Cisco UCS C24 Server Installation and Service Guide

Covers Server Generation M3

Updated February 16, 2018

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-26647-01**

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco UCS C24 Server Installation and Service Guide
© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface vii

Related Documentation vii

Organization vii

Audience viii

Documentation Feedback viii

Conventions viii

Obtaining Documentation and Submitting a Service Request 1-xiii

xiv

CHAPTER 1 **Overview** 1-1

CHAPTER 2 **Installing the Server** 2-1

Unpacking and Inspecting the Server 2-2

Preparing for Server Installation 2-3

Installation Guidelines 2-3

Rack Requirements 2-4

Equipment Requirements 2-4

Slide Rail Adjustment Range 2-4

Installing the Server In a Rack 2-5

Initial Server Setup 2-8

Connecting and Powering On the Server (Standalone Mode) 2-8

NIC Modes and NIC Redundancy Settings 2-12

System BIOS and CIMC Firmware 2-13

Updating the BIOS and CIMC Firmware 2-13

Accessing the System BIOS 2-14

Service Headers and Jumpers 2-15

Header Location on the Motherboard 2-15

Using the BIOS Recovery Header CN34 2-16

Procedure 1: Reboot With recovery.cap File 2-16

Procedure 2: Use Recovery Jumper and recovery.cap File 2-18

Using the Clear CMOS Header CN14 2-19

CHAPTER 3 **Maintaining the Server** 3-1

Server Monitoring and Management Tools 3-1
Cisco Integrated Management Interface (CIMC) 3-1
Server Configuration Utility 3-1
Status LEDs and Buttons 3-2
Front Panel LEDs 3-2
Rear Panel LEDs and Buttons 3-4
Preparing for Server Component Installation 3-6
Required Equipment 3-6
Shutting Down and Powering Off the Server 3-6
Removing and Replacing the Server Top Cover 3-7
Removing and Replacing the Front Chassis Panel 3-8
Replaceable Component Locations 3-9
Serial Number Location 3-9
Color-Coded Touch Points 3-10
Installing or Replacing Server Components 3-11
Replacing Hard Drives or Solid State Drives 3-12
Drive Population Guidelines 3-12
Drive Replacement Procedure 3-13
Replacing a Drive Backplane 3-14
Replacing a SAS Expander 3-16
Replacing Fan Modules 3-18
Replacing DIMMs 3-20
Memory Performance Guidelines and Population Rules 3-20
DIMM Replacement Procedure 3-23
Replacing CPUs and Heatsinks 3-25
Single-CPU Restrictions 3-25
Additional CPU-Related Parts To Order With RMA Replacement Motherboards 3-25
CPU Replacement Procedure 3-26
Replacing the Motherboard RTC Battery 3-31
Replacing a PCIe Riser 3-33
Replacing a PCIe Card 3-35
PCIe Slots 3-35
RAID Card Firmware Compatibility 3-36
Replacing a PCIe Card 3-36
Special Considerations for Cisco UCS Virtual Interface Cards 3-38
RAID Controller Card Cable Routing 3-38
Installing Multiple PCIe Cards and Resolving Limited Resources 3-38
Replacing a SuperCap Power Module (RAID Backup Unit) 3-41

Replacing an Internal USB Flash Drive 3-43
Internal USB Flash Drive Replacement Procedure 3-43
Enabling or Disabling the Internal USB Port 3-44
Installing a Trusted Platform Module 3-45
Enabling the Intel Trusted Execution Technology (TXT) Feature For the TPM 3-46
Replacing a SCU Upgrade ROM Module 3-48
Replacing a Software RAID Key Module 3-49
Replacing Power Supplies 3-51

APPENDIX A **Server Specifications** A-1
Physical Specifications A-1
Power Specifications A-2
450W Power Supply A-2
650W Power Supply A-3
Environmental Specifications A-4

APPENDIX B **Power Cord Specifications** B-1
Supported Power Cords and Plugs B-1
AC Power Cord Illustrations B-3

APPENDIX C **RAID Controller Considerations** C-1
Supported RAID Controllers and Required Cables C-2
RAID Card Firmware Compatibility C-3
Mixing Drive Types in RAID Groups C-3
SuperCap Power Modules (RAID Backup Units) C-4
RAID Controller Migration C-5
Embedded MegaRAID Controller C-6
Notes on Supported Embedded MegaRAID Levels C-7
Installing a SCU Upgrade ROM Module For Embedded RAID SAS Support C-8
Installing a Software RAID Key Module for Embedded RAID 5 Support C-9
Enabling the Integrated RAID Controller in the BIOS C-9
Disabling the Integrated RAID Controller in the BIOS C-9
Launching the LSI Embedded RAID Configuration Utility C-10
Installing LSI MegaSR Drivers For Windows and Linux C-10
Downloading the LSI MegaSR Drivers C-11
Microsoft Windows Driver Installation C-11
Linux Driver Installation C-13
RAID Controller Cabling C-18

Cable Routing C-18
Cisco UCS C24 Server RAID Cabling Instructions C-19
Backplane and Expander Options C-19
Small Form Factor 24-Drive Backplane With Expander Cabling C-19
Small Form Factor 16-Drive Backplane (No Expander) Cabling C-20
Large Form Factor 12-Drive Backplane With Expander Cabling C-21
Restoring RAID Configuration After Replacing a RAID Controller C-22
For More Information C-22

APPENDIX D **Installation for Cisco UCS Integration** D-1

Preface

This preface describes the audience, organization, and conventions of the *Cisco UCS C24 Server Installation and Service Guide*. It also provides information about how to obtain related documentation.

Related Documentation

The documentation set for the Cisco Unified Computing System (UCS) C-Series rack-mount servers is described in the roadmap document at the following link:

Cisco UCS C-Series Documentation Roadmap

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Overview	Provides an overview of the server.
Chapter 2	Installing the Server	Describes how to install the server in a rack, how to cable and power on the server, and how to initially set up the server in standalone mode.
Chapter 3	Maintaining the Server	Describes the server LEDs and buttons, identifies the replaceable components of the server, and describes how to replace them.
Appendix A	Server Specifications	Lists physical, environmental, and power specifications for the server.
Appendix B	Power Cord Specifications	Lists specifications for the supported international power cords.
Appendix C	RAID Controller Considerations	Provides server RAID controller information.
Appendix D	Installation for Cisco UCS Integration	Provides installation and upgrade procedures for installing the server into Unified Computing System (UCS) integration.

Audience

This guide is for experienced network administrators who configure and maintain Cisco servers.

Documentation Feedback

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

Conventions

This document uses the following conventions for notes, cautions, and safety warnings. Notes and cautions contain important information that you should know.

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

Caution Means *reader be careful*. Cautions contain information about something you might do that could result in equipment damage or loss of data.

Safety warnings appear throughout this guide in procedures that, if performed incorrectly, can cause physical injuries. A warning symbol precedes each warning statement.

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

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告　重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

的标准工作程序。请

安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의　중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso　**INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel　**VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير　**إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Opozorilo

POMEMBNI VARNOSTNI NAPOTKI

Ta opozorilni simbol pomeni nevarnost. Nahajate se v situaciji, kjer lahko pride do telesnih poškodb. Preden pričnete z delom na napravi, se morate zavedati nevarnosti udara električnega toka, ter tudi poznati preventivne ukrepe za preprečevanje takšnih nevarnosti. Uporabite obrazložitveno številko na koncu posameznega opozorila, da najdete opis nevarnosti v priloženem varnostnem priročniku.

SHRANITE TE NAPOTKE!

警告

重要安全性指示
此警告符號代表危險，表示可能造成人身傷害。使用任何設備前，請留心電路相關危險，並熟悉避免意外的標準作法。您可以使用每項警告後的聲明編號，查詢本裝置隨附之安全性警告譯文中的翻譯。
請妥善保留此指示

Obtain Documentation and Submit a Service Request

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

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

CHAPTER 1

Overview

This chapter provides an overview of the Cisco UCS C24 server features.

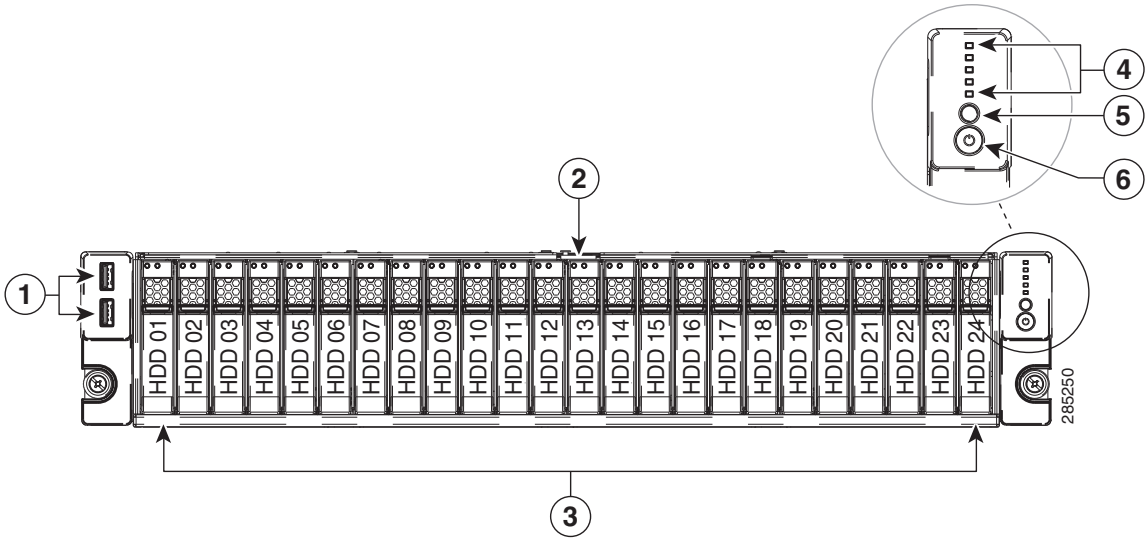
The figures in this chapter show an overview of external server features. Internal server features are illustrated in Figure 3-4 on page 3-9.

The server is orderable in three different versions, each with one of three different front panel/backplane configurations:

- Cisco UCS C24 (small form-factor (SFF) drives, with 24-drive backplane and expander). Holds up to twenty-four 2.5-inch hard drives or solid state drives.
- Cisco UCS C24 (small form-factor (SFF) drives, with 16-drive backplane, no expander). Holds up to sixteen 2.5-inch hard drives or solid state drives.
- Cisco UCS C24 (large form-factor (LFF) drives, with 12-drive backplane and expander). Holds up to twelve 3.5-inch hard drives.

Figure 1-1 shows the front panel features of the Small Form-Factor drives version of the server. This version of the server can be ordered with either a 16-drive direct-connect backplane or a 24-drive backplane with an expander. When the 16-drive backplane is installed, only the first 16 drive bays are used.

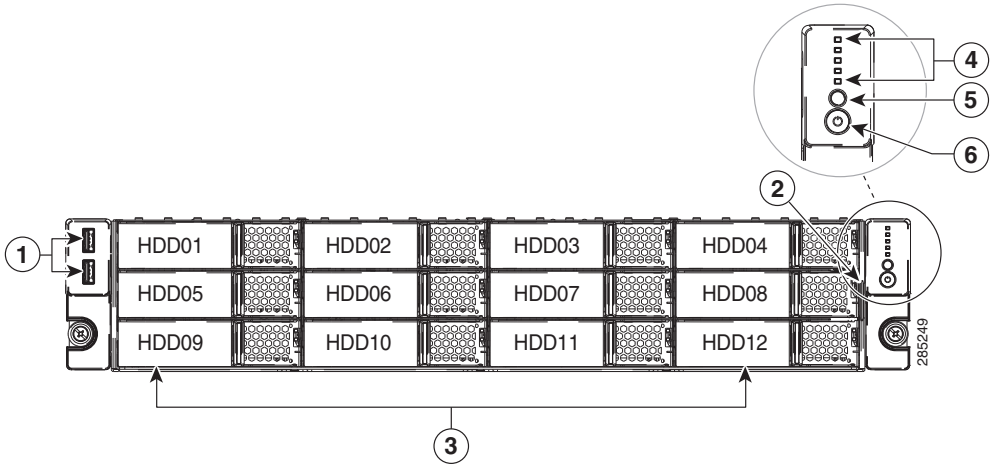
Figure 1-1 Cisco UCS C24 Server (Small Form Factor Drives) Front Panel Features



1	USB 2.0 ports (two)	**4**	Status LEDs (top to bottom): Network activity LED Power supply status LED Temperature status LED Fan Status LED System status LED
2	Pull-out asset tag	**5**	Identification button/LED
3	Drives, hot-swappable • 24-drive backplane version: Up to twenty-four 2.5-inch drives • 16-drive backplane version: Up to sixteen 2.5-inch drives	**6**	**Power button/Power status LED**

Figure 1-2 shows the front panel features of the Large Form Factor drives version of the server. This version of the server has a 12-drive backplane with an expander. For definitions of all LED states, see Status LEDs and Buttons, page 3-2.

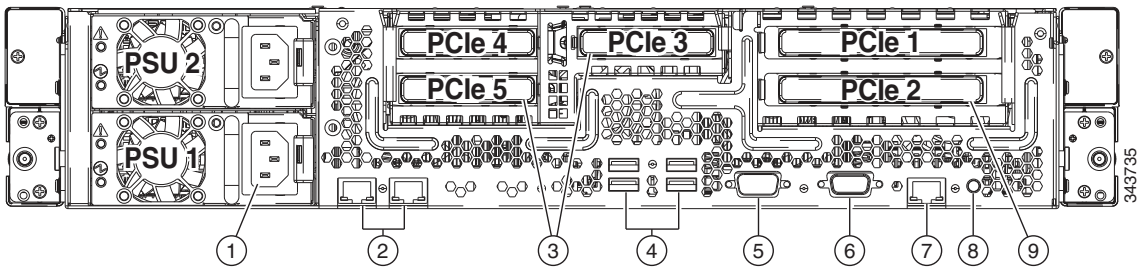
Figure 1-2 Cisco UCS C24 Server (Large Form Factor Drives) Front Panel Features



1	USB 2.0 ports (two)	**4**	Status LEDs (top to bottom): Network activity LED Power supply status LED Temperature status LED Fan Status LED System status LED
2	Asset tag (serial number)	**5**	Identification button/LED
3	Drives, hot-swappable (up to twelve 3.5-inch drives)	**6**	**Power button/Power status LED**

Figure 1-3 shows the rear panel features of the server (identical for all versions of the server). For definitions of all LED states, see Status LEDs and Buttons, page 3-2.

Figure 1-3 Cisco UCS C24 Server Rear Panel Features



1	Power supplies (two)	**6**	VGA video port (DB-15 connector)
2	Dual 1 Gb Ethernet ports (LAN1, LAN2)	**7**	10/100/1000 Ethernet dedicated management port
3	PCIe slots 3, 4, and 5 on riser 2 See PCIe Slots, page 3-35 for slot specifications.	**8**	Rear Identification button/LED
4	USB 2.0 ports (four)	**9**	PCIe slots 1 and 2 on riser 1 See PCIe Slots, page 3-35 for slot specifications.
5	Serial port (DB-9 connector)		–

Table 1-1 lists a summary of server features.

Table 1-1 Cisco UCS C24 Server Features

Chassis	Two rack-unit (2RU) chassis.
Processors	Two Intel Xeon E5-2400 Series processors.
Memory	The server provides 12 DIMM[1] sockets on the motherboard.
Multi-bit error protection	This server supports multi-bit error protection.
Baseboard management	Pilot III BMC, running Cisco Integrated Management Controller (CIMC) firmware. Depending on your CIMC settings, the CIMC can be accessed through the 10/100/1000 Ethernet dedicated management port, the 1-Gb Ethernet LOM ports, or a Cisco P81E virtual interface card.
Network and management I/O	The server provides these connectors: • One 1-Gb Ethernet dedicated management port • Two 1-Gb Base-T Ethernet LAN ports • One RS-232 serial port (DB-9 connector) • One 15-pin VGA[2] connector • Six USB[3] 2.0 connectors
WoL	The 1-Gb Base-T Ethernet LAN ports support the wake-on-LAN (WoL) standard.

Table 1-1 Cisco UCS C24 Server Features (continued)

Power	Two power supplies: Both either 450 W each or 650 W each. Do not mix power supply types. Redundant as 1+1. See Power Specifications, page A-2.
ACPI	This server supports the advanced configuration and power interface (ACPI) 4.0 standard.
Cooling	Four hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Five horizontal PCIe[4] expansion slots on two risers. See PCIe Slots, page 3-35 for specifications of the slots.
InfiniBand	The bus slots in this server support the InfiniBand architecture.
Storage	Drives are installed into front-panel drive bays that provide hot-pluggable access. There are two versions of the server front panel and backplane: • Cisco UCS C24 (small form-factor (SFF) drives, with 24-drive backplane and expander). Holds up to twenty-four 2.5-inch hard drives or solid state drives. • Cisco UCS C24 (small form-factor (SFF) drives, with 16-drive backplane, no expander). Holds up to sixteen 2.5-inch hard drives or solid state drives. • Cisco UCS C24 (large form-factor (LFF) drives, with 12-drive backplane and expander). Holds up to twelve 3.5-inch hard drives.
Internal USB support	The server has one internal USB 2.0 socket on the motherboard that you can use with a USB thumb drive for additional storage. The server can be ordered with an optional blank 8-GB Cisco USB Flash Drive pre-installed in the internal USB port.
Disk Management (RAID)	For a list of RAID[5] controller options and cables, see RAID Controller Considerations, page C-1.
RAID Backup	There are two mounting points inside the chassis that can be used for the SuperCap power module that is used with LSI MegaRAID-CV card.
Video	Matrox G200e video controller. Resolution up to 1920 x1200, 16bpp at 60 Hz. Up to 256 MB of video memory.

1. DIMM = dual inline memory module
2. VGA = video graphics array
3. USB = universal serial bus
4. PCIe = peripheral component interconnect express
5. RAID = redundant array of independent disks

CHAPTER 2

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:

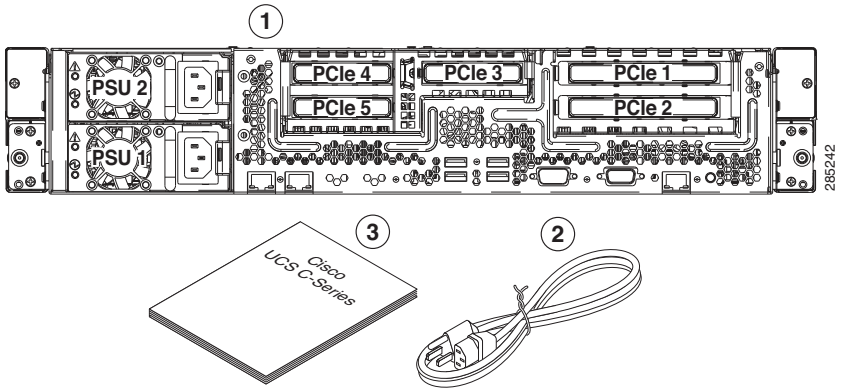
Step 1 Remove the server from its cardboard container and save all packaging material.

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:

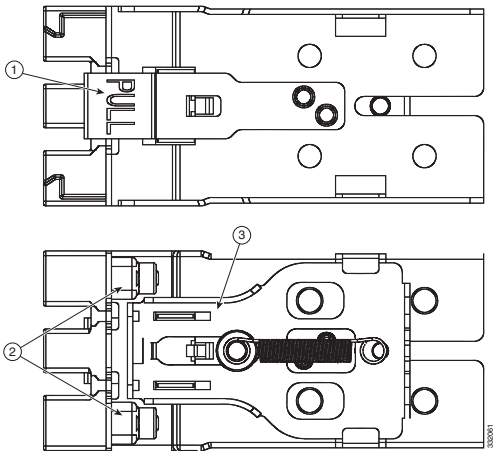
Step 1 Open the front securing latch (see Figure 2-2). The end of the slide-rail assembly marked "FRONT" has a spring-loaded securing latch that must be open before you can insert the mounting pegs into the rack-post holes.

a. On the rear side of the securing-latch assembly, hold open the clip marked "PULL."

b. Slide the spring-loaded securing latch away from the mounting pegs.

c. 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:

a. 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.

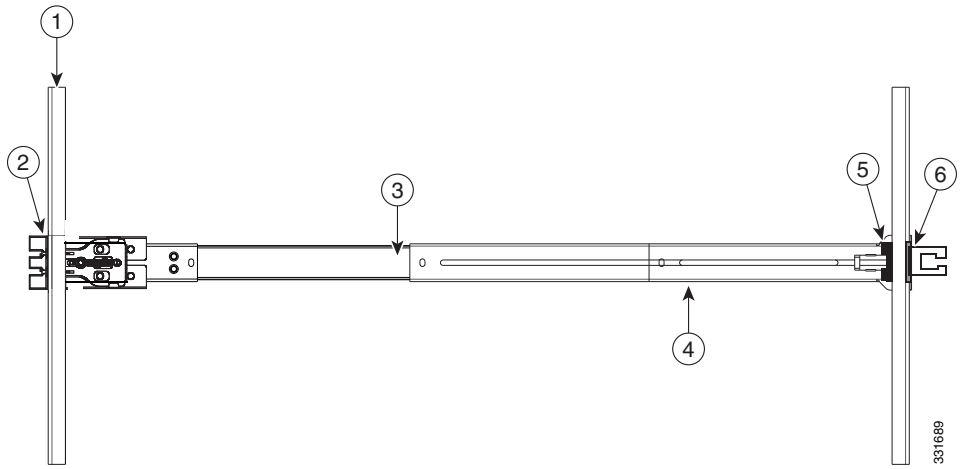
b. Position the front mounting pegs so that they enter the desired front rack-post holes from the front.

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.

c. 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.

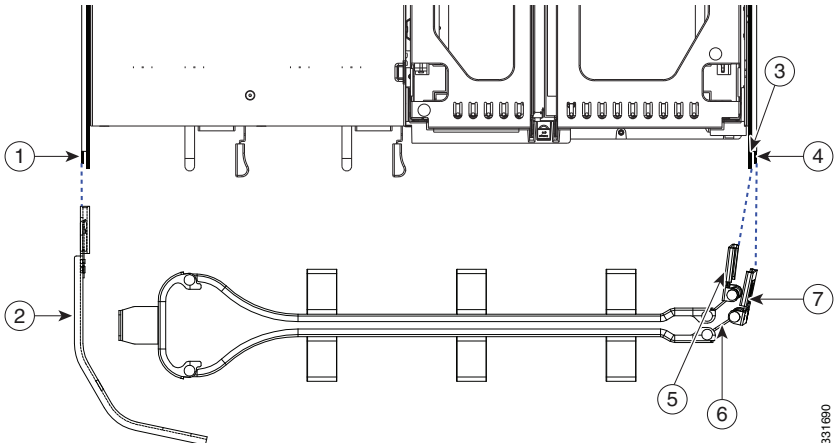
a. Slide the plastic clip on the inner CMA arm over the flange on the mounting bracket that attached to the side of the server. See Figure 2-4.

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:

a. Press the **Power** button to boot the server. Watch for the prompt to press F8.

b. During bootup, press **F8** when prompted to open the Cisco IMC Configuration Utility. Note the differences between versions of Cisco IMC firmware:

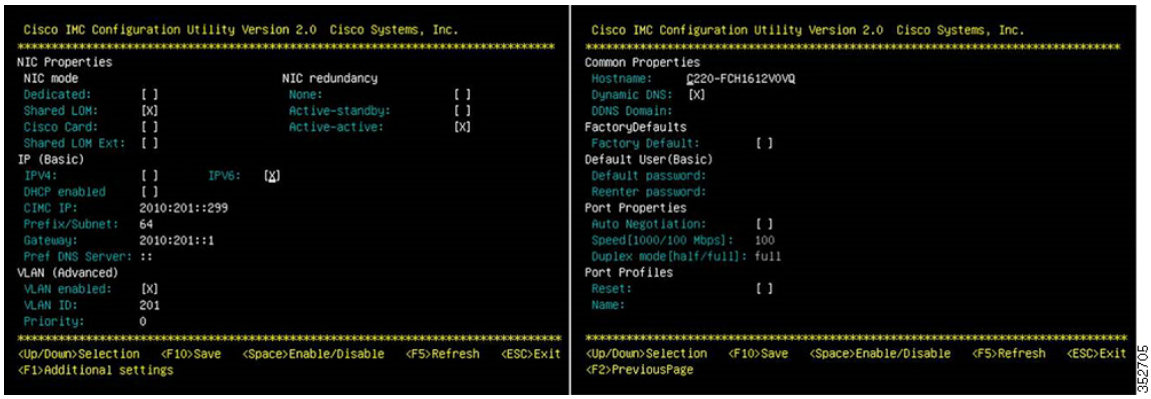
- In Cisco IMC 2.0(1) and later, there are two windows for this utility that you can switch between by pressing F1 or F2 (see Figure 2-5 for sample windows). The IPv4 and IPv6 protocols and dynamic domain name system (DDNS) are supported. You can also define a host name and a DDNS domain.
- In Cisco 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)



Step 4 Set NIC mode and NIC redundancy:

a. 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

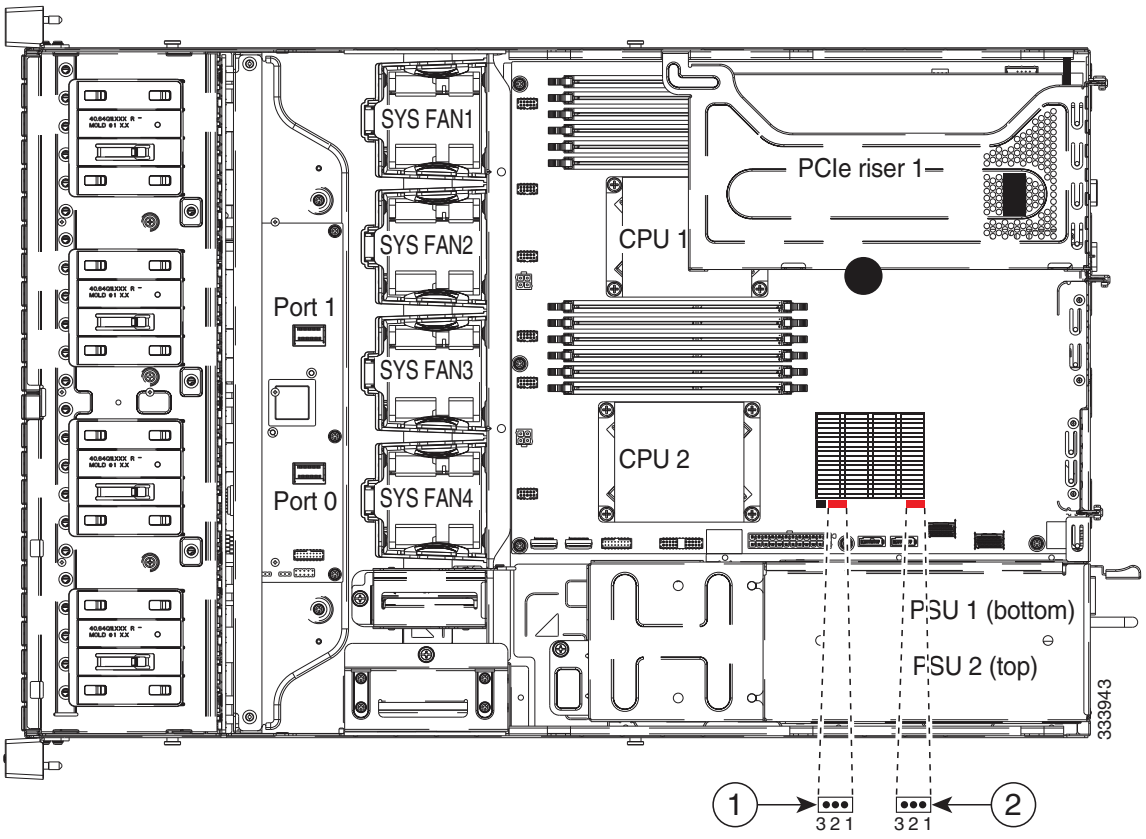
This section includes the following topics:

- 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 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 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.

CHAPTER 3

Maintaining the Server

This chapter describes how to diagnose server system problems using LEDs. It also provides information about how to install or replace hardware components, and it includes the following sections:

- Server Monitoring and Management Tools, page 3-1
- Status LEDs and Buttons, page 3-2
- Preparing for Server Component Installation, page 3-6
- Installing or Replacing Server Components, page 3-11

Server Monitoring and Management Tools

Cisco Integrated Management Interface (CIMC)

You can monitor the server inventory, health, and system event logs by using the built-in Cisco Integrated Management Controller (CIMC) GUI or CLI interfaces. See the user documentation for your firmware release at the following URL:

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

Server Configuration Utility

Cisco has also developed the Cisco Server Configuration Utility for C-Series servers, which can aid and simplify the following tasks:

- Monitoring server inventory and health
- Diagnosing common server problems with diagnostic tools and logs
- Setting the BIOS booting order
- Configuring some RAID configurations
- Installing operating systems

You can download the ISO from Cisco.com. See the user documentation for your version of the utility at the following URL:

http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

Status LEDs and Buttons

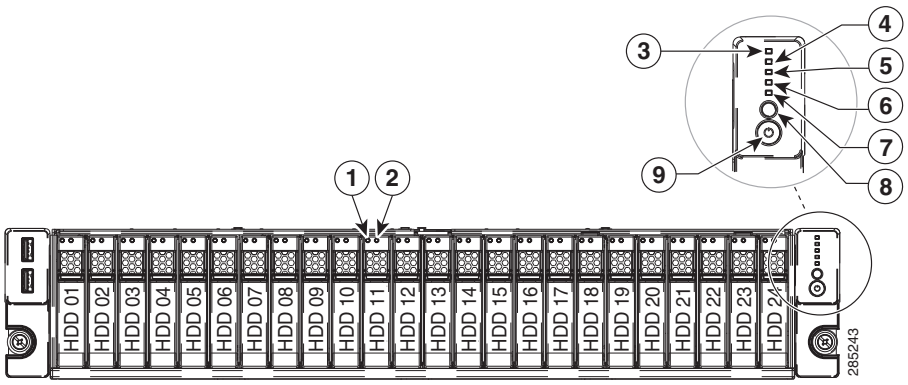
This section describes the location and meaning of LEDs and buttons and includes the following topics

- Front Panel LEDs, page 3-2
- Rear Panel LEDs and Buttons, page 3-4

Front Panel LEDs

Figure 3-1 shows the front panel LEDs. Table 3-1 defines the front panel LED states.

Figure 3-1 Front Panel LEDs



1	Hard drive fault LED	**6**	Fan status LED
2	Hard drive activity LED	**7**	System status LED
3	Network link activity LED	**8**	Identification button/LED
4	Power supply status LED	**9**	Power button/power status LED
5	Temperature status LED		–

Table 3-1 Front Panel LEDs, Definitions of States

LED Name	State
Hard drive fault	• Off—The hard drive is operating properly. • Amber—This hard drive has failed. • Amber, blinking—The device is rebuilding.
Hard drive activity	• Off—There is no hard drive in the hard drive sled (no access, no fault). • Green—The hard drive is ready. • Green, blinking—The hard drive is reading or writing data.
Network link activity	• Off—The Ethernet link is idle. • Green—One or more Ethernet LOM ports are link-active, but there is no activity. • Green, blinking—One or more Ethernet LOM ports are link-active, with activity.

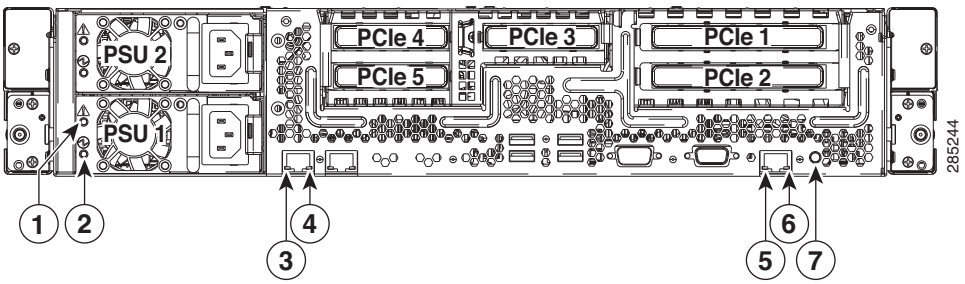
Table 3-1 Front Panel LEDs, Definitions of States (continued)

LED Name	State
Power supply status	• Green—All power supplies are operating normally. • Amber, steady—One or more power supplies are in a degraded operational state. • Amber, blinking—One or more power supplies are in a critical fault state.
Temperature status	• Green—The server is operating at normal temperature. • Amber, steady—One or more temperature sensors have exceeded a warning threshold. • Amber, blinking—One or more temperature sensors have exceeded a critical threshold.
Fan status	• Green—All fan modules are operating properly. • Amber, steady—One fan module has failed. • Amber, blinking—Critical fault, two or more fan modules have failed.
System status	• Green—The server is running in normal operating condition. • Green, blinking—The server is performing system initialization and memory check. • Amber, steady—The server is in a degraded operational state. For example: – Power supply redundancy is lost. – CPUs are mismatched. – At least one CPU is faulty. – At least one DIMM is faulty. – At least one drive in a RAID configuration failed. • Amber, blinking—The server is in a critical fault state. For example: – Boot failed. – Fatal CPU and/or bus error is detected. – Server is in over-temperature condition.
Identification	• Off—The Identification LED is not in use. • Blue—The Identification LED is activated.
Power button/Power status LED	• Off—There is no AC power to 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.

Rear Panel LEDs and Buttons

Figure 3-2 shows the rear panel LEDs and buttons. Table 3-2 defines the LED states.

Figure 3-2 Rear Panel LEDs and Buttons



1	Power supply fault LED	**5**	10/100/1000 Ethernet dedicated management link status LED
2	Power supply AC OK LED	**6**	10/100/1000 Ethernet dedicated management link speed LED
3	1-Gb Ethernet link speed LED	**7**	Identification button/LED
4	1-Gb Ethernet link status LED		–

Table 3-2 Rear Panel LEDs, Definitions of States

LED Name	State
Power supply fault	• Off—The power supply is operating normally. • Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate. • Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).
Power supply AC OK	• Off—There is no AC power to the power supply. • Green, blinking—AC power OK, DC output not enabled. • Green, solid—AC power OK, DC outputs OK.
1-Gb Ethernet link speed	• Off—link speed is 10 Mbps. • Amber—link speed is 100 Mbps. • Green—link speed is 1 Gbps.
1-Gb Ethernet link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
10/100/1000 Ethernet dedicated management link speed	• Off—link speed is 10 Mbps. • Amber—link speed is 100 Mbps. • Green—link speed is 1 Gbps.

Table 3-2 Rear Panel LEDs, Definitions of States (continued)

LED Name	State
10/100/1000 Ethernet dedicated management link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
Identification	• Off—The Identification LED is not in use. • Blue—The Identification LED is activated.

Preparing for Server Component Installation

This section describes how to prepare for component installation, and it includes the following topics:

- Required Equipment, page 3-6
- Shutting Down and Powering Off the Server, page 3-6
- Removing and Replacing the Server Top Cover, page 3-7
- Removing and Replacing the Front Chassis Panel, page 3-8
- Replaceable Component Locations, page 3-9
- Serial Number Location, page 3-9

Required Equipment

The following equipment is used to perform the procedures in this chapter:

- Number 2 Phillips-head screwdriver
- Electrostatic discharge (ESD) strap or other grounding equipment such as a grounded mat

Shutting Down and Powering Off the Server

The server can run in two power modes:

- Main power mode—Power is supplied to all server components and any operating system on your drives can run.
- Standby power mode—Power is supplied only to the service processor and the cooling fans and it is safe to power off the server from this mode.

You can invoke a graceful shutdown or an hard shutdown by using either of the following methods:

- Use the CIMC management interface.
- Use the **Power** button on the server front panel. To use the **Power** button, follow these steps:

Step 1 Check the color of the Power Status LED (see the "Front Panel LEDs" section on page 3-2).

- Green—the server is in main power mode and must be shut down before it can be safely powered off. Go to Step 2.
- Amber—the server is already in standby mode and can be safely powered off. Go to Step 3.

Step 2 Invoke either a graceful shutdown or a hard shutdown:

Caution To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system.

- Graceful shutdown—Press and release the **Power** button. The operating system performs a graceful shutdown and the server goes to standby mode, which is indicated by an amber Power Status LED.
- Emergency shutdown—Press and hold the **Power** button for 4 seconds to force the main power off and immediately enter standby mode.

Step 3 Disconnect the power cords from the power supplies in your server to completely power off the server.

Removing and Replacing the Server Top Cover

To remove or replace the top cover of the server, follow these steps:

Tip You do not have to remove the cover to replace hard drives or power supplies.

Step 1 Remove the top cover (see Figure 3-3).

a. Loosen the two captive thumbscrews that secure the rear edge of the top cover to the chassis.

b. Push the top cover toward the server rear about one-half inch (1.27 cm), until it stops.

c. Lift the top cover straight up from the server and set it aside.

Step 2 Replace the top cover:

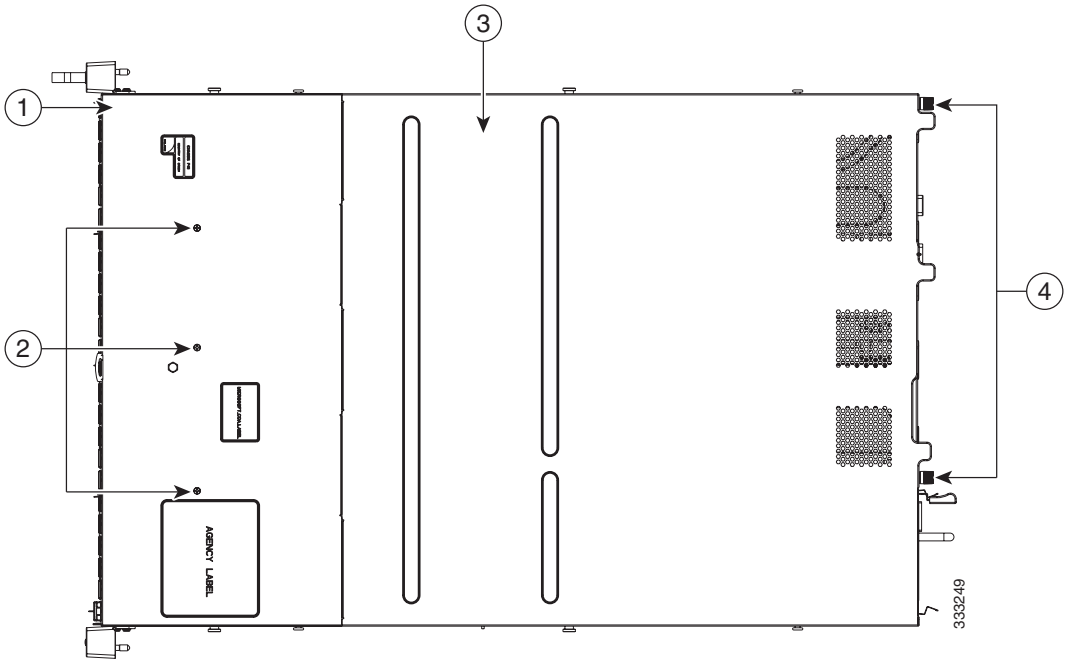
a. Place the cover on top of the server about one-half inch (1.27 cm) behind the lip of the front chassis panel. The cover should sit flat.

Note The rear of the cover has a wrap-around flanged edge that must be correctly aligned with the chassis rear edge when sliding the cover forward.

b. Slide the top cover toward the front chassis panel until it stops.

c. Tighten the two captive thumbscrews that secure the rear edge of the cover to the chassis.

Figure 3-3 Removing the Top Cover or Front Chassis Panel



1	Front chassis panel	3	Top cover
2	Front chassis panel securing screws (three)	4	Top cover thumbscrews (two)

Removing and Replacing the Front Chassis Panel

To remove or replace the front chassis panel of the server, follow these steps:

Tip Remove this panel only if you are instructed to do so in a procedure in this book.

Step 1 Remove the front chassis panel (see Figure 3-3):

- **a.** Remove the top cover from the server as described in Removing and Replacing the Server Top Cover, page 3-7.
- **b.** Use a #2 Phillips-head screwdriver to remove the three screws that secure the front chassis panel to the chassis (see Figure 3-3).
- **c.** Push the panel forward about 1/4-inch, until it stops. The wrap-around front edge of the panel must become free from the front edge of the chassis.
- **d.** Lift the panel straight up from the server and set it aside.

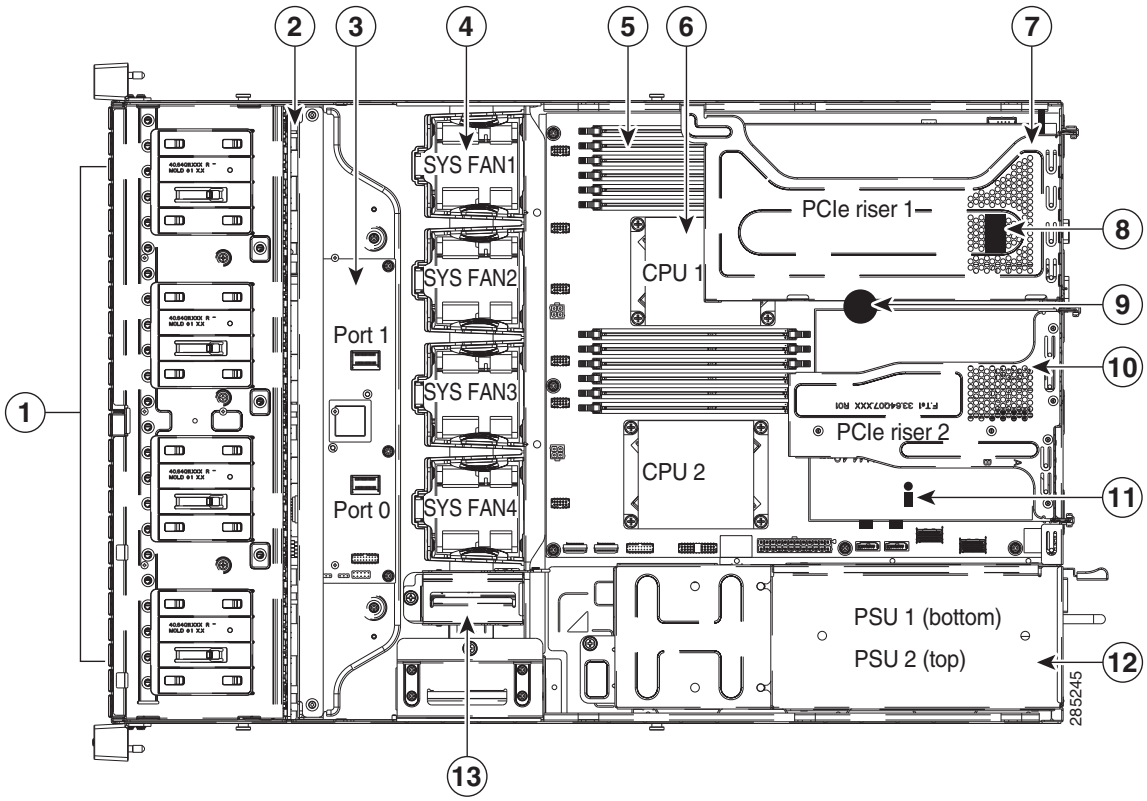
Step 2 Replace the front chassis panel:

- **a.** Set the front chassis panel back in place, with its wrap-around front edge about 1/4 inch (1.27 cm) forward of the chassis front edge.
- **b.** Slide the front chassis panel toward the server rear to lock it in place. The wrap-around front edge of the panel must wrap around the chassis front edge.
- **c.** Replace the three screws that secure the panel to the chassis (see Figure 3-3).
- **d.** Replace the top cover to the server as described in Removing and Replacing the Server Top Cover, page 3-7.

Replaceable Component Locations

This section shows the locations of the components that are discussed in this chapter. The view in Figure 3-4 is from the top down with the top cover, front chassis panel, and air baffle removed.

Figure 3-4 Replaceable Component Locations



1	Drives (hot-swappable, accessed through front panel)	**8**	Internal USB 2.0 port on motherboard
2	Drive backplane (optionally either 24-drive or 16-drive)	**9**	RTC battery on motherboard
3	SAS expander (with 24-drive backplane only)	**10**	PCIe riser 2 (three half-height slots)
4	Fan modules (four)	**11**	Trusted platform module socket on motherboard
5	DIMM slots on motherboard (twelve)	**12**	Power supplies (two, hot-swappable access through rear panel)
6	CPUs and heatsinks (up to two)	**13**	RAID backup unit mounting cage (holds up to two units)
7	PCIe riser 1 (two full-height slots)		

Serial Number Location

The serial number for the server is printed on a label on the top of the server, near the front.

Color-Coded Touch Points

This server has color-coded touch points that indicate thumbscrews and latches on replaceable and hot-swappable components.

- Hot-swappable components have green plastic touch points. This includes the internal cooling fans and the power supplies. (An exception is the drive trays on the front panel, which are hot-swappable but not green).
- Some replaceable but non-hot-swappable components have light-blue plastic touch-points.

Installing or Replacing Server Components

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**
Statement 1029

Warning **Class 1 laser product.**
Statement 1008

Caution When handling server components, wear an ESD strap to avoid damage.

Tip You can press the Identification button on the front panel or rear panel to turn on a flashing Identification LED on the front and rear panels of the server. This allows you to locate the specific server that you are servicing when you go to the opposite side of the rack. You can also activate these LEDs remotely by using the CIMC interface.See the "Status LEDs and Buttons" section on page 3-2 for locations of these LEDs.

This section describes how to install and replace server components, and it includes the following topics:

- Replacing Hard Drives or Solid State Drives, page 3-12
- Replacing a Drive Backplane, page 3-14
- Replacing Fan Modules, page 3-18
- Replacing DIMMs, page 3-20
- Replacing CPUs and Heatsinks, page 3-25
- Replacing the Motherboard RTC Battery, page 3-31
- Replacing a PCIe Riser, page 3-33
- Replacing a PCIe Card, page 3-35
- Replacing a SuperCap Power Module (RAID Backup Unit), page 3-41
- Replacing an Internal USB Flash Drive, page 3-43
- Installing a Trusted Platform Module, page 3-45
- Replacing a SCU Upgrade ROM Module, page 3-48
- Replacing a Software RAID Key Module, page 3-49
- Replacing Power Supplies, page 3-51

Replacing Hard Drives or Solid State Drives

This section includes the following information:

- Drive Population Guidelines, page 3-12
- Drive Replacement Procedure, page 3-13

Drive Population Guidelines

The server is orderable in two different versions, each with one of two different front panel/backplane configurations:

- Cisco UCS C24 (small form-factor (SFF) drives, with 24-drive backplane and expander). Holds up to twenty-four 2.5-inch hard drives or solid state drives.
- Cisco UCS C24 (small form-factor (SFF) drives, with 16-drive backplane, no expander). Holds up to sixteen 2.5-inch hard drives or solid state drives.

Note When the server has the 16-drive backplane, only the first 16 drive bays are used.

- Cisco UCS C24 (large form-factor (LFF) drives, with 12-drive backplane and expander). Holds up to twelve 3.5-inch hard drives.

The drive-bay numbering is shown in Figure 3-5 and Figure 3-6.

Figure 3-5 Drive Numbering, Small Form Factor

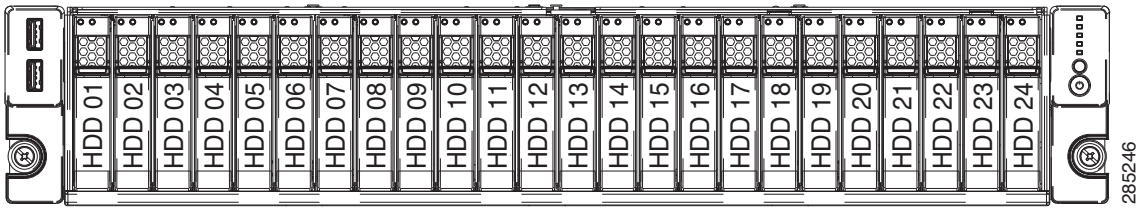
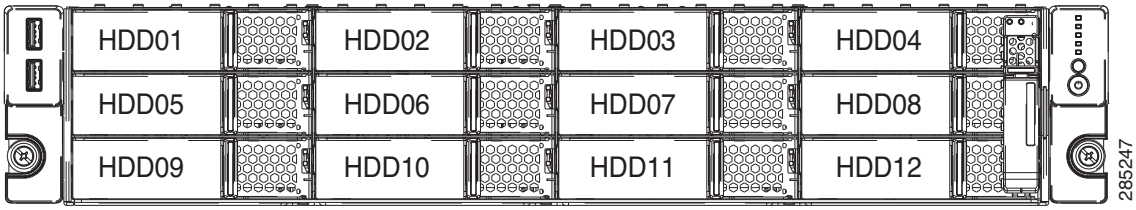


Figure 3-6 Drive Numbering, Large Form Factor



Observe these drive population guidelines for optimal performance:

- When populating drives, add drives in the lowest numbered bays first (populate HDD01 first).

Note **Sixteen-drive backplane option**: If your SFF-drives server has the 16-drive backplane installed, only the first 16 drive bays are used, with population order HDD1 to HDD16. Keep blanking trays in all empty bays to ensure optimal air flow and cooling.

- Keep an empty drive blanking tray in any unused bays to ensure optimal air flow and cooling.

- You can mix hard drives and solid state drives in the same server. However, You cannot configure a logical volume (virtual drive) that contains a mix of hard drives and SSDs. That is, when you create a logical volume, it must contain all hard drives or all SSDs.

Note The LFF-drives version of the server does not support 3.5-inch solid state drives.

Drive Replacement Procedure

To replace or install a hot-pluggable drive, follow these steps:

Tip You do not have to shut down or power off the server to replace hard drives or solid state drives (SSDs) because they are hot-pluggable.

Step 1 Remove the drive that you are replacing or remove a blank drive tray from an empty bay:

a. Press the release button on the face of the drive tray. See Figure 3-7.

b. Grasp and open the ejector lever and then pull the drive tray out of the slot.

c. If you are replacing an existing drive, remove the four drive-tray screws that secure the drive to the tray and then lift the drive out of the tray.

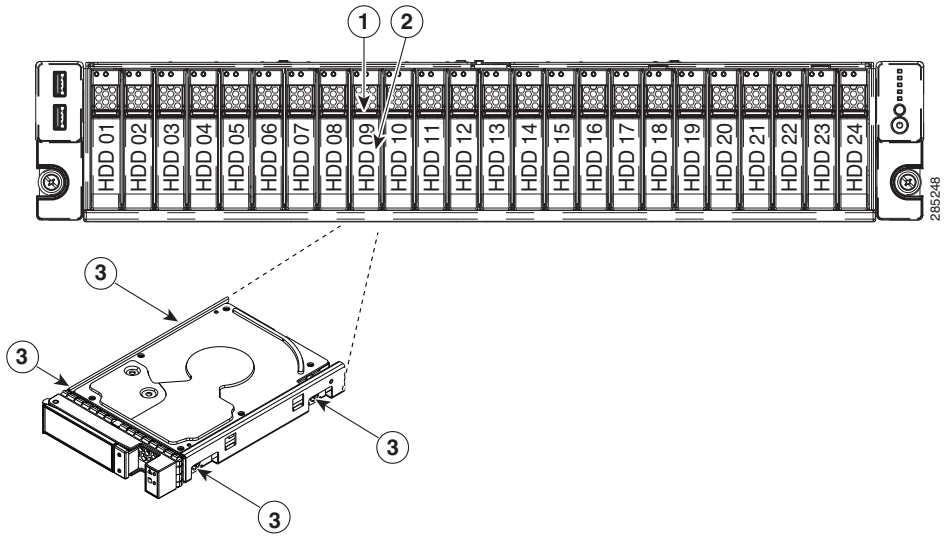
Step 2 Install a new drive:

a. Place a new drive in the empty drive tray and replace the four drive-tray screws.

b. With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.

c. Push the tray into the slot until it touches the backplane, then close the ejector lever to lock the drive in place.

Figure 3-7 Replacing Hard Drives



1	Release button	**3**	Drive tray securing screws (4)
2	Ejector lever		–

Replacing a Drive Backplane

Note The Small Form-Factor (24-drive or 16-drive) and Large Form-Factor (12-drive) backplanes are factory-configurable options. When replacing a backplane, you must replace it with the same version of the backplane.

To install or replace a drive backplane, follow these steps:

Step 1 Prepare the server for component replacement:

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Remove the front chassis panel as described in Removing and Replacing the Front Chassis Panel, page 3-8.

Step 2 Remove all drives and any empty drive trays from the server.

Step 3 Disconnect all cables from the backplane.

Tip Label the cables as you remove them to aid replacement.

Step 4 Disconnect all cables from the SAS expander card.

Step 5 Remove the two screws that secure the backplane assembly to the chassis floor (see Figure 3-8).

Step 6 Lift the backplane assembly, including steel tray and expander card straight up from the chassis.

Step 7 Remove the SAS expander card from the backplane assembly:

a. Remove the three screws that secure the SAS expander to the backplane assembly steel tray (see Figure 3-9).

b. Pull the SAS expander from the sockets on the drive backplane and then set the SAS expander aside on an antistatic surface.

Step 8 Install the SAS expander card to the new backplane assembly:

a. Push the two connectors on the SAS expander into the two sockets on the backplane assembly.

b. Install the three screws that secure the SAS expander to the backplane assembly steel tray (see Figure 3-9).

Step 9 Align the new backplane assembly within the chassis walls, and then lower it evenly to the chassis floor until the screw-holes in the assembly align with the corresponding screw-holes in the chassis floor.

Step 10 Install the two screws that secure the backplane assembly to the chassis floor.

Step 11 Reconnect all cables to the SAS expander.

Step 12 Reconnect all cables to the backplane.

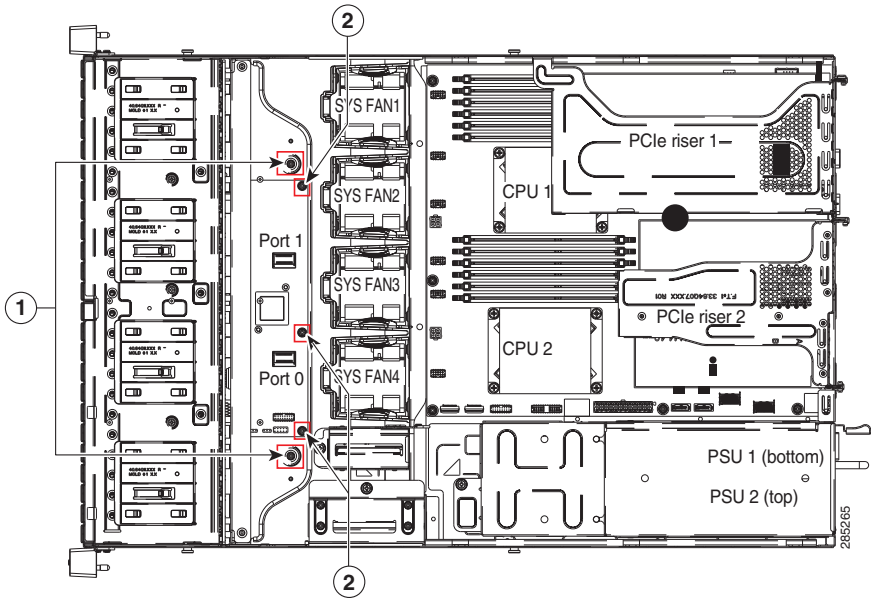
Step 13 Replace all drives and drives trays to the drive bays.

Step 14 Replace the front chassis panel.

Step 15 Replace the top cover.

Step 16 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-8 Replacing the Drive Backplane



1	Backplane assembly securing screws (two)	**2**	SAS expander securing screws (three)

Replacing a SAS Expander

The SAS expander is a card that plugs directly into the drive backplane. The SAS expander allows control of up to 24 drives with one RAID controller card. See Appendix C, "RAID Controller Considerations" for more information about supported RAID controllers.

Note The SAS expander is required for the SFF 24-drive option and the LFF 12-drive option. The SFF 16-drive option does not use the SAS expander.

To install or replace a SAS expander, follow these steps:

Step 1 Prepare the server for component replacement:

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Remove the front chassis panel as described in Removing and Replacing the Front Chassis Panel, page 3-8.

Step 2 Disconnect all cables from the SAS expander.

Tip Label the cables as you remove them to aid replacement.

Step 3 Remove the SAS expander:

a. Remove the three screws that secure the SAS expander to the backplane assembly steel tray (see Figure 3-9).

b. Grasp both ends of the SAS expander and pull evenly to disengage it from the sockets on the drive backplane. Do not tilt the SAS expander until it is free from the sockets on the backplane.

Step 4 Install the new SAS expander:

a. Lower the SAS expander to its position on the backplane assembly. Return the SAS expander to a horizontal position before you begin pushing it into the backplane sockets.

a. Evenly push the two connectors on the edge of the new SAS expander into the two sockets on the backplane. Stop when the screw-holes in the SAS expander align with the screw-holes in the backplane assembly steel tray.

b. Install the three screws that secure the SAS expander to the backplane assembly steel tray (see Figure 3-9).

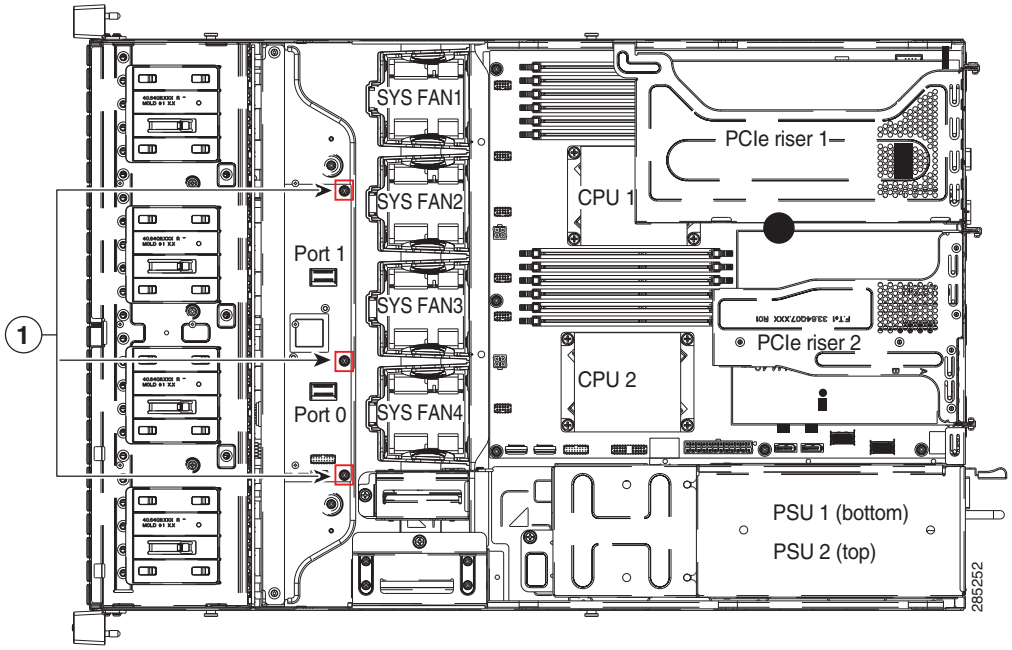
Step 5 Reconnect SAS cables to the new SAS expander.

Step 6 Replace the front chassis panel.

Step 7 Replace the top cover.

Step 8 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-9 Replacing the SAS Expander



1	SAS expander securing screws (three)		–

Replacing Fan Modules

The four hot-pluggable fan modules in the server are numbered as follows when you are facing the front of the server.

Figure 3-10 Fan Module Numbering

FAN1	FAN2	FAN3	FAN4

To replace or install a hot-pluggable fan module, follow these steps:

Caution You do not have to shut down or power off the server to replace fan modules because they are hot-pluggable. However, to maintain proper cooling, do not operate the server for more than one minute with any fan module removed.

Step 1 Remove a fan module that you are replacing (see Figure 3-11):

a. 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.

b. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

c. Grasp and squeeze together the two green plastic finger-latches on the top of the fan module and then lift straight up to disengage the fan from the fan tray connector.

Step 2 Install a new fan module:

a. Set the new fan module in place, aligning the connector on the fan module with the connector on the fan tray (see Figure 3-11).

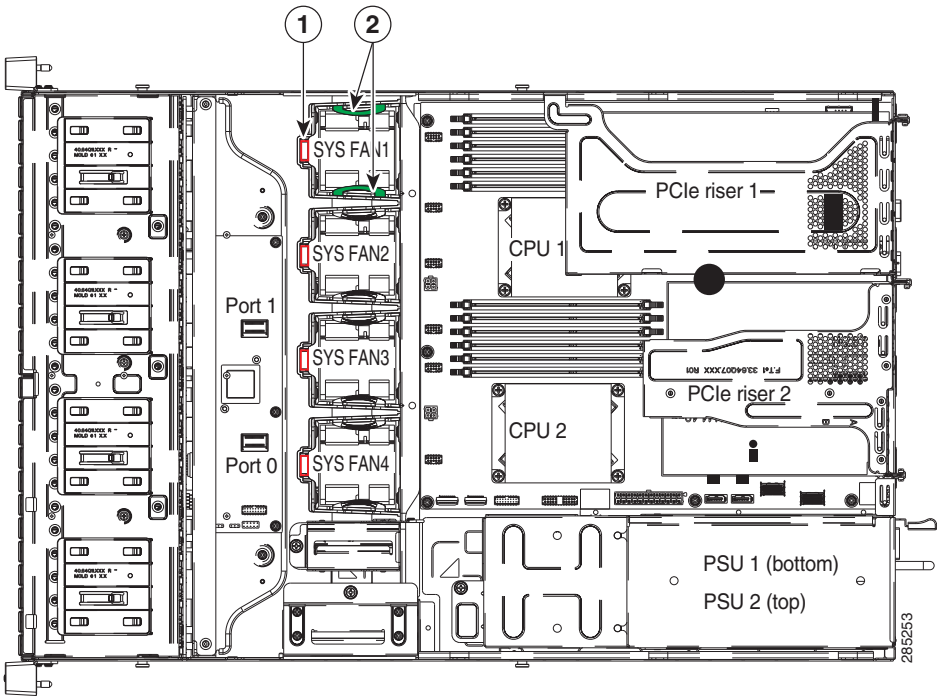
Note The arrow on the top of the fan module should point toward the rear of server.

b. Press down gently on the fan module until the finger-latches click and lock in place.

c. Replace the top cover.

d. Replace the server in the rack.

Figure 3-11 Replacing Fan Modules



1	Fan tray connector (one on each fan module)	**3**	Connector on underside of fan module
2	Finger latches (two on each fan module)		

Replacing DIMMs

This section includes the following topics:

- Memory Performance Guidelines and Population Rules, page 3-20
- DIMM Replacement Procedure, page 3-23

Caution DIMMs and their sockets are fragile and must be handled with care to avoid damage during installation.

Caution Cisco does not support 3rd-party DIMMs. Using non-Cisco DIMMs in the server might result in system problems or damage to the motherboard.

Note To ensure the best server performance, it is important that you are familiar with memory performance guidelines and population rules before you install or replace memory.

Memory Performance Guidelines and Population Rules

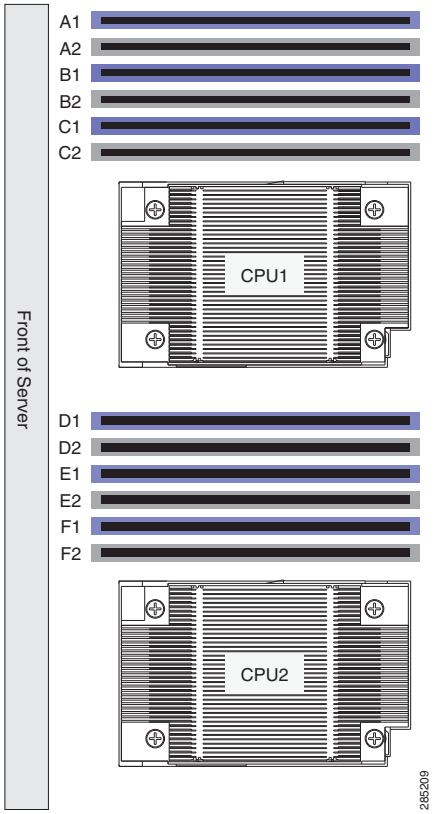
This section describes the type of memory that the server requires and its effect on performance. The section includes the following topics:

- DIMM Slot Numbering, page 3-20
- DIMM Population Rules, page 3-21
- Memory Mirroring, page 3-23

DIMM Slot Numbering

Figure 3-12 shows the numbering of the DIMM slots.

Figure 3-12 DIMM Slots and CPUs



DIMM Population Rules

Observe the following guidelines when installing or replacing DIMMs:

- Each CPU supports three memory channels.
  - CPU1 supports channels A, B, and C.
  - CPU2 supports channels D, E, and F

Note In a single-CPU system, the maximum number of DIMMs is six (only the six slots supported by CPU1).

- Each channel has two DIMM slots (for example, channel A = slots A1 and A2).
  - A channel can operate with one or two DIMMs installed.
  - If a channel has only one DIMM, populate slot 0 first (the blue slot).
- When both CPUs are installed, populate the DIMM slots of each CPU identically.
  - Fill blue slots in the channels first: A1, D1, B1, E1, C1, F1
  - Fill black slots in the channels second: A2, D2, B2, E2, C2, F2
- Any DIMM installed in a DIMM socket for which the CPU is absent is not recognized. In a single-CPU configuration, populate the channels for CPU1 only.

- Although 1600 MHz DIMMs can be run in Power Savings Mode (1.35 V operation), 1600 MHz operation is supported only when the DDR mode is set to Performance Mode (see "Enabling Low-Voltage DIMM Operation.") A 1600 MHz DIMM set to Power Savings Mode operates at 1066 MHz.
- Observe the DIMM mixing rules shown in Table 3-3.

Table 3-3 DIMM Mixing Rules

DIMM Parameter Mixed	Mix Across Single Channel?	Mix Across Multiple Channels?
DIMM size (4, 8, 16 GB)	No—Must be same size in channel.	Yes—Can be different sizes in server.
DIMM speed (1333 or 1600 MHz)	No—Must be same speed in channel.	No—Must be the same speed in server.
DIMM type (RDIMM or UDIMM)	No—Must be same type in channel.	No—Must be the same type in server.

- Memory mirroring reduces the amount of memory available by 50% because only one of the two populated channels provides data. When memory mirroring is enabled, DIMMs must be installed in sets of four as described in Memory Mirroring, page 3-23.
- Note the following restrictions when using UDIMMs. Even though a UDIMM might be rated at 1600 MHz, actual operational speeds are slower because of the Intel implementation.
  - In Performance Mode (1.5 V operation), UDIMMs run at 1333 MHz in 1 DPC configurations or at 1066 MHz in 2 DPC configurations.
  - In Power Saving Mode (1.35 V operation), UDIMMs run at 1333 MHz in 1 DPC configurations or at 1066 MHz in 2 DPC configurations.

Enabling Low-Voltage DIMM Operation

You can enable low voltage (1.35 V) DIMM operation for all DIMMs in the server. There is a setting in the BIOS Setup utility that you can use to change the DDR memory mode to Power Saving mode, as described in the following procedure:

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

Step 2 Select the **Advanced** tab.

Step 3 Select **Low Voltage DDR Mode**.

Step 4 In the pop-up window, select either **Power Saving** or **Performance Mode**:

- Power Saving Mode–Prioritizes low-voltage memory operation.
- Performance Mode–Prioritizes performance memory operation. If you mix low-voltage DIMMs with standard DIMMs, the system defaults to this setting.

Step 5 Press **F10** to save your changes and exit the setup utility.

Memory Mirroring

When memory mirroring is enabled, the memory subsystem simultaneously writes identical data to two channels. If a memory read from one of the channels returns incorrect data due to an uncorrectable memory error, the system automatically retrieves the data from the other channel. A transient or soft error in one channel does not affect the mirrored data, and operation continues unless there is a simultaneous error in exactly the same location on a DIMM and its mirrored DIMM. Memory mirroring reduces the amount of memory available to the operating system by 50% because only one of the two populated channels provides data.

If you choose to enable memory mirroring, populate the DIMM slots in the order shown in Table 3-4 or Table 3-5.

Table 3-4 Two-CPU Memory Mirroring DIMM Population

Number of DIMMs per CPU	CPU 1 Population	CPU2 Population
2	A1; B1	D1; E1
4	A1, B1; A2, B2	D1, E1; D2, E2

Table 3-5 One-CPU Memory Mirroring DIMM Population

Number of DIMMs per CPU	CPU 1 Population	CPU2 Population
2	A1; B1	CPU2 slots not available
4	A1, B1; A2, B2	CPU2 slots not available

DIMM Replacement Procedure

To install a DIMM assembly, follow these steps:

Step 1 Remove the DIMMs that you are replacing:

a. Power off the server as described in Shutting Down and Powering Off the Server, page 3-6.

b. 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.

c. Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-7.

d. Remove PCIe riser 1 to provide clearance and set it aside on an antistatic surface (see Replacing a PCIe Riser, page 3-33).

e. Remove the plastic air baffle that covers the DIMM slots and CPUs.

f. Open the ejector levers at both ends of the DIMM slot, then lift the DIMM out of the slot.

Step 2 Install a new DIMM:

Note Before installing DIMMs, refer to the population guidelines. See Memory Performance Guidelines and Population Rules, page 3-20.

a. Align the new DIMM with the empty slot on the motherboard. Use the alignment key in the DIMM slot to correctly orient the notch on the bottom edge of the DIMM.

b. Push down evenly on the top corners of the DIMM until it is fully seated and the ejector levers on both ends lock into place.

c. Replace the plastic air baffle over the DIMM slots.

d. Replace PCIe riser 1 to it slot. See Replacing a PCIe Riser, page 3-33.

e. Replace the top cover.

f. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Replacing CPUs and Heatsinks

This server can have up to two CPUs. Each CPU supports three DIMM channels (six DIMM slots). See Figure 3-12. This section includes the following topics:

- Single-CPU Restrictions, page 3-25
- Additional CPU-Related Parts To Order With RMA Replacement Motherboards, page 3-25
- Additional CPU-Related Parts To Order With RMA Replacement Motherboards, page 3-25

Single-CPU Restrictions

The minimum configuration is that the server must have at least CPU1 installed. Install CPU1 first, then CPU2.

The following restrictions apply when using a single-CPU configuration:

- The maximum number of DIMMs is six (only the six slots controlled by CPU1 are active).
- PCIe riser 2 is unavailable (PCIe slots 3, 4, and 5).

Additional CPU-Related Parts To Order With RMA Replacement Motherboards

When a return material authorization (RMA) of the motherboard or CPU is done on a Cisco UCS C-series server, there are additional parts that might not be included with the CPU or motherboard spare bill of materials (BOM). The TAC engineer might need to add the additional parts to the RMA to help ensure a successful replacement.

- Scenario 1—You are re-using the existing heatsinks:
  - Heat sink cleaning kit (UCSX-HSCK=)
  - Thermal grease kit for C24 (UCS-CPU-GREASE=)
  - Intel CPU Pick-n-Place tool for EP CPUs (UCS-CPU-EN-PNP=)
- Scenario 2—You are replacing the existing heatsinks:
  - Heat sink (UCSC-HS-EN-M3=)
  - Heat sink cleaning kit (UCSX-HSCK=)
  - Intel CPU Pick-n-Place tool for EP CPUs (UCS-CPU-EN-PNP=)

A CPU heatsink cleaning kit is good for up to four CPU and heatsink cleanings. The cleaning kit contains two bottles of solution, one to clean the CPU and heatsink of old thermal interface material and the other to prepare the surface of the heatsink.

New heatsink spares have preinstalled thermal interface material covered by a small sheet of plastic. It is important to clean the old thermal interface material off of the CPU prior to installing the heatsinks. Therefore, when ordering new heatsinks it is still necessary to order the heatsink cleaning kit at a minimum.

CPU Replacement Procedure

Caution CPUs and their motherboard sockets are fragile and must be handled with care to avoid damaging pins during installation. The CPUs must be installed with heatsinks and their thermal pads to ensure proper cooling. Failure to install a CPU correctly might result in damage to the server.

Caution The Pick-and-Place tools used in this procedure are required to prevent damage to the contact pins between the motherboard and the CPU. Do not attempt this procedure without the required tools, which are included with each CPU option kit. If you do not have the tool, you can order a spare (Cisco PID UCS-CPU-EN-PNP).

To install or replace a CPU heatsink and CPU, follow these steps:

Step 1 Remove the CPU and heatsink that you are replacing:

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

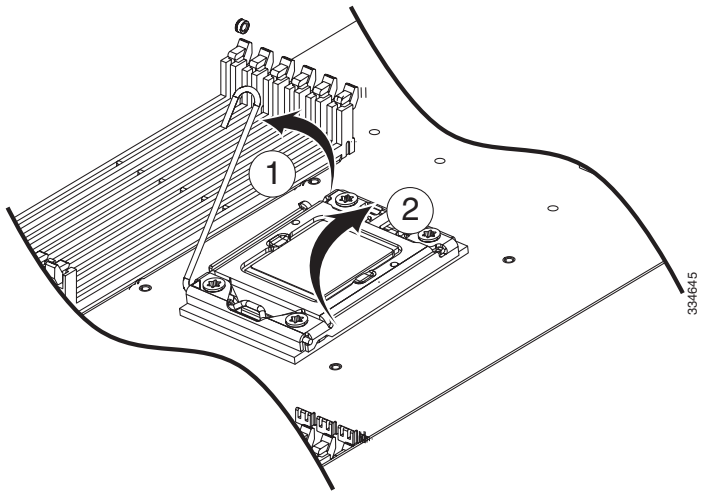
d. Remove the internal air baffle from the server to provide access to the CPUs.

e. Use a #2 Phillips-head screwdriver to loosen the four captive screws that secure the heatsink and then lift it off of the CPU.

Note Alternate loosening each screw evenly to avoid damaging the heatsink or CPU.

f. Unclip the CPU retaining latch, then open the hinged CPU cover plate. See Figure 3-13.

Figure 3-13 CPU Socket Latches

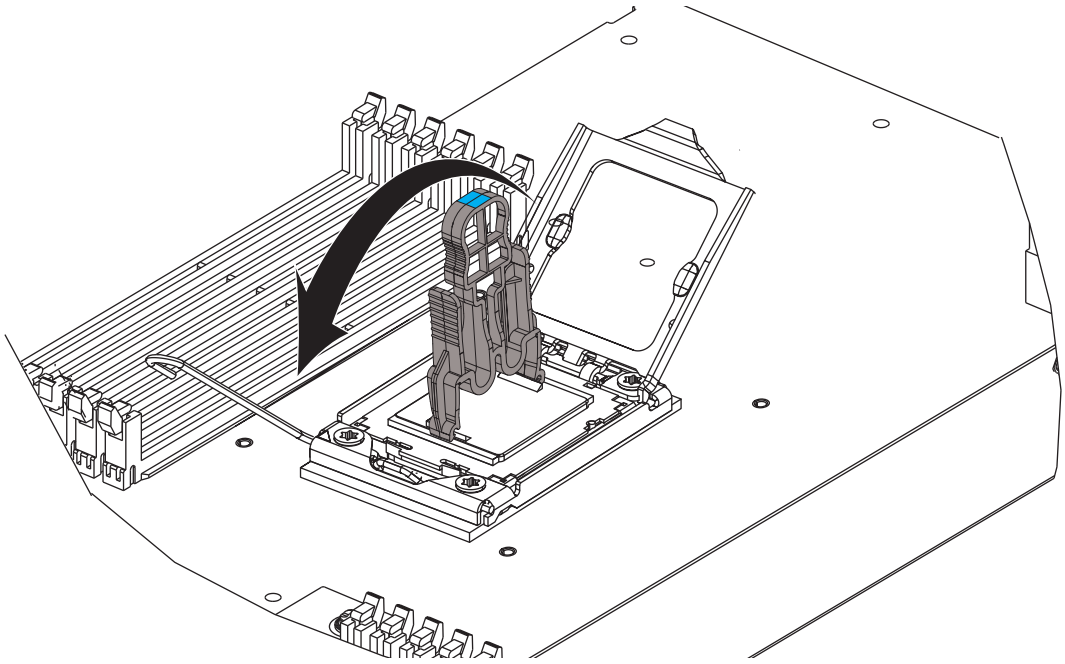


1	Heatsink screws (four)	**4**	Hinged CPU cover plate
2	Heatsink	**5**	CPU
3	CPU retaining latch		

Step 2 Remove a protective cap or an old CPU from the socket (if present):

- If you are removing an old CPU, skip to Step 3.
- If you are installing a new CPU to a socket that was shipped empty, the socket has a protective cap that is intended to prevent bent contact pins. Use the tool as shown in Figure 3-14 to grasp the protective cap and then pivot to remove the cap.

Figure 3-14 Protective Cap Removal Tool



Step 3 Remove an old CPU:

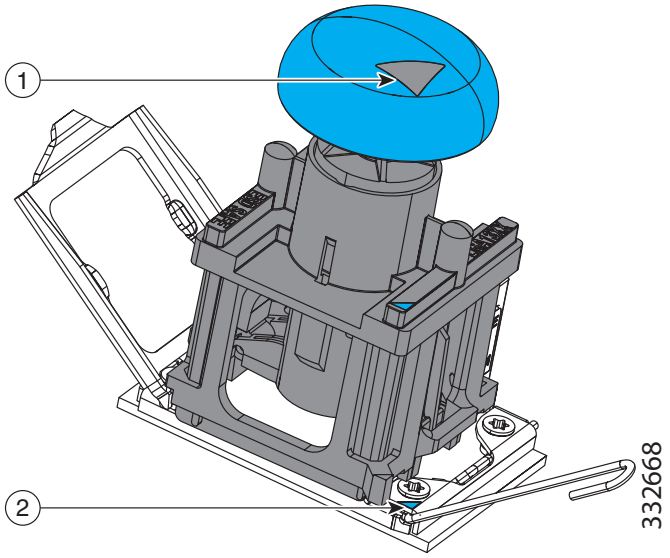
a. Set the Pick-and-Place tool on the CPU in the socket, aligning the arrow on the tool with the registration mark on the socket (the small triangular mark). See Figure 3-15.

b. Press the top button on the tool to grasp the installed CPU.

c. Lift the tool and CPU straight up.

d. Press the top button on the tool to release the old CPU on an anti-static surface.

Figure 3-15 Removing or Inserting a CPU



1	Arrow on tool	**2**	Registration mark on CPU socket

Step 4 Insert the new CPU into the Pick-and-Place tool:

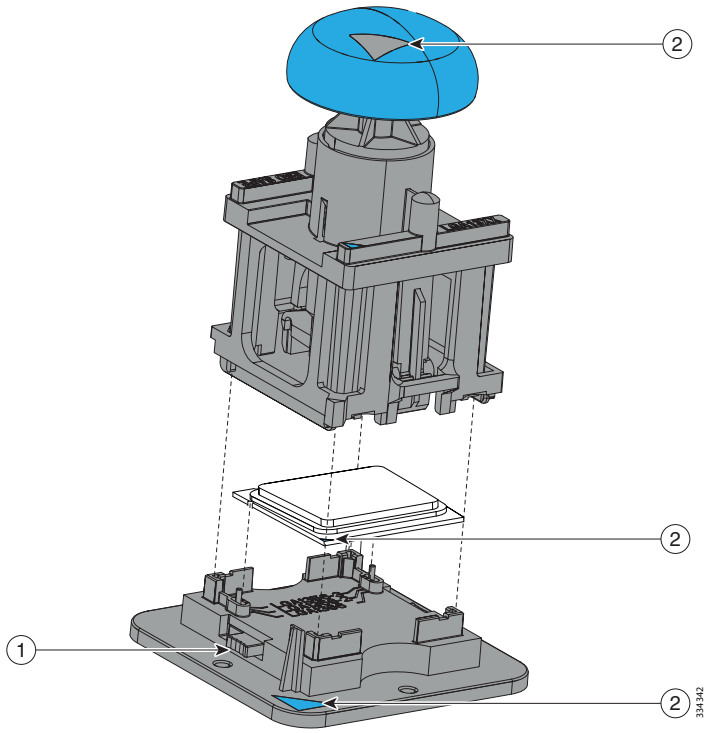
a. Remove the new CPU from the packaging and place it on the pedestal that is included in the kit. Align the registration mark on the corner of the CPU with the arrow on the corner of the pedestal (see Figure 3-16).

b. Set the Pick-and-Place tool on the CPU pedestal, aligning the arrow on the tool with the arrow on the corner of the pedestal. Make sure that the tabs on the tool are fully seated in the slots on the pedestal.

c. Press the top button on the tool to grasp and lock in the CPU.

d. Lift the tool and CPU straight up off the pedestal.

Figure 3-16 CPU and Pick-and-Place Tool on Pedestal



1	Arrow marks for alignment		–

Step 5 Install a new CPU:

a. Set the Pick-and-Place tool with CPU over the empty CPU socket on the motherboard.

Note Align the arrow on the top of the tool with the registration mark (small triangle) that is stamped on the metal of the CPU socket, as shown in Figure 3-15.

b. Press the top button on the tool to set the CPU into the socket. Remove the empty tool.

c. Close the hinged CPU cover plate.

d. Clip down the CPU retaining latch. See Figure 3-13.

Step 6 Install a heatsink:

Caution The heatsink must have a new, undamaged thermal pad on the heatsink-to-CPU surface to ensure proper cooling. If you are replacing a heatsink that was previously used, you must remove the old thermal pad. If you are installing a new heatsink, skip to step d. below.

a. Apply an alcohol-based cleaning solution to the old thermal pad and let it soak for a least 15 seconds.

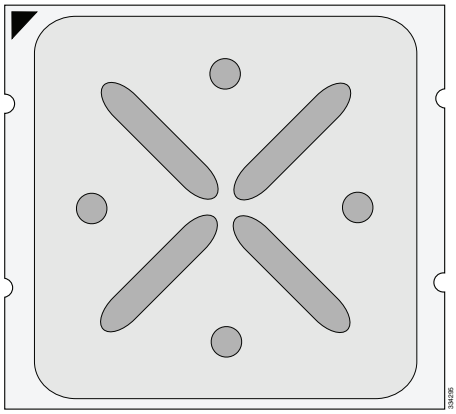
b. Wipe all of the old thermal pad off the old heatsink using a soft cloth that will not scratch the heatsink surface.

c. Apply thermal grease from an included syringe to the top of the CPU.

Apply about 2 cubic centimeters of grease (about half the syringe contents) to the top of the CPU in the pattern that is shown in Figure 3-17.

Note If you do not have a syringe of thermal grease, you can order a spare (Cisco PID UCS-CPU-GREASE).

Figure 3-17 Thermal Grease Application Pattern



d. For a new heatsink, peel the protective film from the thermal pad that is on the bottom of the new heatsink.

Note Do not apply a syringe of thermal grease if you are installing a new heatsink that already has a pre-applied thermal pad.

e. Align the heatsink captive screws with the motherboard standoffs, then use a Number 2 Phillips-head screwdriver to tighten the captive screws evenly.

Note Alternate tightening each screw evenly to avoid damaging the heatsink or CPU.

f. Replace the top cover.

g. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Replacing the Motherboard RTC Battery

Warning **There is danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** [Statement 1015]

The real-time clock (RTC) battery retains system settings when the server is disconnected from power. The battery type is CR2032. Cisco supports the industry-standard CR2032 battery, which can be purchased from most electronic stores.

Step 1 Remove the RTC battery (see Figure 3-18):

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Locate the RTC battery on the motherboard between the PCIe risers (see Figure 3-18).

e. Use a small screwdriver or pointed object to push aside the metal clip that holds the battery in the holder.

Note If you have difficulty reaching the battery because of cards in the PCIe risers, remove PCIe riser 1 to provide access. See Replacing a PCIe Riser, page 3-33.

f. Lift the battery from the holder.

Step 2 Install an RTC battery:

a. Insert the battery into its holder positive-side-up and press down until it clicks in place.

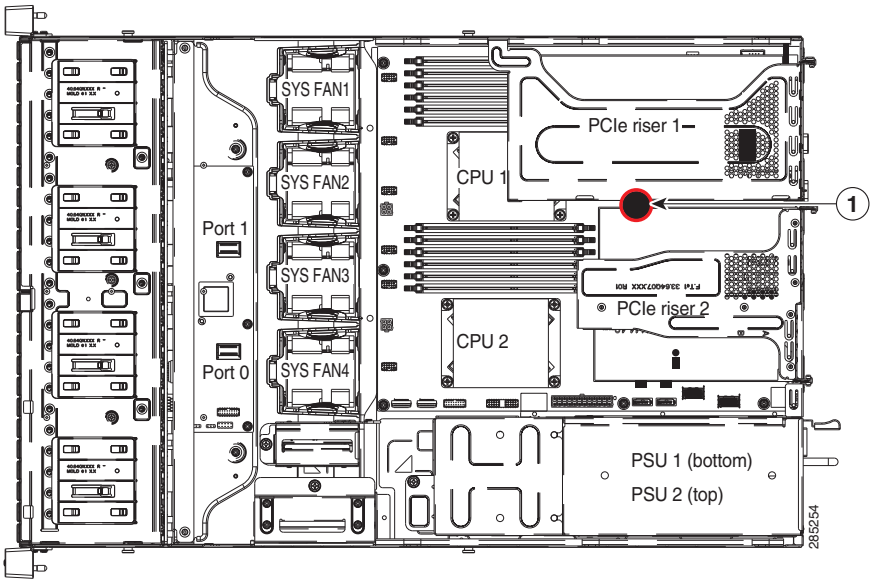
Note The positive side of the battery marked "3V+" should face upward.

b. If you removed PCIe riser 1, replace it to its slot. See Replacing a PCIe Riser, page 3-33.

c. Replace the top cover.

d. Replace the server in the rack, replace cables, and power on the server by pressing the **Power** button.

Figure 3-18 Replacing the Motherboard RTC Battery



1	RTC battery holder on motherboard		–

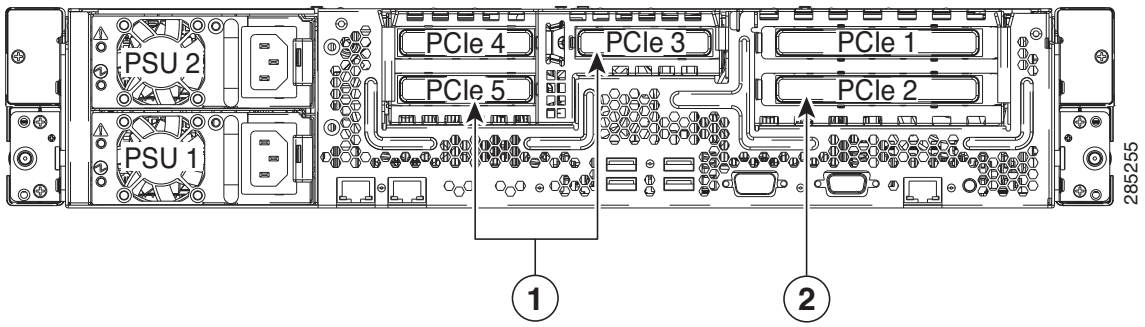
Replacing a PCIe Riser

The server contains two toolless PCIe risers for horizontal installation of PCIe cards.

See PCIe Slots, page 3-35 for specifications of the PCIe slots on the risers.

Note PCIe riser 2 (slots 3, 4, and 5) is not available in single-CPU configurations.

Figure 3-19 Rear Panel, Showing PCIe Slots



1	PCIe riser 2 slots (three half-height slots)	**2**	PCIe riser 1 slots (two full-height slots)

To install or replace a PCIe riser, follow these steps:

Step 1 Remove the PCIe riser that you are replacing:

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Disconnect all cables from any PCIe cards that are installed in the PCIe riser.

e. Grasp both ends of the riser and evenly pull straight up to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic surface.

f. If the riser has a card installed, remove the card from the riser (see Replacing a PCIe Card, page 3-35).

Step 2 Install a new PCIe riser:

a. If you removed a card from the old PCIe riser, install the card to the new riser (see Replacing a PCIe Card, page 3-35).

b. Position the PCIe riser over its socket on the motherboard and over its alignment points in the chassis (see Figure 3-20).

Caution Make sure that the circuit board connector of the riser is aligned correctly with the motherboard socket before you push down to seat the riser in the next step.

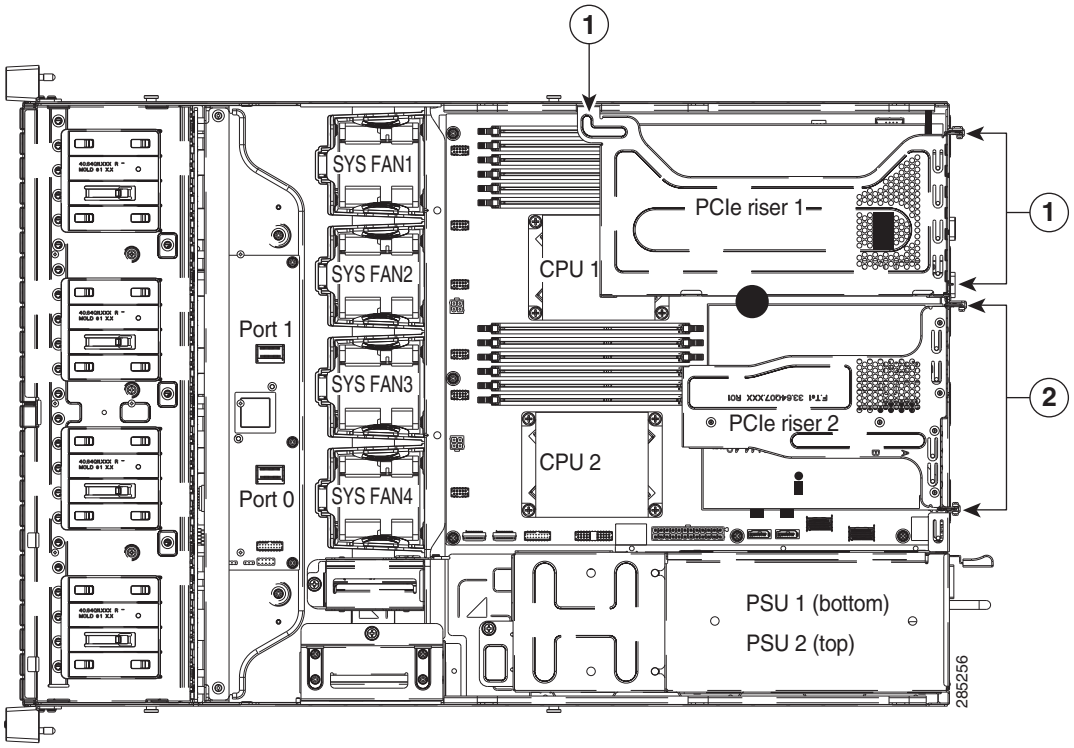
c. Carefully push down on both ends of the PCIe riser to fully engage its circuit board connector with the socket on the motherboard.

d. Reconnect cables to any PCIe cards installed in the riser.

e. Replace the top cover.

f. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-20 Replacing the PCIe Riser



1	PCIe riser 1 alignment point locations (three)	**2**	PCIe riser 2 alignment point locations (two)

Replacing a PCIe Card

Caution Cisco supports all PCIe cards qualified and sold by Cisco. PCIe cards not qualified or sold by Cisco are the responsibility of the customer. Although Cisco will always stand behind and support the C-Series rack-mount servers, customers using standard, off-the-shelf, third-party cards must go to the third-party card vendor for support if any issue with that particular third-party card occurs.

This section includes the following topics:

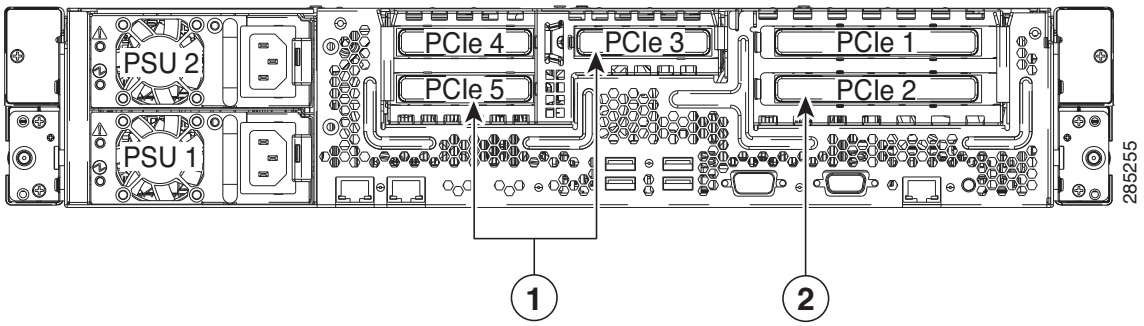
- PCIe Slots, page 3-35
- RAID Card Firmware Compatibility, page 3-36
- Replacing a PCIe Card, page 3-36
- Special Considerations for Cisco UCS Virtual Interface Cards, page 3-38
- RAID Controller Card Cable Routing, page 3-38
- Installing Multiple PCIe Cards and Resolving Limited Resources, page 3-38

PCIe Slots

The server contains two PCIe risers for horizontal installation of PCIe cards. See Figure 3-21 and Table 3-6.

Note In a single-CPU system, PCIe riser 2 (slots 3, 4, 5) is not available.

Figure 3-21 Rear Panel, Showing PCIe Slots



1	PCIe riser 2 slots (slots 3, 4, 5)	**2**	PCIe riser 1 slots (slots 1, 2)

Table 3-6 PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Card Length[1]	Card Height [2]	NCSI[3] Support
1	Gen-3 x16	x16 extended	Full length	Full-height	Yes[4]
2	Gen-3 x4	x8 connector	1/2 length	Full-height	No
3	Gen-3 x8	x16 connector	1/2 length	Half-height	No
4	Gen-3 x8	x8 connector	1/2 length	Half-height	No
5	Gen-3 x4	x8 connector	1/2 length	Half-height	No

1. This is the supported length because of internal clearance.
2. This is the size of the rear panel opening.
3. Network Communications Services Interface protocol.
4. Slot 1 can operate when the server is in standby power mode.

RAID Card Firmware Compatibility

If the PCIe card that you are installing is a RAID controller card, firmware on the RAID controller must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the server. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: HUU Guides

Replacing a PCIe Card

Note If you are installing a Cisco UCS Virtual Interface Card, there are prerequisite considerations. See Special Considerations for Cisco UCS Virtual Interface Cards, page 3-38.

Note If you are installing a RAID controller card, see RAID Controller Considerations, page C-1for more information about supported cards and cabling.

To install or replace a PCIe card, follow these steps:

Step 1 Remove a PCIe card (or a blank filler panel) from the PCIe riser assembly:

a. Shut down and power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in the "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Disconnect cables from the PCIe cards that you are replacing.

Tip Label the cables when you disconnect them to aid correct connection to the new card.

e. Grasp both ends of the riser and evenly pull straight up to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic surface.

f. Remove the single screw that secures the tab of the card to the riser.

g. Pull evenly on both ends of the card to disengage it from the socket on the riser (or remove a blanking panel) and then set the card aside.

Step 2 Install a PCIe card:

a. Align the new card with the empty socket on the riser.

b. Push down evenly on both ends of the card until it is fully seated in the socket.

Ensure that the card rear panel tab sits flat against the riser rear panel opening.

c. Replace the screw that secures the tab of the card to the riser.

d. Position the riser over its socket on the motherboard and over its alignment features in the chassis (see Figure 3-20).

Caution Make sure that the circuit board connector of the riser is aligned correctly with the motherboard socket before you push down to seat the riser in the next step.

e. Carefully push down on both ends of the PCIe riser to fully engage its circuit board connector with the socket on the motherboard.

f. Connect cables to the PCIe card. See RAID Controller Considerations, page C-1 for more information about supported cards and cabling.

g. Replace the top cover.

h. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

i. If you replaced a RAID controller card, continue with Restoring RAID Configuration After Replacing a RAID Controller, page C-22.

Special Considerations for Cisco UCS Virtual Interface Cards

Table 3-7 describes the requirements for the supported Cisco UCS virtual interface cards (VICs).

Table 3-7 Cisco UCS C24 Requirements for Virtual Interface Cards

Virtual Interface Card (VIC)	Number of VICs Supported in Server	Slots That Support VICs [1]	Primary Slot For UCS Integration or Cisco Card NIC Mode	Minimum CIMC Firmware	Minimum VIC Firmware For Use With UCS Integration	Minimum Nexus OS on an Upstream Nexus Fabric Interconnect
Cisco UCS VIC P81E[2] N2XX-ACPCI01	2	PCIE 1 PCIE 2	PCIE 1	1.4(5)	2.0(2)	5.0
Cisco UCS VIC 1225 UCSC-PCIE-CSC-02	2	PCIE 1 PCIE 2	PCIE 1	1.4(6)	2.1(0)	5.0
Cisco UCS VIC1225T UCSC-PCIE-C10T-02	2	PCIE 1 PCIE 2	PCIE 1[3]	1.5(1)	2.1(1)	5.0
Cisco UCS VIC 1285 UCSC-PCIE-C40Q-02	2	PCIE 1 PCIE 2	PCIE 1	1.5(4)	2.2(1b)	5.0

1. See PCIe Slots, page 3-35.
2. See note below.
3. The Cisco UCS VIC1225T is not supported for UCS integration at this time.

Note Cisco UCS VIC P81E is not supported in the following server versions: C24 LFF (12-drive) or C24 16HDD (16-drive direct-connect backplane).

RAID Controller Card Cable Routing

If the PCIe card that you are installing or replacing is a RAID controller card, see RAID Controller Considerations, page C-1 for cable routing and other guidelines.

See also Replacing a SuperCap Power Module (RAID Backup Unit), page 3-41 for instructions on installing a RAID backup unit for a RAID controller card.

Installing Multiple PCIe Cards and Resolving Limited Resources

When a large number of PCIe add-on cards are installed in the server, the system may run out of the following resources required for PCIe devices:

- Option ROM memory space
- 16-bit I/O space

The topics in this section provide guidelines for resolving the issues related to these limited resources.

- Resolving Insufficient Memory Space to Execute Option ROMs, page 3-39
- Resolving Insufficient 16-Bit I/O Space, page 3-40

Resolving Insufficient Memory Space to Execute Option ROMs

The system has very limited memory to execute PCIe legacy option ROMs, so when a large number of PCIe add-on cards are installed in the server, the system BIOS might not able to execute all of the option ROMs. The system BIOS loads and executes the option ROMs in the order that the PCIe cards are enumerated (Slot 1, Slot 2, Slot 3, etc.).

If the system BIOS does not have sufficient memory space to load any PCIe option ROM, it skips loading that option ROM, reports a system event log (SEL) event to the CIMC controller and reports the following error in the Error Manager page of the BIOS Setup utility:

```
ERROR CODE  SEVERITY    INSTANCE    DESCRIPTION
146         Major       N/A         PCI out of resources error.
                                    Major severity requires user
                                    intervention but does not
                                    prevent system boot.
```

To resolve this issue, disable the Option ROMs that are not needed for system booting. The BIOS Setup Utility provides the setup options to enable or disable the Option ROMs at the PCIe slot level for the PCIe expansion slots and at the port level for the onboard NICs. These options can be found in the BIOS Setup Utility **Advanced →PCI Configuration** page.

- **Guidelines for RAID controller booting:**

  If the server is configured to boot primarily from RAID storage, make sure that the option ROMs for the slots where your RAID controllers installed are enabled in the BIOS, depending on your RAID controller configuration.

  If the RAID controller does not appear in the system boot order even with the option ROMs for those slots are enabled, the RAID controller option ROM might not have sufficient memory space to execute. In that case, disable other option ROMs that are not needed for the system configuration to free up some memory space for the RAID controller option ROM.

- **Guidelines for onboard NIC PXE booting:**

  If the system is configured to primarily perform PXE boot from onboard NICs, make sure that the option ROMs for the onboard NICs to be booted from are enabled in the BIOS Setup Utility. Disable other option ROMs that are not needed to create sufficient memory space for the onboard NICs.

Resolving Insufficient 16-Bit I/O Space

The system has only 64 KB of legacy 16-bit I/O resources available. This 64 KB of I/O space is divided between the CPUs in the system because the PCIe controller is integrated into the CPUs. This server BIOS has the capability to dynamically detect the 16-bit I/O resource requirement for each CPU and then balance the 16-bit I/O resource allocation between the CPUs accordingly during the PCI bus enumeration phase of the BIOS POST.

When a large number of PCIe cards are installed in the system, the system BIOS might not have sufficient I/O space for some PCIe devices. If the system BIOS is not able to allocate the required I/O resources for any PCIe devices, the following symptoms have been observed:

- The system might get stuck in an infinite reset loop.
- The BIOS might appear to hang while initializing PCIe devices.
- The PCIe option ROMs might take excessive time to complete, which appears to lock up the system.
- PCIe boot devices might not be accessible from the BIOS.
- PCIe option ROMs might report initialization errors. These errors are seen before the BIOS passes control to the operating system.
- The keyboard might not work.

To work around this problem, rebalance the 16-bit I/O load using the following methods:

1. Physically remove any unused PCIe cards.
2. If the system has one or more Cisco virtual interface cards (VICs) installed, disable the PXE boot on the VICs that are not required for the system boot configuration by using the Network Adapters page in the CIMC WebUI to free up some 16-bit I/O resources. Each VIC uses a minimum 16 KB of 16-bit I/O resource, so disabling PXE boot on Cisco VICs would free up some 16-bit I/O resources that can be used for other PCIe cards that are installed in the system.

Replacing a SuperCap Power Module (RAID Backup Unit)

This server supports installation of up to two SuperCap power modules (SCPMs). The SCPMs mount inside a cage that is next to the cooling fans (see Figure 3-22).

The SCPM is supported only when using the LSI MegaRAID-CV controller card. This supercap module provides approximately 3 years of backup for the disk write-back cache DRAM in the case of sudden power loss by offloading the cache to the NAND flash.

To replace the RAID backup unit, follow these steps:

Step 1 Remove an SCPM (see Figure 3-22).

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in the "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Disconnect the RAID controller cable that is attached to the existing SCPM.

e. Remove the cage that holds the SCPMs (see Figure 3-22).

- Use a screwdriver to loosen the captive thumbscrew that secures the cage to the chassis floor.

Note If you cannot access the thumbscrew, you can remove the front chassis panel to provide clearance. See Removing and Replacing the Front Chassis Panel, page 3-8.

- Push the cage toward the server front about 1/4 inch to free the pegs on the sides of the cage from the keyed slots on the chassis bracket.

f. Remove the SCPM holder, with backup unit, from the cage (see Figure 3-22).

g. Remove the SCPM from the holder.

Step 2 Install a new SCPM:

a. Insert the new SCPM into the empty holder that you removed in the previous step (see Figure 3-22).

b. Insert the holder, with new SCPM, into the cage.

c. Replace the cage to the chassis.

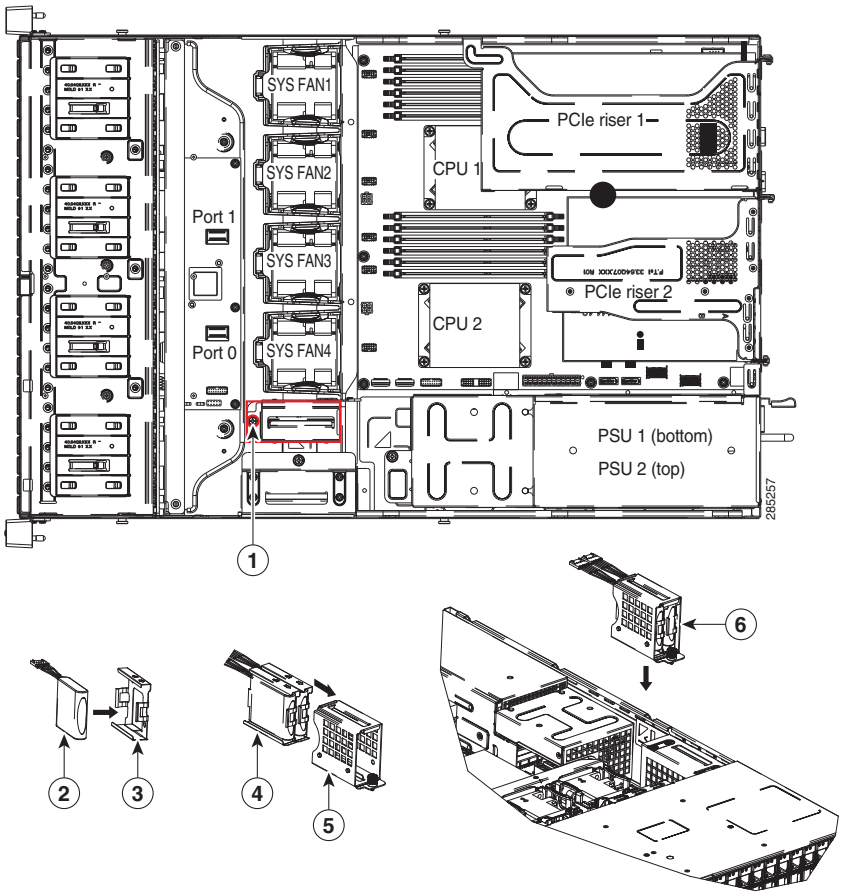
- Set the cage in place in the chassis bracket, aligning the pegs on the sides of the cage with the keyed slots in the chassis bracket.
- Push the cage toward the server rear about 1/4 inch to lock it into the keyed slots on the chassis bracket.
- Use a screwdriver to tighten the captive thumbscrew that secures the cage to the chassis floor.

d. Reconnect the cable from the RAID controller to the new SCPM.

e. Replace the top cover.

f. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-22 Replacing an SCPM



1	Captive thumbscrew on SCPM cage	**4**	SCPM holders with SCPMs installed (up to two)
2	SuperCap power module (SCPM)	**5**	SCPM cage removed from server
3	SCPM holder	**6**	SCPM cage with holders and SCPMs installed (up to two)

Replacing an Internal USB Flash Drive

The server has one internal USB 2.0 socket on the motherboard that you can use with a USB thumb drive for additional storage. The server can be ordered with an optional blank 8-GB Cisco USB Flash Drive pre-installed in the internal USB port.

This section includes the following topics:

- Internal USB Flash Drive Replacement Procedure, page 3-43
- Enabling or Disabling the Internal USB Port, page 3-44

Internal USB Flash Drive Replacement Procedure

To install or replace an internal USB flash drive, follow these steps:

Step 1 Remove the USB flash drive that you are replacing. See Figure 3-23:

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Remove PCIe riser 1 to provide access to the USB flash drive socket that is on the motherboard (see Figure 3-23). See Replacing a PCIe Riser, page 3-33 for more information.

e. Pull the USB flash drive from the socket.

Step 2 Install a USB flash drive:

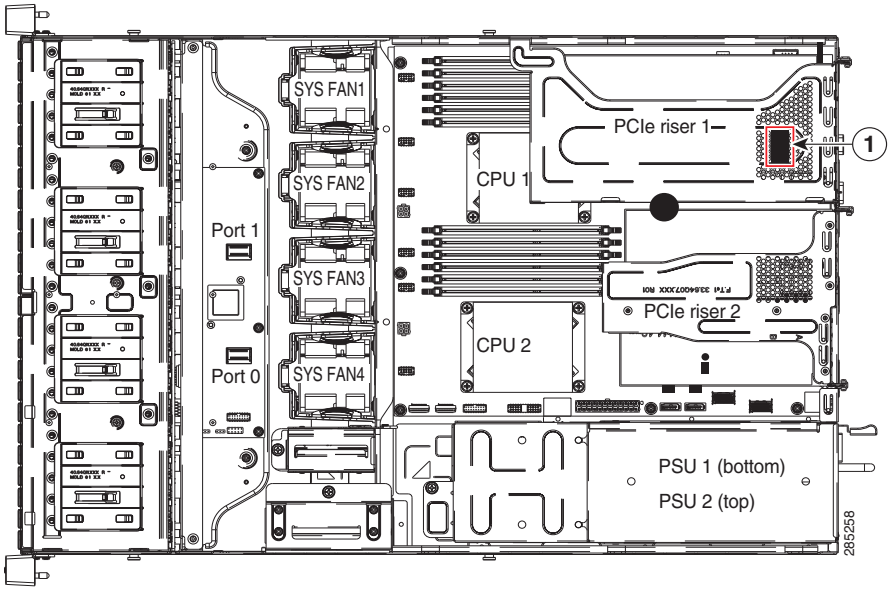
a. Insert the USB flash drive into the socket.

b. Replace PCIe riser 1 to the server. See Replacing a PCIe Riser, page 3-33 for more information.

c. Replace the top cover.

d. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-23 Internal USB Flash Drive Socket (USB 2.0)



1	Cisco USB flash drive socket on motherboard		–

Enabling or Disabling the Internal USB Port

The factory default is for all USB ports on the server to be enabled. However, the internal USB port can be enabled or disabled in the server BIOS. To enable or disable the internal USB port, follow these steps:

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

Step 2 Navigate to the **Advanced** tab.

Step 3 On the Advanced tab, select **USB Configuration**.

Step 4 On the USB Configuration page, select **USB Ports Configuration**.

Step 5 Scroll to **USB Port: Internal**, press **Enter**, and then select either Enabled or Disabled from the pop-up menu.

Step 6 Press F10 to save and exit the utility.

Installing a Trusted Platform Module

The trusted platform module (TPM) is a small circuit board that attaches to a motherboard socket. The socket location is on the motherboard, underneath PCIe riser 1 (see Figure 3-24).

Note For security purposes, the TPM is installed with a one-way screw. It cannot be removed with a standard screwdriver.

To install a trusted platform module (TPM), follow these steps:

Step 1 Prepare the server for component installation.

a. Power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.

b. 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.

c. Remove the top cover as described in the "Removing and Replacing the Server Top Cover" section on page 3-7.

d. Remove PCIe riser 2 to provide access (see Figure 3-24). See Replacing a PCIe Riser, page 3-33.

Step 2 Install a TPM (see Figure 3-24):

a. Locate the TPM socket on the motherboard, as shown in Figure 3-24.

b. Align the connector that is on the bottom of the TPM circuit board with the motherboard TPM socket. Align the screw hole and standoff on the TPM board with the screw hole adjacent to the TPM socket.

c. Push down evenly on the TPM to seat it in the motherboard socket.

d. Install the single one-way screw that secures the TPM to the motherboard.

e. Replace PCIe riser 2 to its motherboard socket. See Replacing a PCIe Riser, page 3-33.

f. Replace the top cover.

g. Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Step 3 Enable the TPM:

Note You must set a BIOS Administrator password before performing this procedure. To set this password, press the **F2** key when prompted during system boot to enter the BIOS Setup utility. Then navigate to **Security > Set Administrator Password** and enter the new password twice as prompted.

a. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.

b. Log into the BIOS Setup utility with your BIOS Administrator password.

c. On the BIOS Setup utility screen, select the **Advanced** tab.

d. Select **Trusted Computing** to open the TPM Security Device Configuration screen.

e. Change TPM SUPPORT to **Enabled**.

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

Step 4 Verify that the TPM is now enabled.

a. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.

b. Log into the BIOS Setup utility with your BIOS Administrator password.

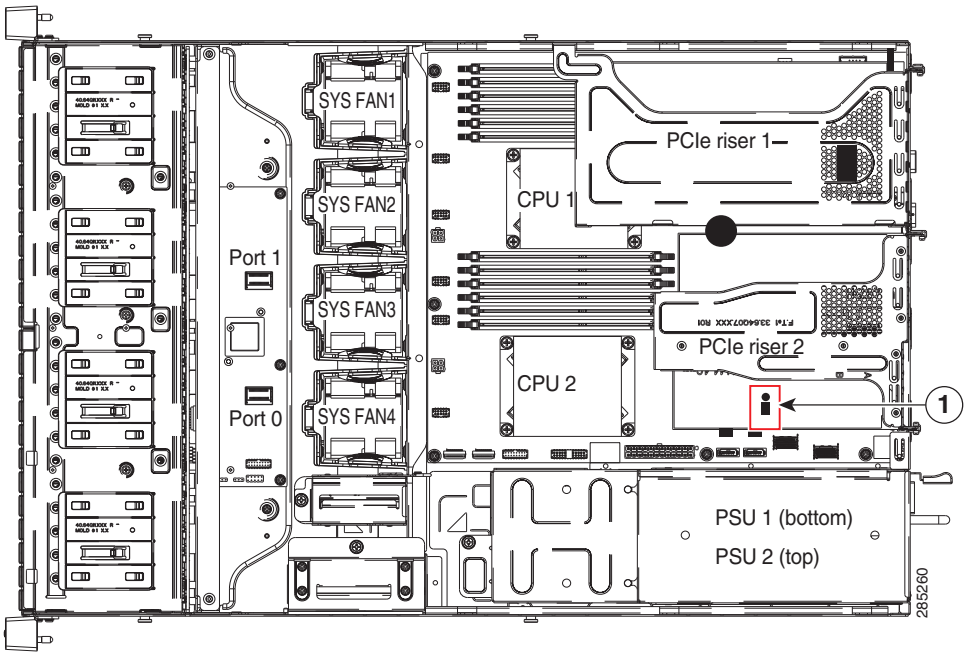
c. Select the **Advanced** tab.

d. Select **Trusted Computing** to open the TPM Security Device Configuration screen.

e. Verify that TPM SUPPORT is Enabled.

Note If you want to use the Intel Trusted Execution Technology (TXT) feature, it must be enabled in the server BIOS as described in Enabling the Intel Trusted Execution Technology (TXT) Feature For the TPM, page 3-46.

Figure 3-24 TPM Socket Location on Motherboard



1	TPM socket and screw hole on motherboard	2	PCIe riser 1

Enabling the Intel Trusted Execution Technology (TXT) Feature For the TPM

Intel TXT provides greater protection for information that is used and stored on the business server. A key aspect of that protection is the provision of an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data, invisibly to the rest of the system. Likewise, Intel TXT provides for a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code.

Note You must set a BIOS Administrator password before performing this procedure. To set this password, press the **F2** key when prompted during system boot to enter the BIOS Setup utility. Then navigate to **Advanced > Security > Set Administrator Password** and enter the new password twice as prompted.

To enable the TXT feature, follow these steps:

Step 1 Verify that a TPM is now installed and enabled in the server:

a. Either attach a VGA monitor and USB keyboard to the server, or log in remotely to the CIMC interface of the server and open a virtual KVM console window.

b. Reboot the server.

c. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.

d. Log in to the BIOS Setup utility with your BIOS Administrator password.

Note You must be logged in as the BIOS administrator to perform this procedure. If you have not done so already, set a BIOS administrator password on the Security tab of the BIOS Setup utility.

e. Select the **Advanced** tab.

f. On the Advanced tab, select **Trusted Computing** to open the TPM Security Device Configuration screen.

g. Verify that **TPM SUPPORT** is **Enabled**. If it is not, set TPM SUPPORT to Enabled.

h. Press **Escape** to return to the BIOS Setup utility **Advanced** tab.

Step 2 Enable the Intel Trusted Execution Technology (TXT) feature:

a. On the Advanced tab, select **Intel TXT(LT-SX) Configuration** to open the Intel TXT(LT-SX) Hardware Support screen.

Note The Intel Trusted Execution Technology feature can be enabled only when the server has a TPM installed on the TPM header.

b. Set **TXT Support** to **Enabled**.

Step 3 On the same screen, verify that the Intel Virtualization Technology (VT) and the Intel VT for Directed I/O (VT-d) features are enabled (the factory default).

a. On the Intel TXT(LT-SX) Hardware Support screen, verify that **VT-d Support** and **VT Support** are both listed as **Enabled**.

- If they are already enabled, skip to Step 4.
- If VT-d Support and VT Support are not enabled, continue with the next steps to enable them.

b. Press **Escape** to return to the BIOS Setup utility **Advanced** tab.

c. On the Advanced tab, select **Processor Configuration** to open the Processor Configuration screen.

d. Set **Intel (R) VT** and **Intel (R) VT-d** to Enabled.

Step 4 Press **F10** to save your changes and exit the BIOS Setup utility.

Step 5 Verify that the Intel TXT, VT, and VT-d features are enabled:

a. Reboot the server.

b. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.

c. Select the **Advanced** tab.

d. Select **Intel TXT(LT-SX) Configuration** and verify that TXT Support, VT-d Support, and VT Support are Enabled.

Replacing a SCU Upgrade ROM Module

To remove and replace a module, use the following procedure.

Step 1 Prepare the server for component installation:

a. Power off the server as described in Shutting Down and Powering Off the Server, page 3-6.

b. 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.

c. Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-7.

Step 2 Remove the SCU upgrade ROM module:

a. Locate the module on the motherboard (see Figure C-1).

b. Grasp the printed circuit board of the module and lift it from the header.

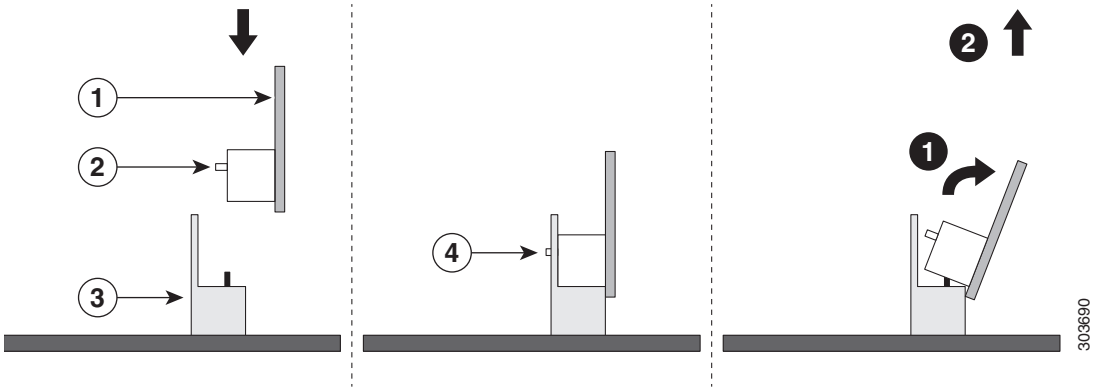
Note The module has a small retention feature that must have clearance from the header before the module can be pulled up. Tilt the module back, then pull up as shown in Figure 3-25.

Step 3 Install a new SCU upgrade ROM module:

a. Align the module with the pins in the motherboard header.

b. Gently press down on the module until it is seated and the retention feature locks into the header.

Figure 3-25 SCU Upgrade ROM Module Retention Feature



1	Printed circuit board on module	**3**	Motherboard header
2	Retention feature on module	**4**	Retention feature in installed position

For more information about using the module and embedded RAID, see Embedded MegaRAID Controller, page C-6.

Replacing a Software RAID Key Module

To remove and replace a software RAID key module, use the following procedure.

Step 1 Prepare the server for component installation:

a. Power off the server as described in Shutting Down and Powering Off the Server, page 3-6.

b. 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.

c. Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-7.

Step 2 Remove the software RAID key module:

a. Locate the module on the motherboard (see Figure C-1).

b. Grasp the printed circuit board of the module and lift it from the header.

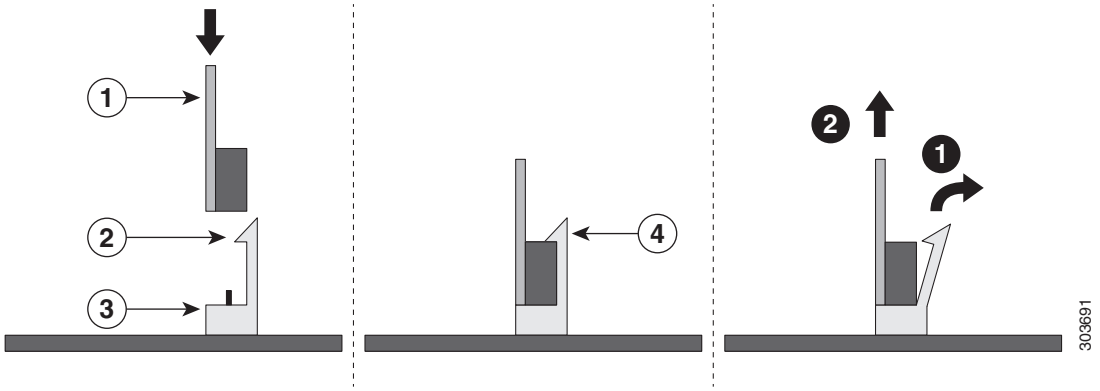
Note The module must have clearance from the retention clip on the header before the module can be pulled up. Open the retention clip, then pull up as shown in Figure 3-26.

Step 3 Install a new software RAID key module:

a. Align the module with the pins in the motherboard header.

b. Gently press down on the module until it is seated and the retention clip locks over the module.

Figure 3-26 Software RAID Key Module Retention Feature



1	Printed circuit board on module	**3**	Motherboard header
2	Retention feature on motherboard header	**4**	Retention feature in installed position

For more information about using the module and embedded RAID, see Embedded MegaRAID Controller, page C-6.

Replacing Power Supplies

The server can have one or two power supplies. When two power supplies are installed they are redundant as 1+1.

Note The power supplies must both be either 450W or 650W; do not mix power supply types.

See Power Specifications, page A-2 for more information about the power supplies. See Rear Panel LEDs and Buttons, page 3-4 for information about the power supply LEDs.

To replace or install a power supply, follow these steps:

Note If you have ordered a server with power supply redundancy (two power supplies), you do not have to power off the server to replace power supplies because they are redundant as 1+1.

Step 1 Remove the power supply that you are replacing or a blank panel from an empty bay (see Figure 3-27):

a. Perform one of the following actions:
   - If your server has only one power supply, shut down and power off the server as described in the "Shutting Down and Powering Off the Server" section on page 3-6.
   - If your server has two power supplies, you do not have to shut down the server.

b. Remove the power cord from the power supply that you are replacing.

c. Grasp the power supply handle while pinching the release lever towards the handle.

d. Pull the power supply out of the bay.

Step 2 Install a new power supply:

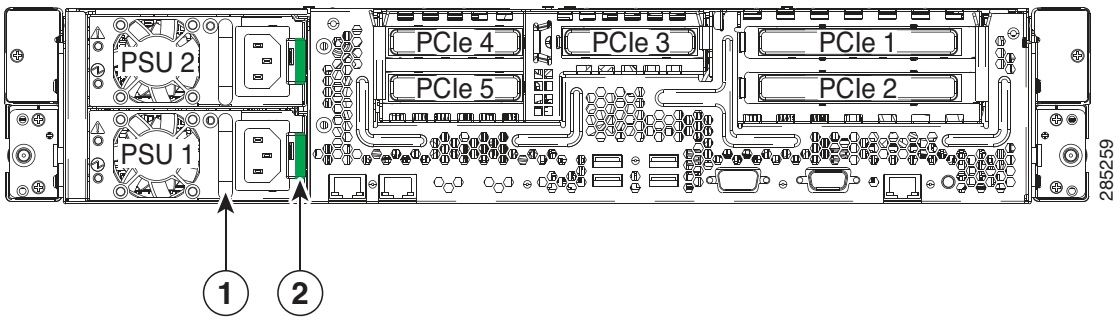
a. Grasp the power supply handle and insert the new power supply into the empty bay.

b. Push the power supply into the bay until the release lever locks.

c. Connect the power cord to the new power supply.

d. If you shut down the server, press the **Power** button to return the server to main power mode.

Figure 3-27 Removing and Replacing Power Supplies



1	Power supply handle	2	Power supply release lever

APPENDIX A

Server Specifications

This appendix lists the technical specifications for the server and includes the following sections:

- Physical Specifications, page A-1
- Power Specifications, page A-2
- Environmental Specifications, page A-4

Physical Specifications

Table A-1 lists the physical specifications for the server.

Table A-1 Physical Specifications

Description	Specification
Height	3.4 in. (8.76 cm)
Width (including slam-latches)	16.9 in. (43.00 cm)
Depth	26.0 in. (66.05 cm)
Weight (fully loaded)	Small Form Factor: 47.2 lbs. (21.4 Kg) Large Form Factor: 53.2 lbs. (24.1 Kg)

Power Specifications

The power specifications for the two power supply options are listed in the following sections:

- 450W Power Supply, page A-2
- 650W Power Supply, page A-3

You can get more specific power information for your exact server configuration by using the Cisco UCS Power Calculator:

http://ucspowercalc.cisco.com

450W Power Supply

Table A-2 lists the specifications for each 450W power supply (Cisco part number UCSC-PSU-450W).

Table A-2 Power Supply Specifications

Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC input current	6 A at 100 VAC 3 A at 208 VAC
Maximum input volt-amperes	600 VA at 100 VAC
Maximum output power per PSU	450 W
Maximum inrush current	27 A (sub-cycle duration)
Maximum hold-up time	12 ms at 650 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP1
Input connector	IEC60320 C13

650W Power Supply

Table A-3 lists the specifications for each 650W power supply (Cisco part number UCSC-PSU-650W).

Table A-3 Power Supply Specifications

Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC input current	7.6 A at 100 VAC 3.65 A at 208 VAC
Maximum input volt-amperes	760 VA at 100 VAC
Maximum output power per PSU	650 W
Maximum inrush current	33 A (sub-cycle duration)
Maximum hold-up time	12 ms at 650 W
Power supply output voltage	12 VDC
Power supply standby voltage	3.3 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP1
Input connector	IEC60320 C14

Environmental Specifications

Table A-4 lists the environmental specifications for the server.

Table A-4 Environmental Specifications

Description	Specification
Temperature, operating:	35 to 104°F (1.7 to 40°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, non-operating (when the server is stored)	–40 to 149°F (–40 to 65°C)
Humidity (RH), noncondensing	10 to 90%
Altitude, operating	0 to 10,000 feet (0 to 3000 m)
Altitude, non-operating (when the server is stored)	0 to 40,000 feet (0 to 12,192 m)
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	Small Form Factor: 5.9 Large Form Factor: 6.3
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	Small Form Factor: 46.0 Large Form Factor: 48.5

APPENDIX B

Power Cord Specifications

This appendix provides supported power cable specifications.

Supported Power Cords and Plugs

Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the server. The jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.

Note Only the approved power cords or jumper power cords provided with the server are supported.

Table B-1 lists the power cords for the server power supplies.

Table B-1 Supported Power Cords for the Server

Description	Length		Power Cord Reference Illustration
	Feet	Meters	
CAB-250V-10A-AR Power Cord, 250 VAC 10 A IRAM 2073 Plug Argentina	8.2	2.5	Figure B-1
CAB-9K10A-AU 250 VAC 10 A 3112 Plug, Australia	8.2	2.5	Figure B-2
CAB-250V-10A-CN Power Cord, 250 VAC 10 A GB 2009 Plug China	8.2	2.5	Figure B-3
CAB-9K10A-EU Power Cord, 250 VAC 10 A M 2511 Plug Europe	8.2	2.5	Figure B-4
CAB-250V-10A-ID Power Cord, 250 VAC 16A EL-208 Plug South Africa, United Arab Emirates, India	8.2	2.5	Figure B-5
CAB-250V-10A-IS Power Cord, 250 VAC 10 A SI32 Plug Israel	8.2	2.5	Figure B-6

Table B-1 Supported Power Cords for the Server (continued)

Description	Length		Power Cord Reference Illustration
	Feet	Meters	
CAB-9K10A-IT Power Cord, 250 VAC 10 A CEI 23-16 Plug Italy	8.2	2.5	Figure B-7
CAB-9K10A-SW Power Cord, 250 VAC 10 A MP232 Plug Switzerland	8.2	2.5	Figure B-8
CAB-9K10A-UK Power Cord, 250 VAC 10 A BS1363 Plug (13 A fuse) United Kingdom	8.2	2.5	Figure B-9
CAB-AC-250V/13A Power Cord, 250 VAC 13 A IEC60320 Plug North America	6.6	2.0	Figure B-10
CAB-N5K6A-NA Power Cord, 250 VAC 13 A NEMA 6-15 Plug, North America	8.2	2.5	Figure B-11
CAB-9K12A-NA Power cord, 125 VAC, 13 A, NEMA 5-15 Plug North America	8.2	2.5	Figure B-12
CAB-C13-CBN Cabinet Jumper Power Cord, 250 VAC 10 A, C13-C14 Connectors	2.2	0.68	Figure B-13
CAB-C13-C14-2M Cabinet Jumper Power Cord, 250 VAC 10 A, C13-C14 Connectors	6.6	2.0	Figure B-14
CAB-C13-C14-AC Cabinet Jumper Power Cord, 250 VAC 10 A, C13-C14 Connectors	9.8	3.0	Figure B-15

AC Power Cord Illustrations

This section includes the AC power cord illustrations. See Figure B-1 through Figure B-15.

Figure B-1 CAB-250V-10A-AR

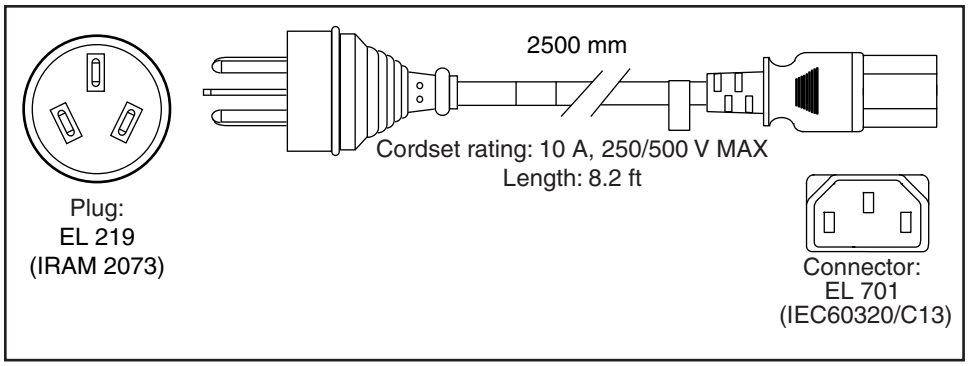


Figure B-2 CAB-9K10A-AU

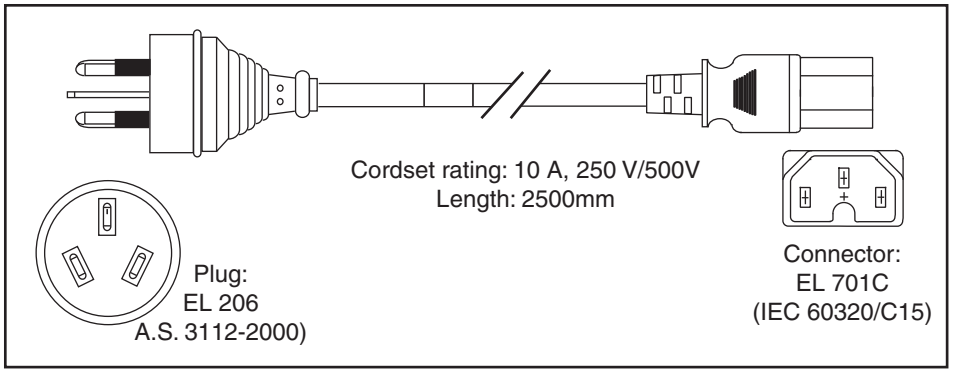


Figure B-3 CAB-250V-10A-CN

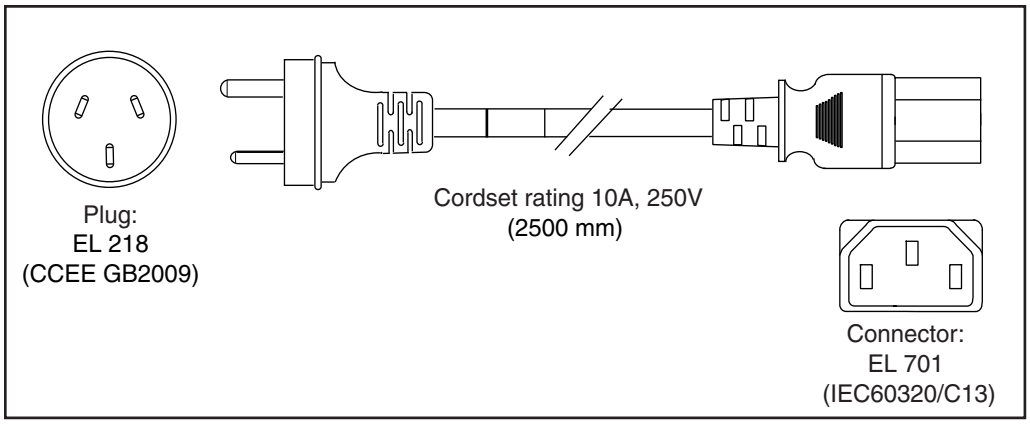


Figure B-4 CAB-9K10A-EU

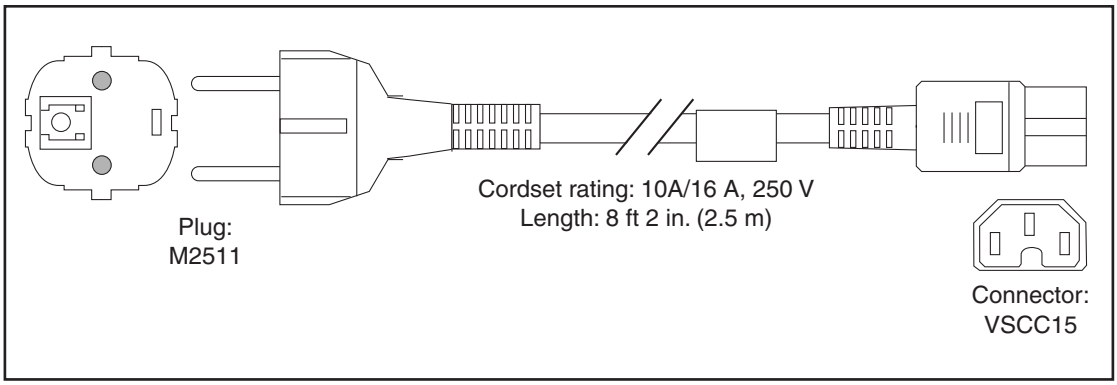


Figure B-5 CAB-250V-10A-ID

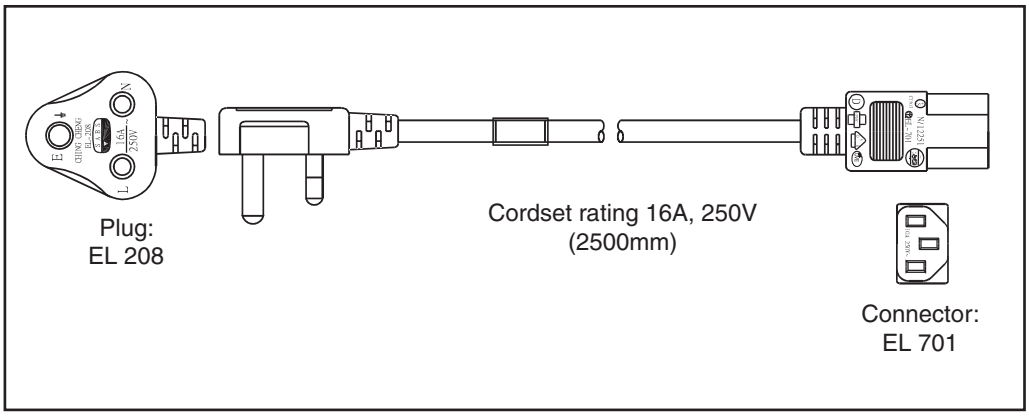


Figure B-6 CAB-250V-10A-IS

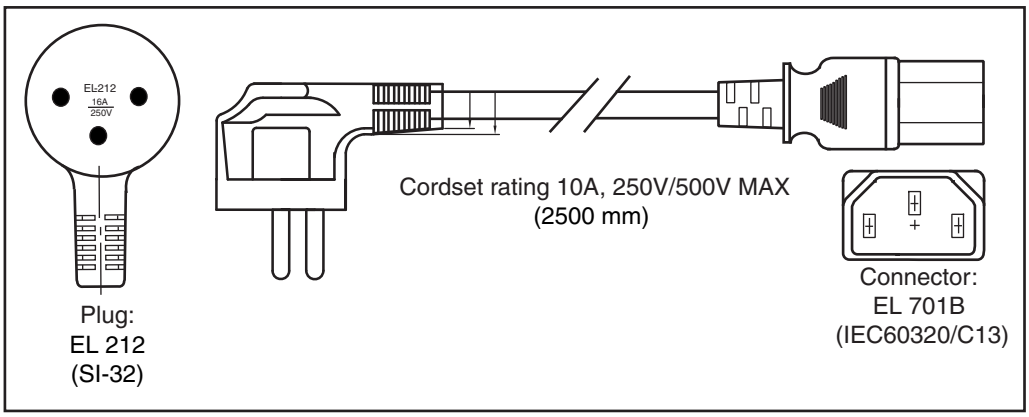


Figure B-7 CAB-9K10A-IT

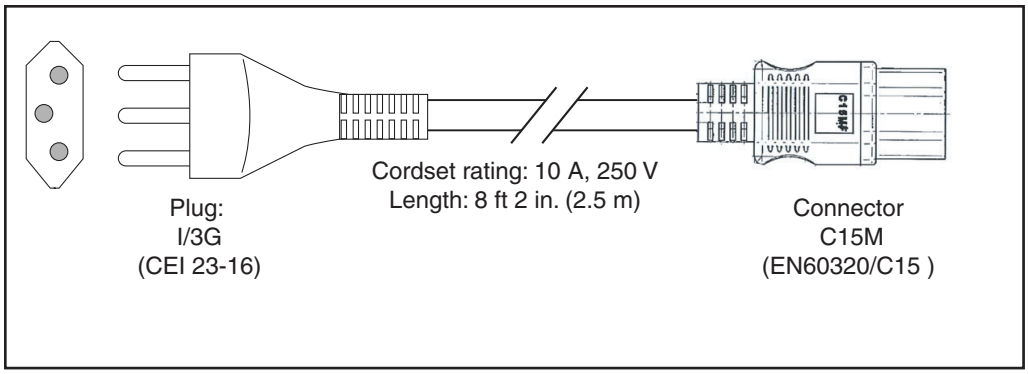


Figure B-8 CAB-9K10A-SW

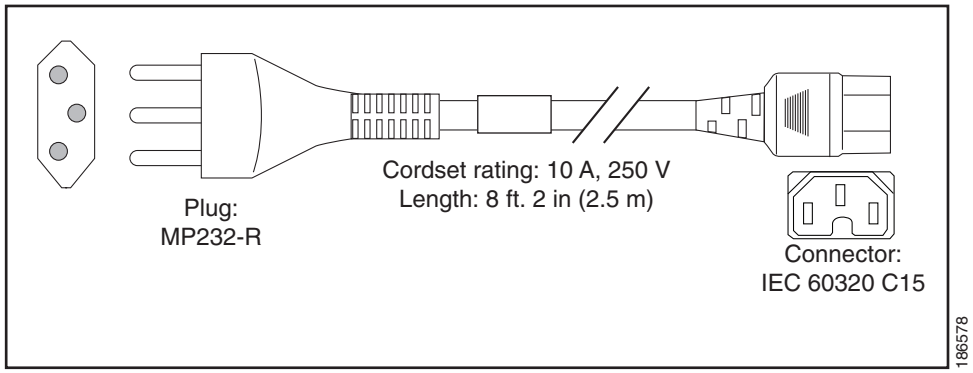


Figure B-9 CAB-9K10A-UK

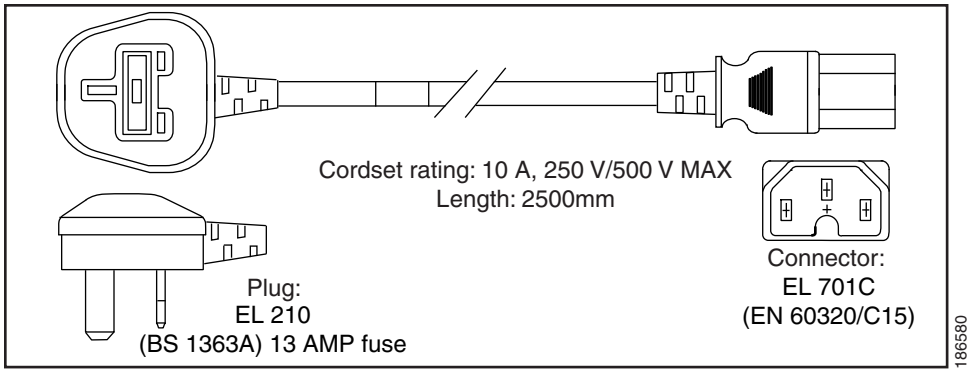


Figure B-10 CAB-AC-250V/13A

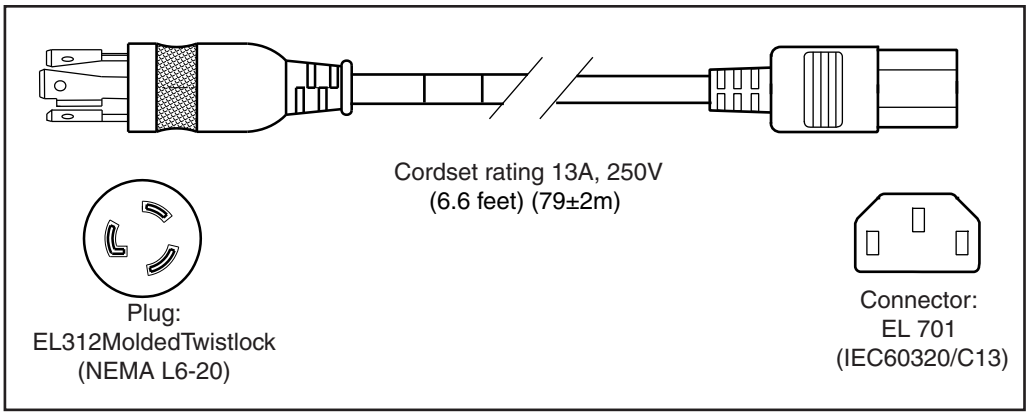


Figure B-11 CAB-N5K6A-NA

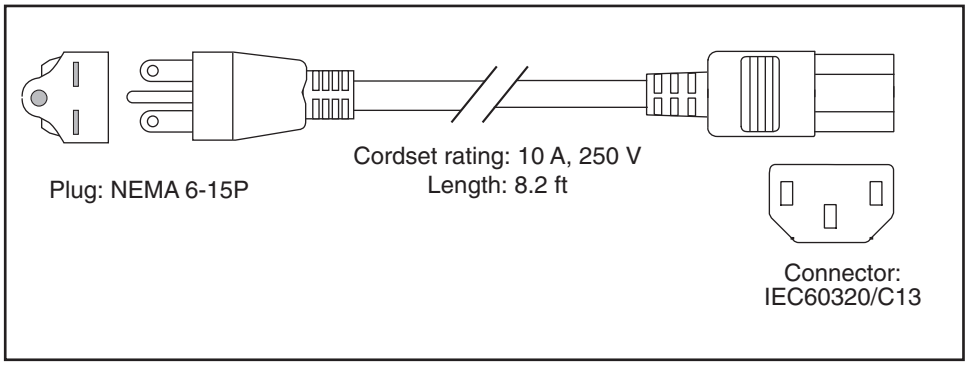


Figure B-12 CAB-9K12A-NA

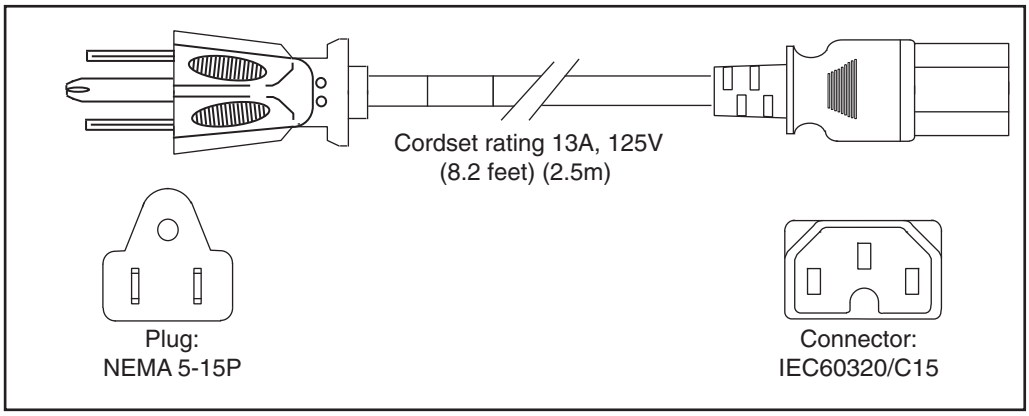


Figure B-13 CAB-C13-CBN, Jumper Power Cord (0.68 m)

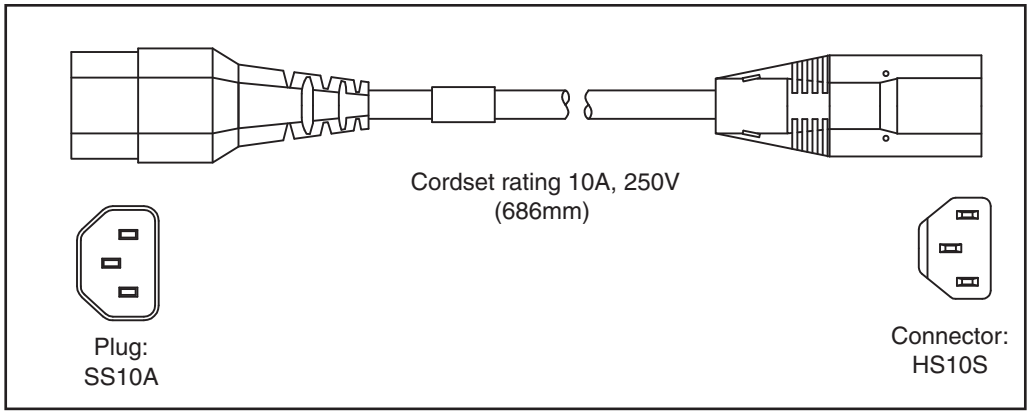


Figure B-14 CAB-C13-C14-2M, Jumper Power Cord (2 m)

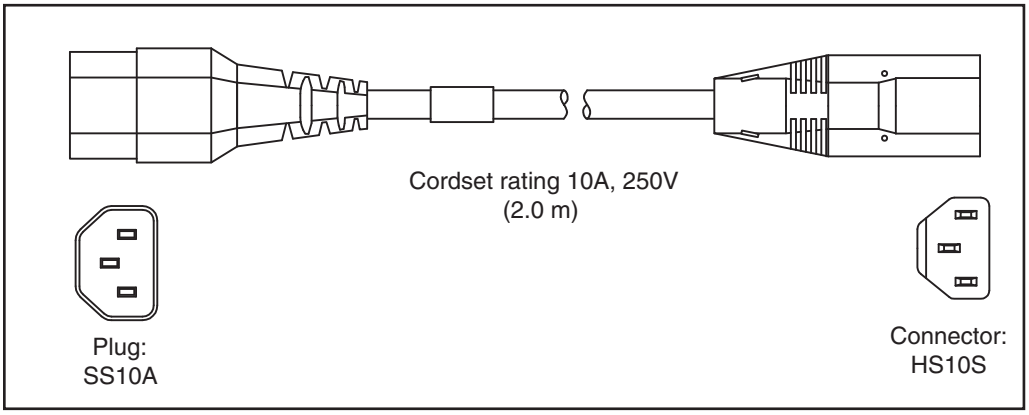
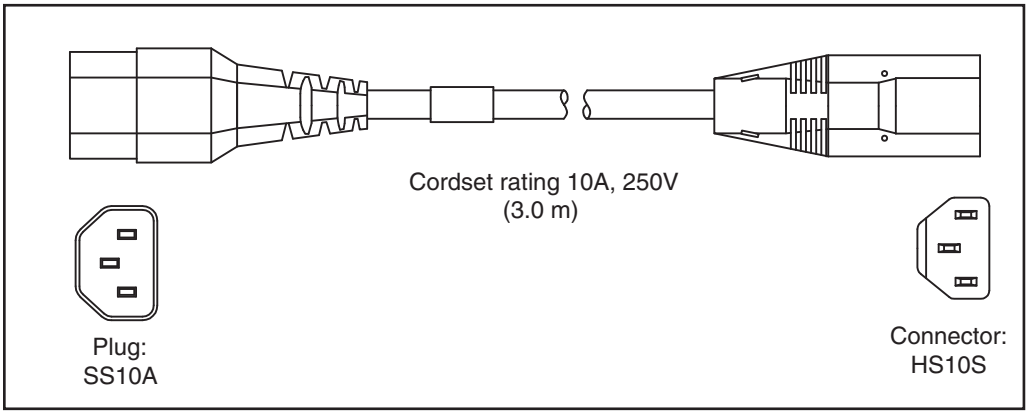


Figure B-15 CAB-C13-C14-AC, Jumper Power Cord (3 m)



APPENDIX C

RAID Controller Considerations

This appendix contains the following sections:

- Supported RAID Controllers and Required Cables, page C-2
- RAID Card Firmware Compatibility, page C-3
- Mixing Drive Types in RAID Groups, page C-3
- SuperCap Power Modules (RAID Backup Units), page C-4
- Embedded MegaRAID Controller, page C-6
- RAID Controller Cabling, page C-18
- Restoring RAID Configuration After Replacing a RAID Controller, page C-22
- For More Information, page C-22

Supported RAID Controllers and Required Cables

This server supports the RAID controller options, cables, and RAID backup units shown in Table C-1.

Caution Do not use the embedded MegaRAID controller and a hardware RAID controller card at the same time. This is not supported and could result in data loss.

Note This server supports up to two internal PCIe-style RAID controllers, plus one external PCIe-style RAID controller. Do not mix *internal* controller types in the server. You can mix internal controllers with an external controller.

Note The embedded RAID option is available only with the SFF 16-drive backplane. It does not operate through an expander.

Note The cables in this section apply to both single- and dual-CPU configurations.

Table C-1 lists the RAID options for the small form factor (SFF) versions of the server.

Table C-1 Cisco UCS C24 Small Form Factor RAID Options

Controller	Style	Maximum Drives	SuperCap Power Module?	RAID Levels Supported	Required Cables (Each PID is a cable-pair kit.)
Embedded RAID[1] on motherboard[2]	Onboard	SFF 16HDD: 4 SATA (default) or 8 SAS[3] internal	No	0, 1, 5[4], 10	SFF 16HDD: UCSC-CABLE-A7
LSI MegaRAID SAS 9220-8i	PCIe	SFF 24HDD: 16 internal[5] SFF 16HDD: 8 internal[6]	No	0, 1, 10	SFF 24HDD: UCSC-CABLE-A6 SFF 16HDD, 1st-controller: UCSC-CABLE-A7 SFF 16HDD, 2nd-controller: UCSC-CABLE-A8
LSI MegaRAID SAS 9240-8i	PCIe	SFF 24HDD: 16 internal[7] SFF 16HDD: 8 internal	No	0, 1, 5, 10, 50	SFF 24HDD: UCSC-CABLE-A6 SFF 16HDD, 1st-controller: UCSC-CABLE-A7 SFF 16HDD, 2nd-controller: UCSC-CABLE-A8
LSI MegaRAID SAS 9265CV-8i	PCIe	SFF 24HDD: 24 internal SFF 16HDD: 8 internal	Yes	0, 1, 5, 6, 10, 50, 60	SFF 24HDD: UCSC-CABLE-A6 SFF 16HDD, 1st-controller: UCSC-CABLE-A7 SFF 16HDD, 2nd-controller: UCSC-CABLE-A8

1. The embedded RAID controller must be enabled in the BIOS.
2. Embedded RAID SAS drive control requires an optional SCU ROM upgrade chip to be installed on the motherboard.
3. Support for eight SAS drives requires an optional SCU upgrade ROM module on the motherboard.
4. Integrated RAID 5 support requires an optional software key.
5. The 9220-8i controller can create a RAID array with maximum 16 drives, even if it detects more than 16 drives.
6. In the 16HDD version, two controller cards can be installed to control a total of 16 drives.
7. The 9240-8i controller can create a RAID array with maximum 16 drives, even if it detects more than 16 drives.

Table C-2 lists the RAID options for the large form factor (LFF) version of the server.

Table C-2 Cisco UCS C24 Large Form Factor RAID Options

Controller	Style	Maximum Drives	SuperCap Power Module	RAID Levels Supported	Required Cables (Each PID is a cable-pair kit.)
LSI MegaRAID SAS 9220-8i	PCIe	12 internal	No	0, 1, 10	12 drives: 2 mini-SAS UCSC-CABLE-A11
LSI MegaRAID SAS 9240-8i	PCIe	12 internal	No	0, 1, 5, 10, 50	12 drives: 2 mini-SAS UCSC-CABLE-A11
LSI MegaRAID SAS 9265CV-8i	PCIe	12 internal	SCPM	0, 1, 5, 6, 10, 50, 60	12 drives: 2 mini-SAS UCSC-CABLE-A11

RAID Card Firmware Compatibility

Firmware on the RAID controller card must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the server. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: HUU Guides

Mixing Drive Types in RAID Groups

Table C-3 lists the technical capabilities for mixing hard disk drive (HDD) and solid state drive (SSD) types in a RAID group. However, see the best practices recommendations that follow for the best performance.

Table C-3 Drive Type Mixing in RAID Groups

Mix of Drive Types in RAID Group	Allowed?
SAS HDD + SATA HDD	Yes
SAS SSD + SATA SSD	Yes
HDD + SSD	No

Best Practices For Mixing Drive Types in RAID Groups

For the best performance, follow these guidelines:

- Use either all SAS or all SATA drives in a RAID group.
- Use the same capacity for each drive in the RAID group.
- Never mix HDDs and SSDs in the same RAID group.

SuperCap Power Modules (RAID Backup Units)

This server supports installation of up to two SuperCap power modules (SCPMs). The SCPMs mount inside a cage that is next to the cooling fans (see Figure C-2).

The SCPM is supported only when using the LSI MegaRAID-CV controller card. This supercap module provides approximately 3 years of backup for the disk write-back cache DRAM in the case of sudden power loss by offloading the cache to the NAND flash.

For SCPM replacement instructions, see Replacing a SuperCap Power Module (RAID Backup Unit), page 3-41.

RAID Controller Migration

This server supports hardware RAID (PCIe controller cards) and embedded software RAID. See Table C-4 for which migrations are allowed and a summary of migration steps.

Table C-4 RAID Controller Migration

Starting RAID Controller	Migrate to HW RAID Allowed?	Migrate to SW RAID Allowed?
None (no drives) Onboard SCU Storage support is Disabled in BIOS	Allowed 1. Install card. 2. Install cables.	Allowed 1. Install desired upgrade modules to motherboard. 2. Enable SCU storage support in BIOS. 3. Install cables.
Embedded SW RAID Onboard SCU Storage support is Enabled in BIOS	**Caution** Data migration from SW RAID to HW RAID is *not* supported and could result in data loss. Allowed only *before* there is data on the drives; data migration is not supported. 1. Disable SCU storage support in BIOS. 2. Install card. 3. Install cables.	Not applicable
HW RAID Onboard SCU Storage support is Disabled in BIOS	Not applicable	Not allowed

Embedded MegaRAID Controller

Note The VMware ESX/ESXi operating system is not supported for use with the embedded MegaRAID controller.

Note The Microsoft Windows Server 2016 Hyper-V hypervisor is supported for use with the embedded MegaRAID controller. Other hypervisors such as Xen and KVM are not supported.

Note The embedded RAID option is available only with the SFF 16-drive backplane. It does not operate through an expander.

This server includes an embedded RAID controller with two mini-SAS connectors on the motherboard (see Figure C-1).

- The default setting for this embedded controller is RAID 0, 1, and 10 support for up to four SATA drives.
- You can upgrade this support to SAS RAID 0, 1, and 10 support for up to eight SAS drives by installing a Storage Controller Unit (SCU) upgrade ROM chip on the motherboard. See Installing a SCU Upgrade ROM Module For Embedded RAID SAS Support, page C-8.
- You can upgrade this support by adding SAS RAID 5 support with an optional software key. See Installing a Software RAID Key Module for Embedded RAID 5 Support, page C-9.

Note You cannot downgrade from using a RAID controller card to using the embedded controller (see RAID Controller Migration, page C-5). Instructions for installing upgrade modules and enabling the embedded controller in the BIOS are included here for those upgrading a server with no RAID controller or drives.

Caution Data migration from SW RAID (embedded RAID) to HW RAID (a controller card) is *not* supported and could result in data loss. Migrations from SW RAID to HW RAID are supported only *before* there is data on the drives, or the case in which there are no drives in the server (see RAID Controller Migration, page C-5).

- You can migrate from using the embedded controller to using a RAID card only *before* there is data on the drives. In this case, you must disable the embedded controller. See Disabling the Integrated RAID Controller in the BIOS, page C-9.
- The required drivers for this controller are already installed and ready to use with the LSI SWRAID Configuration Utility. However, if you will use this controller with Windows or Linux, you must download and install additional drivers for those operating systems. See Installing LSI MegaSR Drivers For Windows and Linux, page C-10.

This section contains the following topics:

- Notes on Supported Embedded MegaRAID Levels, page C-7
- Installing a SCU Upgrade ROM Module For Embedded RAID SAS Support, page C-8
- Installing a Software RAID Key Module for Embedded RAID 5 Support, page C-9
- Enabling the Integrated RAID Controller in the BIOS, page C-9

- Disabling the Integrated RAID Controller in the BIOS, page C-9
- Launching the LSI Embedded RAID Configuration Utility, page C-10
- Installing LSI MegaSR Drivers For Windows and Linux, page C-10

Notes on Supported Embedded MegaRAID Levels

The following RAID levels are supported by the embedded MegaRAID controller.

- RAID 0—You can configure a RAID 0 virtual drive (VD) using one or more physical drives (PDs). This level supports up to eight VDs and PDs.
- RAID 1—A RAID 1 VD is configured from only two PDs. This level supports up to eight PDs (four RAID arrays) and eight VDs.
- RAID 5—You can configure a RAID 5 VD using three or more PDs. This level supports up to eight PDs and eight VDs.
- RAID 10—This is a spanned VD; that is, RAID 0 is implemented on two or more RAID 1 VDs. This level supports up to eight PDs (two to four RAID 1 volumes spanned) and one VD.

Note None of these RAID levels require drives of the same size. The smallest drive in the array determines the size of the VD.

Note An array can be divided into multiple VDs of the same RAID level, except when using RAID 10. Mixed arrays are not permitted. For example, you cannot configure a three-drive array into RAID 0 and RAID 5 VDs. Unlike RAID 0, 1, and 5, you cannot create multiple RAID 10 VDs from the same array. A single RAID 10 VD uses up the entire array.

Installing a SCU Upgrade ROM Module For Embedded RAID SAS Support

The SCU Upgrade ROM module contains a chip on a small circuit board. This module attaches to a motherboard header (see Figure C-1). This chip adds SAS support for up to eight drives.

Note The Cisco PID UCSC-RAID-ROM5= includes the SCU upgrade ROM module.
The Cisco PID UCSC-RAID-ROM55= includes the SCU upgrade ROM module and the RAID 5 key.

To install a SCU upgrade ROM jumper, follow these steps:

Step 1 Locate the SCU_ROM header (see Figure C-1).

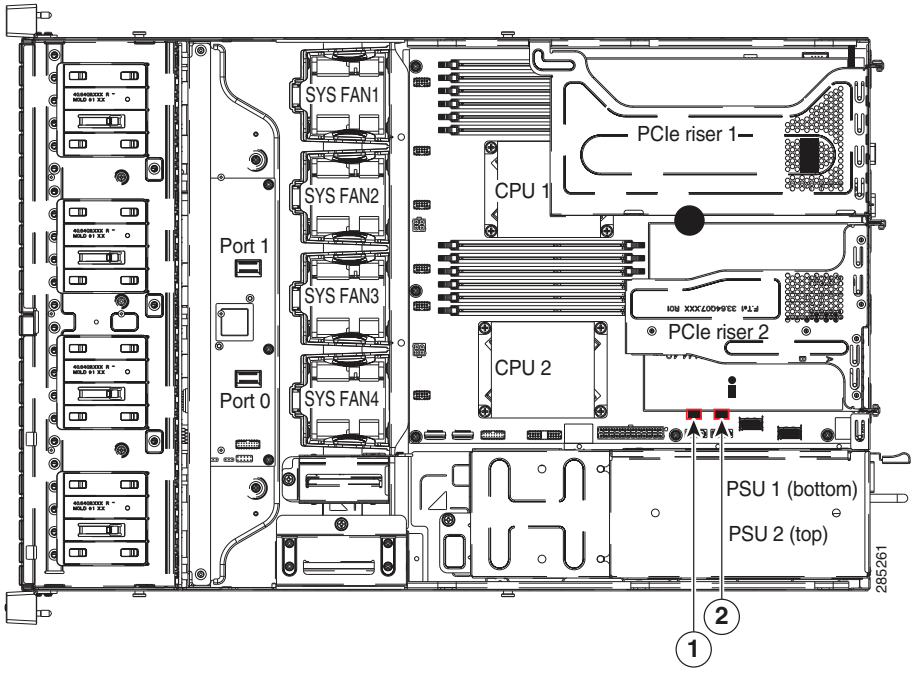
Step 2 Align the connector on the SCU upgrade ROM module with the pins on the header, then gently push the connector onto the pins.

Step 3 Replace the top cover.

Step 4 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Step 5 Continue with either Installing a Software RAID Key Module for Embedded RAID 5 Support, page C-9 or Enabling the Integrated RAID Controller in the BIOS, page C-9.

Figure C-1 SCU Upgrade ROM and RAID 5 Key Header Locations on the Motherboard



1	SCU upgrade ROM header (SCU_ROM)	**2**	RAID 5 software key header (RAID_KEY)

Installing a Software RAID Key Module for Embedded RAID 5 Support

The software RAID key module contains a chip on a small circuit board. This module attaches to a motherboard header. This chip upgrades SAS support to add RAID 5 support (RAID 0, 1, 5, and 10 for up to eight drives). See Figure C-1.

Note You must have the RAID SCU upgrade ROM installed and before you can use the RAID 5 key.

To install a RAID 5 software key module, follow these steps:

Step 1 Locate the RAID_KEY header (see Figure C-1).

Step 2 Align the connector on the RAID key module with the pins on the header, then gently push the connector onto the pins.

Step 3 Replace the top cover.

Step 4 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Enabling the Integrated RAID Controller in the BIOS

This controller must be enabled in the server BIOS to use it.

Step 1 Boot the server and press **F2** when prompted to enter the BIOS Setup utility.

Step 2 Select the **Advanced** tab, then **South Bridge**.

Step 3 Set Onboard SATA Controller to **Enabled**.

Step 4 Select the SATA Mode.

Step 5 Press **F10** to save your changes and exit the utility.

Disabling the Integrated RAID Controller in the BIOS

If you change from using this integrated controller to a RAID controller card, you must disable the integrated controller in the server BIOS.

Step 1 Boot the server and press **F2** when prompted to enter the BIOS Setup utility.

Step 2 Select the **Advanced** tab, then **South Bridge**.

Step 3 Set Onboard SATA Controller to **Disabled**.

Step 4 Press **F10** to save your changes and exit the utility.

Launching the LSI Embedded RAID Configuration Utility

Launch the utility by pressing **Ctrl+M** when you see the prompt during system boot.

For more information about using the Embedded MegaRAID software to configure your disk arrays, see the LSI Embedded MegaRAID Software User Guide.

Installing LSI MegaSR Drivers For Windows and Linux

Note The required drivers for this controller are already installed and ready to use with the LSI SWRAID Configuration Utility. However, if you will use this controller with Windows or Linux, you must download and install additional drivers for those operating systems.

This section explains how to install the LSI MegaSR drivers for the following supported operating systems:

- Microsoft Windows Server
- Red Hat Enterprise Linux (RHEL)
- SuSE Linux Enterprise Server (SLES)

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section contains the following topics:

- Downloading the LSI MegaSR Drivers, page C-11
- Microsoft Windows Driver Installation, page C-11
- Linux Driver Installation, page C-13

Downloading the LSI MegaSR Drivers

The MegaSR drivers are included in the C-series driver ISO for your server and OS. Download the drivers from Cisco.com:

Step 1 Find the drivers 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) Drivers**.

f. Click the release number that you are downloading.

g. Click **Download** to download the drivers 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 want to save the drivers ISO file.

Microsoft Windows Driver Installation

This section explains the steps to install the LSI MegaSR driver in a Windows installation.

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section contains the following topics:

- Windows Server 2008R2 Driver Installation, page C-11
- Updating the Windows Driver, page C-12
- Linux Driver Installation, page C-13

Windows Server 2008R2 Driver Installation

Perform the following steps to install the LSI MegaSR device driver in a new Windows Server 2008R2 operating system. The Windows operating system automatically adds the driver to the registry and copies the driver to the appropriate directory.

Step 1 Create a RAID drive group using the LSI SWRAID Configuration utility before you install this driver for Windows. Launch this utility by pressing **Ctrl+M** when LSI SWRAID is shown during BIOS post.

Step 2 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11.

Step 3 Prepare the drivers on a USB thumb drive:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

```
/<OS>/Storage/Intel/C600/
```

c. Expand the Zip file, which contains the folder with the MegaSR driver files.

d. Copy the expanded folder to a USB thumb drive.

Step 4 Start the Windows driver installation using one of the following methods:

- To install from local media: Connect an external USB DVD drive to the server and then insert the first Windows install disc into the drive. Skip to Step 6.
- To install from remote ISO: Log in to the server's CIMC interface and continue with the next step.

Step 5 Launch a Virtual KVM console window and select the **Virtual Media** tab.

a. Click **Add Image** and browse to select your remote Windows installation ISO file.

b. Select the check box in the Mapped column for the media that you just added, then wait for mapping to complete.

Step 6 Power cycle the server.

Step 7 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 8 On the Boot Manager window, select the physical disc or virtual DVD and press **Enter**. The Windows installation begins when the image is booted.

Step 9 Press Enter when you see the prompt, "Press any key to boot from CD."

Step 10 Observe the Windows installation process and respond to prompts in the wizard as required for your preferences and company standards.

Step 11 When Windows prompts you with "Where do you want to install Windows," install the drivers for embedded MegaRAID:

a. Click **Load Driver**. You are prompted by a Load Driver dialog to select the driver to be installed.

b. Connect the USB thumb drive that you prepared in Step 3 to the target server.

c. On the Windows Load Driver dialog that you opened in Step a, click Browse.

d. Use the dialog to browse to the location of the drivers folder on the USB thumb drive, and click **OK**.

Windows loads the drivers from the folder and when finished, the driver is listed under the prompt, "Select the driver to be installed."

e. Click **Next** to install the drivers.

Updating the Windows Driver

Perform the following steps to update the LSI MegaSR driver for Windows or to install this driver on an existing system booted from a standard IDE drive.

Step 1 Click **Start**, point to **Settings**, and then click **Control Panel**.

Step 2 Double-click **System**, click the **Hardware** tab, and then click **Device Manager**. Device Manager starts.

Step 3 In Device Manager, double-click **SCSI and RAID Controllers**, right-click the device for which you are installing the driver, and then click **Properties**.

Step 4 On the Driver tab, click **Update Driver** to open the Update Device Driver wizard, and then follow the wizard instructions to update the driver.

Linux Driver Installation

This section explains the steps to install the embedded MegaRAID device driver in a Red Hat Enterprise Linux installation or a SuSE Linux Enterprise Server installation.

This section contains the following topics:

- Obtaining the Driver Image File, page C-13
- Preparing Physical Installation Diskettes For Linux, page C-13
- Installing the Red Hat Linux Driver, page C-15
- Installing the SUSE Linux Enterprise Server Driver, page C-16

Obtaining the Driver Image File

See Downloading the LSI MegaSR Drivers, page C-11 for instructions on obtaining the drivers. The Linux driver is offered in the form of `dud-[driver version].img`, which is the boot image for the embedded MegaRAID stack.

Note The LSI MegaSR drivers that Cisco provides for Red Hat Linux and SUSE Linux are for the original GA versions of those distributions. The drivers do not support updates to those OS kernels.

Preparing Physical Installation Diskettes For Linux

This section describes how to prepare physical Linux installation diskettes from the driver image files, using either the Windows operating system or the Linux operating system.

Note Alternatively, you can mount the `dud.img` file as a virtual floppy disk, as described in the installation procedures.

Preparing Physical Installation Diskettes With the Windows Operating System:

Under Windows, you can use the RaWrite floppy image-writer utility to create disk images from image files. Perform the following steps to build installation diskettes.

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11 and save it to your Windows system that has a diskette drive.

Step 2 Extract the `dud.img` file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

`/<OS>/Storage/Intel/C600/`

c. Expand the Zip file, which contains the folder with the driver files.

Step 3 Copy the driver update disk image `dud-[driver version].img` and your file `raw write.exe` to a directory.

Note RaWrite is not included in the driver package.

Step 4 If necessary, use this command to change the file name of the driver update disk to a name with fewer than eight characters: **copy dud-[***driver version***].img dud.img**

Step 5 Open the DOS Command Prompt and navigate to the directory where `raw write.exe` is located.

Step 6 Type the following command to create the installation diskette: **raw write**

Step 7 Press **Enter**.

You are prompted to enter the name of the boot image file.

Step 8 Type the following: **dud.img**

Step 9 Press **Enter**.

You are prompted for the target diskette.

Step 10 Insert a floppy diskette into the floppy drive and type: **A:**

Step 11 Press **Enter**.

Step 12 Press **Enter** again to start copying the file to the diskette.

Step 13 After the command prompt returns and the floppy disk drive LED goes out, remove the diskette.

Step 14 Label the diskette with the image name.

Preparing Installation Disks With a Linux Operating System:

Under Red Hat Linux and SuSE Linux, you can use a driver diskette utility to create disk images from image files. Perform the following steps to create the driver update disk:

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11 and save it to your Linux system that has a diskette drive.

Step 2 Extract the `dud.img` file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

`/<OS>/Storage/Intel/C600/`

c. Expand the Zip file, which contains the folder with the driver files.

Step 3 Copy the driver update disk image `dud-[driver version].img` to your Linux system.

Step 4 Insert a blank floppy diskette into the floppy drive.

Step 5 Confirm that the files are in the selected directory.

Step 6 Create the driver update diskette using the following command:

dd if=dud-[*driver version*].img of=/dev/fd0

Step 7 After the command prompt returns and the floppy disk drive LED goes out, remove the diskette.

Step 8 Label the diskette with the image name.

Installing the Red Hat Linux Driver

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section describes the fresh installation of the Red Hat Enterprise Linux device driver on systems with the embedded MegaRAID stack.

Step 1 Create a RAID drive group using the LSI SWRAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl+M** when LSI SWRAID is shown during BIOS post.

Step 2 Prepare the `dud.img` file using one of the following methods:

- To install from a physical diskette: Use one of the procedures in Preparing Physical Installation Diskettes For Linux, page C-13.
  Then return to Step 4 of this procedure.
- To install from a virtual floppy disk: Download and save the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11.
  Then continue with the next step.

Step 3 Extract the `dud.img` file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

`/<OS>/Storage/Intel/C600/`

c. Copy the `dud-<driver version>.img` file to a temporary location on your workstation.

Step 4 Start the Linux driver installation using one of the following methods:

- To install from local media: Connect an external USB DVD drive to the server and then insert the first RHEL install disc into the drive.
  Then continue with Step 6.
- To install from remote ISO: Log in to the server's CIMC interface. Then continue with the next step.

Step 5 Launch a Virtual KVM console window and select the **Virtual Media** tab.

a. Click **Add Image** and browse to select your remote RHEL installation ISO file.

b. Click **Add Image** again and browse to select your `dud.img` file.

c. Select the check boxes in the Mapped column for the media that you just added, then wait for mapping to complete.

Step 6 Power cycle the server.

Step 7 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 8 On the Boot Manager window, select the physical disc or virtual DVD and press **Enter**.

The RHEL installation begins when the image is booted.

Step 9 Press **Esc** to go to the CLI boot prompt.

Step 10 Type one of the following commands at the boot prompt:

- For RHEL 5.*x* (32- and 64-bit), type:
  linux dd blacklist=isci blacklist=ahci noprobe=<ata*drive number*>
- For RHEL 6.*x* (32- and 64-bit), type:
  linux dd blacklist=isci blacklist=ahci nodmraid noprobe=<ata*drive number*>

Note The **noprobe** values depend on the number of drives. For example, to install RHEL 5.7 on a RAID 5 configuration with three drives, enter:
linux dd blacklist=isci blacklist=ahci noprobe=ata1 noprobe=ata2 noprobe=ata3

Step 11 Press Enter.

The prompt asks whether you have a driver disk.

Step 12 Use the arrow key to select **Yes**, and then press **Enter**.

Step 13 Select **fd0** to indicate that you have a floppy diskette with the driver on it.

Step 14 Do one of the following actions:

- If you prepared the IMG file on a physical diskette in Step 2: Connect an external USB diskette drive to the target server and then insert the diskette in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in Step 5: Select the location of the virtual floppy.

The installer locates and loads the driver for your device. The following message appears:

```
Loading megasr driver...
```

Step 15 Follow the Red Hat Linux installation procedure to complete the installation.

Step 16 Reboot the system.

Installing the SUSE Linux Enterprise Server Driver

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section describes the installation of the SuSE Linux Enterprise Server driver on a system with the embedded MegaRAID stack.

Us e the following procedure to install the SLES drivers.

Step 1 Create a RAID drive group using the LSI SWRAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl+M** when LSI SWRAID is shown during BIOS post.

Step 2 Prepare the `dud.img` file using one of the following methods:

- To install from a physical diskette: Use one of the procedures in Preparing Physical Installation Diskettes For Linux, page C-13.
  Then return to Step 4 of this procedure.
- To install from a virtual floppy disk: Download and save the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-11.
  Then continue with the next step.

Step 3 Extract the `dud.img` file:

a. Burn the ISO image to a disc.

b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

`/<OS>/Storage/Intel/C600/`

c. Copy the `dud-<driver version>.img` file to a temporary location on your workstation.

Step 4 Start the Linux driver installation using one of the following methods:

- To install from local media: Connect an external USB DVD drive to the server and then insert the first RHEL install disc into the drive. Skip to Step 6.
- To install from remote ISO: Log in to the server's CIMC interface and continue with the next step.

Step 5 Launch a Virtual KVM console window and select the **Virtual Media** tab.

a. Click **Add Image** and browse to select your remote RHEL installation ISO file.

b. Click **Add Image** again and browse to select your `dud.img` file.

c. Select the check box in the Mapped column for the media that you just added, then wait for mapping to complete.

Step 6 Power cycle the server.

Step 7 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 8 On the Boot Manager window, select the physical disc or virtual DVD and press **Enter**. The SLES installation begins when the image is booted.

Step 9 When the first SLES screen appears, select **Installation** on the menu.

Step 10 Type one of the following in the Boot Options field:

- For SLES 11 and SLES 11 SP1 (32- and 64-bit), type: **brokenmodules=ahci**
- For SLES 11 SP2 (32-and 64-bit), type: **brokenmodules=ahci brokenmodules=isci**

Step 11 Press **F6** for the driver and select **Yes**.

Step 12 Do one of the following actions:

- If you prepared the IMG file on a physical diskette in Step 2: Connect an external USB diskette drive to the target server and then insert the diskette in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in Step 5: Select the location of the virtual floppy.

"Yes" appears under the F6 Driver heading.

Step 13 Press **Enter** to select Installation.

Step 14 Press **OK**.

The following message appears: LSI Soft RAID Driver Updates added.

Step 15 At the menu, select the driver update medium and press the **Back** button.

Step 16 Continue and complete the installation process by following the prompts.

RAID Controller Cabling

This section includes the following topics:

- Cable Routing, page C-18
- Cisco UCS C24 Server RAID Cabling Instructions, page C-19

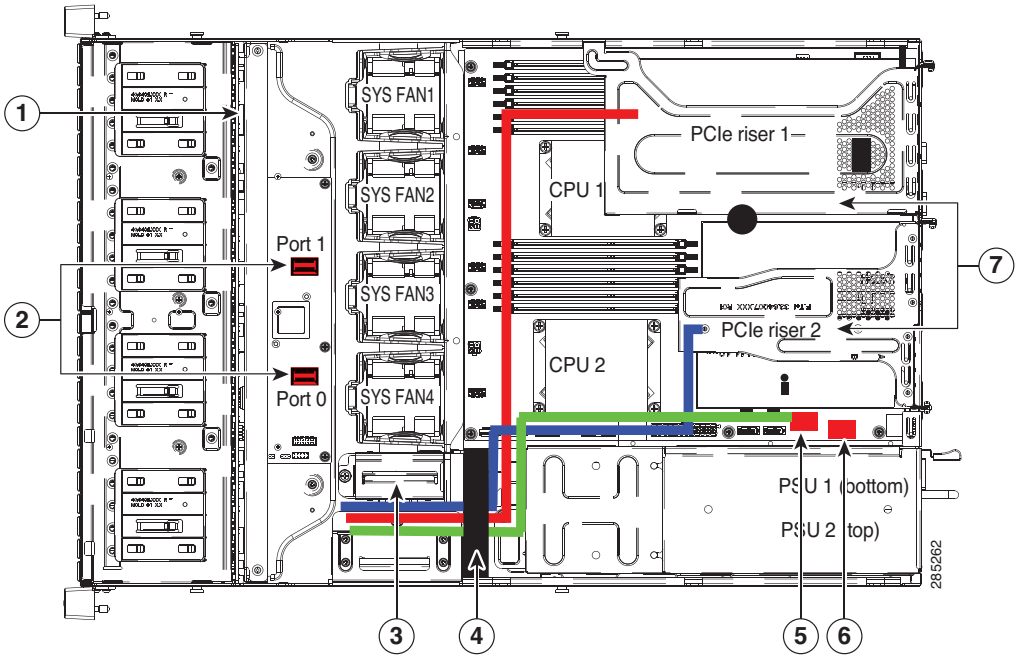
Cable Routing

The RAID controller connectors in this server are shown in Figure C-2. The colored lines indicate the recommended cable-routing paths from the SAS expander or backplane to the possible controller locations:

- The red line is the cable path to a controller in PCIe riser 1. The cable is routed across the chassis in clips on the air baffle (not shown). This is the only riser available in single-CPU configurations.
- The blue line is the cable path to a controller in PCIe riser 2.
- The green line is the cable path to the embedded RAID connectors on the motherboard.

Note The foam rubber air dam must be in place as shown (item 4) when the server is running to ensure correct air flow. The underside of the air dam has an opening that allows the cables to run under it.

Figure C-2 RAID Controller Cable Routing



1	Drive backplane	**5**	Embedded RAID SAS connector (SCU_PORT_0)
2	SAS expander connectors	**6**	Embedded RAID SAS connector (SCU_PORT_1)
3	SCPM mounting cage	**7**	PCIe risers for RAID controller cards
4	Air dam		

Cisco UCS C24 Server RAID Cabling Instructions

This section contains the following topics:

- Backplane and Expander Options, page C-19
- Small Form Factor 24-Drive Backplane With Expander Cabling, page C-19
- Small Form Factor 16-Drive Backplane (No Expander) Cabling, page C-20
- Large Form Factor 12-Drive Backplane With Expander Cabling, page C-21

Backplane and Expander Options

The server is orderable in three different versions, each with one of three different front panel/backplane configurations:

- Cisco UCS C24 (small form-factor (SFF) drives, with 24-drive backplane and expander). Holds up to twenty-four 2.5-inch hard drives or solid state drives.
- Cisco UCS C24 (small form-factor (SFF) drives, with 16-drive backplane, no expander). Holds up to sixteen 2.5-inch hard drives or solid state drives.
- Cisco UCS C240 (large form-factor (LFF) drives, with 12-drive backplane and expander). Holds up to twelve 3.5-inch hard drives.

Note The SAS expander is required for the SFF 24-drive option and the LFF 12-drive option. The SFF 16-drive option does not use the SAS expander.

Small Form Factor 24-Drive Backplane With Expander Cabling

The cable connections required for each type of controller are as follows:

- LSI MegaRAID SAS 9220-8i or 9240-8i PCIe Card (Cable UCSC-CABLE-A6), page C-19
- LSI MegaRAID SAS 9265CV-8i PCIe Card (Cable UCSC-CABLE-A6), page C-19

LSI MegaRAID SAS 9220-8i or 9240-8i PCIe Card (Cable UCSC-CABLE-A6)

These options can control up to 16 drives.

The required UCSC-CABLE-A6 cable kit has two cables. Cable 1 controls drives 1–8 and cable 2 controls drives 9–16.

Step 1 Connect SAS cable 1 from card connector SAS 0 to the Port0 connector on the expander.

Step 2 Connect SAS cable 2 from card connector SAS 1 on the card to the Port1 connector on the expander.

LSI MegaRAID SAS 9265CV-8i PCIe Card (Cable UCSC-CABLE-A6)

This option can control up to 24 drives.

The required UCSC-CABLE-A6 cable kit has two cables. Cable 1 controls drives 1–12 and cable 2 controls drives 13–24.

Step 1 Connect SAS cable 1 from card connector SAS 0 to the Port0 connector on the expander.

Step 2 Connect SAS cable 2 from card connector SAS 1 on the card to the Port1 connector on the expander.

Step 3 If you are using the 9265CV-8i card, you can also install an SCPM for RAID backup. Install the SCPM (see Replacing a SuperCap Power Module (RAID Backup Unit), page 3-41), then attach the cable from the card to the SCPM.

Small Form Factor 16-Drive Backplane (No Expander) Cabling

The SFF 16-drive option does not use a SAS expander, so connections from the controller are made directly to the backplane. The cable connections required for each type of controller are as follows:

- Embedded RAID (Cable UCSC-CABLE-A7), page C-20
- LSI MegaRAID SAS 9266CV-8i, SAS 9220-8i, or SAS 9240-8i PCIe Card (Cable UCSC-CABLE-A7 and -A8), page C-20

Embedded RAID (Cable UCSC-CABLE-A7)

This option can control up to eight drives. This option can be used only with the SFF 16HDD version of the server because this controller does not operate through an expander.

The required UCSC-CABLE-A7 cable kit has two mini-SAS cables. Cable 1 controls drives 1–4 and cable 2 controls drives 5–8.

Step 1 Connect mini-SAS cable 1 from the motherboard connector SCU_PORT_0 to the drives 1–4 connectors on the backplane.

Step 2 Connect the cable 1 SGPIO connector labeled, “S1” to its backplane connector.

Step 3 Connect mini-SAS cable 2 from the motherboard connector SCU_PORT_1 to the drives 5–8 connectors on the backplane.

Step 4 Connect the cable 2 SGPIO connector labeled, “S2” to its backplane connector.

LSI MegaRAID SAS 9266CV-8i, SAS 9220-8i, or SAS 9240-8i PCIe Card (Cable UCSC-CABLE-A7 and -A8)

These option can control up to 8 drives with one controller. You can control up to 16 drives with two controllers and two cable kits.

- Use cable pair UCSC-CABLE-A7 for the first controller.
- Use cable pair UCSC-CABLE-A8 for the second controller, if used.

First Controller (Drives 1 through 8, Cable UCSC-CABLE-A7):

The required UCSC-CABLE-A7 cable kit has two mini-SAS cables. Cable 1 controls drives 1–4 and cable 2 controls drives 5–8. Make the following connections to your first controller card:

Step 1 Connect mini-SAS cable 1 from the card connector SAS1 to the drives 1–4 connectors on the backplane.

Step 2 Connect the cable 1 SGPIO connector labeled, “S1” to its backplane connector.

Step 3 Connect mini-SAS cable 2 from the card connector SAS2 to the drives 5–8 connectors on the backplane.

Step 4 Connect the cable 2 SGPIO connector labeled, “S2” to its backplane connector.

Second Controller (Drives 9 through 16, Cable UCSC-CABLE-A8):

The required UCSC-CABLE-A8 cable kit has two mini-SAS cables. To control 16 drives in this configuration, you must add a second controller card to control drives 9–16. Cable 3 controls drives 9–12 and cable 4 controls drives 13–16. Make the following connections to your second controller card:

Step 1 Connect mini-SAS cable 1 from the card connector SAS1 to the drives 9–12 connectors on the backplane.

Step 2 Connect the cable 1 SGPIO connector labeled, “S1” to its backplane connector.

Step 3 Connect mini-SAS cable 2 from the motherboard connector SAS2 to the drives 13–16 connectors on the backplane.

Step 4 Connect the cable 2 SGPIO connector labeled, “S2” to its backplane connector.

Large Form Factor 12-Drive Backplane With Expander Cabling

The cable connections required for each type of controller are as follows:

LSI MegaRAID SAS 9266CV-8i, SAS 9220-8i, or SAS 9240-8i PCIe Card (Cable UCSC-CABLE-11)

This option can control up to 12 drives.

The required `UCSC-CABLE-11` cable kit has two cables. Cable 1 controls drives 1–6 and cable 2 controls drives 7–12.

Step 1 Connect mini-SAS cable 1 from connector SAS1 on the card to the SAS1 connector on the expander.

Step 2 Connect mini-SAS cable 2 from connector SAS2 on the card to the SAS2 connector on the expander.

Restoring RAID Configuration After Replacing a RAID Controller

When you replace a RAID controller, the RAID configuration that is stored in the controller is lost. Use the following procedure to restore your RAID configuration to your new RAID controller.

Step 1 Replace your RAID controller. See Replacing a PCIe Card, page 3-35.

Step 2 If this was a full chassis swap, replace all drives into the drive bays, in the same order that they were installed in the old chassis.

Step 3 Reboot the server and watch for the prompt to press F.

Note For newer RAID controllers, you are not prompted to press F. Instead, the RAID configuration is imported automatically. In this case, skip to Step 6.

Step 4 Press **F** when you see the following on-screen prompt:

```
Foreign configuration(s) found on adapter.
Press any key to continue or 'C' load the configuration utility,
or 'F' to import foreign configuration(s) and continue.
```

Step 5 Press any key (other than C) to continue when you see the following on-screen prompt:

```
All of the disks from your previous configuration are gone. If this is
an unexpected message, then please power of your system and check your cables
to ensure all disks are present.
Press any key to continue, or 'C' to load the configuration utility.
```

Step 6 Watch the subsequent screens for confirmation that your RAID configuration was imported correctly.

- If you see the following message, your configuration was successfully imported. The LSI virtual drive is also listed among the storage devices.

  N `Virtual Drive(s) found on host adapter.`

- If you see the following message, your configuration was not imported. This can happen if you do not press F quickly enough when prompted. In this case, reboot the server and try the import operation again wen you are prompted to press F.

  `0 Virtual Drive(s) found on host adapter.`

For More Information

The LSI utilities have help documentation for more information about using the utilities.

For basic information about RAID and for using the utilities for the RAID controller cards, see the Cisco UCS Servers RAID Guide.

For more information about using the Embedded MegaRAID software to configure your disk arrays, see the LSI Embedded MegaRAID Software User Guide.

Full LSI documentation is also available:

- LSI MegaRAID SAS Software User's Guide (for LSI MegaRAID)

  http://www.cisco.com/en/US/docs/unified_computing/ucs/3rd-party/lsi/mrsas/userguide/LSI_MR_SAS_SW_UG.pdf

APPENDIX D

Installation for Cisco UCS Integration

The Cisco UCS Manager integration instructions have been moved to the integration guides found here:

Cisco UCS C-Series Server Integration with UCS Manager Guides

Refer to the guide that is for the version of Cisco UCS Manager that you are using.

Also refer to the release notes for Cisco UCS Manager software and C-Series software for any special considerations regarding integration in your release.

- Cisco UCS Manager Release Notes
- Cisco C-Series Software Release Notes