

Cisco UCS C240 M4 Server Installation and Service Guide

May 06, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-32474-01

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 C240 M4 Server Installation and Service Guide
© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

Audience vii

Conventions vii

Related Documentation xiii

Documentation Feedback xiii

Obtaining Documentation and Submitting a Service Request xiii

CHAPTER 1

Overview 1-1

External Features Overview 1-1

Replaceable Component Locations 1-7

Summary of Server Features 1-8

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

Supported Slide Rail Kits 2-4

Slide Rail Adjustment Range and Cable Management Arm Dimensions 2-4

Installing the Server In a Rack 2-5

Installing the Slide Rails 2-5

Installing the Cable Management Arm (Optional) 2-8

Reversing the Cable Management Arm (Optional) 2-9

Initial Server Setup 2-10

Connecting and Powering On the Server (Standalone Mode) 2-10

Local Connection Procedure 2-10

Remote Connection Procedure 2-11

Cisco IMC Configuration Utility Setup 2-12

NIC Modes and NIC Redundancy Settings 2-14

NIC Modes 2-14

NIC Redundancy 2-14

System BIOS and Cisco IMC Firmware 2-15
Updating the BIOS and Cisco IMC Firmware 2-15
Accessing the System BIOS 2-16

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

Server Monitoring and Management Tools 3-1
Cisco Integrated Management Interface 3-1
Server Configuration Utility 3-1
Status LEDs and Buttons 3-2
Front Panel LEDs 3-2
Rear Panel LEDs and Buttons 3-5
Internal Diagnostic LEDs 3-8
Preparing for Server Component Installation 3-9
Required Equipment 3-9
Shutting Down and Powering Off the Server 3-9
Removing and Replacing the Server Top Cover 3-10
Serial Number Location 3-12
Hot-Swap or Hot-Plug Replacement 3-12
Installing or Replacing Server Components 3-13
Replaceable Component Locations 3-14
Replacing Hard Drives or Solid State Drives 3-15
Drive Population Guidelines 3-15
Drive Replacement Procedure 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 3-24
CPU Configuration Rules 3-24
Replacing a CPU and Heatsink 3-24
Additional CPU-Related Parts to Order with RMA Replacement Motherboards 3-28
Replacing a SATA Interposer Board 3-29
Replacing a Cisco Modular RAID Controller Card 3-31
Replacing a Modular RAID Controller Transportable Memory Module (TMM) 3-33
Replacing the Supercap Power Module (RAID Backup Battery) 3-35
Replacing a Software RAID 5 Key Module 3-37
Replacing the Motherboard RTC Battery 3-39
Replacing an Internal SD Card 3-40
Enabling or Disabling the Internal USB Port 3-41

Replacing a PCIe Riser 3-42
Replacing a PCIe Card 3-44
PCIe Slots 3-44
Replacing a PCIe Card 3-46
Special Considerations for Cisco UCS Virtual Interface Cards 3-48
Special Considerations for Cisco UCS Fusion ioDrive3 Storage Accelerator Cards 3-49
Installing Multiple PCIe Cards and Resolving Limited Resources 3-51
Installing an NVIDIA GPU Card 3-53
Overview of Software Requirements 3-53
GPU Card Configuration Rules 3-53
Replacing a GPU Card 3-54
Installing Drivers to Support the NVIDIA GPU Cards 3-55
Replacing Internal SATA Boot Drives 3-57
Replacing an Internal SATA Boot Drive 3-57
Installing a Trusted Platform Module 3-59
Installing the TPM Hardware 3-59
Enabling TPM Support in the BIOS 3-60
Enabling the Intel TXT Feature in the BIOS 3-61
Replacing Power Supplies 3-62
Wiring a DC Power Supply 3-63
Replacing an mLOM Card 3-65
Service DIP Switches 3-67
DIP Switch Location on the Motherboard 3-67
Using the BIOS Recovery DIP Switch 3-68
Procedure 1: Reboot with recovery.cap File 3-68
Procedure 2: Use BIOS Recovery DIP switch and recovery.cap File 3-69
Using the Clear Password DIP Switch 3-70
Using the Clear CMOS DIP Switch 3-71

APPENDIX A **Server Specifications** A-1
Physical Specifications A-1
Power Specifications A-2
650 W AC Power Supply A-2
1200 W AC Power Supply A-3
1400 W AC Power Supply A-3
930 W DC Power Supply A-4
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

Support Matrix For Cisco UCS C240 M4 Server RAID Controllers C-3

Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations C-3

Cisco UCS SAS 9300-8i HBA Support by Server Version C-3

Cisco UCS 9300-8i and 9300-8e Bad Drive and Predictive Failure Behavior C-4

Setting the Preferred Boot Device for Cisco UCS 9300-8i and 9300-8e C-4

Mixing Drive Types in RAID Groups C-5

RAID Backup Units C-5

RAID Controller Cabling C-6

Cable Routing C-6

Cisco UCS C240 M4 Server RAID Controller Cabling Instructions C-7

SFF 8-Drive Direct-Connect Backplane, No Expander C-7

SFF 16-Drive Backplane with Integrated Expander C-7

SFF 24-Drive Backplane with Expander Cabling C-8

LFF 12-Drive Backplane with Expander C-8

Embedded SATA RAID Controller C-9

Embedded SATA RAID Controller Requirements For Front-Facing Drive Control C-9

Embedded SATA RAID: Two SATA Controllers C-10

Embedded SATA RAID Controller Considerations C-11

Installing a SATA Interposer Board For Front-Facing Drive Control C-11

Installing a Software RAID 5 Key Module for Embedded RAID 5 Support C-11

Enabling the Embedded RAID Controller in the BIOS C-12

Enabling SATA Mode and Selecting Option ROM Mode C-12

Disabling the Embedded RAID Controller in the BIOS C-13

Launching the LSI Embedded MegaRAID Configuration Utilities C-13

Installing LSI MegaSR Drivers For Windows and Linux C-14

Downloading the LSI MegaSR Drivers C-14

Microsoft Windows Driver Installation C-15

Linux Driver Installation C-17

Restoring RAID Configuration After Replacing a RAID Controller C-22

For More Information C-23

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



Preface

This preface describes the audience, organization, and conventions of the *Cisco UCS C240 M4 Server Installation and Service Guide*. It also provides information about how to obtain related documentation.

Audience

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

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

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

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

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.

Obtaining Documentation and Submitting 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* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



Overview

This chapter provides an overview of the Cisco UCS C240 M4 server features:

- External Features Overview, page 1-1
- Replaceable Component Locations, page 1-7
- Summary of Server Features, page 1-8

External Features Overview

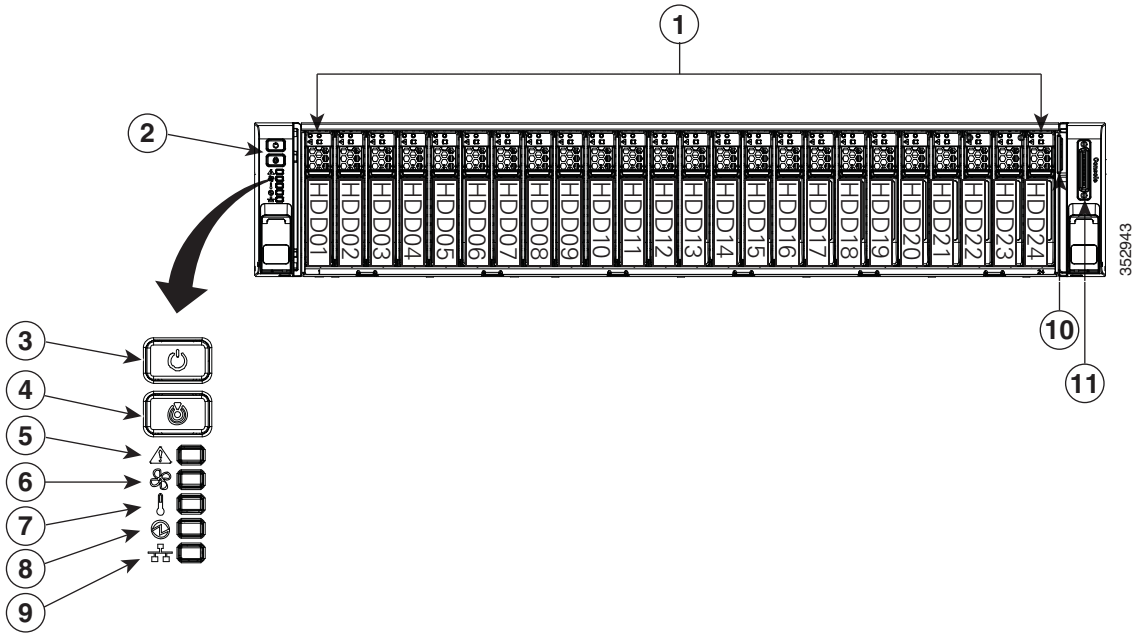
The figures in this chapter show an overview of external server features.

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

- Cisco UCS C240 M4—Small form-factor (SFF) drives with 24-drive backplane and expander. This version holds up to 24 2.5-inch hard drives or solid state drives. See Figure 1-1.
- Cisco UCS C240 M4—SFF drives, with 16-drive backplane and integrated expander. This version holds up to 16 2.5-inch hard drives or solid state drives. See Figure 1-2.
- Cisco UCS C240 M4—SFF drives, with 8-drive direct-connect backplane and no expander. This version holds up to 8 2.5-inch hard drives or solid state drives. See Figure 1-3.
- Cisco UCS C240 M4—Large form-factor (LFF) drives, with 12-drive backplane and integrated expander. This version holds up to 12 3.5-inch hard drives. See Figure 1-4.
- The rear panel features are the same for all four versions of the server. See Figure 1-5.

Figure 1-1 shows the front panel features of the SFF drives, 24-drive version of the server. This version of the server has a 24-drive backplane and an integrated expander.

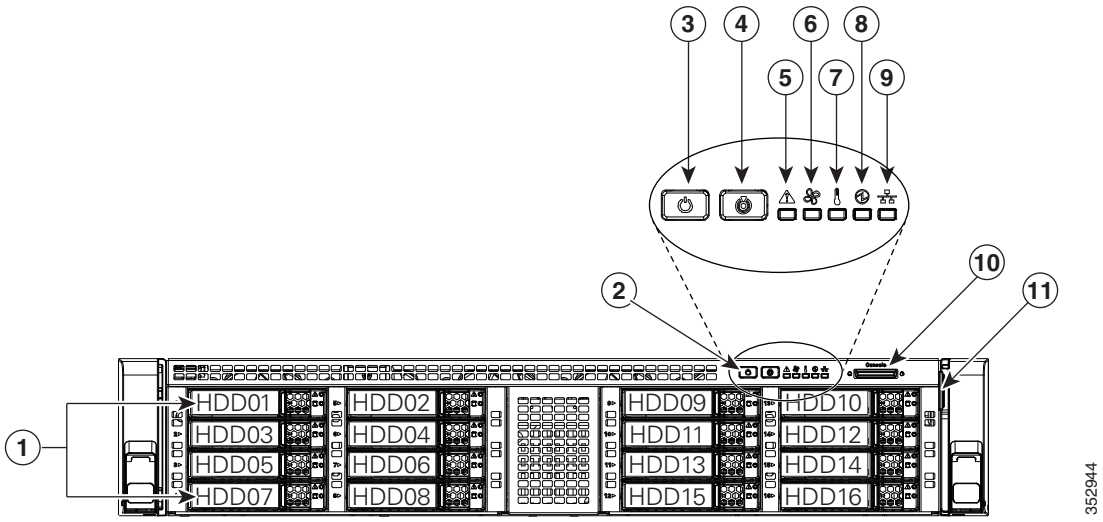
Figure 1-1 Cisco UCS C240 M4 Server (SFF Drives, 24-Drive) Front Panel Features



1	Drive bays 1–24 (up to 24 2.5-inch drives)	**7**	Temperature status LED
2	Operations panel buttons and LEDs	**8**	Power supply status LED
3	Power button/LED	**9**	Network link activity LED
4	Unit Identification button/LED	**10**	Pull-out asset tag
5	System status LED	**11**	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	Fan status LED		

Figure 1-2 shows the front-panel features of the SFF drives, 16-drive version of the server. This version of the server has a 16-drive backplane and an integrated expander.

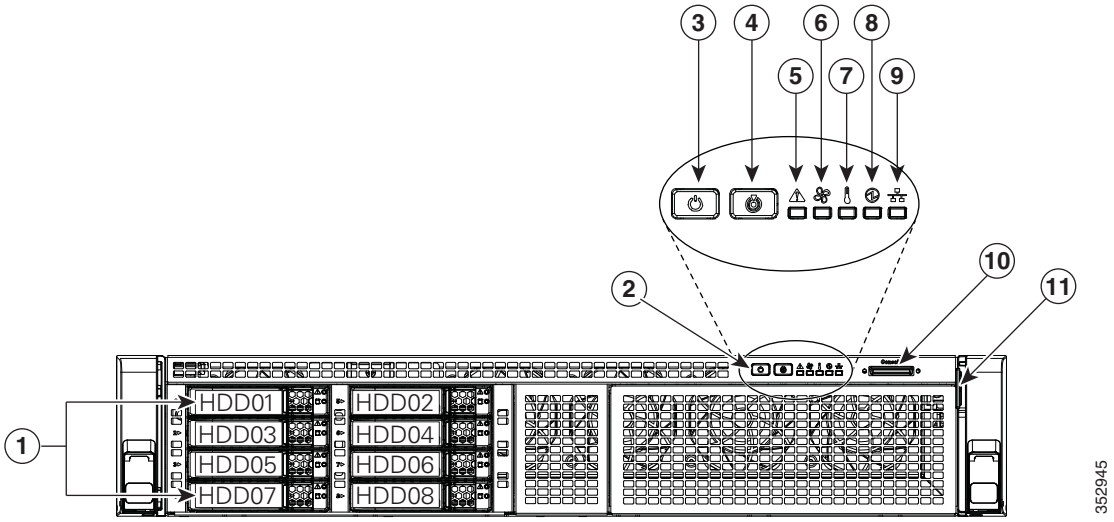
Figure 1-2 Cisco UCS C240 M4 Server (SFF Drives, 16-Drive) Front Panel Features



1	Drive bays 1–16 (up to 16 2.5-inch drives)	**7**	Temperature status LED
2	Operations panel buttons and LEDs	**8**	Power supply status LED
3	Power button/LED	**9**	Network link activity LED
4	Unit Identification button/LED	**10**	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
5	System status LED	**11**	Pull-out asset tag
6	Fan status LED		

Figure 1-3 shows the front-panel features of the SFF drives, 8-drive version of the server. This version of the server has a direct-connect, 8-drive backplane (no expander).

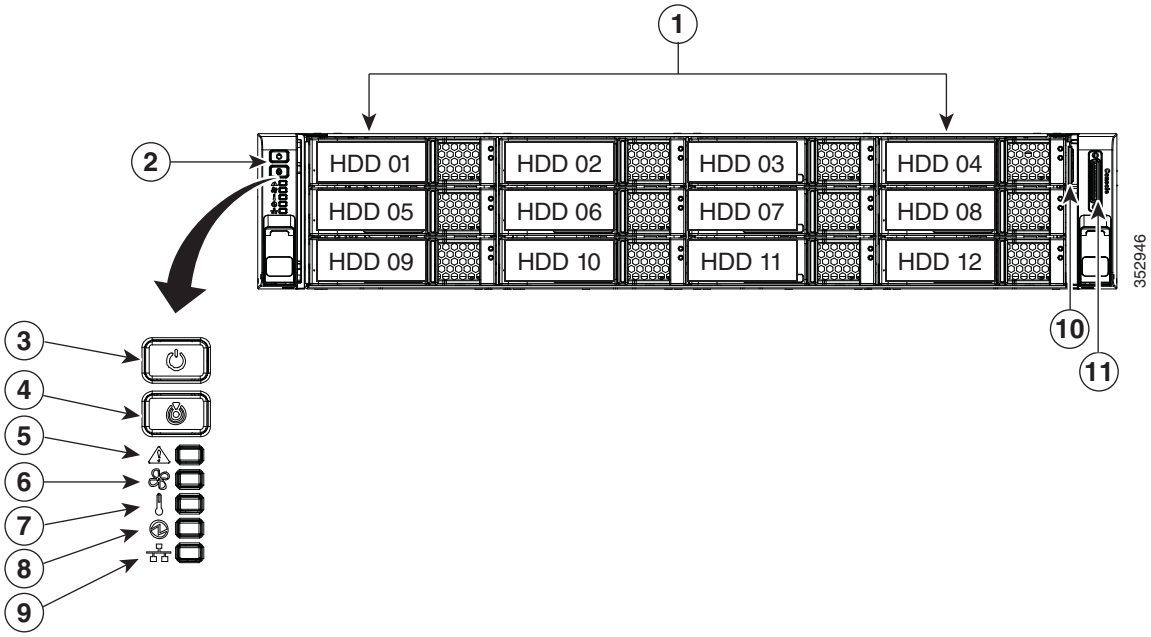
Figure 1-3 Cisco UCS C240 M4 Server (SFF Drives, 8-Drive) Front Panel Features



1	Drive bays 1–16 (up to 16 2.5-inch drives)	**7**	Temperature status LED
2	Operations panel buttons and LEDs	**8**	Power supply status LED
3	Power button/LED	**9**	Network link activity LED
4	Unit Identification button/LED	**10**	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
5	System status LED	**11**	Pull-out asset tag
6	Fan status LED		

Figure 1-4 shows the front panel features of the LFF drives, 12-drive version of the server. This version of the server has a 12-drive backplane with an integrated expander.

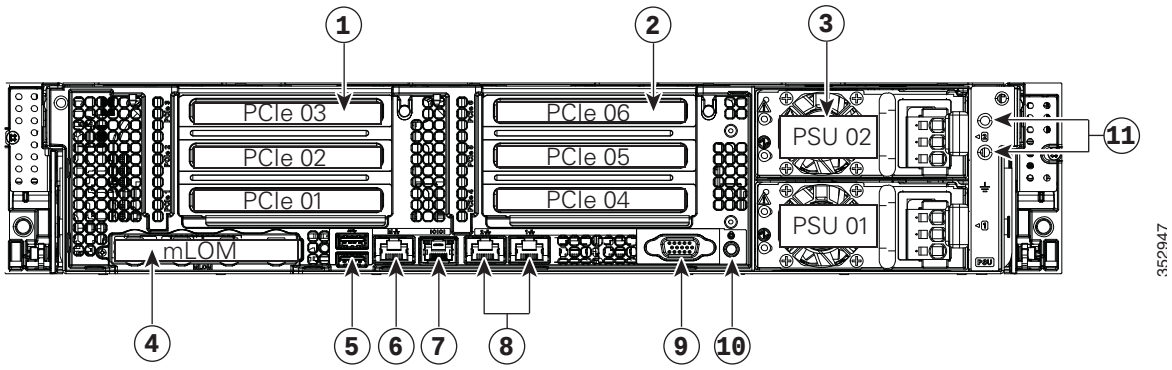
Figure 1-4 Cisco UCS C240 M4 Server (LFF Drives, 12-Drive) Front Panel Features



1	Drive bays 1–16 (up to 16 2.5-inch drives)	**7**	Temperature status LED
2	Operations panel buttons and LEDs	**8**	Power supply status LED
3	Power button/LED	**9**	Network link activity LED
4	Unit Identification button/LED	**10**	Pull-out asset tag
5	System status LED	**11**	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	Fan status LED		

Figure 1-5 shows the rear panel features of the server (identical for all versions of the server).

Figure 1-5 Cisco UCS C240 M4 Server Rear Panel Features

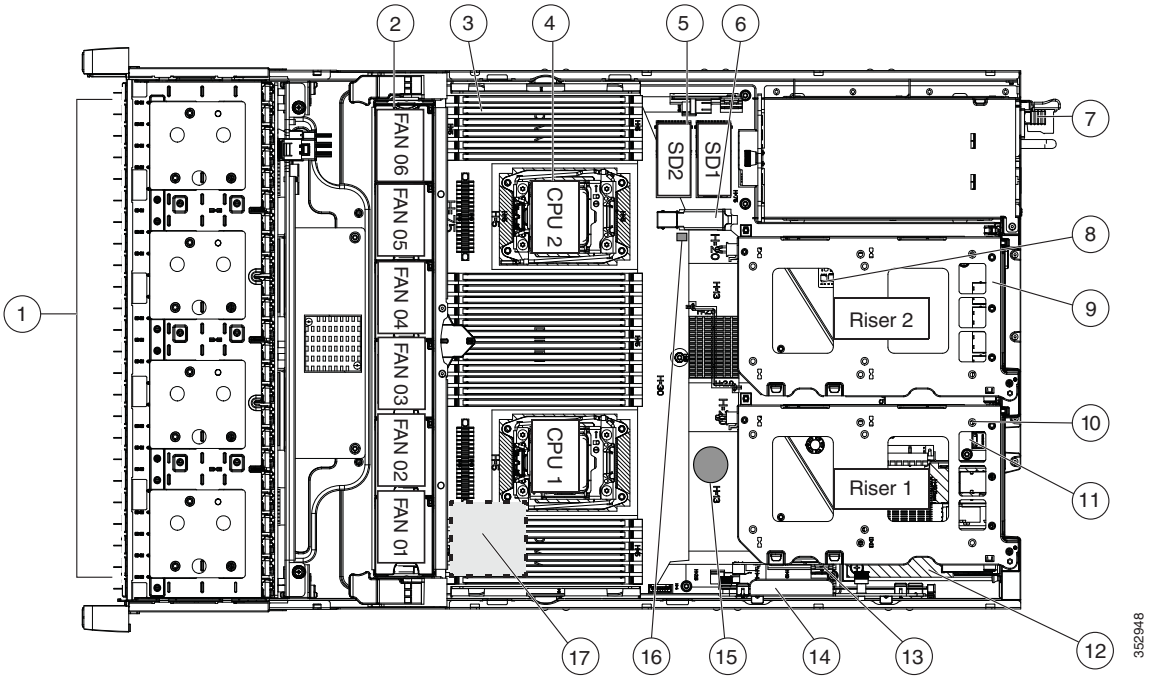


1	PCIe riser 1 (slots 1, 2, 3*) *Slot 3 not present in all versions. See Replacing a PCIe Card, page 3-44 for riser options and slot specifications.	**7**	Serial port (RJ-45 connector)
2	PCIe riser 2 (slots 4, 5, 6)	**8**	Dual 1-Gb Ethernet ports (LAN1, LAN2)
3	Power supplies (DC power supplies shown) See Power Specifications, page A-2 for specifications and options.	**9**	VGA video port (DB-15 connector)
4	Modular LAN-on-motherboard (mLOM) card slot	**10**	Rear Unit Identification button/LED
5	USB 3.0 ports (two)	**11**	Grounding-lug holes (for DC power supplies)
6	1-Gb dedicated management port		

Replaceable Component Locations

Figure 1-6 shows the locations of the field-replaceable components. The view shown is from the top down with the top covers and air baffle removed.

Figure 1-6 Replaceable Component Locations



1	Drives (SAS/SATA drives are hot-swappable and accessed through the front panel)	**10**	PCIe riser 1 (PCIe slots 1, 2, 3*) *Slot 3 not present in all versions. See Replacing a PCIe Card, page 3-44 for riser options and slot specifications.
2	Fan modules (six, hot-swappable)	**11**	SATA boot drives (two sockets available only on PCIe riser 1 option 1C)
3	DIMM sockets on motherboard (up to 24 DIMMs)	**12**	mLOM card socket on motherboard under PCIe riser 1
4	CPUs and heatsinks (two)	**13**	Socket for embedded RAID interposer board
5	Cisco SD card slots on motherboard (two)	**14**	Cisco modular RAID controller PCIe slot (dedicated slot and bracket)
6	USB 3.0 slot on motherboard	**15**	RTC battery on motherboard
7	Power supplies (hot-swappable, accessed through rear panel)	**16**	Embedded RAID header for RAID 5 key
8	Trusted platform module (TPM) socket on motherboard, under PCIe riser 2	**17**	Supercap power module (RAID backup) mounting location on air baffle (not shown)
9	PCIe riser 2 (PCIe slots 4, 5, 6)		

Summary of Server Features

Table 1-1 lists a summary of server features.

Table 1-1 Cisco UCS C240 M4 Server Features

Chassis	Two rack-unit (2RU) chassis.
Processors	Up to two Intel Xeon E5-2600 v3 Series processors.
Memory	24 DDR4 DIMM[1] sockets on the motherboard (12 each CPU).
Multi-bit error protection	Multi-bit error protection is supported.
Baseboard management	BMC, running Cisco Integrated Management Controller (Cisco IMC) firmware. Depending on your Cisco IMC settings, Cisco IMC can be accessed through the 1-Gb dedicated management port, the 1-Gb Ethernet LOM ports, or a Cisco 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 (RJ-45 connector) • One 15-pin VGA[2] connector • Two USB[3] 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector.
Modular I/O	A dedicated socket can be used to add an mLOM card for additional rear-panel connectivity (up to four 1-Gb or 10-Gb Ethernet ports).
WoL	1-Gb BASE-T Ethernet LAN ports support the wake-on-LAN (WoL) standard.
Power	Two power supplies: • AC power supplies optionally 650 W AC, 1200 W AC, or 1400 W AC each. • DC power supplies 930 W DC each. Do not mix power supply types or wattages in the server. Redundant as 1+1. See also Power Specifications, page A-2.
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Up to six horizontal PCIe[4] expansion slots on two risers. Riser 1 can be ordered as one of three different versions: • With slots 1, 2, and 3. • With slots 1 and 2, and a blank slot to accommodate GPU card width. • With slots 1 and 2, plus two connectors for SATA boot drives. Riser 2 contains slots 4, 5, and 6. See Replacing a PCIe Card, page 3-44 for specifications of the slots.
InfiniBand	The InfiniBand architecture is supported by the bus slots.

Table 1-1 Cisco UCS C240 M4 Server Features (continued)

Storage	Drives are installed into front-panel drive bays that provide hot-swappable access for SAS/SATA drives. The server is orderable in four different versions, each with one of four different front panel/backplane configurations • Cisco UCS C240 M4—Small form-factor (SFF) drives with 24-drive backplane and expander. This version holds up to 24 2.5-inch hard drives or solid state drives. • Cisco UCS C240 M4—SFF drives with 16-drive backplane and integrated expander. This version holds up to 16 2.5-inch hard drives or solid state drives. • Cisco UCS C240 M4—SFF drives with 8-drive direct-connect backplane and no expander. This version holds up to 8 2.5-inch hard drives or solid state drives. • Cisco UCS C240 M4—Large form-factor (LFF) drives with 12-drive backplane and integrated expander. This version holds up to 12 3.5-inch hard drives.  **Note** You cannot change the backplane type after-factory. To change a front panel/backplane configuration, a chassis replacement is required.
Internal USB	One internal USB 3.0 port on the motherboard that you can use with a USB thumb drive for additional storage.
SD cards	Two internal bays on the motherboard for up to two SD cards. The two flash drives can be configured in a RAID 1 configuration.
Disk Management (RAID)	Dedicated internal socket for a PCIe-style RAID controller card. The server can optionally use its own embedded SATA RAID controller with the installation of a SATA interposer board. You can optionally add a RAID 5 key to upgrade this SATA RAID. For a list of RAID[5] controller options and required cabling, see RAID Controller Considerations, page C-1.
RAID Backup	Mounting point on the air baffle for the supercap power module that is used with the Cisco modular RAID controller card.
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and 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



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 2-10
- NIC Modes and NIC Redundancy Settings, page 2-14
- System BIOS and Cisco IMC Firmware, page 2-15
- Updating the BIOS and Cisco IMC Firmware, 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

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.

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. 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

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 and Cable Management Arm Dimensions, 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

Caution To ensure proper airflow it is necessary to rack the servers using rail kits. Physically placing the units on top of one another or "stacking" without the use of the rail kits blocks the air vents on top of the servers, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your servers on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the servers. No additional spacing between the servers is required when you mount the units using rail kits.

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.

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, page A-1.
- 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, page A-1. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

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 two RUs, equal to 3.5 in. (88.9 mm).

Equipment Requirements

The slide rails supplied by Cisco Systems for this server do not require tools for installation if you install them in a rack that has square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), or #12-24 UNC threaded holes.

Supported Slide Rail Kits

This server supports one rail kit option: Cisco part UCSC-RAILB-M4= (ball-bearing rail kit).

Do not attempt to use a rail kit that was for the Cisco UCS C240 M3 server; the rail kit for the Cisco UCS C240 M4 server has been designed specifically for it.

Slide Rail Adjustment Range and Cable Management Arm Dimensions

The slide rails for this server have an adjustment range of 26 to 36 inches (660 to 914 mm).

The optional cable management arm (CMA) adds additional length requirements:

- The additional distance from the rear of the server to the rear of the CMA is 5.4 inches (137.4 mm)
- The total length of the server including the CMA is 34.4 inches (874 mm).

Installing the Server In a Rack

This section contains the following sections:

- Installing the Slide Rails, page 2-5
- Installing the Cable Management Arm (Optional), page 2-8
- Reversing the Cable Management Arm (Optional), page 2-9

Installing the Slide Rails

This section describes how to install the server in a rack using the rack kits that are sold by Cisco.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**
This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
Statement 1006

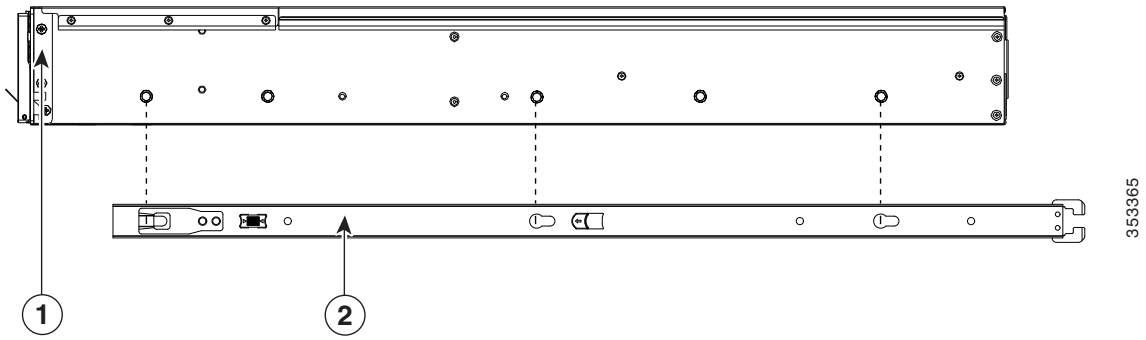
Step 1 Attach the inner rails to the sides of the server:

a. Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the server (see Figure 2-1).

b. Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

c. Install the second inner rail to the opposite side of the server.

Figure 2-1 Attaching Inner Rail to Side of Server

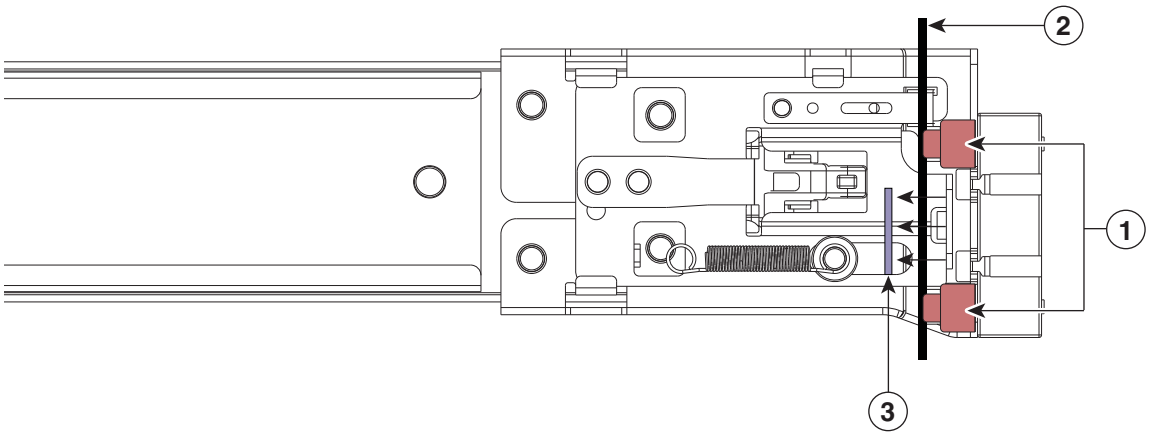


1	Front of server	**2**	Locking clip on inner rail

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

On the outside of the assembly, push the green arrow button toward the rear to open the securing plate.

Figure 2-2 Front Securing Mechanism, Inside of Front End



1	Front mounting pegs	**3**	Securing plate shown pulled back to open position
2	Rack post		

Step 3 Install the slide rails into the rack:

a. Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front (see Figure 2-2).

Note The rack post must be between the mounting pegs and the open securing plate.

b. Push the mounting pegs into the rack-post holes from the outside-front.

c. Press the securing plate release button, marked “PUSH.” The spring-loaded securing plate closes to lock the pegs in place.

d. Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.

The rear mounting pegs enter the rear rack-post holes from the inside of the rack post.

e. Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.

f. Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 4 Insert the server into the slide rails:

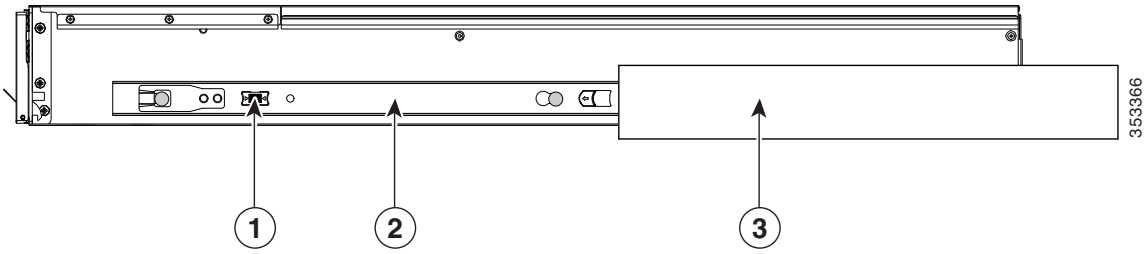
Caution This server can weigh up to 67 pounds (59 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

a. Align the rear of the inner rails that are attached to the server sides with the front ends of the empty slide rails on the rack.

b. Push the inner rails into the slide rails on the rack until they stop at the internal stops.

c. Slide the release clip toward the rear on both inner rails (Figure 2-3), and then continue pushing the server into the rack until its front slam latches engage with the rack posts.

Figure 2-3 Inner Rail Release Clip



1	Inner rail release clip	**3**	Outer rail attached to rack post
2	Inner rail attached to server		

Step 5 (Optional) Secure the server in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with servers installed.

With the server fully pushed into the slide rails, open a hinged slam latch lever on the front of the server and insert the screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the server from being pulled out. Repeat for the opposite slam latch.

Installing the Cable Management Arm (Optional)

Note The CMA is reversible left to right. To reverse the CMA, see Reversing the Cable Management Arm (Optional), page 2-9 before installation.

Step 1 With the server pushed fully into the rack, slide the CMA tab of the CMA arm that is farthest from the server onto the end of the stationary slide rail that is attached to the rack post (see Figure 2-4). Slide the tab over the end of the rail until it clicks and locks.

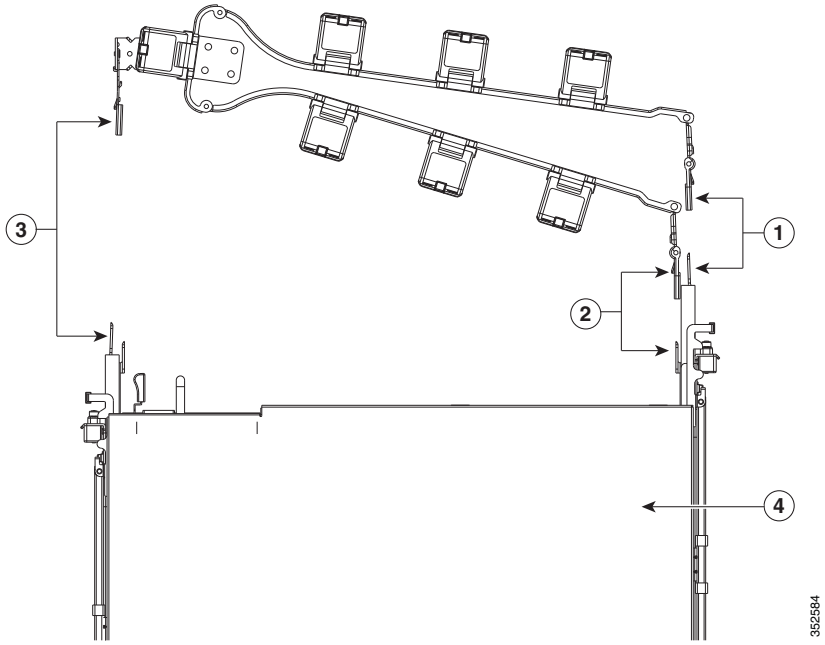
Step 2 Slide the CMA tab that is closest to the server over the end of the inner rail that is attached to the server (see Figure 2-4). Slide the tab over the end of the rail until it clicks and locks.

Step 3 Pull out the width-adjustment slider that is at the opposite end of the CMA assembly until it matches the width of your rack (see Figure 2-4).

Step 4 Slide the CMA tab that is at the end of the width-adjustment slider onto the end of the stationary slide rail that is attached to the rack post (see Figure 2-4). Slide the tab over the end of the rail until it clicks and locks.

Step 5 Open the hinged flap at the top of each plastic cable guide and route your cables through the cable guides as desired.

Figure 2-4 Attaching the Cable Management Arm to the Rear of the Slide Rails



1	CMA tab on arm farthest from server and end of stationary outer slide rail	**3**	CMA tab on width-adjustment slider and end of stationary outer slide rail
2	CMA tab on arm closest to the server and end of inner slide rail attached to server	**4**	Rear of server

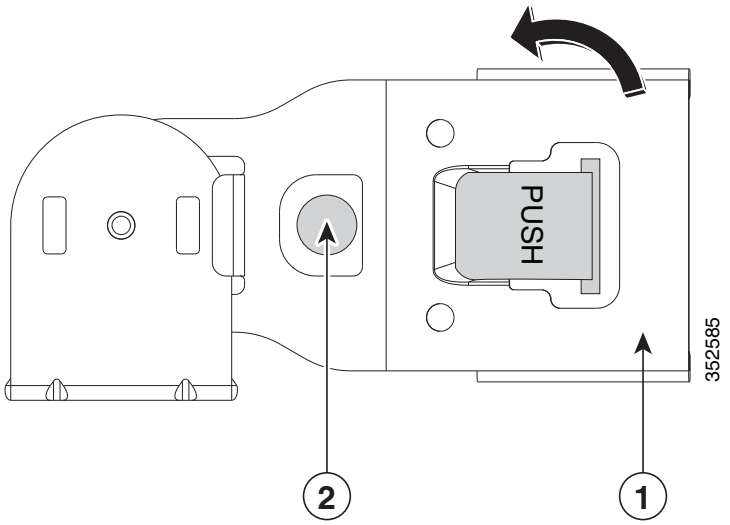
Reversing the Cable Management Arm (Optional)

Step 1 Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.

Step 2 Flip the tabs at the end of each CMA arm so that they point toward the rear of the server.

Step 3 Pivot the tab that is at the end of the width-adjustment slider. Depress and hold the metal button on the outside of the tab and pivot the tab 180 degrees so that it points toward the rear of the server.

Figure 2-5 Reversing the CMA



1	CMA tab on end of width-adjustment slider	**2**	Metal button for rotating

Initial Server Setup

Connecting and Powering On the Server (Standalone Mode)

Note This section describes how to power on the server, assign an IP address, and connect to server management when using the server *in standalone mode*. To use the server in UCS integration, specific cabling and settings are required. See Installation for Cisco UCS Integration, page D-1.

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 Cisco Integrated Management Interface (Cisco IMC). If you want to use the 10/100/1000 dedicated management ports to access Cisco IMC, you can connect to the server and change the NIC mode as described in Step 1 of the following procedure.
- The NIC redundancy is active-active. All Ethernet ports are utilized simultaneously.
- DHCP is enabled.
- IPv4 is enabled. You can change this to IPv6.

There are two methods for connecting to the system for initial setup:

- Local setup—Use this procedure if you want to connect a keyboard and monitor to the system for setup. This procedure requires a KVM cable (Cisco PID N20-BKVM). See Local Connection Procedure, page 2-10.
- Remote setup—Use this procedure if you want to perform setup through your dedicated management LAN. See Remote Connection Procedure, page 2-11.

Note To configure the system remotely, you must have a DHCP server on the same network as the system. Your DHCP server must be preconfigured with the range of MAC addresses for this server node. The MAC address is printed on a label on the rear of the server node. This server node 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.

Local Connection Procedure

Step 1 Attach a power cord to each power supply in your server, and then attach each power cord to a grounded AC power outlet. See 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 system power status by looking at the system Power Status LED on the front panel (see External Features Overview, page 1-1). The system is in standby power mode when the LED is amber.

Step 2 Connect a USB keyboard and VGA monitor to the server using one of the following methods:

- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel (see External Features Overview, page 1-1).
- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel (see External Features Overview, page 1-1 for the connector location). Connect your USB keyboard and VGA monitor to the KVM cable.

Step 3 Open the Cisco IMC Configuration Utility:

a. Press and hold the front panel power button for four seconds to boot the server.

b. During bootup, press **F8** when prompted to open the Cisco IMC Configuration Utility.

This utility has two windows that you can switch between by pressing F1 or F2.

Step 4 Continue with Cisco IMC Configuration Utility Setup, page 2-12.

Remote Connection Procedure

Step 1 Attach a power cord to each power supply in your server, and then attach each power cord to a grounded AC power outlet. See 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 system power status by looking at the system Power Status LED on the front panel (see External Features Overview, page 1-1). The system is in standby power mode when the LED is amber.

Step 2 Plug your management Ethernet cable into the dedicated management port on the rear panel (see External Features Overview, page 1-1).

Step 3 Allow your preconfigured DHCP server to assign an IP address to the server node.

Step 4 Use the assigned IP address to access and log in to the Cisco IMC for the server node. Consult with your DHCP server administrator to determine the IP address.

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

Step 5 From the Cisco IMC Server Summary page, click **Launch KVM Console**. A separate KVM console window opens.

Step 6 From the Cisco IMC Summary page, click **Power Cycle Server**. The system reboots.

Step 7 Select the KVM console window.

Note The KVM console window must be the active window for the following keyboard actions to work.

Step 8 When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.

This utility has two windows that you can switch between by pressing F1 or F2.

Step 9 Continue with Cisco IMC Configuration Utility Setup, page 2-12.

Cisco IMC Configuration Utility Setup

The following procedure is performed after you connect to the system and open the Cisco IMC Configuration Utility.

Step 1 Set NIC mode and NIC redundancy:

a. Set the NIC mode to choose which ports to use to access Cisco IMC for server management (see Figure 1-5 for identification of the ports):

- Shared LOM EXT (default)—This is the shared LOM extended mode, the factory-default setting. 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 Cisco IMC through a Cisco card in standalone mode.
- Dedicated—The dedicated management port is used to access Cisco IMC. You must select a NIC redundancy and IP setting.
- Shared LOM—The 1-Gb Ethernet ports are used to access Cisco IMC. 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 Cisco IMC. You must select a NIC redundancy and IP setting.

  See also the required VIC Slot setting below.
- VIC Slot—If you use the Cisco Card NIC mode, you must select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).
  - If you select Riser1, slot 2 is the primary slot, but you can use slot 1.
  - If you select Riser2, slot 5 is the primary slot, but you can use slot 4.
  - If you select Flex-LOM, you must use an mLOM-style VIC in the mLOM slot.

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. This setting can be used only with the Dedicated NIC mode.
- Active-standby—If an active Ethernet port fails, traffic fails over to a standby port.
- Active-active—All Ethernet ports are utilized simultaneously. Shared LOM EXT mode can have only this NIC redundancy setting. Shared LOM and Cisco Card modes can have both Active-standby and Active-active settings.

Step 2 Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.

Note Before you enable DHCP, you must preconfigure your DHCP server 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 Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

The static IPv4 and IPv6 settings include the following:

- 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 entering **::** (two colons).

- The preferred DNS server address.

  For IPv6, you can set this as none by entering **::** (two colons).

Step 3 (Optional) Use this utility to make VLAN settings.

Step 4 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 5 (Optional) Set a hostname for the server.

Step 6 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 7 (Optional) If you check the Factory Default check box, the server reverts to the factory defaults.

Step 8 (Optional) Set a default user password.

Step 9 (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 10 (Optional) Reset port profiles and the port name.

Step 11 Press **F5** to refresh the settings that 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 12 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.

Use a browser and the IP address of the Cisco IMC to connect to the Cisco IMC management interface. The IP address is based upon the settings that you made (either a static address or the address assigned by your DHCP server).

Note The default username 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

NIC Modes

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

- Shared LOM EXT (default)—This mode is the shared LOM extended mode that is the factory-default setting. 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 Cisco IMC. You must select a NIC redundancy and IP setting.
- Shared LOM—The 1-Gb Ethernet ports are used to access Cisco IMC. 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 Cisco IMC. You must select a NIC redundancy and IP setting.

  See also the required VIC Slot setting below.
- VIC Slot—If you use the Cisco Card NIC mode, you select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).
  - If you select Riser1, slot 2 is the primary slot, but you can also use slot 1.
  - If you select Riser2, slot 5 is the primary slot, but you can also use slot 4.
  - If you select Flex-LOM, you must use an mLOM-style VIC in the mLOM slot.

NIC Redundancy

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. This setting can be used only with the Dedicated NIC mode.
- Active-standby—If an active Ethernet port fails, traffic fails over to a standby port.
- Active-active—All Ethernet ports are utilized simultaneously. Shared LOM EXT mode can have only this NIC redundancy setting. Shared LOM and Cisco Card modes can have both Active-standby and Active-active settings.

  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 Cisco IMC Firmware

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

- Updating the BIOS and Cisco IMC Firmware, page 2-15
- Accessing the System BIOS, page 2-16

Updating the BIOS and Cisco IMC Firmware

Caution When you upgrade the BIOS firmware, you must also upgrade Cisco IMC firmware to the same version or the server will not boot. Do not power on the server until the BIOS and Cisco IMC firmware are matching or the server does not boot.

Cisco provides the Cisco Host Upgrade Utility to assist with simultaneously upgrading the BIOS, Cisco IMC, 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 system components firmware update**: Use the Cisco Host Upgrade Utility to simultaneously upgrade Cisco IMC, BIOS, LOM, LSI storage controller, and Cisco UCS VIC firmware to compatible levels.

  See the *Cisco Host Upgrade Utility Quick Reference Guide* for your firmware level at the documentation roadmap link below.
- 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 Cisco IMC and BIOS firmware by using the Cisco IMC GUI interface.

  See the *Cisco UCS C-Series Rack-Mount Server Configuration Guide.*
- You can upgrade Cisco IMC and BIOS firmware by using the Cisco IMC 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

You can change the BIOS settings for your server. 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**.



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 3-9
- Installing or Replacing Server Components, page 3-13
- Service DIP Switches, page 3-67

Server Monitoring and Management Tools

Cisco Integrated Management Interface

You can monitor the server inventory, health, and system event logs by using the built-in Cisco Integrated Management Controller (Cisco IMC) 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 also download the ISO image 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

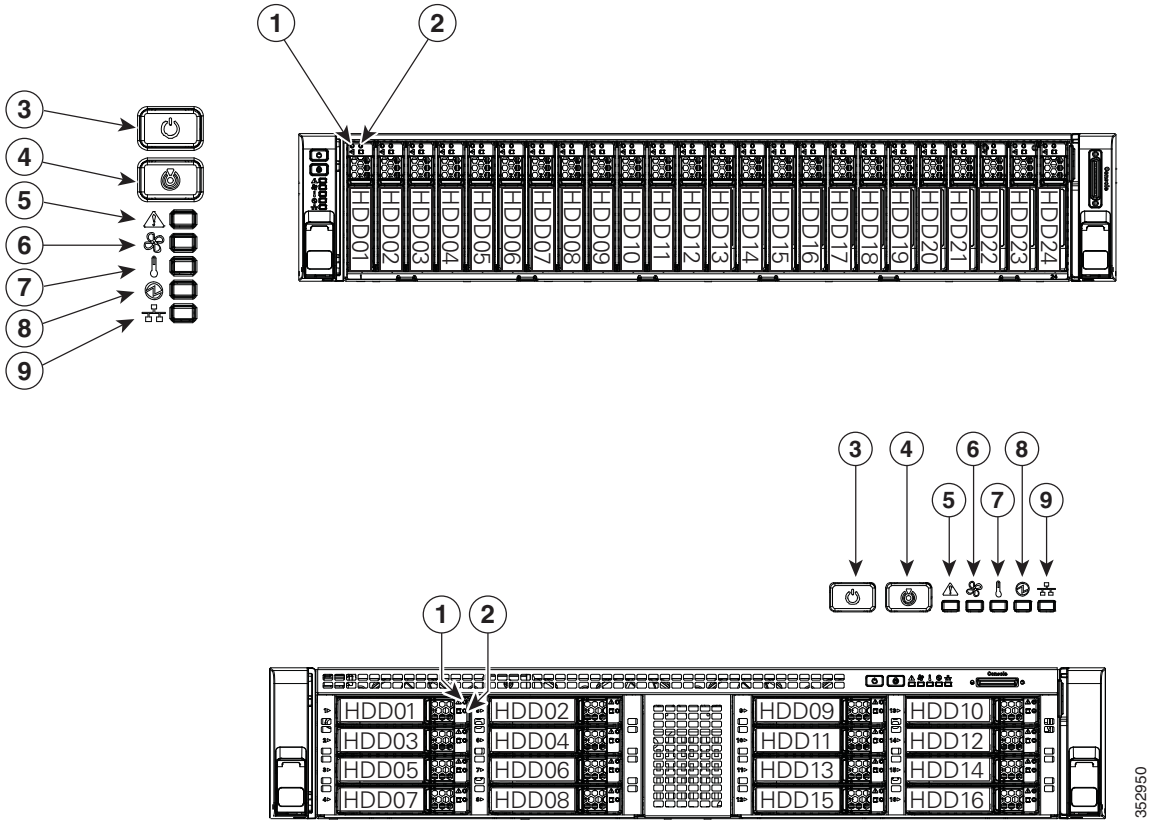
- Front Panel LEDs, page 3-2
- Rear Panel LEDs and Buttons, page 3-5
- Internal Diagnostic LEDs, page 3-8

Front Panel LEDs

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

The small form factor (SFF) drives, 24-drive version and the SFF drives, 16-drive version are shown.

Figure 3-1 Front Panel LEDs



1	Hard drive fault LED (on each drive tray)	**6**	Fan status LED
2	Hard drive activity LED (on each drive tray)	**7**	Temperature status LED
3	Power button/power status LED	**8**	Power supply status LED
4	Unit Identification button/LED	**9**	Network link activity LED
5	System status LED		

Table 3-1 Front Panel LEDs, Definitions of States

	LED Name	State
1	Hard drive fault **Note:** If your controller is a Cisco UCS RAID SAS 9300-8i or 9300-8e HBA, see Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations, page C-3 for differing LED behavior.	• Off—The hard drive is operating properly. • Amber—Drive fault detected. • Amber, blinking—The device is rebuilding. • Amber, blinking with one-second interval—Drive locate function activated.
2	Hard drive activity	• Off—There is no hard drive in the hard drive tray (no access, no fault). • Green—The hard drive is ready. • Green, blinking—The hard drive is reading or writing data.
3	Power button/LED	• Off—There is no AC power to the server. • Amber—The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions. • Green—The server is in main power mode. Power is supplied to all server components.
4	Unit Identification	• Off—The unit identification function is not in use. • Blue—The unit identification function is activated.
5	System status	• Green—The server is running in a 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 an over-temperature condition.
6	Fan status	• Green—All fan modules are operating properly. • Amber, steady—One or more fan modules breached the critical threshold. • Amber, blinking—One or more fan modules breached the non-recoverable threshold.

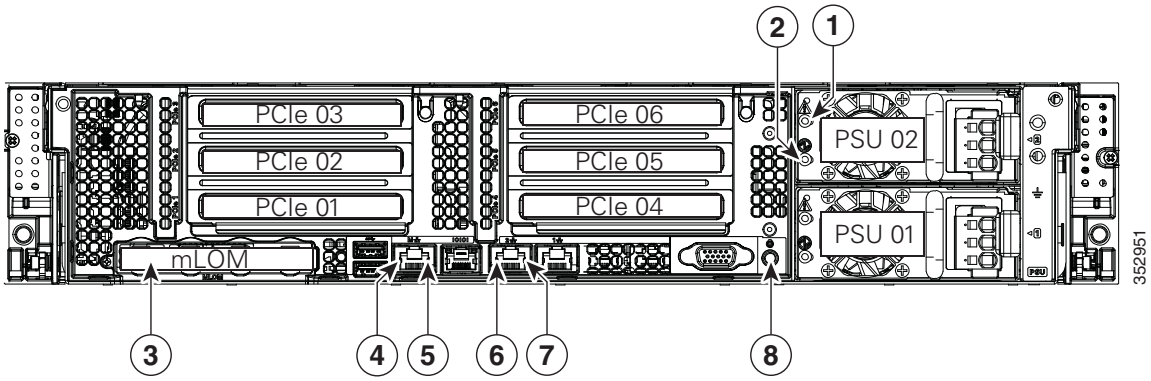
Table 3-1 Front Panel LEDs, Definitions of States (continued)

	LED Name	State
7	Temperature status	• Green—The server is operating at normal temperature. • Amber, steady—One or more temperature sensors breached the critical threshold. • Amber, blinking—One or more temperature sensors breached the non-recoverable threshold.
8	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.
9	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.

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**	1-Gb Ethernet dedicated management link status LED
2	Power supply AC status LED	**6**	1-Gb Ethernet link speed LED
3	Optional mLOM card LEDs (not shown, see Table 3-2)	**7**	1-Gb Ethernet link status LED
4	1-Gb Ethernet dedicated management link speed LED	**8**	Unit Identification button/LED

Table 3-2 Rear Panel LEDs, Definitions of States

	LED Name	State
1	Power supply fault This is a summary; for advanced power supply LED information, see Table 3-3.	• 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).
2	Power supply status This is a summary; for advanced power supply LED information, see Table 3-3.	AC power supplies: • 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. DC power supplies: • Off—There is no DC power to the power supply. • Green, blinking—DC power OK; DC output not enabled. • Green, solid—DC power OK; DC outputs OK.

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

	LED Name	State
3	Optional mLOM 10-Gb SFP+ (there is a single status LED)	• Off—No link is present. • Green, steady—Link is active. • Green, blinking—Traffic is present on the active link.
3	Optional mLOM 10-Gb BASE-T link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps/1 Gbps. • Green—Link speed is 10 Gbps.
3	Optional mLOM 10-Gb BASE-T link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
4	1-Gb Ethernet dedicated management link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
5	1-Gb Ethernet dedicated management link status	• Off—No Link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
6	1-Gb Ethernet link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
7	1-Gb Ethernet link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
8	Unit Identification	• Off—The unit identification function is not in use. • Blue—The unit identification function is activated.

In Table 3-3, read the status and fault LED states together in each row to determine the event that cause this combination.

Table 3-3 Rear Power Supply LED States

Green PSU Status LED State	Amber PSU Fault LED State	Event
• Solid on	• Off	12V main on (main power mode)
• Blinking	• Off	12Vmain off (standby power mode)
• Off	• Off	No AC power input (all PSUs present)
• Off	• On	No AC power input (redundant supply active)
• Blinking	• Solid on	12V over-voltage protection (OVP)
• Blinking	• Solid on	12V under-voltage protection (UVP)
• Blinking	• Solid on	12V over-current protection (OCP)
• Blinking	• Solid on	12V short-circuit protection (SCP)
• Solid on	• Solid on	PSU fan fault/Lock (before OTP)
• Blinking	• Solid on	PSU fan fault/Lock (after OTP)
• Blinking	• Solid on	Over-temperature protection (OTP)
• Solid on	• Blinking	OTP warning
• Solid on	• Blinking	OCP warning
• Blinking	• Off	12V main off (CR slave PSU is in sleep mode)

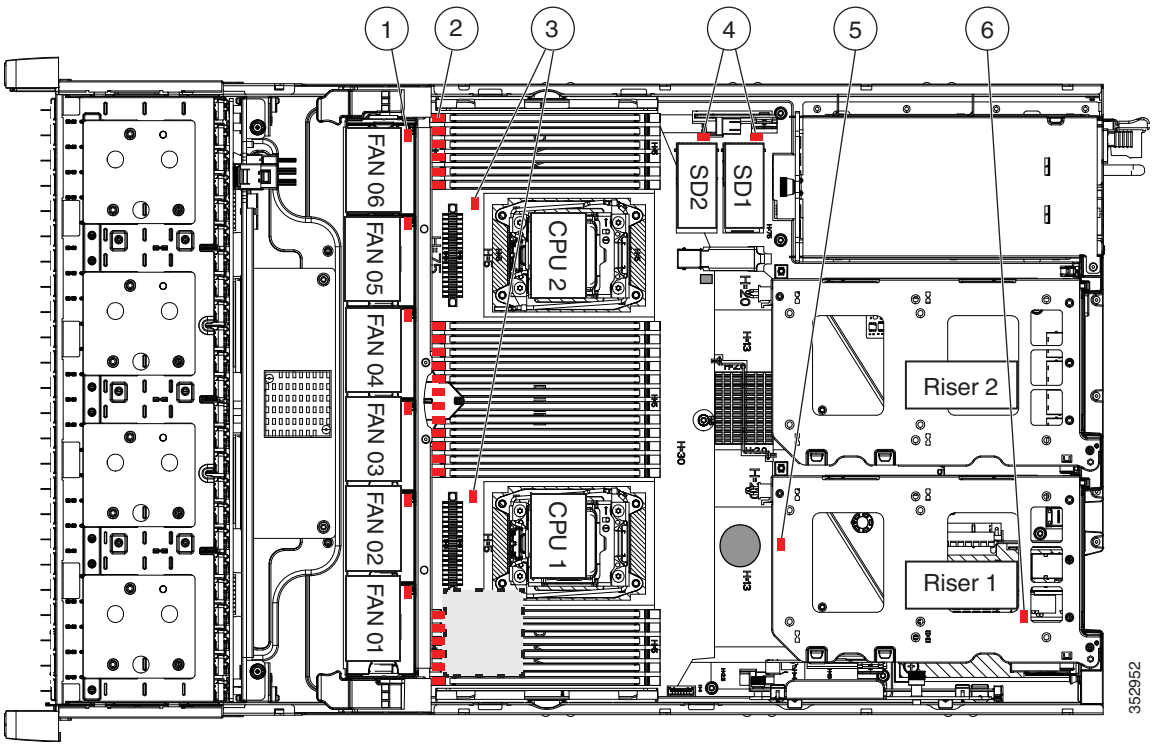
Internal Diagnostic LEDs

The server is equipped with a supercap voltage source that can activate internal component fault LEDs up to 30 minutes after AC power is removed. The server has internal fault LEDs for CPUs, DIMMs, fan modules, SD cards, the RTC battery, and the mLOM card.

To use these LEDs to identify a failed component, press the front or rear Unit Identification button (see Figure 3-1 or Figure 3-2) with AC power removed. An LED lights amber to indicate a faulty component.

See Figure 3-3 for the locations of these internal LEDs.

Figure 3-3 Internal Diagnostic LED Locations



1	Fan module fault LEDs (one on each fan module)	**4**	SD card fault LEDs
2	DIMM fault LEDs (one directly in front of each DIMM socket on the motherboard)	**5**	RTC battery fault LED (under PCIe riser 1)
3	CPU fault LEDs	**6**	mLOM card fault LED (under PCIe riser 1)

Table 3-4 Internal Diagnostic LEDs, Definition of States

LED Name	State
Internal diagnostic LEDs (all)	• Off—Component is functioning normally. • Amber—Component has a fault.

Preparing for Server Component Installation

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

- Required Equipment, page 3-9
- Shutting Down and Powering Off the Server, page 3-9
- Removing and Replacing the Server Top Cover, page 3-10
- Serial Number Location, page 3-12
- Hot-Swap or Hot-Plug Replacement, page 3-12

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 a hard shutdown by using either of the following methods:

- Use the Cisco IMC 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

Step 1 Remove the top cover (see Figure 3-4).

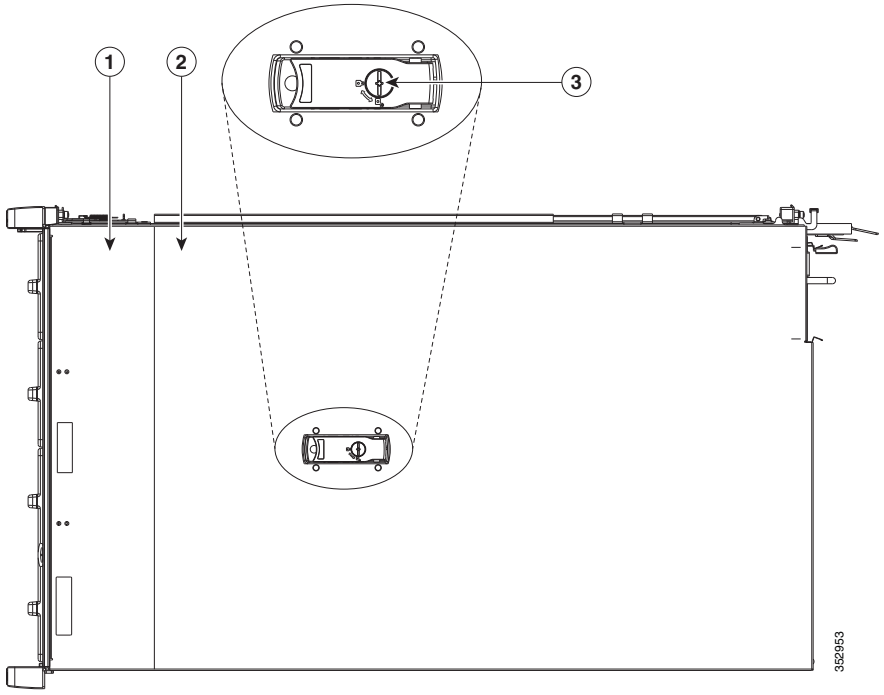
- **a.** If the cover latch is locked, use a screwdriver to turn the lock 90-degrees counterclockwise to unlock it. See Figure 3-4.
- **b.** Lift on the end of the latch that has the green finger grip. The cover is pushed back to the open position as you lift the latch.
- **c.** Lift the top cover straight up from the server and set it aside.

Step 2 Replace the top cover:

Note The latch must be in the fully open position when you set the cover back in place, which allows the opening in the latch to sit over a peg that is on the fan tray.

- **a.** With the latch in the fully open position, place the cover on top of the server about one-half inch (1.27 cm) behind the lip of the front cover panel. The opening in the latch should fit over the peg that sticks up from the fan tray.
- **b.** Press the cover latch down to the closed position. The cover is pushed forward to the closed position as you push down the latch.
- **c.** If desired, lock the latch by using a screwdriver to turn the lock 90-degrees clockwise.

Figure 3-4 Removing the Top Cover



1	Front cover panel	**3**	Locking cover latch
2	Top cover		

Serial Number Location

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

Hot-Swap or Hot-Plug Replacement

Some components can be removed and replaced without powering off and removing AC power from the server.

- Hot-swap replacement—You do not have to precondition or shut down the component in the software before you remove it for the following components:
  - SAS/SATA drives
  - Cooling fan modules
  - Power supplies (when 1+1 redundant)

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

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

Tip You can press the Unit Identification button on the front panel or rear panel to turn on a flashing Unit Identification LED on the front and rear panels of the server. This button 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 Cisco IMC interface.See the "Status LEDs and Buttons" section on page 3-2 for locations of these LEDs.

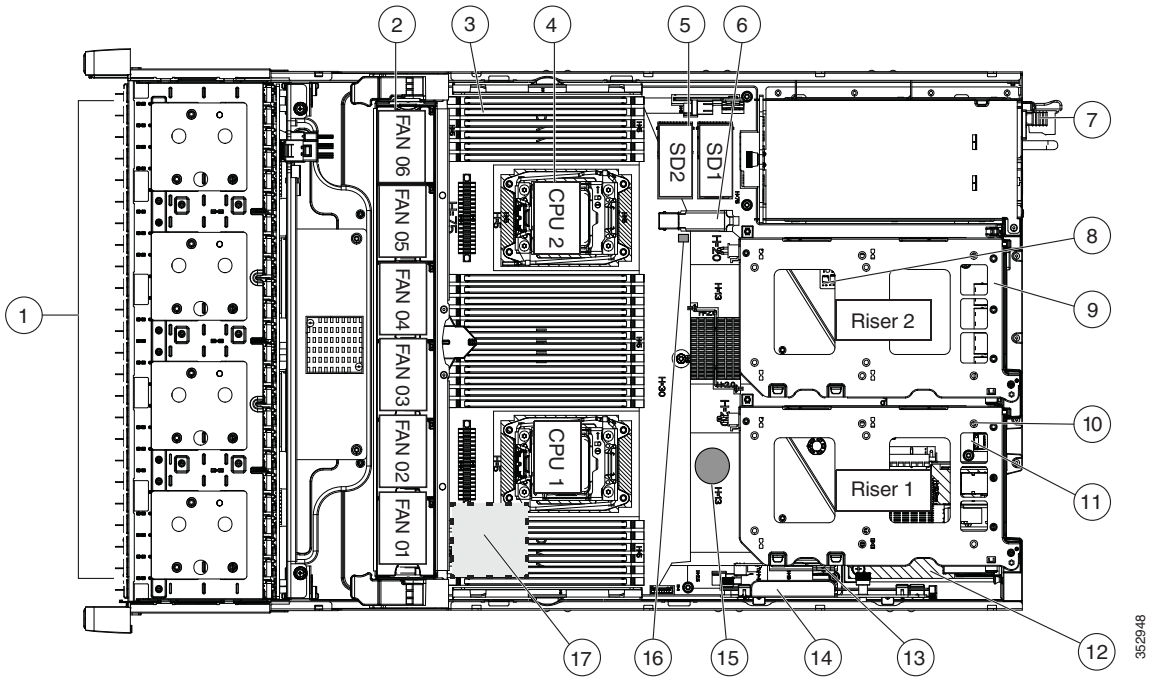
This section describes how to install and replace server components, and it includes the following topics:

- Replaceable Component Locations, page 3-14
- Replacing Hard Drives or Solid State Drives, page 3-15
- Replacing Fan Modules, page 3-18
- Replacing DIMMs, page 3-20
- Replacing CPUs and Heatsinks, page 3-24
- Replacing a SATA Interposer Board, page 3-29
- Replacing a Cisco Modular RAID Controller Card, page 3-31
- Replacing a Modular RAID Controller Transportable Memory Module (TMM), page 3-33
- Replacing the Supercap Power Module (RAID Backup Battery), page 3-35
- Replacing a Software RAID 5 Key Module, page 3-37
- Replacing the Motherboard RTC Battery, page 3-39
- Replacing an Internal SD Card, page 3-40
- Enabling or Disabling the Internal USB Port, page 3-41
- Replacing a PCIe Riser, page 3-42
- Replacing a PCIe Card, page 3-44
- Installing an NVIDIA GPU Card, page 3-53
- Replacing Internal SATA Boot Drives, page 3-57
- Installing a Trusted Platform Module, page 3-59
- Replacing Power Supplies, page 3-62
- Replacing an mLOM Card, page 3-65

Replaceable Component Locations

Figure 3-5 shows the locations of the components that are supported as field-replaceable. The view shown is from the top down, with the top covers and air baffle removed.

Figure 3-5 Replaceable Component Locations



1	Drives (hot-swappable, accessed through front panel)	**10**	PCIe riser 1 (PCIe slots 1, 2, 3*) *Slot 3 not present in all versions. See Replacing a PCIe Card, page 3-44 for riser options and slot specifications.
2	Fan modules (six, hot-swappable)	**11**	SATA boot drives (two sockets, available only on PCIe riser 1 option 1C)
3	DIMM sockets on motherboard (up to 24 DIMMs)	**12**	mLOM card socket on motherboard under PCIe riser 1
4	CPUs and heatsinks (two)	**13**	Socket for embedded RAID interposer board
5	SD card slots on motherboard (two)	**14**	Cisco modular RAID controller PCIe slot (dedicated slot and bracket)
6	USB 3.0 slot on motherboard	**15**	RTC battery on motherboard
7	Power supplies (hot-swappable, accessed through rear panel)	**16**	Embedded RAID header for RAID 5 key
8	Trusted platform module (TPM) socket on motherboard, under PCIe riser 2	**17**	Supercap power module (RAID backup) mounting location on air baffle (not shown)
9	PCIe riser 2 (PCIe slots 4, 5, 6)		

The Technical Specifications Sheets for all versions of this server, which include supported component part numbers, are at Cisco UCS Servers Technical Specifications Sheets.

Replacing Hard Drives or Solid State Drives

This section includes the following information:

- Drive Population Guidelines, page 3-15
- Drive Replacement Procedure, page 3-16

Drive Population Guidelines

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

- Cisco UCS C240 M4—Small form-factor (SFF) drives with 24-drive backplane and expander. This version holds up to 24 2.5-inch hard drives or solid state drives.
- Cisco UCS C240 M4—SFF drives, with 16-drive backplane and integrated expander. This version holds up to 16 2.5-inch hard drives or solid state drives.
- Cisco UCS C240 M4—SFF drives, with 8-drive direct-connect backplane and no expander. This version holds up to 8 2.5-inch hard drives or solid state drives.
- Cisco UCS C240 M4—Large form-factor (LFF) drives, with 12-drive backplane and integrated expander. This version holds up to 12 3.5-inch hard drives.

Note You cannot change the backplane type after-factory. To change a front panel/backplane configuration, a chassis replacement is required.

The drive-bay numbering for all server versions is shown in Figure 3-6 through Figure 3-9.

Figure 3-6 Drive Numbering, SFF Drives, 24-Drive Version

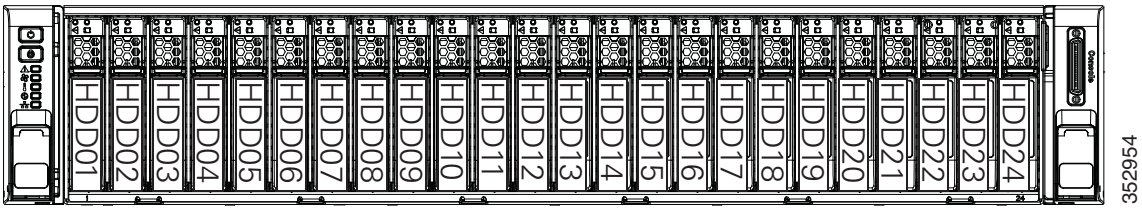


Figure 3-7 Drive Numbering, SFF Drives, 16-Drive Version

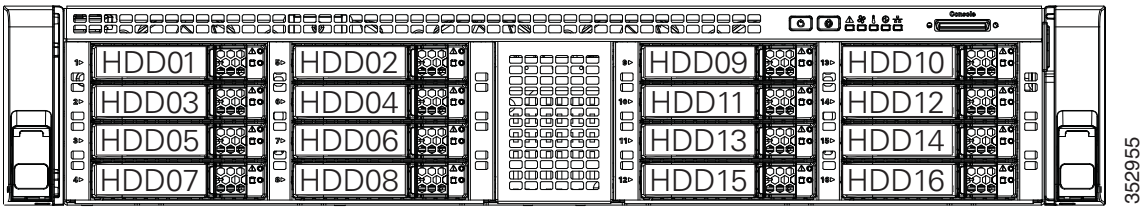


Figure 3-8 Drive Numbering, SFF Drives, 8-Drive Version

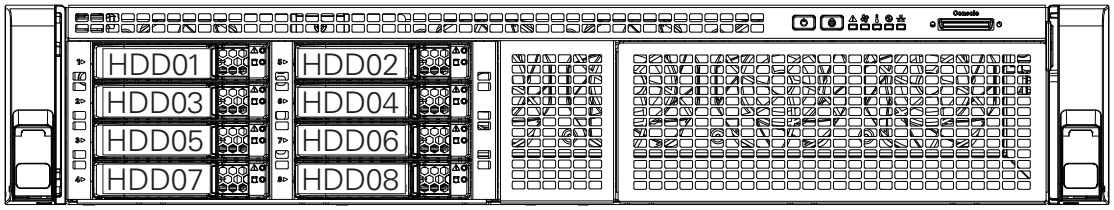
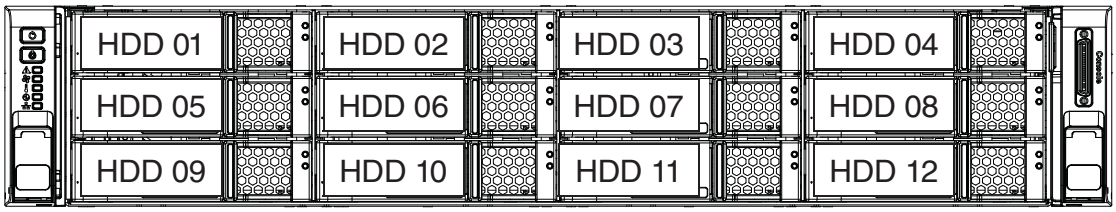


Figure 3-9 Drive Numbering, LFF Drives, 12-Drive Version



Observe these drive population guidelines for optimal performance:

- When populating drives, add drives in the lowest numbered bays first.
- Keep an empty drive blanking tray in any unused bays to ensure optimal airflow 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.

Drive Replacement Procedure

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

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 3-10.

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.

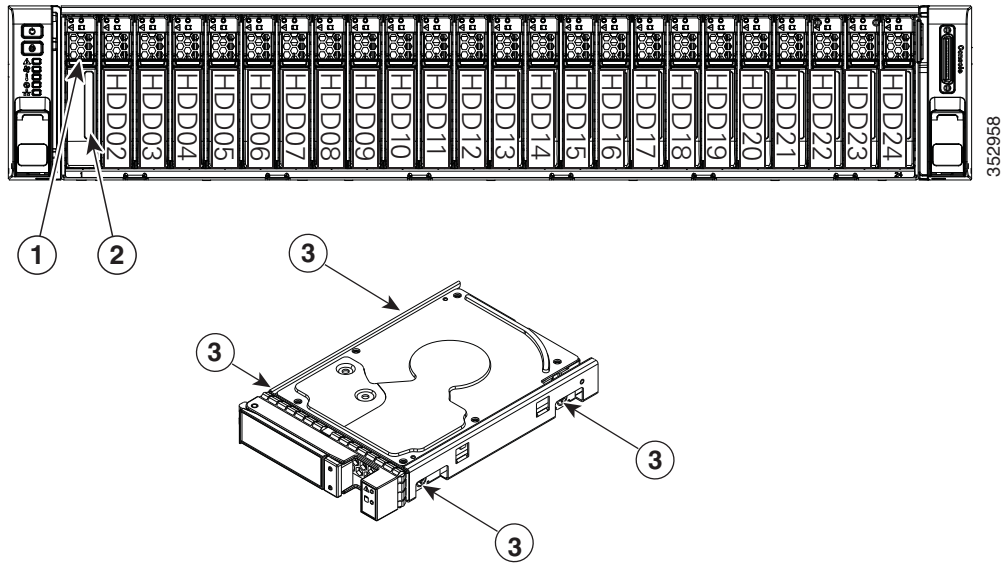
Step 2 Install a new drive:

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, and then close the ejector lever to lock the drive in place.

Figure 3-10 Replacing Drives



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

Replacing Fan Modules

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

Figure 3-11 Fan Module Numbering

FAN 6	FAN 5	FAN 4	FAN 3	FAN 2	FAN 1

Tip A fault LED is on the top of each fan module that lights amber if the fan module fails. To operate these LEDs from the supercap power source, remove AC power cords and then press the Unit Identification button. See also Internal Diagnostic LEDs, page 3-8.

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

Step 1 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 2 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 3 Identify a faulty fan module by looking for a fan fault LED that is lit amber (see Figure 3-12).

Step 4 Remove a fan module that you are replacing (see Figure 3-12):

a. Grasp the top of the fan and pinch the green plastic latch toward the center.

b. Lift straight up to remove the fan module from the server.

Step 5 Install a new fan module:

a. Set the new fan module in place, aligning the connector on the bottom of the fan module with the connector on the motherboard.

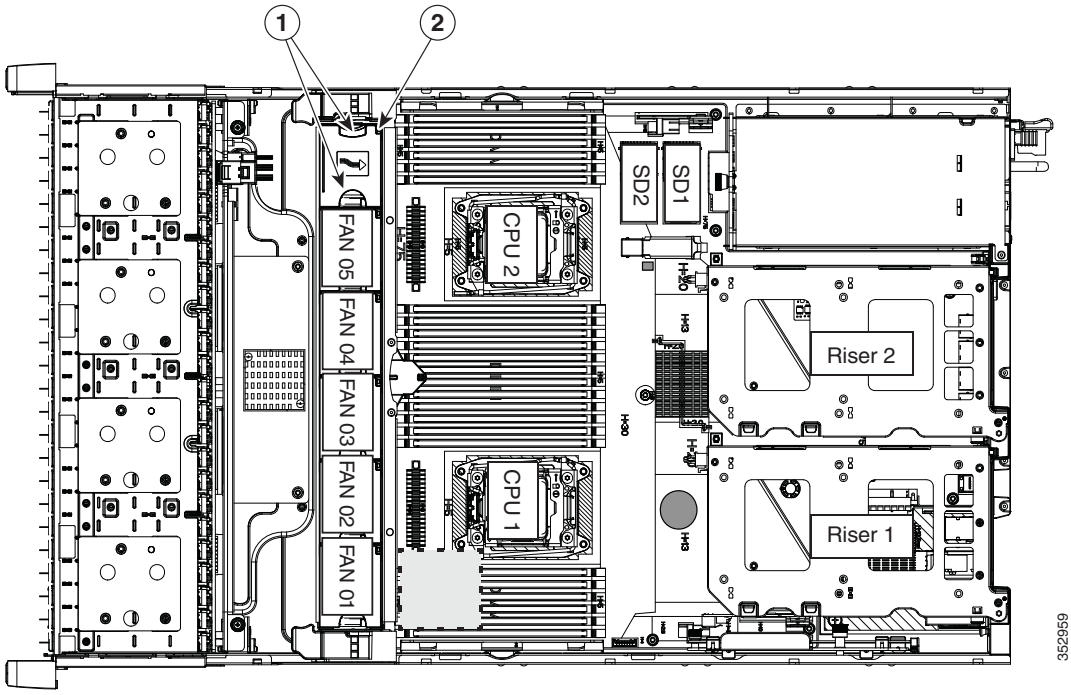
Note The arrow label on the top of the fan module, which indicates the direction of airflow, should point toward the rear of the server.

b. Press down gently on the fan module until the latch clicks and locks in place.

Step 6 Replace the top cover.

Step 7 Replace the server in the rack.

Figure 3-12 Fan Modules Latch and Fault LED



1	Finger latch (on each fan module)	**2**	Fan module fault LED (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 third-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 the memory.

Memory Performance Guidelines and Population Rules

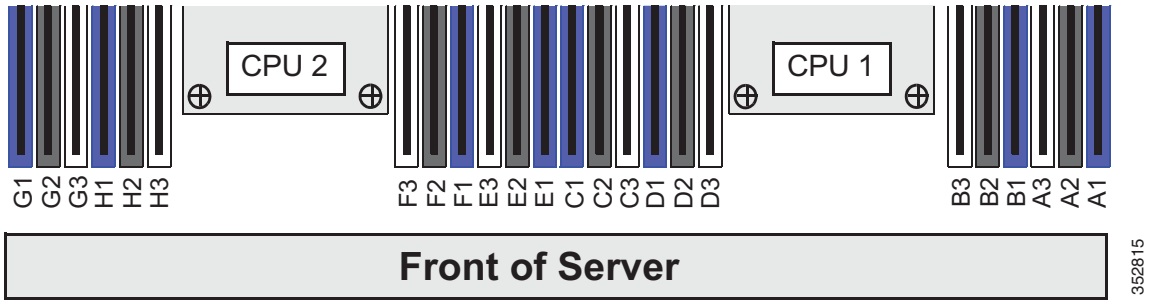
This section describes the type of memory that the server requires and its effect on performance. The section includes the following topics:

- DIMM Socket Numbering, page 3-21
- DIMM Population Rules, page 3-21
- Memory Mirroring and RAS, page 3-22
- Lockstep Channel Mode, page 3-22

DIMM Socket Numbering

Figure 3-13 shows the numbering of the DIMM sockets and CPUs.

Figure 3-13 CPUs and DIMM Socket Numbering on Motherboard



DIMM Population Rules

Observe the following guidelines when installing or replacing DIMMs:

- Each CPU supports four memory channels.
  - CPU1 supports channels A, B, C, and D.
  - CPU2 supports channels E, F, G, and H.
- Each channel has three DIMM sockets (for example, channel A = slots A1, A2, and A3).
  - A channel can operate with one, two, or three DIMMs installed.
  - If a channel has only one DIMM, populate slot 1 first (the blue slot).
- When both CPUs are installed, populate the DIMM sockets of each CPU identically.
  - Fill blue #1 slots in the channels first: A1, E1, B1, F1, C1, G1, D1, H1
  - Fill black #2 slots in the channels second: A2, E2, B2, F2, C2, G2, D2, H2
  - Fill white #3 slots in the channels third: A3, E3, B3, F3, C3, G3, D3, H3
- 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 (A, B, C, D).
- Memory mirroring reduces the amount of memory available by 50 percent because only one of the two populated channels provides data. When memory mirroring is enabled, you must install DIMMs in sets of 4, 6, 8, or 12 as described in Memory Mirroring and RAS, page 3-22.
- Observe the DIMM mixing rules shown in Table 3-5.

Table 3-5 DIMM Mixing Rules for C240 M4 Servers

DIMM Parameter	DIMMs in the Same Channel	DIMMs in the Same Bank
DIMM Capacity: RDIMM = 8 or 16 GB LRDIMM = 32 or 64 GB	• You can mix different capacity DIMMs in the same channel (for example, A1, A2, A3).	• You can mix different capacity DIMMs in the same bank. However, for optimal performance DIMMs in the same bank (for example, A1, B1, C1, D1) should have the same capacity.

Table 3-5 DIMM Mixing Rules for C240 M4 Servers

DIMM Parameter	DIMMs in the Same Channel	DIMMs in the Same Bank
DIMM Speed: 2133 or 2400 MHz	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the channel.	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the bank.
DIMM Type: RDIMMs or LRDIMMs	You cannot mix DIMM types in a channel.	You cannot mix DIMM types in a bank.

Memory Mirroring and RAS

The Intel E5-2600 CPUs within the server support memory mirroring only when an even number of channels are populated with DIMMs. If one or three channels are populated with DIMMs, memory mirroring is automatically disabled. Furthermore, if memory mirroring is used, DRAM size is reduced by 50 percent for reasons of reliability.

For details on populating recommended memory mirroring configurations, see the specification sheet for the server:

- Cisco UCS C240 M4 High Density Rack Server (Small Form-Factor Disk Drive Model) Specification Sheet
- Cisco UCS C240 M4 High Density Rack Server (Large Form-Factor Disk Drive Model) Specification Sheet

Lockstep Channel Mode

When you enable lockstep channel mode, each memory access is a 128-bit data access that spans four channels.

Lockstep channel mode requires that all four memory channels on a CPU must be populated identically with regard to size and organization. DIMM socket populations within a channel (for example, A1, A2, A3) do not have to be identical but the same DIMM slot location across all four channels must be populated the same.

For example, DIMMs in sockets A1, B1, C1, and D1 must be identical. DIMMs in sockets A2, B2, C2, and D2 must be identical. However, the A1-B1-C1-D1 DIMMs do not have to be identical with the A2-B2-C2-D2 DIMMs.

DIMM Replacement Procedure

This section includes the following topics:

- Identifying a Faulty DIMM, page 3-23
- Replacing DIMMs, page 3-23

Identifying a Faulty DIMM

Each DIMM socket has a corresponding DIMM fault LED, directly in front of the DIMM socket. See Figure 3-3 for the locations of these LEDs. The LEDs light amber to indicate a faulty DIMM. To operate these LEDs from the SuperCap power source, remove AC power cords and then press the Unit Identification button.

Replacing DIMMs

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the air baffle that sits over the DIMM sockets and set it aside.

Step 5 Identify the faulty DIMM by observing the DIMM socket fault LEDs on the motherboard (see Figure 3-3).

Step 6 Remove the DIMMs that you are replacing. Open the ejector levers at both ends of the DIMM socket, and then lift the DIMM out of the socket.

Step 7 Install a new DIMM:

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

a. Align the new DIMM with the empty socket on the motherboard. Use the alignment key in the DIMM socket to correctly orient 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.

Step 8 Replace the air baffle.

Step 9 Replace the top cover.

Step 10 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Replacing CPUs and Heatsinks

This section contains the following topics:

- CPU Configuration Rules, page 3-24
- Replacing a CPU and Heatsink, page 3-24
- Additional CPU-Related Parts to Order with RMA Replacement Motherboards, page 3-28

CPU Configuration Rules

This server has two CPU sockets. Each CPU supports four DIMM channels (12 DIMM sockets). See Figure 3-13.

- The server can operate with one CPU or with two identical CPUs installed.
- The minimum configuration is that the server must have at least CPU1 installed. Install CPU1 first, and then CPU2.
- The following restrictions apply when using a single-CPU configuration:
  - The maximum number of DIMMs is 12 (only CPU1 channels A, B, C, and D).
  - PCIe riser 2, which contains PCIe slots 4, 5, and 6 is unavailable.

Replacing a CPU and Heatsink

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 grease to ensure proper cooling. Failure to install a CPU correctly might result in damage to the server.

Note This server uses the new independent loading mechanism (ILM) CPU sockets, so no Pick-and-Place tools are required for CPU handling or installation. Always grasp the plastic frame on the CPU when handling.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the plastic air baffle that sits over the CPUs.

Step 5 Remove the heatsink that you are replacing:

a. Use a Number 2 Phillips-head screwdriver to loosen the four captive screws that secure the heatsink.

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

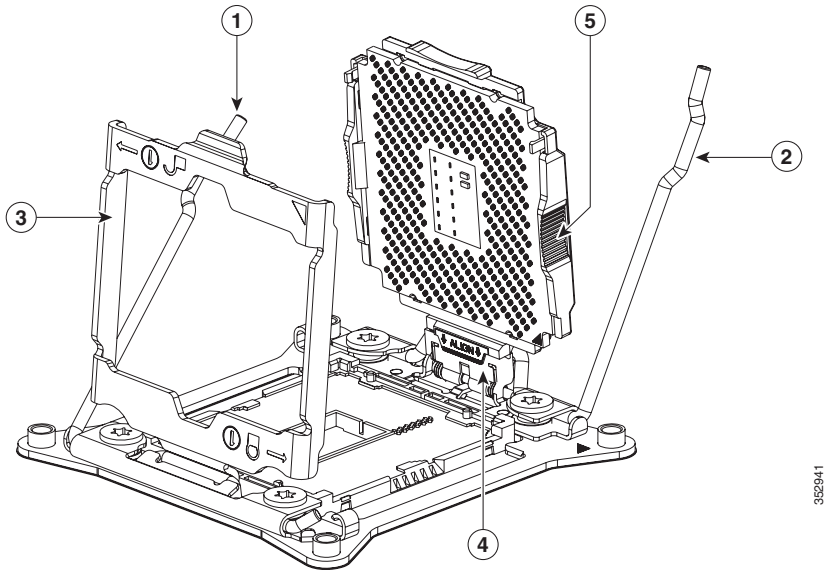
b. Lift the heatsink off of the CPU.

Step 6 Open the CPU retaining mechanism:

a. Unclip the first retaining latch labeled with the icon, and then unclip the second retaining latch labeled with the icon. See Figure 3-14.

b. Open the hinged CPU cover plate.

Figure 3-14 CPU Socket



1	CPU retaining latch	**4**	Hinged CPU seat
2	CPU retaining latch	**5**	Finger-grips on plastic CPU frame
3	Hinged CPU cover plate		

Step 7 Remove any existing CPU:

a. With the latches and hinged CPU cover plate open, swing the CPU in its hinged seat up to the open position, as shown in Figure 3-14.

b. Grasp the CPU by the finger-grips on its plastic frame and lift it up and out of the hinged CPU seat.

c. Set the CPU aside on an antistatic surface.

Step 8 Install a new CPU:

a. Grasp the new CPU by the finger-grips on its plastic frame and align the tab on the frame that is labeled “ALIGN” with the hinged seat, as shown in Figure 3-15.

b. Insert the tab on the CPU frame into the seat until it stops and is held firmly.

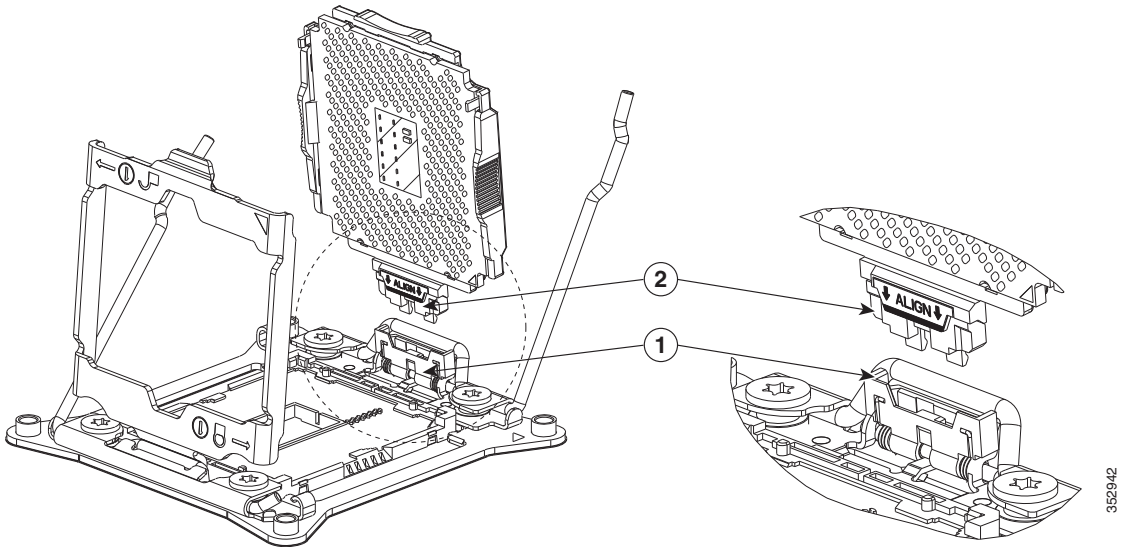
The line below the word “ALIGN” should be level with the edge of the seat, as shown in Figure 3-15.

c. Swing the hinged seat with the CPU down until the CPU frame clicks in place and holds flat in the socket.

d. Close the hinged CPU cover plate.

e. Clip down the CPU retaining latch with the icon, and then clip down the CPU retaining latch with the icon. See Figure 3-14.

Figure 3-15 CPU and Socket Alignment Features



1	SLS mechanism on socket	**2**	Tab on CPU frame (labeled ALIGN)

Step 9 Install a heat sink:

Caution The heat sink must have new thermal grease on the heat sink-to-CPU surface to ensure proper cooling. If you are reusing a heat sink, you must remove the old thermal grease. If you are installing a new heat sink, skip to Step c.

a. Apply the cleaning solution, which is included with the heatsink cleaning kit (shipped with spare CPUs), to the old thermal grease and let it soak for a least 15 seconds.

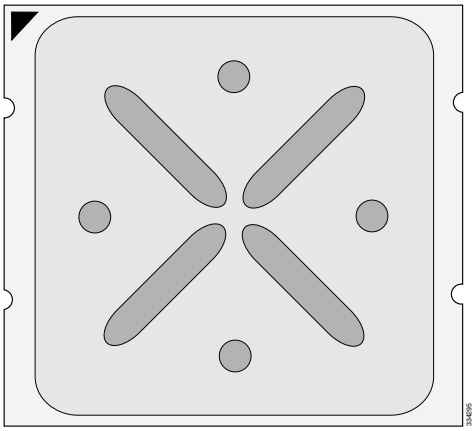
b. Wipe all of the old thermal grease off the old heat sink using the soft cloth that is included with the heatsink cleaning kit. Be careful to not scratch the heat sink surface.

c. Apply thermal grease from the syringe that is included with the new CPU to the top of the CPU.

Apply about half the syringe contents to the top of the CPU in the pattern that is shown in Figure 3-16.

Note If you do not have a syringe of thermal grease, you can order a spare (Cisco PID UCS-CPU-GREASE3=).

Figure 3-16 Thermal Grease Application Pattern



d. Align the four heatsink captive screws with the motherboard standoffs, and 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.

Step 10 Replace the air baffle.

Step 11 Replace the top cover.

Step 12 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

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, additional parts 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.

Note This server uses the new independent loading mechanism (ILM) CPU sockets, so no Pick-and-Place tools are required for CPU handling or installation. Always grasp the plastic frame on the CPU when handling.

- Scenario 1—You are reusing the existing heatsinks:
  - Heat sink cleaning kit (UCSX-HSCK=)
  - Thermal grease kit for C240 M4 (UCS-CPU-GREASE3=)
- Scenario 2—You are replacing the existing heatsinks:
  - Heat sink (UCSC-HS-C240M4=)
  - Heat sink cleaning kit (UCSX-HSCK=)

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 you are ordering new heatsinks, you must order the heatsink cleaning kit.

Replacing a SATA Interposer Board

The server uses a SATA interposer board and cable to connect the embedded RAID (PCH SATA) controller on the motherboard to the drive backplane. See Figure 3-17 for the socket location.

Note The SATA interposer board and embedded RAID can be used only with the SFF, 8-drive backplane version of the server. It does not operate with an expander. You cannot use the embedded RAID controller and a hardware RAID controller card at the same time.

See Embedded SATA RAID Controller, page C-9 for more information about using the embedded RAID controller and options.

Step 1 Power off the server as described in the Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the plastic air baffle that sits over the CPUs to gain access to the interposer cables.

Step 5 Remove PCIe riser 1 from the server to provide clearance. See Replacing a PCIe Riser, page 3-42.

Step 6 Remove any existing PCH SATA interposer board:

- **a.** Disconnect both cable connectors from the interposer board.
- **b.** Lift straight up on the board to remove it from its motherboard socket.

Step 7 Install a new interposer board and cables:

Note The required Y-cable and SATA interposer board are bundled as `UCSC-IP-PCH-C240M4=`.

- **a.** Align the board with the socket, and then gently press down on both top corners to seat it evenly.
- **b.** Connect the single mini-SAS HD cable connector to the single connector on the backplane.
- **c.** Route the cables through the plastic clips on the chassis wall.
- **d.** Connect PORT A and PORT B cable connectors to their corresponding connectors on the new interposer board.

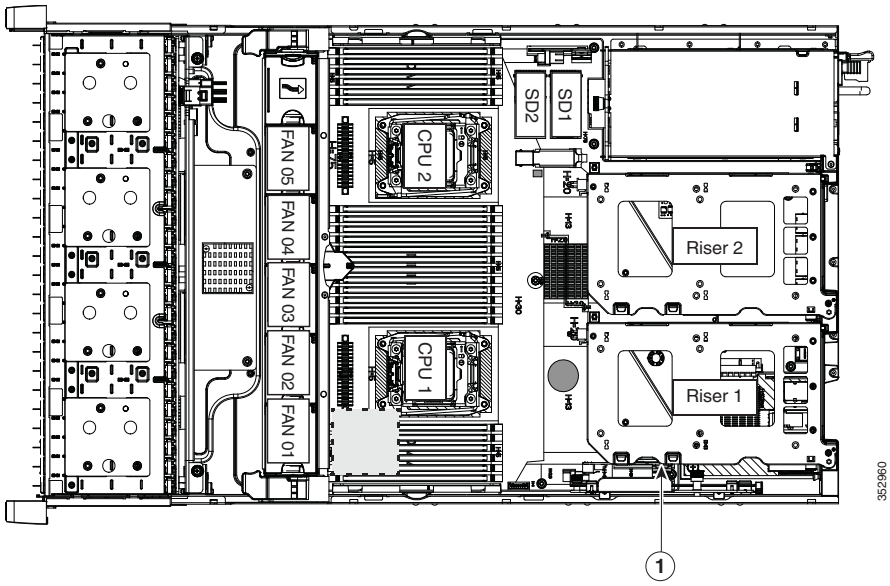
Step 8 Replace PCIe riser 1 to the server.

Step 9 Replace the air baffle.

Step 10 Replace the top cover.

Step 11 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-17 SATA Interposer Board Socket Location



1	SATA interposer board socket on motherboard		

Replacing a Cisco Modular RAID Controller Card

The server has an internal, dedicated PCIe slot on the motherboard for a Cisco modular RAID controller card (see Figure 3-18).

See also:

- Replacing a Modular RAID Controller Transportable Memory Module (TMM), page 3-33
- Replacing the Supercap Power Module (RAID Backup Battery), page 3-35

Note You cannot use a hardware RAID controller card and the embedded RAID controller at the same time. See RAID Controller Considerations, page C-1 for details about RAID support.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove an existing RAID controller card:

a. Disconnect the data cable from the card. Depress the tab on the cable connector and pull.

b. Disconnect the supercap power module cable from the transportable memory module (TMM), if present.

c. Lift straight up on the metal bracket that holds the card. The bracket lifts off of two pegs on the chassis wall.

d. Loosen the two thumbscrews that hold the card to the metal bracket and then lift the card from the bracket.

Step 5 Install a new RAID controller card:

a. Set the new card on the metal bracket, aligned so that the thumbscrews on the card enter the threaded standoffs on the bracket. Tighten the thumbscrews to secure the card to the bracket.

b. Align the two slots on the back of the bracket with the two pegs on the chassis wall.

   The two slots on the bracket must slide down over the pegs at the same time that you push the card into the motherboard socket.

c. Gently press down on both top corners of the metal bracket to seat the card into the socket on the motherboard.

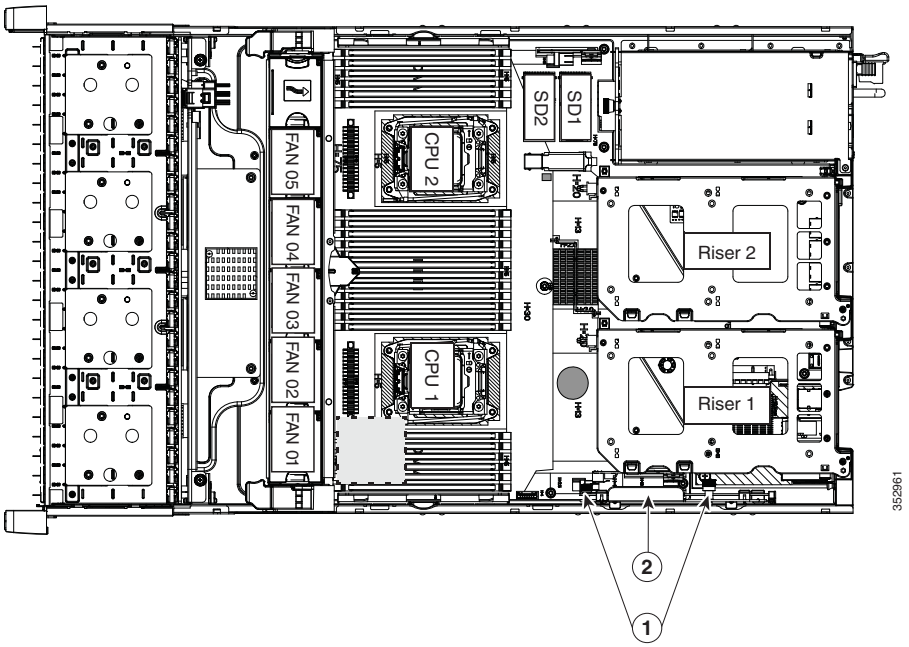
d. Connect the supercap power module cable to its connector on the TMM, if present.

e. Connect the single data cable to the card.

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-18 Modular RAID Controller Card Location



1	Thumbscrews on card	**2**	Cisco modular RAID controller bracket

Replacing a Modular RAID Controller Transportable Memory Module (TMM)

The transportable memory module (TMM) that attaches to the modular RAID controller card can be installed or replaced after-factory.

See also:

- Replacing a Cisco Modular RAID Controller Card, page 3-31
- Replacing the Supercap Power Module (RAID Backup Battery), page 3-35

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the modular RAID controller card from the server:

a. Lift straight up on the metal bracket that holds the card. The bracket lifts off of two pegs on the chassis wall (see Figure 3-18).

b. Disconnect the supercap power module cable from the TMM that is attached to the card.

Step 5 Remove the TMM from the modular RAID controller card (see Figure 3-19):

a. The plastic bracket on the card has a securing plastic clip at each end of the TMM. Gently spread each clip away from the TMM.

b. Pull straight up on the TMM to lift it off the two plastic guide pegs and the socket on the card.

Step 6 Install a TMM to the modular RAID controller card (see Figure 3-19):

a. Align the TMM over the bracket on the card. Align the connector on the underside of the TMM with the socket on the card. Align the two guide holes on the TMM over the two guide pegs on the card.

Caution In the next step, keep the TMM level and parallel with the surface of the card to avoid damaging the connector or socket.

b. Gently lower the TMM so that the guide holes on the TMM go over the guide pegs on the card.

c. Press down on the TMM until the plastic clips on the bracket close over each end of the TMM.

d. Press down on the TMM to fully seat its connector with the socket on the card.

Step 7 Install the modular RAID controller card back into the server:

Note If this is a first-time installation of your TMM, you must also install a supercap power module (SCPM). The SCPM cable attaches to a connector on the TMM. See Replacing the Supercap Power Module (RAID Backup Battery), page 3-35.

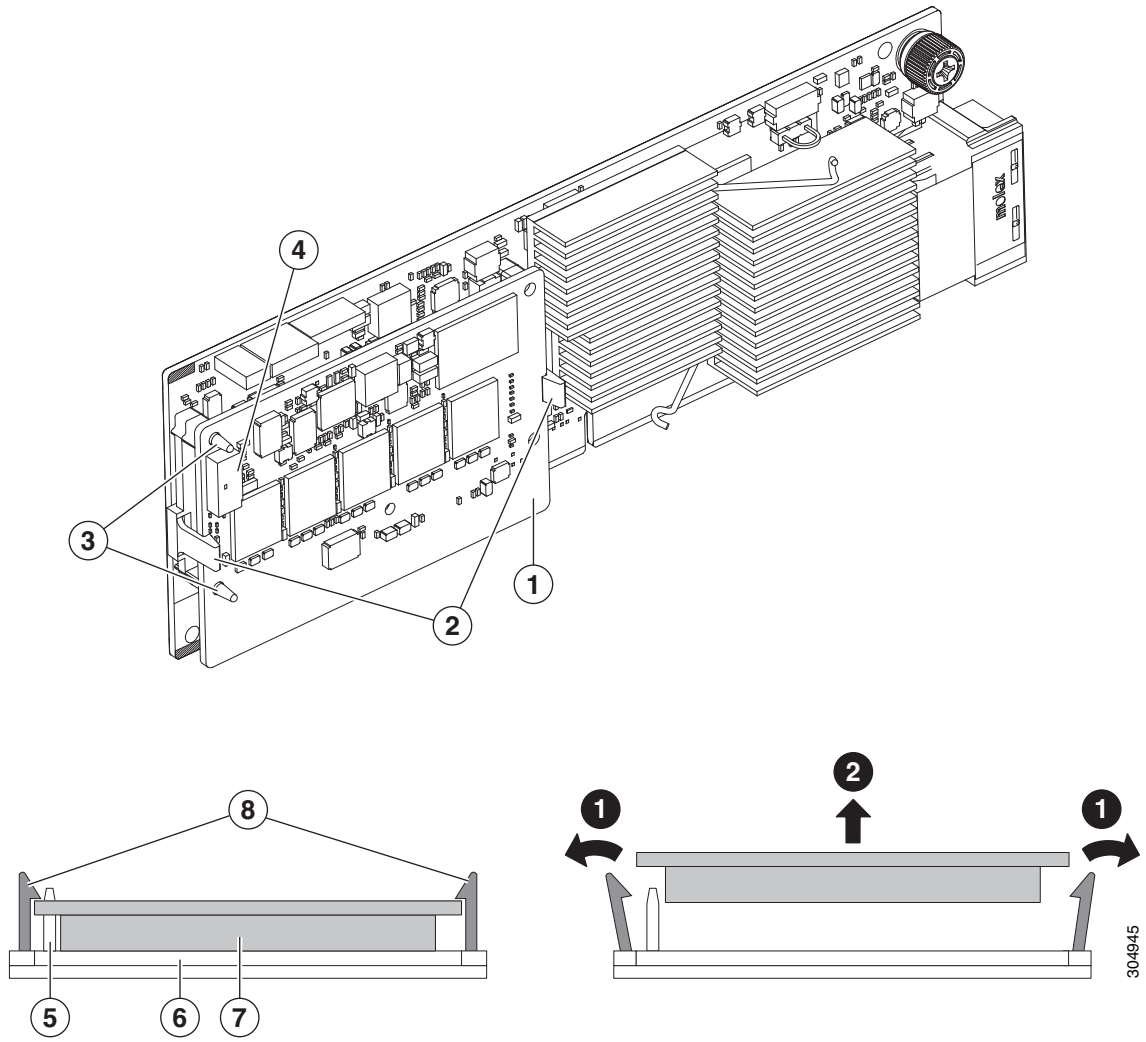
a. Connect the cable from the supercap power module (RAID battery) to the connector on the TMM (see Figure 3-19).

b. Align the two slots on the back of the RAID card bracket with the two pegs on the chassis wall.

The two slots on the bracket must slide down over the pegs at the same time that you push the card into the motherboard socket.

c. Gently press down on both top corners of the metal bracket to seat the card into the socket on the motherboard.

Figure 3-19 TMM on Modular RAID Controller Card



1	TMM on modular RAID card	**5**	Side view, guide peg
2	Securing bracket clips	**6**	Side view, socket on modular RAID card
3	Guide pegs on bracket protruding through guide holes on TMM	**7**	Side view, connector on underside of TMM
4	SCPM cable connector on TMM	**8**	Side view, securing clips

Replacing the Supercap Power Module (RAID Backup Battery)

This server supports installation of one supercap power module (SCPM). The unit mounts to a clip on the removable air baffle (see Figure 3-20). The SCPM requires that you have a transportable memory module (TMM) attached to your RAID controller card because the connector for the SCPM cable is on the TMM.

See also:

- Replacing a Cisco Modular RAID Controller Card, page 3-31
- Replacing a Modular RAID Controller Transportable Memory Module (TMM), page 3-33

The SCPM provides approximately three years of backup for the disk write-back cache DRAM in the case of a sudden power loss by offloading the cache to the NAND flash.

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

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove an existing SCPM:

a. Disconnect the existing SCPM cable from the transportable memory module (TMM) that is attached to the modular RAID controller card.

b. Pull back the plastic clip that closes over the SCPM slightly, and then slide the SCPM free of the clips on the air baffle mounting point (see Figure 3-20).

Step 5 Install a new SCPM:

a. Slide the new backup unit into the holder on the air baffle mounting point until the clip clicks over the top edge of the SCPM.

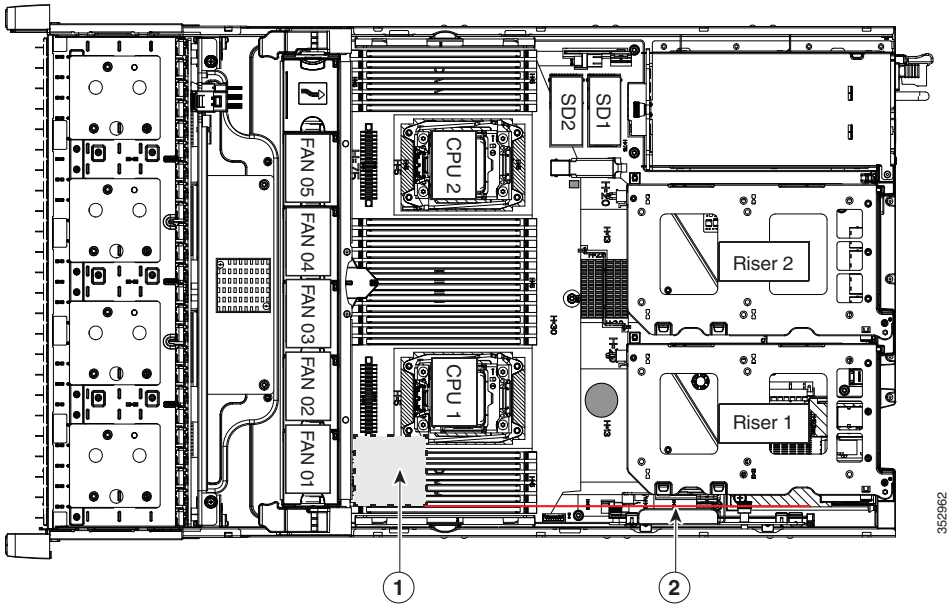
b. Connect the cable from the SCPM to the TMM that is attached to the modular RAID controller card.

Note Put the cable through the opening on the rear of the air baffle (rather than over the air baffle) to keep the cable from interfering with the top cover of the server.

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-20 SCPM (RAID Backup Unit) Mounting Point and Cable Path



1	SCPM mounting point on removable air baffle (air baffle not shown)	**2**	SCPM cable routing path (the red line)

Replacing a Software RAID 5 Key Module

The server has a two-pin header on the motherboard for a RAID 5 key module. This module upgrades the embedded SATA RAID controller options (see Embedded SATA RAID Controller, page C-9).

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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.

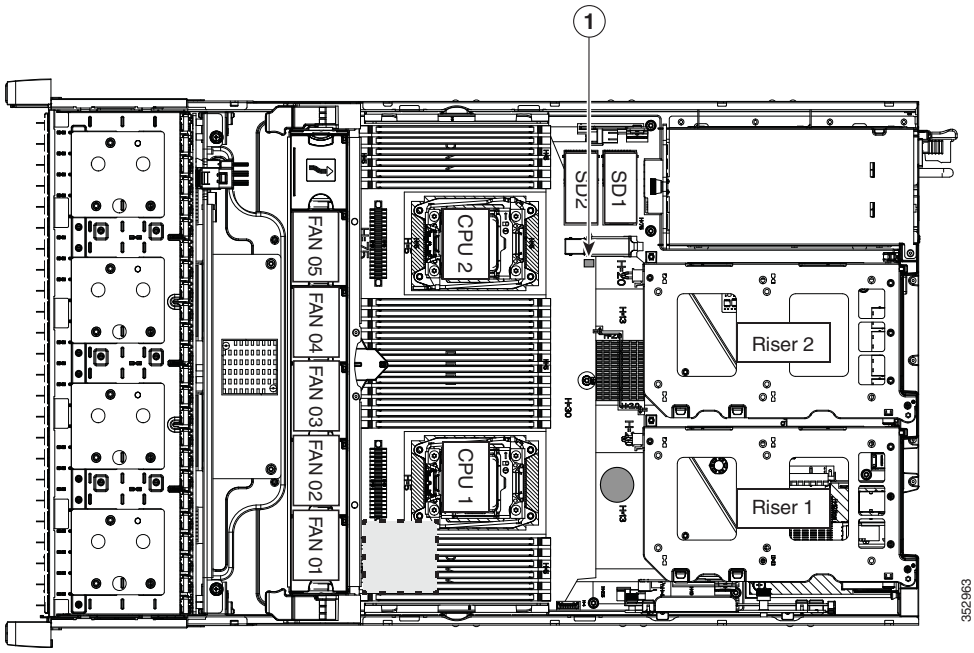
Step 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove any existing software RAID key module:

a. Locate the module on the motherboard (see Figure 3-21).

b. Hold the retention clips on the header open while you grasp the RAID key board and pull straight up (see Figure 3-22).

Figure 3-21 RAID 5 Key Header Location on Motherboard



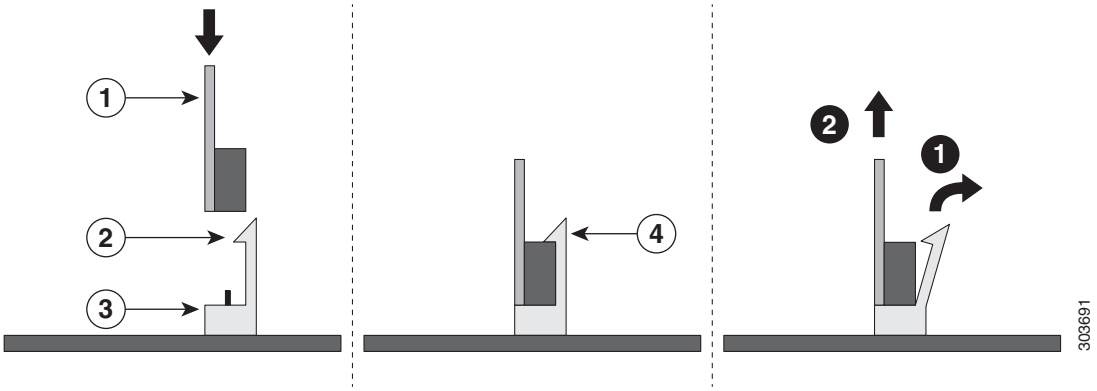
1	Software RAID 5 key header (adds RAID 5 support)		

Step 5 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 (see Figure 3-22).

Figure 3-22 Software RAID 5 Key Module Retention Clip



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

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 RTC battery is on the motherboard near the RAID controller card socket (see Figure 3-23).

The battery type is Panasonic CR2032 or equivalent.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the battery from its holder on the motherboard (see Figure 3-23):

- **a.** Use a small screwdriver or pointed object to press inward on the battery at the prying point (see Figure 3-23).
- **b.** Lift up on the battery and remove it from the holder.

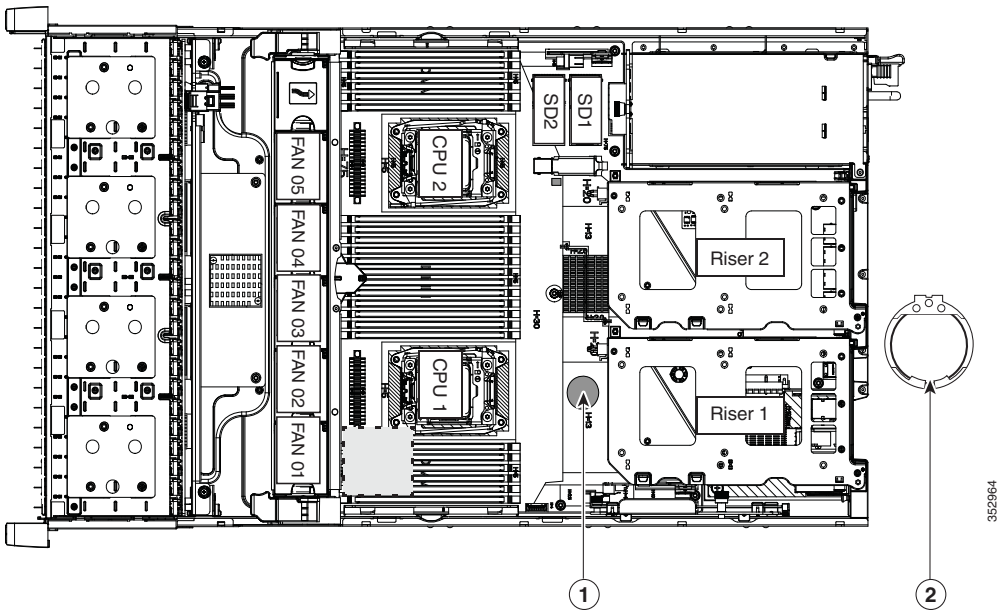
Step 5 Install an RTC battery. Insert the battery into its holder and press down until it clicks in place.

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

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and power on the server by pressing the **Power** button.

Figure 3-23 RTC Battery Location and Prying Point



1	RTC battery holder on motherboard	2	Prying point

Replacing an Internal SD Card

The server has two internal SD card bays on the motherboard.

Dual SD cards are supported. RAID 1 support can be configured through the Cisco IMC interface.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove an SD card (see Figure 3-24).

- **a.** Push on the top of the SD card, and then release it to allow it to spring out from the slot.
- **b.** Remove the SD card from the slot.

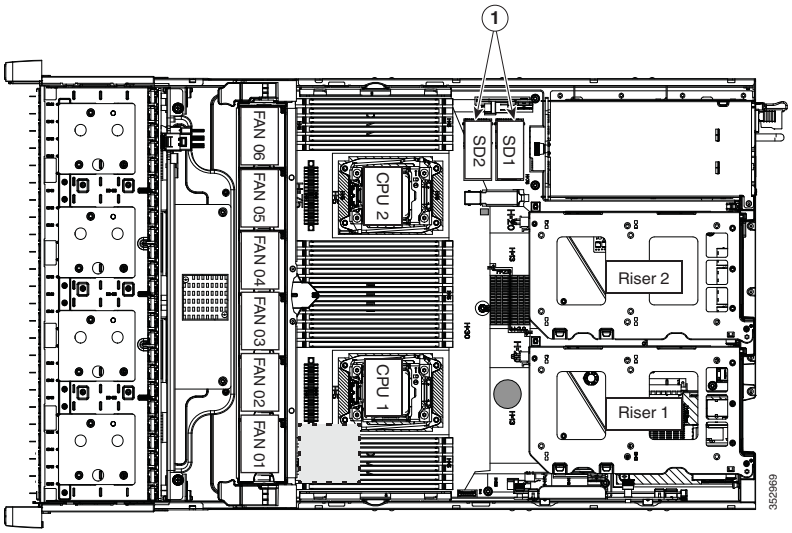
Step 5 Install an SD card:

- **a.** Insert the SD card into the slot with the label side facing up.
- **b.** Press on the top of the card until it clicks in the slot and stays in place.

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-24 SD Card Bay Location and Numbering on the Motherboard



1	SD card bays SD1 and SD2		

Enabling or Disabling the Internal USB Port

Caution We do not recommend that you Hot-swap the internal USB drive while the server is powered on.

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. See Figure 3-5 for the location of the internal USB 3.0 slot on the motherboard.

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, choose **USB Ports Configuration**.

Step 5 Scroll to **USB Port: Internal**, press **Enter**, and then choose either **Enabled** or **Disabled** from the dialog box.

Step 6 Press **F10** to save and exit the utility.

Replacing a PCIe Riser

The server contains two toolless PCIe risers for horizontal installation of PCIe cards. See Replacing a PCIe Card, page 3-44 for the specifications of the PCIe slots on the risers.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the PCIe riser that you are replacing (see Figure 3-25):

- **a.** Grasp the top of the riser and lift straight up on both ends to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic mat.
- **b.** If the riser has a card installed, remove the card from the riser. See Replacing a PCIe Card, page 3-44.

Step 5 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 3-44).
- **b.** Position the PCIe riser over its socket on the motherboard and over its alignment slots in the chassis (see Figure 3-25). There are also two alignment pegs on the motherboard for each riser.

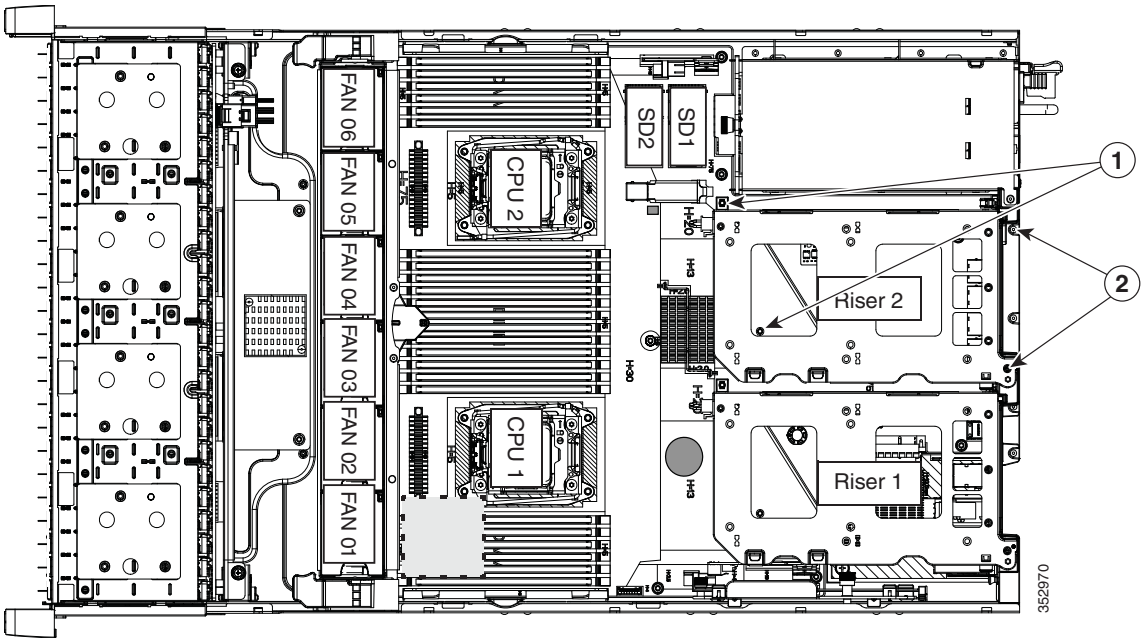
Note The PCIe risers are not interchangeable. If you plug a PCIe riser into the wrong socket, the server will not boot. Riser 1 must plug into the motherboard socket labeled “RISER1.” Riser 2 must plug into the motherboard socket labeled “RISER2.”

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

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-25 PCIe Riser Alignment Features



1	Alignment peg locations on motherboard (two for each riser)	2	Alignment channel locations on chassis (two for each riser)

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 3-44
- Replacing a PCIe Card, page 3-46
- Special Considerations for Cisco UCS Virtual Interface Cards, page 3-48
- Special Considerations for Cisco UCS Fusion ioDrive3 Storage Accelerator Cards, page 3-49
- Installing Multiple PCIe Cards and Resolving Limited Resources, page 3-51

PCIe Slots

The server contains two toolless PCIe risers for horizontal installation of PCIe cards (see Figure 3-26).

- Riser 1 can be ordered as one of three different versions.
  - Version 1: Two slots (PCIE 1 and 2) and a blank to accommodate a GPU card in slot 2. See Table 3-6.
  - Version 2: Three slots (PCIE 1, 2, and 3). See Table 3-7.
  - Version 3: Two slots (PCIE 1 and 2) and two SATA boot-drive sockets. See Table 3-8.
- Riser 2 contains slots PCIE 4, 5, and 6. See Table 3-9.

Figure 3-26 Rear Panel, Showing PCIe Slots

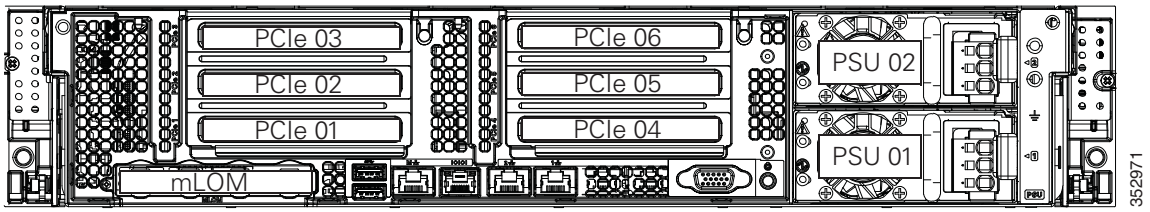


Table 3-6 Riser 1A (UCSC-PCI-1A-240M4) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Card Length[1]	Card Height [2]	NCSI[3] Support
1	Gen-3 x8	x24 connector	3/4 length	Full height	Yes[4]
2	Gen-3 x16	x24 connector	Full length	Full height	Yes
Blank	NA	NA	NA	NA	NA

1. This is the supported length because of internal clearance.
2. This is the size of the rear-panel opening.
3. NCSI = Network Communications Services Interface protocol
4. NCSI is supported in only one slot at a time in this riser version. If a GPU card is present in slot 2, NCSI support automatically moves to slot 1.

Table 3-7 Riser 1B[1] (UCSC-PCI-1B-240M4) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Card Length	Card Height	NCSI Support
1	Gen-3 x8	x16 connector	3/4 length	Full height	No
2	Gen-3 x8	x24 connector	Full length	Full height	Yes
3	Gen-3 x8	x16 connector	Full length	Full height	No

1. GPU cards are not supported in this riser 1B version. There is no GPU power connector in this version. Use riser version 1A or 1C for GPU cards.

Table 3-8 Riser 1C (UCSC-PCI-1C-240M4) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Card Length	Card Height	NCSI Support
1	Gen-3 x8	x16 connector	3/4 length	Full height	Yes
2	Gen-3 x16	x24 connector	Full length	Full height	Yes
SATA boot-drive sockets (two)	NA	NA	NA	NA	NA

Table 3-9 Riser 2 (UCSC-PCI-2-240M4) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Card Length	Card Height	NCSI Support
4	Gen-3 x8	x24 connector	3/4 length	Full height	Yes
5	Gen-3 x16	x24 connector	Full length	Full height	Yes[1]
6	Gen-3 x8	x16 connector	Full length	Full height	No

1. NCSI is supported in only one slot at a time in this riser version. If a GPU card is present in slot 5, NCSI support automatically moves to slot 4.

Replacing a PCIe Card

The Technical Specifications Sheets for all versions of this server, which include supported component part numbers, are at Cisco UCS Servers Technical Specifications Sheets.

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 3-48.

Note If you are installing a Fusion ioDrive2 card, there are prerequisite considerations. See Special Considerations for Cisco UCS Fusion ioDrive3 Storage Accelerator Cards, page 3-49.

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

Step 1 Shut down and power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove a PCIe card (or a blanking panel) from the PCIe riser:

- **a.** Lift straight up on both ends of the riser to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic mat.
- **b.** On the bottom of the riser, loosen the single thumbscrew that holds the securing plate (see Figure 3-27).
- **c.** Swing open the securing plate and remove it from the riser to provide access.
- **d.** Swing open the card-tab retainer that secures the back-panel tab of the card (see Figure 3-27).
- **e.** Pull evenly on both ends of the PCIe card to disengage it from the socket on the PCIe riser (or remove a blanking panel) and then set the card aside.

Step 5 Install a PCIe card:

- **a.** Align the new PCIe card with the empty socket on the PCIe 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 PCIe riser rear panel opening.
- **c.** Close the card-tab retainer (see Figure 3-27).
- **d.** Return the securing plate to the riser. Insert the two hinge-tabs into the two slots on the riser, and then swing the securing plate closed.
- **e.** Tighten the single thumbscrew on the bottom of the securing plate.
- **f.** Position the PCIe riser over its socket on the motherboard and over its alignment features in the chassis (see Figure 3-25).

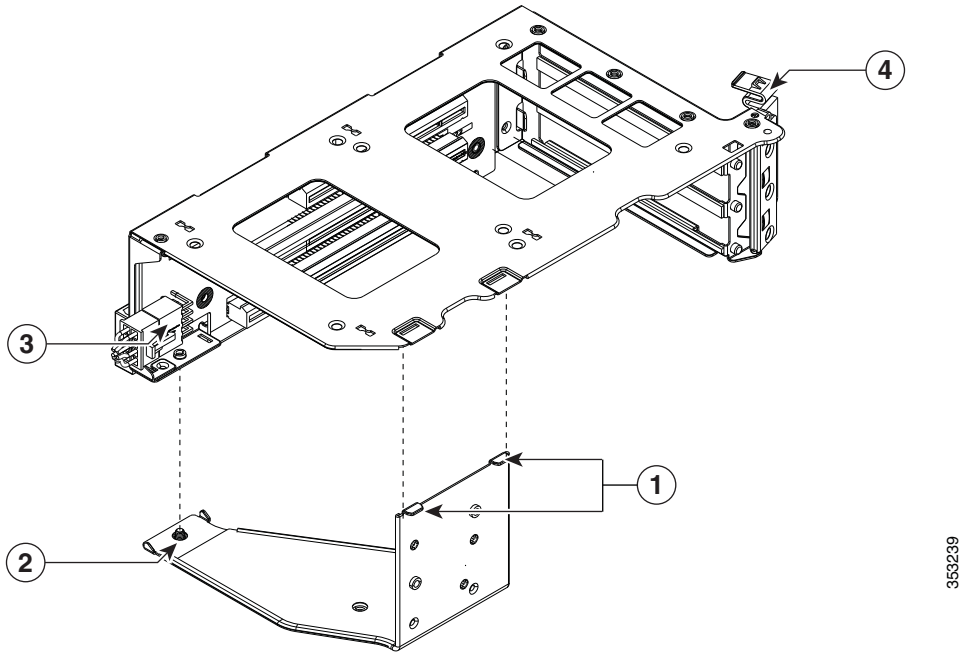
g. Carefully push down on both ends of the PCIe riser to fully engage its circuit board connector with the socket on the motherboard.

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Step 8 If you replaced a RAID controller card, continue with Restoring RAID Configuration After Replacing a RAID Controller, page C-22.

Figure 3-27 PCIe Riser Securing Features (Three-Slot Riser Shown)



1	Securing plate hinge-tabs	**3**	GPU card power connector
2	Securing plate thumbscrew (knob not visible on underside of plate)	**4**	Card-tab retainer in open position

Special Considerations for Cisco UCS Virtual Interface Cards

Table 3-10 describes the requirements for the supported Cisco UCS virtual interface cards (VICs).

The server can support up to two PCIe-style VICs plus one mLOM-style VIC.

Note If you use the Cisco Card NIC mode, you must also make a VIC Slot setting that matches where your VIC is installed. The options are Riser1, Riser2, or Flex-LOM. See NIC Modes and NIC Redundancy Settings, page 2-14.

If you want to use the Cisco UCS VIC card for Cisco UCS Manager integration, also see the Cisco UCS C-Series Server Integration with UCS Manager Guides for details about supported configurations, cabling, and other requirements.

Table 3-10 Cisco UCS C240 M4 Requirements for Virtual Interface Cards

Virtual Interface Card (VIC)	Number of this VIC Supported in Server	Slots That Support VICs	Primary Slot for Cisco UCS Manager Integration	Primary Slot for Cisco Card NIC Mode	Minimum Cisco IMC Firmware	Minimum VIC Firmware
Cisco UCS VIC1225 UCSC-PCIE-CSC-02	4 PCIe	PCIE 2 PCIE 1 PCIE 5 PCIE 4 See footnote[1]	Riser 1: PCIE 2 See footnote.[2]	Riser 1: PCIE 2 Riser 2: PCIE 5	1.4(6)	2.1(0)
Cisco UCS VIC1225T UCSC-PCIE-C10T-02	4 PCIe		Riser 1: PCIE 2 See footnote.[3]	Riser 1: PCIE 2 Riser 2: PCIE 5	1.5(1)	2.1(1)
Cisco UCS VIC1385[4] UCSC-PCIE-C40Q-03	2 PCIe		Not supported at this time	Riser 1: PCIE 2 Riser 2: PCIE 5	2.0(4)	4.0(4b)
Cisco UCS VIC 1227 UCSC-MLOM-CSC-02	1 mLOM	mLOM	mLOM	mLOM	2.0(3)	4.0(0)
Cisco UCS VIC 1227T UCSC-MLOM-C10T-02	1 mLOM	mLOM	mLOM	mLOM	2.0(4)	4.0(4b)

1. For riser PID UCSC-PCI-1B-240M4: slot 2 is the only slot that supports a VIC in riser version 1B. In this riser version, slot 2 is an 8x lane, so if you are using Cisco UCS VIC1385, give it priority on slot 5 instead for best performance.
2. Although all slots support standby power, we recommend that you use an mLOM card for Cisco UCS Manager integration. Slot 2 is the primary PCIe slot for integration, but if an mLOM-style card is present it takes priority over the PCIe slot for integration.
3. Although all slots support standby power, we recommend that you use an mLOM card for Cisco UCS Manager integration. Slot 2 is the primary PCIe slot for integration, but if an mLOM-style card is present it takes priority over the PCIe slot for integration.
4. For Cisco UCS VIC1385, always use the primary slots 2 and 5 for optimal performance. You can use the other supported slots, but you might see degraded performance. If multiple VIC cards are present, give the Cisco UCS VIC1385 priority on the primary slots 2 and 5 for best performance.

Note The Cisco UCS VIC 1227 (UCSC-MLOM-CSC-02) is not compatible to use in *Cisco Card* NIC mode with a certain Cisco SFP+ module. Do not use a Cisco SFP+ module part number 37-0961-01 that has a serial number in the range MOC1238*xxxx* to MOC1309*xxxx*. If you use the Cisco UCS VIC 1227 in Cisco Card NIC mode, use a different part number Cisco SFP+ module, or you can use this part number 37-0961-01 if the serial number is *not* included in the range above. See the data sheet for this adapter for other supported SFP+ modules: Cisco UCS VIC 1227 Data Sheet

Special Considerations for Cisco UCS Fusion ioDrive3 Storage Accelerator Cards

Table 3-11 describes the requirements for the supported Cisco UCS Fusion ioDrive3 cards.

Table 3-11 Cisco UCS C240 M4 Requirements for Fusion ioDrive2 Cards

Card	Maximum Number of Cards Supported	Slots That Support These Cards	Slots That Support >25W Power Override	Minimum Cisco IMC Firmware	Card Height (rear-panel tab)
Cisco UCS 5800 GB MLC Fusion ioDrive3 UCSC-F-FIO-5800M=	6[1]	All	All[2]	2.0(2)	Full height
Cisco UCS 2900 GB MLC Fusion ioDrive3 UCSC-F-FIO-2900M=	6	All	Not applicable	2.0(2)	Half height[3]
Cisco UCS 1450 GB MLC Fusion ioDrive3 UCSC-F-FIO-1450M=	6	All	Not applicable	2.0(2)	Half height
Cisco UCS 1150 GB MLC Fusion ioDrive3 UCSC-F-FIO-1150M=	6	All	Not applicable	2.0(2)	Half height

1. PCIe riser 1 versions UCSC-PCI-1A-240M4 and UCSC-PCI-1C-240M4 have only two slots and therefore, when using those versions only five cards are supported in the server.
2. All slots can be enabled to provide more than the default 25 W power draw for higher performance on some cards. See Enabling Higher Power-Draw for Fusion ioDrive3 Cards, page 3-49.
3. A rear-panel tab adapter is required to fit the half-height cards in full-height slots.

Enabling Higher Power-Draw for Fusion ioDrive3 Cards

Some Fusion ioDrive3 accelerator cards such as the 5800 GB card draw 25 W by default but can achieve higher performance when the PCIe slot is configured to provide more than 25 W for the device.

PCIe Slots That Can Be Configured to Support More Than 25 W Power Draw: All.

All slots can support the higher device power draw of 55 W (75 W maximum) when configured with the override parameter in the IO Accelerator VSL software.

Note See the UCS power calculator to determine the total power draw for your exact server configuration at http://www.cisco.com/assets/cdc_content_elements/flash/dataCenter/cisco_ucs_power_calculator/

How to Enable Higher Power Draw for a Device with the IO Accelerator Override Parameter

The override parameter in the IO Accelerator VSL software (in the `/usr/modprove.d/iomemory-vsl.conf` file) overrides the setting that prevents devices from drawing more than 25 W from the PCIe slot. The parameter is enabled by device, by using the device serial numbers.

Note The override parameter persists in the server and enables full power draw on an enabled device even if the device is removed and then placed in a different slot within the same system. If the device is moved to a slot that is not rated to provide 55 W of power, the server hardware could experience a power drag.

Note The override parameter is a setting for the IO Accelerator VSL software by server and is not stored in the device. When moved to a new server, the device defaults to the 25 W power limit until an external power cable is added or the override parameter is enabled for that device in the new server.

Step 1 Determine the serial number of the installed Fusion device by using the `fio-status` command in the IO Accelerator VSL software. Sample output is shown here:

```
fio-status
Adapter: Dual Controller Adapter
Fusion-io ioDrive2 3.0TB, Product Number:F01-001-2T41-CS-0001, FIO SN:1149D0969
External Power: NOT connected
PCIe Power limit threshold: 24.75W
Connected ioMemory modules:
fct2: SN:1149D0969-1121
fct3: SN:1149D0969-1111
```

In this example, 1149D0969 is the adapter serial number. If you have multiple Fusion ioDrive3 devices installed in your system, use the `fio-beacon` command to verify where each device is physically located.

Note There is also a serial number label on the card, but we recommend that you use the `fio-status` command to confirm the serial number is an adapter serial number (FIO SN in the sample output above).

Step 2 Set the override parameter by editing the `/usr/modprove.d/iomemory-vsl.conf` file, which is installed when you install the device drivers.

Change the value for the `external_power_override` parameter, where the *<value>* for this parameter is a comma-separated list of adapter serial numbers.

```
options iomemory-vsl external_power_override=<value>
```

For example:

```
options iomemory-vsl external_power_override=1149D0969,1159E0972
```

Step 3 Reboot the server or unload and then load the drivers to enforce the parameter changes.

Installing Multiple PCIe Cards and Resolving Limited Resources

When a large number of PCIe add-on cards are installed in the server, the system might 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 3-51
- Resolving Insufficient 16-Bit I/O Space, page 3-52

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, and so on).

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 Cisco IMC 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 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 Cisco IMC Web UI 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.

Installing an NVIDIA GPU Card

This section contains the following topics:

- Overview of Software Requirements, page 3-53
- GPU Card Configuration Rules, page 3-53
- Replacing a GPU Card, page 3-54
- Installing Drivers to Support the NVIDIA GPU Cards, page 3-55

Overview of Software Requirements

Table 3-12 lists the minimum server firmware versions for the GPU cards.

Table 3-12 Server Firmware Minimum Versions

GPU	Cisco IMC/BIOS Minimum Version
NVIDIA GRID K1	2.0(3a)
NVIDIA GRID K2	2.0(3a)
NVIDIA Tesla K10	2.0(3e)
NVIDIA Tesla K20	2.0(3e)
NVIDIA Tesla K20X	2.0(3e)
NVIDIA Tesla K40	2.0(3a)

GPU Card Configuration Rules

The rules for configuring the server with GPUs differ, depending on the server version and other factors. Observe the following rules when populating GPUs in the server:

- For riser 1, use version 1A (slot 2) for GPU cards. This server can be ordered with one of three PCIE riser 1 versions. GPU cards are not supported in version 1B (UCSC-PCI-1B-240M4) or 1C (UCSC-PCI-1C-240M4).
- GPU cards are also supported in PCIe riser 2, slot 5.

Caution **Cisco C240 M4 LFF and C240 M4 SFF 24-drive servers only**: When using NVIDIA GPU cards, you must preserve at least 10 mm of space between servers to ensure adequate air flow and cooling. When using GPU cards with this version of the server, the operating temperature range is 32° to 95° F (0° to 35° C).

- Mixing rules:
  - You can mix GRID K1 and K2 GPU cards in the same server.
  - Do not mix GRID GPU cards with Tesla GPU cards in the same server.
  - Do not mix different models of Tesla GPU cards in the same server.
- All GPU cards require two CPUs and two minimum 1400 W power supplies in the server.
- Table 3-13 shows the rules for populating GPU cards in the server.

Table 3-13 NVIDIA GPU Population Rules

Single GPU	Dual GPU
Riser 1A, slot 2 or Riser 2, slot 5	Riser 1A, slot 2 and Riser 2, slot 5

Note When you install a GPU card in slot 2, NCSI support in riser 1 automatically moves to slot 1. When you install a GPU card in slot 5, NCSI support in riser 2 automatically moves to slot 4. Therefore, you can install a GPU card and a Cisco UCS VIC in the same riser.

Replacing a GPU Card

Step 1 Shut down and power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove the PCIe risers and any existing GPU card:

- **a.** Lift straight up on both ends of the riser to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic mat.
- **b.** On the bottom of the riser, loosen the single thumbscrew that holds the securing plate. See Figure 3-27.
- **c.** Swing open the securing plate and remove it from the riser to provide access.
- **d.** Pull evenly on both ends of the GPU card to disengage it from the socket on the PCIe riser (or remove a blanking panel) and then set the card aside.

Note See GPU Card Configuration Rules, page 3-53 before you install the GPU cards to the risers. Slot population restrictions apply.

Step 5 Install your first GPU card into PCIe slot 2 or slot 5. See Figure 3-26 for the riser and slot locations.

Note GPU cards are not supported in PCIe riser 1 version 1B (UCSC-PCI-1B-240M4) or 1C (UCSC-PCI-1C-240M4). Use riser 1 version 1A (slot 2) or riser 2 (slot 5) for GPU cards.

- **a.** Align the GPU card with the socket on the riser, and then gently push the card's edge connector into the socket. Press evenly on both corners of the card to avoid damaging the connector.
- **b.** Connect the GPU card power cable into the GPU card and into the GPU POWER connector on the PCIe riser (see Figure 3-27).

c. Return the securing plate to the riser. Insert the two hinge-tabs into the two slots on the riser, and then swing the securing plate closed.

d. Tighten the single thumbscrew that holds the securing plate.

e. Position the PCIe riser over its socket on the motherboard and over its alignment features in the chassis (see Figure 3-25).

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

Step 6 Replace the top cover.

Step 7 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Step 8 Continue with Installing Drivers to Support the NVIDIA GPU Cards, page 3-55.

Installing Drivers to Support the NVIDIA GPU Cards

After you install the hardware, you must update to the correct level of server BIOS and then install NVIDIA drivers and other software in this order:

- 1. Updating the C240 M4 Server BIOS, page 3-55
- 2. Updating the NVIDIA Drivers, page 3-55

1. Updating the C240 M4 Server BIOS

Install the latest Cisco UCS C240 M4 server BIOS by using the Host Upgrade Utility for the Cisco UCS C240 M4 server.

Note You must do this procedure before you update the NVIDIA drivers.

Step 1 Navigate to the following URL: http://www.cisco.com/cisco/software/navigator.html.

Step 2 Click **Servers–Unified Computing** in the middle column.

Step 3 Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.

Step 4 Click the name of your model of server in the right-hand column.

Step 5 Click **Unified Computing System (UCS) Server Firmware**.

Step 6 Click the release number.

Step 7 Click **Download Now** to download the ucs-server platform-huu-version_number.iso file.

Step 8 Verify the information on the next page, and then click **Proceed With Download**.

Step 9 Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the file.

Step 10 Use the Host Upgrade Utility to update the server BIOS.

The user guides for the Host Upgrade Utility are at Utility User Guides.

2. Updating the NVIDIA Drivers

After you update the server BIOS, you can install NVIDIA drivers to your hypervisor virtual machine.

Step 1 Install your hypervisor software on a computer. Refer to your hypervisor documentation for the installation instructions.

Step 2 Create a virtual machine in your hypervisor. Refer to your hypervisor documentation for instructions.

Step 3 Install the NVIDIA drivers to the virtual machine. Download the drivers from http://www.nvidia.com/Download/index.aspx.

Step 4 Restart the server.

Step 5 Check that the virtual machine is able to recognize the NVIDIA card. In Windows, use the Device Manager and look under Display Adapters.

Replacing Internal SATA Boot Drives

Note SATA boot drives are supported only in the SFF 24-drive and LFF 12-drive versions of the server.

The SFF 24-drive and LFF 12-drive versions of the server can support two solid-state SATA boot drives, but only when the PCIe riser 1C option is installed (UCSC-PCI-1C-240M4). This version of riser 1 has two SATA boot drive connectors in place of slot 3.

Note The two internal SATA boot drives can be mirrored in a RAID 1 configuration when managed by the embedded RAID controller or in advanced host controller interface (AHCI) mode through your Windows or Linux operating system. The SATA mode must be enabled and selected in the BIOS, as described in Enabling the Embedded RAID Controller in the BIOS, page C-12.

Replacing an Internal SATA Boot Drive

Step 1 Shut down and power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove PCIe riser 1C from the server:

a. Lift straight up on both ends of the riser to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic mat.

b. On the bottom of the riser, loosen the single thumbscrew that holds the securing plate. See Figure 3-27.

c. Swing open the securing plate and remove it from the riser to provide access.

Step 5 Remove an existing SATA boot drive from PCIe riser 1C.

Grasp the carrier-tabs on each side of the boot drive and pinch them together as you pull the boot drive from its cage and the socket on the PCIe riser.

Step 6 Install a new SATA boot drive to PCIe riser 1C.

a. Grasp the two carrier-tabs on either side of the boot drive and pinch them together as you insert the drive into the cage on the riser.

b. Push the drive straight into the cage to engage it with the socket on the riser. Stop when the carrier-tabs click and lock into place on the cage.

Step 7 Return PCIe riser 1C to the server:

a. Return the securing plate to the riser. Insert the two hinge-tabs into the two slots on the riser, and then swing the securing plate closed.

b. Tighten the single thumbscrew that holds the securing plate.

c. Position the PCIe riser over its socket on the motherboard and over its alignment features in the chassis (see Figure 3-25).

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

Step 8 Replace the top cover.

Step 9 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Step 10 Set the boot order for these SATA boot drives in the server BIOS as desired:

a. Boot the server and press **F2** when prompted to enter the BIOS Setup Utility.

b. Select the **Boot Options** tab.

c. Set the boot order for your SATA boot drives.

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

Installing a Trusted Platform Module

The trusted platform module (TPM) is a small circuit board that connects to a motherboard socket and is secured by a one-way screw. The socket location is on the motherboard under PCIe riser 2.

This section contains the following procedures, which must be followed in this order when installing and enabling a TPM:

1. Installing the TPM Hardware, page 3-59
2. Enabling TPM Support in the BIOS, page 3-60
3. Enabling the Intel TXT Feature in the BIOS, page 3-61

Installing the TPM Hardware

Step 1 Prepare the server for component installation:

Step 2 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

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 3-10.

Step 5 Remove PCIe riser 2 to provide clearance. See Replacing a PCIe Riser, page 3-42 for instructions.

Step 6 Install a TPM:

a. Locate the TPM socket on the motherboard, as shown in Figure 3-28.

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 that is 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.

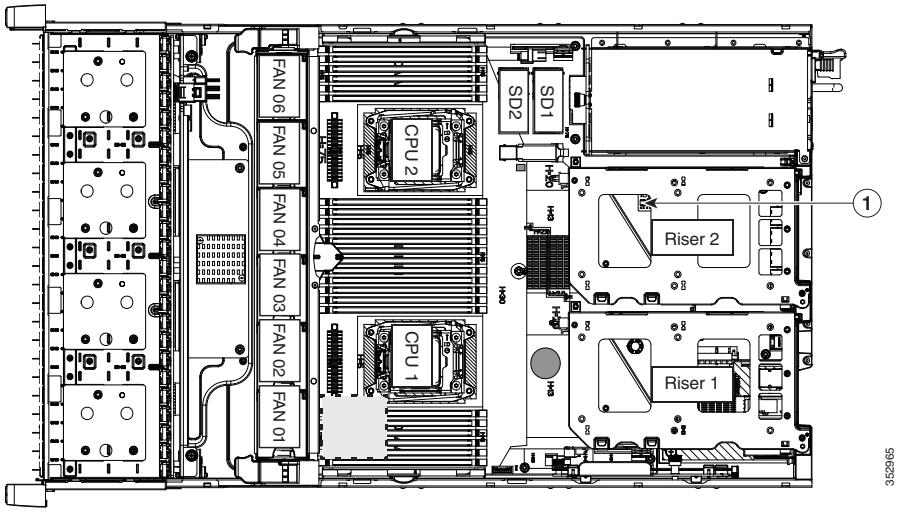
Step 7 Replace PCIe riser 2 to the server. See Replacing a PCIe Riser, page 3-42 for instructions.

Step 8 Replace the top cover.

Step 9 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Step 10 Continue with Enabling TPM Support in the BIOS, page 3-60.

Figure 3-28 TPM Socket Location on Motherboard



1	TPM socket location on the motherboard (under PCIe riser 2)		–

Enabling TPM Support in the BIOS

Note After hardware installation, you must enable TPM support in the BIOS:

Step 1 Enable TPM support:

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

b. Log in to the BIOS Setup Utility with your BIOS Administrator password.

c. On the BIOS Setup Utility window, choose the **Advanced** tab.

d. Choose **Trusted Computing** to open the TPM Security Device Configuration window.

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

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

Step 2 Verify that TPM support 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. Choose the **Advanced** tab.

d. Choose **Trusted Computing** to open the TPM Security Device Configuration window.

e. Verify that TPM SUPPORT and TPM State are Enabled.

Step 3 Continue with Enabling the Intel TXT Feature in the BIOS, page 3-61.

Enabling the Intel TXT Feature in the BIOS

Intel Trusted Execution Technology (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. 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.

Step 1 Reboot the server and watch for the prompt to press F2.

Step 2 When prompted, press **F2** to enter the BIOS Setup utility.

Step 3 Verify that the prerequisite BIOS values are enabled:

a. Choose the **Advanced** tab.

b. Choose **Intel TXT(LT-SX) Configuration** to open the Intel TXT(LT-SX) Hardware Support window.

c. Verify that the following items are listed as Enabled:

- VT-d Support (default is Enabled)
- VT Support (default is Enabled)
- TPM Support
- TPM State

- If VT-d Support and VT Support 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.

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

e. On the Advanced tab, choose **Processor Configuration** to open the Processor Configuration window.

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

Step 4 Enable the Intel Trusted Execution Technology (TXT) feature:

a. Return to the Intel TXT(LT-SX) Hardware Support window if you are not already there.

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

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

Replacing Power Supplies

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

- See Power Specifications, page A-2 for more information about the supported power supplies.
- See Rear Panel LEDs and Buttons, page 3-5 for information about the power supply LEDs.
- See Wiring a DC Power Supply, page 3-63 for information about wiring a DC power supply.

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 and hot-swappable.

Note Do not mix power supply types in the server. Both power supplies must be the same wattage and Cisco product ID (PID).

Step 1 Remove the power supply that you are replacing or a blank panel from an empty bay:

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 Shutting Down and Powering Off the Server, page 3-9.
   - 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.

   For a DC power supply, release the electrical connector block from the power supply by pushing the orange plastic button on the top of the connector inward toward the power supply (see Figure 3-30). Pull the connector block from the power supply.

c. Grasp the power supply handle while pinching the green release lever towards the handle (see Figure 3-29).

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.

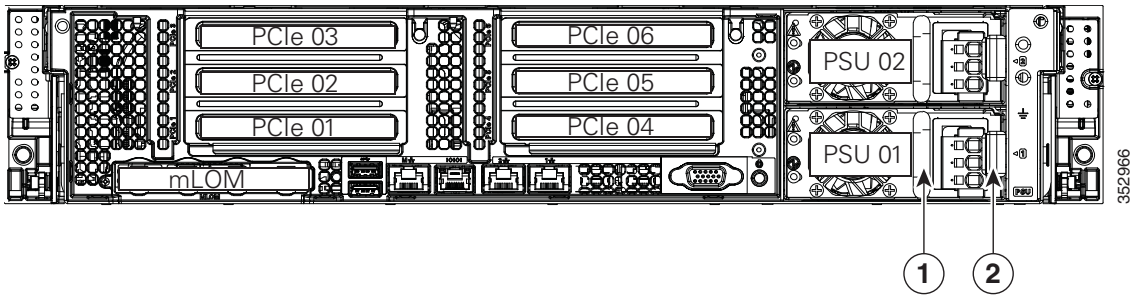
b. Push the power supply into the bay until the release lever locks.

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

   For a DC power supply, push the electrical connector block into the power supply.

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

Figure 3-29 Power Supplies



1	Power supply handle	2	Power supply release lever

Wiring a DC Power Supply

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring. Statement 1022**

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations. Statement 1045**

Warning **When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 1046**

Warning **Installation of the equipment must comply with local and national electrical codes. Statement 1074**

Warning **Hazardous voltage or energy may be present on DC power terminals. Always replace cover when terminals are not in service. Be sure uninsulated conductors are not accessible when cover is in place. Statement 1075**

Note The recommended wire gauge is 8 AWG. The minimum wire gauge is 10 AWG.

Caution Before beginning this wiring procedure, turn off the DC power source from your facility's circuit breaker to avoid electric shock hazard.

Step 1 Turn off the DC power source from your facility's circuit breaker to avoid electric shock hazard.

Step 2 Remove the DC power connector block from the power supply. (The spare PID for this connector is UCSC-CONN-930WDC=.)

To release the connector block from the power supply, push the orange plastic button on the top of the connector inward toward the power supply, and then pull the connector block out.

Step 3 Strip 15 mm (.59 inches) of insulation off the DC wires that you will use.

Step 4 Orient the connector as shown in Figure 3-30, with the orange plastic button toward the top.

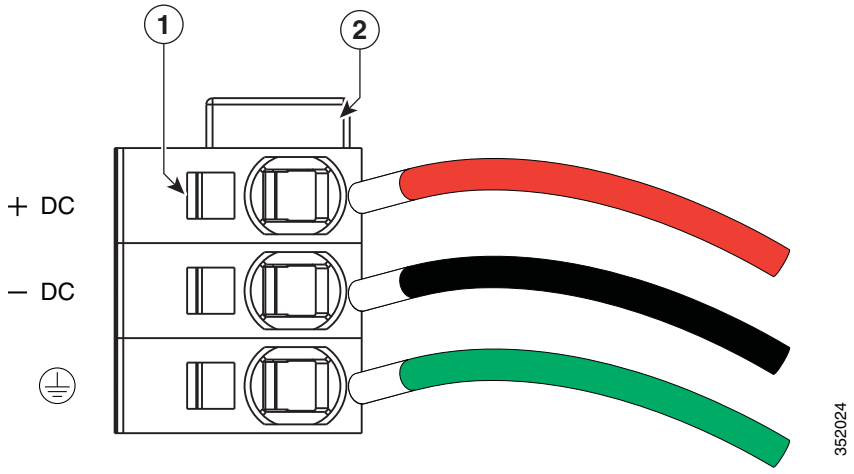
Step 5 Use a small screwdriver to depress the spring-loaded wire retainer lever on the lower spring-cage wire connector. Insert your green (ground) wire into the aperture and then release the lever.

Step 6 Use a small screwdriver to depress the wire retainer lever on the middle spring-cage wire connector. Insert your black (DC negative) wire into the aperture and then release the lever.

Step 7 Use a small screwdriver to depress the wire retainer lever on the upper spring-cage wire connector. Insert your red (DC positive) wire into the aperture and then release the lever.

Step 8 Insert the connector block back into the power supply. Make sure that your red (DC positive) wire aligns with the power supply label "+ DC".

Figure 3-30 930 W, –48 VDC Power Supply Connector Block



1	Wire retainer lever	**2**	Orange plastic button on top of the connector

Replacing an mLOM Card

The server can use an mLOM card to provide additional connectivity. The mLOM card socket remains powered when the server is in 12 V standby power mode and it supports the network communications services (NCSI) protocol.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

Step 2 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 3 Remove the top cover as described in Removing and Replacing the Server Top Cover, page 3-10.

Step 4 Remove PCIe riser 1 to provide clearance. See Replacing a PCIe Riser, page 3-42 for instructions.

Step 5 Remove any existing mLOM card or a blanking panel (see Figure 3-31):

- **a.** Loosen the single thumbscrew that secures the mLOM card to the chassis floor.
- **b.** Slide the mLOM card horizontally to disengage its connector from the motherboard socket.

Step 6 Install a new mLOM card:

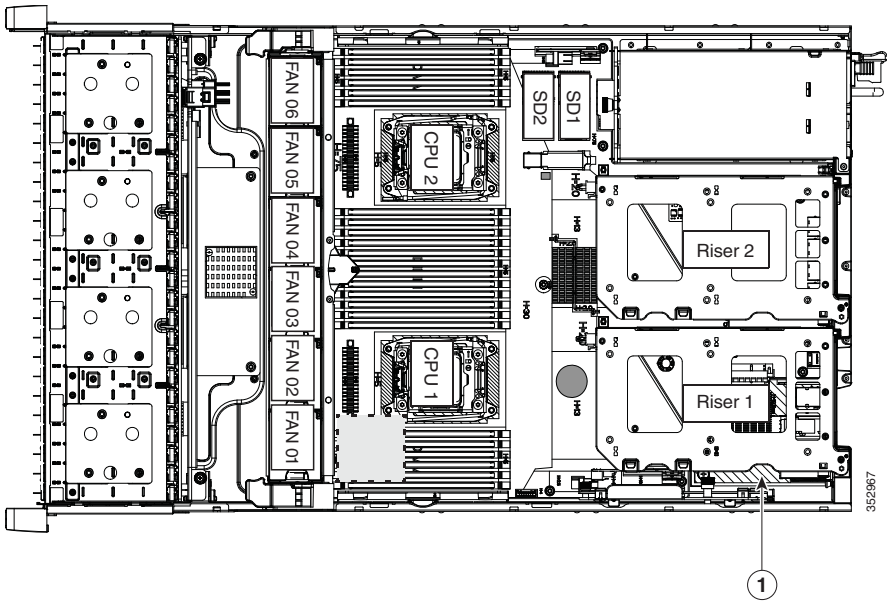
- **a.** Set the mLOM card on the chassis floor so that its connector is aligned with the motherboard socket and its thumbscrew is aligned with the standoff on the chassis floor.
- **b.** Push the card's connector into the motherboard socket horizontally.
- **c.** Tighten the thumbscrew to secure the card to the chassis floor.

Step 7 Return PCIe riser 1 to the server. See Replacing a PCIe Riser, page 3-42 for instructions.

Step 8 Replace the top cover.

Step 9 Replace the server in the rack, replace cables, and then power on the server by pressing the **Power** button.

Figure 3-31 mLOM Card Location



1	mLOM card socket location on motherboard (under PCIe riser 1)		

Service DIP Switches

This section includes the following topics:

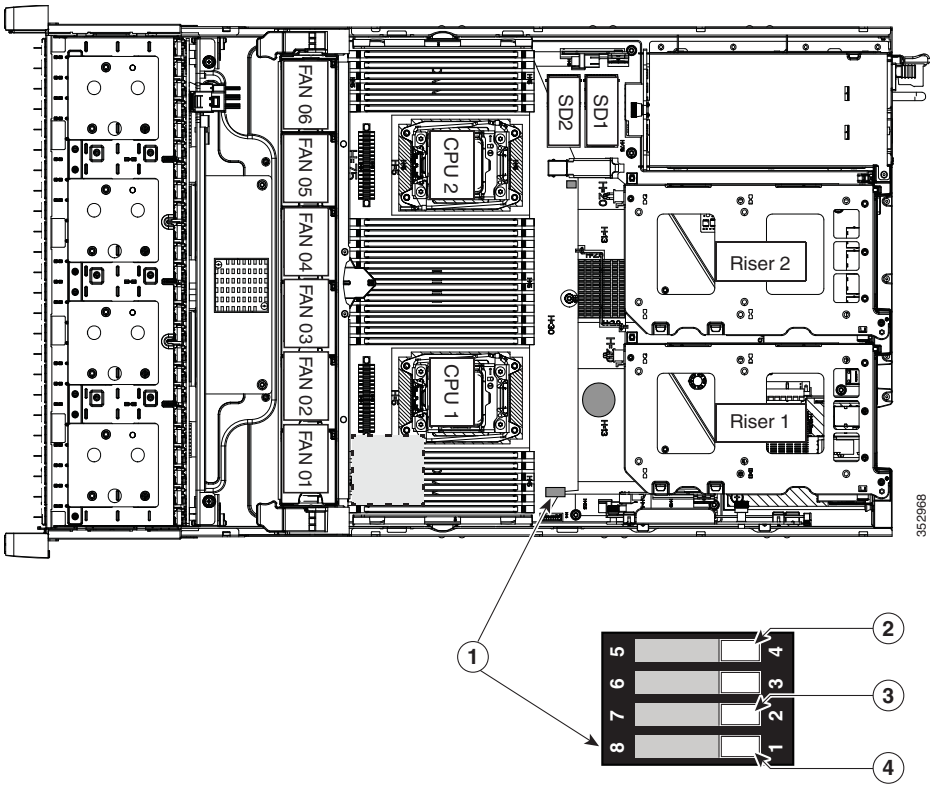
- DIP Switch Location on the Motherboard, page 3-67
- Using the BIOS Recovery DIP Switch, page 3-68
- Using the Clear Password DIP Switch, page 3-70
- Using the Clear CMOS DIP Switch, page 3-71

DIP Switch Location on the Motherboard

See Figure 3-32. The position of the block of DIP switches (SW8) is shown in red. In the magnified view, all switches are shown in the default position.

- BIOS recovery—switch 1.
- Clear password—switch 2.
- Not used—switch 3.
- Clear CMOS—switch 4.

Figure 3-32 Service DIP Switches



1	DIP switch block SW8	**3**	Clear password switch 2
2	Clear CMOS switch 4	**4**	BIOS recovery switch 1

Using the BIOS Recovery DIP Switch

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 Cisco IMC WebGUI or CLI interface.
IF Cisco IMC 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. If that procedure does not recover the BIOS, use procedure 2.

Procedure 1: Reboot with recovery.cap File

Step 1 Download the BIOS update package and extract it to a temporary location.

Step 2 Copy the contents of the extracted recovery folder to the root directory of a USB thumb drive. The recovery folder contains the recovery.cap file that is required in this procedure.

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

Step 3 Insert the USB thumb drive into a USB port on the server.

Step 4 Reboot the server.

Step 5 Return the server to main power mode by pressing the **Power** button on the front panel.

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

```
Found a valid recovery file...Transferring to Cisco IMC
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, and then remove the USB thumb drive from the server.

Note During the BIOS update, Cisco IMC shuts down the server and the screen goes blank for about 10 minutes. Do not unplug the power cords during this update. Cisco IMC powers on the server after the update is complete.

Procedure 2: Use BIOS Recovery DIP switch and recovery.cap File

See Figure 3-32 for the location of the SW8 block of DIP switches.

Step 1 Download the BIOS update package and extract it to a temporary location.

Step 2 Copy the contents of the extracted recovery folder to the root directory of a USB thumb drive. The recovery folder contains the recovery.cap file that is required in this procedure.

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

Step 3 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

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 3-10.

Step 7 Slide the BIOS recovery DIP switch from position 1 to the closed position (see Figure 3-32).

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 Cisco IMC
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, and then remove the USB thumb drive from the server.

Note During the BIOS update, Cisco IMC shuts down the server and the screen goes blank for about 10 minutes. Do not unplug the power cords during this update. Cisco IMC powers 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 Slide the BIOS recovery DIP switch from the closed position back to the default position 1.

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, and then power on the server by pressing the **Power** button.

Using the Clear Password DIP Switch

See Figure 3-32 for the location of this DIP switch. You can use this switch to clear the administrator password.

Step 1 Power off the server as described in Shutting Down and Powering Off the Server, page 3-9.

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 3-10.

Step 5 Slide the clear password DIP switch from position 2 to the closed position (see Figure 3-32).

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. 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 Slide the clear CMOS DIP switch from the closed position back to default position 2 (see Figure 3-32).

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, and then power on the server by pressing the **Power** button.

Using the Clear CMOS DIP Switch

See Figure 3-32 for the location of this DIP switch. You can use this switch 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 3-9.

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 3-10.

Step 5 Slide the clear CMOS DIP switch from position 4 to the closed position (see Figure 3-32).

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. 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 clear CMOS DIP switch from the closed position back to default position 4 (see Figure 3-32).

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, and then power on the server by pressing the **Power** button.



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. (8.70 cm)
Width (including slam latches)	19.0 in. (48.26 cm)
Depth (length)	29.0 in. (73.70 cm)
Depth, including slam latches and power supply handles	31.5 in. (80.00 cm)
Maximum Weight (fully loaded)	SFF 8-drive: 52.9 lb. (24.0 Kg) SFF 16-drive: 58.9 lb. (26.7 Kg) SFF 24-drive: 62.7 lb. (28.4 Kg) LFF 12-drive: 67.5 lb. (30.6 Kg)

Power Specifications

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

- 650 W AC Power Supply, page A-2
- 1200 W AC Power Supply, page A-3
- 1400 W AC Power Supply, page A-3
- 930 W DC Power Supply, page A-4

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

http://www.cisco.com/assets/cdc_content_elements/flash/dataCenter/cisco_ucs_power_calculator/

650 W AC Power Supply

Table A-2 lists the specifications for each 650 W AC power supply (Cisco part number UCSC-PSU2V2-650W=).

Table A-2 Power Supply Specifications

Description	Specification
AC input voltage range	90 to 264 VAC (self-ranging, 180 to 264 VAC nominal)
AC input frequency	Range: 47 to 63 Hz (single phase, 50 to 60Hz nominal)
AC line input current (steady state)	7.6 A peak at 100 VAC 3.65 A peak at 208 VAC
Maximum output power for each power supply	650 W
Power supply output voltage	Main power: 12 VDC Standby power: 12 VDC

1200 W AC Power Supply

Table A-3 lists the specifications for each 1200 W AC power supply (Cisco part number UCSC-PSU2V2-1200W=).

Table A-3 Power Supply Specifications

Description	Specification
AC input voltage range	90 to 264 VAC (self-ranging, 180 to 264 VAC nominal)
AC input frequency	Range: 47 to 63 Hz (single phase, 50 to 60Hz nominal)
AC line input current (steady state)	11A peak at 100 VAC 7 A peak at 208 VAC
Maximum output power for each power supply	1200 W
Power supply output voltage	Main power: 12 VDC Standby power: 12 VDC

1400 W AC Power Supply

Table A-2 lists the specifications for each 1400 W AC power supply (Cisco part number UCSC-PSU2-1400=).

Table A-4 1400 W Power Supply Specifications

Description	Specification
Class	RSP1
AC input voltage	200 to 240 VAC nominal (range: 180 to 264 VAC)
AC input frequency	50 to 60 Hz nominal (range: 47 to 63 Hz)
Maximum AC-input current	8.5 A at 200 VAC
Maximum output power for each power supply	1400 W (two or four power supplies can be installed)
Power supply output voltage	Main power: 12 VDC Standby power: 12 VDC
Rated output load	Main power: 116.6 DC Amps Standby power: 2.5 DC Amps

930 W DC Power Supply

Table A-5 lists the specifications for each 930 W DC power supply (Cisco part number UCSC-PSU-930WDC=).

Table A-5 930 W DC Power Supply Specifications

Description	Specification
Class	RSP1
Input	
DC input voltage range	–48 to –60 VDC nominal (self-ranging, –40 to –72 VDC)
DC line input current (steady state)	23 A peak at –48 VDC
Output	
12 V main power output	930 W
12 V standby power output	30 W
Power supply output voltage	Main power: 12 VDC Standby power: 12 VDC

Environmental Specifications

Table A-6 lists the environmental specifications for the server.

Table A-6 Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, nonoperating (when the server is in storage or is transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), noncondensing	10 to 90%
Altitude, operating	0 to 10,000 feet
Altitude, nonoperating (when the server is in storage or is transported)	0 to 40,000 feet
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.8
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	43



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	
SFS-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
SFS-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
SFS-250V-10A-ID Power Cord, 250 VAC 16A EL-208 Plug South Africa, United Arab Emirates, India	8.2	2.5	Figure B-5
SFS-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 SFS-250V-10A-AR

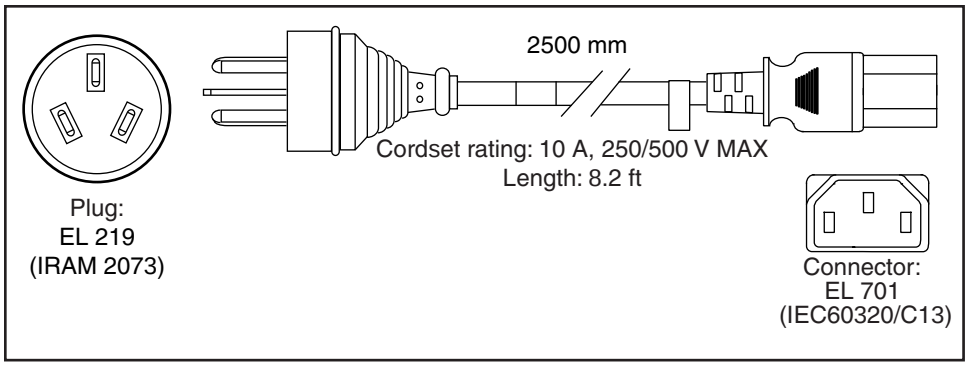


Figure B-2 CAB-9K10A-AU

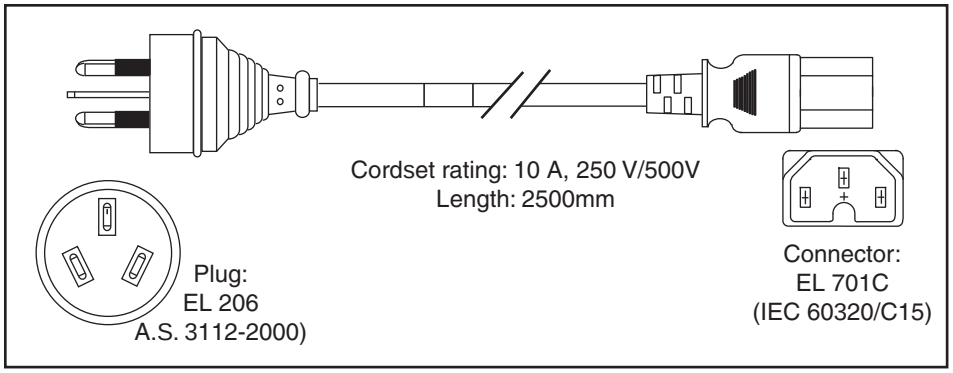


Figure B-3 SFS-250V-10A-CN

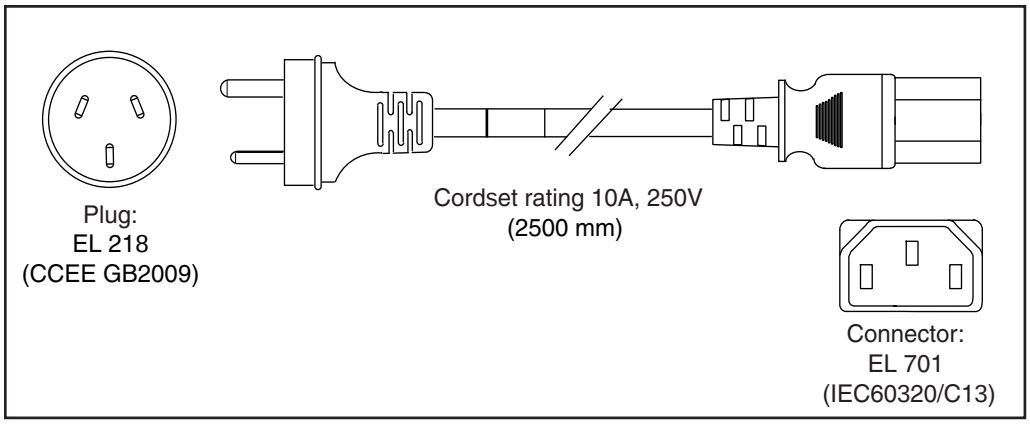


Figure B-4 CAB-9K10A-EU

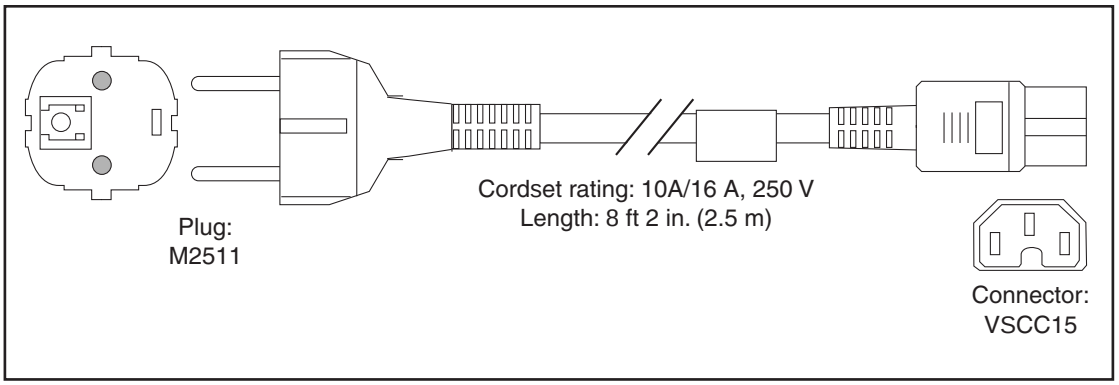


Figure B-5 SFS-250V-10A-ID

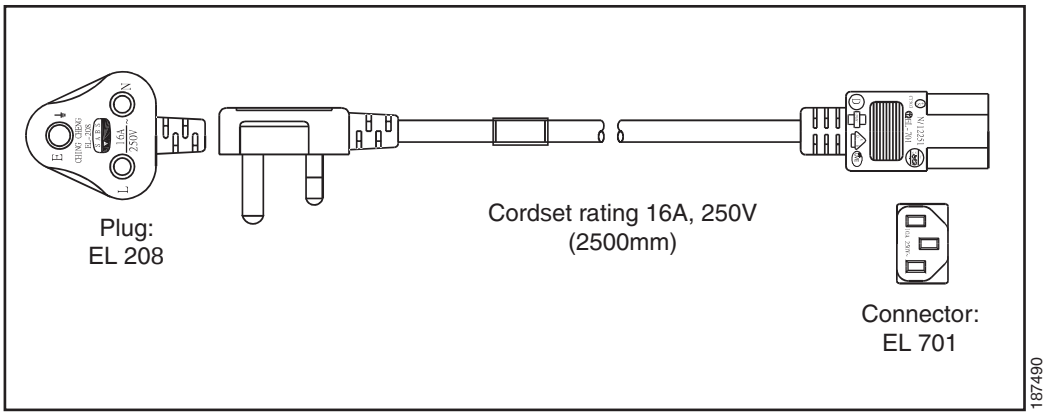


Figure B-6 SFS-250V-10A-IS

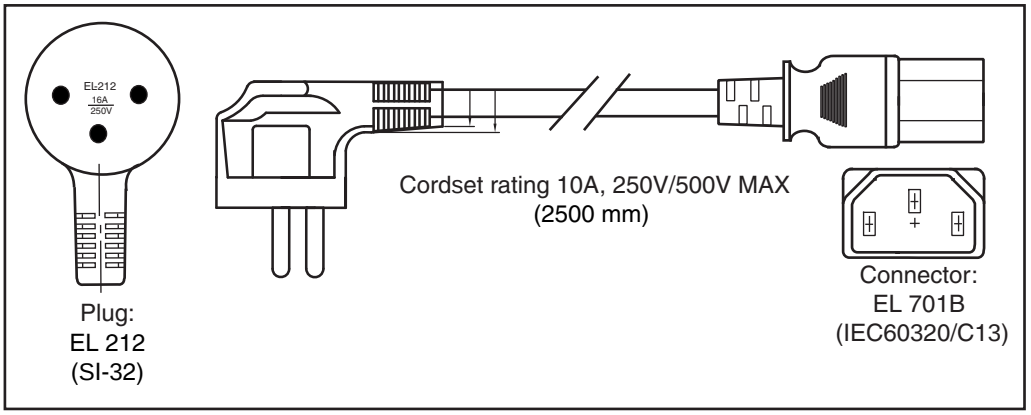


Figure B-7 CAB-9K10A-IT

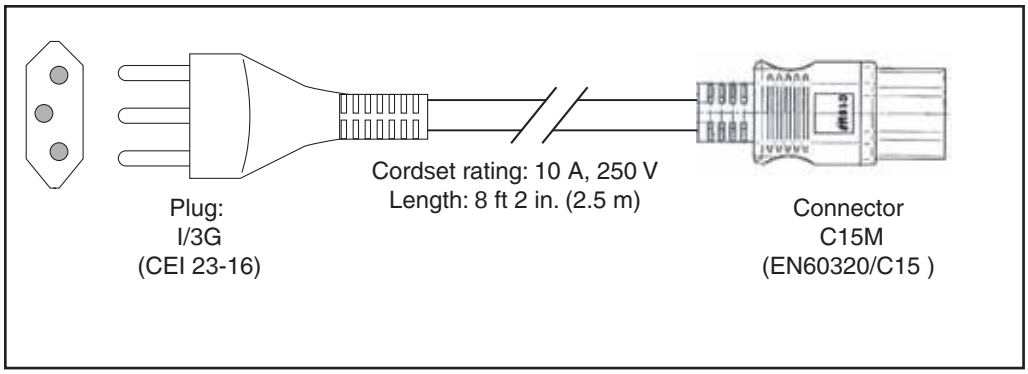


Figure B-8 CAB-9K10A-SW

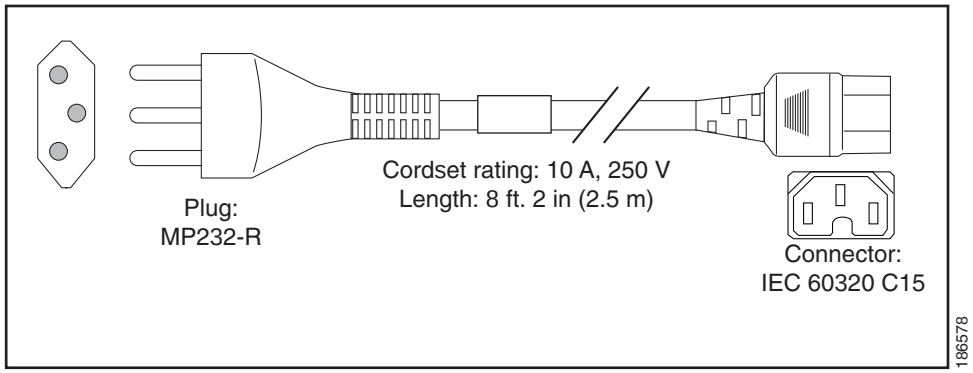


Figure B-9 CAB-9K10A-UK

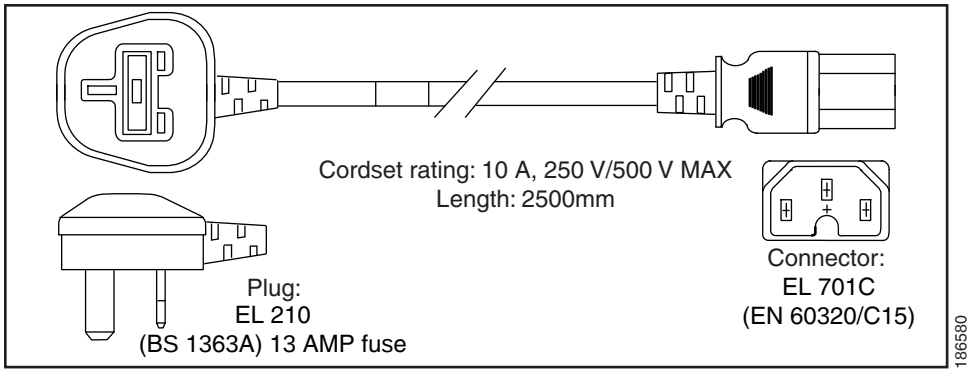


Figure B-10 CAB-AC-250V/13A

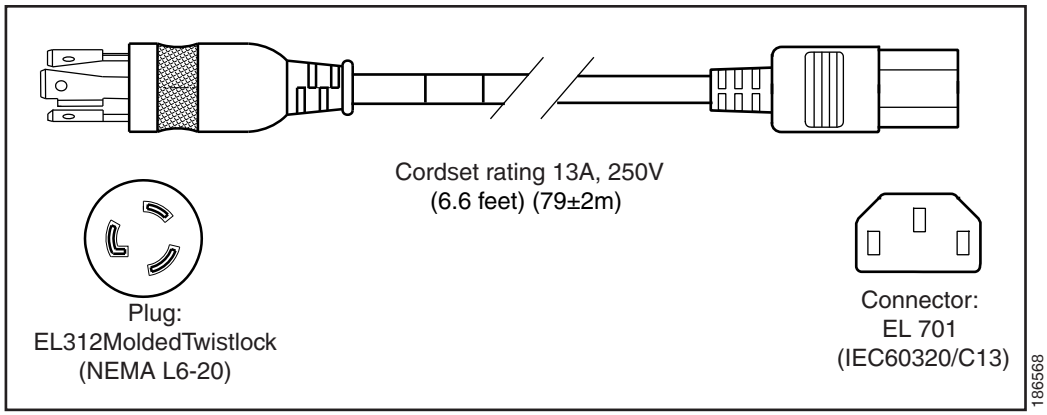


Figure B-11 CAB-N5K6A-NA

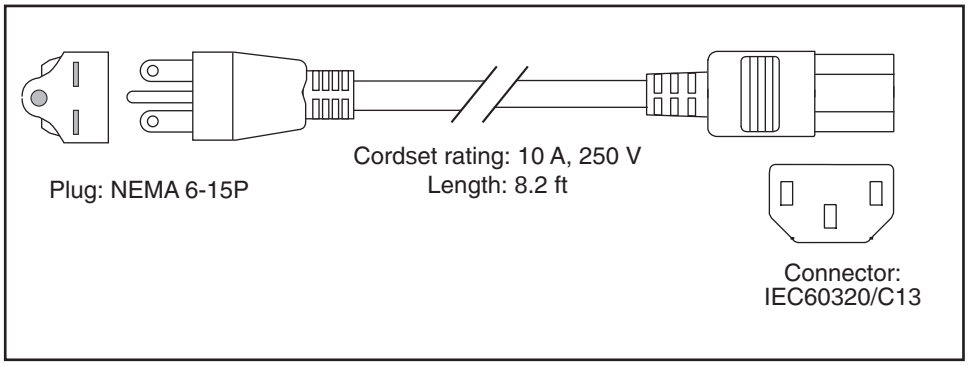


Figure B-12 CAB-9K12A-NA

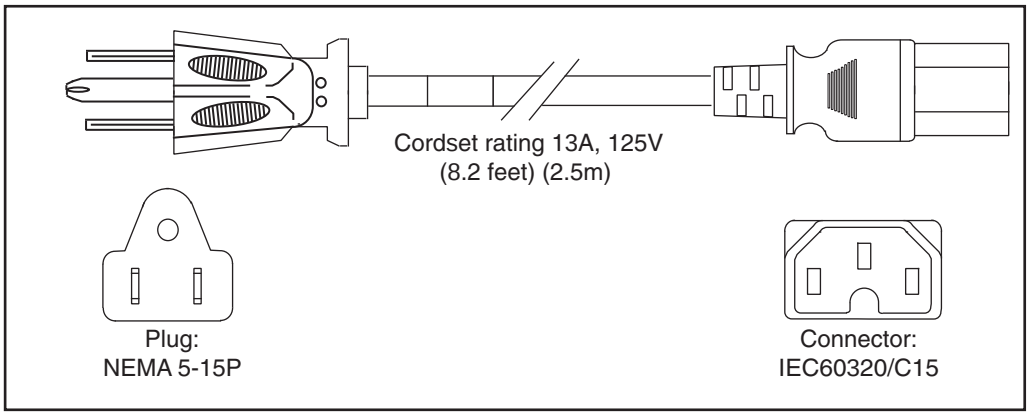


Figure B-13 CAB-C13-CBN, Jumper Power Cord (0.68 m)

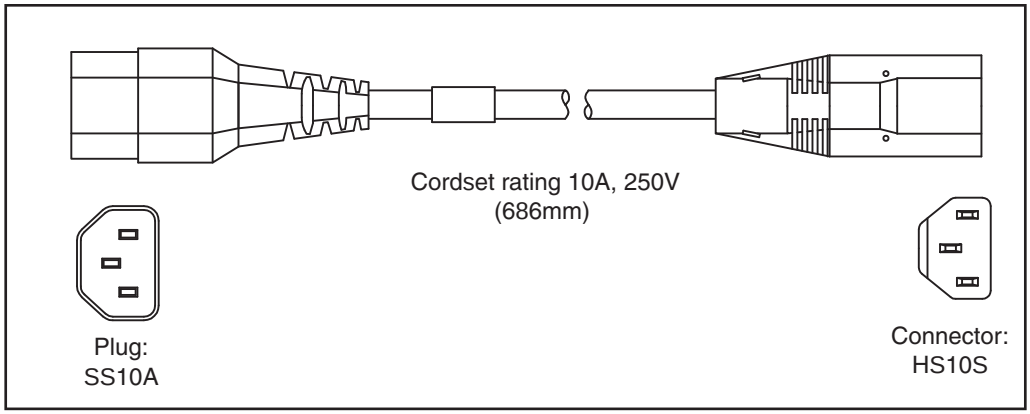


Figure B-14 CAB-C13-C14-2M, Jumper Power Cord (2 m)

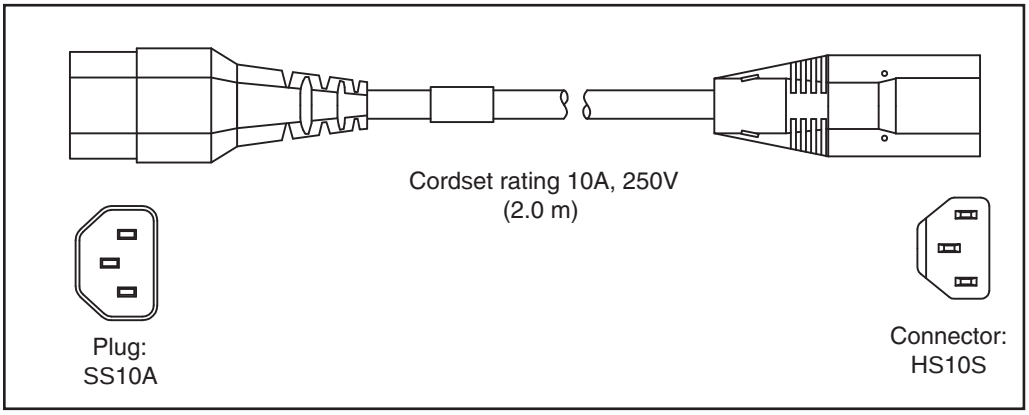
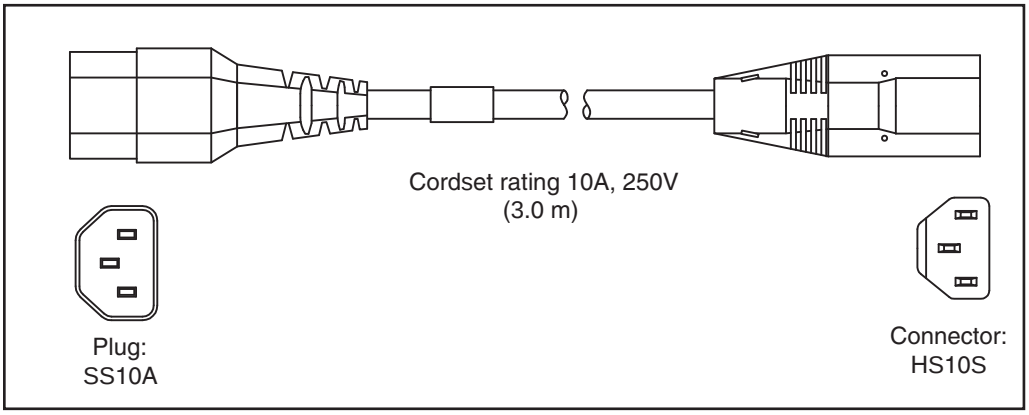


Figure B-15 CAB-C13-C14-AC, Jumper Power Cord (3 m)





RAID Controller Considerations

This appendix contains the following sections:

- Supported RAID Controllers and Required Cables, page C-2
- Support Matrix For Cisco UCS C240 M4 Server RAID Controllers, page C-3
- Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations, page C-3
- Mixing Drive Types in RAID Groups, page C-5
- RAID Backup Units, page C-5
- RAID Controller Cabling, page C-6
- Embedded SATA RAID Controller, page C-9
- Restoring RAID Configuration After Replacing a RAID Controller, page C-22
- For More Information, page C-23

Also see these procedures for replacing RAID-related hardware:

- Replacing a Cisco Modular RAID Controller Card, page 3-31
- Replacing a Modular RAID Controller Transportable Memory Module (TMM), page 3-33
- Replacing the Supercap Power Module (RAID Backup Battery), page 3-35
- Replacing a SATA Interposer Board, page 3-29
- Replacing a Software RAID 5 Key Module, page 3-37

Supported RAID Controllers and Required Cables

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

Caution In a SFF 8-drive server, do not use the embedded software RAID controller and a hardware RAID controller card to control the front-facing drives at the same time. This combination is not supported and could result in data loss. You can use the embedded software RAID controller to control internal SSD boot drives (SFF 24-drive and LFF 12-drive server versions only) while you use a hardware RAID controller card to control the front-facing drives.

Note See Support Matrix For Cisco UCS C240 M4 Server RAID Controllers, page C-3 for information about controller support by server version and drive type.

Table C-1 Cisco UCS C240 M4 RAID Options

Controller	Style	Supported Server Version/ Maximum Front-Facing Drives Controlled	SCPM	RAID Levels	Required Cables
Embedded RAID (PCH SATA)	On board	• SFF 8-drives/no expander: 8 internal SATA drives	No	0, 1, 5[1], 10	• SFF 8-drives/no expander: Cable and required SATA interposer board bundled as UCSC-IP-PCH-C240M4=
Cisco UCS 12G SAS Modular RAID Controller This controller can be ordered with modular flash-based write cache (FBWC) options: 512 MB, 1 GB, 2 GB, or 4 GB.	PCIe	• SFF 8-drives/no expander: 8 internal drives • SFF 16-drives/expander: 16 internal drives • SFF 24-drives/expander: 24 internal drives • LFF 12-drives/expander: 12 internal drives	Yes[2]	Variable by cache size: • No cache: 0, 1, 10 • 512MB cache: 0, 1, 5, 10, 50 • 1GB, 2GB, or 4GB cache: 0, 1, 5, 6, 10, 50, 60	• SFF 8-drives/no expander: (UCS-240CBLMR8=) • SFF 16 drives/expander: (UCS-240CBLMR16=) • SFF 24 drives/expander: (UCS-240CBLMR24=) • LFF 12 drives/expander: (UCS-240CBLMR12=)
Cisco UCS SAS 9300-8i HBA Note: See also Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations, page C-3.	PCIe	• SFF 24-drives/expander: 24 internal drives • LFF 12-drives/expander: 12 internal drives	No	Non-RAID	• SFF 24 drives/expander: (240CBLHBA24=) • LFF 12 drives/expander: (240CBLHBA12=)
Cisco UCS SAS 9300-8e HBA Note: See also Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations, page C-3.	PCIe	• All server versions 8 external SAS+SATA ports, controlling up to 1024 non-RAID external drives	No	Non-RAID	• External drive cables are not sold by Cisco.

1. Embedded RAID 5 support requires an optional RAID 5 key module.
2. SCPM = SuperCap power module (RAID backup unit). See RAID Backup Units, page C-5.

Support Matrix For Cisco UCS C240 M4 Server RAID Controllers

Table C-2 lists the support for the available controllers by server version.

Table C-2 Support Matrix For C240 M4 RAID Controllers

C240 M4 Version	Boot SSD (Internal) Supported?	Embedded Software RAID Control Boot SSD (Internal)?	AHCI Mode Control Boot SSD (Internal)?	Hardware Controller Card Control Boot SSD (Internal)?	Embedded Software RAID Control Front-Facing drives?[1]	AHCI mode Control Front-Facing drives?	Cisco 12G Modular RAID Controller Card Control Front-Facing Drives?	SAS 9300-8i HBA Controller Card Control Front-Facing Drives? [2]
SFF 8 HDD	No	N/A	N/A	N/A	Yes	No	Yes	N/A
LFF 12 HDD	Yes	Yes	Yes	No	No	No	Yes	Yes
SFF 16 HDD	No	N/A	N/A	N/A	No	No	Yes	N/A
SFF 24 HDD	Yes	Yes	Yes	No	No	No	Yes	Yes

1. You cannot mix hardware and software RAID control of the front-facing drives in a server. You can use software RAID to control the internal boot SSDs while you use a hardware RAID controller card to control the front-facing drives in a server.
2. The Cisco UCS SAS 9300-8i non-RAID HBA is supported only in slot 1 of the LFF 12 HDD and SFF 24 HDD versions of this server. See Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations, page C-3.

Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations

This section contains the following topics:

- Cisco UCS SAS 9300-8i HBA Support by Server Version, page C-3
- Cisco UCS 9300-8i and 9300-8e Bad Drive and Predictive Failure Behavior, page C-4
- Setting the Preferred Boot Device for Cisco UCS 9300-8i and 9300-8e, page C-4

Cisco UCS SAS 9300-8i HBA Support by Server Version

The Cisco UCS SAS 9300-8i HBA has the following support at this time:

Table C-3 Cisco UCS SAS 9300-8i HBA Support

Server Version	PCIe Slot Support	Mix With Cisco UCS SAS 9300-8e HBA?	Mix With AHCI Support for Internal SSDs (SATA Boot Drives)	Mix With Embedded RAID (SWRAID)
SFF, 8 HDD	Not supported	Not supported	Not supported	Not supported
SFF, 16 HDD	Not supported	Not supported	Not supported	Not supported
SFF, 24 HDD	Slot 1 only	Yes	Yes	No
LFF, 12 HDD	Slot 1 only	Yes	Yes	No

Cisco UCS 9300-8i and 9300-8e Bad Drive and Predictive Failure Behavior

The bad drive and predictive failure behavior for the Cisco UCS RAID SAS 9300-8i and 9300-e HBA cards is different than that for LSI MegaRAID cards. The list below compares behavior for these HBA cards and LSI MegaRAID cards.

- Bad/invalid/0MB drive handling:
  - MegaRAID: The bad drive is marked BAD in the GUI/CLI interfaces and the fault LED on the drive is solid amber.
  - HBA: The bad drive is not shown in the GUI/CLI and there is no LED indication.
- Drive predictive failure:
  - MegaRAID: If the drive is part of a RAID volume with a spare, the software performs an auto-copy backup and then marks the drive failed/BAD with the fault LED on the drive solid amber.
  - HBA: There is no error handling and there is no LED indication. The operating system must handle the fault.

Setting the Preferred Boot Device for Cisco UCS 9300-8i and 9300-8e

Currently, the boot device order for these HBAs does not map to a physical slot as seen in the Boot Option dialog of the server BIOS Setup Utility. This makes it difficult to differentiate between multiple devices.

Use the following procedure to select the preferred boot device in the LSI BIOS CU SAS Topology screen. When you select the preferred boot device in the BIOS CU SAS Topology screen, it is displayed at the top of the list in the server BIOS Setup Utility Boot Option dialog, making it easy to identify.

Step 1 In the LSI SAS BIOS CU, navigate to the SAS Topology screen.

Step 2 Press **Alt+B** to select or deselect a device as the preferred boot device. On this screen, you can identify the device by slot number.

Step 3 Press **Alt+A** to select or deselect a device as the alternate boot device. On this screen, you can identify the device by slot number. The alternate boot device is used if the preferred boot device is not detected.

Step 4 Return to the BIOS CU SAS Topology screen.

The Device Info column shows which devices you selected with the designators `Boot` and `Alt`.

Step 5 In the server BIOS Setup Utility, open the Boot Option dialog.

The preferred device that you selected in the LSI BIOS CU is listed at the top of the list.

Step 6 Select the device at the top of the list as your boot option.

Mixing Drive Types in RAID Groups

Table C-4 lists the technical capabilities for mixing hard disk drive (HDD) and solid state drive (SSD) types in a RAID group. However, see the recommendations that follow for the best performance.

Table C-4 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

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.

RAID Backup Units

This server supports installation of one SuperCap power module (SCPM). The units mount to clips on the removable air baffle (see Figure 3-20).

The SCPM provides approximately three years of backup for the disk write-back cache DRAM in the case of a sudden power loss by offloading the cache to the NAND flash.

For SCPM replacement instructions, see Replacing the Supercap Power Module (RAID Backup Battery), page 3-35.

RAID Controller Cabling

This section includes the following topics:

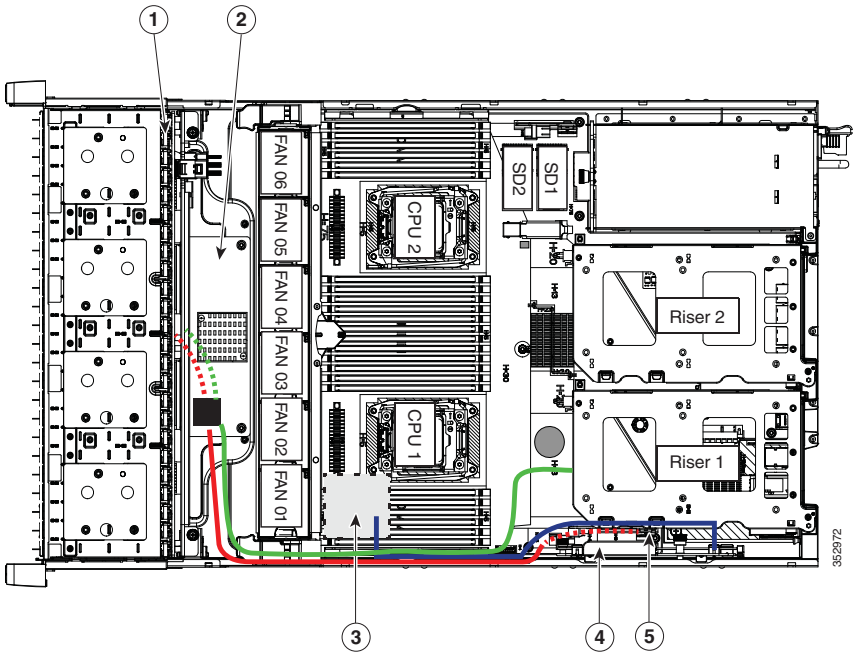
- Cable Routing, page C-6
- Cisco UCS C240 M4 Server RAID Controller Cabling Instructions, page C-7

Cable Routing

The RAID controller connectors in this server are shown in Figure C-1.

- The red line shows the recommended cable routing path from the Cisco modular RAID controller card or the embedded SATA RAID interposer board to the drive backplane or expander. Cable clips on the chassis wall secure the cables.
- The blue line shows the recommended cable routing path from the Cisco modular RAID controller to the SCPM on the removable air baffle. The SCPM cable should pass through the opening on the rear of the air baffle to avoid interfering with the top cover.
- The green line shows the recommended cable routing path from an HBA in slot 1 to the drive backplane or expander.

Figure C-1 RAID Controller Connectors and Cable Paths



1	Drive backplane The SFF 16-drive and LFF 12-drive options have an expander integrated into the backplane.	**4**	Cisco modular RAID controller PCIe slot (dedicated slot on motherboard)
2	Expander The SFF 24-drive version (shown) has an expander separate from the backplane.	**5**	Embedded SATA RAID interposer board socket on motherboard
3	SCPM mounting location on removable air baffle (air baffle not shown)		

Cisco UCS C240 M4 Server RAID Controller Cabling Instructions

This section contains cabling instructions for controlling front-facing drives in the four server versions and their supported cables:

- SFF 8-Drive Direct-Connect Backplane, No Expander, page C-7
- SFF 16-Drive Backplane with Integrated Expander, page C-7
- SFF 24-Drive Backplane with Expander Cabling, page C-8
- LFF 12-Drive Backplane with Expander, page C-8

SFF 8-Drive Direct-Connect Backplane, No Expander

The SFF 8-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

This option can control up to eight front-facing SATA drives (in two groups of four drives).

The required `UCSC-IP-PCH-C240M4=` kit includes the SATA interposer board and one Y-cable (mini-SAS HD to mini-SAS 36-pin x2).

Make the following connections:

1. Connect the PORT A cable connector to the PORT A connector on the interposer board.
2. Connect the PORT B cable connector to the PORT B connector on the interposer board.
3. Connect the single mini-SAS HD cable connector to the single connector on the backplane.

Cisco UCS 12G Modular RAID Controller

This option can control up to eight drives.

The required `UCS-240CBLMR8=` cable kit has one cable with a mini-SAS HD connector on each end.

Make the following connections:

1. Connect one end of the cable to the modular RAID controller card.
2. Connect the other end of the cable to the single mini-SAS HD connector on the backplane.

SFF 16-Drive Backplane with Integrated Expander

The SFF 16-drive option has a SAS expander integrated with the backplane.

Cisco UCS 12G Modular RAID Controller

This option can control up to 16 drives.

The required `UCS-C240CBLMR16=` cable kit has one cable with a mini-SAS HD connector on each end.

Make the following connections:

1. Connect one end of the cable to the modular RAID controller card.
2. Connect the other end of the cable to the single mini-SAS HD connector on the backplane.

SFF 24-Drive Backplane with Expander Cabling

The SFF 24-drive option has a backplane and SAS expander.

Note No cabling is required for the embedded SATA RAID controller to control the internal SSD boot drives.

Cisco UCS 12G Modular RAID Controller

This option can control up to 24 drives.

The required UCS-240CBLMR24= cable kit has one cable with a mini-SAS HD connector on each end.

Make the following connections:

1. Connect one end of the cable to the modular RAID controller card.
2. Connect the other end of the cable to the single mini-SAS HD connector on the expander.

Cisco UCS SAS 9300-8i HBA

This option can control up to 24 drives (non-RAID).

The required 240CBLHBA24= cable kit has one cable with a mini-SAS HD connector on each end.

Make the following connections:

1. Connect one end of the cable to the modular RAID controller card.
2. Connect the other end of the cable to the single mini-SAS HD connector on the expander.

LFF 12-Drive Backplane with Expander

The LFF 12-drive option has a SAS expander integrated with the backplane.

Note No cabling is required for the embedded SATA RAID controller to control the internal SSD boot drives.

Cisco UCS 12G Modular RAID Controller

This option can control up to 12 drives.

The required UCS-240CBLMR12= cable kit has one Y-cable with a mini-SAS HD double connector on one end and two mini-SAS HD single connectors on the other end.

1. Connect the mini-SAS double connector to the modular RAID controller card.
2. Connect single connector PORT A to the PORT A connector on the backplane.
3. Connect single connector PORT B to the PORT B connector on the backplane.

Cisco UCS SAS 9300-8i HBA

This option can control up to 12 drives (non-RAID).

The required 240CBLHBA12= cable kit has one Y-cable with a mini-SAS HD double connector on one end and two mini-SAS HD single connectors on the other end.

Make the following connections:

1. Connect the mini-SAS double connector to the modular RAID controller card.
2. Connect single connector PORT A to the PORT A connector on the backplane.
3. Connect single connector PORT B to the PORT B connector on the backplane.

Embedded SATA RAID Controller

Note VMware ESX/ESXi or any other virtualized environments are not supported for use with the embedded MegaRAID controller. Hypervisors such as Hyper-V, Xen, or KVM are also not supported for use with the embedded MegaRAID controller.

This server includes an embedded MegaRAID controller hub that can control up to eight SATA-only front-facing drives (SFF 8-drive server only). It can also control up to two internal boot SSDs (SFF 24-drive and LFF 12-drive servers only).

This section contains the following topics:

- Embedded SATA RAID Controller Requirements For Front-Facing Drive Control, page C-9
- Embedded SATA RAID: Two SATA Controllers, page C-10
- Embedded SATA RAID Controller Considerations, page C-11
- Installing a SATA Interposer Board For Front-Facing Drive Control, page C-11
- Installing a Software RAID 5 Key Module for Embedded RAID 5 Support, page C-11
- Enabling the Embedded RAID Controller in the BIOS, page C-12
- Disabling the Embedded RAID Controller in the BIOS, page C-13
- Launching the LSI Embedded MegaRAID Configuration Utilities, page C-13
- Installing LSI MegaSR Drivers For Windows and Linux, page C-14

Embedded SATA RAID Controller Requirements For Front-Facing Drive Control

The embedded SATA RAID controller hub requires the following items:

- For front-facing drive control—The SFF, 8-drive version of the server.

  The embedded RAID option is available for front-facing drive control only with the SFF 8-drive, direct-connect backplane.
- A SATA interposer board and Y-cable (bundled as `UCSC-IP-PCH-C240M4=`).

  This interposer board plugs into the motherboard and provides cable connectors.
- (Optional) A SATA RAID 5 key module.

  This optional module can be installed to a motherboard header to add SATA RAID 5 support for front-facing drives.
- The embedded SATA RAID controller must be enabled in the server BIOS.
- (Optional) LSI MegaSR drivers for Windows or Linux.

Note The embedded SATA RAID controller can also manage internal SSD boot drives in a RAID 1 array. For that case, the requirement is either the LFF 12-drive or the SFF 24-drive version of the server. Only the LFF 12-drive and the SFF 24-drive versions of the server support internal boot SSDs. No cabling is required for managing the internal SSD boot drives.

Embedded SATA RAID: Two SATA Controllers

The embedded RAID Patsburgh controller hub (PCH) is split into two controllers: SATA and sSATA (secondary SATA). These two controllers are seen as separate RAID controllers in the Cisco IMC interface and are configurable separately.

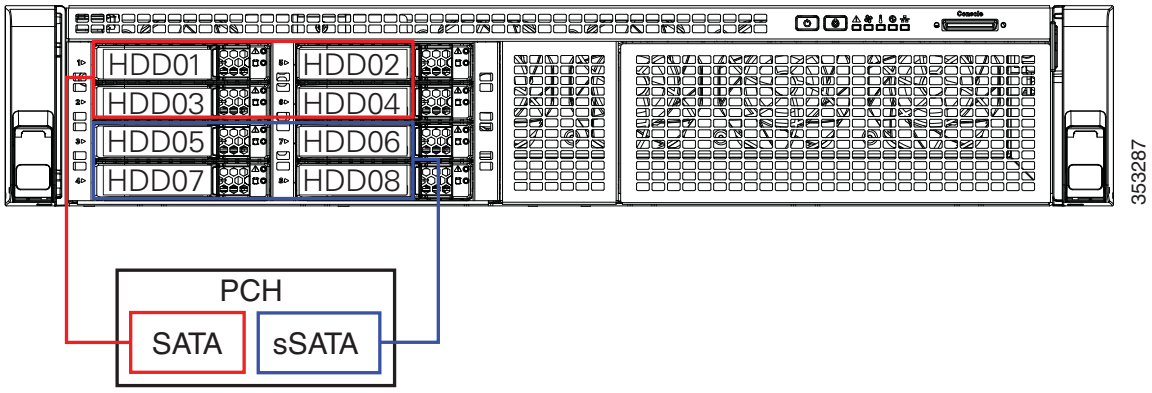
- The first SATA controller controls front-facing drives 1–4; it can also control the two internal SATA SSD boot drives (see Table C-5).
- The secondary sSATA controller controls front-facing drives 5–8 (see Table C-5).

Table C-5 SATA and sSATA Listing of Drives in LSI SW RAID Utilities

SATA	sSATA
0—Front HDD 01	0—Front HDD 05
1—Front HDD 02	1—Front HDD 06
2—Front HDD 03	2—Front HDD 07
3—Front HDD 04	3—Front HDD 08
4—SSD internal boot drive	
5—SSD internal boot drive	

- When configuring RAID groups, you cannot create a group that spans more than four drives.
  - The first SATA controller can control a RAID group of up to four drives, comprised of only front drives 1–4 (see Figure C-2).
  - The first SATA controller can also control a RAID 1 group of the two internal SATA boot drives.
  - The secondary sSATA controller can control a RAID group of up to four drives, comprised of only front drives 5–8 (see Figure C-2).

Figure C-2 Embedded RAID Controller Drive Groups



- See Enabling the Embedded RAID Controller in the BIOS, page C-12 for instructions on enabling the two SATA controllers.
- Each controller is listed separately in the BIOS. You can select the boot order of the controllers in the BIOS (use the **Boot Options** tab in the BIOS Setup Utility).

Note To set the boot order for virtual drives, use the LSI Embedded RAID Configuration Utility (legacy or UEFI version). See Launching the LSI Embedded MegaRAID Configuration Utilities, page C-13.

Embedded SATA RAID Controller Considerations

Note the following considerations for controlling front-facing drives (SFF 8-drive server version only):

- The default setting for this embedded controller hub is SATA RAID 0, 1, and 10 support for up to eight front-facing SATA drives.
- You can upgrade to SATA RAID 0, 1, 5, and 10 support for up to eight front-facing SATA drives (in two groups of four drives) by installing a RAID 5 key module on the motherboard. See Installing a Software RAID 5 Key Module for Embedded RAID 5 Support, page C-11.
- When you order the server with this embedded controller, the controller is enabled in the BIOS. Instructions for enabling the controller are included for the case in which a server is reset to defaults (Disabled). See Enabling the Embedded RAID Controller in the BIOS, page C-12.
- You cannot downgrade from using a HW RAID controller card to using the software RAID embedded controller for front-facing drive control.

Caution Data migration from software RAID (embedded RAID) to HW RAID (a controller card) is *not* supported and could result in data loss. Migrations from software 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.

- The required drivers for this controller are already installed and ready to use with the LSI software RAID Configuration Utility (legacy version or UEFI via the server BIOS). 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-14.

Installing a SATA Interposer Board For Front-Facing Drive Control

The Embedded RAID controller requires a SATA interposer board for front-facing drive control. The RAID cables included connect from this board to the eight-drive, direct-connect backplane.

To install a SATA interposer board, see Replacing a SATA Interposer Board, page 3-29.

Installing a Software RAID 5 Key Module for Embedded RAID 5 Support

The software RAID 5 key module contains a chip on a small circuit board. This module attaches to a two-pin motherboard header. This chip upgrades support to add embedded SATA RAID 5 support for front-facing drive control.

To install a RAID 5 key module, see Replacing a Software RAID 5 Key Module, page 3-37.

Enabling the Embedded RAID Controller in the BIOS

Note The default setting in the BIOS for the embedded controller is disabled.

When you enable this controller, both the primary (SATA) and secondary (sSATA) controllers are enabled.

Enabling SATA Mode and Selecting Option ROM Mode

Step 1 Set the SATA mode for managing the two boot drives:

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

b. Choose the **Advanced** tab, and then choose **LOM and PCIe Slots Configuration**.

c. Select **PCH SATA Mode** and then choose one of the options from the dialog:

- AHCI—Advanced host controller interface. You can manage the internal SSD boot drives by using your operating system's storage management feature.
- Disabled—The embedded RAID controller is disabled.
- LSI SW RAID—In supported server versions, you can manage the internal SSD boot drives or the front-facing drives by using the server's embedded SATA RAID controller. For support by server version, see Support Matrix For Cisco UCS C240 M4 Server RAID Controllers, page C-3.

Note Before you change from LSI SW RAID mode to AHCI mode, delete all the RAID volumes configured in the connected physical drives.

d. If you selected LSI SW RAID mode and you want to set the option ROM mode, continue with the next step. If not, skip to Step 3.

Note There is no option ROM mode in AHCI SATA mode.

Step 2 Optional: Set the SATA option ROM mode for the two boot drives (only with LSI SW RAID SATA mode):

a. Choose the **Advanced** tab, and then choose **LOM and PCIe Slots Configuration**.

b. Select **PCH SATA OPROM Mode** and then choose one of the options from the dialog:

- Enabled—You can boot from these boot drives. You can use the UEFI management interface or the free-standing legacy management utility.
- Disabled—You cannot boot from these boot drives.
- UEFI Only—Select this to enable booting but manage RAID only by using the UEFI version of the LSI utility that is built into the server BIOS. See Launching the LSI Embedded MegaRAID Configuration Utilities, page C-13.
- Legacy Only—Select this enable booting but manage RAID only by using the free-standing version of the LSI utility. See Launching the LSI Embedded MegaRAID Configuration Utilities, page C-13.

Step 3 Press **F10** to save your changes and exit the utility.

Disabling the Embedded RAID Controller in the BIOS

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

Step 2 Select the **Advanced** tab, and then select **LOM and PCIe Slots Configuration**.

Step 3 Set PCH SATA Mode to **Disabled**.

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

Launching the LSI Embedded MegaRAID Configuration Utilities

You can use one of the two LSI utilities:

- Launch the legacy free-standing utility by pressing **Ctrl+M** when you see the prompt during system boot.
- Launch the UEFI version of the LSI utility that is built into the server BIOS as follows:

1. Press **F2** when you see the prompt during system boot to open the BIOS Setup Utility.
2. Select the **Advanced** tab.
3. Open the UEFI utility for the primary (SATA) or the secondary controller (sSATA) by selecting one of the following:
   - LSI SW RAID Configuration Utility (SATA)
   - LSI SW RAID Configuration Utility (sSATA)

Note The secondary SATA (sSATA) UEFI utility is activated only in a SFF 8-drive version of the server where it can be used to control front-facing drives 5–8. It is not used when controlling the internal boot drives in a SFF 24-drive or LFF 12-drive version of the server.

Note These UEFI options are activated only if you have already set the PCH SATA OPROM Mode to Enabled or UEFI Only. See Enabling SATA Mode and Selecting Option ROM Mode, page C-12.

For 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 software RAID 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-14
- Microsoft Windows Driver Installation, page C-15
- Linux Driver Installation, page C-17

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, and 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 describes how to install the LSI MegaSR driver in a Windows installation.

This section contains the following topics:

- Windows Server 2008R2 Driver Installation, page C-15
- Updating the Windows Driver, page C-16
- Linux Driver Installation, page C-17

Windows Server 2008R2 Driver Installation

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 Software RAID Configuration Utility before you install this driver for Windows. Launch this utility by pressing **Ctrl-M** when `LSI SWRAID` is shown during the BIOS POST.

Step 2 Download the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page C-14.

Step 3 Prepare the drivers on a USB thumb drive:

- **a.** Burn the ISO image to a disk.
- **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 installation disk into the drive. Skip to Step 6.
- To install from remote ISO, log in to the server's Cisco IMC interface and continue with the next step.

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

- **a.** Click **Add Image** and browse to select your remote Windows installation ISO file.
- **b.** Check the check box in the Mapped column for the media that you just added, and 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, choose the physical disk 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 box 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 box to browse to the location of the drivers folder on the USB thumb drive, and then 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

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-17
- Preparing Physical Installation Disks For Linux, page C-17
- Installing the Red Hat Linux Driver, page C-19
- Installing the SUSE Linux Enterprise Server Driver, page C-20

Obtaining the Driver Image File

See Downloading the LSI MegaSR Drivers, page C-14 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 Disks For Linux

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

Note The driver image is too large for a floppy disk, so use a USB thumb drive instead.

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

Preparing Physical Installation Disks with the Windows Operating System

Under Windows, you can use the RaWrite floppy image-writer utility to create disk images from image files.

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-14 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 filename 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 Enter 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 Enter: **dud.img**

Step 9 Press **Enter**.

You are prompted for the target disk.

Step 10 Insert a floppy disk into the server and enter: **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 disk.

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 disk utility to create disk images from image files.

Note The driver image is too large for a floppy disk, so use a USB thumb drive instead.

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page C-14 and save it to your Linux system that has a disk 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 USB thumb drive into a port on your Linux system.

Step 5 Create a directory and mount the DUD image to that directory:

mkdir <*destination_folder*>

mount -oloop <*driver_image*> <*destination_folder*>

Step 6 Copy the contents in the directory to your USB thumb drive.

Installing the Red Hat Linux Driver

Note This server supports Red Hat Linux 6.5 or later.

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 Software RAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl-M** when `LSI SWRAID` is shown during the BIOS POST.

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

- To install from a physical disk: Use one of the procedures in Preparing Physical Installation Disks For Linux, page C-17.
  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-14.
  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 installation disk into the drive.
  Then continue with Step 6.
- To install from remote ISO, log in to the server's Cisco IMC interface. Then continue with the next step.

Step 5 Launch a Virtual KVM console window and click 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. Check 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 disk or virtual DVD and press **Enter**.

The RHEL installation begins when the image is booted.

Step 9 Enter one of the following commands at the boot prompt:

- For RHEL 6.*x* (32- and 64-bit), enter:
  linux dd blacklist=isci blacklist=ahci nodmraid noprobe=<ata*drive number*>
- For RHEL 7.x (32- and 64-bit), enter:
  linux dd modprobe.blacklist=ahci nodmraid

Note The **noprobe** values depend on the number of drives. For example, to install RHEL 6.5 on a RAID 5 configuration with three drives, enter
Linux dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2

Step 10 Press **Enter**.

The prompt asks whether you have a driver disk.

Step 11 Use the arrow key to choose **Yes**, and then press **Enter**.

Step 12 Choose **fd0** to indicate that you have a floppy disk with the driver on it.

Step 13 Do one of the following actions:

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

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

Loading megasr driver...

Step 14 Follow the Red Hat Linux installation procedure to complete the installation.

Step 15 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.

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 the BIOS POST.

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

- To install from a physical disk, use one of the procedures in Preparing Physical Installation Disks For Linux, page C-17.
  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-14.
  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 Cisco IMC interface and continue with the next step.

Step 5 Launch a Virtual KVM console window and click 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. Check the check box in the Mapped column for the media that you just added, and 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 disk or virtual DVD and press **Enter**. The SLES installation begins when the image is booted.

Step 9 When the first SLES screen appears, choose **Installation**.

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

- For SLES 11 and SLES 11 SP1 (32- and 64-bit), enter: **brokenmodules=ahci**
- For SLES 11 SP2 (32-and 64-bit), enter: **brokenmodules=ahci brokenmodules=isci**
- For SLES 12, enter: **brokenmodules=ahci**

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

Step 12 Do one of the following actions:

- If you prepared the IMG file on a physical disk in Step 2, insert the USB thumb drive to the target server and then insert the disk in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in Step 5, choose the location of the virtual floppy.

"Yes" appears under the F6 Driver heading.

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

Step 14 Press **OK**.

The following message is displayed: `LSI Soft RAID Driver Updates added.`

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

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

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 3-44.

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 situation can happen if you do not press F quickly enough when prompted. In this case, reboot the server and try the import operation again when 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 that are supported in Cisco servers, see the Cisco UCS Servers RAID Guide.

Full Avago Technologies/LSI documentation is also available:

- For hardware SAS MegaRAID—Avago Technologies/LSI 12 Gb/s MegaRAID SAS Software User's Guide, Rev. F
- For embedded software MegaRAID—LSI Embedded MegaRAID Software User Guide



Installation for Cisco UCS Integration

The Cisco UCS 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.