Cisco UCS C-Series Server Integration with Cisco UCS Manager 2.0(2) and 2.0(3)

First Published: August 07, 2012

Last Modified: November 25, 2014

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-27660-01

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

Conventions

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

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

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

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

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 IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

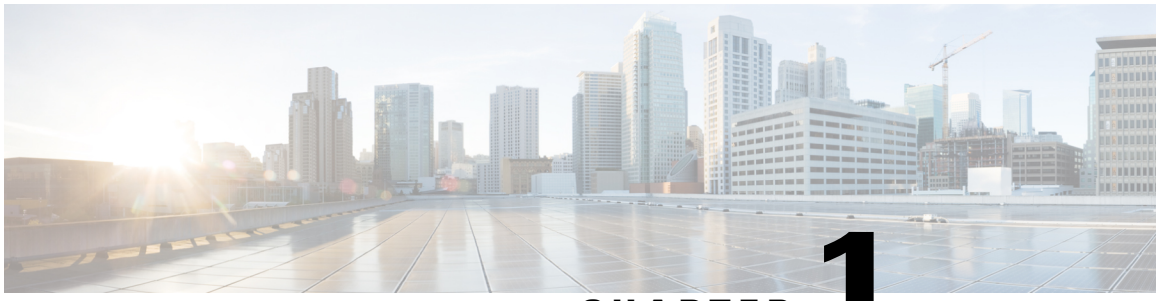
For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Other Documentation Resources

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

Documentation Feedback

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



CHAPTER 1

Cisco UCS C-Series Integration with Cisco UCS Manager

This chapter includes the following sections:

Overview

This guide contains information and procedures for installing Cisco UCS Rack Mount Servers releases 1.4.3c, 1.4.4a and 1.4.5d for integration with Cisco UCS Manager release 2.0.2(2).

Cisco UCS C-Series Rack-Mount Servers are managed by the built-in standalone software, Cisco Integrated Management Controller (CIMC) . When a C-Series Rack-Mount Server is integrated with Cisco UCS Manager, the CIMC does not manage the server anymore. Instead it is managed with the Cisco UCS Manager software. You will manage the server using the Cisco UCS Manager GUI or Cisco UCS Manager CLI.

Important If your server is not factory new, make sure to reset the CIMC to factory default settings before integrating the server with Cisco UCS Manager.

You can integrate Cisco UCS C-Series Rack-Mount Servers with Cisco UCS Manager in either one of the following setup:

- **Cluster setup**: Using two fabric extenders (FEXes) to connect the C-Series Rack-Mount Server with two fabric interconnects.
- **Non-cluster setup**: Connecting the C-Series Rack-Mount Server with one FEX and one FI.

Integrating Release 1.4.3c or 1.4.4a or 1.4.5d Servers with Cisco UCS Manager 2.0(2) and 2.0(3)

The prerequisites for integration with Cisco UCS Manager are built into the C-Series Rack-Mount Server releases 1.4.3c, 1.4.4a and 1.4.5d. You can connect them to the Cisco UCS Manager 2.0.2 domain immediately. If your server is at a release that does not support integration with Cisco UCS Manager 2.0.2 or 2.0.3 , you must upgrade your server to the required release level for integration. For more information on required server CIMC version, see Required Items for Integration with Cisco UCS Manager 2.0(2) and 2.0(3), on page 2. For more information on upgrading the CIMC release for integration, see Upgrading and Connection Procedures, on page 12.

Note The LOM ports on Cisco UCS C-Series Rack-Mount Servers integrated with Cisco UCS Manager can not be used for data traffic.

See the following URLs for additional information about the equipment in this configuration.

For information about the Cisco UCS 6100 Series or 6200 Series fabric interconnects (FIs) in the configuration, see the documentation at the following links:

- Cisco UCS 6100 Series Fabric Interconnect documentation
- Cisco UCS 6200 Series Fabric Interconnect documentation

For information about the Cisco Nexus 2232PP fabric extenders (FEXes) in the configuration, see the documentation at the following link:

Cisco Nexus 2000 Series Fabric Extender documentation

Required Items for Integration with Cisco UCS Manager 2.0(2) and 2.0(3)

The following are the required items for C-Series server CIMC versions 1.4.3c, 1.4.4a, 1.4.5d to be integration with Cisco UCS Manager versions 2.0.2 and 2.0(2):

Note The hardware configuration will contain redundant network fabrics and paths for both management traffic and data traffic.

- A Cisco UCS system running Cisco UCS Manager software release 2.0(2) or 2.0(3).

- Any of the Cisco UCS C-Series servers and corresponding Cisco UCS Manager release version:

Server	CIMC Version	Minimum UCS Manager Version
Cisco UCS C22 M3 Server	1.4.5d	2.0(3)
Cisco UCS C24 M3 Server	1.4.5d	2.0(3)
Cisco UCS C200 M2 Server	1.4.3c	2.0(2)
Cisco UCS C210 M2 Server	1.4.3c	2.0(2)
Cisco UCS C220 M3 Server	1.4.4a	2.0(2)
Cisco UCS C240 M3 Server	1.4.4a	2.0(2)
Cisco UCS C250 M2 Server	1.4.3c	2.0(2)
Cisco UCS C260 M2 Server	1.4.3c	2.0(2)
Cisco UCS C460 M2 Server	1.4.3c	2.0(2)

Note

- When the Cisco UCS C-Series server is discovered, check if the firmware package is at the required level for the Cisco UCS Manager version. If not, you must update or downgrade to the required firmware level.
- If you install Cisco UCS P81E Virtual Interface Card (N2XX-ACPCI01), and want to use this card for UCS integration, the minimum card-firmware level requirement is 2.0(2g). See the section on Special Considerations for the Cisco UCS P81E Virtual Interface Card (N2XX-ACPCI01), in Install and Upgrade Guides.

- Two Cisco UCS 6100 Series or 6200 Series FIs. The switch ports that carry server traffic must be enabled as server ports.
- Two Cisco Nexus 2232PP FEXes.

Note

- Cisco UCS Manager releases 2.0.2 and after support only Cisco Nexus 2232PP FEXes. If you have Cisco Nexus 2248 FEX, you must migrate to Cisco Nexus 2232PP FEX.
- You must plug a power cord into each of the two power supplies in the FEX. If a power is connected and there are issues in the hardware, you might see “Major” faults reported during power-on self test (POST). For example, you might see this error: `Power supply 1 in fex 6 power: error`. You can clear these errors by connecting the missing power cord to the FEX power supply.

- Two RJ-45 Ethernet cables.
- Six 10-Gb SFP cables.

Note

- Two cables for linking the data traffic path between server and FEX.
- Four cables for uplinks from FEX to fabric interconnects. Each of these four cables used for uplink from FEX to FIs can either use supported 10-gb twinaxial cable or one of the following SFP type cables:
  - SFP - 10GE-SR
  - FET - 10GE

Important Do not mix SFP types on an uplink. If you mix the SFP types on an uplink, you will see `Discovery Failed` errors.

- Two 1000BASE-T SFP transceivers (GLC-T)

FEX Connection Mode and Discovery

You can connect the FEX to the FI in two ways. Cisco UCS Manager FI discovers the FEX based on the FEX/Chassis discovery mode. The FEX connection modes are:

- **Hard-Pinning mode**: The server facing FEX ports are pinned to the connected uplink ports when the FEX is discovered. Cisco UCS Manager pins the server-facing ports to the uplink ports based on the number of acknowledged uplink ports. After the pinning, if you add a new uplink or delete an existing uplink, you must manually acknowledge the FEX to apply the changes.
- **Port-Channel mode**: Port-Channel mode does not have pinning. A single port channel works as the uplink to all server-facing ports. And all uplink ports are members of this single port channel. If one of the uplink ports go down, the traffic is automatically distributed to another available uplink port.

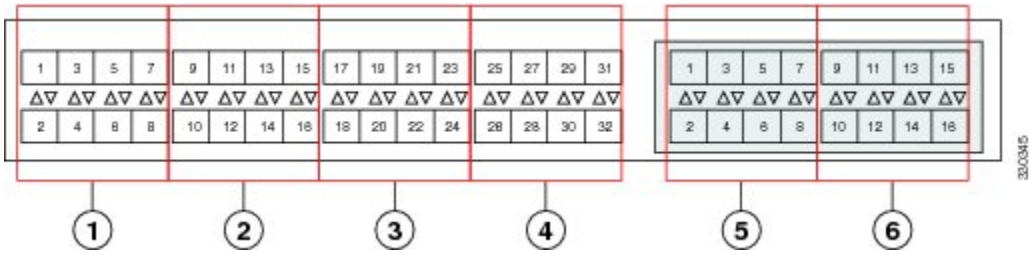
Note Port channel mode applies only to the 6200 series FIs.

In port-channel mode, when you cable between FEX and the FI, the available virtual interface (VIF) namespace varies, depending on where the uplinks are connected to the FI ports:

- When port-channel uplinks from the FEX are connected only within a set of eight ports managed by a single chip, Cisco UCS Manager maximizes the number of VIFs used in service profiles deployed on the servers.
- If uplink connections are distributed across ports managed by separate chips, the VIF count is decreased. For example, if you connect seven members of the port channel to ports 1–7, but the eighth member to port 9, this port channel can only support VIFs as though it had one member.

The Cisco UCS 6200 Series FI has six sets of eight contiguous ports. Each set of ports is managed by a single chip. For more information on FEX discovery policies and port-channel allocation, see the appropriate Cisco UCS Manager Configuration Guide.

Figure 1: Six Sets of Ports in Fabric Interconnect and Expansion Module



Maximum Configurable vNICs/vHBAs Based on Number of FEX Uplinks

The following table describes maximum configurable vNICs/vHBAs based on number of FEX uplinks:

Table 1: Cisco UCS 6100 Fabric Interconnect

Acknowledged link between FEX and FI	Maximum configurable vNICs/vHBA per VIC adapter
1	Not supported
2	4
4	10
8	22

Table 2: Cisco UCS 6200 Fabric Interconnect

Acknowledged link between FEX and FI	Maximum configurable vNICs/vHBA per VIC adapter
1	13
2	28
4	58
8	118

Note For a non-VIC adapter the maximum number of vNICs are 2 and the maximum number of vHBAs are 2.

Supported RAID Controller Configurations

Only servers without expanders can have more than one RAID controllers in the Cisco UCS Manager integrated mode. The following servers are allowed to have more than one RAID controllers in the Cisco UCS Manager integrated mode:

- Cisco UCS C24 M3 (UCSC-C24-M3S2)
- Cisco UCS C420 M3 (UCSC-C420-M3)
- Cisco UCS C240 M3 (UCSC-C240-M3S2)
- Cisco UCS C240 M3 NEBS (UCSC-C240-SNEBS)
- Cisco UCS C260 M2 (C260-BASE-2646)

Any server not on this list that has more than one RAID controllers installed fails discovery.

Connecting the C-Series Server with Cisco UCS Domain in Cluster Setup

Before connecting the server with the Cisco UCS domain, make sure you have the recommended card-firmware level for the integration. The card-firmware level for Cisco UCS P81E Virtual Interface Card must be a minimum 2.0(2g) for the integration. If you do not have this card-firmware level, update the server firmware in stand alone mode before the integration. If you connect a card with earlier firmware version to Cisco UCS Manager 2.0(2x), during the discovery process, you will get discovery and association/disassociation failures. If you encounter these problems, see the upgrade procedure and upgrade the card firmware level.

To view illustrations on the connectivity for each C-Series Rack-Mount Server, see Physical Connectivity Illustrations for Cluster Setup, on page 7.

Important Make sure the server CIMC is set to factory default settings to integrate with Cisco UCS Manager.

Procedure

Step 1 Install the server in the rack. See the *Install and Upgrade Guide* for the server that you are using. The install guides are available at the following url: Install and Upgrade Guides.

Step 2 To connect the management traffic paths, do the following:

a) Insert one GLC-T transceiver into a port of the FEX that is connected to Fabric A. You can use any port on the FEX.

b) Insert one GLC-T transceiver into a port of the FEX that is connected to Fabric B. You can use any port on the FEX.

c) Connect an RJ-45 Ethernet cable between a 1-Gb port on the rear panel of the server and the transceiver that you inserted into the FEX in Fabric A.
d) Connect an RJ-45 Ethernet cable between a 1-Gb port on the rear panel of the server and the transceiver that you inserted into the FEX in Fabric B.

Step 3 To connect the data traffic paths, do the following:

a) Connect a 10-Gb SFP cable between the 10-Gb adapter card in the server and a port on a FEX in Fabric A. You can use any port on the FEX.
b) Connect a 10-Gb SFP cable between the 10-Gb adapter card in the server and a port on a FEX in Fabric B. You can use any port on the FEX.

Step 4 Connect the paths from the FEXes to the FIs. These paths carry both data and management traffic.

a) Connect two 10-Gb SFP cables between FEX A and two ports on FI A. You can use any ports on FI A, but the ports must be enabled for server traffic.
b) Connect two 10-Gb SFP cables between FEX B and two ports on FI B. You can use any ports on FI B, but the ports must be enabled for server traffic.

Note

- On the FEX, you can use only the right block of eight ports for uplinks.
- The maximum number of uplinks is eight. Based on the Cisco UCS Manager FI discovery policy the port cabling requirement between the FEX and FI vary.
- Do not mix SFP types on an uplink. If you do, you will see `Discovery Failed` errors.

Step 5 Attach a power cord to each power supply in your server, and then attach the power cord to a grounded AC power outlet.

Step 6 Reboot the server.

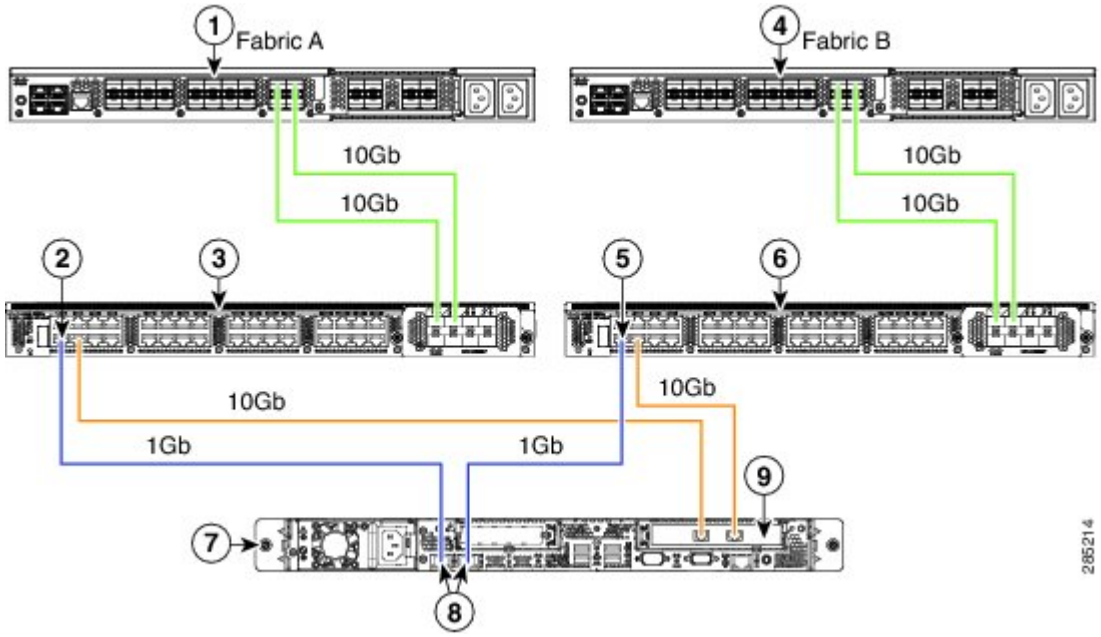
Step 7 To view and configure settings for the server from within the Cisco UCS Manager software, see the information and instructions in the Cisco UCS Manager Configuration Guide for Release 2.0.

Physical Connectivity Illustrations for Cluster Setup

The following image shows a samples of the physical connectivity for C-Series Rack-Mount Server with Cisco UCS Domain, Cisco UCS Manager, release 2.0(2) and above.

This image shows the cabling configuration for Cisco UCS Manager integration with a C-Series Rack-Mount Server. The paths shown in blue carry management traffic. The paths shown in gold carry data traffic.

Figure 2: Cluster Setup Cabling Configuration



1	Cisco UCS 6100 Series or 6200 FI (Fabric A)	6	Cisco Nexus 2232PP FEX (Fabric B)
2	GLC-T transceiver in FEX port (Fabric A)	7	C-Series Rack-Mount Server
3	Cisco Nexus 2232PP FEX (Fabric A)	8	1-Gb Ethernet LOM ports
4	Cisco UCS 6100 Series or 6200 FI (Fabric B)	9	10-Gb Adapter card in supported PCIe slot
5	GLC-T transceiver in FEX port (Fabric B)		

Managing the Rack-Mount Server in Cisco UCS Manager after Integration

You can manage and monitor all rack-mount servers that have been integrated with a Cisco UCS domain through Cisco UCS Manager. After the integration, you will perform all rack-mount server management tasks only through the service profiles from Cisco UCS Manager GUI or Cisco UCS Manager CLI. The C-Series Rack-Mount Server Cisco IMC is not accessible when you start managing the server with Cisco UCS Manager.

Cisco UCS Manager provides information, errors, and faults for each rack-mount server that it has discovered.

For more information on managing C-Series Rack-Mount Servers from Cisco UCS Manager, see the chapter on Managing Rack-Mount Servers in your release specific Cisco UCS Manager Configuration Guide.

Reverting a Server From Cisco UCS Domain Mode to Standalone Mode

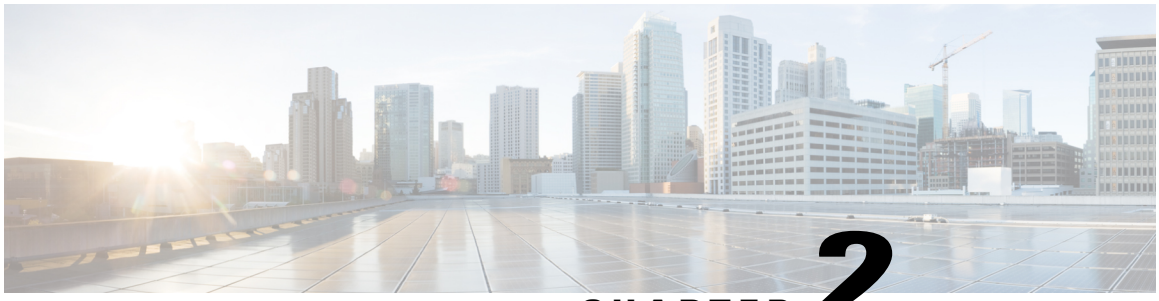
When you manage a Cisco UCS C-Series server with Cisco UCS Manager software, a UCS Manager service profile is associated with the server. If you want to revert a C-Series server to standalone mode (so that it can be managed by CIMC software), you must do the following actions in UCS Manager:

Procedure

Step 1 Disassociate the UCS Manager service profile from the server.

Step 2 Decommission the server.

Caution If you do not disassociate the service profile from the server, MAC and WWN numbers assigned by UCS Manager might be kept by the server. This can cause numbering duplication and conflicts with other servers that are managed by UCS Manager. Also, if you revert a server to standalone mode without disassociating its service profile, any LSI RAID controller will not show as a bootable device in the standalone server, preventing local booting.



CHAPTER 2

Upgrading Earlier Release Servers for Cisco UCS Manager Integration

This chapter includes the following sections:

Overview

If your server version is earlier than 1.4.3 release, and you want to integrate that server with Cisco UCS Manager, you have to upgrade the CIMC version to 1.4.3 or later.

Important

- The server must be a Generation M2 (or later) server.

See the following URLs for additional information about the equipment in this configuration.

- For information about the Cisco UCS 6100 Series or 6200 Series fabric interconnects (FIs) in the configuration, see the documentation at the following links:
  - Cisco UCS 6100 Series Fabric Interconnect documentation
  - Cisco UCS 6200 Series Fabric Interconnect documentation
- For information about the Cisco Nexus 2232PP fabric extenders (FEXes) in the configuration, see the documentation at the following link:

  Cisco Nexus 2000 Series Fabric Extender documentation

Required Items for Upgrade

The following are the minimum Server CIMC version and Cisco UCS Manager version requirements for upgrade for C-Series server integration with Cisco UCS Manager:

Server	CIMC Version	Minimum UCS Manager Version
Cisco UCS C22 M3 Server	1.4.5d	2.0(3)
Cisco UCS C24 M3 Server	1.4.5d	2.0(3)
Cisco UCS C200 M2 Server	1.4.3c	2.0(2)
Cisco UCS C210 M2 Server	1.4.3c	2.0(2)
Cisco UCS C220 M3 Server	1.4.4a	2.0(2)
Cisco UCS C240 M3 Server	1.4.4a	2.0(2)
Cisco UCS C250 M2 Server	1.4.3c	2.0(2)
Cisco UCS C260 M2 Server	1.4.3c	2.0(2)
Cisco UCS C460 M2 Server	1.4.3c	2.0(2)

Upgrading and Connection Procedures

If your C-Series Rack-Mount Server card-firmware does not meet the required criteria for integration with Cisco UCS Manager, you must upgrade the server. Before upgrading, the server must be installed in your rack and connected to power. Upgrading an earlier release server to latest release version is a two step procedure:

- Upgrading the C-Series Server Firmware, on page 12
- Connecting the C-Series Server with Cisco UCS Domain in Cluster Setup, on page 6

Upgrading the C-Series Server Firmware

If your server CIMC release version does not meet the requirement for integration with Cisco UCS Manager, make sure to upgrade the server firmware before connecting the server with Cisco UCS domain. For more information on upgrading the C-Series server firmware, see the host upgrade utility quick start guide for your release http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

Procedure

Step 1 Find the Host Upgrade Utility ISO file download for your server online and download it to a temporary location on your workstation:

a) See the following URL: **http://www.cisco.com/cisco/software/navigator.html**
b) Click **Unified Computing and Servers** in the middle column.
c) Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.
d) Click your model of server in the right-hand column.
e) Click **Unified Computing System (UCS) Server Firmware**.
f) Click the release number that you are downloading.
g) Click **Download Now** to download the ISO file.
h) Verify the information on the next page, then click **Proceed With Download**.
i) Continue through the subsequent screens to accept the license agreement and then browse to a location where you will save the ISO file.

Step 2 Prepare the ISO. For local upgrade, on a local media and for remote upgrade, as a virtual device:

Option	Description
Local upgrade	Perform the steps before going to Step 3: **1** Burn the ISO image onto a writable DVD. **2** Connect a VGA monitor and USB keyboard to the Cisco C-Series server. **3** Insert the DVD into the DVD drive of the Cisco C-Series server or an external DVD drive.

Option	Description
Remote upgrade	Perform the steps before going to Step 3: **1** Use a browser to connect to the CIMC Manager software on the server that you are upgrading. **2** Enter the CIMC IP address for that server in the address field of the browser, then enter your user name and password. **3** Launch a KVM Console window (click the KVM keyboard icon). **4** When the Virtual KVM Console window launches, select **Tools** > **Launch Virtual Media**. **5** In the Virtual Media Session window, click **Add Image** and navigate to the utility ISO file and select it. Navigate to the location where you downloaded the ISO. The ISO image is displayed in the **Client View** area. **6** In the **Virtual Media Session** window, select the check box in the **Mapped** column for the ISO file that you added, and then wait for mapping to complete. Observe the progress in the **Details** area. Now the ISO image is mapped to the remote device.

Step 3 Boot the server and press F6 when prompted to open the Boot Menu screen.

Step 4 On the Boot Menu screen, select the device where you prepared the ISO in Step 2:

- If you are upgrading locally, select the physical CD/DVD device and then press Enter (for example, SATA5:TSSTcorp CDDVDW TS-L633C).
- If you are upgrading remotely, select Cisco Virtual CD/DVD and then press Enter.

The server is rebooted from the device you choose.

Step 5 A screen appears with the server BIOS and CIMC firmware versions. Answer the prompt, `Have you read the Cisco EULA (end user license agreement)?`

- Press y to accept the EULA and continue the update.
- Press n to read the EULA. The EULA is displayed and you are prompted to press y to continue the update, or n to cancel. If you press n, the server will reboot without updating.
- Press q to exit without updating. This selection reboots the server.

The **Host Upgrade Menu** screen displays.

Step 6 Upgrade all the firmware by entering the number for the **All the above** menu item at the `Enter Choice` prompt:
The utility selects the correct firmware components for your server and then upgrades the firmware. Watch your console screen until you see confirmation that the upgrades were successful, then go to Step 7.

Step 7 In **Host Upgrade Menu**, at the `Enter Choice` prompt, enter the number for the **Reboot (Configures CIMC to UCSM mode—default factory settings)** menu item to reboot the server with UCSM mode settings. The utility reboots the server with UCSM mode settings. This mode allows integration with the Cisco UCS environment.

Note

- The new CIMC firmware is activated automatically during this reboot.
- These UCSM mode settings enable DHCP, Active-Active NIC redundancy, and Shared LOM NIC mode, which enables CIMC control through the 1-Gb LOM ports, rather than the management port. Any static IP addresses and the management port are disabled, so you lose connection with the CIMC.

What to Do Next

After upgrading the server to the compatible server release version, you must establish the physical connection for the server to make it a part of Cisco UCS domain.To connect the server to your Cisco UCS FEXes and FIs, see Connecting the C-Series Server with Cisco UCS Domain in Cluster Setup, on page 6.

Migrating the Configuration to Release 2.0(2) or Later

When a Cisco UCS C-Series server is integrated with Cisco UCS Manager, discovered and associated with a service profile, you can migrate the configuration to a later version of Cisco UCS Manager.

Note

- This migration process causes server downtime.
- This procedure describes the scenario where management path from the server connects to the FEX and the data path connects directly to the FI.

Procedure

Step 1 Shut down the server OS.

Step 2 In Cisco UCS Manager, decommission all C-series servers from the Cisco UCS domain.

Step 3 **Unconfigure** all FI server ports that are connected to the Nexus 2248 FEX.
Issue an NX-OS **show fex** command to verify that the FEX is unconfigured. Wait until the command return does not list the FEX.

Step 4 Disconnect the cable that connects the FEX and the FI.

Step 5 In Cisco UCS Manager CLI, issue a **remove fex** *fex_ID* command to remove the FEX from the database.

Step 6 In Cisco UCS Manager GUI, **Unconfigure** all FI server ports that are connected to the server's adapter card.

Step 7 Disconnect the cable that connects the FI and the server's adapter card.

Step 8 Disconnect the cable that connects the FEX and the server's LOM connector.

Step 9 Upgrade your Cisco UCS Manager software to release 2.0(2xx) or later and the FI firmware to the corresponding level.

Step 10 Repeat steps 3 through 9 on the second fabric interconnect in your configuration.

Step 11 Connect the C-Series server directly to your network and upgrade the firmware by using the standalone CIMC utility.

a) Connect an Ethernet line from your LAN to one of the 1-Gb LOM ports on the server. Do not use the dedicated management port, this is disabled in the Cisco UCS Manager integrated mode.

b) Follow the instructions in Updating Cisco UCS P81E VIC Firmware and uboot Image in Integrated Servers, then return to the next step in this procedure.

Step 12 Physically replace the Nexus 2248 FEX with a Nexus 2232PP FEX in your rack.

Step 13 Connect the cables as shown in the image. See Physical Connectivity Illustrations for Cluster Setup
In this new configuration, the data and management paths both connect from the server to the FEX. The paths between the FEX and the FI carry both data and management traffic.

Important Issuing an NX-OS **show fex** command to verify the FEX. Wait until the command return lists the new Nexus 2232PP FEX. The FEX will automatically upgrade to the corresponding FI firmware version.

Step 14 After both fabric interconnects are cabled, from Cisco UCS Manager, re-commission the decommissioned C-series servers.
When the server is discovered in Cisco UCS Manager, the previously assigned service profile is automatically re-associated with the server.

Updating Cisco UCS P81E VIC Firmware and uboot Image in Integrated Servers

If your Cisco UCS P81E VIC firmware and uboot version is earlier than 2.0(2g), when you integrate the server with any Cisco UCS Manager version, the UCS Manager software will return discovery and associate/disassociate failures. To avoid such failures you can do the following:

- Before you integrate the server with UCS System, upgrade your P81E VIC firmware and uboot image to the required minimum 2.0(2g) level in standalone mode.
- If your server is already integrated, you cannot upgrade the P81E VIC uboot image in the UCS Manager software. You have to remove the server from the integration and then use Cisco Host Upgrade Utility to upgrade the card and server firmware.

  The following procedure provides the process to upgrade when your server is integrated with Cisco UCS Manager.

Procedure

Step 1 Decommission the server from UCS Manager.

Step 2 Disconnect the cables from the 1-Gb LOM ports on the server.

Step 3 Connect an Ethernet line from your LAN to one of the 1-Gb LOM ports (not to the dedicated management port, which is disabled in UCSM mode).

Step 4 Find the Host Upgrade Utility ISO file download for your server online and download it to a temporary location on your workstation:

a) See the following URL: **http://www.cisco.com/cisco/software/navigator.html**
b) Click **Unified Computing and Servers** in the middle column.
c) Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.
d) Click your model of server in the right-hand column.

e) Click **Unified Computing System (UCS) Server Firmware**.
f) Click the release number that you are downloading.
g) Click **Download Now** to download the ISO file.
h) Verify the information on the next page, then click **Proceed With Download**.
i) Continue through the subsequent screens to accept the license agreement and then browse to a location where you will save the ISO file.

Step 5 Prepare the ISO. For local upgrade, on a local media and for remote upgrade, as a virtual device:

Option	Description
Local upgrade	Perform the steps before going to Step 3: **1** Burn the ISO image onto a writable DVD. **2** Connect a VGA monitor and USB keyboard to the Cisco C-Series server. **3** Insert the DVD into the DVD drive of the Cisco C-Series server or an external DVD drive.
Remote upgrade	Perform the steps before going to Step 3: **1** Use a browser to connect to the CIMC Manager software on the server that you are upgrading. **2** Enter the CIMC IP address for that server in the address field of the browser, then enter your user name and password. **3** Launch a KVM Console window (click the KVM keyboard icon). **4** When the Virtual KVM Console window launches, select **Tools** > **Launch Virtual Media**. **5** In the Virtual Media Session window, click **Add Image** and navigate to the utility ISO file and select it. Navigate to the location where you downloaded the ISO. The ISO image is displayed in the **Client View** area. **6** In the **Virtual Media Session** window, select the check box in the **Mapped** column for the ISO file that you added, and then wait for mapping to complete. Observe the progress in the **Details** area. Now the ISO image is mapped to the remote device.

Step 6 Boot the server and press F6 when prompted to open the Boot Menu screen.

Step 7 On the Boot Menu screen, select the device where you prepared the ISO in Step 2:

- If you are upgrading locally, select the physical CD/DVD device and then press Enter (for example, SATA5:TSSTcorp CDDVDW TS-L633C).
- If you are upgrading remotely, select **Cisco Virtual CD/DVD** and then press Enter.

The server is rebooted from the device you choose.

Step 8 A screen appears with the server BIOS and CIMC firmware versions. Answer the prompt, `Have you read the Cisco EULA (end user license agreement)?`

- Press y to accept the EULA and continue the update.
- Press n to read the EULA. The EULA is displayed and you are prompted to press y to continue the update, or n to cancel. If you press n, the server will reboot without updating.
- Press q to exit without updating. This selection reboots the server.

The **Host Upgrade Menu** screen displays.

Step 9 Select the option to **Update UCS P81E VIC**. This will update the card firmware and uboot image to the required level.

Step 10 Select the option to **Update CIMC Firmware**. This will update the CIMC firmware.

Step 11 Verify the firmware levels on the next screen.

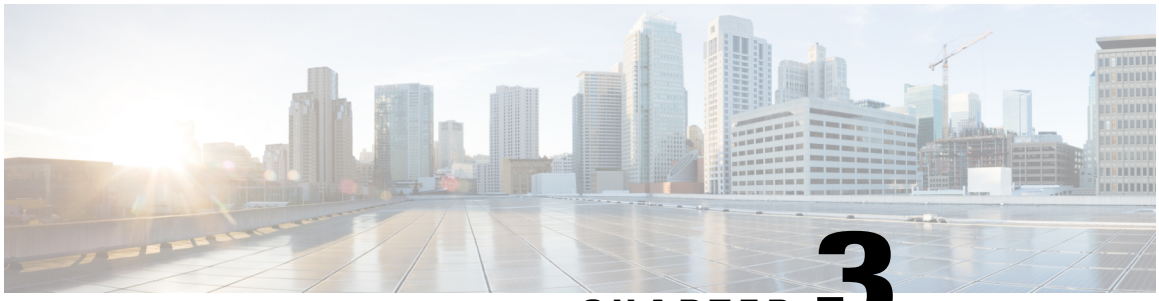
Step 12 Select the option to **Reboot the machine**.

Step 13 When you see the F8 prompt during rebooting, press F8 to open the CIMC Configuration Utility.

Step 14 In the CIMC Configuration Utility, select the option **CIMC Factory Default**, then press F10 to save your changes.

Step 15 Return the cables from the FEXes to the 1-Gb LOM ports on the server.

Step 16 Recommission the server in UCS Manager.



CHAPTER 3

Supported Network Adapter Cards for UCSM Mode

This chapter includes the following sections:

Overview

The following Network Adapter cards support Cisco UCS Manager integration :

- Cisco Virtual Interface Cards (VICs)
- Converged Network Adapters (CNAs)
- Ethernet adapters

Supported Adapter Cards

The following table shows the officially supported adapter cards for C-Series Rack-Mount Servers integration with Cisco UCS Manager.

Note

- Cisco UCS Manager provides management support for up to four adapter cards from the following list.
- Make sure to check the number of supported VICs by server type from C-Series Hardware Installation Guide.

Table 3: Supported Adapter Cards

Adapter/Server Model	C22 M3S	C24 M3S	C200 M2	C210 M2	C220 M3	C220 M4	C240 M3	C240 M4	C250 M2	C260 M2	C420 M3	C460 M2	C460 M4
Cisco UCS 1225 VIC (UCSC-PCIE-CSC-02)	Y	Y	-	-	Y	Y	Y	Y	-	Y	Y	Y	Y
Cisco UCS P81E VIC (N2XX-ACPCI01)	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	Y	-
Cisco UCS 1227 (mLOM) UCSC-MLOM-CSC-02	-	-	-	-	-	Y	-	Y	-	-	-	-	-
Emulex OCe10102-F CNA (N2XX-AEPCI01)	-	-	Y	Y	-	-	-	-	Y	Y	-	Y	-
Emulex OCe11102-FX CNA (UCSC-PCIE-ESFP)	Y	Y	-	-	Y	Y	Y	Y	-	-	Y	-	Y
Emulex OCe 14102 (UCSC-PCIE-E14102)	-	-	-	-	-	Y	-	Y	-	-	-	-	-
QLogic QLE8152 CNA (N2XX-AQPCI01)	-	-	Y	Y	-	-	-	-	Y	Y	-	Y	-
QLogic QLE8242 CNA (UCSC-PCIE-QSFP)	Y	Y	-	-	Y	-	Y	-	-	-	Y	-	-
Broadcom BCM57711 10Gb (N2XX-ABPCI02)	-	-	Y	Y	-	-	-	-	Y	-	-	Y	-
Broadcom BCM57712 10Gb UCSC-PCIE-BSFP	Y	Y	Y	Y	Y	-	Y	-	Y	Y	Y	Y	-

Adapter/Server Model	C22 M3S	C24 M3S	C200 M2	C210 M2	C220 M3	C220 M4	C240 M3	C240 M4	C250 M2	C260 M2	C420 M3	C460 M2	C460 M4
Broadcom BCM 57810 10Gb UCSC-PCIE-B3SFP	-	-	-	-	Y	Y	Y	Y	-	Y	Y	-	Y
Intel X520 10Gb (N2XX-AIPCI01)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

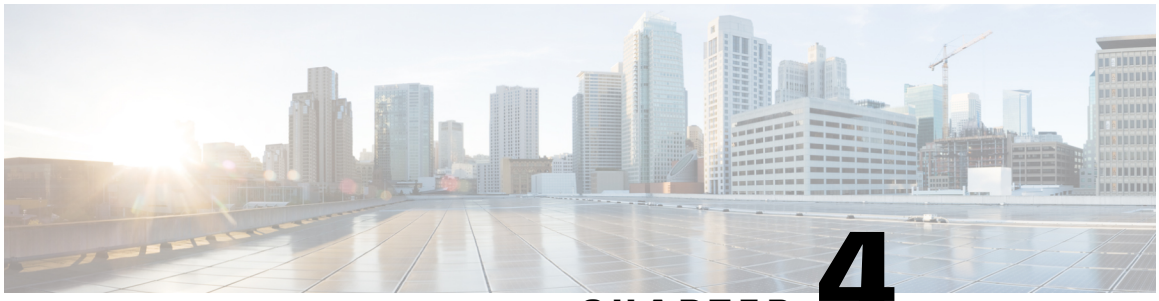
Note

- In the Cisco UCS C22 Servers, the Cisco UCS P81E VIC is supported only on the small form-factor (SFF) drives version. It is not supported on the large form-factor (LFF) drives version of the server.
- In the Cisco UCS C24 Servers, the Cisco UCS P81E VIC is -
  - Supported only on the small form-factor (SFF) drives version. It is not supported on the large form-factor (LFF) drives version of the server.
  - Not supported on the 16-drive backplane version.

Table 4: Supported Adapter Cards

Adapter/Server Model	C22 M3	C24 M3	C200 M2	C210 M2	C220 M3	C240 M3	C250 M2	C260 M2	C460 M2
Cisco UCS P81E VIC (N2XX-ACPCI01)	Y	Y	Y	Y	Y	Y	Y	Y	Y
Emulex OCe10102-F CNA (N2XX-AEPCI01)	-	-	Y	Y	-	-	Y	Y	Y
Emulex OCe11102-FX CNA (UCSCPCIE-ESFP)	Y	Y	-	-	Y	Y	-	-	-
QLogic QLE8152 CNA (N2XX-AQPCI01)	-	-	Y	Y	-	-	Y	Y	Y

Adapter/Server Model	C22 M3	C24 M3	C200 M2	C210 M2	C220 M3	C240 M3	C250 M2	C260 M2	C460 M2
QLogic QLE8242 CNA (QLE8242 CNA)	Y	Y	-	-	Y	Y	-	-	-
Broadcom BCM57711 10Gb (N2XX-ABPCI02)	-	-	Y	Y	-	-	Y	Y	Y
Intel X520 10Gb (N2XX-AIPCI01)	Y	Y	Y	Y	Y	Y	Y	Y	Y



CHAPTER 4

Special Considerations for Integrated Servers

This chapter includes the following sections:

Overview

When you connect the C-Series servers in Cisco UCS system, make sure to review the following information:

- Updating Cisco UCS P81E VIC Firmware and uboot Image in Integrated Servers, on page 16
- Integrated Server Power States vs Service Profile Power States, on page 26
- Cautions and Limitations for Adapter Cards, on page 26
- FEX Considerations, on page 27

Supported FEX-to-FI Uplink Cable SFP Types

The C-Series UCSM integration requires six 10-Gb SFP cables for the following purposes:

- Linking the data traffic paths between server and 2232PP FEX - 2 cables
- Uplinks from the 2232PP FEXes to the FIs - 4 cables

  Each of the four uplinks from the FEXes to the FIs can use either a Cisco 10-Gb twinax cable, or one of the following SFP types:

  - SFP-10GE-SR

- FET-10GE

Caution Do not mix SFP types on an uplink. If you mix SFP types on an uplink, you will get **Discovery failed** errors.

Upgrading the C-Series Server Firmware

If your server CIMC release version does not meet the requirement for integration with Cisco UCS Manager, make sure to upgrade the server firmware before connecting the server with Cisco UCS domain. For more information on upgrading the C-Series server firmware, see the host upgrade utility quick start guide for your release http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

Procedure

Step 1 Find the Host Upgrade Utility ISO file download for your server online and download it to a temporary location on your workstation:

a) See the following URL: **http://www.cisco.com/cisco/software/navigator.html**
b) Click **Unified Computing and Servers** in the middle column.
c) Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.
d) Click your model of server in the right-hand column.
e) Click **Unified Computing System (UCS) Server Firmware**.
f) Click the release number that you are downloading.
g) Click **Download Now** to download the ISO file.
h) Verify the information on the next page, then click **Proceed With Download**.
i) Continue through the subsequent screens to accept the license agreement and then browse to a location where you will save the ISO file.

Step 2 Prepare the ISO. For local upgrade, on a local media and for remote upgrade, as a virtual device:

Option	Description
Local upgrade	Perform the steps before going to Step 3: **1** Burn the ISO image onto a writable DVD. **2** Connect a VGA monitor and USB keyboard to the Cisco C-Series server. **3** Insert the DVD into the DVD drive of the Cisco C-Series server or an external DVD drive.

Option	Description
Remote upgrade	Perform the steps before going to Step 3: **1** Use a browser to connect to the CIMC Manager software on the server that you are upgrading. **2** Enter the CIMC IP address for that server in the address field of the browser, then enter your user name and password. **3** Launch a KVM Console window (click the KVM keyboard icon). **4** When the Virtual KVM Console window launches, select **Tools** > **Launch Virtual Media**. **5** In the Virtual Media Session window, click **Add Image** and navigate to the utility ISO file and select it. Navigate to the location where you downloaded the ISO. The ISO image is displayed in the **Client View** area. **6** In the **Virtual Media Session** window, select the check box in the **Mapped** column for the ISO file that you added, and then wait for mapping to complete. Observe the progress in the **Details** area. Now the ISO image is mapped to the remote device.

Step 3 Boot the server and press F6 when prompted to open the Boot Menu screen.

Step 4 On the Boot Menu screen, select the device where you prepared the ISO in Step 2:

- If you are upgrading locally, select the physical CD/DVD device and then press Enter (for example, SATA5:TSSTcorp CDDVDW TS-L633C).
- If you are upgrading remotely, select Cisco Virtual CD/DVD and then press Enter.

The server is rebooted from the device you choose.

Step 5 A screen appears with the server BIOS and CIMC firmware versions. Answer the prompt, `Have you read the Cisco EULA (end user license agreement)?`

- Press y to accept the EULA and continue the update.
- Press n to read the EULA. The EULA is displayed and you are prompted to press y to continue the update, or n to cancel. If you press n, the server will reboot without updating.
- Press q to exit without updating. This selection reboots the server.

The **Host Upgrade Menu** screen displays.

Step 6 Upgrade all the firmware by entering the number for the **All the above** menu item at the `Enter Choice` prompt:
The utility selects the correct firmware components for your server and then upgrades the firmware. Watch your console screen until you see confirmation that the upgrades were successful, then go to Step 7.

Step 7 In **Host Upgrade Menu**, at the `Enter Choice` prompt, enter the number for the **Reboot (Configures CIMC to UCSM mode—default factory settings)** menu item to reboot the server with UCSM mode settings. The utility reboots the server with UCSM mode settings. This mode allows integration with the Cisco UCS environment.

Note

- The new CIMC firmware is activated automatically during this reboot.
- These UCSM mode settings enable DHCP, Active-Active NIC redundancy, and Shared LOM NIC mode, which enables CIMC control through the 1-Gb LOM ports, rather than the management port. Any static IP addresses and the management port are disabled, so you lose connection with the CIMC.

What to Do Next

After upgrading the server to the compatible server release version, you must establish the physical connection for the server to make it a part of Cisco UCS domain.To connect the server to your Cisco UCS FEXes and FIs, see Connecting the C-Series Server with Cisco UCS Domain in Cluster Setup, on page 6.

Integrated Server Power States vs Service Profile Power States

Using the power button or Cisco UCS Manager, if you set the desired power status to Down for an integrated C-Series server's associated service profile, when you try to rest the server to the desired power state, the server becomes out of sync with the actual power state. This may cause the server to shut down unexpectedly at a later time.

Use the Boot Server action in Cisco UCS Manager to safely reboot a server from a power-down state.

The following table shows how the physical server power states can differ from the Cisco UCS Manager service profile power states when the power button on the server is used.

Table 5: Difference in Server Power State and Service Profile Power State

Initial Service Profile Power State	Server Initial Power State	Action From Physical Power Button	Actual Server Power State After the Action	Power State Under UCSM Equipment Tab	Desired Power State Under Service Profile
Down	Off	Push button to turn on	On	On	Down
Up	On	Push button to turn off	Off	Off	Up

Cautions and Limitations for Adapter Cards

Make sure to consider the following when using the adapter cards in Cisco UCS C-Series server integration with Cisco UCS Manager:

- Cisco UCS Manager supports only four UCS managed adapter cards in the integrated Cisco UCS C-series servers, even if the server has more than four PCI slots. If you have more than four adapter cards in the server, after integration, the rack server discovery fails in Cisco UCS Manager.
- When you add, remove, or replace an adapter card in a UCS-managed server, you must first decommission the server in Cisco UCS Manager. After the operation, you must then recommission the server.

- If an integrated server contains two Cisco UCS P81E Virtual Interface Cards, the vNICs/vHBAs on Adapter 1 might have a higher PCI order in Cisco UCS Manager than the vNICs/vHBAs on Adapter 2.

Acknowledged Links between 2232PP FEX and FI	Maximum vNIC+vHBA for VIC adapter with 6100 FI	Maximum vNIC+vHBA for VIC adapter with 6200 FI
1	1	13
2	4	28
4	10	58
8	22	118

Note The available vNIC can be failover or non-failover vNIC.

- In C200 or C210 servers, BIOS version 1.4(3c) and later, you have an option to enable or disable SR-IOV/ARI (single-root I/O virtualization/alternative routing-ID interpretation) bus reservation. Whenever you change the SR-IOV/ARI bus reservation settings on a UCS-managed server, you must re-acknowledge the server.

FEX Considerations

Re-acknowledge Attached Servers After a 2232PP FEX Is Decommissioned/Recommissioned

Whenever you decommission or recommission a Cisco UCS 2232PP FEX, all the servers that are connected to that FEX must be re-acknowledged in UCS Manager.