

Installing the Server

This chapter describes how to install the server, and it includes the following sections:

- [Unpacking and Inspecting the Server, page 2-2](#)
- [Preparing for Server Installation, page 2-3](#)
- [Installing the Server In a Rack, page 2-5](#)
- [Initial Server Setup, page 2-8](#)
- [NIC Modes and NIC Redundancy Settings, page 2-12](#)
- [System BIOS and CIMC Firmware, page 2-13](#)
- [Updating the BIOS and CIMC Firmware, page 2-13](#)
- [Service Headers and Jumpers, page 2-15](#)



Note

Before you install, operate, or service a server, review the [Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers](#) for important safety information.



Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.
Statement 1071

SAVE THESE INSTRUCTIONS

Unpacking and Inspecting the Server


Caution

When handling internal server components, wear an ESD strap and handle modules by the carrier edges only.


Tip

Keep the shipping container in case the server requires shipping in the future.

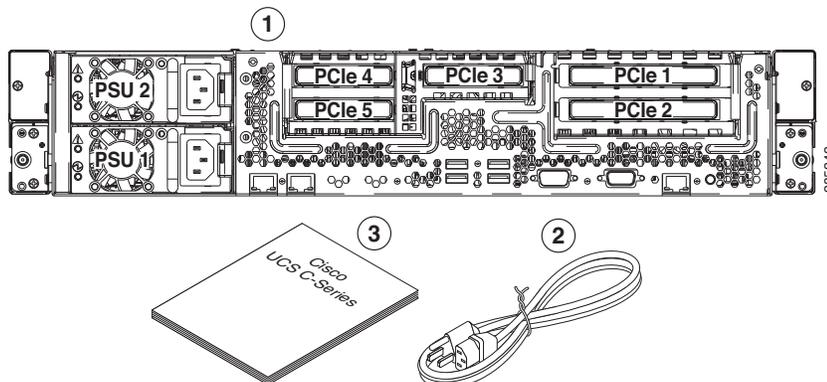

Note

The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

To inspect the shipment, follow these steps:

- Step 1** Remove the server from its cardboard container and save all packaging material.
- Step 2** Compare the shipment to the equipment list provided by your customer service representative and [Figure 2-1](#). Verify that you have all items.
- Step 3** Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:
- Invoice number of shipper (see the packing slip)
 - Model and serial number of the damaged unit
 - Description of damage
 - Effect of damage on the installation

Figure 2-1 Shipping Box Contents



1	Server	3	Documentation
2	Power cord (optional, up to two)		—

Preparing for Server Installation

This section provides information about preparing for server installation, and it includes the following topics:

- [Installation Guidelines, page 2-3](#)
- [Rack Requirements, page 2-4](#)
- [Equipment Requirements, page 2-4](#)
- [Slide Rail Adjustment Range, page 2-4](#)

Installation Guidelines



Warning

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 35° C (95° F).

Statement 1047



Warning

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

Statement 1019



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.

Statement 1005



Warning

Installation of the equipment must comply with local and national electrical codes.

Statement 1074

When you are installing a server, use the following guidelines:

- Plan your site configuration and prepare the site before installing the server. See the [Cisco UCS Site Preparation Guide](#) for the recommended site planning tasks.
- Ensure that there is adequate space around the server to allow for servicing the server and for adequate airflow. The airflow in this server is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the [Server Specifications](#).
- Ensure that the cabinet or rack meets the requirements listed in the “[Rack Requirements](#)” section on [page 2-4](#).
- Ensure that the site power meets the power requirements listed in the [Server Specifications](#). If available, you can use an uninterruptible power supply (UPS) to protect against power failures.



Caution

Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

Rack Requirements

This section provides the requirements for the standard open racks.

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per server must be one RU, equal to 1.75 in. (44.45 mm).

Equipment Requirements

The slide rails supplied by Cisco Systems for this server do not require tools for installation. The inner rails (mounting brackets) are pre-attached to the sides of the server.

Slide Rail Adjustment Range

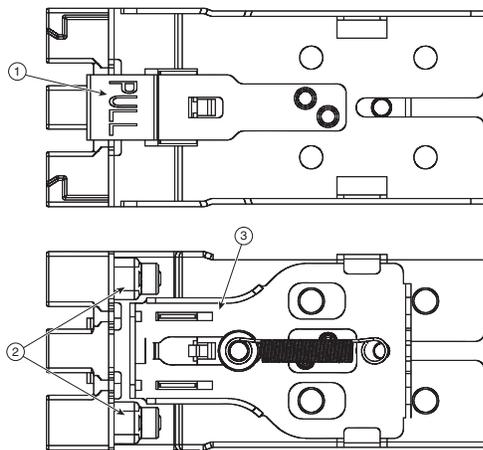
The slide rails for this server have an adjustment range of 24 to 36 inches (610 to 914 mm).

Installing the Server In a Rack

To install the slide rails and the server into a rack, follow these steps:

- Step 1** Open the front securing latch (see [Figure 2-2](#)). The end of the slide-rail assembly marked “FRONT” has a spring-loaded securing latch that must be open before you can insert the mounting pegs into the rack-post holes.
- On the rear side of the securing-latch assembly, hold open the clip marked “PULL.”
 - Slide the spring-loaded securing latch away from the mounting pegs.
 - Release the clip marked “PULL” to lock the securing latch in the open position.

Figure 2-2 Front Securing Latch



1	Clip marked “PULL” on rear of assembly	3	Spring-loaded securing latch on front of assembly
2	Front mounting pegs		

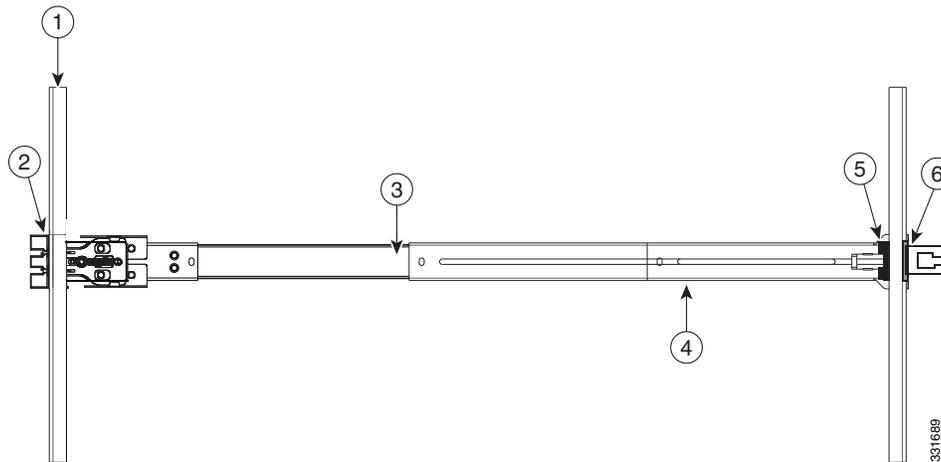
- Step 2** Install the slide rails onto the rack:
- Position a slide-rail assembly inside the two left-side rack posts (see [Figure 2-3](#)).
Use the “FRONT” and “REAR” markings on the slide-rail assembly to orient the assembly correctly with the front and rear rack posts.
 - Position the front mounting pegs so that they enter the desired front rack-post holes from the front.



Note

The mounting pegs that protrude through the rack-post holes are designed to fit round or square holes, or smaller #10-32 round holes when the mounting peg is compressed. If your rack has #10-32 rack-post holes, align the mounting pegs with the holes and then compress the spring-loaded pegs to expose the #10-32 inner peg.

- Expand the length-adjustment bracket until the rear mounting pegs protrude through the desired holes in the rear rack post.
Use your finger to hold the rear securing latch open when you insert the rear mounting pegs to their holes. When you release the latch, it wraps around the rack post and secures the slide-rail assembly.

Figure 2-3 Attaching a Slide-Rail Assembly

1	Front-left rack post	4	Length-adjustment bracket
2	Front mounting pegs	5	Rear mounting pegs
3	Slide-rail assembly	6	Rear securing latch

- d. Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are level and at the same height with each other.
- e. Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 3 Insert the server into the slide rails:

Note The inner rails are pre-attached to the sides of the server at the factory. You can order replacement inner rails if these are damaged or lost (Cisco PID UCSC-RAIL1-I).

- a. Align the inner rails that are attached to the server sides with the front ends of the empty slide rails.
- b. Push the server into the slide rails until it stops at the internal stops.
- c. Push in the plastic release clip on each inner rail (labelled PUSH), and then continue pushing the server into the rack until its front latches engage the rack posts.

Step 4 Attach the (optional) cable management arm (CMA) to the rear of the slide rails:

Note The CMA is designed for mounting on either the right or left slide rails. These instructions describe an installation to the rear of the right slide rails, as viewed from the rear of server.

- a. Slide the plastic clip on the inner CMA arm over the flange on the mounting bracket that attached to the side of the server. See [Figure 2-4](#).

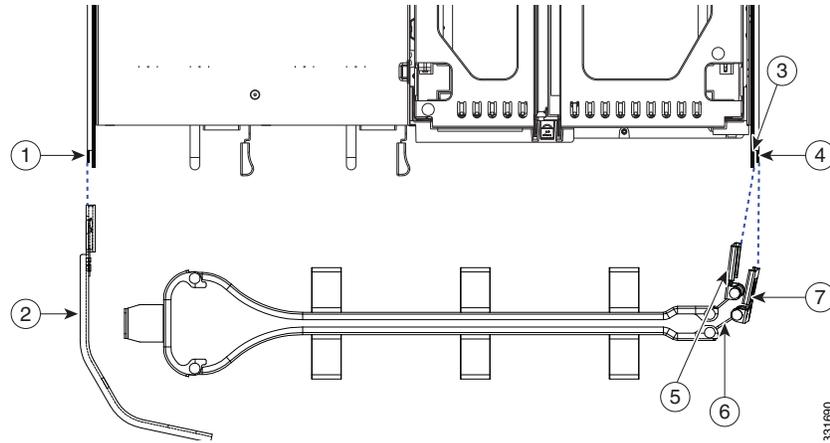


Note Whether you are mounting the CMA to the left or right slide rails, be sure to orient the engraved marking, “UP” so that it is always on the upper side of the CMA. See [Figure 2-4](#).

- b. Slide the plastic clip on the outer CMA arm over the flange on the slide rail. See [Figure 2-4](#).

- c. Attach the CMA retaining bracket to the left slide rail. Slide the plastic clip on the bracket over the flange on the end of the left slide rail. See [Figure 2-4](#).

Figure 2-4 Attaching the Cable Management Arm (Rear of Server Shown)



1	Flange on rear of outer left slide rail	5	Inner CMA arm attachment clip
2	CMA retaining bracket	6	“UP” orientation marking
3	Flange on rear of right mounting bracket	7	Outer CMA arm attachment clip
4	Flange on rear of outer right slide rail		

Step 5 Continue with the [“Initial Server Setup”](#) section on page 2-8.

Initial Server Setup

Connecting and Powering On the Server (Standalone Mode)

The server is shipped with these default settings:

- The NIC mode is Shared LOM EXT.
Shared LOM EXT mode enables the 1-Gb Ethernet ports and the ports on any installed Cisco virtual interface card (VIC) to access the Cisco Integrated Management Interface (Cisco IMC). If you want to use the 10/100 dedicated management ports to access the Cisco IMC, you can connect to the server and change the NIC mode as described in [Step 4](#) of the following procedure.
- The NIC redundancy is active-active. All Ethernet ports are utilized simultaneously.
- DHCP is enabled.
- Internet protocol version 4 (IPv4) is enabled.

Use the following procedure to perform initial setup of the server:

Step 1 Attach a supplied power cord to each power supply in your server, and then attach the power cord to a grounded AC power outlet. See the [Power Specifications, page A-2](#) for power specifications.

Wait for approximately two minutes to let the server boot in standby power during the first bootup.

You can verify power status by looking at the Power Status LED (see [Figure 1-1 on page 1-2](#)):

- Off—There is no AC power present in the server.
- Amber—The server is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.
- Green—The server is in main power mode. Power is supplied to all server components.



Note During bootup, the server beeps once for each USB device that is attached to the server. Even if there are no external USB devices attached, there is a short beep for each virtual USB device such as a virtual floppy drive, CD/DVD drive, keyboard, or mouse. A beep is also emitted if a USB device is hot-plugged or hot-unplugged during BIOS power-on self test (POST), or while you are accessing the BIOS Setup utility or the EFI shell.

Step 2 Connect a USB keyboard and VGA monitor to the server.

- Step 3** Open the Cisco IMC Configuration Utility:
- Press the **Power** button to boot the server. Watch for the prompt to press F8.
 - During bootup, press **F8** when prompted to open the Cisco IMC Configuration Utility. Note the differences between versions of Cisco IMC firmware:
 - In Cisco IMC 2.0(1) and later, there are two windows for this utility that you can switch between by pressing F1 or F2 (see [Figure 2-5](#) for sample windows). The IPv4 and IPv6 protocols and dynamic domain name system (DDNS) are supported. You can also define a host name and a DDNS domain.
 - In Cisco IMC earlier than release 2.0(1), there is only one window for this utility. Only the IPv4 protocol is supported. DDNS is not supported.

**Note**

The first time that you enter the Cisco IMC Configuration Utility, you are prompted to change the default password. The default password is *password*. The Strong Password feature is enabled.

The following are the requirements for Strong Password:

- The password can have minimum 8 characters; maximum 14 characters.
- The password must not contain the user's name.
- The password must contain characters from three of the following four categories:
 - English uppercase letters (A through Z).
 - English lowercase letters (a through z).
 - Base 10 digits (0 through 9).
 - Non-alphabetic characters !, @, #, \$, %, ^, &, *, -, _, =, “

Figure 2-5 Cisco IMC Configuration Utility Window 1 and Window 2 (Cisco IMC 2.0(1) and Later)

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode
Dedicated: [ ]
Shared LOM: [X]
Cisco Card: [ ]
Shared LOM Ext: [ ]
IP (Basic)
IPv4: [ ] IPv6: [X]
DHCP enabled: [ ]
CIMC IP: 2010:201::299
Prefix/Subnet: 64
Gateway: 2010:201::1
Pref DNS Server: ::
VLAN (Advanced)
VLAN enabled: [X]
VLAN ID: 201
Priority: 0
*****
<Up/Down>Selection <F10>Save <Space>Enable/Disable <F5>Refresh <ESC>Exit
<F1>Additional settings

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
Hostname: C220-FCH1612V0VQ
Dynamic DNS: [X]
DDNS Domain:
FactoryDefaults
Factory Default: [ ]
Default User(Basic)
Default password:
Reenter password:
Port Properties
Auto Negotiation: [ ]
Speed[1000/100 Mbps]: 100
Duplex mode[half/full]: full
Port Profiles
Reset: [ ]
Name:
*****
<Up/Down>Selection <F10>Save <Space>Enable/Disable <F5>Refresh <ESC>Exit
<F2>PreviousPage
  
```

- Step 4** Set NIC mode and NIC redundancy:
- Set the NIC mode to your choice for which ports to use to access the CIMC for server management (see [Figure 1-3](#) for identification of the ports):
 - Shared LOM EXT (default)—This is shared LOM extended mode. This is the factory-default setting, along with Active-active NIC redundancy and DHCP-enabled. With this mode, the shared LOM and Cisco Card interfaces are both enabled.

In this mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco card are disabled. Use the Cisco Card NIC mode if you want to connect to the CIMC through a Cisco card in standalone mode.

- **Dedicated**—The dedicated management port is used to access the CIMC. You must select a NIC redundancy and IP setting.
- **Shared LOM**—The 1-Gb Ethernet ports are used to access the CIMC. You must select a NIC redundancy and IP setting.
- **Cisco Card**—The ports on an installed Cisco UCS virtual interface card (VIC) are used to access the CIMC. You must select a NIC redundancy and IP setting.



Note The Cisco Card NIC mode is currently supported only with a Cisco UCS VIC that is installed in PCIe slot 2. See also [Special Considerations for Cisco UCS Virtual Interface Cards, page 3-38](#).

- b. Use this utility to change the NIC redundancy to your preference. This server has three possible NIC redundancy settings:
- **None**—The Ethernet ports operate independently and do not fail over if there is a problem.
 - **Active-standby**—If an active Ethernet port fails, traffic fails over to a standby port.
 - **Active-active**—All Ethernet ports are utilized simultaneously. See [NIC Modes and NIC Redundancy Settings, page 2-12](#) for more information.

Step 5 Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.



Note Before you enable DHCP, your DHCP server must be preconfigured with the range of MAC addresses for this server. The MAC address is printed on a label on the rear of the server. This server has a range of six MAC addresses assigned to the Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.



Note In Cisco IMC 2.0(1) and later, you can choose whether to use IPv4 or IPv6 IP addresses by checking either the IPv4 or IPv6 check box.

The static IPv4 and IPv6 settings include:

- The Cisco IMC IP address.
- The prefix/subnet.
For IPv6, valid values are 1–127.
- The gateway.
For IPv6, if you do not know the gateway, you can set it as none by typing :: (two colons).
- The preferred DNS server address.
For IPv6, you can set this as none by typing :: (two colons).

Step 6 Optional: Use this utility to make VLAN settings.

Step 7 Continue with the next action based on which release of Cisco IMC your server is running:

- Cisco IMC earlier than release 2.0(1)—Skip to [Step 14](#).

- Cisco IMC 2.0(1) and later—Press **F1** to go to the second settings window, then continue with the next step. From the second window, you can press **F2** to switch back to the first window.

Step 8 Optional: Set a host name for the server.

Step 9 Optional: Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 10 Optional: If you select the Factory Default check box, the server will be set back to the factory defaults.

Step 11 Optional: Set a default user password.

Step 12 Optional: Enable auto-negotiation of port settings or set the port speed and duplex mode manually.



Note Auto-negotiation is applicable only when you use the *Dedicated* NIC mode. Auto-negotiation sets the port speed and duplex mode automatically based on the switch port to which the server is connected. If you disable auto-negotiation, you must set the port speed and duplex mode manually.

Step 13 Optional: Reset port profiles and the port name.

Step 14 Press **F5** to refresh the settings you made. You might have to wait about 45 seconds until the new settings appear and the message, `Network settings configured` is displayed before you reboot the server in the next step.

Step 15 Press **F10** to save your settings and reboot the server.



Note If you chose to enable DHCP, the dynamically assigned IP and MAC addresses are displayed on the console screen during bootup.

Step 16 Connect to the CIMC for server management. Connect Ethernet cables from your LAN to the server by using the ports that you selected by your NIC Mode setting in [Step 4](#). The Active-active and Active-passive NIC redundancy settings require you to connect to two ports.

Step 17 Use a browser and the IP address of the CIMC to connect to the CIMC Setup Utility. The IP address is based upon the settings that you made in [Step 4](#) (either a static address or the address assigned by your DHCP server).



Note The default user name for the server is *admin*. The default password is *password*.

To manage the server, see the *Cisco UCS C-Series Rack-Mount Server Configuration Guide* or the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide* for instructions on using those interfaces. The links to these documents are in the C-Series documentation roadmap:

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

NIC Modes and NIC Redundancy Settings

This server has the following NIC mode settings that you can choose from:

- **Shared LOM EXT (default)**—This is shared LOM extended mode. This is the factory default setting, along with Active-active NIC redundancy and DHCP-enabled. With this mode, the shared LOM and Cisco Card interfaces are both enabled.

In this mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco card are disabled. If the system determines that the Cisco card connection is getting its IP address from a Cisco UCS Manager system, the reply has parameters that automatically move the server to UCSM mode.

- **Dedicated**—The dedicated management port is used to access the CIMC. You must select a NIC redundancy and IP setting.
- **Shared LOM**—The 1-Gb Ethernet ports are used to access the CIMC. You must select a NIC redundancy and IP setting.
- **Cisco Card**—The ports on an installed Cisco UCS virtual interface card (VIC) are used to access the CIMC. You must select a NIC redundancy and IP setting.



Note The Cisco Card NIC mode is currently supported only with a Cisco UCS VIC that is installed in PCIe slot 2. See also [Special Considerations for Cisco UCS Virtual Interface Cards, page 3-38](#).

This server has the following NIC redundancy settings that you can choose from:

- **None**—The Ethernet ports operate independently and do not fail over if there is a problem.
- **Active-standby**—If an active Ethernet port fails, traffic fails over to a standby port.
- **Active-active**—All Ethernet ports are utilized simultaneously.

The active/active setting uses Mode 5 or Balance-TLB (adaptive transmit load balancing). This is channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

System BIOS and CIMC Firmware

This section includes information about the system BIOS and it includes the following sections:

- [Updating the BIOS and CIMC Firmware, page 2-13](#)
- [Accessing the System BIOS, page 2-14](#)

Updating the BIOS and CIMC Firmware



Caution

When you upgrade the BIOS firmware, you must also upgrade the CIMC firmware to the same version or the server will not boot. Do not power off the server until the BIOS and CIMC firmware are matching or the server will not boot.

Cisco provides the Cisco Host Upgrade Utility to assist with simultaneously upgrading the BIOS, CIMC, and other firmware to compatible levels.

The server uses firmware obtained from and certified by Cisco. Cisco provides release notes with each firmware image. There are several methods for updating the firmware:

- **Recommended method for systems running firmware level 1.2 or later:** Use the Cisco Host Upgrade Utility to simultaneously upgrade the CIMC, BIOS, LOM, LSI storage controller, and Cisco UCS P81E VIC firmware to compatible levels.

See the *Cisco Host Upgrade Utility Quick Reference Guide* for your firmware level at the documentation roadmap link below.



Note

Your system firmware must be at minimum level 1.2 to use the Cisco Host Upgrade Utility. If your firmware is prior to level 1.2, you must use the methods below to update the BIOS and CIMC firmware individually.

- You can upgrade the BIOS using the EFI interface, or upgrade from a Windows or Linux platform. See the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*.
- You can upgrade the CIMC and BIOS firmware by using the CIMC GUI interface. See the *Cisco UCS C-Series Rack-Mount Server Configuration Guide*.
- You can upgrade the CIMC and BIOS firmware by using the CIMC CLI interface. See the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide*.

For links to the documents listed above, see the documentation roadmap at the following URL:

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

Accessing the System BIOS

To change the BIOS settings for your server, follow these steps. Detailed instructions are also printed on the BIOS screens.

Step 1 Enter the BIOS setup utility by pressing the **F2** key when prompted during bootup.



Note The version and build of the current BIOS are displayed on the Main page of the utility.

Step 2 Use the arrow keys to select the BIOS menu page.

Step 3 Highlight the field to be modified by using the arrow keys.

Step 4 Press **Enter** to select the field that you want to change, and then modify the value in the field.

Step 5 Press the right arrow key until the Exit menu screen is displayed.

Step 6 Follow the instructions on the Exit menu screen to save your changes and exit the setup utility (or Press **F10**). You can exit without saving changes by pressing **Esc**.

Service Headers and Jumpers

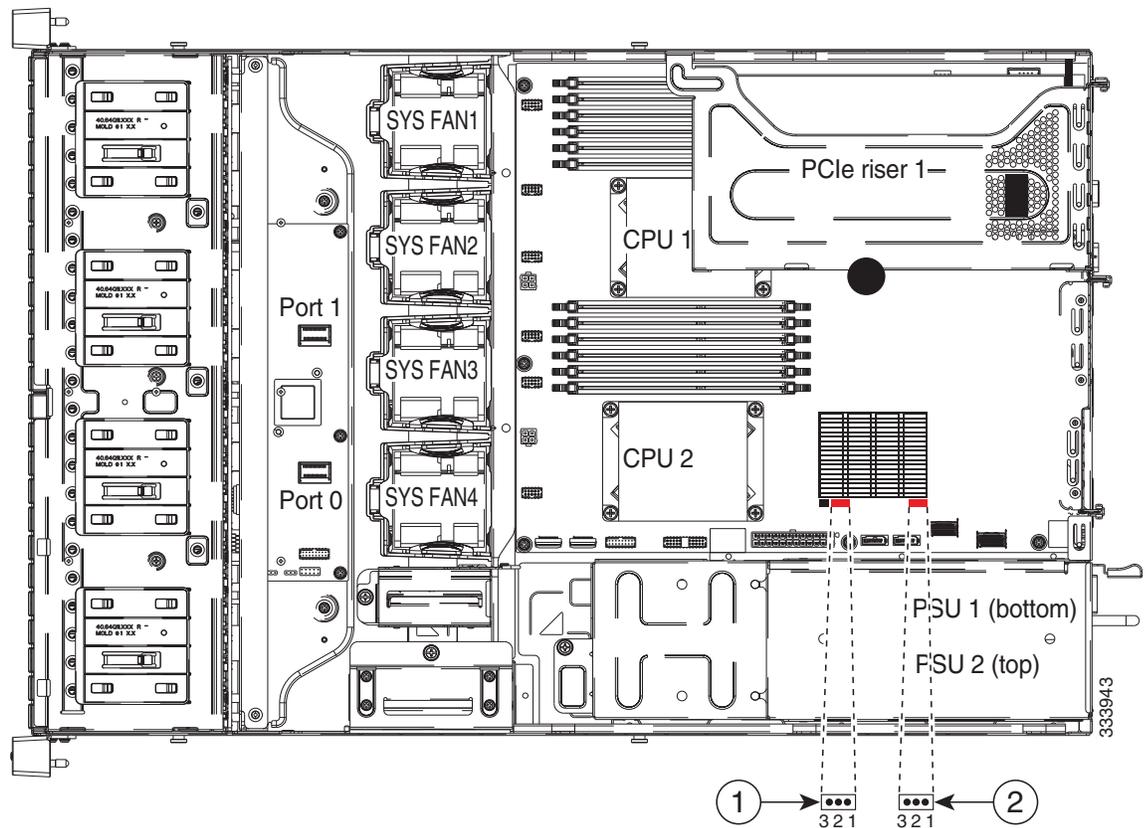
This section includes the following topics:

- [Header Location on the Motherboard, page 2-15](#)
- [Using the BIOS Recovery Header CN34, page 2-16](#)
- [Using the Clear CMOS Header CN14, page 2-19](#)

Header Location on the Motherboard

See [Figure 2-6](#). The headers are shown in red on the motherboard, with PCIe riser 2 removed. The header pins are shown in the magnified view.

Figure 2-6 Service Header Locations



1	CN34 BIOS Recovery	2	CN14 Clear CMOS
---	--------------------	---	-----------------

Using the BIOS Recovery Header CN34

Depending on which stage the BIOS becomes corrupted, you might see different behavior.

- If the BIOS BootBlock is corrupted, you might see the system get stuck on the following message:

```
Initializing and configuring memory/hardware
```

- If it is a non-BootBlock corruption, the following message is displayed:

```
****BIOS FLASH IMAGE CORRUPTED****
Flash a valid BIOS capsule file using CIMC WebGUI or CLI interface.
IF CIMC INTERFACE IS NOT AVAILABLE, FOLLOW THE STEPS MENTIONED BELOW.
1. Connect the USB stick with recovery.cap file in root folder.
2. Reset the host.
IF THESE STEPS DO NOT RECOVER THE BIOS
1. Power off the system.
2. Mount recovery jumper.
3. Connect the USB stick with recovery.cap file in root folder.
4. Power on the system.
Wait for a few seconds if already plugged in the USB stick.
REFER TO SYSTEM MANUAL FOR ANY ISSUES.
```



Note

As indicated by the message shown above, there are two procedures for recovering the BIOS. Try procedure 1 first, then if that does not recover the BIOS, use procedure 2.



Note

The server must have CIMC version 1.4(6) or later to use these procedures.

Procedure 1: Reboot With recovery.cap File

- Step 1** Download the BIOS update package and extract it to a temporary location.
- Step 2** Copy the contents of the extracted `recovery` folder to the root directory of a USB thumb drive. The `recovery` folder contains the `recovery.cap` file that is required in this procedure.



Note

The `recovery.cap` file must be in the root directory of the USB thumb drive. Do not rename this file. The USB thumb drive must be formatted with either FAT16 or FAT32 file systems.

- Step 3** Insert the USB thumb drive into a USB port on the server.
- Step 4** Reboot the server.
- Step 5** Return the server to main power mode by pressing the **Power** button on the front panel.

The server boots with the updated BIOS boot block. When the BIOS detects a valid `recovery.cap` file on the USB thumb drive, it displays this message:

```
Found a valid recovery file...Transferring to CIMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds...
```

- Step 6** Wait for server to complete the BIOS update, then remove the USB thumb drive from the server.

**Note**

During the BIOS update, the CIMC will shut down the server and the screen will be blank for about 10 minutes. Do not unplug the power cords during this update. The CIMC will power on the server after the update is complete.

Procedure 2: Use Recovery Jumper and recovery.cap File

See [Figure 2-6](#) for the location of the CN34 header.

-
- Step 1** Download the BIOS update package and extract it to a temporary location.
- Step 2** Copy the contents of the extracted `recovery` folder to the root directory of a USB thumb drive. The `recovery` folder contains the `recovery.cap` file that is required in this procedure.
-  **Note** The `recovery.cap` file must be in the root directory of the USB thumb drive. Do not rename this file. The USB thumb drive must be formatted with either FAT16 or FAT32 file systems.
-
- Step 3** Power off the server as described in [Shutting Down and Powering Off the Server, page 3-6](#).
- Step 4** Disconnect all power cords from the power supplies.
- Step 5** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
-  **Caution** If you cannot safely view and access the component, remove the server from the rack.
-
- Step 6** Remove the top cover as described in [Removing and Replacing the Server Top Cover, page 3-7](#).
- Step 7** Move the shorting jumper to pins 2 and 3 of the CN34 header (see [Figure 2-6](#)).
- Step 8** Reconnect AC power cords to the server. The server powers up to standby power mode.
- Step 9** Insert the USB thumb drive that you prepared in [Step 2](#) into a USB port on the server.
- Step 10** Return the server to main power mode by pressing the **Power** button on the front panel.
- The server boots with the updated BIOS boot block. When the BIOS detects a valid `recovery.cap` file on the USB thumb drive, it displays this message:
- ```
Found a valid recovery file...Transferring to CIMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds...
```
- Step 11** Wait for server to complete the BIOS update, then remove the USB thumb drive from the server.
-  **Note** During the BIOS update, the CIMC will shut down the server and the screen will be blank for about 10 minutes. Do not unplug the power cords during this update. The CIMC will power on the server after the update is complete.
- 
- Step 12** After the server has fully booted, power off the server again and disconnect all power cords.
- Step 13** Move the jumper back to the default pins 1 and 2 of the header.
-  **Note** If you do not move the jumper, after recovery completion you see the prompt, `Please remove the recovery jumper`.
- 
- Step 14** Replace the top cover, replace the server in the rack, replace power cords and any other cables, then power on the server by pressing the **Power** button.

## Using the Clear CMOS Header CN14

See [Figure 2-6](#) for the location of this header. You can jumper this header to clear the server's CMOS settings in the case of a system hang. For example, if the server hangs because of incorrect settings and does not boot, use this jumper to invalidate the settings and reboot with defaults.

**Caution**

Clearing the CMOS removes any customized settings and might result in data loss. Make a note of any necessary customized settings in the BIOS before you use this clear CMOS procedure.

- Step 1** Power off the server as described in [Shutting Down and Powering Off the Server, page 3-6](#).
- Step 2** Disconnect all power cords from the power supplies.
- Step 3** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

**Caution**

If you cannot safely view and access the component, remove the server from the rack.

- Step 4** Remove the top cover as described in [Removing and Replacing the Server Top Cover, page 3-7](#).
- Step 5** Move the shorting jumper to pins 2 and 3 of the CN14 header (see [Figure 2-6](#)).
- Step 6** Reinstall the top cover and reconnect AC power cords to the server. The server powers up to standby power mode, indicated when the Power LED on the front panel is amber.
- Step 7** Return the server to main power mode by pressing the **Power** button on the front panel. The server is in main power mode when the Power LED is green.

**Note**

You must allow the entire server, not just the service processor, to reboot to main power mode to complete the reset. This is because the state of the jumper cannot be determined without the host CPU running.

- Step 8** Press the **Power** button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.
- Step 9** Remove the top cover from the server.
- Step 10** Move the shorting jumper from header pins 2 and 3, back to its default position on pins 1 and 2.

**Note**

If you do not move the jumper, the CMOS settings are reset to the default every time that you power-cycle the server.

- Step 11** Replace the top cover, replace the server in the rack, replace power cords and any other cables, then power on the server by pressing the **Power** button.

