMC GUI displays the following fields: • **TFTP Server IP Address**—The IP address of the TFTP server to which the configuration file will be exported. • **Path and Filename**—The path and filename CIMC should use when exporting the file to the TFTP server.

Step 5 Click **Export**.

Importing a CIMC Configuration

Before You Begin

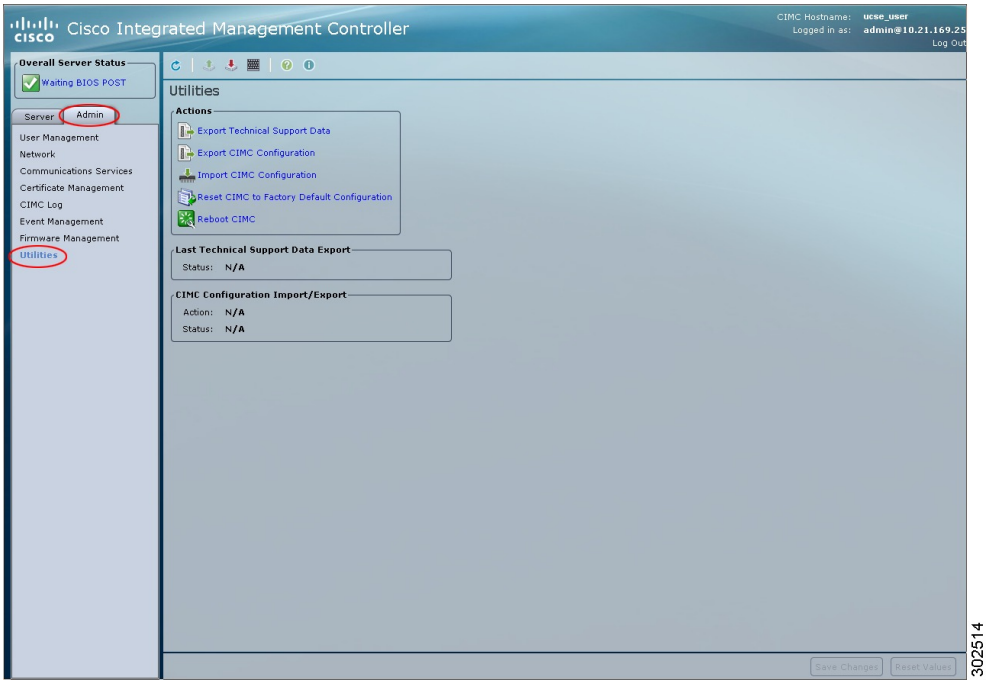
If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, CIMC does not overwrite the current values with those saved in the configuration file.

Procedure

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

Step 2 On the **Admin** tab, click **Utilities**.

Figure 62: Utilities



Step 3 In the **Actions** area of the **Utilities** pane, click **Import CIMC Configuration**.

Step 4 In the **Import CIMC Configuration** dialog box, complete the following fields:

Name	Description
Import from a local file radio button	Select this option and click **Import** to navigate to the XML configuration file stored on a drive that is local to the computer running the CIMC GUI. When you select this option, CIMC GUI displays the **File** field and a **Browse** button that lets you navigate to the file you want to import.
Import from TFTP server radio button	Select this option to import the XML configuration file from a TFTP server. When you select this option, CIMC GUI displays the following fields: • **TFTP Server IP Address**—The IP address of the TFTP server on which the configuration file resides. • **Path and Filename**—The path and filename of the configuration file on the TFTP server.

Step 5 Click **Import**.

CHAPTER 15

Diagnostic Tests

This chapter includes the following sections:

Diagnostic Tests Overview

Diagnostics is a standalone utility that runs on the E-Series Server independent of the operating system or applications running on the server. If you experience problems with the E-Series Server, you can use diagnostics tests to run a preliminary check and isolate the problem. Diagnostic tests can be executed on the server CPU, memory, and block devices. Block devices include hard drive, USB drive, and SD cards.

If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco Technical Assistance Center (TAC) at: http://www.cisco.com/cisco/web/support/index.html to isolate the problem.

If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.

Caution Diagnostic tests are non-destructive, but if there is a power or equipment failure when the tests are running, there is a possibility that the disk data might get corrupted. We highly recommend that you backup the data before running these tests.

Basic Workflow for Executing Diagnostic Tests

1. Backup data.
2. The diagnostics image is pre-installed on the E-Series Server at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository.
3. Mount the diagnostics image onto the HDD virtual drive of a USB controller.

4 Set the boot order to make EFI Shell as the first boot device.

5 Reboot the server.

6 Run diagnostic tests from the EFI Shell.

7 Reset the virtual media boot order to its original setting.

Mapping the Diagnostics Image to the Host

Before You Begin

- Backup data.
- Log into CIMC as a user with admin privileges.
- The diagnostics image is pre-installed on the E-Series Server at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository. See Obtaining Software from Cisco Systems.

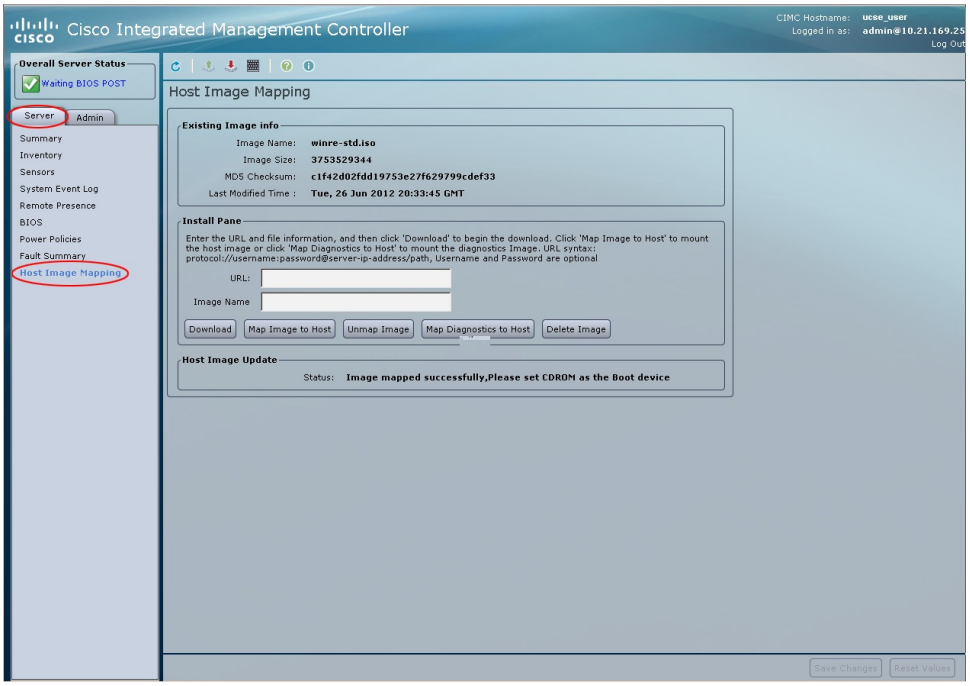
Note If you start an image update while an update is already in process, both updates will fail.

Procedure

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

Step 2 On the **Server** tab, click **Host Image Mapping**.

Figure 63: Host Image Mapping



Step 3 In the **Install Pane**, complete the following fields:

Name	Description
URL field	The URL of the remote server on which the diagnostics image is located. If the remote server requires user authentication, you must add the username and password of the remote server in the URL. The remote server can be an FTP, FTPS, HTTP, or HTTPS server. The URL syntax must be: *protocol://username:password@server-ip-address/path/filename*
Image Name field	The name of the diagnostics image. The image name must have .diag as the file extension.

Step 4 Click **Download**.
The diagnostics file is downloaded from the specified FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository.

Step 5 Click **Map Diagnostics to Host**.
The diagnostics image is mounted on the HDD virtual drive of the USB controller.

Step 6 Set the boot order to make **EFI Shell** as the first boot device.
To set the boot order, see Configuring the Server Boot Order.

Step 7 Reboot the server.
The EFI Shell appears.

What to Do Next

Run diagnostic tests.

Running Diagnostic Tests

From the EFI Shell, use the following procedure to run diagnostic tests.

Before You Begin

- Backup data. All tests are non-destructive, but if there is power or equipment failure when the tests are running, there is a possibility that the disk data might get corrupted. We highly recommend that you backup data before executing these tests.
- Use the CIMC CLI or the CIMC GUI to download and map the diagnostics image onto the HDD virtual drive of the USB controller.
- Reboot the server. The EFI Shell displays.

Procedure

	Command or Action	Purpose
Step 1	Shell > **dir** *virtual-media-drive-name***:**	Displays all the file packages that exist in the specified virtual media drive. The drive name starts with fs0 and can be fs0, fs1, fs2, and so on. **Note** Make sure that you add a colon after the virtual media drive name. For example, **dir fs1:**
Step 2	Shell > *virtual-media-drive-name***:**	Enters the virtual media drive in which the diagnostic file is located.
Step 3	Virtual Media Drive :\> **cp** *package-file-name* **dsh.pkg**	Copies the package file for which you are running diagnostics into the diagnostics shell package file.
Step 4	Virtual Media Drive :\> **dsh**	Enters the Diagnostics Shell. At the confirmation prompt, answer **y**.
Step 5	Server: SRV > **run all**	Executes all available diagnostic tests and displays the progress and status of the tests. Diagnostic tests are run on the server CPU, memory, and block devices. Block devices include hard drive, USB drive, and SD cards.

	Command or Action	Purpose
		To execute a specific diagnostic test on the server, use the **run** *test-name* command where *test-name* can be one of the following: • **cpux64**—CPU diagnostic test. • **diskx64**—Block devices diagnostic test. Block devices include hard drive, USB drive, and SD cards. • **memoryx64**—Memory diagnostic test. **Note** Diagnostic tests can run for approximately 10 minutes.
Step 6	(Optional) Server: SRV > **results**	Displays a summary of the diagnostic test with **Passed** or **Failed** test status. **Note** The summary report indicates the number of tests that failed and passed. It does not provide information about which tests failed or passed. To determine which tests failed and passed, see the output of the **run all** command.
Step 7	(Optional) Server: SRV > **show**	Displays a list of global parameters and diagnostic test modules that were administered on the server.
Step 8	Server: SRV > **exit**	Exits from Diagnostic Shell.
Step 9	Open a service request with Cisco TAC.	If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco TAC to isolate the problem. If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.

This example runs all diagnostic tests:

```
Shell > dir fs1:
  06/27/12  07:48p            1,435,424  Dsh.efi
  06/27/12  08:03p               10,036  dsh-e140d.pkg
  06/25/12  06:00p               10,140  dsh-e140s.pkg
  06/27/12  08:04p               10,042  dsh-e160d.pkg
          4 File(s)   1,465,642 bytes
Shell > fs1:
fs1:\> cp dsh-e140d.pkg dsh.pkg
copying fs0:\OBD\dsh-e140d.pkg -> fs0:\OBD\dsh.pkg
- [ok]
fs1:\> dsh
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk datacorruption during
power or equipment failure when the tests are in progress. Therefore, before
executing these tests, we highly recommend that you backup the data.


For questions or concerns with this utility, please open a Service Request
with Cisco TAC at http://www.cisco.com/cisco/web/support/index.html
```

```
(Y)es to continue test. (N)o to exit(y/n): Y
Cisco Diagnostics  Shell 1.03(0.3) Thu 06/28/-16:35:08.95-canis-diag@cisco.com
UCS-E140D-M1/K9:SRV>

Server: SRV > run all
Server: SRV > results
Test Name          : all
Test Status        : Passed
Failed/Run History : 0/17
Start Time         : 06/27/12 14:38:19
End Time           : 06/27/12 14:43:36
Diag Version       : 1.03(0.3) Mon 04/02/-17:07:57.19-canis-diag@cisco.com
Board S/N          : FOC160724BY

Server: SRV > show
Server: SRV > exit
```

What to Do Next

Reset the virtual media boot order to its original setting.

INDEX

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W