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 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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1721R)

© 2016–2017 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface xvii
  Audience xvii
  Conventions xvii
  Related Cisco UCS Documentation xix
  Documentation Feedback xix

CHAPTER 1

New and Changed Information 1
  New and Changed Information 1

CHAPTER 2

Server Management Overview 3
  Server Management Overview 3
  Cisco UCS Manager User Documentation 3

CHAPTER 3

Server License Management 5
  Licenses 5
  C-Direct Rack Licensing Support 7
  Obtaining the Host ID for a Fabric Interconnect 8
  Obtaining a License 9
  Downloading Licenses to the Fabric Interconnect from the Local File System 10
  Downloading Licenses to the Fabric Interconnect from a Remote Location 11
  Installing a License 12
  Viewing the Licenses Installed on a Fabric Interconnect 12
  Determining the Grace Period Available for a Port or Feature 13
  Determining the Expiry Date of a License 13
  Uninstalling a License 13
CHAPTER 4

Registering Cisco UCS Domains with Cisco UCS Central 15
  Registration of Cisco UCS Domains 15
  Policy Resolution between Cisco UCS Manager and Cisco UCS Central 15
  Registering a Cisco UCS Domain with Cisco UCS Central 17
  Configuring Policy Resolutions between Cisco UCS Manager and Cisco UCS Central 18
  Setting Cisco UCS Central Registration Properties in Cisco UCS Manager 18
  Unregistering a Cisco UCS Domain from Cisco UCS Central 19

CHAPTER 5

Power Capping and Power Management in Cisco UCS 21
  Power Capping in Cisco UCS 22
  Power Policy Configuration 22
  Power Policy for Cisco UCS Servers 22
  Configuring the Power Policy 23
  Power Supply for Redundancy Method 23
  Configuring Policy Driven Chassis Group Power Capping 24
  Policy Driven Chassis Group Power Capping 24
  Power Control Policy 24
    Creating a Power Control Policy 24
    Deleting a Power Control Policy 26
  Power Groups in UCS Manager 27
    Creating a Power Group 29
    Adding a Chassis to a Power Group 30
    Removing a Chassis from a Power Group 31
    Deleting a Power Group 31
  Blade Level Power Capping 31
  Manual Blade Level Power Cap 31
  Setting the Blade-Level Power Cap for a Server 32
  Viewing the Blade-Level Power Cap 33
  Global Power Profiling Policy Configuration 33
  Global Power Profiling Policy 33
  Configuring the Global Power Profile Policy 34
  Global Power Allocation Policy Configuration 34
  Global Power Allocation Policy 34
Configuring the Global Power Allocation Policy 34
Power Management During Power-on Operations 35
Power Sync Policy Configuration 36
Power Sync Policy 36
Power Synchronization Behavior 36
Creating a Power Sync Policy 37
Changing a Power Sync Policy 38
Deleting a Power Sync Policy 39
Rack Server Power Management 39
UCS Mini Power Management 39

CHAPTER 6  Blade Server Hardware Management 41
Blade Server Management 41
   Guidelines for Removing and Decommissioning Blade Servers 42
   Recommendations for Avoiding Unexpected Server Power Changes 42
Booting a Blade Server 43
Booting a Rack-Mount Server from the Service Profile 44
Determining the Boot Order of a Blade Server 44
Shutting Down a Blade Server 45
Shutting Down a Server from the Service Profile 45
Resetting a Blade Server 46
Resetting a Blade Server to Factory Default Settings 46
Reacknowledging a Blade Server 47
Removing a Server from a Chassis 48
Deleting the Inband Configuration from a Blade Server 48
Decommissioning a Blade Server 49
Removing a Non-Existent Blade Server Entry 49
Recommissioning a Blade Server 50
Reacknowledging a Server Slot in a Chassis 50
Removing a Non-Existent Blade Server from the Configuration Database 51
Turning the Locator LED for a Blade Server On and Off 51
Turning the Local Disk Locator LED on a Blade Server On and Off 52
Resetting the CMOS for a Blade Server 52
Resetting the CIMC for a Blade Server 53
Clearing TPM for a Blade Server 53
Viewing the POST Results for a Blade Server 54
Issuing an NMI from a Blade Server 54
Viewing Health Events for a Blade Server 55
Health LED Alarms 56
  Viewing Health LED Alarms 57
Smart SSD 57
  Monitoring SSD Health 58

CHAPTER 7

Rack-Mount Server Hardware Management 59

  Rack-Mount Server Management 59
Guidelines for Removing and Decommissioning Rack-Mount Servers 60
Recommendations for Avoiding Unexpected Server Power Changes 60
Booting a Rack-Mount Server 61
Booting a Rack-Mount Server from the Service Profile 62
Determining the Boot Order of a Rack-Mount Server 62
Shutting Down a Rack-Mount Server 63
Shutting Down a Server from the Service Profile 63
Resetting a Rack-Mount Server 64
Resetting a Rack-Mount Server to Factory Default Settings 64
Reacknowledging a Rack-Mount Server 65
Deleting the Inband Configuration from a Rack-Mount Server 66
Decommissioning a Rack-Mount Server 66
Recommissioning a Rack-Mount Server 67
Renumbering a Rack-Mount Server 67
Removing a Non-Existent Rack-Mount Server from the Configuration Database 68
Turning the Locator LED for a Rack-Mount Server On and Off 68
Turning the Local Disk Locator LED on a Rack-Mount Server On and Off 69
Resetting the CMOS for a Rack-Mount Server 69
Resetting the CIMC for a Rack-Mount Server 70
Clearing TPM for a Rack-Mount Server 70
Issuing an NMI from a Rack-Mount Server 71
Viewing Health Events for a Rack-Mount Server 71
Viewing the POST Results for a Rack-Mount Server 73
CHAPTER 8

Compute Cartridge Hardware Management 75
Compute Cartridges 75
Removing a Cartridge 75
Acknowledging a Cartridge Slot in a Chassis 75

CHAPTER 9

Modular Server Hardware Management 77
Modular Server Management 77
Booting a Modular Server 77
Booting a Rack-Mount Server from the Service Profile 78
Determining the Boot Order of a Modular Server 78
Shutting Down a Modular Server 79
Shutting Down a Server from the Service Profile 79
Resetting a Modular Server 80
Reacknowledging a Modular Server 80
Deleting the Inband Configuration from a Modular Server 81
Recommissioning a Server 81
Recommissioning a Modular Server 82
Turning the Locator LED for a Server On and Off 82
Turning the Local Disk Locator LED on a Modular Server On and Off 83
Resetting the CMOS for a Modular Server 83
Resetting the CIMC for a Modular Server 84
Issuing an NMI from a Server 84
Viewing Health Events on a Server 85
Health LED Alarms 86
Viewing Health LED Alarms 87
Viewing the POST Results for a Modular Server 87

CHAPTER 10

S3X60 Server Node Hardware Management 89
Cisco UCS S3260 Server Node Management 89
Booting a Cisco UCS S3260 Server Node 90
Booting a Cisco UCS S3260 Server Node from the Service Profile 90
Determining the Boot Order of a Cisco UCS S3260 Server Node 90
Shutting Down a Cisco UCS S3260 Server Node 91
Shutting Down a Cisco UCS S3260 Server Node from the Service Profile 91
Resetting a Cisco UCS S3260 Server Node 92
Resetting a Cisco UCS S3260 Server Node to Factory Default Settings 93
Reacknowledging a Cisco UCS S3260 Server Node 94
Removing a Cisco UCS S3260 Server Node from a Chassis 94
Deleting the Inband Configuration from a Cisco UCS S3260 Server Node 95
Deecommissioning a Cisco UCS S3260 Server Node 95
Recommissioning a Cisco UCS S3260 Server Node 96
Reacknowledging a Server Slot in a S3260 Chassis 96
Removing a Non-Existent Cisco UCS S3260 Server Node from the Configuration Database 97
Turning the Locator LED for a Cisco UCS S3260 Server Node On and Off 97
Turning the Local Disk Locator LED on a Cisco UCS S3260 Server Node On and Off 98
Resetting the CIMC for a Cisco UCS S3260 Server Node 98
Resetting the CMOS for a Cisco UCS S3260 Server Node 99
Issuing an NMI from a Cisco UCS S3260 Server Node 99
Viewing the POST Results for a Cisco UCS S3260 Server Node 100
Viewing Health Events for a Cisco UCS S3260 Server Node 100
Health LED Alarms 102
Viewing Health LED Alarms 102

CHAPTER 11  103
Server Pools 103
Configuring Server Pools 103
Server Pools 103
Creating a Server Pool 103
Deleting a Server Pool 104
Adding Servers to a Server Pool 104
Removing Servers from a Server Pool 105
Configuring UUID Suffix Pools 105
UUID Suffix Pools 105
Creating a UUID Suffix Pool 105
Deleting a UUID Suffix Pool 107
Configuring IP Pools 107
IP Pools 107
Creating an IP Pool 108
Adding a Block to an IP Pool 109
Deleting a Block from an IP Pool 111
Deleting an IP Pool 111

CHAPTER 12

Server Boot 113
Boot Policy 113
UEFI Boot Mode 114
UEFI Secure Boot 115
CIMC Secure Boot 115
Determining the CIMC Secure Boot Status 116
Enabling CIMC Secure Boot on a Rack Server 116
Creating a Boot Policy 117
SAN Boot 118
Configuring a SAN Boot for a Boot Policy 118
iSCSI Boot 119
iSCSI Boot Process 120
iSCSI Boot Guidelines and Prerequisites 120
Initiator IQN Configuration 122
Enabling MPIO on Windows 122
Configuring iSCSI Boot 123
Creating an iSCSI Adapter Policy 124
Deleting an iSCSI Adapter Policy 126
Creating an iSCSI Authentication Profile 126
Deleting an iSCSI Authentication Profile 127
Creating an iSCSI Initiator IP Pool 127
Creating an iSCSI Boot Policy 128
Creating an iSCSI vNIC for a Service Profile 129
Deleting an iSCSI vNIC from a Service Profile 131
Setting the Initiator IQN at the Service Profile Level 131
Changing the Initiator IQN at the Service Profile Level 132
Setting iSCSI Boot Parameters 132
Modifying iSCSI Boot Parameters 135
IQN Pools 140
Creating a vNIC for a Service Profile 164
Deleting a vNIC from a Service Profile 164
Creating a vHBA for a Service Profile 165
Changing the WWPN for a vHBA 165
Clearing Persistent Binding for a vHBA 166
Deleting a vHBA from a Service Profile 166
Adding a vHBA Initiator Group to a Service Profile 166
Deleting a Service Profile 168

Service Profile Association 169
Associating a Service Profile with a Server or Server Pool 169
Disassociating a Service Profile from a Server or Server Pool 170

Service Profile Templates 170
Initial and Existing Templates 170
Creating a Service Profile Template 171
Creating One or More Service Profiles from a Service Profile Template 172
Creating a Template Based Service Profile for a Blade Server 172
Creating a Template Based Service Profile for a Rack-Mount Server 173
Creating a Service Profile Template from a Service Profile 174
Setting an Asset Tag for a Service Profile 174

Service Profile Template Tasks 174
Binding a Service Profile to a Service Profile Template 174
Unbinding a Service Profile from a Service Profile Template 175
Changing the UUID in a Service Profile Template 175
Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template 176
Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template 177
Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template 178
Deleting the Inband Configuration from a Service Profile Template 178

Service Profile Association 179
Associating a Service Profile with a Server or Server Pool 179
Associating a Service Profile Template with a Server Pool 180
Disassociating a Service Profile from a Server or Server Pool 180
Disassociating a Service Profile Template from its Server Pool 181

CHAPTER 14  Server-Related Policies 183
## BIOS Settings

183

- **Server BIOS Settings** 183
  - **Main BIOS Settings** 184
  - **Processor BIOS Settings** 186
  - **Intel Directed I/O BIOS Settings** 207
  - **RAS Memory BIOS Settings** 208
  - **Serial Port BIOS Settings** 210
  - **USB BIOS Settings** 211
  - **PCI Configuration BIOS Settings** 215
  - **QPI BIOS Settings** 217
  - **LOM and PCIe Slots BIOS Settings** 217
  - **Graphics Configuration BIOS Settings** 227
  - **Boot Options BIOS Settings** 227
  - **Server Management BIOS Settings** 230

- **BIOS Policy** 236
  - **Default BIOS Settings** 237
  - **Creating a BIOS Policy** 237
  - **Modifying the BIOS Defaults** 238
  - **Viewing the Actual BIOS Settings for a Server** 239

## Trusted Platform Module

239

- **Trusted Platform Module** 239
  - **Intel Trusted Execution Technology** 240
  - **Configuring Trusted Platform** 240
  - **Configuring Trusted Platform** 241
  - **Viewing TPM Properties** 242

## Consistent Device Naming

242

- **Guidelines and Limitations for Consistent Device Naming** 242
- **Configuring Consistent Device Naming in a BIOS Policy** 245
- **Configuring a CDN Name for a vNIC** 245

## CIMC Security Policies

246

- **IPMI Access Profile** 246
- **Creating an IPMI Access Profile** 246
- **Deleting an IPMI Access Profile** 247
- **KVM Management Policy** 248
Creating a KVM Management Policy 248

Graphics Card Policies 248
  Creating a Graphics Card Policy 249

Local Disk Policies 249
  Local Disk Configuration Policy 249
  Guidelines for all Local Disk Configuration Policies 250
  Guidelines for Local Disk Configuration Policies Configured for RAID 251
  Creating a Local Disk Configuration Policy 253
  Changing a Local Disk Configuration Policy 256
  Deleting a Local Disk Configuration Policy 256

FlexFlash Support 257
  FlexFlash FX3S Support 259
  Starting Up Blade Servers with FlexFlash SD Cards 260
  Enabling FlexFlash SD Card Support 261
  Enabling Auto-Sync 261
  Formatting the SD Cards 262
  Resetting the FlexFlash Controller 262

Scrub Policy 262
  Scrub Policy Settings 262
  Creating a Scrub Policy 263
  Deleting a Scrub Policy 264

DIMM Error Management 265
  DIMM Correctable Error Handling 265
  Resetting Memory Errors 265
  DIMM Blacklisting 265
    Enabling DIMM Blacklisting 265

Serial over LAN Policy Settings 267
  Serial over LAN Policy Overview 267
  Creating a Serial over LAN Policy 267
  Deleting a Serial over LAN Policy 268

Server Autoconfiguration Policies 268
  Server Autoconfiguration Policy Overview 268
  Creating an Autoconfiguration Policy 269
  Deleting an Autoconfiguration Policy 270
Server Discovery Policy Settings 270
Server Discovery Policy Overview 270
Creating a Server Discovery Policy 271
Deleting a Server Discovery Policy 272
Hardware Change Discovery Policy 272
Configuring Hardware Change Discovery Policy 272
Server Inheritance Policy Settings 273
Server Inheritance Policy Overview 273
Creating a Server Inheritance Policy 273
Deleting a Server Inheritance Policy 274
Server Pool Policy Settings 274
Server Pool Policy Overview 274
Creating a Server Pool Policy 274
Deleting a Server Pool Policy 275
Server Pool Policy Qualifications Settings 276
Server Pool Policy Qualification Overview 276
Creating Server Pool Policy Qualifications 276
Deleting Server Pool Policy Qualifications 281
Deleting Qualifications from Server Pool Policy Qualifications 281
vNIC/vHBA Placement Policy Settings 281
vNIC/vHBA Placement Policies 281
vCon to Adapter Placement 282
For N20-B6620-2 and N20-B6625-2 Blade Servers 283
For All Other Supported Servers 283
vNIC/vHBA to vCon Assignment 284
Creating a vNIC/vHBA Placement Policy 286
Deleting a vNIC/vHBA Placement Policy 288
Explicitly Assigning a vNIC to a vCon 288
Explicitly Assigning a vHBA to a vCon 290
Placing Static vNICs Before Dynamic vNICs 291
vNIC/vHBA Host Port Placement 293
Configuring Host Port Placement 293
CIMC Mounted vMedia 293
Creating a vMedia Policy 294
Adding a vMedia Policy to a Service Profile 297
Viewing CIMC vMedia Policy 299

CHAPTER 15  
Firmware Upgrades 301
   Firmware Upgrades 301
   Verifying Firmware Versions on Components 301

CHAPTER 16  
Diagnostics Configuration 303
   Overview of Cisco UCS Manager Diagnostics 303
   Creating a Diagnostics Policy 303
   Diagnostics Test on a Blade Server 304
      Starting a Diagnostics Test on a Blade Server 304
      Stopping a Diagnostics Test on a Blade Server 305
   Starting a Diagnostics Tests on All Servers 305
   Stopping a Diagnostics Tests on All Servers 306
   Viewing the Server Diagnostics Status/Result 306
   Diagnostics Troubleshooting 307
Preface

• Audience, on page xvii
• Conventions, on page xvii
• Related Cisco UCS Documentation, on page xix
• Documentation Feedback, on page xix

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

• Server administration
• Storage administration
• Network administration
• Network security

Conventions

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>GUI elements such as tab titles, area names, and field labels appear in this font.</td>
</tr>
<tr>
<td></td>
<td>Main titles such as window, dialog box, and wizard titles appear in this font.</td>
</tr>
<tr>
<td>TUI elements</td>
<td>In a Text-based User Interface, text the system displays appears in this font.</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in this font.</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in this font.</td>
</tr>
<tr>
<td></td>
<td>Variables in a CLI command appear in this font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>Text Type</td>
<td>Indication</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

Note

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

Tip

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

Timesaver

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

Caution

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

Warning

IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS
Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the Cisco UCS B-Series Servers Documentation Roadmap available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the Cisco UCS C-Series Servers Documentation Roadmap available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

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

- New and Changed Information, on page 1

New and Changed Information

This section provides information on new features and changed behavior in Cisco UCS Manager, Release 3.1 (x).

**New Features and Changed Behavior in Cisco UCS Manager, Release 3.1 (3)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom User Label – Asset Tag</td>
<td>Service profiles now have a customer label field that is visible to the operating system or hypervisor running on the server through the SMBIOS asset tag field.</td>
<td>Setting an Asset Tag for a Service Profile, on page 174</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>The Cisco UCS Manager diagnostics tool enables you to verify the health of the hardware components on your servers.</td>
<td>Overview of Cisco UCS Manager Diagnostics, on page 303</td>
</tr>
<tr>
<td>Hardware Change Discovery Policy</td>
<td>When UCSM detects any change in the server hardware component, a critical “hardware inventory mismatch” fault is raised. You must acknowledge the server to clear the fault and complete the hardware inventory.</td>
<td>Hardware Change Discovery Policy, on page 272</td>
</tr>
</tbody>
</table>
### New and Changed Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Transition Log</td>
<td>The Power Transition Log was added which logs the last five server power transitions, the power transition source timestamp of the latest power transition, and the count of the last consecutive server power transitions from the same source.</td>
<td>Viewing the Power Transition Log, on page 73</td>
</tr>
<tr>
<td>Graphics Card Policies</td>
<td>This release extends graphics card support to include the ability to change the graphics card mode from a graphics card policy.</td>
<td>Graphics Card Policies, on page 248</td>
</tr>
<tr>
<td>Smart SSD</td>
<td>Cisco UCS Manager supports monitoring SSD health. This feature is called Smart SSD.</td>
<td>Smart SSD, on page 57</td>
</tr>
</tbody>
</table>

### New Features and Changed Behavior in Cisco UCS Manager, Release 3.1 (2)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated Power Sync Policy</td>
<td>Cisco UCS Manager does not power on the blade server after shallow discovery when the power state for a service profile is set to ON.</td>
<td>Power Sync Policy, on page 36</td>
</tr>
</tbody>
</table>
Server Management Overview

Cisco UCS Manager enables you to manage general and complex server deployments. For example, you can manage a general deployment with a pair of Fabric Interconnects (FIs), which is the redundant server access layer that you get with the first chassis that can scale up to 20 chassis' and up to 160 physical servers. This can be a combination of blades and rack mount servers to support the workload in your environment. As you add more servers, you can continue to perform server provisioning, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, and auditing.

By default, the Cisco UCS 6332 40 GB FIs, the UCS Mini 6324 40 GB FIs, and the UCS 6200 Series 10 GB FIs include centralized management. You can manage the UCS Blade Servers and Rack-Mount Servers that are in the same domain from one console. You can also manage the UCS Mini from the Cisco UCS Manager.

To ensure the optimum server performance, you can configure the amount of power that you allocate to servers. You can also set the server boot policy, the location from which the server boots, and the order in which the boot devices are invoked. You can create service profiles for the UCS B-Series Blade Servers and the UCS Mini to assign to servers. Service profiles enable you to assign BIOS settings, security settings, the number of vNICs and vHBAs, and anything else that you want to apply to a server.

Cisco UCS Manager User Documentation

Cisco UCS Manager offers you a new set of smaller, use-case based documentation described in the following table:

<table>
<thead>
<tr>
<th>Guide</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Manager Getting Started Guide</td>
<td>Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration and configuration best practices.</td>
</tr>
<tr>
<td>Guide</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco UCS Manager Administration Guide</td>
<td>Discusses password management, role-based access configuration, remote authentication, communication services, CIMC session management, organizations, backup and restore, scheduling options, BIOS tokens, and deferred deployments.</td>
</tr>
<tr>
<td>Cisco UCS Manager Infrastructure Management Guide</td>
<td>Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.</td>
</tr>
<tr>
<td>Cisco UCS Manager Firmware Management Guide</td>
<td>Discusses downloading and managing firmware, upgrading through Auto Install, upgrading through service profiles, directly upgrading at endpoints using firmware auto sync, managing the capability catalog, deployment scenarios, and troubleshooting.</td>
</tr>
<tr>
<td>Cisco UCS Manager Server Management Guide</td>
<td>Discusses the new licenses, registering Cisco UCS domain with Cisco UCS Central, power capping, server boot, server profiles, and server-related policies.</td>
</tr>
<tr>
<td>Cisco UCS Manager Storage Management Guide</td>
<td>Discusses all aspects of storage management, such as SAN and VSAN in Cisco UCS Manager.</td>
</tr>
<tr>
<td>Cisco UCS Manager Network Management Guide</td>
<td>Discusses all aspects of network management, such as LAN and VLAN connectivity in Cisco UCS Manager.</td>
</tr>
<tr>
<td>Cisco UCS Manager System Monitoring Guide</td>
<td>Discusses all aspects of system and health monitoring, including system statistics in Cisco UCS Manager.</td>
</tr>
</tbody>
</table>
Server License Management

- Licenses, on page 5
- C-Direct Rack Licensing Support, on page 7
- Obtaining the Host ID for a Fabric Interconnect, on page 8
- Obtaining a License, on page 9
- Downloading Licenses to the Fabric Interconnect from the Local File System, on page 10
- Downloading Licenses to the Fabric Interconnect from a Remote Location, on page 11
- Installing a License, on page 12
- Viewing the Licenses Installed on a Fabric Interconnect, on page 12
- Determining the Grace Period Available for a Port or Feature, on page 13
- Determining the Expiry Date of a License, on page 13
- Uninstalling a License, on page 13

Licenses

Each Cisco UCS fabric interconnect comes with several port licenses that are factory installed and shipped with the hardware. You can purchase fabric interconnects fully licensed or partially licensed. You can also purchase additional licenses after delivery.

The following four new licenses are added for the 6300 Series FI and are only valid on the 6332 and 6332-16UP FIs.

- 40G_ETH_PORT_ACTIVATION_PKG – Licenses used for 40 GB Ethernet ports
- 40G_ETH_C_PORT_ACTIVATION_PKG – Licenses used for 40 GB Ethernet ports directly connected to rack servers (C-Direct)
- 10G_C_PORT_ACTIVATION_PKG – Licenses used for the first 16 10 GB unified ports on the 6332-16UP that are directly connected to rack servers (C-Direct)
- 10G_PORT_ACTIVATION_PKG – Licenses used for the first 16 10 GB unified ports on the 6332-16UP

Note

The 10G_PORT_ACTIVATION_PKG and 10G_C_PORT_ACTIVATION_PKG licenses are only valid for the 6332-16UP FIs, and can only be installed on them.
The following licenses are used when S3260 system is connected to FI as appliance (appliance port) or Cisco UCS Manager managed node (server port):

**Table 1: S3260 system License Requirement**

<table>
<thead>
<tr>
<th>FI Model</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>6200</td>
<td>ETH_PORT_ACTIVATION_PKG</td>
</tr>
<tr>
<td>6332</td>
<td>40G_ETH_PORT_ACTIVATION_PKG</td>
</tr>
<tr>
<td>6332-16UP</td>
<td>10G_PORT_ACTIVATION_PKG</td>
</tr>
</tbody>
</table>

At a minimum, each fabric interconnect ships with the following counted licenses pre-installed:

<table>
<thead>
<tr>
<th>Fabric Interconnect</th>
<th>Default Base Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS 6248 (unified ports)</td>
<td>For the 12 first enabled Ethernet ports and any Fibre Channel ports in the expansion module.</td>
</tr>
<tr>
<td>Cisco UCS 6296 (unified ports)</td>
<td>For the first 18 enabled Ethernet ports and any Fibre Channel ports in the expansion module.</td>
</tr>
<tr>
<td>Cisco UCS 6324</td>
<td>For 4 non-breakout ports only. The fifth port, which does not include a license, is further broken in to four 10 GB ports.</td>
</tr>
<tr>
<td>Cisco UCS 6332 16UP</td>
<td>For four 40 GB ports and eight 10 GB ports.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The first 16 ports are 10 GB. The remaining are 40 GB.</td>
</tr>
<tr>
<td>Cisco UCS 6332</td>
<td>For eight 40 GB ports.</td>
</tr>
</tbody>
</table>

**Port License Consumption**

Port licenses are not bound to physical ports. When you disable a licensed port, that license is retained for use with the next enabled port. To use additional fixed ports, you must purchase and install licenses for those ports. All ports, regardless of their type (fibre, Ethernet) consume licenses if they are enabled.

For breakout capable ports available in the 6332 and the 6332-16UP platforms, 40 GB licenses remain applied to the main port even if that port is a breakout port, and that port continues to consume only one 40 GB license.

---

**Note**

The initial configuration of a port will enable it, and consume a license.

---

**Important**

Licenses are not portable across product generations. Licenses purchased for 6200 series fabric interconnects cannot be used to enable ports on 6300 series fabric interconnects or vice-versa.
Each Cisco UCS 6324 Fabric Interconnect comes with a factory installed port license that is shipped with the hardware. This license is for the eight 40 GB unified ports, and can be used for any supported purpose. The C-direct port license is factory installed with a grace period, and can be used for Cisco UCS rack servers.

**Grace Period**

If you attempt to use a port that does not have an installed license, Cisco UCS initiates a 120 day grace period. The grace period is measured from the first use of the port without a license and is paused when a valid license file is installed. The amount of time used in the grace period is retained by the system.

---

**Note**

Each physical port has its own grace period. Initiating the grace period on a single port does not initiate the grace period for all ports.

---

If a licensed port is unconfigured, that license is transferred to a port functioning within a grace period. If multiple ports are acting within grace periods, the license is moved to the port whose grace period is closest to expiring.

**High Availability Configurations**

To avoid inconsistencies during failover, we recommend that both fabric interconnects in the cluster have the same number of ports licensed. If symmetry is not maintained and failover occurs, Cisco UCS enables the missing licenses and initiates the grace period for each port being used on the failover node.

---

**C-Direct Rack Licensing Support**

**Release 3.2(3k) and Earlier**

Each Cisco UCS fabric interconnect is shipped with a default number of port licenses that are factory licensed and shipped with the hardware. C-direct support is only applicable on ports that are connected to the rack servers. The 10G_C_PORT_ACTIVATION_PKG and the 40G_ETH_C_PORT_ACTIVATION_PKG are added to the existing license package with all the same properties as the existing licensing feature. The **Subordinate Quantity** property is added to the 10G_PORT_ACTIVATION_PKG and 40G_ETH_PORT_ACTIVATION_PKG to track ports connected to rack servers.

The License Tab in the Cisco UCS Manager GUI displays the new license and the **Subordinate Quantity** for the license. You can also use the `show feature` and `show usage` commands under `scope license` to view the license feature, the vendor version type, and the grace period for each license.

Ports connected to rack servers can use existing 10G_PORT_ACTIVATION_PKG, 40G_ETH_PORT_ACTIVATION_PKG if the license is available or if the license is not in use. Otherwise, you must purchase a 10G_C_PORT_ACTIVATION_PKG, the 40G_ETH_C_PORT_ACTIVATION_PKG to avoid the license grace period.

There is no change in the 10 GB ports. The 10G_PORT_ACTIVATION_PKG and 10G_C_PORT_ACTIVATION_PKG license packages include all of the same properties as the existing the ETH_PORT_ACTIVATION_PKG and the ETH_PORT_C_ACTIVATION_PKG license features.
Configuration and Restrictions

- The C-Direct rack licensing feature accounts for the rack server ports that are directly connected to the FI, but not to a CIMC port. The default quantity for the 10G_C_PORT_ACTIVATION_PKG and the 40G_ETH_C_PORT_ACTIVATION_PKG is always 0.

- When a 40 GB port, or a breakout port under a 40 GB breakout port is enabled without any connections, this port is allotted a license under the 40G_ETH_PORT_ACTIVATION_PKG, if available. If this port is connected to a Direct-Connect rack server after a time lag, it triggers a complete re-allocation of licenses, then this port passes through one of the following license allocation scenarios occurs:

  When you enable a breakout port under a 40 GB breakout port, if that port is connected to a Direct-Connect rack server, and the 40G_C_PORT_ACTIVATION_PKG license files are installed on the FI, the following license allocation occurs:
  - If no other ports under the breakout port are enabled, the parent 40 GB port is allotted a license under the 40G_C_PORT_ACTIVATION_PKG, and the used quantity is incremented for this instance.
  - If other ports are enabled, and if at least one port is not connected to a Direct Connect rack server, even if the port is not being used, the parent 40 GB port is allotted a license under the 40G_ETH_PORT_ACTIVATION_PKG, and the used quantity is incremented for this instance.

- When you enable a breakout port under a 40 GB breakout port and that port is connected to a Direct-Connect rack server, and the 40G_C_PORT_ACTIVATION_PKG license files are not installed on the FI, the following license allocation occurs:
  - If no ports under the breakout port are enabled, the parent 40 GB port is allotted a license under the 40G_ETH_PORT_ACTIVATION_PKG. The subordinate quantity is increased if the licenses are available in the 40G_ETH_PORT_ACTIVATION_PKG. If the licenses are not available, the used quantity under this feature is increased and the entire port goes into the grace period.
  - If other ports are enabled and at least one port is not connected to a Direct Connect rack server, even if the port is not being used, the parent 40 GB port is allotted a license under the 40G_ETH_PORT_ACTIVATION_PKG, and the used quantity is incremented for this instance.

Obtaining the Host ID for a Fabric Interconnect

The host ID is also known as the serial number.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Fabric Interconnects.
Step 3  Click the node for the fabric interconnect for which you want to obtain the host ID.
Step 4  In the Work pane, click the General tab.
Step 5
In the Properties area, the host ID is listed in the Serial Number (SN) field.

What to do next
Obtain the required licenses from Cisco.

Obtaining a License

Note
This process may change after the release of this document. If one or more of these steps no longer applies, contact your Cisco representative for information on how to obtain a license file.

Before you begin
Obtain the following:
• Host ID or serial number for the fabric interconnect
• Claim certificate or other proof of purchase document for the fabric interconnect or expansion module

Procedure

Step 1
Obtain the product authorization key (PAK) from the claim certificate or other proof of purchase document.

Step 2
Locate the website URL in the claim certificate or proof of purchase document.

Step 3
Access the website URL for the fabric interconnect and enter the serial number and the PAK. Cisco sends you the license file by email. The license file is digitally signed to authorize use on only the requested fabric interconnect. The requested features are also enabled once Cisco UCS Manager accesses the license file.

What to do next
Install the license on the fabric interconnect.
Downloading Licenses to the Fabric Interconnect from the Local File System

In a cluster setup, Cisco recommends that you download and install licenses to both fabric interconnects in matching pairs. An individual license is only downloaded to the fabric interconnect that is used to initiate the download.

**Before you begin**

Obtain the required licenses from Cisco.

**Procedure**

1. In the Navigation pane, click **Admin**.
2. Expand **All > License Management**.
3. Click the node for the fabric interconnect to which you want to download the license.
4. In the **Work** pane, click the **Download Tasks** tab.
5. Click **Download License**.
6. In the **Download License** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.
7. In the **Filename** field, type the full path and name of the license file.
   
   You cannot have spaces anywhere in the path name or the file name. For example, `c:\Path\Folder_Name\License.lic` is a valid path, but `c:\Path\Folder Name\License.lic` is invalid due to the space in "Folder Name".

   If you do not know the exact path to the folder where the license file is located, click **Browse** and navigate to the file.
8. Click **OK**.

   Cisco UCS Manager GUI begins downloading the license to the fabric interconnect.
9. (Optional) Monitor the status of the download on the **Download Tasks** tab.

   **Note** If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect, click **Equipment**, and expand the **Local Storage Information** area on the **General** tab.

10. Repeat this task until all the required licenses have been downloaded to the fabric interconnect.
What to do next
After all of the download tasks complete, install the licenses.

Downloading Licenses to the Fabric Interconnect from a Remote Location

Note
In a cluster setup, Cisco recommends that you download and install licenses to both fabric interconnects in matching pairs. An individual license is only downloaded to the fabric interconnect that is used to initiate the download.

Before you begin
Obtain the required licenses from Cisco.

Procedure

Step 1
In the Navigation pane, click Admin.

Step 2
Expand All > License Management.

Step 3
Click the node for the fabric interconnect to which you want to download the license.

Step 4
In the Work pane, click the Download Tasks tab.

Step 5
Click Download License.

Step 6
In the Download License dialog box, click the Remote File System radio button in the Location of the Image File field.

Step 7
Specify the protocol, and enter the required information.

You cannot have spaces anywhere in the path name or the file name. For example, 
c:\Path\Folder_Name\License.lic is a valid path, but c:\Path\Folder Name\License.lic is invalid due to the space in "Folder Name".

Note
If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.

Step 8
Click OK.
Cisco UCS Manager GUI begins downloading the license to the fabric interconnect.

Step 9
(Optional) Monitor the status of the download on the Download Tasks tab.

Note
If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the Packages tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect, click Equipment, and expand the Local Storage Information area on the General tab.
Step 10
Repeat this task until all the required licenses have been downloaded to the fabric interconnect.

What to do next
After all of the download tasks complete, install the licenses.

Installing a License

Before you begin
Obtain the required licenses from Cisco.

Procedure

Step 1 In the Navigation pane, click Admin.
Step 2 Expand All > License Management.
Step 3 In the Work pane, click the Downloaded License Files tab.
Step 4 Choose the license you want to install from the table.

Note There is no downtime required or impact to traffic when installing a new port license.

Step 5 Click the Install License button.
Step 6 In the Install License dialog box, click Yes.
Cisco UCS Manager GUI installs the license and activates the unlicensed port or feature.

Viewing the Licenses Installed on a Fabric Interconnect

Procedure

Step 1 In the Navigation pane, click Admin.
Step 2 Expand All > License Management.
Step 3 In the Work pane, click the Installed Licenses tab to view the details of all licenses installed on the fabric interconnect.
Step 4 Click a license in the table to view the details of that license in the Contents tab.
You may need to expand the license file to view the details of individual licenses in the file.
Determining the Grace Period Available for a Port or Feature

**Procedure**

- **Step 1** In the Navigation pane, click Admin.
- **Step 2** Expand All > License Management.
- **Step 3** In the Work pane, click the General tab.
- **Step 4** Click a feature in the table to view details for that feature, including the operational state and used grace period.

Determining the Expiry Date of a License

**Procedure**

- **Step 1** In the Navigation pane, click Admin.
- **Step 2** Expand All > License Management.
- **Step 3** In the Work pane, click the Installed Licenses tab.
- **Step 4** Click a license in the table to view the details of that license in the Contents tab below.
- **Step 5** In the Contents tab, expand the license file to view all licenses in the file.
- **Step 6** In the Expiry column, view the expiry date of the license.

Uninstalling a License

**Note**

Permanent licenses cannot be uninstalled if they are in use. You can only uninstall a permanent license that is not in use. If you try to delete a permanent license that is being used, Cisco UCS Manager rejects the request and display an error message.

**Before you begin**

Back up the Cisco UCS Manager configuration.

**Procedure**

- **Step 1** In the Navigation pane, click Admin.
Step 2  Expand All > License Management.
Step 3  In the Work pane, click the Installed Licenses tab.
Step 4  Choose the license you want to uninstall from the table.
Step 5  Click the Clear License button.
Step 6  If a confirmation dialog box displays, click Yes.

Cisco UCS Manager deactivates the license, removes the license from the list of licenses, and deletes the license from the fabric interconnect. The port is moved into unlicensed mode. In a cluster setup, you must uninstall the license from the other fabric interconnect.
Chapter 4

Registering Cisco UCS Domains with Cisco UCS Central

- Registration of Cisco UCS Domains, on page 15
- Policy Resolution between Cisco UCS Manager and Cisco UCS Central, on page 15
- Registering a Cisco UCS Domain with Cisco UCS Central, on page 17
- Configuring Policy Resolutions between Cisco UCS Manager and Cisco UCS Central, on page 18
- Setting Cisco UCS Central Registration Properties in Cisco UCS Manager, on page 18
- Unregistering a Cisco UCS Domain from Cisco UCS Central, on page 19

Registration of Cisco UCS Domains

You can have Cisco UCS Central manage some or all of the Cisco UCS domains in your data center.

If you want Cisco UCS Central to manage a Cisco UCS domain, you need to register that domain. When you register, you must choose which types of policies and other configurations will be managed by Cisco UCS Central and Cisco UCS Manager. Cisco UCS Central can manage the same types of policies and configurations for all registered Cisco UCS domains. You can also choose to have different settings for each registered Cisco UCS domain.

Perform the following before registering a Cisco UCS domain with Cisco UCS Central:

- Configure an NTP server and the correct time zone in both Cisco UCS Manager and Cisco UCS Central to ensure that they are in sync. If the time and date in the Cisco UCS domain and Cisco UCS Central are out of sync, the registration might fail.
- Obtain the hostname or IP address of Cisco UCS Central
- Obtain the shared secret that was configured when Cisco UCS Central was deployed.

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

For each Cisco UCS domain that you register with Cisco UCS Central, you can choose which application will manage certain policies and configuration settings. This policy resolution does not have to be the same for every Cisco UCS domain that you register with the same Cisco UCS Central.
Unregistering a Cisco UCS domain with Cisco UCS Central will terminate all open sessions.

You have the following options for resolving these policies and configuration settings:

- **Local**—The policy or configuration is determined and managed by Cisco UCS Manager.
- **Global**—The policy or configuration is determined and managed by Cisco UCS Central.

The following table contains a list of the policies and configuration settings that you can choose to have managed by either Cisco UCS Manager or Cisco UCS Central:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure &amp; Catalog Firmware</strong></td>
<td>Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Time Zone Management</strong></td>
<td>Determines whether the date and time is defined locally or comes from Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Communication Services</strong></td>
<td>Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Global Fault Policy</strong></td>
<td>Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>User Management</strong></td>
<td>Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>DNS Management</strong></td>
<td>Determines whether DNS servers are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Backup &amp; Export Policies</strong></td>
<td>Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Determines whether Call Home, Syslog, and TFTPCore Exporter settings are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>SEL Policy</strong></td>
<td>Determines whether managed endpoints are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Power Management</strong></td>
<td>Determines whether the power management is defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Power Supply Unit</strong></td>
<td>Determines whether power supply units are defined locally or in Cisco UCS Central.</td>
</tr>
<tr>
<td><strong>Port Configuration</strong></td>
<td>Determines whether port configuration is defined locally or in Cisco UCS Central.</td>
</tr>
</tbody>
</table>
Registering a Cisco UCS Domain with Cisco UCS Central

Before you begin

Configure an NTP server and the correct time zone in both Cisco UCS Manager and Cisco UCS Central to ensure that they are in sync. If the time and date in the Cisco UCS domain and Cisco UCS Central are out of sync, the registration might fail.

Procedure

Step 1 In the Navigation pane, click Admin.
Step 2 Expand All > Communication Management.
Step 3 Click the UCS Central node.
Step 4 In the Actions area, click UCS Central.
Step 5 In the Actions area, click Register With UCS Central.
Step 6 In the Register with UCS Central dialog box, do the following:
   a) Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address</td>
<td>The hostname or IP address of the virtual machine where Cisco UCS Central is deployed. Note: If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>The shared secret (or password) that was configured when Cisco UCS Central was deployed.</td>
</tr>
</tbody>
</table>

b) In the Policy Resolution Control area, click one of the following radio buttons for each of the fields:
   • Local—The policy or configuration is determined and managed by Cisco UCS Manager.
   • Global—The policy or configuration is determined and managed by Cisco UCS Central.

c) Click OK.
Configuring Policy Resolutions between Cisco UCS Manager and Cisco UCS Central

Procedure

Step 1 In the Navigation pane, click Admin.
Step 2 Expand All > Communication Management.
Step 3 Click the UCS Central node.
Step 4 In the Actions area, click UCS Central.
Step 5 In the Policy Resolution Control area, click one of the following radio buttons for each of the fields:
  • Local—The policy or configuration is determined and managed by Cisco UCS Manager.
  • Global—The policy or configuration is determined and managed by Cisco UCS Central.
Step 6 Click Save Changes.

Setting Cisco UCS Central Registration Properties in Cisco UCS Manager

Procedure

Step 1 In the Navigation pane, click Admin.
Step 2 Expand All > Communication Management.
Step 3 Click the UCS Central node.
Step 4 In the Actions area, click UCS Central.
Step 5 In the Status area, complete the following as appropriate:
a) Click the radio button for the Cleanup Mode that you want to use.

This can be one of the following:

  • Localize Global—When a Cisco UCS domain is unregistered, all global policies in the Cisco UCS domain will be localized to Cisco UCS Manager. The policies remain in the Cisco UCS domain, policy ownership is now local to Cisco UCS Manager, and Cisco UCS Manager admin users can make changes.

Note If you reregister the Cisco UCS domain with Cisco UCS Central, there can be policy conflicts due to the policies existing both in Cisco UCS Central and in Cisco UCS Manager. Either delete the local policies, or set the local policies to global before you try to create and associate a global service profile.
• **Deep Remove Global**—This option should only be used after careful consideration. When a Cisco UCS domain is unregistered, all global policies in the Cisco UCS domain are removed. If there are global service profiles, they will now refer to Cisco UCS Manager local default policies, and one of the following occurs:
  • If there are local default policies present, the server will reboot.
  • If there are no local default policies, the service profile association fails with a configuration error.

**Note** The deep remove global cleanup mode does not remove global VSANs and VLANs when you unregister from Cisco UCS Central. Those must be removed manually if desired.

b) Optionally check the **Suspend State** check box.

   If checked, the Cisco UCS domain is temporarily removed from Cisco UCS Central, and all global policies revert to their local counterparts. All service profiles maintain their current identities. However, global pools are no longer visible and cannot be accessible by new service profiles.

c) Optionally check the **Acknowledge State** check box.

   If the event ID stream that represents time and consistency between Cisco UCS Manager and Cisco UCS Central becomes skewed or inconsistent, Cisco UCS Manager places itself in a Suspended State and disconnects itself from Cisco UCS Central.

   If you check this check box, you acknowledge that inconsistencies exist between Cisco UCS Manager and Cisco UCS Central and are still willing to reconnect the Cisco UCS domain with Cisco UCS Central.

**Step 6** Click **Save Changes**.

---

**Unregistering a Cisco UCS Domain from Cisco UCS Central**

When you unregister a Cisco UCS domain from Cisco UCS Central, Cisco UCS Manager no longer receives updates to global policies.

**Procedure**

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

**Step 2** Expand **All > Communication Management**.

**Step 3** Click the **UCS Central** node.

**Step 4** In the **Actions** area, click **UCS Central**.

**Step 5** In the **Actions** area, click **Unregister From UCS Central**.

**Step 6** If a confirmation dialog box displays, click **Yes**.

**Step 7** Click **OK**.

For more information on the impact of unregistering and registering a Cisco UCS Domain with Cisco UCS Central, see **Policy Resolution between Cisco UCS Manager and Cisco UCS Central**.
CHAPTER 5

Power Capping and Power Management in Cisco UCS

• Power Capping in Cisco UCS, on page 22
• Power Policy Configuration, on page 22
• Power Policy for Cisco UCS Servers, on page 22
• Configuring the Power Policy, on page 23
• Power Supply for Redundancy Method, on page 23
• Configuring Policy Driven Chassis Group Power Capping, on page 24
• Policy Driven Chassis Group Power Capping, on page 24
• Power Control Policy, on page 24
• Power Groups in UCS Manager, on page 27
• Blade Level Power Capping, on page 31
• Manual Blade Level Power Cap, on page 31
• Setting the Blade-Level Power Cap for a Server, on page 32
• Viewing the Blade-Level Power Cap, on page 33
• Global Power Profiling Policy Configuration, on page 33
• Global Power Profiling Policy, on page 33
• Configuring the Global Power Profile Policy, on page 34
• Global Power Allocation Policy Configuration, on page 34
• Global Power Allocation Policy, on page 34
• Configuring the Global Power Allocation Policy, on page 34
• Power Management During Power-on Operations, on page 35
• Power Sync Policy Configuration, on page 36
• Power Sync Policy, on page 36
• Power Synchronization Behavior, on page 36
• Creating a Power Sync Policy, on page 37
• Changing a Power Sync Policy, on page 38
• Deleting a Power Sync Policy, on page 39
• Rack Server Power Management, on page 39
• UCS Mini Power Management, on page 39
Power Capping in Cisco UCS

You can control the maximum power consumption on a server through power capping, as well as manage the power allocation in the Cisco UCS Manager for blade servers, UCS C220 and C240 M4 rack servers, UCS Mini, and mixed UCS domains.

UCS Manager supports power capping on the following:

- UCS 6200 Series Fabric Interconnects
- UCS Mini 6324
- UCS 6300 Series Fabric Interconnects

You can use Policy Driven Chassis Group Power Cap, or Manual Blade Level Power Cap methods to allocate power that applies to all of the servers in a chassis.

Cisco UCS Manager provides the following power management policies to help you allocate power to your servers:

<table>
<thead>
<tr>
<th>Power Management Policies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Policy</td>
<td>Specifies the redundancy for power supplies in all chassis in a Cisco UCS domain.</td>
</tr>
<tr>
<td>Power Control Policies</td>
<td>Specifies the priority to calculate the initial power allocation for each blade in a chassis.</td>
</tr>
<tr>
<td>Global Power Allocation</td>
<td>Specifies the Policy Driven Chassis Group Power Cap or the Manual Blade Level Power Cap to apply to all servers in a chassis.</td>
</tr>
<tr>
<td>Global Power Profiling</td>
<td>Specifies how the power cap values of the servers are calculated. If it is enabled, the servers will be profiled during discovery through benchmarking. This policy applies when the Global Power Allocation Policy is set to Policy Driven Chassis Group Cap.</td>
</tr>
</tbody>
</table>

Power Policy Configuration

Power Policy for Cisco UCS Servers

The power policy is global and is inherited by all of the chassis' managed by the Cisco UCS Manager instance. You can add the power policy to a service profile to specify the redundancy for power supplies in all chassis' in the Cisco UCS domain. This policy is also known as the PSU policy.

For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*. 
Configuring the Power Policy

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Click the Equipment node.
Step 3  In the Work pane, click the Policies tab.
Step 4  Click the Global Policies subtab.
Step 5  In the Power Policy area, click one of the following radio buttons in the Redundancy field:

- **Non Redundant**—Cisco UCS Manager turns on the minimum number of power supplies (PSUs) needed and balances the load between them. If any additional PSUs are installed, Cisco UCS Manager sets them to a "turned-off" state. If the power to any PSU is disrupted, the system may experience an interruption in service until Cisco UCS Manager can activate a new PSU and rebalance the load.

  In general, a Cisco UCS chassis requires at least two PSUs for non-redundant operation. Only smaller configurations (requiring less than 2500W) can be powered by a single PSU.

- **N+1**—The total number of PSUs to satisfy non-redundancy, plus one additional PSU for redundancy, are turned on and equally share the power load for the chassis. If any additional PSUs are installed, Cisco UCS Manager sets them to a "turned-off" state. If the power to any PSU is disrupted, Cisco UCS Manager can recover without an interruption in service.

  In general, a Cisco UCS chassis requires at least three PSUs for N+1 operation.

- **Grid**—Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails (which causes a loss of power to one or two PSUs), the surviving PSUs on the other power circuit continue to provide power to the chassis.

  For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Step 6  Click Save Changes.

Power Supply for Redundancy Method

<table>
<thead>
<tr>
<th>PSU Redundancy</th>
<th>Max Power @ 220 V (Watts)</th>
<th>Max Power @ 110 V (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1+1 (N+1) OR 1 (N)</td>
<td>2500</td>
<td>1300</td>
</tr>
<tr>
<td>2+1 (N+1) OR 2 (N) or 2+2 (Grid)</td>
<td>5000</td>
<td>2600</td>
</tr>
<tr>
<td>3+1 (N+1) OR 3 (N)</td>
<td>5472</td>
<td>3900</td>
</tr>
<tr>
<td>4 (N)</td>
<td>5472</td>
<td>5200</td>
</tr>
</tbody>
</table>
Configuring Policy Driven Chassis Group Power Capping

Policy Driven Chassis Group Power Capping

When you select the Policy Driven Chassis Group Power Cap in the Global Cap Policy, Cisco UCS can maintain the over-subscription of servers without risking power failures. You can achieve over-subscription through a two-tier process. For example, at the chassis level, Cisco UCS divides the amount of power available among members of the power group, and at the blade level, the amount of power allotted to a chassis is divided among blades based on priority.

Each time a service profile is associated or disassociated, Cisco UCS Manager recalculates the power allotment for each blade server within the chassis. If necessary, power from lower-priority service profiles is redistributed to higher-priority service profiles.

UCS power groups cap power in less than one second to safely protect data center circuit breakers. A blade must stay at its cap for 20 seconds before the chassis power distribution is optimized. This is intentionally carried out over a slower timescale to prevent reacting to transient spikes in demand.

---

**Note**

The system reserves enough power to boot a server in each slot, even if that slot is empty. This reserved power cannot be leveraged by servers requiring more power. Blades that fail to comply with the power cap are penalized.

---

Power Control Policy

Cisco UCS uses the priority set in the power control policy along with the blade type and configuration to calculate the initial power allocation for each blade within a chassis. During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies.

Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

---

**Note**

You must include the power control policy in a service profile and that service profile must be associated with a server for it to take effect.

---

Creating a Power Control Policy

**Procedure**

**Step 1**

In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand the node for the organization where you want to create the policy.
        If the system does not include multitenancy, expand the root node.
Step 4  Right-click Power Control Policies and choose Create Power Control Policy.
Step 5  In the Create Power Control Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name field</strong></td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric</td>
</tr>
<tr>
<td></td>
<td>characters. You cannot use spaces or any special characters other than -</td>
</tr>
<tr>
<td></td>
<td>(hyphen), _ (underscore), : (colon), and . (period), and you cannot change</td>
</tr>
<tr>
<td></td>
<td>this name after the object is saved.</td>
</tr>
<tr>
<td><strong>Description field</strong></td>
<td>A description of the policy. Cisco recommends including information about</td>
</tr>
<tr>
<td></td>
<td>where and when to use the policy.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 256 characters. You can use any characters or spaces except `</td>
</tr>
<tr>
<td></td>
<td>(accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign),</td>
</tr>
<tr>
<td></td>
<td>&gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
<tr>
<td><strong>Fan Speed Policy</strong></td>
<td>Fan speed is for rack servers only. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low Power</strong>—The fan runs at the minimum speed required to keep the server</td>
</tr>
<tr>
<td></td>
<td>cool.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Balanced</strong>—The fan runs faster when needed based on the heat generated</td>
</tr>
<tr>
<td></td>
<td>by the server. When possible, the fan returns to the minimum required speed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Performance</strong>—The fan is kept at the speed needed for better server</td>
</tr>
<tr>
<td></td>
<td>performance. This draws more power but means the fan is already at speed</td>
</tr>
<tr>
<td></td>
<td>if the server begins to heat up.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High Power</strong>—The fan is kept at an even higher speed that emphasizes</td>
</tr>
<tr>
<td></td>
<td>performance over power consumption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Max Power</strong>—The fan is kept at the maximum speed at all times. This</td>
</tr>
<tr>
<td></td>
<td>option provides the most cooling and uses the most power.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any</strong>—The server determines the optimal fan speed.</td>
</tr>
</tbody>
</table>

Cisco UCS Manager Server Management Guide, Release 3.1
**Deleting a Power Control Policy**

**Procedure**

1. In the Navigation pane, click Servers.
2. Expand Servers > Policies > Organization_Name.
3. Expand the Power Control Policies node.
4. Right-click the policy you want to delete and select Delete.
5. If a confirmation dialog box displays, click Yes.

**What to do next**

Include the policy in a service profile or service profile template.
Power Groups in UCS Manager

A power group is a set of chassis that all draw power from the same power distribution unit (PDU). In Cisco UCS Manager, you can create power groups that include one or more chassis, then set a peak power cap in AC watts for that power grouping.

Implementing power capping at the chassis level requires the following:

• IOM, CIMC, and BIOS version 1.4 or higher
• Two Power Supply Units (PSUs)

The peak power cap is a static value that represents the maximum power available to all blade servers within a given power group. If you add or remove a blade from a power group, but do not manually modify the peak power value, the power group adjusts the peak power cap to accommodate the basic power-on requirements of all blades within that power group.

A minimum of 890 AC watts should be set for each chassis. This converts to 800 watts of DC power, which is the minimum amount of power required to power an empty chassis. To associate a half-width blade, the group cap needs to be set to 1475 AC watts. For a full-width blade, it needs to be set to 2060 AC watts.

After a chassis is added to a power group, all service profile associated with the blades in the chassis become part of that power group. Similarly, if you add a new blade to a chassis, that blade inherently becomes part of the chassis’ power group.

---

**Note**

Creating a power group is not the same as creating a server pool. However, you can populate a server pool with members of the same power group by creating a power qualifier and adding it to server pool policy.

When a chassis is removed or deleted, the chassis gets removed from the power group.

UCS Manager supports explicit and implicit power groups.

- **Explicit**: You can create a power group, add chassis' and racks, and assign a budget for the group.
- **Implicit**: Ensures that the chassis is always protected by limiting the power consumption within safe limits. By default, all chassis that are not part of an explicit power group are assigned to the default group and the appropriate caps are placed. New chassis that connect to UCS Manager are added to the default power group until you move them to a different power group.
The following table describes the error messages you might encounter while assigning power budget and working with power groups.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient budget for power group (\text{POWERGROUP_NAME}) and/or Chassis N cannot be capped as group cap is low. Please consider raising the cap. and/or Admin committed insufficient for power group (\text{GROUP_NAME}), using previous value N and/or Power cap application failed for chassis N</td>
<td>One of these messages displays if you did not meet the minimum limit when assigning the power cap for a chassis, or the power requirement increased because of the addition of blades or change of power policies.</td>
<td>Increase the power cap limit to the Minimum Power Cap for Allowing Operations (W) value displayed on the Power Group page for the specified power group.</td>
</tr>
<tr>
<td>Chassis N cannot be capped as the available PSU power is not enough for the chassis and the blades. Please correct the problem by checking input power or replace the PSU</td>
<td>Displays when the power budget requirement for the chassis is more than the PSU power that is available.</td>
<td>Check the PSU input power and redundancy policy to ensure that enough power is available for the chassis. If a PSU failed, replace the PSU.</td>
</tr>
<tr>
<td>Power cap application failed for server N</td>
<td>Displays when the server is consuming more power than allocated and cannot be capped, or the server is powered on when no power is allocated.</td>
<td>Do not power on un-associated servers.</td>
</tr>
<tr>
<td>P-State lowered as consumption hit power cap for server</td>
<td>Displays when the server is capped to reduce the power consumption below the allocated power.</td>
<td>This is an information message. If a server should not be capped, in the service profile set the value of the power control policy Power Capping field to no-cap.</td>
</tr>
<tr>
<td>Chassis N has a mix of high-line and low-line PSU input power sources.</td>
<td>This fault is raised when a chassis has a mix of high-line and low-line PSU input sources connected.</td>
<td>This is an unsupported configuration. All PSUs must be connected to similar power sources.</td>
</tr>
</tbody>
</table>
Creating a Power Group

Before you begin

Make sure that the global power allocation policy is set to Policy Driven Chassis Group Cap on the Global Policies tab.

Procedure

Step 1
In the Navigation pane, click Equipment.

Step 2
Click the Equipment node.

Step 3
In the Work pane, click the Policies tab.

Step 4
Click the Power Groups subtab.

Step 5
On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 6
On the first page of the Create Power Group wizard, complete the following fields:

a) Enter a unique name and description for the power group. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

b) Click Next.

Step 7
On the Add Chassis Members page of the Create Power Group wizard, do the following:

a) In the Chassis table, choose one or more chassis to include in the power group.

b) Click the >> button to add the chassis to the Selected Chassis table that displays all chassis included in the power group.

You can use the << button to remove one or more chassis from the power group.

c) Click Next.

Step 8
On the Add Rack Members page of the Create Power Group wizard, do the following:

a) In the Rack Unit table, choose one or more rack units to include in the power group.

b) Click the >> button to add the rack to the Selected Rack Unit table that displays all racks included in the power group.

You can use the << button to remove one or more rack units from the power group.

c) Click Next.

Step 9
On the Add FEX Members page of the Create Power Group wizard, do the following:

a) In the FEX table, choose one or more FEX to include in the power group.

b) Click the >> button to add the chassis to the Selected FEX table that displays all FEX included in the power group.

You can use the << button to remove one or more FEX from the power group.

c) Click Next.
Step 10 On the **Add FI Members** page of the **Create Power Group** wizard, do the following:

a) In the **FI** table, choose one or more FI to include in the power group.

b) Click the >> button to add the FI to the **Selected FI** table that displays all chassis included in the power group.

You can use the << button to remove one or more FI from the power group.

c) Click **Next**.

Step 11 On the **Power Group Attributes** page of the **Create Power Group** wizard, do the following:

a) Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Cap</strong> field</td>
<td>The maximum peak power (in watts) available to the power group. Enter an integer between 0 and 1000000.</td>
</tr>
</tbody>
</table>
| **Enable Dynamic Reallocation** field | This can be one of the following:  
  • **Chassis**—Cisco UCS monitors power usage and changes the blade allocations as required to maximize power utilization.  
  • **None**—Blade allocations are not adjusted dynamically. |

b) Click **Finish**.

---

### Adding a Chassis to a Power Group

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.

**Step 2** Click the **Equipment** node.

**Step 3** In the **Work** pane, click the **Power Groups** tab.

**Step 4** Right-click the power group to which you want to add a chassis and choose **Add Chassis Members**.

**Step 5** In the **Add Chassis Members** dialog box, do the following:

a) In the **Chassis** table, choose one or more chassis to include in the power group.

b) Click the >> button to add the chassis to the **Selected Chassis** table that displays all chassis included in the power group.

You can use the << button to remove one or more chassis from the power group.

c) Click **OK**.
Removing a Chassis from a Power Group

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Power Groups tab.</td>
</tr>
<tr>
<td>4</td>
<td>Expand the power group from which you want to remove a chassis.</td>
</tr>
<tr>
<td>5</td>
<td>Right-click the chassis that you want to remove from the power group and choose Delete.</td>
</tr>
<tr>
<td>6</td>
<td>If a confirmation dialog box displays, click Yes.</td>
</tr>
</tbody>
</table>

Deleting a Power Group

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Power Groups tab.</td>
</tr>
<tr>
<td>4</td>
<td>Right-click the power group that you want to delete and choose Delete.</td>
</tr>
<tr>
<td>5</td>
<td>If a confirmation dialog box displays, click Yes.</td>
</tr>
</tbody>
</table>

Blade Level Power Capping

Manual Blade Level Power Cap

When manual blade-level power cap is configured in the global cap policy, you can set a power cap for each blade server in a Cisco UCS domain.

The following configuration options are available:

- **Watts**—You can specify the maximum amount of power that the server can consume at one time. This maximum can be any amount between 0 watts and 1100 watts.
- **Unbounded**—No power usage limitations are imposed on the server. The server can use as much power as it requires.

If the server encounters a spike in power usage that meets or exceeds the maximum configured for the server, Cisco UCS Manager does not disconnect or shut down the server. Instead, Cisco UCS Manager reduces the power that is made available to the server. This reduction can slow down the server, including a reduction in CPU speed.
If you configure the manual blade-level power cap using Equipment > Policies > Global Policies > Global Power Allocation Policy, the priority set in the Power Control Policy is no longer relevant.

Setting the Blade-Level Power Cap for a Server

Before you begin

Make sure the global power allocation policy is set to Manual Blade Level Cap on the Global Policies tab.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server for which you want to set the power budget.
Step 4  In the Work pane, click the General tab.
Step 5  In the Power Budget area, do the following:
   a)  Click the Expand icon to the right of the heading to display the fields.
   b)  Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>Whether this server is power capped. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>* Unbounded*—The server is not power capped under any circumstances.</td>
</tr>
<tr>
<td></td>
<td>* Enabled*—The Cisco UCS Manager GUI displays the Watts field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  Power capping goes into effect only if there is insufficient power available to the chassis to meet the demand. If there is sufficient power, the server can use as many watts as it requires.</td>
</tr>
<tr>
<td>Watts</td>
<td>The maximum number of watts that the server can use if there is not enough power to the chassis to meet the demand. The value range is from 0 and 10000000.</td>
</tr>
</tbody>
</table>

Step 6  Click Save Changes.
Viewing the Blade-Level Power Cap

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis.
Step 3 Choose the chassis for which you want to view the server power usage.
Step 4 Do one of the following:
   • To view the power usage for all servers in the chassis, click the Power tab in the Work pane.
   • To view the power usage for one server in the chassis, expand the chassis and click the server. Then click the Power tab in the Work pane.
Step 5 If necessary, expand the Motherboards node to view the power counters.

Global Power Profiling Policy Configuration

Global Power Profiling Policy

The Global Power Profiling Policy specifies how power allocation is applied to all of the servers in a chassis. The policy applies when you set the Global Power Allocation Policy to Policy Driven Chassis Group Cap. You can set the Global Power Profiling Policy to one of the following:

• Disabled—The minimum and maximum power cap values of the blades are calculated based on the static power consumption values of each of the components.

• Enabled—The minimum and maximum power cap values of the blades are measured as part of the server discovery. These values are similar to the actual power consumption of the blades.

---

Note

After enabling the Global Power Profiling Policy, you must re-acknowledge the blades to obtain the minimum and maximum power cap.

---

Important

Power profiling is not supported in Cisco UCS B460 M4 blades.
Configuring the Global Power Profile Policy

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Policies tab.</td>
</tr>
<tr>
<td>4</td>
<td>Click the Global Policies subtab.</td>
</tr>
<tr>
<td>5</td>
<td>In the Global Power Profiling Policy area, check the Profile Power checkbox to enable the Global Power Profiling Policy.</td>
</tr>
<tr>
<td>6</td>
<td>Click Save Changes.</td>
</tr>
</tbody>
</table>

**Global Power Allocation Policy Configuration**

**Global Power Allocation Policy**

The Global Power Allocation Policy allows you to specify the Policy Driven Chassis Group Power Cap or Manual Blade-level Power Cap power allocation method applied to servers in a chassis.

Cisco recommends using the default Policy Driven Chassis Group Power Cap power allocation method.

---

**Important**

Any change to the Manual Blade level Power Cap configuration results in the loss of any groups or configuration options set for the Policy Driven Chassis Group Power Cap.

---

**Configuring the Global Power Allocation Policy**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Equipment node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Policies tab.</td>
</tr>
<tr>
<td>4</td>
<td>Click the Global Policies subtab.</td>
</tr>
</tbody>
</table>
| 5    | In the Global Power Allocation Policy area, click one of the following radio buttons in the Allocation Method field to determine the power cap management mode used in the Cisco UCS domain:  
  - **Manual Blade Level Cap**—Power allocation is configured on each individual blade server in all chassis.  
    If you select this option, you cannot create power groups. |
• **Policy Driven Chassis Group Cap**—Power allocation is configured at the chassis level through power control policies included in the associated service profiles. If you select this option, you can also create power groups that contain one or more chassis in the Cisco UCS domain.

By default, power allocation is done for each chassis through a power control policy.

**Step 6**

Click **Save Changes**.

---

## Power Management During Power-on Operations

### Boot Staggering during Power on

Cisco UCS Manager attempts to boot as many blades as possible based on the amount of available power. If the power required to boot a blade is not available, Cisco UCS Manager stagnates the boot in the Finite State Machine (FSM) CheckPowerAvailability stage, and raises the following fault on the blade: *Insufficient power available to power-on server x/y*.

When the required power becomes available, the FSM proceeds with blade power on. After a blade powers off, the allocated power budget is reclaimed.

---

**Note**

When the power budget that was allocated to the blade is reclaimed, the allocated power displays as 0 Watts.

---

**Limitation**

If you power on a blade outside of the Cisco UCS Manager and if there is not enough power available for allocation, the following fault is raised:

*Power cap application failed for server x/y*

---

### Power Allocation during Service Profile Association

The power allocated to a blade during service profile association depends on the Power Control Policy used, and the power that is available from the power group. After the power is allocated to a server during a successful service profile association, the blade is guaranteed the minimum power cap. If the Power Control Policy priority is set to no-cap, a blade is allocated a potential maximum power cap, which might exceed the measured maximum power cap that displays.

---

**Note**

If the priority of an associated blade is changed to no-cap, and is not able to allocate the maximum power cap, you might see one of the following faults:

- **PSU-insufficient**—There is not enough available power for the PSU.
- **Group-cap-insufficient**—The group cap value is not sufficient for the blade.
Power Sync Policy Configuration

Power Sync Policy

Cisco UCS Manager includes a global (default) power sync policy to address power synchronization issues between the associated service profiles and the servers. You can use the power sync policy to synchronize the power state when the power state of the service profile differs from the actual power state of the server. The policy allows you to control when to synchronize the power state on the associated service profiles for the servers. The power sync policy does not affect other power-related policies.

The power synchronization policy applies to all the service profiles by default. You cannot delete the default power sync policy, but you can edit the default policy. You can create your own power sync policies and apply them to the service profiles. You can also create a power sync policy that is specific to a service profile and it always takes precedence over the default policy.

Cisco UCS Manager creates a fault on the associated service profile when the power sync policy referenced in the service profile does not exist. Cisco UCS Manager automatically clears the fault once you create a power sync policy for the specified service profile or change the reference to an existing policy in the service profile.

Power Synchronization Behavior

Cisco UCS Manager synchronizes the power state only when the actual power state of the server is OFF. The current power synchronization behavior is based on the actual power state and the preferred power state after shallow association occurs.

For example, the following events trigger shallow association:

- Fabric Interconnects(FI) and IOM disconnected.
- IOM reset
- FI power loss or reboot
- Chassis reacknowledgment
- Chassis power loss
- Service profile change

The following table describes the current power synchronization behavior:

<table>
<thead>
<tr>
<th>Event</th>
<th>Preferred Power State</th>
<th>Actual Power State Before Event</th>
<th>Actual Power State After Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shallow Association</td>
<td>ON</td>
<td>OFF</td>
<td>ON</td>
</tr>
<tr>
<td>Shallow Association</td>
<td>OFF</td>
<td>OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>Shallow Association</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
</tr>
<tr>
<td>Shallow Association</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
</tr>
</tbody>
</table>
Creating a Power Sync Policy

Procedure

**Step 1**  
In the Navigation pane, click Servers.

**Step 2**  
Expand Servers > Policies.

**Step 3**  
Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the root node.

**Step 4**  
Right-click Power Sync Policies and choose Create Power Sync Policy.

**Step 5**  
In the Create Power Sync Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
</tbody>
</table>
The options that allow you to synchronize the desired power state of the associated service profile to the physical server. This can be one of the following:

- **Default Sync**—After the initial server association, any configuration change or management connectivity changes that you perform trigger a server reassociation. This option synchronizes the desired power state to the physical server if the physical server power state is off and the desired power state is on. This is the default behavior.

- **Always Sync**—When the initial server association or the server reassociation occurs, this option synchronizes the desired power state to the physical power state, even if the physical server power state is on and desired power state is off.

- **Initial Only Sync**—This option only synchronizes the power to a server when a service profile is associated to the server for the first time, or when the server is re-commissioned. When you set this option, resetting the power state from the physical server side does not affect the desired power state on the service profile.

### Changing a Power Sync Policy

#### Procedure

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers > Policies**.
3. Expand the node for the organization where you want to create the policy.
   - If the system does not include multitenancy, expand the **root** node.
4. Choose a service profile policy from the **root** node.
5. In the **Work** pane, click the **Policies** tab.

---

What to do next

Include the policy in a service profile or service profile template.
Step 6  Click the Change Power Sync Policy from the Actions area.

The information displayed depends on what you choose in the Select the Power Sync Policy drop-down list. You can choose:

- **No Power Sync Policy**—If you choose this option, Cisco UCS Manager GUI does not display any other information. When you choose this option, Cisco UCS Manager implicitly uses the default power sync policy. Cisco UCS Manager searches for the default power sync policy under service profile organizations. If the policy is not found, then it uses the default power sync policy under root.

- **Use an Existing Power Sync Policy**—if you want to select a global policy. Cisco UCS Manager GUI displays the Power Sync Policy drop-down list that enables you to choose an existing policy.

- **Create a Local Power Sync Policy**—if you want to create a power sync policy that can only be accessed by this service profile. You can also create a power sync policy by using the Create Power Sync Policy link from the Power Sync Policy area.

---

**Deleting a Power Sync Policy**

**Procedure**

- **Step 1**  In the Navigation pane, click Servers.
- **Step 2**  Expand Servers > Policies > Organization_Name.
- **Step 3**  Expand the Power Sync Policies node.
- **Step 4**  Right-click the policy you want to delete and select Delete.
- **Step 5**  If a confirmation dialog box displays, click Yes.

---

**Rack Server Power Management**

Power capping is supported for following rack servers:

- Cisco UCS C220 M4 Server
- Cisco UCS C240 M4 Server

**UCS Mini Power Management**

You can manage power of the blade servers in 6324 Fabric Interconnect (FI), which is used for remote offices and branch sites, and for limited server deployments. UCS Manager supports Dual Line Power Supply Unit and 110V when used with the 6324 Fabric Interconnect. You can manager how you want to allocate power when using 110V power supplies, because they might not provide enough power for a fully loaded chassis. Dual power supplies is standard for both AC and DC-48V on the UCS Mini 6324.
Blade Server Hardware Management

• Blade Server Management, on page 41
• Booting a Blade Server, on page 43
• Booting a Rack-Mount Server from the Service Profile, on page 44
• Determining the Boot Order of a Blade Server, on page 44
• Shutting Down a Blade Server, on page 45
• Shutting Down a Server from the Service Profile, on page 45
• Resetting a Blade Server, on page 46
• Resetting a Blade Server to Factory Default Settings, on page 46
• Reacknowledging a Blade Server, on page 47
• Removing a Server from a Chassis, on page 48
• Deleting the Inband Configuration from a Blade Server, on page 48
• Decommissioning a Blade Server, on page 49
• Removing a Non-Existent Blade Server Entry, on page 49
• Recommissioning a Blade Server, on page 50
• Reacknowledging a Server Slot in a Chassis, on page 50
• Removing a Non-Existent Blade Server from the Configuration Database, on page 51
• Turning the Locator LED for a Blade Server On and Off, on page 51
• Turning the Local Disk Locator LED on a Blade Server On and Off, on page 52
• Resetting the CMOS for a Blade Server, on page 52
• Resetting the CIMC for a Blade Server, on page 53
• Clearing TPM for a Blade Server, on page 53
• Viewing the POST Results for a Blade Server, on page 54
• Issuing an NMI from a Blade Server, on page 54
• Viewing Health Events for a Blade Server, on page 55
• Health LED Alarms, on page 56
• Smart SSD, on page 57

Blade Server Management

You can manage and monitor all blade servers in a Cisco UCS domain through Cisco UCS Manager. You can perform some blade server management tasks, such as changes to the power state, from the server and service profile.

The remaining management tasks can only be performed on the server.
The power supply units go into power save mode when a chassis has two blades or less. When a third blade is added to the chassis and is fully discovered, the power supply units return to regular mode.

If a blade server slot in a chassis is empty, Cisco UCS Manager provides information, errors, and faults for that slot. You can also re-acknowledge the slot to resolve server mismatch errors and to have Cisco UCS Manager rediscover the blade server in the slot.

**Guidelines for Removing and Decommissioning Blade Servers**

Consider the following guidelines when deciding whether to remove or decommission a blade server using Cisco UCS Manager:

**Decommissioning a Blade Server**

If you want to temporarily decommission a physically present and connected blade server, you can temporarily remove it from the configuration. A portion of the server's information is retained by Cisco UCS Manager for future use, in case the blade server is recommissioned.

**Removing a Blade Server**

Removing is performed when you physically remove a blade server from the Cisco UCS Manager by disconnecting it from the chassis. You cannot remove a blade server from Cisco UCS Manager if it is physically present and connected to a chassis. After the physical removal of the blade server is completed, the configuration for that blade server can be removed in Cisco UCS Manager.

During removal, active links to the blade server are disabled, all entries from databases are removed, and the server is automatically removed from any server pools that it was assigned to during discovery.

---

**Note**

Only servers added to a server pool automatically during discovery are removed automatically. Servers that were manually added to a server pool must be removed manually.

To add a removed blade server back to the configuration, it must be reconnected, then rediscovered. When a server is reintroduced to Cisco UCS Manager, it is treated as a new server and is subject to the deep discovery process. For this reason, it is possible for Cisco UCS Manager to assign the server a new ID that might be different from the ID that it held before.

**Recommendations for Avoiding Unexpected Server Power Changes**

If a server is not associated with a service profile, you can use any available means to change the server power state, including the physical **Power** or **Reset** buttons on the server.

If a server is associated with, or assigned to, a service profile, you should only use the following methods to change the server power state:

- In Cisco UCS Manager GUI, go to the **General** tab for the server or the service profile associated with the server and select **Boot Server** or **Shutdown Server** from the **Actions** area.

- In Cisco UCS Manager CLI, scope to the server or the service profile associated with the server and use the **power up** or **power down** commands.
Do not use any of the following options on an associated server that is currently powered off:

- **Reset** in the GUI
- **cycle cycle-immediate** or **reset hard-reset-immediate** in the CLI
- The physical **Power** or **Reset** buttons on the server

If you reset, cycle, or use the physical power buttons on a server that is currently powered off, the server's actual power state might become out of sync with the desired power state setting in the service profile. If the communication between the server and Cisco UCS Manager is disrupted or if the service profile configuration changes, Cisco UCS Manager might apply the desired power state from the service profile to the server, causing an unexpected power change.

Power synchronization issues can lead to an unexpected server restart, as shown below:

<table>
<thead>
<tr>
<th>Desired Power State in Service Profile</th>
<th>Current Server Power State</th>
<th>Server Power State After Communication Is Disrupted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Powered Off</td>
<td>Powered On</td>
</tr>
<tr>
<td>Down</td>
<td>Powered On</td>
<td>Powered On</td>
</tr>
</tbody>
</table>

**Note** Running servers are not shut down regardless of the desired power state in the service profile.

**Booting a Blade Server**

If the **Boot Server** link is dimmed in the **Actions** area, you must shut down the server first.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.

**Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.

**Step 3** Choose the server that you want to boot.

**Step 4** In the **Work** pane, click the **General** tab.

**Step 5** In the **Actions** area, click **Boot Server**.

**Step 6** If a confirmation dialog box displays, click **Yes**.

After the server boots, the **Overall Status** field on the **General** tab displays an OK status.
Booting a Rack-Mount Server from the Service Profile

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles.
Step 3  Expand the node for the organization where you want to create the service profile.
        If the system does not include multitenancy, expand the root node.
Step 4  Choose the service profile that requires the associated server to boot.
Step 5  In the Work pane, click the General tab.
Step 6  In the Actions area, click Boot Server.
Step 7  If a confirmation dialog box displays, click Yes.
Step 8  Click OK in the Boot Server dialog box.

After the server boots, the Overall Status field on the General tab displays an ok status or an up status.

Determining the Boot Order of a Blade Server

Tip
You can also view the boot order tabs from the General tab of the service profile associated with a server.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Click the server for which you want to determine the boot order.
Step 4  In the Work pane, click the General tab.
Step 5  If the Boot Order Details area is not expanded, click the Expand icon to the right of the heading.
Step 6  To view the boot order assigned to the server, click the Configured Boot Order tab.
Step 7  To view what will boot from the various devices in the physical server configuration, click the Actual Boot Order tab.

Note  The Actual Boot Order tab always shows "Internal EFI Shell" at the bottom of the boot order list.
Shutting Down a Blade Server

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the Shutdown Server link is dimmed in the Actions area, the server is not running.

---

**Procedure**

**Step 1** In the Navigation pane, click Equipment.

**Step 2** Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3** Choose the server that you want to shut down.

**Step 4** In the Work pane, click the General tab.

**Step 5** In the Actions area, click Shutdown Server.

**Step 6** If a confirmation dialog box displays, click Yes.

After the server has been successfully shut down, the Overall Status field on the General tab displays a power-off status.

---

Shutting Down a Server from the Service Profile

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the Shutdown Server link is dimmed in the Actions area, the server is not running.

**Procedure**

**Step 1** In the Navigation pane, click Servers.

**Step 2** Expand Servers > Service Profiles.

**Step 3** Expand the node for the organization where you want to create the service profile.

If the system does not include multitenancy, expand the root node.

**Step 4** Choose the service profile that requires the associated server to shut down.

**Step 5** In the Work pane, click the General tab.

**Step 6** In the Actions area, click Shutdown Server.
Step 7  If a confirmation dialog box displays, click Yes.

After the server successfully shuts down, the Overall Status field on the General tab displays a down status or a power-off status.

### Resetting a Blade Server

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shut down the operating system. If the operating system does not support a graceful shutdown, the server is power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee the completion of these operations before the server is reset.

#### Note

If you are trying to boot a server from a power-down state, you should not use Reset.

If you continue the power-up with this process, the desired power state of the servers become out of sync with the actual power state and the servers might unexpectedly shut down at a later time. To safely reboot the selected servers from a power-down state, click Cancel, then select the Boot Server action.

### Procedure

1. In the Navigation pane, click Equipment.
2. Expand Equipment > Chassis > Chassis Number > Servers.
3. Choose the server that you want to reset.
4. In the Work pane, click the General tab.
5. In the Actions area, click Reset.
6. In the Reset Server dialog box, do the following:
   a) Click the Power Cycle option.
   b) (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.
   c) Click OK.

The reset may take several minutes to complete. After the server has been reset, the Overall Status field on the General tab displays an ok status.

### Resetting a Blade Server to Factory Default Settings

You can now reset a blade server to its factory settings. By default, the factory reset operation does not affect storage drives and flexflash drives. This is to prevent any loss of data. However, you can choose to reset these devices to a known state as well.
**Important**

Resetting storage devices will result in loss of data.

Perform the following procedure to reset the server to factory default settings.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.

**Step 2** Expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.

**Step 3** Choose the server that you want to reset to its factory default settings.

**Step 4** In the **Work** pane, click the **General** tab.

**Step 5** In the **Actions** area, click **Server Maintenance**.

**Step 6** In the **Maintenance** dialog box, do the following:

- a) Click **Reset to Factory Default**.
- b) Click **OK**.

**Step 7** From the **Maintenance Server** dialog box that appears, select the appropriate options:

- To delete all storage, check the **Scrub Storage** checkbox.

- To place all disks into their initial state after deleting all storage, check the **Create Initial Volumes** checkbox.

You can check this checkbox only if you check the **Scrub Storage** checkbox. For servers that support JBOD, the disks will be placed in a JBOD state. For servers that do not support JBOD, each disk will be initialized with a single R0 volume that occupies all the space in the disk.

**Important** Do not check the **Create Initial Volumes** box if you want to use storage profiles. Creating initial volumes when you are using storage profiles may result in configuration errors.

- To delete all flexflash storage, check the **Scrub FlexFlash** checkbox.

Cisco UCS Manager resets the server to its factory default settings.

---

**Reacknowledging a Blade Server**

Perform the following procedure to rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.

**Step 2** Expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.

**Step 3** Choose the server that you want to acknowledge.
Removing a Server from a Chassis

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Choose the server that you want to remove from the chassis.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Server Maintenance.
Step 6 In the Maintenance dialog box, click Re-acknowledge, then click OK.

The server is removed from the Cisco UCS configuration.

Step 7 Go to the physical location of the chassis and remove the server hardware from the slot.

For instructions on how to remove the server hardware, see the Cisco UCS Hardware Installation Guide for your chassis.

What to do next

If you physically re-install the blade server, you must re-acknowledge the slot for the Cisco UCS Manager to rediscover the server.

For more information, see Reacknowledging a Server Slot in a Chassis, on page 50.

Deleting the Inband Configuration from a Blade Server

This procedure removes the inband management IP address configuration from a blade server. If this action is greyed out, no inband configuration was completed.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers > Server Name.
Step 3  In the Work area, click the Inventory tab.
Step 4  Click the CIMC subtab.
Step 5  In the Actions area, click Delete Inband Configuration.
Step 6  Click Yes in the Delete confirmation dialog box.

The inband configuration for the server is deleted.

Note  If an inband service profile is configured in Cisco UCS Manager with a default VLAN and pool name, the server CIMC will automatically get an inband configuration from the inband profile approximate one minute after deleting the inband configuration here.

Decommissioning a Blade Server

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server that you want to decommission.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Server Maintenance.
Step 6  In the Maintenance dialog box, do the following:
  a) Click Decommission.
  b) Click OK.

The server is removed from the Cisco UCS configuration.

What to do next

If you physically re-install the blade server, you must re-acknowledge the slot for the Cisco UCS Manager to rediscover the server.

For more information, see Reacknowledging a Server Slot in a Chassis, on page 50.

Removing a Non-Existent Blade Server Entry

Perform the following procedure after decommissioning the server and physically removing the server hardware. This procedure removes the non-existing stale entry of a blade server from the Decommissioned tab.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2 In the Work pane, click the Decommissioned tab.
Step 3 On the row for each blade server that you want to remove from the list, check the check box in the Decommission column, then click Save Changes.
Step 4 If a confirmation dialog box displays, click Yes.

Recommissioning a Blade Server

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment node.
Step 3 Click the Chassis node.
Step 4 In the Work pane, click the Decommissioned tab.
Step 5 On the row for each blade server that you want to recommission, check the check box in the Decommission column, then click Save Changes.
Step 6 If a confirmation dialog box displays, click Yes.
Step 7 (Optional) Monitor the progress of the server recommission and discovery on the FSM tab for the server.

Reacknowledging a Server Slot in a Chassis

Perform the following procedure if you decommissioned a blade server without removing the physical hardware from the chassis, and you want Cisco UCS Manager to rediscover and recommission the server.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Choose the server whose slot you want to reacknowledge.
Step 4 If Cisco UCS Manager displays a Resolve Slot Issue dialog box, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The here link in the Situation</td>
<td>Click this link and then click Yes in the confirmation dialog box. Cisco UCS Manager reacknowledges the slot and discovers the server in the slot.</td>
</tr>
<tr>
<td>OK</td>
<td>Click this button if you want to proceed to the General tab. You can use the Reacknowledge Slot link in the Actions area to have Cisco UCS Manager reacknowledge the slot and discover the server in the slot.</td>
</tr>
</tbody>
</table>
Removing a Non-Existent Blade Server from the Configuration Database

Perform the following procedure if you physically removed the server hardware without first decommissioning the server. You cannot perform this procedure if the server is physically present.

If you want to physically remove a server, see Removing a Server from a Chassis, on page 48.

Procedure

**Step 1**
In the **Navigation** pane, click **Equipment**.

**Step 2**
Expand **Equipment > Chassis > Chassis Number > Servers**.

**Step 3**
Choose the server that you want to remove from the configuration database.

**Step 4**
In the **Work** pane, click the **General** tab.

**Step 5**
In the **Actions** area, click **Server Maintenance**.

**Step 6**
In the **Maintenance** dialog box, click **Remove**, then click **OK**.

Cisco UCS Manager removes all data about the server from its configuration database. The server slot is now available for you to insert new server hardware.

Turning the Locator LED for a Blade Server On and Off

Procedure

**Step 1**
In the **Navigation** pane, click **Equipment**.

**Step 2**
Expand **Equipment > Chassis > Chassis Number > Servers**.

**Step 3**
Choose the server for which you want to turn the locator LED on or off.

**Step 4**
In the **Work** pane, click the **General** tab.

**Step 5**
In the **Actions** area, click one of the following:

- **Turn on Locator LED**—Turns on the LED for the selected server.
- **Turn off Locator LED**—Turns off the LED for the selected server.
- **Turn on Master Locator LED**—For the Cisco UCS B460 M4 blade server, turns on the LED for the master node.
- **Turn off Master Locator LED**—For the Cisco UCS B460 M4 blade server, turns off the LED for the master node.
- **Turn on Slave Locator LED**—For the Cisco UCS B460 M4 blade server, turns on the LED for the slave node.
• **Turn off Locator LED**—For the Cisco UCS B460 M4 blade server, turns off the LED for the slave node.

---

**Turning the Local Disk Locator LED on a Blade Server On and Off**

**Before you begin**

• Ensure the server, on which the disk is located, is powered on. If the server is off, you are unable to turn on or off the local disk locator LED.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
**Step 3** Choose the server for which you want to turn the local disk locator LED on or off.
**Step 4** In the **Work** pane, click the **Inventory > Storage > Disks** tabs.

The Storage Controller inventory appears.

**Step 5** Click a disk.
The disk details appear.

**Step 6** In the **Details** area, click **Toggle Locator LED**.
If the **Locator LED** state is **On**, it will turn **Off**. If the **Locator LED** state is **Off**, it will turn **On**.

**Step 7** Click **Save Changes**.

---

**Resetting the CMOS for a Blade Server**

Sometimes, troubleshooting a server might require you to reset the CMOS. Resetting the CMOS is not part of the normal maintenance of a server.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
**Step 3** Choose the server for which you want to reset the CMOS.
**Step 4** In the **Work** pane, click the **General** tab.
**Step 5** In the **Actions** area, click **Recover Server**.
Step 6

In the Recover Server dialog box, click Reset CMOS, then click OK.

---

**Resetting the CIMC for a Blade Server**

Sometimes, with the firmware, troubleshooting a server might require you to reset the CIMC. Resetting the CIMC is not part of the normal maintenance of a server. After you reset the CIMC, the CIMC reboots with the running version of the firmware for that server.

If the CIMC is reset, the power monitoring functions of Cisco UCS become briefly unavailable until the CIMC reboots. Typically, the reset only takes 20 seconds; however, it is possible that the peak power cap can exceed during that time. To avoid exceeding the configured power cap in a low power-capped environment, consider staggering the rebooting or activation of CIMCs.

**Procedure**

**Step 1**

In the Navigation pane, click Equipment.

**Step 2**

Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**

Choose the server for which you want to reset the CIMC.

**Step 4**

In the Work pane, click the General tab.

**Step 5**

In the Actions area, click Recover Server.

**Step 6**

In the Recover Server dialog box, click Reset CIMC (Server Controller), then click OK.

---

**Clearing TPM for a Blade Server**

You can clear TPM only on Cisco UCS M4 and higher blade and rack-mount servers that include support for TPM.

⚠️ **Caution**

Clearing TPM is a potentially hazardous operation. The OS may stop booting. You may also see loss of data.

**Before you begin**

TPM must be enabled.

**Procedure**

**Step 1**

In the Navigation pane, click Equipment.

**Step 2**

Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**

Choose the server for which you want to clear TPM.

**Step 4**

In the Work pane, click the General tab.
Step 5  In the Actions area, click Recover Server.
Step 6  In the Recover Server dialog box, click Clear TPM, then click OK.

Viewing the POST Results for a Blade Server

You can view any errors collected during the Power On Self-Test process for a server and its adapters.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server for which you want to view the POST results.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click View POST Results.

The POST Results dialog box lists the POST results for the server and its adapters.

Step 6  (Optional) Click the link in the Affected Object column to view the properties of that adapter.
Step 7  Click OK to close the POST Results dialog box.

Issuing an NMI from a Blade Server

Perform the following procedure if the system remains unresponsive and you need Cisco UCS Manager to issue a Non-Maskable Interrupt (NMI) to the BIOS or operating system from the CIMC. This action creates a core dump or stack trace, depending on the operating system installed on the server.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server that you want to issue the NMI.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Server Maintenance.
Step 6  In the Maintenance dialog box, do the following:
   a) Click Diagnostic Interrupt.
   b) Click OK.

Cisco UCS Manager sends an NMI to the BIOS or operating system.
Viewing Health Events for a Blade Server

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server for which you want to view health events.
Step 4  In the Work pane, click the Health tab.

The health events triggered for this server appear. The fields in this tab are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Summary area</td>
<td>Comma-separated names of all the health events that are triggered for the component.</td>
</tr>
<tr>
<td>Health Qualifier field</td>
<td>Comma-separated names of all the health events that are triggered for the component.</td>
</tr>
</tbody>
</table>
| Health Severity field                | Highest severity of all the health events that are triggered for the component. This can be one of the following:  
• critical  
• major  
• minor  
• warning  
• info  
• cleared  
| Note                                 | The severity levels listed here are from highest to lowest severity.         |
| Health Details area                  |                                                                             |
### Health LED Alarms

The blade health LED is located on the front of each Cisco UCS B-Series blade server. Cisco UCS Manager allows you to view the sensor faults that cause the blade health LED to change color from green to amber or blinking amber.

The health LED alarms display the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity</strong></td>
<td>The severity of the alarm. This can be one of the following:</td>
</tr>
<tr>
<td><strong>column</strong></td>
<td>• Critical—The blade health LED is blinking amber. This is indicated with a</td>
</tr>
<tr>
<td></td>
<td>red dot.</td>
</tr>
<tr>
<td></td>
<td>• Minor—The blade health LED is amber. This is indicated with an orange dot.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A brief description of the alarm.</td>
</tr>
<tr>
<td><strong>column</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Sensor ID</strong></td>
<td>The ID of the sensor that triggered the alarm.</td>
</tr>
<tr>
<td><strong>column</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Viewing Health LED Alarms

**Procedure**

1. **Step 1** In the **Navigation** pane, click **Equipment**.
2. **Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
3. **Step 3** Click the server for which you want to view health LED alarms.
4. **Step 4** In the **Work** pane, click the **General** tab.
5. **Step 5** In the **Actions** area, click **View Health LED Alarms**.

The **View Health LED Alarms** dialog box lists the health LED alarms for the selected server.

6. **Step 6** Click **OK** to close the **View Health LED Alarms** dialog box.

---

### Smart SSD

Beginning with release 3.1(3), Cisco UCS Manager supports monitoring SSD health. This feature is called Smart SSD. It provides statistical information about the properties like wear status in days, percentage life remaining, and so on. For every property, a minimum, a maximum and an average value is recorded and displayed. The feature also allows you to provide threshold limit for the properties.

**Note**

The Smart SSD feature is supported only for a selected range of SSDs. It is not supported for any HDDs.

The SATA range of supported SSDs are:

- Intel
- Samsung
- Micron

The SAS range of supported SSDs are:

- Toshiba
- Sandisk
- Samsung
- Micron
• Power-On Hours and Power Cycle Count are not available on SAS SSDs.

• Smart SSD feature is supported only on M4 servers and later.

---

### Monitoring SSD Health

#### Procedure

**Step 1** Navigate to **Equipment > Rack-Mounts > Servers > Server Number > Inventory > Storage**.

**Step 2** Click the controller component for which you want to view the SSD health.

**Step 3** In the **Work** pane, click the **Statistics** tab.

**Step 4** Click the SSD for which you want to view the health properties.

You can view the values for

- **PercentageLifeLeft**: Displays the duration of life so action can be taken when required.
- **PowerCycleCount**: Displays the number of times the SSD is power cycled across the server reboot.
- **PowerOnHours**: Displays the duration for which the SSD is on. You can replace or turn the SSD off based on the requirement.

**Note** If there is a change in any other property, updated **PowerOnHours** is displayed.

- **WearStatusInDays**: Provides guidance about the SSD wear based on the workload characteristics run at that time.

**Note** These values are updated on an hourly basis.

You can specify the threshold limit for the values and faults are raised when the value reaches or exceeds the threshold limit. Smart SSD feature tracks temperature and raises a fault as the temperature crosses the threshold limit (90°C) and moves the disk to the degraded state notifying the reason for degradation.

---

*Cisco UCS Manager Server Management Guide, Release 3.1*
CHAPTER 7

Rack-Mount Server Hardware Management

- Rack-Mount Server Management, on page 59
- Guidelines for Removing and Decommissioning Rack-Mount Servers, on page 60
- Recommendations for Avoiding Unexpected Server Power Changes, on page 60
- Booting a Rack-Mount Server, on page 61
- Booting a Rack-Mount Server from the Service Profile , on page 62
- Determining the Boot Order of a Rack-Mount Server, on page 62
- Shutting Down a Rack-Mount Server, on page 63
- Shutting Down a Server from the Service Profile , on page 63
- Resetting a Rack-Mount Server, on page 64
- Resetting a Rack-Mount Server to Factory Default Settings, on page 64
- Reacknowledging a Rack-Mount Server, on page 65
- Deleting the Inband Configuration from a Rack-Mount Server, on page 66
- Decommissioning a Rack-Mount Server, on page 66
- Recommissioning a Rack-Mount Server, on page 67
- Renumbering a Rack-Mount Server, on page 67
- Removing a Non-Existent Rack-Mount Server from the Configuration Database, on page 68
- Turning the Locator LED for a Rack-Mount Server On and Off, on page 68
- Turning the Local Disk Locator LED on a Rack-Mount Server On and Off, on page 69
- Resetting the CMOS for a Rack-Mount Server, on page 69
- Resetting the CIMC for a Rack-Mount Server, on page 70
- Clearing TPM for a Rack-Mount Server, on page 70
- Issuing an NMI from a Rack-Mount Server, on page 71
- Viewing Health Events for a Rack-Mount Server, on page 71
- Viewing the POST Results for a Rack-Mount Server, on page 73
- Viewing the Power Transition Log, on page 73

Rack-Mount Server Management

You can manage and monitor all rack-mount servers that are integrated with a Cisco UCS domain through Cisco UCS Manager. All management and monitoring features are supported for rack-mount servers except power capping. Some rack-mount server management tasks, such as changes to the power state, can be performed from both the server and service profile. The remaining management tasks can only be performed on the server.
Cisco UCS Manager provides information, errors, and faults for each rack-mount server that it has discovered.

Tip
For information on how to integrate a supported Cisco UCS rack-mount server with Cisco UCS Manager, see the Cisco UCS C-series server integration guide or Cisco UCS S-series server integration guide for your Cisco UCS Manager release.

Guidelines for Removing and Decommissioning Rack-Mount Servers

Consider the following guidelines when deciding whether to remove or decommission a rack-mount server using Cisco UCS Manager:

Decommissioning a Rack-Mount server
Decommissioning is performed when a rack-mount server is physically present and connected but you want to temporarily remove it from the configuration. Because it is expected that a decommissioned rack-mount server will be eventually recommissioned, a portion of the server's information is retained by Cisco UCS Manager for future use.

Removing a Rack-Mount server
Removing is performed when you physically remove the server from the system by disconnecting the rack-mount server from the fabric extender. You cannot remove a rack-mount server from Cisco UCS Manager if it is physically present and connected to the fabric extender. Once the rack-mount server is disconnected, the configuration for that rack-mount server can be removed in Cisco UCS Manager.

During removal, management interfaces are disconnected, all entries from databases are removed, and the server is automatically removed from any server pools that it was assigned to during discovery.

Note
Only those servers added to a server pool automatically during discovery will be removed automatically. Servers that have been manually added to a server pool have to be removed manually.

If you need to add a removed rack-mount server back to the configuration, it must be reconnected and then rediscovered. When a server is reintroduced to Cisco UCS Manager it is treated like a new server and is subject to the deep discovery process. For this reason, it's possible that Cisco UCS Manager will assign the server a new ID that may be different from the ID that it held before.

Recommendations for Avoiding Unexpected Server Power Changes

If a server is not associated with a service profile, you can use any available means to change the server power state, including the physical **Power** or **Reset** buttons on the server.
If a server is associated with, or assigned to, a service profile, you should only use the following methods to change the server power state:

- In Cisco UCS Manager GUI, go to the General tab for the server or the service profile associated with the server and select Boot Server or Shutdown Server from the Actions area.
- In Cisco UCS Manager CLI, scope to the server or the service profile associated with the server and use the power up or power down commands.

**Important**

Do not use any of the following options on an associated server that is currently powered off:

- Reset in the GUI
- cycle cycle-immediate or reset hard-reset-immediate in the CLI
- The physical Power or Reset buttons on the server

If you reset, cycle, or use the physical power buttons on a server that is currently powered off, the server's actual power state might become out of sync with the desired power state setting in the service profile. If the communication between the server and Cisco UCS Manager is disrupted or if the service profile configuration changes, Cisco UCS Manager might apply the desired power state from the service profile to the server, causing an unexpected power change.

Power synchronization issues can lead to an unexpected server restart, as shown below:

<table>
<thead>
<tr>
<th>Desired Power State in Service Profile</th>
<th>Current Server Power State</th>
<th>Server Power State After Communication Is Disrupted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Powered Off</td>
<td>Powered On</td>
</tr>
<tr>
<td>Down</td>
<td>Powered On</td>
<td>Powered On</td>
</tr>
</tbody>
</table>

**Note**

Running servers are not shut down regardless of the desired power state in the service profile.

**Booting a Rack-Mount Server**

If the Boot Server link is dimmed in the Actions area, you must shut down the server first.

**Procedure**

**Step 1** In the Navigation pane, click Equipment.
**Step 2** Expand Equipment > Rack Mounts > Servers.
**Step 3** Choose the server that you want to boot.
**Step 4** In the Work pane, click the General tab.
**Step 5** In the Actions area, click Boot Server.
Step 6 If a confirmation dialog box displays, click Yes.

After the server boots, the Overall Status field on the General tab displays an OK status.

## Booting a Rack-Mount Server from the Service Profile

### Procedure

**Step 1** In the Navigation pane, click Servers.
**Step 2** Expand Servers > Service Profiles.
**Step 3** Expand the node for the organization where you want to create the service profile.
If the system does not include multitenancy, expand the root node.
**Step 4** Choose the service profile that requires the associated server to boot.
**Step 5** In the Work pane, click the General tab.
**Step 6** In the Actions area, click Boot Server.
**Step 7** If a confirmation dialog box displays, click Yes.
**Step 8** Click OK in the Boot Server dialog box.
After the server boots, the Overall Status field on the General tab displays an ok status or an up status.

## Determining the Boot Order of a Rack-Mount Server

**Tip** You can also view the boot order tabs from the General tab of the service profile associated with a server.

### Procedure

**Step 1** In the Navigation pane, click Equipment.
**Step 2** Expand Equipment > Rack Mounts > Servers.
**Step 3** Click the server for which you want to determine the boot order.
**Step 4** In the Work pane, click the General tab.
**Step 5** If the Boot Order Details area is not expanded, click the Expand icon to the right of the heading.
**Step 6** To view the boot order assigned to the server, click the Configured Boot Order tab.
**Step 7** To view what will boot from the various devices in the physical server configuration, click the Actual Boot Order tab.
The Actual Boot Order tab always shows "Internal EFI Shell" at the bottom of the boot order list.

Shutting Down a Rack-Mount Server

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence. If the Shutdown server link is dimmed in the Actions area, the server is not running.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > Servers.
Step 3 Choose the server that you want to shut down.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Shutdown Server.
Step 6 If a confirmation dialog box displays, click Yes.

After the server has been successfully shut down, the Overall Status field on the General tab displays a power-off status.

Shutting Down a Server from the Service Profile

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence. If the Shutdown Server link is dimmed in the Actions area, the server is not running.

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Service Profiles.
Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multitenancy, expand the root node.
Step 4 Choose the service profile that requires the associated server to shut down.
Step 5 In the Work pane, click the General tab.
Step 6 In the Actions area, click Shutdown Server.
Step 7 If a confirmation dialog box displays, click Yes.
After the server successfully shuts down, the Overall Status field on the General tab displays a down status or a power-off status.

Resetting a Rack-Mount Server

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shut down the operating system. If the operating system does not support a graceful shutdown, the server is power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee the completion of these operations before the server is reset.

If you are trying to boot a server from a power-down state, you should not use Reset.

If you continue the power-up with this process, the desired power state of the servers become out of sync with the actual power state and the servers might unexpectedly shut down at a later time. To safely reboot the selected servers from a power-down state, click Cancel, then select the Boot Server action.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > Servers.
Step 3 Choose the server that you want to reset.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Reset.
Step 6 In the Reset Server dialog box, do the following:
   a) Click the Power Cycle option.
   b) (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.
   c) Click OK.

The reset may take several minutes to complete. After the server is reset, the Overall Status field on the General tab displays an ok status.

Resetting a Rack-Mount Server to Factory Default Settings

You can now reset a rack-mount server to its factory settings. By default, the factory reset operation does not affect storage, including storage drives and flexflash drives. This is to prevent any loss of data. However, you can choose to reset these devices to a known state as well.

Important

Resetting storage devices will result in loss of data.
Perform the following procedure to reset the server to factory default settings.

Procedure

Step 1: In the Navigation pane, click Equipment.
Step 2: Expand Equipment > Rack Mounts > Servers.
Step 3: Choose the server that you want to reset to its factory default settings.
Step 4: In the Work pane, click the General tab.
Step 5: In the Actions area, click Server Maintenance.
Step 6: In the Maintenance dialog box, click Reset to Factory Default, then click OK.
Step 7: From the Maintenance Server dialog box that appears, select the appropriate options:
   • To delete all storage, check the Scrub Storage checkbox.
   • To place all disks into their initial state after deleting all storage, check the Create Initial Volumes checkbox.

You can check this checkbox only if you check the Scrub Storage checkbox. For servers that support JBOD, the disks will be placed in a JBOD state. For servers that do not support JBOD, each disk will be initialized with a single R0 volume that occupies all the space in the disk.

Important: Do not check the Create Initial Volumes checkbox if you want to use storage profiles. Creating initial volumes when you are using storage profiles may result in configuration errors.

• To delete all flexflash storage, check the Scrub FlexFlash checkbox.

Cisco UCS Manager resets the server to its factory default settings.

Reacknowledging a Rack-Mount Server

Perform the following procedure to rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

Procedure

Step 1: In the Navigation pane, click Equipment.
Step 2: Expand Equipment > Rack Mounts > Servers.
Step 3: Choose the server that you want to acknowledge.
Step 4: In the Work pane, click the General tab.
Step 5: In the Actions area, click Server Maintenance.
Step 6: In the Maintenance dialog box, do the following:
   a) Click Re-acknowledge.
   b) Click OK.
Cisco UCS Manager disconnects the server, then builds the connections between the server and the fabric interconnect or fabric interconnects in the system. The acknowledgment may take several minutes to complete. After the server is acknowledged, the **Overall Status** field on the **General** tab displays an OK status.

---

**Deleting the Inband Configuration from a Rack-Mount Server**

This procedure removes the inband management IP address configuration from a rack server. If this action is greyed out, no inband configuration was configured.

**Procedure**

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Equipment** > **Rack Mounts** > **Servers** > **Server Number**.

**Step 3** In the **Work** area, click the **Inventory** tab.

**Step 4** Click the **CIMC** subtab.

**Step 5** In the **Actions** area, click **Delete Inband Configuration**.

**Step 6** Click **Yes** in the **Delete** confirmation dialog box.

The inband configuration for the server is deleted.

**Note** If an inband service profile is configured in Cisco UCS Manager with a default VLAN and pool name, the server CIMC automatically gets an inband configuration from the inband profile approximate one minute after deleting the inband configuration here.

---

**Decommissioning a Rack-Mount Server**

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.

**Step 2** Expand **Equipment** > **Rack Mounts** > **Servers**.

**Step 3** Choose the server that you want to decommission.

**Step 4** In the **Work** pane, click the **General** tab.

**Step 5** In the **Actions** area, click **Server Maintenance**.

**Step 6** In the **Maintenance** dialog box, click **Decommission**, then click **OK**.

The server is removed from the Cisco UCS configuration.
Recommissioning a Rack-Mount Server

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Under Equipment, click the Rack-Mounts node.</td>
</tr>
<tr>
<td>3</td>
<td>In the Work pane, click the Decommissioned tab.</td>
</tr>
</tbody>
</table>
| 4      | On the row for each rack-mount server that you want to recommission, do the following:  
|        |   a) In the Recommission column, check the check box.  
|        |   b) Click Save Changes |
| 5      | If a confirmation dialog box displays, click Yes. |
| 6      | (Optional) Monitor the progress of the server recommission and discovery on the FSM tab for the server. |

Renumbering a Rack-Mount Server

**Before you begin**

If you are swapping IDs between servers, you must first decommission both servers, then wait for the server decommission FSM to complete before proceeding with the renumbering steps.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Expand Equipment &gt; Rack Mounts &gt; Servers.</td>
</tr>
</tbody>
</table>
| 3      | Expand the Servers node and verify that it does not include the following:  
|        |   • The rack-mount server you want to renumber  
|        |   • A rack-mount server with the number you want to use |
|        | If either of these servers are listed in the Servers node, decommission those servers. You must wait until the decommission FSM is complete and the servers are not listed in the node before continuing. This might take several minutes. |
| 4      | Choose the rack-mount server that you want to renumber. |
| 5      | On the Equipment tab, click the Rack-Mounts node. |
| 6      | In the Work pane, click the Decommissioned tab. |
| 7      | On the row for each rack-mount server that you want to renumber, do the following:  
|        |   a) Double-click in the ID field, and enter the new number that you want to assign to the rack-mount server.  
|        |   b) In the Recommission column, check the check box.  
|        |   c) Click Save Changes |
Step 8 If a confirmation dialog box displays, click Yes.

Step 9 (Optional) Monitor the progress of the server recommission and discovery on the FSM tab for the server.

---

Removing a Non-Existent Rack-Mount Server from the Configuration Database

Perform the following procedure if you physically removed the server hardware without first decommissioning the server. You cannot perform this procedure if the server is physically present.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > Servers.
Step 3 Choose the server that you want to remove from the configuration database.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Server Maintenance.
Step 6 In the Maintenance dialog box, click Remove, then click OK.

Cisco UCS Manager removes all data about the server from its configuration database. The server slot is now available for you to insert new server hardware.

---

Turning the Locator LED for a Rack-Mount Server On and Off

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > Servers.
Step 3 Choose the server for which you want to turn the locator LED on or off.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click one of the following:
   • Turn on Locator LED
   • Turn off Locator LED
Turning the Local Disk Locator LED on a Rack-Mount Server On and Off

Before you begin

• Ensure the server, on which the disk is located, is powered on. If the server is off, you are unable to turn on or off the local disk locator LED.

Procedure

**Step 1**
In the Navigation pane, click Equipment.

**Step 2**
Expand Equipment > Rack Mounts > Servers.

**Step 3**
Choose the server for which you want to turn the local disk locator LED on or off.

**Step 4**
In the Work pane, click the Inventory > Storage > Disks tabs.
The Storage Controller inventory appears.

**Step 5**
Click a disk.
The disk details appear.

**Step 6**
In the Details area, click Toggle Locator LED.
If the Locator LED state is On, it will turn Off. If the Locator LED state is Off, it will turn On.

**Step 7**
Click Save Changes.

Resetting the CMOS for a Rack-Mount Server

Sometimes, troubleshooting a server might require you to reset the CMOS. Resetting the CMOS is not part of the normal maintenance of a server.

Procedure

**Step 1**
In the Navigation pane, click Equipment.

**Step 2**
Expand Equipment > Rack Mounts > Servers.

**Step 3**
Choose the server for which you want to reset the CMOS.

**Step 4**
In the Work pane, click the General tab.

**Step 5**
In the Actions area, click Recover Server.

**Step 6**
In the Recover Server dialog box, click Reset CMOS, then click OK.
Resetting the CIMC for a Rack-Mount Server

Sometimes, with the firmware, troubleshooting a server might require you to reset the CIMC. Resetting the CIMC is not part of the normal maintenance of a server. After you reset the CIMC, the CIMC reboots with the running version of the firmware for that server.

**Procedure**

1. In the **Navigation** pane, click **Equipment**.
2. Expand **Equipment** > **Rack Mounts** > **Servers**.
3. Choose the server for which you want to reset the CIMC.
4. In the **Work** pane, click the **General** tab.
5. In the **Actions** area, click **Recover Server**.
6. In the **Recover Server** dialog box, click **Reset CIMC (Server Controller)**, then click **OK**.

Clearing TPM for a Rack-Mount Server

You can clear TPM only on Cisco UCS M4 and higher blade and rack-mount servers that include support for TPM.

**Caution**

Clearing TPM is a potentially hazardous operation. The OS may stop booting. You may also see loss of data.

**Before you begin**

TPM must be enabled.

**Procedure**

1. In the **Navigation** pane, click **Equipment**.
2. Expand **Equipment** > **Rack Mounts** > **Servers**.
3. Choose the server for which you want to clear TPM.
4. In the **Work** pane, click the **General** tab.
5. In the **Actions** area, click **Recover Server**.
6. In the **Recover Server** dialog box, click **Clear TPM**, then click **OK**.
Issuing an **NMI** from a Rack-Mount Server

Perform the following procedure if the system remains unresponsive and you need Cisco UCS Manager to issue a Non-Maskable Interrupt (NMI) to the BIOS or operating system from the CIMC. This action creates a core dump or stack trace, depending on the operating system installed on the server.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click <strong>Equipment</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand <strong>Equipment &gt; Rack Mounts &gt; Servers</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server that you want to issue the NMI.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the <strong>General</strong> tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click <strong>Server Maintenance</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Maintenance dialog box, click <strong>Diagnostic Interrupt</strong>, then click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

Cisco UCS Manager sends an NMI to the BIOS or operating system.

---

Viewing Health Events for a Rack-Mount Server

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click <strong>Equipment</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand <strong>Equipment &gt; Rack Mounts &gt; Servers</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server for which you want to view health events.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the <strong>Health</strong> tab</td>
</tr>
</tbody>
</table>

The health events triggered for this server appear. The fields in this tab are:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health Summary</strong> area</td>
<td></td>
</tr>
<tr>
<td><strong>Health Qualifier</strong> field</td>
<td>Comma-separated names of all the health events that are triggered for the component.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Health Severity field | Highest severity of all the health events that are triggered for the component. This can be one of the following:  
  • critical  
  • major  
  • minor  
  • warning  
  • info  
  • cleared  
  **Note** The severity levels listed here are from highest to lowest severity. |

**Health Details area**

| **Severity column** | Severity of the health event. This can be one of the following:  
  • critical  
  • major  
  • minor  
  • warning  
  • info  
  • cleared  
  **Note** The severity levels listed here are from highest to lowest severity. |

| Name column | Name of the health event. |
| Description column | Detailed description of the health event. |
| Value column | Current value of the health event. |

**Details area**

The **Details** area displays the **Name**, **Description**, **Severity**, and **Value** details of any health event that you select in the **Health Details area**.
Viewing the POST Results for a Rack-Mount Server

You can view any errors collected during the Power On Self-Test process for a server and its adapters.

Procedure

**Step 1** In the Navigation pane, click **Equipment**.
**Step 2** Expand **Equipment > Rack Mounts > Servers**.
**Step 3** Choose the server for which you want to view the POST results.
**Step 4** In the Work pane, click the **General** tab.
**Step 5** In the Actions area, click **View POST Results**.

The POST Results dialog box lists the POST results for the server and its adapters.

**Step 6** (Optional) Click the link in the **Affected Object** column to view the properties of that adapter.
**Step 7** Click **OK** to close the POST Results dialog box.

Viewing the Power Transition Log

You can view the **Power Transition Log**, which displays the last five server power transitions. The information provided includes the **Power Change Source** and the **Timestamp**.

Only unique power transition events are displayed. In case of a UCSM initiated power transition, the FSM causing the power transition is displayed.

Procedure

**Step 1** Navigate to **Equipment > Rack-Mounts > Servers**
**Step 2** Choose the server for which you want to view the power transition log.

The Power Transition Log is under the **General** tab.
Viewing the Power Transition Log
Compute Cartridge Hardware Management

- Compute Cartridges, on page 75
- Removing a Cartridge, on page 75
- Acknowledging a Cartridge Slot in a Chassis, on page 75

Compute Cartridges

Compute cartridges consist of up to two Cisco UCS modular servers. Each individual server is independently manageable through its own CIMC instance, and has its own memory and CPU. The cartridge does not contain any I/O adapters or local storage within it.

Removing a Cartridge

Physically remove the cartridge from its chassis before performing the following procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; Cartridges</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the cartridge that you want to remove from the configuration database.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Remove Cartridge, then click OK.</td>
</tr>
</tbody>
</table>

Cisco UCS Manager removes all data about the cartridge from its configuration database. The cartridge slot is now available for you to insert new cartridge hardware.

Acknowledging a Cartridge Slot in a Chassis

When a cartridge is replaced by another cartridge or relocated to a new slot in the same chassis or a different chassis, it goes into the mismatch state and the Re-acknowledge Slot action becomes available. Perform the following steps to re-acknowledge the cartridge slot if the cartridge slot is in the mismatch state.
Note When you swap two cartridges, acknowledging one of the cartridges automatically resolves the slot status of both slots.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Cartridges
Step 3 Choose the cartridge that you want to re-acknowledge.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Re-acknowledge Slot, then click OK.
Modular Server Hardware Management

- Modular Server Management, on page 77
- Booting a Modular Server, on page 77
- Booting a Rack-Mount Server from the Service Profile, on page 78
- Determining the Boot Order of a Modular Server, on page 78
- Shutting Down a Modular Server, on page 79
- Shutting Down a Server from the Service Profile, on page 79
- Resetting a Modular Server, on page 80
- Reacknowledging a Modular Server, on page 80
- Deleting the Inband Configuration from a Modular Server, on page 81
- Decommissioning a Server, on page 81
- Recommissioning a Modular Server, on page 82
- Turning the Locator LED for a Server On and Off, on page 82
- Turning the Local Disk Locator LED on a Modular Server On and Off, on page 83
- Resetting the CMOS for a Modular Server, on page 83
- Resetting the CIMC for a Modular Server, on page 84
- Issuing an NMI from a Server, on page 84
- Viewing Health Events on a Server, on page 85
- Health LED Alarms, on page 86
- Viewing the POST Results for a Modular Server, on page 87

Modular Server Management

Modular servers are contained in compute cartridges. You cannot remove servers from their cartridges.

Booting a Modular Server

If the Boot Server link is dimmed in the Actions area, you must shut down the server first.

Procedure

Step 1 In the Navigation pane, click Equipment.
Booting a Rack-Mount Server from the Service Profile

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles.
Step 3  Expand the node for the organization where you want to create the service profile.
        If the system does not include multitenancy, expand the root node.
Step 4  Choose the service profile that requires the associated server to boot.
Step 5  In the Work pane, click the General tab.
Step 6  In the Actions area, click Boot Server.
Step 7  If a confirmation dialog box displays, click Yes.
Step 8  Click OK in the Boot Server dialog box.

After the server boots, the Overall Status field on the General tab displays an OK status.

Determining the Boot Order of a Modular Server

Tip
You can also view the boot order tabs from the General tab of the service profile associated with a server.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3  Click the server for which you want to determine the boot order.
Step 4  In the Work pane, click the General tab.
Step 5  If the Boot Order Details area is not expanded, click the Expand icon to the right of the heading.
Step 6
To view the boot order assigned to the server, click the Configured Boot Order tab.

Step 7
To view what will boot from the various devices in the physical server configuration, click the Actual Boot Order tab.

Note The Actual Boot Order tab always shows "Internal EFI Shell" at the bottom of the boot order list.

---

Shutting Down a Modular Server

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the Shutdown Server link is dimmed in the Actions area, the server is not running.

Procedure

Step 1
In the Navigation pane, click Equipment.

Step 2
Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers

Step 3
Choose the server that you want to shut down.

Step 4
In the Work pane, click the General tab.

Step 5
In the Actions area, click Shutdown Server.

Step 6
If a confirmation dialog box displays, click Yes.

After the server has been successfully shut down, the Overall Status field on the General tab displays a power-off status.

---

Shutting Down a Server from the Service Profile

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the Shutdown Server link is dimmed in the Actions area, the server is not running.

Procedure

Step 1
In the Navigation pane, click Servers.

Step 2
Expand Servers > Service Profiles.

Step 3
Expand the node for the organization where you want to create the service profile.

If the system does not include multitenancy, expand the root node.

Step 4
Choose the service profile that requires the associated server to shut down.

Step 5
In the Work pane, click the General tab.
Step 6  
In the **Actions** area, click **Shutdown Server**.

Step 7  
If a confirmation dialog box displays, click **Yes**.

After the server successfully shuts down, the **Overall Status** field on the **General** tab displays a down status or a power-off status.

---

**Resetting a Modular Server**

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shut down the operating system. If the operating system does not support a graceful shutdown, the server is power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee the completion of these operations before the server is reset.

---

**Note**

If you are trying to boot a server from a power-down state, you should not use **Reset**.

If you continue the power-up with this process, the desired power state of the servers become out of sync with the actual power state and the servers might unexpectedly shut down at a later time. To safely reboot the selected servers from a power-down state, click **Cancel**, then select the **Boot Server** action.

---

**Procedure**

1. **Step 1** In the **Navigation** pane, click **Equipment**.
2. **Step 2** Expand **Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers**
3. **Step 3** Choose the server that you want to reset.
4. **Step 4** In the **Work** pane, click the **General** tab.
5. **Step 5** In the **Actions** area, click **Reset**.
6. **Step 6** In the **Reset Server** dialog box, do the following:
   a) Click the **Power Cycle** option.
   b) (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.
   c) Click **OK**.

The reset may take several minutes to complete. After the server has been reset, the **Overall Status** field on the **General** tab displays an ok status.

---

**Reacknowledging a Modular Server**

Perform the following procedure to rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.
Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3  Choose the server that you want to acknowledge.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Server Maintenance.
Step 6  In the Maintenance dialog box, click Re-acknowledge, then click OK.

Cisco UCS Manager disconnects the server and then builds the connections between the server and the fabric interconnect or fabric interconnects in the system. The acknowledgment may take several minutes to complete. After the server has been acknowledged, the Overall Status field on the General tab displays an OK status.

Deleting the Inband Configuration from a Modular Server

This procedure removes the inband management IP address configuration from a server. If this action is greyed out, no inband configuration was completed.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3  Choose the server for which you want to delete the inband management IP configuration.
Step 4  In the Work area, click the Inventory tab.
Step 5  Click the CIMC subtab.
Step 6  In the Actions area, click Delete Inband Configuration.
Step 7  Click Yes in the Delete confirmation dialog box.

The inband configuration for the server is deleted.

Note  If an inband service profile is configured in Cisco UCS Manager with a default VLAN and pool name, the server CIMC will automatically get an inband configuration from the inband profile approximate one minute after deleting the inband configuration here.

Decommissioning a Server

Decommissioning of a server is performed to temporarily remove the server from the UCSM configuration.
Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3  Choose the server that you want to decommission.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Server Maintenance.
Step 6  In the Maintenance dialog box, do the following:
   a) Click Decommission.
   b) Click OK.

The server is removed from the Cisco UCS configuration.

What to do next

If you physically re-install the server, you must re-acknowledge the slot to have Cisco UCS Manager rediscover the server.

Recommissioning a Modular Server

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment node.
Step 3  Click the Chassis node.
Step 4  In the Work pane, click the Decommissioned tab.
Step 5  On the row for each server that you want to recommission, check the check box in the Recommission column, then click Save Changes.
Step 6  If a confirmation dialog box displays, click Yes.
Step 7  (Optional) Monitor the progress of the server recommission and discovery on the FSM tab for the server.

Turning the Locator LED for a Server On and Off

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3 Choose the server for which you want to turn the locator LED on or off.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click one of the following:
• Turn on Locator LED—Turns on the LED for the selected server.
• Turn off Locator LED—Turns off the LED for the selected server.

Turning the Local Disk Locator LED on a Modular Server On and Off

Before you begin
• Ensure the server, on which the disk is located, is powered on. If the server is off, you are unable to turn on or off the local disk locator LED.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3 Choose the server for which you want to turn the local disk locator LED on or off.
Step 4 In the Work pane, click the Inventory > Storage > Disks tabs. The Storage Controller inventory appears.
Step 5 Click a disk. The disk details appear.
Step 6 In the Details area, click Toggle Locator LED. If the Locator LED state is On, it will turn Off. If the Locator LED state is Off, it will turn On.
Step 7 Click Save Changes.

Resetting the CMOS for a Modular Server

Sometimes, troubleshooting a server might require you to reset the CMOS. Resetting the CMOS is not part of the normal maintenance of a server.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3 Choose the server for which you want to reset the CMOS.
Resetting the CIMC for a Modular Server

Sometimes, with the firmware, troubleshooting a server might require you to reset the CIMC. Resetting the CIMC is not part of the normal maintenance of a server. After you reset the CIMC, the CIMC reboots with the running version of the firmware for that server.

If the CIMC is reset, the power monitoring functions of Cisco UCS become briefly unavailable until the CIMC reboots. Typically, the reset only takes 20 seconds; however, it is possible that the peak power cap can exceed during that time. To avoid exceeding the configured power cap in a low power-capped environment, consider staggering the rebooting or activation of CIMCs.

**Procedure**

1. In the Navigation pane, click Equipment.
2. Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
3. Choose the server for which you want to reset the CIMC.
4. In the Work pane, click the General tab.
5. In the Actions area, click Recover Server.
6. In the Recover Server dialog box, click Reset CMOS, then click OK.

Issuing an NMI from a Server

Perform the following procedure if the system remains unresponsive and you need Cisco UCS Manager to issue a Non-Maskable Interrupt (NMI) to the BIOS or operating system from the CIMC. This action creates a core dump or stack trace, depending on the operating system installed on the server.

**Procedure**

1. In the Navigation pane, click Equipment.
2. Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
3. Choose the server from which you want to issue the NMI.
4. In the Work pane, click the General tab.
5. In the Actions area, click Server Maintenance.
6. In the Maintenance dialog box, do the following:
   a) Click Diagnostic Interrupt.
   b) Click OK.
Cisco UCS Manager sends an NMI to the BIOS or operating system.

Viewing Health Events on a Server

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; Cartridges &gt; Cartridge Number &gt; Servers</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server for which you want to view health events.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the Health tab</td>
</tr>
</tbody>
</table>

The health events triggered for this server appear. The fields in this tab are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health Summary area</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Health Qualifier field</strong></td>
<td>Comma-separated names of all the health events that are triggered for the component.</td>
</tr>
<tr>
<td><strong>Health Severity field</strong></td>
<td>Highest severity of all the health events that are triggered for the component. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• critical</td>
</tr>
<tr>
<td></td>
<td>• major</td>
</tr>
<tr>
<td></td>
<td>• minor</td>
</tr>
<tr>
<td></td>
<td>• warning</td>
</tr>
<tr>
<td></td>
<td>• info</td>
</tr>
<tr>
<td></td>
<td>• cleared</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The severity levels listed here are from highest to lowest severity.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Health Details area</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Health LED Alarms

The server health LED is located on the front of each Cisco UCS M-Series server. Cisco UCS Manager allows you to view the sensor faults that cause the server health LED to change color from green to amber or blinking amber.

The health LED alarms display the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity</strong> column</td>
<td>The severity of the alarm. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Critical—The blade health LED is blinking amber. This is indicated with a red dot.</td>
</tr>
<tr>
<td></td>
<td>• Minor—The blade health LED is amber. This is indicated with an orange dot.</td>
</tr>
<tr>
<td><strong>Description</strong> column</td>
<td>A brief description of the alarm.</td>
</tr>
<tr>
<td><strong>Sensor ID</strong> column</td>
<td>The ID of the sensor the triggered the alarm.</td>
</tr>
</tbody>
</table>
### Viewing Health LED Alarms

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; Cartridges &gt; Cartridge Number &gt; Servers</td>
</tr>
<tr>
<td>3</td>
<td>Click the server for which you want to view health LED alarms.</td>
</tr>
<tr>
<td>4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the Actions area, click View Health LED Alarms.</td>
</tr>
<tr>
<td>6</td>
<td>Click OK to close the View Health LED Alarms dialog box.</td>
</tr>
</tbody>
</table>

The View Health LED Alarms dialog box lists the health LED alarms for the selected server.

### Viewing the POST Results for a Modular Server

You can view any errors collected during the Power On Self-Test process for a server.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; Cartridges &gt; Cartridge Number &gt; Servers</td>
</tr>
<tr>
<td>3</td>
<td>Choose the server for which you want to view the POST results.</td>
</tr>
<tr>
<td>4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the Actions area, click View POST Results.</td>
</tr>
<tr>
<td>6</td>
<td>Click OK to close the POST Results dialog box.</td>
</tr>
</tbody>
</table>

The POST Results dialog box lists the POST results for the server.
S3X60 Server Node Hardware Management

- Cisco UCS S3260 Server Node Management, on page 89
- Booting a Cisco UCS S3260 Server Node, on page 90
- Booting a Cisco UCS S3260 Server Node from the Service Profile, on page 90
- Determining the Boot Order of a Cisco UCS S3260 Server Node, on page 90
- Shutting Down a Cisco UCS S3260 Server Node, on page 91
- Shutting Down a Cisco UCS S3260 Server Node from the Service Profile, on page 91
- Resetting a Cisco UCS S3260 Server Node, on page 92
- Resetting a Cisco UCS S3260 Server Node to Factory Default Settings, on page 93
- Reacknowledging a Cisco UCS S3260 Server Node, on page 94
- Removing a Cisco UCS S3260 Server Node from a Chassis, on page 94
- Deleting the Inband Configuration from a Cisco UCS S3260 Server Node, on page 95
- Decommissioning a Cisco UCS S3260 Server Node, on page 95
- Recommissioning a Cisco UCS S3260 Server Node, on page 96
- Reacknowledging a Server Slot in a S3260 Chassis, on page 96
- Removing a Non-Existent Cisco UCS S3260 Server Node from the Configuration Database, on page 97
- Turning the Locator LED for a Cisco UCS S3260 Server Node On and Off, on page 97
- Turning the Local Disk Locator LED on a Cisco UCS S3260 Server Node On and Off, on page 98
- Resetting the CIMC for a Cisco UCS S3260 Server Node, on page 98
- Resetting the CMOS for a Cisco UCS S3260 Server Node, on page 99
- Issuing an NMI from a Cisco UCS S3260 Server Node, on page 99
- Viewing the POST Results for a Cisco UCS S3260 Server Node, on page 100
- Viewing Health Events for a Cisco UCS S3260 Server Node, on page 100
- Health LED Alarms, on page 102

Cisco UCS S3260 Server Node Management

You can manage and monitor all Cisco UCS S3260 server nodes in a Cisco UCS domain through Cisco UCS Manager. You can perform some server management tasks, such as changes to the power state, from the server and service profile.

The remaining management tasks can only be performed on the server.

If a server slot in a chassis is empty, Cisco UCS Manager provides information, errors, and faults for that slot. You can also re-acknowledge the slot to resolve server mismatch errors and rediscover the server in the slot.
Booting a Cisco UCS S3260 Server Node

If the Boot Server link is dimmed in the Actions area, you must shut down the server first.

Procedure

**Step 1**
In the Navigation pane, click Equipment.

**Step 2**
Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**
Choose the server that you want to boot.

**Step 4**
In the Work pane, click the General tab.

**Step 5**
In the Actions area, click Boot Server.

**Step 6**
If a confirmation dialog box displays, click Yes.

After the server boots, the Overall Status field on the General tab displays an OK status.

Booting a Cisco UCS S3260 Server Node from the Service Profile

Procedure

**Step 1**
In the Navigation pane, click Servers.

**Step 2**
Expand Servers > Service Profiles.

**Step 3**
Expand the node for the organization where you want to create the service profile, or where the appropriate service profile already exists.

If the system does not include multitenancy, expand the root node.

**Step 4**
Choose the service profile that requires the associated server to boot.

**Step 5**
In the Work pane, click the General tab.

**Step 6**
In the Actions area, click Boot Server.

**Step 7**
If a confirmation dialog box displays, click Yes.

**Step 8**
Click OK in the Boot Server dialog box.

After the server boots, the Overall Status field on the General tab displays an ok status or an up status.

Determining the Boot Order of a Cisco UCS S3260 Server Node

Tip
You can also view the boot order tabs from the General tab of the service profile associated with a server.
Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Click the server for which you want to determine the boot order.
Step 4  In the Work pane, click the General tab.
Step 5  If the Boot Order Details area is not expanded, click the Expand icon to the right of the heading.
Step 6  To view the boot order assigned to the server, click the Configured Boot Order tab.
Step 7  To view what will boot from the various devices in the physical server configuration, click the Actual Boot Order tab.

Shutting Down a Cisco UCS S3260 Server Node

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the Shutdown Server link is dimmed in the Actions area, the server is not running.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server that you want to shut down.
Step 4  In the Work pane, click the General tab.
Step 5  In the Actions area, click Shutdown Server.
Step 6  If a confirmation dialog box displays, click Yes.

After the server has been successfully shut down, the Overall Status field on the General tab displays a power-off status.

Shutting Down a Cisco UCS S3260 Server Node from the Service Profile

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

If the Shutdown Server link is dimmed in the Actions area, the server is not running.
**Procedure**

**Step 1** In the *Navigation* pane, click *Servers*.

**Step 2** Expand *Servers > Service Profiles*.

**Step 3** Expand the node for the organization with the associated service profile.

**Step 4** Choose the service profile associated with the server to be shut down.

**Step 5** In the *Work* pane, click the *General* tab.

**Step 6** In the *Actions* area, click *Shutdown Server*.

**Step 7** If a confirmation dialog box displays, click *Yes*.

After the server successfully shuts down, the *Overall Status* field on the *General* tab displays a down status or a power-off status.

---

**Resetting a Cisco UCS S3260 Server Node**

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shut down the operating system. If the operating system does not support a graceful shutdown, the server is power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee the completion of these operations before the server is reset.

**Note**

If you are trying to boot a server from a power-down state, you should not use *Reset*.

If you continue the power-up with this process, the desired power state of the servers become out of sync with the actual power state and the servers might unexpectedly shut down at a later time. To safely reboot the selected servers from a power-down state, click *Cancel*, then select the *Boot Server* action.

---

**Procedure**

**Step 1** In the *Navigation* pane, click *Equipment*.

**Step 2** Expand *Equipment > Chassis > Chassis Number > Servers*.

**Step 3** Choose the server that you want to reset.

**Step 4** In the *Work* pane, click the *General* tab.

**Step 5** In the *Actions* area, click *Reset*.

**Step 6** In the *Reset Server* dialog box, do the following:

a) Click the *Power Cycle* option.

b) (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.

c) Click *OK*. 
The reset may take several minutes to complete. After the server has been reset, the Overall Status field on the General tab displays an ok status.

**Resetting a Cisco UCS S3260 Server Node to Factory Default Settings**

You can now reset a Cisco UCS S3260 Server Node to its factory settings. By default, the factory reset operation does not affect storage drives. This is to prevent any loss of data. However, you can choose to reset these devices to a known state as well.

The following guidelines apply to Cisco UCS S3260 Server Nodes when using scrub policies:

- For Cisco UCS S3260 Server Nodes, you cannot delete storage by using the scrub policy.
- Cisco UCS S3260 Server Nodes do not support FlexFlash drives.
- For Cisco UCS S3260 Server Nodes, you can only reset the BIOS by using the scrub policy.

**Important**

Resetting storage devices will result in loss of data.

Perform the following procedure to reset the server to factory default settings.

**Procedure**

**Step 1**
In the Navigation pane, click Equipment.

**Step 2**
Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**
Choose the server that you want to reset to its factory default settings.

**Step 4**
In the Work pane, click the General tab.

**Step 5**
In the Actions area, click Server Maintenance.

**Step 6**
In the Maintenance dialog box, do the following:

a) Click Reset to Factory Default.

b) Click OK.

**Step 7**
From the Maintenance Server dialog box that appears, select the appropriate options:

- To delete all storage, check the Scrub Storage check box.

  **Note** For Cisco UCS S3260 Server Nodes, you cannot delete storage using the scrub policy.

- To place all disks into their initial state after deleting all storage, check the Create Initial Volumes check box.

You can check this check box only if you check the Scrub Storage check box. For servers that support JBOD, the disks will be placed in a JBOD state. For servers that do not support JBOD, each disk will be initialized with a single R0 volume that occupies all the space in the disk.

**Important** Do not check the Create Initial Volumes box if you want to use storage profiles. Creating initial volumes when you are using storage profiles may result in configuration errors.
Reacknowledging a Cisco UCS S3260 Server Node

Perform the following procedure to rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

**Procedure**

1. In the **Navigation** pane, click **Equipment**.
2. Expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.
3. Choose the server that you want to acknowledge.
4. In the **Work** pane, click the **General** tab.
5. In the **Actions** area, click **Server Maintenance**.
6. In the **Maintenance** dialog box, click **Re-acknowledge**, then click **OK**.

Cisco UCS Manager disconnects the server and then builds the connections between the server and the fabric interconnect or fabric interconnects in the system. The acknowledgment may take several minutes to complete. After the server has been acknowledged, the **Overall Status** field on the **General** tab displays an OK status.

Removing a Cisco UCS S3260 Server Node from a Chassis

**Procedure**

1. In the **Navigation** pane, click **Equipment**.
2. Expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.
3. Choose the server that you want to remove from the chassis.
4. In the **Work** pane, click the **General** tab.
5. In the **Actions** area, click **Server Maintenance**.
6. In the **Maintenance** dialog box, click **Decommission**, then click **OK**.

The server is removed from the Cisco UCS configuration.

7. Go to the physical location of the chassis and remove the server hardware from the slot.

For instructions on how to remove the server hardware, see the Cisco UCS Hardware Installation Guide for your chassis.
What to do next

If you physically reinstall the server, you must re-acknowledge the slot for Cisco UCS Manager to re-discover the server.

Deleting the Inband Configuration from a Cisco UCS S3260 Server Node

This procedure removes the inband management IP address configuration from a blade server. If this action is grayed out, no inband configuration was completed.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; Servers &gt; Server Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work area, click the Inventory tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the CIMC subtab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Delete Inband Configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Yes in the Delete confirmation dialog box.</td>
</tr>
</tbody>
</table>

The inband configuration for the server is deleted.

Note: If an inband service profile is configured in Cisco UCS Manager with a default VLAN and pool name, the server CIMC will automatically get an inband configuration from the inband profile approximately one minute after deleting the inband configuration here.

Decommissioning a Cisco UCS S3260 Server Node

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Equipment.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Equipment &gt; Chassis &gt; Chassis Number &gt; Servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the server that you want to decommission.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Actions area, click Server Maintenance.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Maintenance dialog box, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) Click Decommission.</td>
</tr>
<tr>
<td></td>
<td>b) Click OK.</td>
</tr>
</tbody>
</table>
The server is removed from the Cisco UCS configuration.

What to do next

If you physically reinstall the server, you must re-acknowledge the slot for Cisco UCS Manager to rediscover the server.

Recommissioning a Cisco UCS S3260 Server Node

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Click the Chassis node.
Step 3 In the Work pane, click the Decommissioned tab.
Step 4 On the row for each server that you want to recommission, check the check box in the Recommission column, then click Save Changes.
Step 5 If a confirmation dialog box displays, click Yes.
Step 6 (Optional) Monitor the progress of the server recommission and discovery on the FSM tab for the server.

Reacknowledging a Server Slot in a S3260 Chassis

Perform the following procedure if you decommissioned a server without removing the physical hardware from the chassis, and you want Cisco UCS Manager to rediscover and reacknowledge the server.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Choose the server whose slot you want to reacknowledge.
Step 4 If Cisco UCS Manager displays a Resolve Slot Issue dialog box, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The here link in the Situation area</td>
<td>Click this link and then click Yes in the confirmation dialog box. Cisco UCS Manager reacknowledges the slot and discovers the server in the slot.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>OK</td>
<td>Click this button if you want to proceed to the <strong>General</strong> tab. You can use the <strong>Reacknowledge Slot</strong> link in the <strong>Actions</strong> area to have Cisco UCS Manager reacknowledge the slot and discover the server in the slot.</td>
</tr>
</tbody>
</table>

**Removing a Non-Existent Cisco UCS S3260 Server Node from the Configuration Database**

Perform the following procedure if you physically removed the server hardware without first decommissioning the server. You cannot perform this procedure if the server is physically present.

If you want to physically remove a server, see **Removing a Cisco UCS S3260 Server Node from a Chassis**, on page 94.

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** Expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.
**Step 3** Choose the server that you want to remove from the configuration database.
**Step 4** In the **Work** pane, click the **General** tab.
**Step 5** In the **Actions** area, click **Server Maintenance**.
**Step 6** In the **Maintenance** dialog box, click **Remove**, then click **OK**.

Cisco UCS Manager removes all data about the server from its configuration database. The server slot is now available for you to insert new server hardware.

**Turning the Locator LED for a Cisco UCS S3260 Server Node On and Off**

**Procedure**

**Step 1** In the **Navigation** pane, click **Equipment**.
**Step 2** Expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.
**Step 3** Choose the server for which you want to turn the locator LED on or off.
**Step 4** In the **Work** pane, click the **General** tab.
**Step 5** In the **Actions** area, click one of the following:
• **Turn on Locator LED**—Turns on the LED for the selected server.
• **Turn off Locator LED**—Turns off the LED for the selected server.

---

## Turning the Local Disk Locator LED on a Cisco UCS S3260 Server Node On and Off

### Before you begin
- Ensure that the disk is zoned. Turning the locator LED on and off cannot be done on disks that are not zoned.
- Ensure the server, on which the disk is located, is powered on. If the server is off, you are unable to turn on or off the local disk locator LED.

### Procedure

**Step 1** In the Navigation pane, click **Equipment**.

**Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.

**Step 3** Choose the server for which you want to turn the local disk locator LED on or off.

**Step 4** In the Work pane, click the **Inventory > Storage > Disks** tabs.

The Storage Controller inventory appears.

**Step 5** Click a disk.

The disk details appear.

**Step 6** In the Details area, click **Toggle Locator LED**.

If the **Locator LED** state is **On**, it will turn **Off**. If the **Locator LED** state is **Off**, it will turn **On**.

**Step 7** Click **Save Changes**.

---

## Resetting the CIMC for a Cisco UCS S3260 Server Node

Sometimes, with the firmware, troubleshooting a server might require you to reset the CIMC. Resetting the CIMC is not part of the normal maintenance of a server. After you reset the CIMC, the CIMC reboots with the running version of the firmware for that server.

If the CIMC is reset, the power monitoring functions of Cisco UCS become briefly unavailable until the CIMC reboots. Typically, the reset only takes 20 seconds; however, it is possible that the peak power cap can exceed during that time. To avoid exceeding the configured power cap in a low power-capped environment, consider staggering the rebooting or activation of CIMCs.
Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Choose the server for which you want to reset the CIMC.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Recover Server.
Step 6 In the Recover Server dialog box, click Reset CIMC (Server Controller), then click OK.

Resetting the CMOS for a Cisco UCS S3260 Server Node

Sometimes, troubleshooting a server might require you to reset the CMOS. Resetting the CMOS is not part of the normal maintenance of a server.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Choose the server for which you want to reset the CMOS.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Recover Server.
Step 6 In the Recover Server dialog box, click Reset CMOS, then click OK.

Issuing an NMI from a Cisco UCS S3260 Server Node

Perform the following procedure if the system remains unresponsive and you need Cisco UCS Manager to issue a Non-Maskable Interrupt (NMI) to the BIOS or operating system from the CIMC. This action creates a core dump or stack trace, depending on the operating system installed on the server.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Choose the server that you want to issue the NMI.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Server Maintenance.
Step 6 In the Maintenance dialog box, do the following:
   a) Click Diagnostic Interrupt.
b) Click OK. Cisco UCS Manager sends an NMI to the BIOS or operating system.

### Viewing the POST Results for a Cisco UCS S3260 Server Node

You can view any errors collected during the Power On Self-Test process for a server and its adapters.

**Procedure**

- **Step 1**: In the Navigation pane, click Equipment.
- **Step 2**: Expand Equipment > Chassis > Chassis Number > Servers.
- **Step 3**: Choose the server for which you want to view the POST results.
- **Step 4**: In the Work pane, click the General tab.
- **Step 5**: In the Actions area, click View POST Results.

The POST Results dialog box lists the POST results for the server and its adapters.

- **Step 6**: (Optional) Click the link in the Affected Object column to view the properties of that adapter.
- **Step 7**: Click OK to close the POST Results dialog box.

### Viewing Health Events for a Cisco UCS S3260 Server Node

**Procedure**

- **Step 1**: In the Navigation pane, click Equipment.
- **Step 2**: Expand Equipment > Chassis > Chassis Number > Servers.
- **Step 3**: Choose the server for which you want to view health events.
- **Step 4**: In the Work pane, click the Health tab

The health events triggered for this server appear. The fields in this tab are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Summary area</td>
<td>Comma-separated names of all the health events that are triggered for the component.</td>
</tr>
</tbody>
</table>
### Name

<table>
<thead>
<tr>
<th><strong>Health Severity field</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest severity of all the health events that are triggered for the component. This can be one of the following:</td>
<td></td>
</tr>
<tr>
<td>• critical</td>
<td></td>
</tr>
<tr>
<td>• major</td>
<td></td>
</tr>
<tr>
<td>• minor</td>
<td></td>
</tr>
<tr>
<td>• warning</td>
<td></td>
</tr>
<tr>
<td>• info</td>
<td></td>
</tr>
<tr>
<td>• cleared</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  The severity levels listed here are from highest to lowest severity.

### Health Details area

<table>
<thead>
<tr>
<th><strong>Severity column</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity of the health event. This can be one of the following:</td>
<td></td>
</tr>
<tr>
<td>• critical</td>
<td></td>
</tr>
<tr>
<td>• major</td>
<td></td>
</tr>
<tr>
<td>• minor</td>
<td></td>
</tr>
<tr>
<td>• warning</td>
<td></td>
</tr>
<tr>
<td>• info</td>
<td></td>
</tr>
<tr>
<td>• cleared</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  The severity levels listed here are from highest to lowest severity.

<table>
<thead>
<tr>
<th><strong>Name column</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the health event.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description column</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed description of the health event.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Value column</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current value of the health event.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Details area</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Details area displays the Name, Description, Severity, and Value details of any health event that you select in the Health Details area.</td>
<td></td>
</tr>
</tbody>
</table>
Health LED Alarms

The server health LED is located on the front of each server. Cisco UCS Manager allows you to view the sensor faults that cause the blade health LED to change color from green to amber or blinking amber.

The health LED alarms display the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity</strong></td>
<td>The severity of the alarm. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Critical - The server health LED blinks amber. This is indicated with a red dot.</td>
</tr>
<tr>
<td></td>
<td>• Minor - The server health LED is amber. This is indicated with an orange dot.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A brief description of the alarm.</td>
</tr>
<tr>
<td><strong>Sensor ID</strong></td>
<td>The ID of the sensor that triggered the alarm.</td>
</tr>
<tr>
<td><strong>Sensor Name</strong></td>
<td>The name of the sensor that triggered the alarm.</td>
</tr>
</tbody>
</table>

Viewing Health LED Alarms

**Procedure**

- **Step 1** In the Navigation pane, click Equipment.
- **Step 2** Expand Equipment > Chassis > Chassis Number > Servers.
- **Step 3** Click the server for which you want to view health LED alarms.
- **Step 4** In the Work pane, click the General tab.
- **Step 5** In the Actions area, click View Health LED Alarms.

The View Health LED Alarms dialog box lists the health LED alarms for the selected server.

- **Step 6** Click OK to close the View Health LED Alarms dialog box.
Server Pools

- Configuring Server Pools, on page 103
- Configuring UUID Suffix Pools, on page 105
- Configuring IP Pools, on page 107

Configuring Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multitenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

Creating a Server Pool

Procedure

**Step 1**  
In the *Navigation* pane, click *Servers*.

**Step 2**  
Expand *Servers > Pools*.

**Step 3**  
Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the *root* node.

**Step 4**  
Right-click the *Server Pools* node and select *Create Server Pool*.

**Step 5**  
On the *Set Name and Description* page of the *Create Server Pool* wizard, complete the following fields:
### Deleting a Server Pool

**Procedure**

1. **Step 1** In the Navigation pane, click Servers.
2. **Step 2** Expand Servers > Pools > Organization_Name.
3. **Step 3** Expand the Server Pools node.
4. **Step 4** Right-click the pool you want to delete and select Delete.
5. **Step 5** If a confirmation dialog box displays, click Yes.

### Adding Servers to a Server Pool

**Procedure**

1. **Step 1** In the Navigation pane, click Servers.
2. **Step 2** Expand Servers > Pools > Organization_Name.
3. **Step 3** Right-click the pool to which you want to add one or more servers and select Add Servers to Server Pool.
4. **Step 4** In the Add Servers to Server Pool dialog box, do the following:
   a) In the Servers table, select the servers that you want to add to the server pool.

      You can use the Shift key or Ctrl key to select multiple entries.
Removing Servers from a Server Pool

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Pools > Organization_Name.
Step 3 Right-click the pool from which you want to remove one or more servers and select Add Servers to Server Pool.
Step 4 In the Add Servers to Server Pool dialog box, do the following:
   a) In the Pooled Servers table, select the servers that you want to remove from the server pool.
      You can use the Shift key or Ctrl key to select multiple entries.
   b) Click the >> button to move those servers to the Pooled Servers table and add them to the server pool.
   c) Click OK.

Configuring UUID Suffix Pools

UUID Suffix Pools

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

Creating a UUID Suffix Pool

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Pools.
Step 3 Expand the node for the organization where you want to create the pool.
If the system does not include multitenancy, expand the root node.
Creating a UUID Suffix Pool

**Step 4**
Right-click **UUID Suffix Pools** and select **Create UUID Suffix Pool**.

**Step 5**
In the **Define Name and Description** page of the **Create UUID Suffix Pool** wizard, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name field</strong></td>
<td>The name of the UUID pool. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td><strong>Description field</strong></td>
<td>The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except <code>*</code> (accent mark), <code>\</code> (backslash), <code>^</code> (carat), <code>&quot;</code> (double quote), <code>=</code> (equal sign), <code>&gt;</code> (greater than), <code>&lt;</code> (less than), or <code>'</code> (single quote).</td>
</tr>
<tr>
<td><strong>Prefix field</strong></td>
<td>This can be one of the following: • <strong>Derived</strong>—The system creates the suffix. • <strong>other</strong>—You specify the desired suffix. If you select this option, Cisco UCS Manager GUI displays a text field where you can enter the desired suffix, in the format XXXXXXXX-XXXX-XXXX.</td>
</tr>
<tr>
<td><strong>Assignment Order field</strong></td>
<td>This can be one of the following: • <strong>Default</strong>—Cisco UCS Manager selects a random identity from the pool. • <strong>Sequential</strong>—Cisco UCS Manager selects the lowest available identity from the pool.</td>
</tr>
</tbody>
</table>

**Step 6**
Click **Next**.

**Step 7**
In the **Add UUID Blocks** page of the **Create UUID Suffix Pool** wizard, click **Add**.

**Step 8**
In the **Create a Block of UUID Suffixes** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From field</strong></td>
<td>The first UUID in the block.</td>
</tr>
<tr>
<td><strong>Size field</strong></td>
<td>The number of UUIDs in the block.</td>
</tr>
</tbody>
</table>

**Step 9**
Click **OK**.

**Step 10**
Click **Finish** to complete the wizard.

**What to do next**
Include the UUID suffix pool in a service profile and/or template.
Deleting a UUID Suffix Pool

If you delete a pool, Cisco UCS Manager does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

1. In the Navigation pane, click Servers.
2. Expand Servers > Pools > Organization_Name.
3. Expand the UUID Suffix Pools node.
4. Right-click the pool you want to delete and select Delete.
5. If a confirmation dialog box displays, click Yes.

Configuring IP Pools

IP Pools

IP pools are collections of IP addresses that do not have a default purpose. You can create IPv4 or IPv6 address pools in Cisco UCS Manager to do the following:

- Replace the default management IP pool ext-mgmt for servers that have an associated service profile. Cisco UCS Manager reserves each block of IP addresses in the IP pool for external access that terminates in the Cisco Integrated Management Controller (CIMC) on a server. If there is no associated service profile, you must use the ext-mgmt IP pool for the CIMC to get an IP address.
- Replace the management inband or out-of-band IP addresses for the CIMC.

Note: You cannot create iSCSI boot IPv6 pools in Cisco UCS Manager.

You can create IPv4 address pools in Cisco UCS Manager to do the following:

- Replace the default iSCSI boot IP pool iscsi-initiator-pool. Cisco UCS Manager reserves each block of IP addresses in the IP pool that you specify.
- Replace both the management IP address and iSCSI boot IP addresses.
The IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

Creating an IP Pool

Procedure

Step 1
In the Navigation pane, click LAN.

Step 2
In the LAN tab, expand LAN > Pools > Organization_Name.

Step 3
Right-click IP Pools and select Create IP Pool.

Step 4
In the Define Name and Description page of the Create IP Pool wizard, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the IP address pool.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 32 alphanumeric characters. You cannot use</td>
</tr>
<tr>
<td></td>
<td>spaces or any special characters other than - (hyphen), _ (underscore),</td>
</tr>
<tr>
<td></td>
<td>: (colon), and . (period), and you cannot change this name after the object</td>
</tr>
<tr>
<td></td>
<td>is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>The user-defined description of the IP address pool.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 256 characters. You can use any characters or spaces except</td>
</tr>
<tr>
<td></td>
<td><code>(accent mark), \\ (backslash),</code> (carat), &quot; (double quote), = (equal sign),</td>
</tr>
<tr>
<td></td>
<td>&gt; (greater than), &lt; (less than), or ‘ (single quote).</td>
</tr>
<tr>
<td>Assignment Order field</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Default—Cisco UCS Manager selects a random identity from the pool.</td>
</tr>
<tr>
<td></td>
<td>• Sequential—Cisco UCS Manager selects the lowest available identity from</td>
</tr>
<tr>
<td></td>
<td>the pool.</td>
</tr>
</tbody>
</table>

Step 5
Click Next.

Step 6
In the Add IPv4 Blocks page of the Create IP Pool wizard, click Add.

Step 7
In the Create a Block of IPv4 Addresses dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From field</td>
<td>The first IPv4 address in the block.</td>
</tr>
<tr>
<td>Size field</td>
<td>The number of IP addresses in the pool.</td>
</tr>
<tr>
<td>Subnet Mask field</td>
<td>The subnet mask associated with the IPv4 addresses in the block.</td>
</tr>
<tr>
<td>Default Gateway field</td>
<td>The default gateway associated with the IPv4 addresses in the block.</td>
</tr>
</tbody>
</table>
The primary DNS server that this block of IPv4 addresses should access.

Secondary DNS field

The secondary DNS server that this block of IPv4 addresses should access.

Step 8
Click Next.

Step 9
In the Add IPv6 Blocks page of the Create IP Pool wizard, click Add.

Step 10
In the Create a Block of IPv6 Addresses dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From field</td>
<td>The first IPv6 address in the block.</td>
</tr>
<tr>
<td>Size field</td>
<td>The number of IP addresses in the pool.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The network address prefix associated with the IPv6 addresses in the block.</td>
</tr>
<tr>
<td>Default Gateway field</td>
<td>The default gateway associated with the IPv6 addresses in the block.</td>
</tr>
<tr>
<td>Primary DNS field</td>
<td>The primary DNS server that this block of IPv6 addresses should access.</td>
</tr>
<tr>
<td>Secondary DNS field</td>
<td>The secondary DNS server that this block of IPv6 addresses should access.</td>
</tr>
</tbody>
</table>

Step 11
Click OK.

Step 12
Click Finish to complete the wizard.

Step 13
What to do next
Include the IP pool in a service profile and template.

Adding a Block to an IP Pool

You can add blocks of IPv4 or IPv6 addresses to IP pools.

Procedure

Step 1
In the Navigation pane, click LAN.

Step 2
In the LAN tab, expand LAN > Pools > Organization_Name.

Step 3
Expand the IP Pools node.

Step 4
Right-click the desired IP pool and select one of:
• Create Block of IPv4 Addresses
• Create Block of IPv6 Addresses

**Step 5** Complete the fields in the appropriate dialog box.

a) In the **Create a Block of IPv4 Addresses** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>The range of IPv4 addresses assigned to the block.</td>
</tr>
<tr>
<td>From column</td>
<td>The first IPv4 address in the block.</td>
</tr>
<tr>
<td>To column</td>
<td>The last IPv4 address in the block.</td>
</tr>
<tr>
<td>Subnet column</td>
<td>The subnet mask associated with the IPv4 addresses in the block.</td>
</tr>
<tr>
<td>Default Gateway column</td>
<td>The default gateway associated with the IPv4 addresses in the block.</td>
</tr>
<tr>
<td>Primary DNS column</td>
<td>The primary DNS server that this block of IPv4 addresses should access.</td>
</tr>
<tr>
<td>Secondary DNS column</td>
<td>The secondary DNS server that this block of IPv4 addresses should access.</td>
</tr>
</tbody>
</table>

b) In the **Create a Block of IPv6 Addresses** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>The range of IPv6 addresses assigned to the block.</td>
</tr>
<tr>
<td>From column</td>
<td>The first IPv6 address in the block.</td>
</tr>
<tr>
<td>To column</td>
<td>The last IPv6 address in the block.</td>
</tr>
<tr>
<td>Prefix column</td>
<td>The network address prefix associated with the IPv6 addresses in the block.</td>
</tr>
<tr>
<td>Default Gateway column</td>
<td>The default gateway associated with the IPv6 addresses in the block.</td>
</tr>
<tr>
<td>Primary DNS column</td>
<td>The primary DNS server that this block of IPv6 addresses should access.</td>
</tr>
<tr>
<td>Secondary DNS column</td>
<td>The secondary DNS server that this block of IPv6 addresses should access.</td>
</tr>
</tbody>
</table>

**Step 6** Click **OK**.
Deleting a Block from an IP Pool

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click LAN.</td>
</tr>
<tr>
<td>2</td>
<td>In the LAN tab, expand LAN &gt; Pools &gt; Root.</td>
</tr>
<tr>
<td>3</td>
<td>Expand the IP Pools node.</td>
</tr>
<tr>
<td>4</td>
<td>Expand the pool for which you want to delete a block of IP addresses.</td>
</tr>
<tr>
<td>5</td>
<td>Right-click the IP address block that you want to delete and select Delete.</td>
</tr>
<tr>
<td>6</td>
<td>If a confirmation dialog box displays, click Yes.</td>
</tr>
</tbody>
</table>

Deleting an IP Pool

If you delete a pool, Cisco UCS Manager does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click LAN.</td>
</tr>
<tr>
<td>2</td>
<td>In the LAN tab, expand LAN &gt; Pools &gt; Organization_Name.</td>
</tr>
<tr>
<td>3</td>
<td>Expand the IP Pools node.</td>
</tr>
<tr>
<td>4</td>
<td>Right-click the IP pool you want to delete and select Delete.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You cannot delete the default pools ext-mgmt and iscsi-initiator-pool.</td>
</tr>
<tr>
<td>5</td>
<td>If a confirmation dialog box displays, click Yes.</td>
</tr>
</tbody>
</table>
Deleting an IP Pool
CHAPTER 12

Server Boot

- Boot Policy, on page 113
- UEFI Boot Mode, on page 114
- UEFI Secure Boot, on page 115
- CIMC Secure Boot, on page 115
- Creating a Boot Policy, on page 117
- SAN Boot, on page 118
- iSCSI Boot, on page 119
- LAN Boot, on page 143
- Local Devices Boot, on page 144
- Deleting a Boot Policy, on page 150
- UEFI Boot Parameters, on page 150

Boot Policy

The Cisco UCS Manager enables you to create a boot policy for blade servers and rack servers.

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu and determines the following:

- Selection of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You can either create a named boot policy to associate with one or more service profiles, or create a boot policy for a specific service profile. A boot policy must be included in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, Cisco UCS Manager applies the default boot policy.
Changes to a boot policy might be propagated to all servers created with an updating service profile template that includes that boot policy. Re-association of the service profile with the server to rewrite the boot order information in the BIOS is automatically triggered.

You can also specify the following for the boot policy:

- Local LUN name. The name specified is the logical name in the storage profile, not the deployed name. Specify only a primary name. Specifying a secondary name results in a configuration error.

- Specific JBOD disk number for booting from JBOD disks.

- Any LUN for backward compatibility; however, we do not recommend this. Other devices must not have bootable images to ensure a successful boot.

---

**UEFI Boot Mode**

Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. Cisco UCS Manager uses UEFI to replace the BIOS firmware interfaces. This allows the BIOS to run in UEFI mode while still providing legacy support.

You can choose either legacy or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported only on M3 and higher servers, and allows you to enable UEFI secure boot mode.

UEFI PXE boot is supported with all Cisco VIC adapters on Cisco UCS rack servers integrated with Cisco UCS Manager. Beginning with Cisco UCS Manager Release 2.2(1), UEFI PXE boot is supported on all Cisco blade servers.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is not supported with the following combinations:
  - Gen-3 Emulex and QLogic adapters on Cisco UCS blade and rack servers integrated with Cisco UCS Manager.
  - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.

- If you want to use UEFI boot mode with two iSCSI LUNs, you must manually specify a common iSCSI initiator name in the service profile that is applied to both underlying iSCSI eNICs rather than allowing Cisco UCS Manager to select the name from an IQN suffix pool. If you do not supply a common name, Cisco UCS Manager will not be able to detect the second iSCSI LUN.

- You cannot mix UEFI and legacy boot mode on the same server.

- The server will boot correctly in UEFI mode only if the boot devices configured in the boot policy have UEFI-aware operating systems installed. If a compatible OS is not present, the boot device is not displayed on the Actual Boot Order tab in the Boot Order Details area.

- In some corner cases, the UEFI boot may not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation could occur in the following situations:
• If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is manually powered on using the Equipment tab or the front panel.

• If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.

• If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

You can create UEFI boot parameters in Cisco UCS Manager. UEFI Boot Parameters, on page 150 provides more information.

UEFI Secure Boot

The following limitations apply to UEFI secure boot:

• UEFI boot mode must be enabled in the boot policy.

• UEFI boot mode is available only for drives.

• The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.

\[\text{Note}\]

UEFI boot mode is supported on Cisco UCS C-Series and S-Series rack servers beginning with Release 2.2(3a).

• User-generated encryption keys are not supported.

• UEFI secure boot can only be controlled by Cisco UCS Manager.

• If you want to downgrade to an earlier version of Cisco UCS Manager, and you have a server in secure boot mode, you must disassociate, then re-associate the server before downgrading. Otherwise, server discovery is not successful.

CIMC Secure Boot

With CIMC secure boot, only Cisco signed firmware images can be installed and run on the servers. When the CIMC is updated, the image is certified before the firmware is flashed. If certification fails, the firmware is not flashed. This prevents unauthorized access to the CIMC firmware.

Guidelines and Limitations for CIMC Secure Boot

• CIMC secure boot is supported on Cisco UCS M3 rack servers.

\[\text{Note}\]

CIMC secure boot is enabled by default on the Cisco UCS C220 M4, C240 M4 rack servers, and is automatically enabled on the Cisco UCS C460 M4 rack server after upgrading to CIMC firmware release 2.2(3) or higher.
• After CIMC secure boot is enabled, you cannot disable it.

• After CIMC secure boot is enabled on a server, you cannot downgrade to a CIMC firmware image prior to 2.1(3).

**Determining the CIMC Secure Boot Status**

**Procedure**

**Step 1** In the Navigation pane, click Equipment.

**Step 2** Expand Equipment > Rack-Mounts > Servers > Server Name.

**Step 3** In the Work area, click the Inventory tab.

**Step 4** Click the CIMC subtab.

**Step 5** In the CIMC area, note the Secure Boot Operational State field.

This can be one of the following:

• **Unsupported**—CIMC secure boot is not supported on the server.

• **Disabled**—CIMC secure boot is supported, but is disabled on the server.

• **Enabling**—CIMC secure boot was enabled, and the operation is in process.

• **Enabled**—CIMC secure boot is enabled on the server.

**Enabling CIMC Secure Boot on a Rack Server**

**Procedure**

**Step 1** In the Navigation pane, click Equipment.

**Step 2** Expand Equipment > Rack-Mounts > Servers > Server Name.

**Step 3** In the Work area, click the Inventory tab.

**Step 4** Click the CIMC subtab.

**Step 5** In the Actions area, click Enable Secure Boot.

CIMC secure boot is only supported on Cisco UCS M3 rack servers. If CIMC secure boot is not supported or is already enabled, this action is greyed.

**Step 6** Click Yes in the Enable Secure Boot confirmation dialog box.

**Note** After enabled, you cannot disable CIMC secure boot.
Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Procedure

**Step 1**
In the Navigation pane, click Servers.

**Step 2**
Expand Servers > Policies.

**Step 3**
Expand the node for the organization where you want to create the policy. If the system does not include multitenancy, expand the root node.

**Step 4**
Right-click Boot Policies and select Create Boot Policy. The Create Boot Policy wizard displays.

**Step 5**
Enter a unique name and description for the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

**Step 6**
(Optional) After you make changes to the boot order, check the Reboot on Boot Order Change check box to reboot all servers that use this boot policy. For boot policies applied to a server with a non-Cisco VIC adapter, even if the Reboot on Boot Order Change check box is not checked, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.

**Step 7**
(Optional) If desired, check the Enforce vNIC/vHBA/iSCSI Name check box.

- If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table match the server configuration in the service profile.

- If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

**Step 8**
In the Boot Mode field, choose the Legacy or UEFI radio button.

**Step 9**
If you selected UEFI, check the Boot Security checkbox if you want to enable UEFI boot security.

**Step 10**
Configure one or more of the following boot options for the boot policy and set their boot order:

- Local Devices boot—To boot from local devices, such as local disks on the server, virtual media, or remote virtual disks, continue with Configuring a Local Disk Boot for a Boot Policy, on page 145.

- SAN boot—To boot from an operating system image on the SAN, continue with Configuring a SAN Boot for a Boot Policy, on page 118.

You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.
• LAN boot—To boot from a centralized provisioning server, continue with Configuring a LAN Boot for a Boot Policy, on page 143.

• iSCSI boot—To boot from an iSCSI LUN, continue with Creating an iSCSI Boot Policy, on page 128.

What to do next
Include the boot policy in a service profile and template.
After a server is associated with a service profile that includes this boot policy, you can verify the boot order in the Boot Order Details area on the General tab for the server.

SAN Boot
You can configure a boot policy to boot one or more servers from an operating system image on the SAN. The boot policy can include a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

Cisco recommends using a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the same operating system image. Therefore, the new server appears as the same server to the network.

To use a SAN boot, ensure that the following is configured:
• The Cisco UCS domain must be able to communicate with the SAN storage device that hosts the operating system image.
• A boot target LUN (Logical Unit Number) on the device where the operating system image is located.

Note
SAN boot is not supported on Gen-3 Emulex adapters on Cisco UCS blade and rack servers.

Configuring a SAN Boot for a Boot Policy
You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Tip
If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server might boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

This procedure continues directly from Creating a Boot Policy, on page 117.
Before you begin

If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, Cisco recommends that you first remove all local disks and other SAN LUNs from the boot policy in the server service profile.

This does not apply to the UCS Mini Series.

Procedure

Step 1
Click the down arrows to expand the vHBAs area.

Step 2
Click the Add SAN Boot link.

Step 3
In the Add San Boot dialog box, specify the vHBA and type, then click OK.

You can specify a Primary or a Secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary. The Any option is for unsupported adapters that connect directly to the SAN storage device and bypasses UCS Manager. Do not use the Any option with SAN boot for a supported set of adaptors which are managed by UCSM. For unsupported adaptors, use the instructions from the vendor to configure the adaptor for booting.

Step 4
If this vHBA points to a bootable SAN image, click the Add SAN Boot Target link and, in the Add SAN Boot Target dialog box, specify the boot target LUN, boot target WWPN, and type, then click OK:

Step 5
Do one of the following:

• Add another boot device to the Boot Order table.
• Click OK to finish.

What to do next

Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the Boot Order Details area on the General tab for the server.

iSCSI Boot

iSCSI boot enables a server to boot its operating system from an iSCSI target machine located remotely over a network.

iSCSI boot is supported on the following Cisco UCS hardware:

• Cisco UCS blade servers that have the Cisco UCS M51KR-B Broadcom BCM57711 network adapter and use the default MAC address provided by Broadcom.
• Cisco UCS M81KR Virtual Interface Card
• Cisco UCS VIC-1240 Virtual Interface Card
• Cisco UCS VIC-1280 Virtual Interface Card
• Cisco UCS VIC-1340 Virtual Interface Card
• Cisco UCS rack servers that have the Cisco UCS M61KR-B Broadcom BCM57712 network adapter.
• Cisco UCS P81E Virtual Interface Card
• Cisco UCS VIC 1225 Virtual Interface Card on Cisco UCS rack servers

There are prerequisites that must be met before you configure iSCSI boot. For a list of these prerequisites, see iSCSI Boot Guidelines and Prerequisites, on page 120.

For a high-level procedure for implementing iSCSI boot, see Configuring iSCSI Boot, on page 123.

iSCSI Boot Process

Cisco UCS Manager uses the iSCSI vNIC and iSCSI boot information created for the service profile in the association process to program the adapter, located on the server. After the adapter is programmed, the server reboots with the latest service profile values. After the power on self-test (POST), the adapter attempts to initialize using these service profile values. If the adapter can use the values and log in to its specified target, the adapter initializes and posts an iSCSI Boot Firmware Table (iBFT) to the host memory and a valid bootable LUN to the system BIOS. The iBFT that is posted to the host memory contains the initiator and target configuration that is programmed on the primary iSCSI vNIC.

Note

Previously, the host could see only one of the boot paths configured, depending on which path completed the LUN discovery first, and would boot from that path. Now, when there are two iSCSI boot vNICs configured, the host sees both of the boot paths. So for multipath configurations, a single IQN must be configured on both the boot vNICs. If there are different IQNs configured on the boot vNICs on a host, the host boots with the IQN that is configured on the boot vNIC with the lower PCI order.

The next step, which is the installation of the operating system (OS), requires an OS that is iBFT capable. During installation of the OS, the OS installer scans the host memory for the iBFT table and uses the information in the iBFT to discover the boot device and create an iSCSI path to the target LUN. Some OSs requires a NIC driver to complete this path. If this step is successful, the OS installer finds the iSCSI target LUN on which to install the OS.

Note

The iBFT works at the OS installation software level and might not work with HBA mode (also known as TCP offload). Whether iBFT works with HBA mode depends on the OS capabilities during installation. Also, for a server that includes a Cisco UCS M51KR-B Broadcom BCM57711 adapter, the iBFT normally works at a maximum transmission unit (MTU) size of 1500, regardless of the MTU jumbo configuration. If the OS supports HBA mode, you might need to set HBA mode, dual-fabric support, and jumbo MTU size after the iSCSI installation process.

iSCSI Boot Guidelines and Prerequisites

These guidelines and prerequisites must be met before configuring iSCSI boot:
• After the iSCSI boot policies are created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create iSCSI boot policies.

• To set up iSCSI boot from a Windows 2008 server where the second vNIC (failover vNIC) must boot from an iSCSI LUN, consult Microsoft Knowledge Base Article 976042. Microsoft has a known issue where Windows might fail to boot from an iSCSI drive or cause a bugcheck error if the networking hardware is changed. To work around this issue, follow the resolution recommended by Microsoft.

• The storage array must be licensed for iSCSI boot and the array side LUN masking must be properly configured.

• Two IP addresses must be determined, one for each iSCSI initiator. If possible, the IP addresses should be on the same subnet as the storage array. The IP addresses are assigned statically or dynamically using the Dynamic Host Configuration Protocol (DHCP).

• You cannot configure boot parameters in the Global boot policy. Instead, after configuring boot parameters, include the boot policy in the appropriate service profile.

• The operating system (OS) must be iSCSI Boot Firmware Table (iBFT) compatible.
  
  • For RHEL 7.x, the kernel parameter "rd.iscsi.ibft=1" is required before the installation. If the parameter is not entered, the iSCSI boot may fail.

• For Cisco UCS M51KR-B Broadcom BCM57711 network adapters:
  
  • Servers that use iSCSI boot must contain the Cisco UCS M51KR-B Broadcom BCM57711 network adapter. For information on installing or replacing an adapter card, see the Cisco UCS B250 Extended Memory Blade Server Installation and Service Note. The service note is accessible from the Cisco UCS B-Series Servers Documentation Roadmap at http://www.cisco.com/go/unifiedcomputing/b-series-doc.

  • Set the MAC addresses on the iSCSI device.

  • If you are using the DHCP Vendor ID (Option 43), configure the MAC address of an iSCSI device in /etc/dhcpd.conf.

  • HBA mode (also known as TCP offload) and the boot to target setting are supported. However, only Windows OS supports HBA mode during installation.

  • Before installing the OS, disable the boot to target setting in the iSCSI adapter policy, then after installing the OS, re-enable the boot to target setting.

  __________
  Note
  Each time you change an adapter policy setting, the adapter reboots to apply the new setting.

• When installing the OS on the iSCSI target, the iSCSI target must be ordered before the device where the OS image resides. For example, if you are installing the OS on the iSCSI target from a CD, the boot order should be the iSCSI target and then the CD.

• After the server is iSCSI booted, do not modify the Initiator Name, Target name, LUN, iSCSI device IP, or Netmask/gateway using the Broadcom tool.
• Do not interrupt the POST (power on self-test) process or the Cisco UCS M51KR-B Broadcom BCM57711 network adapter will fail to initialize.

• For Cisco UCS M81KR Virtual Interface Card and Cisco UCS VIC-1240 Virtual Interface Card:

  For Cisco UCS VIC-1240 Virtual Interface Card:
  • Do not set MAC addresses on the iSCSI device.

  • HBA mode and the boot to target setting are not supported.

  • When installing the OS on the iSCSI target, the iSCSI target must be ordered after the device where the OS image resides. For example, if you are installing the OS on the iSCSI target from a CD, the boot order should be the CD and then the iSCSI target.

  • If you are using the DHCP Vendor ID (Option 43), the MAC address of the overlay vNIC must be configured in /etc/dhcpd.conf.

  • After the server is iSCSI booted, do not modify the IP details of the overlay vNIC.

• The VMware ESX/ESXi operating system does not support storing a core dump file to an iSCSI boot target LUN. Dump files must be written to a local disk.

**Initiator IQN Configuration**

Cisco UCS uses the following rules to determine the initiator IQN for an adapter iSCSI vNIC at the time a service profile is associated with a physical server:

• An initiator IQN at the service profile level and at the iSCSI vNIC level cannot be used together in a service profile.

• If an initiator IQN is specified at the service profile level, all of the adaptor iSCSI vNICs are configured to use the same initiator IQN, except in the case of DHCP Option 43, where the initiator IQN is set to empty on the adapter iSCSI vNIC.

• When an initiator IQN is set at the iSCSI vNIC level, the initiator IQN at the service profile level is removed, if one is present.

• If there are two iSCSI vNIC in a service profile and only one of them has the initiator IQN set, the second one is configured with the default IQN pool. You can change this configuration later. The only exception is if DHCP Option 43 is configured. In this case, the initiator IQN on the second iSCSI vNIC is removed during service profile association.

---

**Note**

If you change an iSCSI vNIC to use the DHCP Option 43 by setting the vendor ID, it does not remove the initiator IQN configured at the service profile level. The initiator IQN at the service profile level can still be used by another iSCSI vNIC which does not use the DHCP Option 43.

---

**Enabling MPIO on Windows**

You can enable (MPIO) to optimize connectivity with storage arrays.
If you change the networking hardware, Windows might fail to boot from an iSCSI drive. For more information, see Microsoft support Article ID: 976042.

Before you begin

The server on which you enable the Microsoft Multipath I/O (MPIO) must have a Cisco VIC driver.

If there are multiple paths configured to the boot LUN, only one path should be enabled when the LUN is installed.

Procedure

**Step 1**
In the service profile associated with the server, configure the primary iSCSI vNIC. For more information, see Creating an iSCSI vNIC for a Service Profile, on page 129.

**Step 2**
Using the primary iSCSI vNIC, install the Windows operating system on the iSCSI target LUN.

**Step 3**
After Windows installation completes, enable MPIO on the host.

**Step 4**
In the service profile associated with the server, add the secondary iSCSI vNIC to the boot policy. For more information, see Creating an iSCSI Boot Policy, on page 128.

---

**Configuring iSCSI Boot**

When you configure an adapter or blade in Cisco UCS to iSCSI boot from a LUN target, complete all of the following steps.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>(Optional) Configure the iSCSI boot adapter policy.</td>
<td>For more information, see Creating an iSCSI Boot Policy, on page 128</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) Configure the authentication profiles for the initiator and target.</td>
<td>For more information, see Creating an iSCSI Authentication Profile, on page 126</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) To configure the iSCSI initiator to use an IP address from a pool of IP addresses, add a block of IP addresses to the iSCSI initiator pool.</td>
<td>For more information, see Creating an iSCSI Initiator IP Pool, on page 127</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Create a boot policy that can be used in any service profile. Alternatively, you can create a local boot policy only for the specific service policy. However, Cisco recommends that you</td>
<td>For more information about creating a boot policy that can be used in any service profile, see Creating an iSCSI Boot Policy, on page 128</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>create a boot policy that can be shared with multiple service profiles.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 5

If you created a boot policy that can be used in any service profile, assign it to the service profile. Otherwise, proceed to the next step.

You can assign the boot policy to the service profile while configuring the iSCSI boot and vNIC parameters in the service profile in step 7.

#### Step 6

Create an iSCSI vNIC in a service profile.

For more information, see [Creating an iSCSI vNIC for a Service Profile](#)

#### Step 7

Configure the iSCSI boot parameters, including the iSCSI qualifier name (IQN), initiator, target interfaces, and iSCSI vNIC parameters in a service profile in expert mode or service profile template.

For more information, see [Creating a Service Profile with the Expert Wizard](#) or [Creating a Service Profile Template](#), respectively.

#### Step 8

Verify the iSCSI boot operation.

For more information, see [Verifying iSCSI Boot](#).

#### Step 9

For RHEL 7.x, the kernel parameter "rd.iscsi.ibft=1" is required before installing the OS. If the parameter is not entered, the iSCSI boot may fail.

#### Step 10

Install the OS on the server.

For more information, see one of the following guides:
- *Cisco UCS B-Series Blade Servers VMware Installation Guide*
- *Cisco UCS B-Series Blade Servers Linux Installation Guide*
- *Cisco UCS B-Series Blade Servers Windows Installation Guide*

#### Step 11

Boot the server.

---

### Creating an iSCSI Adapter Policy

#### Procedure

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers > Policies**.
3. Expand the node for the organization where you want to create the policy.
   - If the system does not include multitenancy, expand the **root** node.
4. Right-click **Adapter Policies** and choose **Create iSCSI Adapter Policy**.
**Step 5** In the **Create iSCSI Adapter Policy** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> field</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than -(hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td><strong>Connection Timeout</strong> field</td>
<td>The number of seconds to wait until Cisco UCS assumes that the initial login has failed and the iSCSI adapter is unavailable.</td>
</tr>
<tr>
<td></td>
<td>Enter an integer between 0 and 255. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds).</td>
</tr>
<tr>
<td><strong>LUN Busy Retry Count</strong> field</td>
<td>The number of times to retry the connection in case of a failure during iSCSI LUN discovery.</td>
</tr>
<tr>
<td></td>
<td>Enter an integer between 0 and 60. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds).</td>
</tr>
<tr>
<td><strong>DHCP Timeout</strong> field</td>
<td>The number of seconds to wait before the initiator assumes that the DHCP server is unavailable.</td>
</tr>
<tr>
<td></td>
<td>Enter an integer between 60 and 300 (default: 60 seconds).</td>
</tr>
<tr>
<td><strong>Enable TCP Timestamp</strong> check box</td>
<td>Check this box if you want to use a TCP Timestamp. With this setting, transmitted packets are given a time stamp of when the packet was sent so that the packet's round-trip time can be calculated, when needed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This option only applies to servers with the Cisco UCS NIC M51KR-B adapter.</td>
</tr>
<tr>
<td><strong>HBA Mode</strong> check box</td>
<td>Check this box to enable HBA mode (also known as TCP offload).</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> This option should only be enabled for servers with the Cisco UCS NIC M51KR-B adapter running the Windows operating system.</td>
</tr>
<tr>
<td><strong>Boot to Target</strong> check box</td>
<td>Check this box to boot from the iSCSI target.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This option only applies to servers with the Cisco UCS NIC M51KR-B adapter. It should be disabled until you have installed an operating system on the server.</td>
</tr>
</tbody>
</table>
Deleting an iSCSI Adapter Policy

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand the node for the organization where you want to create the policy.
        If the system does not include multitenancy, expand the root node.
Step 4  Expand the Adapter Policies node.
Step 5  Right-click the adapter policy and choose Delete.
Step 6  If a confirmation dialog box displays, click Yes.

Creating an iSCSI Authentication Profile

For iSCSI boot, you need to create both an initiator and a target iSCSI authentication profile.

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the root node.

**Step 4**
Right-click iSCSI Authentication Profiles and choose Create iSCSI Authentication Profile.

**Step 5**
In the Create Authentication Profile dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> field</td>
<td>The name of the authentication profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td><strong>User Id</strong> field</td>
<td>The user Id associated with this profile. Enter between 1 and 128 characters, spaces, or special characters.</td>
</tr>
<tr>
<td><strong>Password</strong> field</td>
<td>The password associated with this profile. Enter between 12 and 16 characters, including special characters.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong> field</td>
<td>The password again for confirmation purposes.</td>
</tr>
</tbody>
</table>

**Step 6**
Click OK.

---

**What to do next**
Include the authentication profile in a service profile and template.

---

**Deleting an iSCSI Authentication Profile**

**Procedure**

**Step 1**
In the Navigation pane, click Servers.

**Step 2**
Expand Servers > Policies.

**Step 3**
Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the root node.

**Step 4**
Expand the iSCSI Authentication Profiles node.

**Step 5**
Right-click the IP pool you want to delete and choose Delete.

**Step 6**
If a confirmation dialog box displays, click Yes.

---

**Creating an iSCSI Initiator IP Pool**

You can create a group of IP addresses to be used for iSCSI boot. Cisco UCS Manager reserves the block of IPv4 addresses you specify.
The IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

**Procedure**

**Step 1** In the **Navigation** pane, click **LAN**.

**Step 2** Expand **LAN > Pools**.

**Step 3** Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

**Step 4** Expand the **IP Pools** node.

**Step 5** Right-click **IP Pool iscsi-initiator-pool** and choose **Create Block of IPv4 Addresses**.

**Step 6** In the **Create a Block of IPv4 Addresses** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>The range of IPv4 addresses assigned to the block.</td>
</tr>
<tr>
<td>From column</td>
<td>The first IPv4 address in the block.</td>
</tr>
<tr>
<td>To column</td>
<td>The last IPv4 address in the block.</td>
</tr>
<tr>
<td>Subnet column</td>
<td>The subnet mask associated with the IPv4 addresses in the block.</td>
</tr>
<tr>
<td>Default Gateway column</td>
<td>The default gateway associated with the IPv4 addresses in the block.</td>
</tr>
<tr>
<td>Primary DNS column</td>
<td>The primary DNS server that this block of IPv4 addresses should access.</td>
</tr>
<tr>
<td>Secondary DNS column</td>
<td>The secondary DNS server that this block of IPv4 addresses should access.</td>
</tr>
</tbody>
</table>

**Step 7** Click **OK**.

**What to do next**

Configure one or more service profiles or service profile templates to obtain the iSCSI initiator IP address from the iSCSI initiator IP pool.

**Creating an iSCSI Boot Policy**

You can add up to two iSCSI vNICs per boot policy. One vNIC acts as the primary iSCSI boot source, and the other acts as the secondary iSCSI boot source.

**Procedure**

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Servers > Policies**.
Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the root node.

Step 4 Right-click **Boot Policies** and choose **Create Boot Policy**.
The **Create Boot Policy** wizard displays.

Step 5 Enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 (Optional) To reboot a server that uses this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

**Note** This applies only to servers using the standard boot order.

Step 7 (Optional) If desired, check the **Enforce vNIC/vHBA/iSCSI Name** check box.
- If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the **Boot Order** table match the server configuration in the service profile.
- If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

Step 8 To add a iSCSI boot to the boot policy, do the following:
a) Click the down arrows to expand the iSCSI vNICs area.
b) Click the **Add iSCSI Boot** link.
c) In the **Add iSCSI Boot** dialog box, enter a name for the iSCSI vNIC, and click **OK**.
d) Repeat steps b and c to create another iSCSI vNIC.

---

**What to do next**
Include the boot policy in a service profile and template.
After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the **Boot Order Details** area on the **General** tab for the server.

### Creating an iSCSI vNIC for a Service Profile

**Procedure**

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Servers > Service Profiles**.

---

**Creating an iSCSI vNIC for a Service Profile**
**Step 3**

Expand the node for the organization that contains the service profile for which you want to create an iSCSI vNIC.

**Step 4**

Expand the service profile for which you want to create a iSCSI vNIC.

**Step 5**

Right-click the iSCSI vNICs node and choose **Create vNICs**.

**Step 6**

In the **Create iSCSI vNIC** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> field</td>
<td>The name of the iSCSI vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td><strong>Overlay vNIC</strong> drop-down list</td>
<td>The LAN vNIC associated with this iSCSI vNIC, if any.</td>
</tr>
<tr>
<td><strong>iSCSI Adapter Policy</strong> drop-down list</td>
<td>The iSCSI adapter policy associated with this iSCSI vNIC, if any.</td>
</tr>
<tr>
<td><strong>Create iSCSI Adapter Policy</strong> link</td>
<td>Click this link to create a new iSCSI adapter policy that will be available to all iSCSI vNICs.</td>
</tr>
<tr>
<td><strong>MAC Address</strong> field</td>
<td>The MAC address associated with this iSCSI vNIC, if any. If the MAC address is not set, the Cisco UCS Manager GUI displays <strong>Derived</strong>.</td>
</tr>
<tr>
<td><strong>MAC Pool</strong> field</td>
<td>The MAC pool associated with this iSCSI vNIC, if any.</td>
</tr>
<tr>
<td><strong>VLAN</strong> drop-down list</td>
<td>The virtual LAN associated with this iSCSI vNIC. The default VLAN is <strong>default</strong>. <strong>Note</strong> For the Cisco UCS M81KR Virtual Interface Card and the Cisco UCS VIC-1240 Virtual Interface Card, the VLAN that you specify must be the same as the native VLAN on the overlay vNIC. For the Cisco UCS M51KR-B Broadcom BCM57711 Adapter, the VLAN that you specify can be any VLAN assigned to the overlay vNIC.</td>
</tr>
</tbody>
</table>

**Step 7**

In the **MAC Address Assignment** drop-down list in the **iSCSI MAC Address** area, choose one of the following:

- Leave the MAC address unassigned, select **Select (None used by default)**. Select this option if the server that will be associated with this service profile contains a Cisco UCS M81KR Virtual Interface Card adapter or a Cisco UCS VIC-1240 Virtual Interface Card.

  **Important** If the server that will be associated with this service profile contains a Cisco UCS NIC M51KR-B adapter, you must specify a MAC address.

- A specific MAC address, select **00:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link.
A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

If this Cisco UCS domain is registered with Cisco UCS Central, there might be two pool categories. **Domain Pools** are defined locally in the Cisco UCS domain and **Global Pools** are defined in Cisco UCS Central.

**Step 8**
(Optional) If you want to create a MAC pool that will be available to all service profiles, click **Create MAC Pool** and complete the fields in the **Create MAC Pool** wizard.

For more information, see the Creating a MAC Pool section in Cisco UCS Manager Network Management Guide, Release 3.1.

**Step 9**
Click **OK**.

**Step 10**
(Optional) If you want to set or change the initiator name, from the iSCSI vNICs tab, click **Reset Initiator Name** or **Change Initiator Name** and complete the fields in the **Change Initiator Name** dialog box or click . For more information, see Setting the Initiator IQN at the Service Profile Level, on page 131.

---

### Deleting an iSCSI vNIC from a Service Profile

**Procedure**

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers** > **Service Profiles**.
3. Expand the node for the organization that contains the service profile from which you want to delete an iSCSI vNIC.
4. Expand the service profile from which you want to delete an iSCSI vNIC.
5. Expand the iSCSI vNICs node.
6. Right-click the iSCSI vNIC you want to delete and choose **Delete**.
7. If a confirmation dialog box displays, click **Yes**.

---

### Setting the Initiator IQN at the Service Profile Level

**Procedure**

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers** > **Service Profiles**.
3. Expand the desired node for the organization.
4. Click the service profile with the iSCSI vNIC that you want to change.
5. In the **Work** pane, click the **iSCSI vNICs** tab.
Changing the Initiator IQN at the Service Profile Level

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Service Profiles.
Step 3 Expand the desired node for the organization.
Step 4 Click the service profile with the iSCSI vNIC that you want to change.
Step 5 In the Work pane, click the iSCSI vNICs tab.
Step 6 In the Actions area, click Change Initiator Name.
Step 7 In the Change Initiator Name dialog box, change the values in the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator Name Assignment drop-down list</td>
<td>Choose the IQN initiator name that you want to use from the drop-down list.</td>
</tr>
<tr>
<td>Initiator Name field</td>
<td>If you selected a manual initiator name assignment, enter the initiator name.</td>
</tr>
<tr>
<td>Create IQN Suffix Pool link</td>
<td>Click to create a new IQN suffix pool.</td>
</tr>
</tbody>
</table>

Step 8 Click OK.

Setting iSCSI Boot Parameters

You can set iSCSI boot parameters, including the boot order, boot policy, iSCSI authentication profile, initiator interface, and target interface for an iSCSI vNIC.

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Service Profiles.
Step 3 Expand the node for the organization that contains the service profile for which you want to create iSCSI boot parameters. If the system does not include multi-tenancy, expand the root node.
Step 4 Click the service profile for which you want to create iSCSI boot parameters.
Step 5 Click the Boot Order tab.
Step 6 In the Specific Boot Policy area, click the down arrows to expand the iSCSI vNICs area.
**Step 7**
In the iSCSI vNICs area, double-click the iSCSI vNICs from which you want to boot the server to add them to the Boot Order table.

**Step 8**
In the iSCSI vNICs area, click the Set Boot Parameters link.

If there are two iSCSI vNICs, choose the one for which you want to set boot parameters.

**Step 9**
In the Set iSCSI Boot Parameters dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the iSCSI vNIC for which you are setting the boot parameters.</td>
</tr>
<tr>
<td>Authentication Profile drop-down list</td>
<td>The name of the associated iSCSI authentication profile.</td>
</tr>
<tr>
<td>Create Authentication Profile link</td>
<td>Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs.</td>
</tr>
</tbody>
</table>

**Step 10**
In the Initiator Name area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator Name Assignment drop-down list</td>
<td>Select how the iSCSI boot initiator name is assigned. Choose one of the following methods:</td>
</tr>
<tr>
<td></td>
<td>• Manual—You will enter a name in the Initiator Name field. The initiator name can contain up to 223 characters.</td>
</tr>
<tr>
<td></td>
<td>• Pools—Choose an IQN suffix pool from which the name will be assigned.</td>
</tr>
<tr>
<td>Note</td>
<td>Setting the Initiator Name from the Set iSCSI Boot Parameters dialog box sets the initiator IQN at the iSCSI vNIC level and not at the service profile level. If more than one path is configured, you must set the initiator IQN from the iSCSI vNICs tab or when creating a service profile.</td>
</tr>
<tr>
<td></td>
<td>If you need to, you can change or reset the initiator name. For more information, see Changing the Initiator IQN at the Service Profile Level, on page 132.</td>
</tr>
<tr>
<td>Create IQN Suffix Pool link</td>
<td>Click this link to create a new IQN suffix pool that will be available to all iSCSI vNICs.</td>
</tr>
<tr>
<td>Initiator Name field</td>
<td>A regular expression that defines the name of the iSCSI initiator. You can enter any alphanumeric string as well as the following special characters:</td>
</tr>
<tr>
<td></td>
<td>• . (period)</td>
</tr>
<tr>
<td></td>
<td>• : (colon)</td>
</tr>
<tr>
<td></td>
<td>• - (dash)</td>
</tr>
</tbody>
</table>
Step 11  From the **Initiator IP Address Policy** drop-down list, choose of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (DHCP used by default)</td>
<td>The system selects an interface automatically using DHCP. Proceed to Step 13.</td>
</tr>
<tr>
<td>Static</td>
<td>A static IPv4 address is assigned to the iSCSI boot vNIC based on the information entered in this area. Proceed to Step 12.</td>
</tr>
<tr>
<td>Pool</td>
<td>An IPv4 address is assigned to the iSCSI boot vNIC from the management IP address pool. Proceed to Step 13.</td>
</tr>
</tbody>
</table>

Step 12  If you chose **Static** from the **Initiator IP Address Policy** drop-down list, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address field</td>
<td>The IPv4 address assigned to the iSCSI boot vNIC. If you want to specify this address, you must select <strong>Static</strong> in the <strong>Initiator IP Address Policy</strong> drop-down list.</td>
</tr>
<tr>
<td>Subnet Mask field</td>
<td>The subnet mask associated with the IPv4 address.</td>
</tr>
<tr>
<td>Default Gateway field</td>
<td>The default gateway associated with the IPv4 address.</td>
</tr>
<tr>
<td>Primary DNS field</td>
<td>The primary DNS server address.</td>
</tr>
<tr>
<td>Secondary DNS field</td>
<td>The secondary DNS server address.</td>
</tr>
</tbody>
</table>

Step 13  For the iSCSI target interface, choose one of the following radio buttons:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI Static Target Interface</td>
<td>The system creates a static target interface that you need to configure. Proceed to Step 14.</td>
</tr>
<tr>
<td>iSCSI Auto Target Interface</td>
<td>The system creates an auto target interface. You need to specify whether the auto target uses an initiator or a DHCP vendor ID. Proceed to Step 16.</td>
</tr>
</tbody>
</table>

Step 14  If you chose **iSCSI Static Target Interface**, in the **Static Target Interface** table, click **Add**.

Step 15  In the **Create iSCSI Static Target** dialog box, complete the following fields:
A regular expression that defines the iSCSI Qualified Name (IQN) or Extended Unique Identifier (EUI) name of the iSCSI target.

You can enter any alphanumeric characters as well as the following special characters:

- . (period)
- : (colon)
- - (dash)

Important This name must be properly formatted using standard IQN or EUI guidelines.

The following examples show properly formatted iSCSI target names:

- iqn.2001-04.com.example
- iqn.2001-04.com.example:storage.tape1.sys1.xyz
- iqn.2001-04.com.example:storage.disk2.sys1.xyz
- eui.02004567A425678D

Priority field The system-assigned priority for the iSCSI target.

Port field The port associated with the iSCSI target.
Enter an integer between 1 and 65535. The default is 3260.

Authentication Profile drop-down list The name of the associated iSCSI authentication profile.

Create iSCSI Authentication Profile link Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs.

IPv4 Address field The IPv4 address assigned to the iSCSI target.

LUN Id field The LUN identifier in the iSCSI target.

Step 16 If you chose iSCSI Auto Target Interface, enter either the initiator name or the DHCP vendor ID in the DHCP Vendor Id field. The initiator must have already been configured. The vendor ID can be up to 32 alphanumeric characters.

Step 17 Click OK.

Modifying iSCSI Boot Parameters

You can modify iSCSI boot parameters, including the boot order, boot policy, iSCSI authentication profile, initiator interface, and target interface for an iSCSI vNIC.
**Procedure**

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Servers > Service Profiles**.

**Step 3** Expand the node for the organization that contains the service profile for which you want to modify iSCSI boot parameters. If the system does not include multi-tenancy, expand the root node.

**Step 4** Click the service profile for which you want to modify iSCSI boot parameters.

**Step 5** Click the **Boot Order** tab.

**Step 6** In the **Specific Boot Policy** area, click the down arrows to expand the **iSCSI vNICs** area.

**Step 7** To add or delete an iSCSI vNIC from the boot order or to change the boot order, do one of the following:

- To add an iSCSI vNIC, in the **iSCSI vNICs** area, double-click an iSCSI vNIC to add it to the **Boot Order** table.
- To delete an iSCSI vNIC from the boot order, in the **Boot Order** table, select the iSCSI vNIC and click **Delete**.
- To change the iSCSI vNIC boot order, in the **Boot Order** table, select the iSCSI vNIC and click either **Move Up** or **Move Down**.

**Step 8** To change the boot parameters, in the **iSCSI vNICs** area, click the **Set Boot Parameters** link.

If there are two iSCSI vNICs, choose the one for which you want to change boot parameters.

**Step 9** In the **Set iSCSI Boot Parameters** dialog box, change the values in any of the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> field</td>
<td>The name of the iSCSI vNIC for which you are setting the boot parameters.</td>
</tr>
<tr>
<td><strong>Authentication Profile</strong> drop-down list</td>
<td>The name of the associated iSCSI authentication profile.</td>
</tr>
<tr>
<td><strong>Create Authentication Profile</strong> link</td>
<td>Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs.</td>
</tr>
</tbody>
</table>

**Step 10** In the **Initiator Name** area, complete the following fields:
**Initiator Name Assignment** drop-down list

Select how the iSCSI boot initiator name is assigned. Choose one of the following methods:

- **Manual**—You will enter a name in the **Initiator Name** field. The initiator name can contain up to 223 characters.
- **Pools**—Choose an IQN suffix pool from which the name will be assigned.

**Note**

Setting the Initiator Name from the Set iSCSI Boot Parameters dialog box sets the initiator IQN at the iSCSI vNIC level and not at the service profile level. If more than one path is configured, you must set the initiator IQN from the iSCSI vNICs tab or when creating a service profile.

If you need to, you can change or reset the initiator name. For more information, see Changing the Initiator IQN at the Service Profile Level, on page 132.

**Create IQN Suffix Pool** link

Click this link to create a new IQN suffix pool that will be available to all iSCSI vNICs.

**Initiator Name** field

A regular expression that defines the name of the iSCSI initiator.

You can enter any alphanumeric string as well as the following special characters:

- . (period)
- : (colon)
- - (dash)

**Step 11**

From the **Initiator IP Address Policy** drop-down list, change the selection to one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (DHCP used by default)</td>
<td>The system selects an interface automatically using DHCP. Proceed to Step 13.</td>
</tr>
<tr>
<td>Static</td>
<td>A static IPv4 address is assigned to the iSCSI boot vNIC based on the information entered in this area. Proceed to Step 12.</td>
</tr>
<tr>
<td>Pool</td>
<td>An IPv4 address is assigned to the iSCSI boot vNIC from the management IP address pool. Proceed to Step 13.</td>
</tr>
</tbody>
</table>

**Step 12**

If you chose **Static** from the **Initiator IP Address Policy** drop-down list, complete or change the following fields:
### Step 13
For the iSCSI target interface, choose one of the following radio buttons:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI Static Target Interface</td>
<td>The system creates a static target interface that you need to configure. Proceed to Step 14.</td>
</tr>
<tr>
<td>iSCSI Auto Target Interface</td>
<td>The system creates an auto target interface. You need to specify whether the auto target uses an initiator or a DCHP vendor ID. Proceed to Step 15.</td>
</tr>
</tbody>
</table>

### Step 14
If you chose **iSCSI Static Target Interface**, do one of the following in the **Static Target Interface** table:

- To add an iSCSI static target interface, click **Add** or to modify an iSCSI target interface, select the iSCSI target interface that you want to change and click **Modify**. Then and complete or change the following fields in the **Create iSCSI Static Target** dialog box:
### Name | Description
--- | ---
**iSCSI Target Name** field | A regular expression that defines the iSCSI Qualified Name (IQN) or Extended Unique Identifier (EUI) name of the iSCSI target. You can enter any alphanumeric characters as well as the following special characters:
- . (period)
- : (colon)
- - (dash)

**Important** This name must be properly formatted using standard IQN or EUI guidelines.

The following examples show properly formatted iSCSI target names:
- iqn.2001-04.com.example
- iqn.2001-04.com.example:storage.tape1.sys1.xyz
- iqn.2001-04.com.example:storage.disk2.sys1.xyz
- eui.02004567A425678D

**Priority** field | The system-assigned priority for the iSCSI target.

**Port** field | The port associated with the iSCSI target.

Enter an integer between 1 and 65535. The default is 3260.

**Authentication Profile** drop-down list | The name of the associated iSCSI authentication profile.

**Create iSCSI Authentication Profile** link | Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs.

**IPv4 Address** field | The IPv4 address assigned to the iSCSI target.

**LUN Id** field | The LUN identifier in the iSCSI target.

- **Step 15** If you chose **iSCSI Auto Target Interface**, change the entry to either the initiator name or the DHCP vendor ID in the **DHCP Vendor Id** field. The initiator must have already been configured. The vendor ID can be up to 32 alphanumeric characters.

To delete an iSCSI target interface, select the iSCSI target interface that you want to delete and click **Delete**.

**Note** If you have two iSCSI static targets and you delete the first priority target, the second priority target becomes the first priority target, although Cisco UCS Manager still shows it as the second priority target.
IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain.

IQN pool members are of the form prefix:suffix:number, where you can specify the prefix, suffix, and a block (range) of numbers.

An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but sharing the same prefix.

Creating an IQN Pool

In most cases, the maximum IQN size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

Procedure

Step 1
In the Navigation pane, click SAN.

Step 2
Expand SAN > Pools.

Step 3
Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the root node.

Step 4
Right-click IQN Pools and select Create IQN Suffix Pool.

Step 5
In the Define Name and Description page of the Create IQN Suffix Pool wizard, fill in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the iSCSI Qualified Name (IQN) pool. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description</td>
<td>The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
</tbody>
</table>
### Field

**Prefix**

The prefix for any IQN blocks created for this pool. Enter from 1 to 150 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use `iqn1.alpha.com`.

### Assignment Order field

This can be one of the following:

- **Default**—Cisco UCS Manager selects a random identity from the pool.
- **Sequential**—Cisco UCS Manager selects the lowest available identity from the pool.

---

**Step 6**  
Click Next.

**Step 7**

In the Add IQN Blocks page of the Create IQN Suffix Pool wizard, click Add.

**Step 8**

In the Create a Block of IQN Suffixes dialog box, fill in the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Suffix field | The suffix for this block of iSCSI Qualified Names (IQNs). Enter from 1 to 64 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use `alphadc-1`.
| From field | The first suffix number in the block.
| Size field | The number of suffixes in the block.

**Step 9**

Click OK.

**Step 10**

Click Finish to complete the wizard.

---

### What to do next

Include the IQN suffix pool in a service profile and template.

### Adding a Block to an IQN Pool

#### Procedure

**Step 1**

In the Navigation pane, click SAN.

**Step 2**

Expand SAN > Pools.

**Step 3**

Expand the node for the organization containing the pool.

If the system does not include multitenancy, expand the root node.
Deleting a Block from an IQN Pool

If you delete an address block from a pool, Cisco UCS Manager does not reallocate any addresses in that block that were assigned to vNICs or vHBAs. All assigned addresses from a deleted block remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

**Step 1** In the Navigation pane, click SAN.

**Step 2** Expand SAN > Pools.

**Step 3** Expand the node for the organization containing the pool.

If the system does not include multitenancy, expand the root node.

**Step 4** Expand the IQN Pools node.

**Step 5** Choose the IQN pool for which you want to delete a block of IQN suffixes.

**Step 6** In the Work pane, click the IQN Blocks tab.

**Step 7** Right-click the block to be deleted and select Delete.

**Step 8** Click Yes to confirm the deletion.

**Step 9** Click Save Changes.
Deleting an IQN Pool

If you delete a pool, Cisco UCS Manager does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

Step 1: In the Navigation pane, click SAN.
Step 2: Expand SAN > Pools.
Step 3: Expand the node for the organization containing the pool.
Step 4: If the system does not include multitenancy, expand the root node.
Step 5: Expand the IQN Pools node.
Step 6: Right-click the pool that you want to delete and select Delete.
Step 7: If a confirmation dialog box displays, click Yes.

LAN Boot

You can configure a boot policy to boot one or more servers from a centralized provisioning server on the LAN. A LAN (or PXE) boot is frequently used to install operating systems on a server from that LAN server.

You can add more than one type of boot device to a LAN boot policy. For example, you could add a local disk or virtual media boot as a secondary boot device.

Configuring a LAN Boot for a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

You can add more than one type of boot device to a boot policy. For example, you can add a local disk or virtual media boot as a secondary boot device.

This procedure continues directly from Creating a Boot Policy, on page 117.

Procedure

Step 1: Click the down arrows to expand the vNICs area.
Step 2: Click the Add LAN Boot link.
Step 3  In the Add LAN Boot dialog box, enter the name of the vNIC that you want to use for the LAN boot in the vNIC field, then click OK.

Step 4  Do one of the following:
   • Add another boot device to the Boot Order table.
   • Click OK to finish.

What to do next
Include the boot policy in the service profile template.
After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the Boot Order Details area on the General tab for the server.

Local Devices Boot
Cisco UCS Manager allows you to boot from different local devices.

Note  For Cisco UCS M3 and higher blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can only select a top-level device.

Local Disk Boot
If a server has a local drive, you can configure a boot policy to boot the server from the top-level local disk device or from any of the following second-level devices:
   • Local LUN—Enables boot from local disk or local LUN.
   • Local JBOD—Enables boot from a bootable JBOD.
   • SD card—Enables boot from SD card.
   • Internal USB—Enables boot for internal USB.
   • External USB—Enables boot from external USB.
   • Embedded Local LUN—Enables boot from the embedded local LUN on the Cisco UCS 240 M4 server.
   • Embedded Local Disk—Enables boot from the embedded local disk on the Cisco UCS C240 M4SX and the M4L servers.

Note  Second-level devices are only available for Cisco UCS M3 and higher blade and rack servers using enhanced boot order. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can choose only the top-level Add Local Disk.
Virtual Media Boot

You can configure a boot policy to boot one or more servers from a virtual media device that is accessible from the server. A virtual media device mimics the insertion of a physical CD/DVD disk (read-only) or floppy disk (read-write) into a server. This type of server boot is typically used to manually install operating systems on a server.

Note

Second-level devices are only available for Cisco UCS M3 and higher blade and rack servers using enhanced boot order. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can choose only the top-level Add CD/DVD or Add Floppy.

Remote Virtual Drive Boot

You can configure a boot policy to boot one or more servers from a remote virtual drive that is accessible from the server.

Configuring a Local Disk Boot for a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

You can add more than one type of boot device to a boot policy. For example, you could add an SD card boot as a secondary boot device.

This procedure continues directly from Creating a Boot Policy, on page 117.

Procedure

Step 1
Click the down arrows to expand the Local Devices area.

Step 2
Click any of the following links to add the device to the Boot Order table:

- Add Local Disk or
  - Add Local LUN
  - Add SD Card
  - Add Internal USB
  - Add External USB

Note
For Cisco UCS M3 and higher blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can only select a top-level device.

Step 3
Do one of the following:

- Add another boot device to the Boot Order table.
- Click OK to finish.
What to do next

Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the Boot Order Details area on the General tab for the server.

Configuring a Virtual Media Boot for a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

You can add more than one type of boot device to a boot policy. For example, you could add a local disk boot as a second boot device.

Note

Virtual Media requires the USB to be enabled. If you modify the BIOS settings that affect the USB functionality, you also affect the Virtual Media. Therefore, Cisco recommends that you leave the following USB BIOS defaults for best performance:

- Make Device Non Bootable—set to disabled
- USB Idle Power Optimizing Setting—set to high-performance

This procedure continues directly from Creating a Boot Policy, on page 117.

Procedure

Step 1
Click the down arrows to expand the Local Devices area.

Step 2
Click any of the following links to add the device to the Boot Order table:

- Add CD/DVD or
  - Add Local CD/DVD
  - Add Remote CD/DVD (For KVM CD/DVD in rack servers)
    In a setup with M5 blade servers, if an ISO is mapped to the KVM console, use only Add Remote CD/DVD in Boot Order.

- Add Floppy or
  - Add Local Floppy
  - Add Remote Floppy

- Add Remote Virtual Drive

Note
For Cisco UCS M3 and higher blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can only select a top-level device.
Step 3 Do one of the following:
  - Add another boot device to the Boot Order table.
  - Click OK to finish.

What to do next
Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the Boot Order Details area on the General tab for the server.

Configuring a NVMe Boot for a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

You can add more than one type of boot device to a boot policy. For example, you could add an SD card boot as a secondary boot device.

This procedure continues directly from Creating a Boot Policy, on page 117.

Procedure

Step 1 Click the down arrows to expand the Local Devices area.
Step 2 Click Add NVMe to add the device to the Boot Order table.
Note NVMe boot policy is available only with Uefi boot mode.
Step 3 Do one of the following:
  - Add another boot device to the Boot Order table.
  - Click OK to finish.

What to do next
Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the Boot Order Details area on the General tab for the server.

Adding a Boot Policy to a vMedia Service Profile

This procedure describes how to set the boot policy options for vMedia on the Server Boot Order page of the Create Service Profile (expert) wizard.
# Procedure

**Step 1**  
In the **Navigation** pane, click **Servers**.

**Step 2**  
Expand **Servers > Service Profiles**.

**Step 3**  
Expand the node for the organization where you want to create the service profile.  
If the system does not include multitenancy, expand the **root** node.

**Step 4**  
Right-click the organization and select **Create Service Profile (expert)**.  
The **Unified Computing System Manager** pane displays.

**Step 5**  
In the **Name** field, enter a unique name that you can use to identify the service profile.  
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.  
This name must be unique within the organization or sub-organization in which you are creating the service profile.

**Step 6**  
From the **UUID Assignment** drop-down list, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select (pool default used by default)   | Assigns a UUID from the default UUID Suffix pool.  
                                         | Continue with Step 8.                                                      |
| Hardware Default                        | Uses the UUID assigned to the server by the manufacturer.  
                                         | If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.  
                                         | Continue with Step 8.                                                      |
| XXXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX | Uses the UUID that you manually assign.  
                                         | Continue with Step 7.                                                     |
| Pools Pool_Name                         | Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list.  
                                         | Each pool name is followed by two numbers in parentheses that show the number of UUIDs available in the pool and the total number of UUIDs in the pool.  
                                         | If you do not want use any of the existing pools, but want to create a pool that all service
### Adding a Boot Policy to a vMedia Service Profile

<table>
<thead>
<tr>
<th>Step 7</th>
<th>(Optional) If you selected the <code>XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</code> option, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a) In the <strong>UUID</strong> field, enter the valid UUID that you want to assign to the server that uses this service profile.</td>
</tr>
</tbody>
</table>

| Step 8 | (Optional) If you want to create a new UUID Suffix pool to use in this service profile, click **Create UUID Suffix Pool** and complete the fields in the **Create UUID Suffix Pool** wizard. For more information, see Creating a UUID Suffix Pool, on page 105. |

| Step 9 | (Optional) In the text box, enter a description of this service profile. The user-defined description for this service profile. Enter up to 256 characters. You can use any characters or spaces except `'(accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or `'(single quote). |

| Step 10 | Click **Next**. |

| Step 11 | Navigate to **Create Service Profile (expert)** and click **Server Boot Order**. The **Boot Policy** pane displays. |

| Step 12 | From the **Boot Policy** drop-down list, choose one of the following: |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Boot Policy to use</strong></td>
<td>Assigns the default boot policy to this service profile. Continue with Step 13.</td>
</tr>
<tr>
<td><strong>Create a Specific Boot Policy</strong></td>
<td>Enables you to create a local boot policy that can only be accessed by this service profile.</td>
</tr>
<tr>
<td>**Boot Policies **</td>
<td>Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but want to create a policy that all service profiles can access, click <strong>Create Boot Policy</strong>. Otherwise, choose a policy from the list and continue with Step 13.</td>
</tr>
</tbody>
</table>

| Step 13 | If you created a new boot policy accessible to all service profiles and template, choose that policy from the **Boot Policy** drop-down list. |

| Step 14 | Click **Next**. |

**What to do next**

Associate your Service Profile with a Cisco UCS server.
Deleting a Boot Policy

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Policies &gt; Organization_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the Boot Policies node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the policy you want to delete and choose Delete.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If a confirmation dialog box displays, click Yes.</td>
</tr>
</tbody>
</table>

UEFI Boot Parameters

UEFI boot mode for servers is dependent on information that is stored on the platform hardware. The boot entry, which contains information about the UEFI OS boot loader, is stored in the BIOS flash of the server. In Cisco UCS Manager releases earlier than Release 2.2(4), when a service profile is migrated from one server to another server, the boot loader information is not available on the destination server. Hence, the BIOS cannot load the boot loader information for the server to boot in UEFI boot mode.

Cisco UCSM Release 2.2(4) introduces UEFI boot parameters to provide the BIOS with information about the location of the UEFI OS boot loader on the destination server from where the BIOS loads it. Now, the server can use the boot loader information and boot in UEFI boot mode.

Guidelines and Limitations for UEFI Boot Parameters

- You can configure UEFI boot parameters only if the boot mode is UEFI.
- When you upgrade Cisco UCS Manager to Release 2.2(4) and higher UEFI boot failure during service profile migration is not handled automatically. You must explicitly create the UEFI boot parameters in the target device to successfully boot to the UEFI-capable OS.
- UEFI boot parameters are supported on all M3 and higher servers that support second-level boot order.
- You can specify UEFI boot parameters for the following device types:
  - SAN LUN
  - ISCSI LUN
  - Local LUN
- UEFI boot parameters are specific to each operating system. You can specify UEFI boot parameters for the following operating systems:
  - VMware ESX
  - SuSE Linux
• Microsoft Windows
• Red Hat Enterprise Linux 7

Setting UEFI Boot Parameters

Before you begin

Ensure that the Boot Mode of the boot policy is Uefi.

Procedure

Step 1
In the Navigation pane, click Servers.

Step 2
Expand Servers > Policies.

Step 3
Expand Boot Policies and select the boot policy for which you want to configure UEFI boot parameters.

Step 4
In the Work pane, click the General tab.

Step 5
To set UEFI boot parameters for a LUN, select the LUN in the Boot Order area and click Set Uefi Boot Parameters.

Important You can configure UEFI boot parameters only for local LUNs, SAN LUNs, and iSCSI LUNs.

Step 6
In the Set Uefi Boot Parameters dialog box, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Loader Name</td>
<td>Specifies the name of the boot loader. This is a mandatory field. Example—grub.efi</td>
</tr>
<tr>
<td>Boot Loader Path</td>
<td>Specifies the path where the boot loader is located. The name of the boot loader must not be included in this field. Only the path must be specified. Example—\EFI\RedHat</td>
</tr>
<tr>
<td>Boot Loader Description</td>
<td>Describes the boot loader. This is the human readable name that appears in the F6 boot menu.</td>
</tr>
</tbody>
</table>

Step 7
Click OK

Step 8
Click Save Changes.

Modifying UEFI Boot Parameters

Before you begin

Ensure that the Boot Mode of the boot policy is Uefi.
Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand Boot Policies, and select the boot policy for which you want to modify UEFI boot parameters.
Step 4  In the Work pane, click the General tab.
Step 5  To modify UEFI boot parameters for a LUN with UEFI boot parameters, select the LUN in the Boot Order area and click Modify Uefi Boot Parameters.

Important  You can configure UEFI boot parameters only for local LUNs, SAN LUNs, and iSCSI LUNs.

Step 6  In the Modify Uefi Boot Parameters dialog box, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Loader Name</td>
<td>Specifies the name of the boot loader. This is a mandatory field.</td>
</tr>
<tr>
<td>Boot Loader Path</td>
<td>Specifies the path where the boot loader is located. This is a mandatory field.</td>
</tr>
<tr>
<td>Boot Loader Description</td>
<td>Describes the boot loader.</td>
</tr>
</tbody>
</table>

Step 7  Click OK
Step 8  Click Save Changes.
Service Profiles

- Service Profiles in UCS Manager, on page 153
- Service Profiles that Override Server Identity, on page 154
- Service Profiles that Inherit Server Identity, on page 154
- Guidelines and Recommendations for Service Profiles, on page 155
- Methods of Creating Service Profiles, on page 155
- Inband Service Profiles, on page 159
- Service Profile Tasks, on page 159
- Service Profile Association, on page 169
- Service Profile Templates, on page 170
- Service Profile Template Tasks, on page 174
- Service Profile Association, on page 179

Service Profiles in UCS Manager

A service profile defines a single server and its storage and networking characteristics. You can create a service profile for Cisco UCS Manager and UCS Mini. When a service profile is deployed to a server, UCS Manager automatically configures the server, adapters, fabric extenders, and fabric interconnects to match the configuration specified in the service profile.

A service profile includes four types of information:

- **Server definition**: Defines the resources (e.g. a specific server or a blade inserted to a specific chassis) that are required to apply to the profile.

- **Identity information**: Includes the UUID, MAC address for each virtual NIC (vNIC), and WWN specifications for each HBA.

- **Firmware revision specifications**: Used when a certain tested firmware revision is required to be installed or for some other reason a specific firmware is used.

- **Connectivity definition**: Configures network adapters, fabric extenders, and parent interconnects, however this information is abstract as it does not include the details of how each network component is configured.

The UCS system provides two types of service profiles: Service profiles that inherit server identity and service profiles that override server identity.
Service Profiles that Override Server Identity

This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies set up in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server, then associate it with another server. This re-association can be done either manually or through an automated server pool policy. The burned-in settings, such as UUID and MAC address on the new server are overwritten with the configuration in the service profile. As a result, the change in the server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Unless the service profile contains power management policies, a server pool qualification policy, or another policy that requires a specific hardware configuration, you can use the profile for any type of server in the Cisco UCS domain.

You can associate these service profiles with either a rack-mount server or a blade server. The ability to migrate the service profile depends upon whether you choose to restrict migration of the service profile.

Note

If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association might fail.

Service Profiles that Inherit Server Identity

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved or migrated to another server.

You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two NICs
- For a converged network adapter or a virtual interface card, the WWN addresses for the two HBAs
- BIOS versions
- Server UUID
Important

The server identity and configuration information inherited through this service profile might not have the values burned into the server hardware at the manufacturer if those values were changed before this profile is associated with the server.

Guidelines and Recommendations for Service Profiles

In addition to any guidelines or recommendations that are specific to policies and pools included in service profiles and service profile templates, such as the local disk configuration policy, adhere to the following guidelines and recommendations that impact the ability to associate a service profile with a server:

Limit to the Number of vNICs that Can Be Configured on a Rack-Mount Server

You can configure up to 56 vNICs per supported adapter, such as the Cisco UCS P81E Virtual Interface Card (N2XX-ACPCI01), on any rack-mount server that is integrated with Cisco UCS Manager.

No Power Capping Support for Rack-Mount Servers

Power capping is not supported for rack servers. If you include a power control policy in a service profile that is associated with a rack-mount server, the policy is not implemented.

QoS Policy Guidelines for vNICs

You can only assign a QoS policy to a vNIC if the priority setting for that policy is not set to fc, which represents the Fibre Channel system class. You can configure the priority for the QoS policy with any other system class.

QoS Policy Guidelines for vHBAs

You can only assign a QoS policy to a vHBA if the priority setting for that policy is set to fc, which represents the Fibre Channel system class.

The Host Control setting for a QoS policy applies to vNICs only. It has no effect on a vHBA.

Methods of Creating Service Profiles

Creating a Service Profile with the Expert Wizard

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles.
Step 3  Expand the node for the organization where you want to create the service profile.

If the system does not include multitenancy, expand the root node.
Creating a Service Profile with the Expert Wizard

**Step 4** Right-click the organization and select **Create Service Profile (expert)**.

**Step 5** In the **Identify Service Profile** panel, specify the service profile **Name**, UUID assignment and click **Next**.

You can provide an optional description for this service profile. If the UUID is not available, you can also create a UUID Suffix Pool from this panel.

**Note** To create a service profile quickly, you can click **Finish** after specifying the name. Cisco UCS Manager creates a new service profile with the specified name and all system default values.

**Step 6** (Optional) In the **Networking** panel, specify the required information for the **Dynamic vNIC Connection Policy** and **LAN Connectivity** sections, then click **Next**.

You can create a dynamic vNIC connection policy and LAN connectivity policy from this panel.

**Note** Dynamic vNICs, usNICs, and VMQs are not supported when creating a vNIC for a LAN Connectivity Policy. RoCE, VXLAN, NvGRE are not supported when configuring the Ethernet Adapter Policy.

**Step 7** (Optional) In the **Storage** panel, specify the SAN configuration information such as, **Local Storage Policy**, **SAN Connectivity**, WWNN and VSAN, then click **Next**.

You can create a local disk configuration policy and SAN connectivity policy from this panel.

**Note** FC vNICs are not supported when configuring vHBA under the Storage Policy.

**Step 8** (Optional) In the **Zoning** panel, specify the required zoning information, then click **Next**.

You can create the vHBA initiator groups from this panel.

**Step 9** (Optional) In the **vNIC/vHBA Placement** panel, specify the placement method and PCI order, then click **Next**.

You can create a placement policy from this panel.

**Step 10** (Optional) In the **Server Boot Order** panel, specify the **Boot Policy** from the drop-down list, then click **Next**.

You can create a boot policy from this panel.

**Step 11** (Optional) In the **Maintenance Policy** panel, specify the maintenance policy, then click **Next**.

You can create a new maintenance policy and specify a maintenance schedule from this panel.

**Step 12** (Optional) In the **Server Assignment** panel, specify the **Server Assignment** from the drop down list and the power state to apply on assignment, then click **Next**.

You can create a server pool or a host firmware package from this panel.

**Step 13** (Optional) In the **Operational Policies** panel, specify the system operational information such as, **BIOS Configuration**, **External IPMI Management Configuration**, **Management IP Address**, **Monitoring Configuration (Thresholds)**, **Power Control Policy Configuration**, and **Scrub Policy**, then click **Finish**.

**Note** To set up an Outband IPv4 address or an Inband IPv4 or IPv6 address, click the respective tabs and complete the required fields.

If you do not find the policies you need for each of these configurations, you can create them from this panel.
Creating a Service Profile that Inherits Server Identity

Procedure

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Servers > Service Profiles**.

**Step 3** Expand the node for the organization where you want to create the service profile.

If the system does not include multitenancy, expand the **root** node.

**Step 4** Right-click the organization and select **Create Service Profile**.

**Step 5** In the **Naming** area of the **Create Service Profile** dialog box, complete the following fields:

a) In the **Name** field, enter a unique name that you can use to identify the service profile.

This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.

b) In the **Description** field, enter a description of this service profile.

**Step 6** In the **vNICs** area of the **Create Service Profile** dialog box, choose the primary and secondary vNICs.

**Step 7** In the **vHBAs** area of the **Create Service Profile** dialog box, choose the primary and secondary vHBAs.

**Step 8** In the **Boot Order** area of the **Create Service Profile** dialog box, choose the primary and secondary boot devices.

**Step 9** (Optional) In the **Select** column of the **Server Association (optional)** area, click the radio button for a server to associate this service profile with that server.

**Step 10** Click **OK**.

Creating a Hardware Based Service Profile for a Blade Server

You cannot move a hardware based service profile to another server.

Procedure

**Step 1** In the **Navigation** pane, click **Equipment**.

**Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.

**Step 3** Choose the server for which you want to create a hardware based service profile.

**Step 4** In the **Work** pane, click the **General** tab.

**Step 5** In the **Actions** area, click **Create Service Profile**.

**Step 6** In the **Create Service Profile for Server** dialog box, do the following:

a) From the **Create Service Profile in Organization** drop-down list, select the organization in which you want to create the service profile.

b) Click the **Hardware Based Service Profile** radio button.

c) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.

d) If you want Cisco UCS Manager to create vNICs for the service profile, check the Create Default vNICs check box.
e) If you want Cisco UCS Manager to create vHBAs for the service profile, check the Create Default vHBAs check box.
f) Click OK.

Cisco UCS Manager inherits and automatically applies the identity and configuration information in the server, creates the service profile, and associates it with the server.

Creating a Hardware Based Service Profile for a Rack-Mount Server

You cannot move a hardware based service profile to another server.

**Procedure**

**Step 1** In the Navigation pane, click Equipment.

**Step 2** Expand Equipment > Rack Mounts > Servers.

**Step 3** Choose the server for which you want to create a hardware based service profile.

**Step 4** In the Work pane, click the General tab.

**Step 5** In the Actions area, click Create Service Profile.

**Step 6** In the Create Service Profile for Server dialog box, do the following:

a) From the Create Service Profile in Organization drop-down list, select the organization in which you want to create the service profile.

b) Click the Hardware Based Service Profile radio button.

c) In the Name field, enter a unique name for the service profile.

This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.

d) If you want Cisco UCS Manager to create vNICs for the service profile, check the Create Default vNICs check box.

e) If you want Cisco UCS Manager to create vHBAs for the service profile, check the Create Default vHBAs check box.

f) Click OK.

Cisco UCS Manager inherits and automatically applies the identity and configuration information in the server, creates the service profile, and associates it with the server.
Inband Service Profiles

Deleting the Inband Configuration from a Service Profile

This procedure removes the inband management IP address configuration from a service profile. If this action is greyed out, no inband configuration was configured.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Service Profiles &gt; Service_Profile_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Actions area, click Delete Inband Configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Yes in the Delete confirmation dialog box.</td>
</tr>
</tbody>
</table>

The inband management IP address configuration for the service profile is deleted.

Service Profile Tasks

Renaming a Service Profile

When you rename a service profile, the following occurs:

- Event logs and audit logs that reference the previous name for the service profile are retained under that name.
- A new audit record is created to log the rename operation.
- All records of faults against the service profile under its previous name are transferred to the new service profile name.

Note

You cannot rename a service profile with pending changes.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Service Profiles.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization that includes the service profile you want to rename.</td>
</tr>
</tbody>
</table>
If the system does not include multitenancy, expand the root node.

**Step 4**  Click the service profile you want to rename.

**Step 5**  In the Work pane, click the General tab.

**Step 6**  In the Actions area, click Rename Service Profile.

**Step 7**  In the Rename Service Profile dialog box, enter the new name for the service profile in the New Name field.

This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.

**Step 8**  Click OK.

---

**Cloning a Service Profile**

**Procedure**

**Step 1**  In the Navigation pane, click Servers.

**Step 2**  Expand Servers > Service Profiles.

**Step 3**  Expand the node for the organization where you want to create the service profile.

If the system does not include multitenancy, expand the root node.

**Step 4**  Right-click the service profile you want to clone and select Create a Clone.

**Step 5**  In the Create Clone From Service Profile dialog box:

a) Enter the name you want to use for the new profile in the Clone Name field.

   This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.

   This name must be unique within the organization or sub-organization in which you are creating the service profile.

b) Click OK.

**Step 6**  Navigate to the service profile you just created and make sure that all options are correct.

---

**Changing the UUID in a Service Profile**

**Procedure**

**Step 1**  In the Navigation pane, click Servers.

**Step 2**  Expand Servers > Service Profiles.

**Step 3**  Expand the node for the organization that contains the service profile for which you want to change the UUID.
If the system does not include multitenancy, expand the root node.

**Step 4** Choose the service profile that requires the UUID for the associated server to be changed.

**Step 5** In the **Work** pane, click the **General** tab.

**Step 6** In the **Actions** area, click **Change UUID**.

**Step 7** From the **UUID Assignment** drop-down list, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (pool default used by default)</td>
<td>Assigns a UUID from the default UUID Suffix pool.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 9.</td>
</tr>
<tr>
<td><strong>Hardware Default</strong></td>
<td>Uses the UUID assigned to the server by the manufacturer.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.</td>
</tr>
<tr>
<td><strong>XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</strong></td>
<td>Uses the UUID that you manually assign.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 8.</td>
</tr>
<tr>
<td><strong>Pools Pool_Name</strong></td>
<td>Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.</td>
</tr>
<tr>
<td></td>
<td>Continue with Step 9.</td>
</tr>
</tbody>
</table>

**Step 8** (Optional) If you selected the **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** option, do the following:

a) In the **UUID** field, enter the valid UUID that you want to assign to the server which uses this service profile.

b) To verify that the selected UUID is available, click the **here** link.

**Step 9** Click **OK**.
Modifying the Boot Order in a Service Profile

Procedure

**Step 1**
In the **Navigation** pane, click **Servers**.

**Step 2**
Expand **Servers > Service Profiles**.

**Step 3**
Expand the node for the organization that includes the service profile for which you want to change the boot order.

If the system does not include multi-tenancy, expand the **root** node.

**Step 4**
Click the service profile for which you want to change the boot order.

**Step 5**
In the **Work** pane, click the **Boot Order** tab.

**Step 6**
Click **Modify Boot Policy** to change the existing boot policy.

**Step 7**
In the **Modify Boot Policy** dialog box, choose one of the following from the **Boot Policy** drop-down list:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Boot Policy to use</td>
<td>Assigns the default boot policy to this service profile. Continue with Step 14.</td>
</tr>
<tr>
<td>Create a Specific Boot Policy</td>
<td>Enables you to create a local boot policy that can only be accessed by this service profile. Continue with Step 8.</td>
</tr>
<tr>
<td>Boot Policies <strong>Policy_Name</strong></td>
<td>Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, click <strong>Create Boot Policy</strong> and continue with Step 2. Otherwise, continue with Step 14.</td>
</tr>
</tbody>
</table>

**Step 8**
If you chose to create a boot policy, in the **Create Boot Policy** dialog box, enter a unique name and description for the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

**Step 9**
(Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.

In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

**Step 10**
(Optional) If desired, check the **Enforce vNIC/vHBA/iSCSI Name** check box.

- If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the **Boot Order** table match the server configuration in the service profile.
• If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

**Step 11**

To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.
b) Click one of the following links to add the device to the **Boot Order** table:

- **Add Local Disk** or
  - Add Local LUN
  - Add Local JBOD
  - Add SD Card
  - Add Internal USB
  - Add External USB
  - Add Embedded Local LUN
  - Add Embedded Local Disk

- **Add CD/DVD** or
  - Add Local CD/DVD
  - Add Local Remote CD/DVD

  In a setup with M5 blade servers, if an ISO is mapped to the KVM console, use only **Add Remote CD/DVD** in **Boot Order**.

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

**Step 12**

To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.
b) Click the **Add LAN Boot** link.
c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.
d) Add another device to the **Boot Order** table, or click **OK** to finish.

**Step 13**

To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.
b) Click the **Add SAN Boot** link.
c) In the **Add San Boot** dialog box, specify the vHBA and type, then click **OK**.
d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, specify the boot target LUN, boot target WWPN, and type, then click **OK**.
e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

**Step 14**

Click **OK**.
Creating a vNIC for a Service Profile

**Procedure**

**Step 1** In the Navigation pane, click Servers.

**Step 2** Expand Servers > Service Profiles.

**Step 3** Expand the node for the organization that contains the service profile for which you want to create a vNIC.

**Step 4** Expand the service profile for which you want to create a vNIC.

**Step 5** Right-click the vNICs node and choose Create vNICs.

**Step 6** In the Create vNIC dialog box, enter the name, select a MAC Address Assignment, and check the Use vNIC Template check box if you want to use an existing vNIC template.

You can also create a MAC pool from this area.

**Step 7** Choose the Fabric ID, select the VLANs that you want to use, enter the CDN Name and MTU, and choose a Pin Group.

You can also create a VLAN and a LAN pin group from this area.

**Step 8** In the Operational Parameters area, choose a Stats Threshold Policy.

**Step 9** In the Adapter Performance Profile area, choose an Adapter Policy, QoS Policy, and a Network Control Policy.

You can also create an Ethernet adapter policy, QoS policy, and network control policy from this area.

**Step 10** In the Connection Policies area, choose the Dynamic vNIC, usNIC or VMQ radio button, then choose the corresponding policy.

You can also create a dynamic vNIC, usNIC, or VMQ connection policy from this area.

**Step 11** Click OK.

Deleting a vNIC from a Service Profile

**Procedure**

**Step 1** In the Navigation pane, click Servers.

**Step 2** Expand Servers > Service Profiles.

**Step 3** Expand the node for the organization that contains the service profile from which you want to delete a vNIC.

**Step 4** Expand the service profile from which you want to delete a vNIC.

**Step 5** Expand the vNICs node.

**Step 6** Right-click the vNIC you want to delete and choose Delete.

**Step 7** If a confirmation dialog box displays, click Yes.
Creating a vHBA for a Service Profile

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <em>Navigation</em> pane, click <em>Servers</em>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand <em>Servers &gt; Service Profiles</em>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization that contains the service profile for which you want to create a vHBA.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand the service profile for which you want to create a vHBA.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Right-click the <em>vHBAs</em> node and choose <em>Create vHBAs</em>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the <em>Create vHBAs</em> dialog box, enter the name and optional description.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose the <em>Fabric ID, Select VSAN, Pin Group, Persistent Binding,</em> and <em>Max Data Field Size.</em> You can also create a VSAN or SAN pin group from this area.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the <em>Operational Parameters</em> area, choose the <em>Stats Threshold Policy.</em></td>
</tr>
<tr>
<td>Step 9</td>
<td>In the <em>Adapter Performance Profile</em> area, choose the <em>Adapter Policy</em> and <em>QoS Policy.</em> You can also create a fibre channel adapter policy or QoS policy from this area.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

Changing the WWPN for a vHBA

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <em>Navigation</em> pane, click <em>Servers</em>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand <em>Servers &gt; Service Profiles</em>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization that contains the service profile for which you want to change the WWPN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand <em>Service_Profile_Name &gt; vHBAs</em>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the vHBA for which you want to change the WWPN.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the <em>Work</em> pane, click the <em>General</em> tab.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the <em>Actions</em> area, click <em>Change World Wide Name</em>.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the <em>Change World Wide Port Name</em> dialog box, complete the required fields.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>
Clearing Persistent Binding for a vHBA

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles.
Step 3  Expand the node for the organization that contains the service profile for which you want to modify the vHBA.
Step 4  Expand Service_Profile_Name > vHBAs.
Step 5  Click the vHBA for which you want to clear the persistent binding.
Step 6  In the Work pane, click the General tab.
Step 7  In the Actions area, click Clear Persistent Binding.
Step 8  If a confirmation dialog box displays, click Yes.

Deleting a vHBA from a Service Profile

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles.
Step 3  Expand the node for the organization that contains the service profile from which you want to delete a vHBA.
Step 4  Expand the service profile from which you want to delete a vHBA.
Step 5  Expand the vHBAs node.
Step 6  Right-click the vHBA you want to delete and choose Delete.
Step 7  If a confirmation dialog box displays, click Yes.

Adding a vHBA Initiator Group to a Service Profile

Procedure

Step 1  Expand Servers > Service Profiles.
Step 2  Expand the node for the organization that contains the service profile to which you want to add a vHBA initiator group.

If the system does not include multitenancy, expand the root node.

Step 3  Choose the service profile to which you want to add a vHBA initiator group.
Step 4  In the Work pane, click the Storage > vHBA Initiator Groups.
Step 5  On the icon bar at the right of the Select vHBA Initiator Groups table, click +.
Step 6  
In the **Create vHBA Initiator Group** dialog box, complete the following fields to set the name and description:

<table>
<thead>
<tr>
<th>Name field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Name** | The name of the vHBA initiator group.  
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved. |
| **Description** | A description of the group.  
Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ’ (single quote). |

Step 7  
In the **Select vHBA Initiators** table, check the check box in the **Select** column for each vHBA you want to include in the vHBA initiator group.

Step 8  
To add a storage connection policy to the initiator group, choose one of the following options:

- Choose an existing storage connection policy from the **Storage Connection Policy** drop-down list. Continue with Step 10.

- Click the **Create Storage Connection Policy** link if you want to create a new storage connection policy that will be available for use by other vHBA initiator groups within the Cisco UCS domain. For more information, see Creating a Fibre Channel Storage Connection Policy. After you create the storage connection policy, continue with Step 10.

- Choose the **Specific Storage Connection Policy** option to create a storage connection policy that is only available to this vHBA initiator group. Continue with Step 9.

Step 9  
In the **Specific Storage Connection Policy** area, complete the following fields to create a storage connection policy that is only available to this vHBA initiator group:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Description** | A description of the policy. Cisco recommends including information about where and when to use the policy.  
Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ’ (single quote). |
Deleting a Service Profile

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles > Organization_Name.
Step 3  Right-click the service profile you want to delete and select Delete.
Step 4  If a confirmation dialog box displays, click Yes.
Step 5  Click OK.
Service Profile Association

Associating a Service Profile with a Server or Server Pool

Follow this procedure if you did not associate the service profile with a blade server or server pool when you created it, or to change the blade server or server pool with which a service profile is associated.

Procedure

Step 1  In the Navigation pane, click Servers.

Step 2  Expand Servers > Service Profiles.

Step 3  Expand the node for the organization that contains the service profile that you want to associate with a new server or server pool.

If the system does not include multitenancy, expand the root node.

Step 4  Right-click the service profile you want to associate with a server and select Associate Service Profile.

Step 5  In the Associate Service Profile dialog box, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Pool</td>
<td>Select a server pool from the drop-down list. Cisco UCS Manager assigns a server from this pool to the service profile. Continue with Step 7.</td>
</tr>
<tr>
<td>Server</td>
<td>Navigate to the desired available server in the navigation tree and select the server which will be assigned to the service profile. Continue with Step 7.</td>
</tr>
<tr>
<td>Custom Server</td>
<td>Specifies the chassis and slot that contains the server that will be assigned to the service profile. If the server is not in the slot or is otherwise unavailable, the service profile will be associated with the server when it becomes available. Continue with Step 6.</td>
</tr>
</tbody>
</table>

Step 6  If you chose Custom Server, do the following:

a)  In the Chassis Id field, enter the number of the chassis where the selected server is located.

b)  In the Server Id field, enter the number of the slot where the selected server is located.

Step 7  If you want to restrict the migration of the service profile after it is associated with a server, check the Restrict Migration check box.

If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association might fail.

Step 8  Click OK.
Disassociating a Service Profile from a Server or Server Pool

When you disassociate a service profile, Cisco UCS Manager attempts to shutdown the operating system on the server. If the operating system does not shutdown within a reasonable length of time, Cisco UCS Manager forces the server to shutdown.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Service Profiles.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization that contains the service profile that you want to disassociate from a server or server pool. If the system does not include multitenancy, expand the root node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the service profile you want to disassociate from a server and select Disassociate Service Profile.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Disassociate Service Profile dialog box, click Yes to confirm that you want to disassociate the service profile.</td>
</tr>
<tr>
<td>Step 6</td>
<td>(Optional) Monitor the status and FSM for the server to confirm that the disassociation completed.</td>
</tr>
</tbody>
</table>

Service Profile Templates

Initial and Existing Templates

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.

Tip

If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

Initial template

Service profiles created from an initial template inherit all the properties of the template. Service profiles created from an initial service profile template are bound to the template. However, changes to the initial template do not automatically propagate to the bound service profiles. If you want to propagate changes to bound service profiles, unbind and rebind the service profile to the initial template.
**Updating template**

Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

**Note**

Service profiles that are created from the initial template and normal service profiles fetch the lowest available IDs in the sequential pool when you press **Reset**.

Service profiles created from updating template might attempt to retain the same ID when you press **Reset** even when lower IDs of sequential pool are free.

---

**Creating a Service Profile Template**

**Procedure**

**Step 1**
In the **Navigation** pane, click **Servers**.

**Step 2**
Expand **Servers > Service Profile Templates**.

**Step 3**
Expand the node for the organization where you want to create the service profile template.

If the system does not include multitenancy, expand the **root** node.

**Step 4**
Right-click the organization and choose **Create Service Profile Template**.

**Step 5**
In the **Identify Service Profile Template** panel, specify the service profile **Name**, **Type**, and **UUID Assignment**, then click **Next**.

You can provide an optional description for this service profile template.

**Note**

To create a service profile template quickly, you can click **Finish** after specifying the name. Cisco UCS Manager creates a new service profile template with the specified name and all system default values.

**Step 6**
(Optional) In the **Networking** panel, specify the required information for the **Dynamic vNIC Connection Policy** and **LAN Connectivity** sections, then click **Next**.

You can create a dynamic vNIC connection policy and LAN connectivity policy from this panel.

**Step 7**
(Optional) In the **Storage** panel, specify the SAN configuration information such as, **Local Storage Policy**, **SAN Connectivity**, **WWNN**, and **vHBAs**, then click **Next**.

You can create a local disk configuration policy and SAN connectivity policy from this panel.

**Step 8**
(Optional) In the **Zoning** panel, specify the required zoning information, then click **Next**.

You can create the vHBA initiator groups from this panel.

**Step 9**
(Optional) In the **vNIC/vHBA Placement** panel, specify the placement method and PCI order, then click **Next**.

You can create a placement policy from this panel.

**Step 10**
(Optional) In the **Server Boot Order** panel, specify the **Boot Policy** from the drop-down list, then click **Next**.
You can create a boot policy from this panel.

**Step 11**  
(Optional) In the **Maintenance Policy** panel, specify the maintenance policy, then click **Next**.

You can create a new maintenance policy and specify a maintenance schedule from this panel.

**Step 12**  
(Optional) In the **Server Assignment** panel, specify the **Pool Assignment** from the drop down list and the power state to apply on assignment, then click **Next**.

You can create a server pool or a host firmware package from this panel.

**Step 13**  
(Optional) In the **Operational Policies** panel, specify the system operational information such as, **BIOS Configuration**, **External IPMI Management Configuration**, **Management IP Address**, **Monitoring Configuration (Thresholds)**, **Power Control Policy Configuration**, and **Scrub Policy**, then click **Finish**.

**Note**  
To set up an Outband IPv4 address or an Inband IPv4 or IPv6 address, click the respective tabs and complete the required fields.

If you do not find the policies you need for each of these configurations, you can create them from this panel.

---

**Creating One or More Service Profiles from a Service Profile Template**

**Procedure**

**Step 1**  
In the **Navigation** pane, click **Servers**.

**Step 2**  
Expand **Servers > Service Profile Templates**.

**Step 3**  
Expand the node for the organization that contains the service profile template that you want to use as the basis for your service profiles.

If the system does not include multitenancy, expand the **root** node.

**Step 4**  
Right-click the service profile template from which you want to create the profiles and select **Create Service Profiles From Template**.

**Step 5**  
In the **Create Service Profiles From Template** dialog box, complete the required fields.

**Step 6**  
Click **OK**.

---

**Creating a Template Based Service Profile for a Blade Server**

**Before you begin**

A qualified service profile template with the desired values must exist in Cisco UCS Manager.

**Procedure**

**Step 1**  
In the **Navigation** pane, click **Equipment**.
Creating a Template Based Service Profile for a Rack-Mount Server

Before you begin

A qualified service profile template with the desired values must exist in Cisco UCS Manager.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Rack Mounts > Servers.
Step 3 Choose the server for which you want to create a template based service profile.
Step 4 In the Work pane, click the General tab.
Step 5 In the Actions area, click Create Service Profile.
Step 6 In the Create Service Profile for Server dialog box, do the following:
   a) Click the Template Based Service Profile radio button.
   b) In the Name field, enter a unique name for the service profile.
      This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special
      characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique
      across all service profiles and service profile templates within the same organization.
   c) From the Service Profile Template drop-down list, select the template from which you want to create
      the service profile associated with this server.
      Note The drop-down list only lists service profile templates compatible with the selected blade server.
   d) Click OK.
Creating a Service Profile Template from a Service Profile

**Procedure**

- **Step 1**: In the Navigation pane, click Servers.
- **Step 2**: Expand Servers > Service Profiles.
- **Step 3**: Expand the node for the organization that contains the service profile that you want to use as the basis for your template.
  - If the system does not include multitenancy, expand the root node.
- **Step 4**: Right-click the service profile from which you want to create the template and select Create a Service Profile Template.
- **Step 5**: In the Create Template From Service Profile dialog box, complete the required fields.
- **Step 6**: Click OK.

Setting an Asset Tag for a Service Profile

**Procedure**

- **Step 1**: Navigate to Servers > Service Profiles.
- **Step 2**: Expand the node for which you want to create the asset tag.
  - If the system does not include multitenancy expand the root node.
- **Step 3**: In the Work pane, click the General tab.
- **Step 4**: In the Asset Tag field, enter a name to identify the server.
  - The name can be between 2 to 32 alphanumeric characters. You can use space or any special characters other than `` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
- **Step 5**: Click Save Changes.
- **Step 6**: Reboot the server manually for the changes to be in effect.

Service Profile Template Tasks

**Binding a Service Profile to a Service Profile Template**

You can bind a service profile to a service profile template. When you bind the service profile to a template, Cisco UCS Manager configures the service profile with the values defined in the service profile template. If the existing service profile configuration does not match the template, Cisco UCS Manager reconfigures the
service profile. You can only change the configuration of a bound service profile through the associated template.

**Procedure**

**Step 1**  In the **Navigation** pane, click **Servers**.

**Step 2**  Expand **Servers > Service Profiles**.

**Step 3**  Expand the node for the organization that includes the service profile you want to bind.

If the system does not include multi-tenancy, expand the **root** node.

**Step 4**  Click the service profile you want to bind.

**Step 5**  In the **Work** pane, click the **General** tab.

**Step 6**  In the **Actions** area, click **Bind to a Template**.

**Step 7**  In the **Bind to a Service Profile Template** dialog box, do the following:

a)  From the **Service Profile Template** drop-down list, choose the template to which you want to bind the service profile.

b)  Click **OK**.

---

### Changing the UUID in a Service Profile Template

**Procedure**

**Step 1**  In the **Navigation** pane, click **Servers**.

**Step 2**  Expand **Servers > Service Profile Templates**.
Step 3  Expand the node for the organization that contains the service profile template for which you want to change the UUID.

If the system does not include multitenancy, expand the root node.

Step 4  Choose the service profile template whose UUID assignment you want to change.

Step 5  In the Work pane, click the General tab.

Step 6  In the Actions area, click Change UUID.

Step 7  From the UUID Assignment drop-down list, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select (pool default used by default)</td>
<td>Assigns a UUID from the default UUID Suffix pool.</td>
</tr>
<tr>
<td>Hardware Default</td>
<td>Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.</td>
</tr>
<tr>
<td>Pools Pool_Name</td>
<td>Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.</td>
</tr>
</tbody>
</table>

Step 8  Click OK.

---

**Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template**

If you change the UUID suffix pool assigned to an updating service profile template, Cisco UCS Manager does not change the UUID assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a UUID from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the UUID. You can only reset the UUID assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a UUID assigned from a UUID suffix pool.
- The UUID suffix pool name is specified in the service profile. For example, the pool name is not empty.
- The UUID value is not 0, and is therefore not derived from the server hardware.

**Procedure**

Step 1  In the Navigation pane, click Servers.

Step 2  Expand Servers > Service Profiles.
Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template

If you change the MAC pool assigned to an updating service profile template, Cisco UCS Manager does not change the MAC address assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a MAC address from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the MAC address. You can only reset the MAC address assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a MAC address assigned from a MAC pool.
- The MAC pool name is specified in the service profile. For example, the pool name is not empty.
- The MAC address value is not 0, and is therefore not derived from the server hardware.

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Service Profiles.
Step 3  Expand the node for the organization that contains the service profile for which you want to reset the MAC address.
        If the system does not include multitenancy, expand the root node.
Step 4  Expand Service_Profile_Name > vNICs.
Step 5  Click the vNIC for which you want to reset the MAC address.
Step 6  In the Work pane, click the General tab.
Step 7  In the Actions area, click Reset MAC Address.
Step 8  If a confirmation dialog box displays, click Yes.
Step 9  Click OK.
### Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template

If you change the WWPN pool assigned to an updating service profile template, Cisco UCS Manager does not change the WWPN assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a WWPN from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the WWPN. You can only reset the WWPN assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a WWPN assigned from a WWPN pool.
- The WWPN pool name is specified in the service profile. For example, the pool name is not empty.
- The WWPN value is not 0, and is therefore not derived from the server hardware.

#### Procedure

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers > Service Profiles**.
3. Expand the node for the organization that contains the service profile for which you want to reset the WWPN. If the system does not include multitenancy, expand the **root** node.
4. Expand **Service_Profile_Name > vHBAs**.
5. Click the vHBA for which you want to reset the WWPN.
6. In the **Work** pane, click the **General** tab.
7. In the **Actions** area, click **Reset WWPN**.
8. If a confirmation dialog box displays, click **Yes**.
9. Click **OK**.

### Deleting the Inband Configuration from a Service Profile Template

This procedure removes the inband management IP address configuration from a service profile template. If this action is greyed out, no inband configuration was configured.

#### Procedure

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers > Service Profile Template > Service_Profile_Template_Name**.
3. In the **Work** pane, click the **General** tab.
4. In the **Actions** area, click **Delete Inband Configuration**.
5. Click **Yes** in the **Delete** confirmation dialog box.
The inband management IP address configuration for the service profile template is deleted.

---

**Service Profile Association**

**Associating a Service Profile with a Server or Server Pool**

Follow this procedure if you did not associate the service profile with a blade server or server pool when you created it, or to change the blade server or server pool with which a service profile is associated.

**Procedure**

**Step 1**  
In the Navigation pane, click **Servers**.

**Step 2**  
Expand **Servers > Service Profiles**.

**Step 3**  
Expand the node for the organization that contains the service profile that you want to associate with a new server or server pool.

If the system does not include multitenancy, expand the **root** node.

**Step 4**  
Right-click the service profile you want to associate with a server and select **Associate Service Profile**.

**Step 5**  
In the **Associate Service Profile** dialog box, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Pool</strong></td>
<td>Select a server pool from the drop-down list. Cisco UCS Manager assigns a server from this pool to the service profile. Continue with Step 7.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>Navigate to the desired available server in the navigation tree and select the server which will be assigned to the service profile. Continue with Step 7.</td>
</tr>
<tr>
<td><strong>Custom Server</strong></td>
<td>Specifies the chassis and slot that contains the server that will be assigned to the service profile. If the server is not in the slot or is otherwise unavailable, the service profile will be associated with the server when it becomes available. Continue with Step 6.</td>
</tr>
</tbody>
</table>

**Step 6**  
If you chose **Custom Server**, do the following:

a) In the **Chassis Id** field, enter the number of the chassis where the selected server is located.

b) In the **Server Id** field, enter the number of the slot where the selected server is located.

**Step 7**  
If you want to restrict the migration of the service profile after it is associated with a server, check the **Restrict Migration** check box.
If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association might fail.

**Step 8**  
Click OK.

---

**Associating a Service Profile Template with a Server Pool**

Follow this procedure if you did not associate the service profile template with a server pool when you created it, or to change the server pool with which a service profile created from this template is associated.

**Procedure**

**Step 1**  
In the Navigation pane, click Servers.

**Step 2**  
Expand Servers > Service Profile Templates.

**Step 3**  
Expand the node for the organization that contains the service profile that you want to associate with a server pool.

If the system does not include multitenancy, expand the root node.

**Step 4**  
Right-click the service profile template you want to associate with a server pool and select Associate with Server Pool.

The Associate with Server Pool dialog box opens.

**Step 5**  
From the Server Pool section of the Pool Assignment drop-down list, select a server pool.

If you select Assign Later, the service profile template is not associated with a server pool.

**Step 6**  
(Optional) From the Select Qualification drop-down list, select the server pool policy qualifications you want to apply to a server that is associated with a service profile created from this template.

**Step 7**  
Click OK.

---

**Disassociating a Service Profile from a Server or Server Pool**

When you disassociate a service profile, Cisco UCS Manager attempts to shutdown the operating system on the server. If the operating system does not shutdown within a reasonable length of time, Cisco UCS Manager forces the server to shutdown.

**Procedure**

**Step 1**  
In the Navigation pane, click Servers.

**Step 2**  
Expand Servers > Service Profiles.

**Step 3**  
Expand the node for the organization that contains the service profile that you want to disassociate from a server or server pool.
If the system does not include multitenancy, expand the root node.

Step 4  Right-click the service profile you want to disassociate from a server and select Disassociate Service Profile.

Step 5  In the Disassociate Service Profile dialog box, click Yes to confirm that you want to disassociate the service profile.

Step 6  (Optional) Monitor the status and FSM for the server to confirm that the disassociation completed.

---

Disassociating a Service Profile Template from its Server Pool

**Procedure**

Step 1  In the Navigation pane, click Servers.

Step 2  Expand Servers > Service Profile Templates.

Step 3  Expand the node for the organization that contains the service profile that you want to disassociate from its server pool.

If the system does not include multitenancy, expand the root node.

Step 4  Right-click the service profile template you want to disassociate from its server pool and select Disassociate Template.

Step 5  If a confirmation dialog box displays, click Yes.
Disassociating a Service Profile Template from its Server Pool
Server-Related Policies

- BIOS Settings, on page 183
- Trusted Platform Module, on page 239
- Consistent Device Naming, on page 242
- CIMC Security Policies, on page 246
- Graphics Card Policies, on page 248
- Local Disk Policies, on page 249
- Scrub Policy, on page 262
- DIMM Error Management, on page 265
- Serial over LAN Policy Settings, on page 267
- Server Autoconfiguration Policies, on page 268
- Server Discovery Policy Settings, on page 270
- Server Inheritance Policy Settings, on page 273
- Server Pool Policy Settings, on page 274
- Server Pool Policy Qualifications Settings, on page 276
- vNIC/vHBA Placement Policy Settings, on page 281
- CIMC Mounted vMedia, on page 293

BIOS Settings

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in an Cisco UCS domain. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enable you to fine tune the BIOS settings for a server managed by Cisco UCS Manager.

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS domain, or you can use only one of them. You can also use Cisco UCS Manager to view the actual BIOS settings on a server and determine whether they are meeting current needs.
Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

## Main BIOS Settings

The following table lists the main server BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Properties</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Reboot on BIOS Settings Change** | When the server is rebooted after you change one or more BIOS settings.  
If you enable this setting, the server is rebooted according to the maintenance policy in the server's service profile. For example, if the maintenance policy requires user acknowledgment, the server is not rebooted and the BIOS changes are not applied until a user acknowledges the pending activity.  
If you do not enable this setting, the BIOS changes are not applied until the next time the server is rebooted, whether as a result of another server configuration change or a manual reboot. |
| **BIOS Setting**              |                                                                                                                                           |
| **Quiet Boot**                | What the BIOS displays during Power On Self-Test (POST).  
This can be one of the following:  
  - **Disabled**—The BIOS displays all messages and Option ROM information during boot.  
  - **Enabled**—The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.  
  - **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST error pause</td>
<td>What happens when the server encounters a critical error during POST. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The BIOS continues to attempt to boot the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Resume on AC power loss</td>
<td>How the server behaves when power is restored after an unexpected power loss. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stay Off</strong>—The server remains off until manually powered on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last State</strong>—The server is powered on and the system attempts to restore its last state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reset</strong>—The server is powered on and automatically reset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Front panel lockout</td>
<td>Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The power and reset buttons on the front panel are active and can be used to affect the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
Consistent Device Naming allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made.

Whether consistent device naming is enabled or not. This can be one of the following:

- **Disabled** — Consistent device naming is disabled for the BIOS policy.
- **Enabled** — Consistent device naming is enabled for the BIOS policy. This enables Ethernet interfaces to be named consistently.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### Processor BIOS Settings

The following table lists the processor BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| CDN Control        | Consistent Device Naming allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made. Whether consistent device naming is enabled or not. This can be one of the following:  
  - **Disabled** — Consistent device naming is disabled for the BIOS policy.  
  - **Enabled** — Consistent device naming is enabled for the BIOS policy. This enables Ethernet interfaces to be named consistently.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Intel Turbo Boost Tech | Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following:  
  - **Disabled** — The processor does not increase its frequency automatically.  
  - **Enabled** — The processor uses Turbo Boost Technology if required.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
### Processor BIOS Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Enhanced Intel SpeedStep Tech** | Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:  
  - **Disabled** — The processor never dynamically adjusts its voltage or frequency.  
  - **Enabled** — The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  

We recommend that you contact your operating system vendor to make sure your operating system supports this feature. |
| **Intel HyperThreading Tech** | Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:  
  - **Disabled** — The processor does not permit hyperthreading.  
  - **Enabled** — The processor allows for the parallel execution of multiple threads.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  

We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |
| **Core Multi Processing** | Sets the state of logical processor cores per CPU in a package. If you disable this setting, Intel Hyper Threading technology is also disabled. This can be one of the following:  
  - **All** — Enables multiprocessing on all logical processor cores.  
  - **1 through n** — Specifies the number of logical processor cores per CPU that can run on the server. To disable multiprocessing and have only one logical processor core per CPU running on the server, choose 1.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  

We recommend that you contact your operating system vendor to make sure your operating system supports this feature. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Execute Disable Bit**     | Classifies memory areas on the server to specify where the application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:  
  - **Disabled** — The processor does not classify memory areas.  
  - **Enabled** — The processor classifies memory areas.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  

We recommend that you contact your operating system vendor to make sure your operating system supports this feature. |
| **Intel Virtualization Technology** | Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:  
  - **Disabled** — The processor does not permit virtualization.  
  - **Enabled** — The processor allows multiple operating systems in independent partitions.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  

**Note** If you change this option, you must power cycle the server before the setting takes effect. |
| **Hardware Prefetcher**     | Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following:  
  - **Disabled** — The hardware prefetcher is not used.  
  - **Enabled** — The processor uses the hardware prefetcher when cache issues are detected.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  

**Note** CPU Performance must be set to Custom in order to specify this value. For any value other than Custom, this option is overridden by the setting in the selected CPU performance profile. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
</table>
| **Adjacent Cache Line Prefetcher** | Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following:  
  • Disabled — The processor only fetches the required line.  
  • Enabled — The processor fetches both the required line and its paired line.  
  • Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. | CPU Performance must be set to Custom in order to specify this value. For any value other than Custom, this option is overridden by the setting in the selected CPU performance profile. |
| **DCU Streamer Prefetch**        | Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:  
  • Disabled — The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines.  
  • Enabled — The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.  
  • Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |                                                                         |
| **DCU IP Prefetcher**            | Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:  
  • Disabled — The processor does not preload any cache data.  
  • Enabled — The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.  
  • Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |                                                                         |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| KTI Prefetch drop-down list | KTIprefetchismechanismtogettheprojection started early on a DDR bus. This can be one of the following:  
  - **Disabled** — The processor does not preload any cache data.  
  - **Enabled** — The KTI prefetcher preloads the L1 cache with the data it determines to be the most relevant.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| LLC Prefetch drop-down list | Whether the processor uses the LLC Prefetch mechanism to fetch the date into the LLC. This can be one of the following:  
  - **Disabled** — The processor does not preload any cache data.  
  - **Enabled** — The LLC prefetcher preloads the L1 cache with the data it determines to be the most relevant.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| XPT Prefetch drop-down list | Whether XPT prefetch is used to enable a read request sent to the last level cache to issue a copy of that request to the memory controller prefetcher. This can be one of the following:  
  - **Disabled** — The CPU does not use the XPT Prefetch option.  
  - **Enabled** — The CPU enables the XPT prefetcher option.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Direct Cache Access      | Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following:  
  - **Auto** — The CPU determines how to place data from I/O devices into the processor cache.  
  - **Disabled** — Data from I/O devices is not placed directly into the processor cache.  
  - **Enabled** — Data from I/O devices is placed directly into the processor cache.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor C State</td>
<td>Whether the system can enter a power savings mode during idle periods. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The system remains in a high-performance state even when idle.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The system can reduce power to system components such as the DIMMs and CPUs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td>We recommend that you contact your operating system vendor to make sure your operating system supports this feature.</td>
</tr>
</tbody>
</table>

| Processor C1E       | Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server. This can be one of the following:                              |
|                     | • **Disabled**—The CPU continues to run at its maximum frequency in the C1 state.                                                                                                |
|                     | • **Enabled**—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state.                                                                                      |
|                     | • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.                                                                               |

| Processor C3 Report  | Whether the processor sends the C3 report to the operating system. This can be one of the following:                                                                                                        |
|                     | • **Enabled**—The processor sends the C3 report to the OS.                                                                                                                                               |
|                     | • **Disabled**—The processor does not send the C3 report.                                                                                                                                               |
|                     | • **ACPI C2**—The processor sends the C3 report using the advanced configuration and power interface (ACPI) C2 format.                                                                               |
|                     | • **ACPI C3**—The processor sends the C3 report using the ACPI C3 format.                                                                                                                               |
|                     | • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.                                                                     |

On the Cisco UCS B440 Server, the BIOS Setup menu uses enabled and disabled for these options. If you specify acpi-c2 or acpi-c3, the server sets the BIOS value for that option to enabled.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor C6 Report</td>
<td>Whether the processor sends the C6 report to the operating system. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The processor does not send the C6 report.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—The processor sends the C6 report.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Processor C7 Report</td>
<td>Whether the processor sends the C7 report to the operating system. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• C7—The processor sends the report using the C7 format.</td>
</tr>
<tr>
<td></td>
<td>• C7s—The processor sends the report using the C7s format.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The processor does not send the C7 report.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—The processor sends the C7 report.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Processor CMCI drop-down list</td>
<td>Enables CMCI generation. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The processor disables CMCI.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—The processor enables CMCI.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CPU Performance</td>
<td>Sets the CPU performance profile for the server. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Custom —</td>
</tr>
<tr>
<td></td>
<td>• Enterprise—For M3 and higher servers, all prefetchers and data reuse are enabled. For M1 and M2 servers, data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled.</td>
</tr>
<tr>
<td></td>
<td>• High Throughput—Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled.</td>
</tr>
<tr>
<td></td>
<td>• HPC—All prefetchers are enabled and data reuse is disabled. This setting is also known as high-performance computing.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Max Variable MTRR Setting</td>
<td>Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Auto Max—BIOS uses the default value for the processor.</td>
</tr>
<tr>
<td></td>
<td>• 8—BIOS uses the number specified for the variable MTRR.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Local X2 APIC</td>
<td>Allows you to set the type of Application Policy Infrastructure Controller (APIC) architecture. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Processor disables Local X2 APIC.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Processor enables Local X2 APIC.</td>
</tr>
<tr>
<td></td>
<td>• XAPIC—Uses the standard xAPIC architecture.</td>
</tr>
<tr>
<td></td>
<td>• X2APIC—Uses the enhanced x2APIC architecture to support 32 bit addressability of processors.</td>
</tr>
<tr>
<td></td>
<td>• AUTO—Automatically uses the xAPIC architecture that is detected.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
### Processor BIOS Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Technology</td>
<td>Enables you to configure the CPU power management settings for the following options:</td>
</tr>
<tr>
<td></td>
<td>• Enhanced Intel Speedstep Technology</td>
</tr>
<tr>
<td></td>
<td>• Intel Turbo Boost Technology</td>
</tr>
<tr>
<td></td>
<td>• Processor Power State C6</td>
</tr>
</tbody>
</table>

Power Technology can be one of the following:

• **Disabled** — The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored.

• **Energy Efficient** — The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.

• **Performance** — The server automatically optimizes the performance for the BIOS parameters mentioned above.

• **Custom** — The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters.

• **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
### Energy Performance

Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following:

- **Performance** — The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power.

- **Balanced Performance** — The server provides all server components with enough power to keep a balance between performance and power.

- **Balanced Energy** — The server provides all server components with enough power to keep a balance between performance and power.

- **Energy Efficient** — The server provides all server components with less power to keep reduce power consumption.

- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

**Note** Power Technology must be set to Custom or the server ignores the setting for this parameter.

### Frequency Floor Override

Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:

- **Disabled** — The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance.

- **Enabled** — The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
### Processor BIOS Settings

#### P STATE Coordination

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>• HW ALL</strong>—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package).**</td>
<td></td>
</tr>
<tr>
<td><strong>• SW ALL</strong>—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors.**</td>
<td></td>
</tr>
<tr>
<td><strong>• SW ANY</strong>—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain.**</td>
<td></td>
</tr>
<tr>
<td><strong>• Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.**</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  
*Power Technology* must be set to *Custom* or the server ignores the setting for this parameter.

#### DRAM Clock Throttling

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>• Auto</strong>—CPU determines the DRAM Clock Throttling settings.**</td>
<td></td>
</tr>
<tr>
<td><strong>• Balanced</strong>—DRAM clock throttling is reduced, providing a balance between performance and power.**</td>
<td></td>
</tr>
<tr>
<td><strong>• Performance</strong>—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power.**</td>
<td></td>
</tr>
<tr>
<td><strong>• Energy Efficient</strong>—DRAM clock throttling is increased to improve energy efficiency.**</td>
<td></td>
</tr>
<tr>
<td><strong>• Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.**</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Channel Interleaving</strong></td>
<td>Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU determines what interleaving is done.</td>
</tr>
<tr>
<td></td>
<td>• 1 Way—</td>
</tr>
<tr>
<td></td>
<td>• 2 Way</td>
</tr>
<tr>
<td></td>
<td>• 3 Way</td>
</tr>
<tr>
<td></td>
<td>• 4-way—The maximum amount of channel interleaving is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Rank Interleaving</strong></td>
<td>Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU determines what interleaving is done.</td>
</tr>
<tr>
<td></td>
<td>• 1 Way—</td>
</tr>
<tr>
<td></td>
<td>• 2 Way</td>
</tr>
<tr>
<td></td>
<td>• 4-way</td>
</tr>
<tr>
<td></td>
<td>• 8 Way—The maximum amount of rank interleaving is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Sub NUMA Clustering</strong> drop-down list</td>
<td>Whether the CPU supports sub NUMA clustering, in which the tag directory and the memory channel are always in the same region. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Sub NUMA clustering does not occur.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Sub NUMA clustering occurs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IMC Interleave</td>
<td>This BIOS option controls the interleaving between the Integrated Memory Controllers (IMCs).</td>
</tr>
<tr>
<td></td>
<td>• <strong>1-way Interleave</strong> — There is no interleaving.</td>
</tr>
<tr>
<td></td>
<td>• <strong>2-way Interleave</strong> — Addresses are interleaved between the two IMCs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> — CPU determines the IMC Interleaving mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Memory Interleaving</td>
<td>Whether the CPU interleaves the physical memory so that the memory can be accessed while another is being refreshed. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>2 Way Node Interleave</strong> —</td>
</tr>
<tr>
<td></td>
<td>• <strong>4 Way Node Interleave</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Numa - 1 Way Node Interleave</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>8 Way interleaving Inter Socket</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Demand Scrub</td>
<td>Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — Single bit memory errors are not corrected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Patrol Scrub       | Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:  
|                    | • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address.  
|                    | • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.  
|                    | • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Altitude           | The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:  
|                    | • **Auto**—The CPU determines the physical elevation.  
|                    | • **300 M**—The server is approximately 300 meters above sea level.  
|                    | • **900 M**—The server is approximately 900 meters above sea level.  
|                    | • **1500 M**—The server is approximately 1500 meters above sea level.  
|                    | • **3000 M**—The server is approximately 3000 meters above sea level.  
<p>|                    | • <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package C State Limit</td>
<td>The amount of power available to the server components when they are idle. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> — The CPU determines the physical elevation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Limit</strong> — The server may enter any available C state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C0</strong> — The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C1</strong> — When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C3</strong> — When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C6</strong> — When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C2</strong> — When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C7</strong> — When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>C7s</strong> — When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves more power than C7, but it also requires the longest time for the server to return to high performance mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
### Description

**CPU Hardware Power Management**

Enables processor Hardware Power Management (HWPM). This can be one of the following:

- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
- **Disabled** — HWPM is disabled.
- **HWPM Native Mode** — HWPM native mode is enabled.
- **HWPM OOB Mode** — HWPM Out-Of-Box mode is enabled.
- **Native Mode with no Legacy** (only GUI)

**Energy Performance Tuning**

Determines if the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS.

- **BIOS**
- **OS**
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

**Workload Configuration**

This feature allows for workload optimization. The options are Balanced and I/O Sensitive:

- **Balanced**
- **IO Sensitive**
- **NUMA** — (Only GUI)
- **UMA** — (Only GUI)
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Cisco recommends using Balanced.

**Core Performance Boost**

Whether the AMD processor increases its frequency on some cores when it is idle or not being used much. This can be one of the following:

- **Auto** — The CPU automatically determines how to boost performance.
- **Disabled** — Core performance boost is disabled.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global C-state Control</strong> drop-down list</td>
<td>Whether the AMD processors control IO-based C-state generation and DF C-states This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU automatically determines how to control IO-based C-state generation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Global C-state control is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Global C-state control is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>

| L1 Stream HW Prefetcher drop-down list | Whether the processor allows the AMD hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L1 cache when necessary. This can be one of the following: |
|                                       | • **Auto**—The CPU determines how to place data from I/O devices into the processor cache.                                                   |
|                                       | • **Disabled**—The hardware prefetcher is not used.                                                                                         |
|                                       | • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.                                                     |
|                                       | • **Platform Default** —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.           |

<p>| L2 Stream HW Prefetcher drop-down list | Whether the processor allows the AMD hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L2 cache when necessary. This can be one of the following: |
|                                       | • <strong>Auto</strong>—The CPU determines how to place data from I/O devices into the processor cache.                                                   |
|                                       | • <strong>Disabled</strong>—The hardware prefetcher is not used.                                                                                         |
|                                       | • <strong>Enabled</strong>—The processor uses the hardware prefetcher when cache issues are detected.                                                     |
|                                       | • <strong>Platform Default</strong> —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.           |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **AMD Memory Interleaving** drop-down list | Whether the AMD CPU interleaves the physical memory so that the memory can be accessed while another is being refreshed. This controls fabric level memory interleaving. Channel, die and socket have requirements based on memory populations and will be ignored if the memory does not support the selected option. This can be one of the following:  
  - **Auto**—The CPU determines how to interleave memory.  
  - **Channel**—Interleaves the physical address space over multiple channels, as opposed to each channel owning single consecutive address spaces.  
  - **Die**—Interleaves the physical address space over multiple dies, as opposed to each die owning single consecutive address spaces.  
  - **None**—Consecutive memory blocks are accessed from the same physical memory.  
  - **Socket**—Interleaves the physical address space over multiple sockets, as opposed to each socket owning single consecutive address spaces.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| **AMD Memory Interleaving Size** drop-down list | Determines the size of the memory blocks to be interleaved. It also determines the starting address of the interleave (bit 8, 9, 10 or 11). This can be one of the following:  
  - **1 KB**  
  - **2 KB**  
  - **256 Bytes**  
  - **512 Bytes**  
  - **Auto**—The CPU determines the size of the memory block.  
  - **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chipselect Interleaving</strong></td>
<td>Whether memory blocks across the DRAM chip selects for node 0 are interleaved. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU automatically determines how to interleave chip selects.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Chip selects are not interleaved within the memory controller.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Bank Group Swap</strong></td>
<td>Determines how physical addresses are assigned to applications. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU automatically determines how to assign physical addresses to applications.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Bank group swap is not used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Bank group swap is used to improve the performance of applications.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Determinism Slider</strong></td>
<td>Allows AMD processors to determine how to operate. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU automatically uses default power determinism settings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Performance</strong>—Processor operates at the best performance in a consistent manner.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Power</strong>—Processor operates at the maximum allowable performance on a per die basis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>IOMMU drop-down list</strong></td>
<td>Input Output Memory Management Unit (IOMMU) allows AMD processors to map virtual addresses to physical addresses. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> — The CPU determines how map these addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — IOMMU is not used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — Address mapping takes place through the IOMMU.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Downcore control drop-down list</strong></td>
<td>Allows AMD processors to disable cores and, thus, select how many cores to enable. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>FOUR (2+2)</strong> — Two cores enabled on each CPU complex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>FOUR (4+0)</strong> — Four cores enabled on one CPU complex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SIX (3+3)</strong> — Three cores enabled on each CPU complex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>THREE (3+0)</strong> — Three cores enabled on one CPU complex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TWO (1+1)</strong> — Two cores enabled on each CPU complex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TWO (2+0)</strong> — Two cores enabled on one CPU complex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> — The CPU determines how many cores need to be enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>SVM Mode drop-down list</strong></td>
<td>Whether the processor uses AMD Secure Virtual Machine Technology. This can be one of the following: This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — The processor does not use SVM Technology.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses SVM Technology.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>SMT Mode</strong> drop-down list</td>
<td>Whether the processor uses AMD Simultaneous MultiThreading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> — The processor allows for the parallel execution of multiple threads.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> — The processor does not permit multithreading.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>SMEE</strong> drop-down list</td>
<td>Whether the processor uses the Secure Memory Encryption Enable (SMEE) function, which provides memory encryption support. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — The processor does not use the SMEE function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses the SMEE function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>DCPMM Firmware Downgrade</strong></td>
<td>Whether the processor uses the DCPMM firmware downgrade function. This can be one of the following:</td>
</tr>
<tr>
<td>drop-down list</td>
<td>• <strong>Disabled</strong> — The processor does not use the DCPMM firmware downgrade function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses the DCPMM firmware downgrade function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Intel Speed Select</strong> drop-down list</td>
<td>How the Intel Speed Select function is configured. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Base</strong> — The processor uses Base.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Config 1</strong> — The processor uses Config 1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Config 2</strong> — The processor uses Config 2.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
## Intel Directed I/O BIOS Settings

The following table lists the Intel Directed I/O BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intel VT for directed I/O</strong></td>
<td>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — The processor does not use virtualization technology.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses virtualization technology.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This option must be enabled if you want to change any of the other Intel Directed I/O BIOS settings.</td>
</tr>
<tr>
<td><strong>Intel VTD interrupt Remapping</strong></td>
<td>Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — The processor does not support remapping.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses VT-d Interrupt Remapping as required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Intel VTD coherency support</strong></td>
<td>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — The processor does not support coherency.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses VT-d Coherency as required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Intel VTD ATS support</strong></td>
<td>Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — The processor does not support ATS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong> — The processor uses VT-d ATS as required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong> — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following:

- **Disabled**—The processor does not support pass-through DMA.
- **Enabled**—The processor uses VT-d Pass-through DMA as required.
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### RAS Memory BIOS Settings

The following table lists the RAS memory BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intel VTD pass through DMA support</strong></td>
<td>Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The processor does not support pass-through DMA.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor uses VT-d Pass-through DMA as required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory RAS configuration</strong></td>
<td>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum Performance</strong>—System performance is optimized.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mirroring</strong>—System reliability is optimized by using half the system memory as backup. This mode is used for UCS M4 and lower blade servers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Lockstep</strong>—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sparing</strong>—System reliability is optimized by holding memory in reserve so that it can be used in case other DIMMs fail. This mode provides some memory redundancy, but does not provide as much redundancy as mirroring.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ADDDC Sparing</strong>—System reliability is optimized by holding memory in reserve so that it can be used in case other DIMMs fail. This mode provides some memory redundancy, but does not provide as much redundancy as mirroring.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NUMA optimized</td>
<td>Whether the BIOS supports NUMA. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The BIOS does not support NUMA.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Mirroring Mode</td>
<td>Memory mirroring enhances system reliability by keeping two identical data images in memory.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if you choose the mirroring option for Memory RAS Config. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Inter-Socket — Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets.</td>
</tr>
<tr>
<td></td>
<td>• Intra-Socket — One IMC is mirrored with another IMC in the same socket.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Sparing Mode</td>
<td>Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if you choose sparing option for Memory RAS Config. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• DIMM Sparing — One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM.</td>
</tr>
<tr>
<td></td>
<td>• Rank Sparing — A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LV DDR Mode</td>
<td>Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <em>Auto</em>—The CPU determines whether to prioritize low voltage or high frequency memory operations.</td>
</tr>
<tr>
<td></td>
<td>• <em>Power Saving Mode</em>—The system prioritizes low voltage memory operations over high frequency memory operations.</td>
</tr>
<tr>
<td></td>
<td>This mode may lower memory frequency in order to keep the voltage low.</td>
</tr>
<tr>
<td></td>
<td>• <em>Performance Mode</em>—The system prioritizes high frequency operations over low voltage operations.</td>
</tr>
<tr>
<td></td>
<td>• <em>Platform Default</em>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>DRAM Refresh Rate</td>
<td>The refresh interval rate for internal memory. This can be one of the following:</td>
</tr>
<tr>
<td>set dram-refresh-rate-config</td>
<td></td>
</tr>
<tr>
<td>dram-refresh</td>
<td>• 1x</td>
</tr>
<tr>
<td></td>
<td>• 2x</td>
</tr>
<tr>
<td></td>
<td>• 3x</td>
</tr>
<tr>
<td></td>
<td>• 4x</td>
</tr>
<tr>
<td></td>
<td>• <em>Auto</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Platform Default</em>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>DDR3 Voltage Selection</td>
<td>The voltage to be used by the dual-voltage RAM. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• DDR3-1500mv</td>
</tr>
<tr>
<td></td>
<td>• DDR3-1350mv</td>
</tr>
<tr>
<td></td>
<td>• <em>Platform Default</em>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>

**Serial Port BIOS Settings**

The following table lists the serial port BIOS settings that you can configure through a BIOS policy or the default BIOS settings:
### USB BIOS Settings

The following table lists the USB BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial port A enable</td>
<td>Whether serial port A is enabled or disabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The serial port is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The serial port is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>

### Make Device Non Bootable

Whether the server can boot from a USB device. This can be one of the following:

- **Disabled**—The server can boot from a USB device.
- **Enabled**—The server cannot boot from a USB device.
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### Legacy USB Support

Whether the system supports legacy USB devices. This can be one of the following:

- **Disabled**—USB devices are only available to EFI applications.
- **Enabled**—Legacy USB support is always available.
- **Auto**—Disables legacy USB support if no USB devices are connected.
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
### USB BIOS Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Idle Power Optimizing Setting</td>
<td>Whether the USB Idle Power Optimizing setting is used to reduce USB EHCI idle power consumption. Depending upon the value you choose, this setting can have an impact on performance. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>high-performance</strong>—The USB System Idle Power Optimizing setting is disabled, because optimal performance is preferred over power savings.</td>
</tr>
<tr>
<td></td>
<td>Selecting this option can significantly improve performance. We recommend you select this option unless your site has server power restrictions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Lower Idle Power</strong>—The USB System Idle Power Optimizing setting is enabled, because power savings are preferred over optimal performance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>USB Front Panel Access Lock</td>
<td>USB front panel access lock is configured to enable or disable the front panel access to USB ports. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Port 60/64 Emulation</td>
<td>Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—60h/64 emulation is not supported.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—60h/64 emulation is supported.</td>
</tr>
<tr>
<td></td>
<td>You should select this option if you are using a non-USB aware operating system on the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USB Port Front</td>
<td>Whether the front panel USB devices are enabled or disabled. This can be</td>
</tr>
<tr>
<td></td>
<td>one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Disables the front panel USB ports. Devices connected to</td>
</tr>
<tr>
<td></td>
<td>these ports are not detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Enables the front panel USB ports. Devices connected to these</td>
</tr>
<tr>
<td></td>
<td>ports are detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>USB Port Internal</td>
<td>Whether the internal USB devices are enabled or disabled. This can be one</td>
</tr>
<tr>
<td></td>
<td>of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Disables the internal USB ports. Devices connected to these</td>
</tr>
<tr>
<td></td>
<td>ports are not detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Enables the internal USB ports. Devices connected to these</td>
</tr>
<tr>
<td></td>
<td>ports are detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>USB Port KVM</td>
<td>Whether the KVM ports are enabled or disabled. This can be one of the</td>
</tr>
<tr>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Disables the KVM keyboard and/or mouse devices. Keyboard</td>
</tr>
<tr>
<td></td>
<td>and/or mouse will not work in the KVM window.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Enables the KVM keyboard and/or mouse devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>USB Port Rear</strong></td>
<td>Whether the rear panel USB devices are enabled or disabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>USB Port SD Card</strong></td>
<td>Whether the SD card drives are enabled or disabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Enables the SD card drives.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>USB Port VMedia</strong></td>
<td>Whether the virtual media devices are enabled or disabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Disables the vMedia devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Enables the vMedia devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>All USB Devices</strong></td>
<td>Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—All USB devices are disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—All USB devices are enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
The following table lists the PCI configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xHCI Mode</td>
<td>Whether xHCI mode is enabled or disabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—xHCI mode is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—xHCI mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>

## PCI Configuration BIOS Settings

The following table lists the PCI configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum memory below 4GB</td>
<td>Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Does not maximize memory usage. Choose this option for all operating systems with PAE support.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Maximizes memory usage below 4GB for an operating system without PAE support.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Memory mapped IO above 4GB</td>
<td>Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Does not map I/O of 64-bit PCI devices to 4GB or greater address space.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Maps I/O of 64-bit PCI devices to 4GB or greater address space.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>VGA Priority</strong></td>
<td>Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Onboard</strong>—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Offboard</strong>—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Onboard VGA Disabled</strong>—Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The vKVM does not function when the onboard VGA is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only onboard VGA devices are supported with Cisco UCS B-Series servers.</td>
</tr>
<tr>
<td><strong>ASPM Support</strong></td>
<td>Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—ASPM support is disabled in the BIOS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The CPU determines the power state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ForceL0</strong>—Force all links to L0 standby (L0s) state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>BME DMA Mitigation Support</strong></td>
<td>Allows you to disable the PCI BME bit to mitigate the threat from an unauthorized external DMA. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—PCI BME bit is disabled in the BIOS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—PCI BME bit is enabled in the BIOS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
QPI BIOS Settings

The following table lists the QPI BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QPI Link Frequency Select</td>
<td>The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 6.4 GT/s</td>
</tr>
<tr>
<td></td>
<td>• 7.2 GT/s</td>
</tr>
<tr>
<td></td>
<td>• 8.0 GT/s</td>
</tr>
<tr>
<td></td>
<td>• 9.6 GT/s</td>
</tr>
<tr>
<td></td>
<td>• Auto—The CPU determines the QPI link frequency.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>QPI Snoop Mode</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Home Snoop—The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions.</td>
</tr>
<tr>
<td></td>
<td>• Cluster On Die—This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads.</td>
</tr>
<tr>
<td></td>
<td>• Home Directory Snoop with OSB</td>
</tr>
<tr>
<td></td>
<td>• Early Snoop—The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized.</td>
</tr>
<tr>
<td></td>
<td>• Auto — The CPU determines the QPI Snoop mode.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>

LOM and PCIe Slots BIOS Settings

The following table lists the USB BIOS settings that you can configure through a BIOS policy or the default BIOS settings:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCIe Slot SAS OptionROM</strong></td>
<td>Whether Option ROM is available on the SAS port. This can be one of the</td>
</tr>
<tr>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>PCIe Slot n Link Speed</strong></td>
<td>This option allows you to restrict the maximum speed of an adapter card</td>
</tr>
<tr>
<td></td>
<td>installed in PCIe slot ( n ). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Gen 1 — 2.5GT/s (gigatransfers per second) is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• Gen 2 — 5GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• Gen 3 — 8GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• Auto — The maximum speed is set automatically.</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The maximum speed is not restricted.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>PCIe Slot n OptionROM</strong></td>
<td>Whether Option ROM is available on the port. This can be one of the</td>
</tr>
<tr>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>PCIe Slot HBA OptionROM</strong></td>
<td>Whether Option ROM is available on the HBA port. This can be one of the</td>
</tr>
<tr>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained</td>
</tr>
<tr>
<td></td>
<td>in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PCIe Slot MLOM OptionROM</td>
<td>Whether Option ROM is available on the MLOM port. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>PCIe Slot N× OptionROM</td>
<td>Whether Option ROM is available on the port. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>PCIe 10G LOM 2 Link</td>
<td>Whether Option ROM is available on the 10G LOM port. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>PCI ROM CLP</td>
<td>PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SIOC1 Option ROM</td>
<td>Whether the server can use Option ROM present in System IO Controller 1 (SIOC1). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>SIOC2 Option ROM</td>
<td>Whether the server can use Option ROM present in System IO Controller 2 (SIOC2). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>SBMEZZ1 Option ROM</td>
<td>Whether the server can use Option ROM present in SBMezz1 controller. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>IOESlot1 Option ROM</td>
<td>Whether option ROM is enabled on the IOE slot 1. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled — The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• UEFI Only — The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• Legacy Only — The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IOEMEZZ 1 OptionROM</td>
<td>Whether option ROM is enabled on the IOE Mezz1. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>IOE Slot2 Option ROM</td>
<td>Whether option ROM is enabled on the IOE slot 2. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>IO ENVME1 Option ROM</td>
<td>Whether option ROM is enabled on the IOE NVMe1. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>IO ENVME2 Option ROM</td>
<td>Whether option ROM is enabled on the IOE NVMe2. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **SBNVME1 Option ROM** | Whether the server can use Option ROM present in SBNVMe1 controller. This can be one of the following:  
- **Disabled**—The expansion slot is not available.  
- **Enabled**—The expansion slot is available.  
- **UEFI Only**—The expansion slot is available for UEFI only.  
- **Legacy Only**—The expansion slot is available for legacy only.  
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| **PCIe Slot MRAID OptionROM drop-down list** | Whether Option ROM is available on the MRAID port. This can be one of the following:  
- **Disabled**—The expansion slot is not available.  
- **Enabled**—The expansion slot is available.  
- **UEFI Only**—The expansion slot is available for UEFI only.  
- **Legacy Only**—The expansion slot is available for legacy only.  
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| **PCIe Slot RAID OptionROM** | Whether Option ROM is available on the RAID port. This can be one of the following:  
- **Disabled**—The expansion slot is not available.  
- **Enabled**—The expansion slot is available.  
- **UEFI Only**—The expansion slot is available for UEFI only.  
- **Legacy Only**—The expansion slot is available for legacy only.  
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| **PCIe Slot Rear Nvme OptionRom** | Whether Option ROM is available on the Rear NVME port. This can be one of the following:  
- **Disabled**—The expansion slot is not available.  
- **Enabled**—The expansion slot is available.  
- **UEFI Only**—The expansion slot is available for UEFI only.  
- **Legacy Only**—The expansion slot is available for legacy only.  
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rear NVME1 Link Speed</td>
<td>This option allows you to restrict the maximum speed of an NVME card installed in the rear PCIe slot 1. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 1</strong>—2.5GT/s (gigatransfers per second) is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 2</strong>—5GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 3</strong>—8GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The maximum speed is set automatically.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The maximum speed is not restricted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Rear NVME2 Link Speed</td>
<td>This option allows you to restrict the maximum speed of an NVME card installed in the rear PCIe slot 2. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 1</strong>—2.5GT/s (gigatransfers per second) is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 2</strong>—5GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 3</strong>—8GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The maximum speed is set automatically.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The maximum speed is not restricted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Front NVME1 Link Speed</td>
<td>This option allows you to restrict the maximum speed of an NVME card installed in the front PCIe slot 1. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 1</strong>—2.5GT/s (gigatransfers per second) is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 2</strong>—5GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gen 3</strong>—8GT/s is the maximum speed allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The maximum speed is set automatically.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The maximum speed is not restricted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Front NVME2 Link Speed | This option allows you to restrict the maximum speed of an NVME card installed in the front PCIe slot 2. This can be one of the following:  
  - Gen 1—2.5GT/s (gigatransfers per second) is the maximum speed allowed.  
  - Gen 2—5GT/s is the maximum speed allowed.  
  - Gen 3—8GT/s is the maximum speed allowed.  
  - Auto—The maximum speed is set automatically.  
  - Disabled—The maximum speed is not restricted.  
  - Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| HBA Link Speed      | This option allows you to restrict the maximum speed of an HBA card. This can be one of the following:  
  - Gen 1—2.5GT/s (gigatransfers per second) is the maximum speed allowed.  
  - Gen 2—5GT/s is the maximum speed allowed.  
  - Gen 3—8GT/s is the maximum speed allowed.  
  - Auto—The maximum speed is set automatically.  
  - Disabled—The maximum speed is not restricted.  
  - Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| MLOM Link Speed     | This option allows you to restrict the maximum speed of an MLOM adapter. This can be one of the following:  
  - Gen 1—2.5GT/s (gigatransfers per second) is the maximum speed allowed.  
  - Gen 2—5GT/s is the maximum speed allowed.  
  - Gen 3—8GT/s is the maximum speed allowed.  
  - Auto—The maximum speed is set automatically.  
  - Disabled—The maximum speed is not restricted.  
  - Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRAID Link Speed</td>
<td>This option allows you to restrict the maximum speed of MRAID. This can be one of the following:&lt;br&gt;&lt;br&gt;• Gen 1—2.5GT/s (gigatransfers per second) is the maximum speed allowed.&lt;br&gt;• Gen 2—5GT/s is the maximum speed allowed.&lt;br&gt;• Gen 3—8GT/s is the maximum speed allowed.&lt;br&gt;• Auto—The maximum speed is set automatically.&lt;br&gt;• Disabled—The maximum speed is not restricted.&lt;br&gt;• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>RAID Link Speed</td>
<td>This option allows you to restrict the maximum speed of RAID. This can be one of the following:&lt;br&gt;&lt;br&gt;• Gen 1—2.5GT/s (gigatransfers per second) is the maximum speed allowed.&lt;br&gt;• Gen 2—5GT/s is the maximum speed allowed.&lt;br&gt;• Gen 3—8GT/s is the maximum speed allowed.&lt;br&gt;• Auto—The maximum speed is set automatically.&lt;br&gt;• Disabled—The maximum speed is not restricted.&lt;br&gt;• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>All Onboard LOM</td>
<td>Whether all onboard LOM ports are enabled or disabled. This can be one of the following:&lt;br&gt;&lt;br&gt;• Enabled—All onboard LOM are enabled.&lt;br&gt;• Disabled—All onboard LOM are disabled.&lt;br&gt;• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>LOM Port 1 OptionRom</td>
<td>Whether Option ROM is available on the LOM port 1. This can be one of the following:&lt;br&gt;&lt;br&gt;• Disabled—The expansion slot is not available.&lt;br&gt;• Enabled—The expansion slot is available.&lt;br&gt;• UEFI Only—The expansion slot is available for UEFI only.&lt;br&gt;• Legacy Only—The expansion slot is available for legacy only.&lt;br&gt;• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>LOM Port 2 OptionRom</strong></td>
<td>Whether Option ROM is available on the LOM port 2. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>Slot n State</strong></td>
<td>The state of the adapter card installed in PCIe slot n. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The expansion slot is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The expansion slot is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UEFI Only</strong>—The expansion slot is available for UEFI only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Legacy Only</strong>—The expansion slot is available for legacy only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>CDN Support for LOMs</strong></td>
<td>Whether the Ethernet Networking Identifier naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—OS Ethernet Network Identifier is named in a consistent device naming (CDN) convention according to the physical LAN on Motherboard(LOM) port numbering; LOM Port 0, LOM Port 1 and so on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. By default, CDN option is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td><strong>VMD Enable</strong></td>
<td>Whether NVMe SSDs that are connected to the PCIe bus can be hot swapped. It also standardizes the LED status light on these drives. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Hot swap of NVMe SSDs that are connected to the PCIe bus is allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Hot swap of NVMe SSDs that are connected to the PCIe bus is not allowed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
Graphics Configuration BIOS Settings

The following tables list the graphics configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Graphics</td>
<td>Enables integrated graphics. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td>- —Integrated graphic is enabled.</td>
</tr>
<tr>
<td></td>
<td>- —Integrated graphics is disabled.</td>
</tr>
<tr>
<td>Integrated Graphics Aperture Size</td>
<td>Allows you to set the size of mapped memory for the integrated graphics controller. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Onboard Graphics</td>
<td>Enables onboard graphics (KVM). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td>- —Onboard graphics is enabled.</td>
</tr>
<tr>
<td></td>
<td>- —Onboard graphics is disabled.</td>
</tr>
</tbody>
</table>

Boot Options BIOS Settings

The following table lists the boot options BIOS settings that you can configure through a BIOS policy or the default BIOS settings:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot option retry</td>
<td>Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>disabled</strong>—Waits for user input before retrying NON-EFI based boot options.</td>
</tr>
<tr>
<td></td>
<td>• <strong>enabled</strong>—Continually retries NON-EFI based boot options without waiting for user input.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>SAS RAID</td>
<td>Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>disabled</strong>—The Intel SAS Entry RAID Module is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>enabled</strong>—The Intel SAS Entry RAID Module is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>SAS RAID module</td>
<td>How the Intel SAS Entry RAID Module is configured. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>it-ir-raid</strong>—Configures the RAID module to use Intel IT/IR RAID.</td>
</tr>
<tr>
<td></td>
<td>• <strong>intel-esrtii</strong>—Configures the RAID module to use Intel Embedded Server RAID Technology II.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Onboard SCU Storage Support</td>
<td>Whether the onboard software RAID controller is available to the server. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>disabled</strong>—The software RAID controller is not available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>enabled</strong>—The software RAID controller is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
### P-SATA mode drop-down list
This option allows you to select the P-SATA mode. This can be one of the following:
- **Disabled** — P-SATA mode is disabled.
- **LSI SW RAID** — Sets both SATA and sSATA controllers to RAID mode for LSI SW RAID.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### Power On Password drop-down list
This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS. It can be one of the following:
- **Disabled** — Power On Password is disabled.
- **Enabled** — Power On Password is enabled.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### IPV6 PXE Support drop-down list
Enables or disables IPV6 support for PXE. This can be one of the following:
- **Disabled** — IPV6 PXE support is not available.
- **Enabled** — IPV6 PXE support is always available.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

---

**Note**
BIOS parameter virtualization capability in Cisco UCS Manager maps a unified set of BIOS settings in a service profile to the actual BIOS supporting parameters. However, not all BIOS setting items are applicable to every server model/platform. When you create a custom BIOS policy and have the **Boot Option Retry** selected, and when there is no bootable option available, the reboot fails on the Cisco UCS B420 M3 or Cisco UCS B420 M4 servers and Cisco UCS Manager displays this message: *Reboot and Select proper Boot device or Insert Boot Media in selected Boot device and press a key.* You must manually set a boot option after the boot path is corrected, in order to enable the servers to reboot after a power outage. For more information about BIOS default server policies and the BIOS options and their default settings, see **BIOS Policy**, on page 236 and **Server BIOS Settings**, on page 183.
Server Management BIOS Settings

The following tables list the server management BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

**General Settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assert NMI on SERR</td>
<td>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The BIOS does not generate an NMI or log an error when a SERR occurs.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable <strong>Assert NMI on PERR</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Assert NMI on PERR</td>
<td>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The BIOS does not generate an NMI or log an error when a PERR occurs.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable <strong>Assert NMI on SERR</strong> to use this setting.</td>
</tr>
</tbody>
</table>
|                     | • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Boot Watchdog Timer</td>
<td>Whether the BIOS programs the watchdog timer with a predefined timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The watchdog timer is not used to track how long the server takes to boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the predefined length of time, the CIMC resets the system and logs an error.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td>This feature requires either operating system support or Intel Management software.</td>
</tr>
<tr>
<td>OS Boot Watchdog Timer Policy</td>
<td>What action the system takes if the watchdog timer expires. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Power Off</strong>—The server is powered off if the watchdog timer expires during OS boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reset</strong>—The server is reset if the watchdog timer expires during OS boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if you enable the OS Boot Watchdog Timer.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>OS Boot Watchdog Timer Timeout</td>
<td>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>5-minutes</strong>—The watchdog timer expires 5 minutes after the OS begins to boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10-minutes</strong>—The watchdog timer expires 10 minutes after the OS begins to boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>15-minutes</strong>—The watchdog timer expires 15 minutes after the OS begins to boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>20-minutes</strong>—The watchdog timer expires 20 minutes after the OS begins to boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if you enable the OS Boot Watchdog Timer.</td>
</tr>
<tr>
<td>FRB-2 Timer</td>
<td>Whether the FRB-2 timer is used to recover the system if it hangs during POST. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The FRB-2 timer is not used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The FRB-2 timer is started during POST and used to recover the system if necessary.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
</tbody>
</table>
### Console Redirection Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console redirection</td>
<td>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—No console redirection occurs during POST.</td>
</tr>
<tr>
<td></td>
<td>• <strong>serial-port-a or COM0 or Enabled</strong>—Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>serial-port-b or COM1</strong>—Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Note</td>
<td>If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.</td>
</tr>
</tbody>
</table>

### Flow Control

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Control</td>
<td>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—No flow control is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RTS-CTS</strong>—RTS/CTS is used for flow control.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Default</strong>—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.</td>
</tr>
<tr>
<td>Note</td>
<td>This setting must match the setting on the remote terminal application.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Baud rate**  | What Baud rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:  
|                | • 9.6k—A 9600 Baud rate is used.  
|                | • 19.2k—A 19200 Baud rate is used.  
|                | • 38.4k—A 38400 Baud rate is used.  
|                | • 57.6k—A 57600 Baud rate is used.  
|                | • 115.2k—A 115200 Baud rate is used.  
|                | • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.  
| **Note**       | This setting must match the setting on the remote terminal application.  |
| **Terminal type** | What type of character formatting is used for console redirection. This can be one of the following:  
|                | • **PC-ANSI**—The PC-ANSI terminal font is used.  
|                | • **VT100**—A supported vt100 video terminal and its character set are used.  
|                | • **VT100-PLUS**—A supported vt100-plus video terminal and its character set are used.  
|                | • **VT-UTF8**—A video terminal with the UTF-8 character set is used.  
| **Note**       | This setting must match the setting on the remote terminal application.  |
### Legacy OS redirection

Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following:

- **Disabled** — The serial port enabled for console redirection is hidden from the legacy operating system.
- **Enabled** — The serial port enabled for console redirection is visible to the legacy operating system.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### Putty KeyPad

Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following:

- **VT100** — The function keys generate `ESC OP` through `ESC O[`.
- **LINUX** — Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate `ESC [A` through `ESC [[E`.
- **XTERMR6** — Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate `ESC OP` through `ESC OS`, which are the sequences produced by the top row of the keypad on Digital terminals.
- **SCO** — The function keys F1 to F12 generate `ESC [M` through `ESC [X`. The function and shift keys generate `ESC [Y` through `ESC [j`. The control and function keys generate `ESC [k` through `ESC [v`. The shift, control and function keys generate `ESC [w` through `ESC [}`.
- **ESCN** — The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as `ESC [11~` and `ESC [12~`.
- **VT400** — The function keys behave like the default mode. The top row of the numeric keypad generates `ESC OP` through `ESC OS`.
- **Platform Default** — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
### Out of Band Management drop-down list

**Name:** Out of Band Management

**Description:** Used for Windows Special Administration Control (SAC). This option allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following:

- **Disabled**—Configures the COM port 0 as a general purpose port for use with the Windows Operating System.
- **Enabled**—Configures the COM port 0 as a remote management port for Windows Emergency Management services.
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

### Redirection After BIOS POST drop-down list

- **set console-redir-config putty-function-keypad**

**Name:** Redirection After BIOS POST

**Description:** Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following:

- **Always Enable**—BIOS Legacy console redirection is active during the OS boot and run time.
- **Bootloader**—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.
- **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

---

**BIOS Policy**

The BIOS policy is a policy that automates the configuration of BIOS settings for a server or group of servers. You can create global BIOS policies available to all servers in the root organization, or you can create BIOS policies in sub-organizations that are only available to that hierarchy.

To use a BIOS policy, do the following:

1. Create the BIOS policy in Cisco UCS Manager.
2. Assign the BIOS policy to one or more service profiles.
3. Associate the service profile with a server.

During service profile association, Cisco UCS Manager modifies the BIOS settings on the server to match the configuration in the BIOS policy. If you do not create and assign a BIOS policy to a service profile, the server uses the default BIOS settings for that server platform.
Default BIOS Settings

Cisco UCS Manager includes a set of default BIOS settings for each type of server supported by Cisco UCS. The default BIOS settings are available only in the root organization and are global. Only one set of default BIOS settings can exist for each server platform supported by Cisco UCS. You can modify the default BIOS settings, but you cannot create an additional set of default BIOS settings.

Each set of default BIOS settings are designed for a particular type of supported server and are applied to all servers of that specific type which do not have a BIOS policy included in their service profiles.

Unless a Cisco UCS implementation has specific needs that are not met by the server-specific settings, we recommend that you use the default BIOS settings that are designed for each type of server in the Cisco UCS domain.

Cisco UCS Manager applies these server platform-specific BIOS settings as follows:

- The service profile associated with a server does not include a BIOS policy.
- The BIOS policy is configured with the platform-default option for a specific setting.

You can modify the default BIOS settings provided by Cisco UCS Manager. However, any changes to the default BIOS settings apply to all servers of that particular type or platform. If you want to modify the BIOS settings for only certain servers, we recommend that you use a BIOS policy.

Creating a BIOS Policy

Note

Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Procedure

1. In the Navigation pane, click Servers.
2. Expand Servers > Policies.
3. Expand the node for the organization where you want to create the policy.
   If the system does not include multitenancy, expand the root node.
4. Right-click BIOS Policies and select Create BIOS Policy.
5. On the Main page of the Create BIOS Policy wizard, enter a name for the BIOS policy in the Name field.
   This name can be between 1 and 16 alphanumerics. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
6. In the Create BIOS Policy wizard, do the following to configure the BIOS settings:
a) If you want to change a BIOS setting, click the desired radio button or make the appropriate choice from the drop-down list.

For descriptions and information about the options for each BIOS setting, see the following topics:

- **Main** page: Main BIOS Settings, on page 184
- **Processor** page: Processor BIOS Settings, on page 186
- **Intel Directed IO** page: Intel Directed I/O BIOS Settings, on page 207
- **RAS Memory** page: RAS Memory BIOS Settings, on page 208
- **Serial Port** page: Serial Port BIOS Settings, on page 210
- **USB** page: USB BIOS Settings, on page 211
- **PCI Configuration** page: PCI Configuration BIOS Settings, on page 215
- **Boot Options** page: Boot Options BIOS Settings, on page 227
- **Server Management** page: Server Management BIOS Settings, on page 230

b) Click **Next** after each page.

**Step 7**
After you configure all of the BIOS settings for the policy, click **Finish**.

---

**Modifying the BIOS Defaults**

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Unless a Cisco UCS implementation has specific needs that are not met by the server-specific settings, we recommend that you use the default BIOS settings that are designed for each type of server in the Cisco UCS domain.

**Procedure**

**Step 1**
In the **Navigation** pane, click **Servers**.

**Step 2**
Expand **Servers > Policies**.

**Step 3**
Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

**Step 4**
Expand **BIOS Defaults** and select the server model number for which you want to modify the default BIOS settings.

**Step 5**
In the **Work** pane, click the appropriate tab and then click the desired radio button or make a choice from the drop-down list to modify the default BIOS settings:

For descriptions and information about the options for each BIOS setting, see the following topics. Not all BIOS settings are available for each type of server.

- **Main** tab: Main BIOS Settings, on page 184
Step 6  Click Save Changes.

Viewing the Actual BIOS Settings for a Server

Follow this procedure to see the actual BIOS settings on a server.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Servers.
Step 3  Choose the server for which you want to view the actual BIOS settings.
Step 4  On the Work pane, click the Inventory tab.
Step 5  Click the Motherboard subtab.
Step 6  In the BIOS Settings area, click the Expand icon to the right of the heading to open that area.

Each tab in the BIOS Settings area displays the settings for that server platform. Some of the tabs contain subtabs with additional information.

trusted_platform_module

trusted_platform_module

The Trusted Platform Module (TPM) is a component that can securely store artifacts that are used to authenticate the server. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all
environments. It is a requirement for the Intel Trusted Execution Technology (TXT) security feature, which must be enabled in the BIOS settings for a server equipped with a TPM. Cisco UCS M4 and higher blade and rack-mount servers include support for TPM. TPM is enabled by default on these servers.

**Important**

- If you upgrade Cisco UCS Manager to Release 2.2(4) and higher, TPM is enabled.
- When TPM is enabled and you downgrade Cisco UCS Manager from Release 2.2(4), TPM is disabled.

**Intel Trusted Execution Technology**

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, invisible 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. Cisco UCS M4 and higher blade and rack-mount servers include support for TXT. TXT is disabled by default on these servers.

TXT can be enabled only after TPM, Intel Virtualization technology (VT) and Intel Virtualization Technology for Directed I/O (VT-d) are enabled. When you only enable TXT, it also implicitly enables TPM, VT, and VT-d.

**Configuring Trusted Platform**

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Policies.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization where you want to configure TPM.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand BIOS Policies and select the BIOS policy for which you want to configure TPM.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Work pane, click the Advanced tab.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click the Trusted Platform subtab.</td>
</tr>
<tr>
<td>Step 7</td>
<td>To configure TPM, click one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Option</strong></td>
</tr>
<tr>
<td></td>
<td>disabled</td>
</tr>
<tr>
<td></td>
<td>enabled</td>
</tr>
<tr>
<td></td>
<td>Platform Default</td>
</tr>
</tbody>
</table>

| Step 8 | To configure TXT, click one of the following: |
|        | **Option** | **Description** |
|        | disabled   | Disables TXT |
**Step 9**  
Click **Save Changes**.

---

### Configuring Trusted Platform

#### Procedure

**Step 1**  
In the **Navigation** pane, click **Servers**.

**Step 2**  
Expand **Servers > Policies**.

**Step 3**  
Expand the node for the organization where you want to configure TPM.

**Step 4**  
Expand **BIOS Policies** and select the BIOS policy for which you want to configure TPM.

**Step 5**  
In the **Work pane**, click the **Advanced** tab.

**Step 6**  
Click the **Trusted Platform** subtab.

**Step 7**  
To configure TPM, click one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disables TPM</td>
</tr>
<tr>
<td>enable</td>
<td>Enables TPM</td>
</tr>
<tr>
<td>Platform Default</td>
<td>Enables TPM</td>
</tr>
</tbody>
</table>

**Step 8**  
To configure TXT, click one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disables TXT</td>
</tr>
<tr>
<td>enable</td>
<td>Enables TXT</td>
</tr>
<tr>
<td>Platform Default</td>
<td>Disables TXT</td>
</tr>
</tbody>
</table>

**Step 9**  
Click **Save Changes**.
Viewing TPM Properties

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  Expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
Step 3  Choose the server for which you want to view the TPM settings.
Step 4  On the Work pane, click the Inventory tab.
Step 5  Click the Motherboard subtab.

Consistent Device Naming

When there is no mechanism for the Operating System to label Ethernet interfaces in a consistent manner, it becomes difficult to manage network connections with server configuration changes. Consistent Device Naming (CDN), introduced in Cisco UCS Manager Release 2.2(4), allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more persistent when adapter or other configuration changes are made.

To configure CDN for a vNIC, do the following:
- Enable consistent device naming in the BIOS policy.
- Associate the BIOS policy with a service profile.
- Configure consistent naming for a vNIC.

Guidelines and Limitations for Consistent Device Naming

- CDN is supported on the following Operating Systems:
  - Windows 2012 R2
  - Windows 2016
  - Red Hat Enterprise Linux (RHEL) 6.x and 7.x
- Consistent device naming (CDN) is supported on all M3 and higher blade and rack-mount servers.
- BIOS and adapter firmware must be part of the Release 2.2(4) or higher bundle to support CDN.
- In Cisco UCS Manager Release 3.1 and later releases, CDN is supported on the following adapters:
  - Cisco UCS VIC 1385 (UCSC-PCIE-C40Q-03)
  - Cisco UCS VIC 1387 (UCSC-MLOM-C40Q-03)
- If the RHEL Operating System is installed on the server, CDN will appear when running the command "biosdevname -d" as "sysfs label". CDN will not change the kernel name.
• In Cisco UCS Manager Release 2.2(4), CDN is supported only on the following adapters:
  - Cisco UCS VIC 1225 (UCSC-PCIE-CSC-02)
  - Cisco UCS MLOM 1227 (UCSC-MLOM-CSC-02)
  - Cisco UCS VIC 1225T (UCSC-PCIE-C10T-02)
  - Cisco UCS MLOM 1227T (UCSC-MLOM-C10T-02)
  - Cisco UCS VIC 1240 (UCSB-MLOM-40G-01)
  - Cisco UCS VIC 1280 (UCS-VIC-M82-8P)
  - Cisco UCS VIC 1340 (UCSB-MLOM-40G-03)
  - Cisco UCS VIC 1380 (UCSB-VIC-M83-8P)

• CDN is supported for vNIC template and dynamic vNIC.

• Multiple vNICs within the same service profile cannot have the same CDN name.

• When a CDN name is not specified for a vNIC, the vNIC name is used as the CDN name.

• The CDN name that you configure for a vNIC appears as Admin CDN Name. The CDN name that is finally applied to the vNIC appears as Oper CDN Name. For example, if the Admin CDN Name for a vNIC called "vnic0" is cdn0, then the Oper CDN Name for this vNIC will be cdn0, but if the Admin CDN Name for the same vNIC is not specified, the Oper CDN Name will be vnic0.

• In Cisco UCS Manager Release 3.1 and later releases, downgrade of the adapter firmware is prevented if a CDN-enabled BIOS policy is assigned to a server.

• In Cisco UCS Manager Release 2.2(4), downgrade of Cisco UCS Manager is prevented if CDN is enabled in a BIOS policy that is assigned to an associated server.

• In Cisco UCS Manager Release 2.2(4), downgrade of the BIOS firmware is prevented if a CDN-enabled BIOS policy is assigned to a server.

• In Cisco UCS Manager Release 2.2(4), downgrade of the adapter firmware is prevented if a CDN-enabled BIOS policy is assigned to a server.

• When the applied BIOS policy is changed from CDN-disabled to CDN-enabled or from CDN-enabled to CDN-disabled, the host reboots with a warning, irrespective of whether reboot on BIOS update is enabled or not.

• It is recommended that you enable CDN in the BIOS policy and add CDN names to the vNICs before the Windows Operating System is installed.

• If the Windows Operating System is already installed on the server and CDN is then enabled in the BIOS policy, do the following:
  1. Uninstall the network drivers.
  2. Scan the system for hidden devices and uninstall them.
  3. Rescan the system for new hardware and install the network drivers again.

If this is not done, the vNICs will not come up with the configured CDN names.
• When the applied BIOS policy is changed from CDN-disabled to CDN-enabled or from CDN-enabled to CDN-disabled on a service profile, do the following:

1. Uninstall the network drivers.
2. Scan the system for hidden devices and delete them.
3. Re-scan the system for new hardware and install the network drivers again.

---

**Note**

When the BIOS policy is changed from CDN-enabled to CDN-disabled, ensure that the CDN names are removed from all the vNICs on the system.

---

• If any change is made to the vNICs, the BDF of all the devices on the system also changes. Following are some of the scenarios that trigger a change in the BDF of all the vNICs present on the system:

  • When a vNIC is added or deleted
  • When a vNIC is moved from one adapter on the system to another adapter on the system

When these changes are made to the system, do the following:

1. Uninstall the network driver from all the present network interfaces.
2. Scan the system for hidden devices and uninstall them.
3. Re-scan the system for new hardware and install the network driver on the network controllers again.

If the hidden devices are not deleted, the CDN names of the network adapters will not appear as configured on Cisco UCS Manager.

---

**CDN with a Mixed Set of Adapters**

When a CDN name is configured for a vNIC in a system with a mixed set of CDN-supported adapters and CDN-unsupported adapters, then system placement may not place CDN-configured vNICs on adapters that support CDN.

If CDN is enabled in the BIOS policy, and system placement places a CDN-configured vNIC (Admin CDN configured) on an adapter that does not support CDN, an info fault will be raised, but the configuration issue for the service profile will be ignored.

If CDN is enabled in the BIOS policy, and system placement places a vNIC (Admin CDN not configured) on an adapter that does not support CDN, an info fault will be raised, but the configuration issue for the service profile will be ignored. The **Oper CDN Name** in this case will be empty and will not be derived from the vNIC name.

If you want to deploy the CDN name as the host network interface name for a server, you must manually place a vNIC on a supported adapter.
Configuring Consistent Device Naming in a BIOS Policy

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Policies.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand root.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand BIOS Policies.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the BIOS policy for which you want to configure CDN.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Under the Main tab, click one of the following in the Consistent Device Naming field to configure CDN:</td>
</tr>
<tr>
<td></td>
<td><strong>Option</strong></td>
</tr>
<tr>
<td></td>
<td>disabled</td>
</tr>
<tr>
<td></td>
<td>enabled</td>
</tr>
<tr>
<td></td>
<td>Platform Default</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Save Changes.</td>
</tr>
</tbody>
</table>

Configuring a CDN Name for a vNIC

When a CDN name is not specified for a vNIC, the vNIC name is used as the CDN name.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Service Profiles.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization that contains the vNIC for which you want to configure a CDN name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand the service profile and vNICs node that contain the vNIC for which you want to configure a CDN name.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the vNIC.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click on the General tab.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Properties area, choose User Defined as the CDN Source.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Enter the CDN name for the vNIC in the CDN Name field.</td>
</tr>
</tbody>
</table>

**Note** The CDN name that you configure for a vNIC appears as CDN Name. The CDN name that is finally applied to the vNIC appears as Oper CDN Name. For example, if the CDN Name for a vNIC called "vnic0" is cdn0, then the Oper CDN Name for this vNIC will be cdn0, but if the CDN Name for the same vNIC is not specified, the Oper CDN Name will be vnic0.
Step 9 Click Save Changes.

CIMC Security Policies

Cisco UCS Manager provides the following policies to increase security:

- KVM Management Policy
- IPMI Access Profile

IPMI Access Profile

This policy allows you to determine whether IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the CIMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You can also restrict remote connectivity by disabling or enabling IPMI over LAN in the IPMI access profile. IPMI over LAN is disabled by default on all unassociated servers, and on all servers without an IPMI access policy. When an IPMI access policy is created, the IPMI over LAN is set to enabled by default. If you do not change the value to disabled, IPMI over LAN will be enabled on all associated servers.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating an IPMI Access Profile

Before you begin

An IPMI profile requires that one or more of the following resources already exist in the system:

- Username with appropriate permissions that can be authenticated by the operating system of the server
- Password for the username
- Permissions associated with the username

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies.
Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the root node.
Step 4 Right-click IPMI Access Profiles and select Create IPMI Access Profile.
Step 5 In the Create IPMI Access Profile dialog box:
a) Enter a unique name and description for the profile.
b) In the **IPMI Over LAN** field, choose whether to allow or restrict remote connectivity.
c) Click **OK**.

**Step 6**  
In the **IPMI Users** area of the navigator, click **+**.

**Step 7**  
In the **Create IPMI User** dialog box:

a) Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name field</strong></td>
<td>The username to associate with this IPMI profile. Enter 1 to 16 alphanumeric characters. You can also use @ (at sign), _ (underscore), and - (hyphen). You cannot change this name once the profile has been saved.</td>
</tr>
<tr>
<td><strong>Password field</strong></td>
<td>The password associated with this username. Enter 1 to 20 standard ASCII characters, except for = (equal sign), $ (dollar sign), and</td>
</tr>
<tr>
<td><strong>Confirm Password field</strong></td>
<td>The password a second time for confirmation purposes.</td>
</tr>
</tbody>
</table>
| **Role field** | The user role. This can be one of the following:  
  * **Admin**  
  * **Read Only** |
| **Description field** | User-defined description of the IPMI user. |

b) Click **OK**.

**Step 8**  
Repeat Steps 6 and 7 to add another user.

**Step 9**  
Click **OK** to return to the IPMI profiles in the **Work** pane.

---

**What to do next**

Include the IPMI profile in a service profile and/or template.

### Deleting an IPMI Access Profile

#### Procedure

**Step 1**  
In the **Navigation** pane, click **Servers**.

**Step 2**  
Expand **Servers > Policies > Organization_Name**.

**Step 3**  
Expand the **IPMI Profiles** node.

**Step 4**  
Right-click the profile you want to delete and select **Delete**.
KVM Management Policy

The KVM Management policy allows you to determine whether vMedia encryption is enabled when you access a server via KVM.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Note

After a KVM vMedia session is mapped, if you change the KVM management policy, it will result in a loss of the vMedia session. You must re-map the KVM vMedia session again.

Creating a KVM Management Policy

Procedure

Step 1
In the Navigation pane, click Servers.

Step 2
Expand Servers > Policies.

Step 3
Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the root node.

Step 4
Right-click KVM Management Policies and select Create KVM Management Policy.

Step 5
In the Create KVM Management Policy dialog box:

a) Enter a unique name and description for the policy.

b) In the vMedia Encryption field, choose whether to enable vMedia encryption.

c) Click OK.

Note
After a KVM vMedia session is mapped, if you change the KVM management policy, it will result in a loss of the vMedia session. You must re-map the KVM vMedia session again.

Graphics Card Policies

Cisco UCS Manager Release 3.1(3) extends graphics card support to include the ability to change the graphics card mode. You can now configure graphics card modes by using a graphics card policy. The graphics card modes are:

- Compute
- Graphics
Creating a Graphics Card Policy

Note
Cisco UCS Manager pushes the configuration changes to the GPU through the Graphics Card policy to the Processor Node Utility Operating System (PNuOS). These changes do not take effect until the server is rebooted.

Procedure

Step 1
In the Navigation pane, click Servers.

Step 2
Expand Servers > Policies.

Step 3
Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the root node.

Step 4

Step 5
On the Main page of the Create Graphics Card Policy dialog box:

a) Enter a unique name for the policy.

b) (Optional) Enter a description for the policy.

c) In the Graphics Card Mode field, choose one of the options:

• Compute

• Graphics

• Any Configuration

d) Click OK.

Local Disk Policies

Local Disk Configuration Policy
This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

• No Local Storage—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Striped**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.

- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.

- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory > Storage** tab for the server.

To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.

- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.

- **RAID 6 Striped Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.

- **RAID 10 Mirrored and Striped**—RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

- **RAID 50 Striped Parity and Striped**—Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.

- **RAID 60 Striped Dual Parity and Striped**—Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

You must include this policy in a service profile and that service profile must be associated with a server for the policy to take effect.

---

**Note**

For a Cisco UCS C-Series server integrated with Cisco UCS Manager, with an embedded on-board RAID controller, the local disk mode should always be **Any Configuration**, and the RAID must be configured directly on the controller.

---

**Guidelines for all Local Disk Configuration Policies**

Before you create a local disk configuration policy, consider the following guidelines:

**No Mixed HDDs and SSDs**

Do not include HDDs and SSDs in a single server or RAID configuration.
Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or re-assign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes those with Any Configuration or JBOD configuration.

JBOD Mode Support

The B200 M3 server supports JBOD mode for local disks.

Note

Only B200 M1, B200 M2, B200 M3, B250 M1, B250 M2 and B22 M3 blade servers support the JBOD mode for local disks.

Guidelines for Local Disk Configuration Policies Configured for RAID

Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server. You can do this either by configuring the local disk configuration policy in the service profile using one of the defined RAID modes for that server, or you can use the Any Configuration mode with the LSI Utilities toolset to create the RAID volumes.

If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

Server May Not Boot After RAID1 Cluster Migration if Any Configuration Mode Specified in Service Profile

After RAID1 clusters are migrated, you need to associate a service profile with the server. If the local disk configuration policy in the service profile is configured with Any Configuration mode rather than RAID1, the RAID LUN remains in “inactive” state during and after association. As a result, the server cannot boot.

To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the Any Configuration mode.

Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with a MegaRAID storage controllers. JBOD mode and operations are not intended for nor are they fully functional on these servers.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID
Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

**Maximum of One RAID Volume and One RAID Controller in Blade Servers**

A blade server can have a maximum of one RAID volume irrespective of how many drives are present in the server. All the local hard drives must be connected to only one RAID controller. For example, a B200 M3 server has an LSI controller and an Intel Patsburg controller, but only the LSI controller can be used as a RAID controller.

In addition, do not use third party tools to create multiple RAID LUNs on blade servers. Cisco UCS Manager does not support that configuration.

**Number of Disks Selected in Mirrored RAID Should Not Exceed Two**

If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

**License Required for Certain RAID Configuration Options on Some Servers**

Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Manager associates a service profile containing this local disk policy with a server, Cisco UCS Manager verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Manager displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

**B420 M3 Server Does Not Support All Configuration Modes**

The B420 M3 server does not support the following configuration modes in a local disk configuration policy:

- No RAID
- RAID 6 Striped Dual Parity

In addition, the B420 M3 does not support JBOD modes or operations.

**Single-Disk RAID 0 Configurations Not Supported on Some Blade Servers**

A single-disk RAID 0 configuration is not supported in the following blade servers:

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2
Creating a Local Disk Configuration Policy

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand the node for the organization where you want to create the policy.
        If the system does not include multitenancy, expand the root node.
Step 4  Right-click Local Disk Config Policies and choose Create Local Disk Configuration Policy.
Step 5  In the Create Local Disk Configuration Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (caret), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
</tbody>
</table>
Creating a Local Disk Configuration Policy

This can be one of the following local disk policy modes:

- **No Local Storage**
- **RAID 0 Striped**
- **RAID 1 Mirrored**
- **Any Configuration**
- **No RAID**

If you choose No RAID and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the No RAID mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the Inventory > Storage tab for the server.

To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the No RAID configuration mode.

- **RAID 5 Striped Parity**
- **RAID 6 Striped Dual Parity**
- **RAID 10 Mirrored and Striped**
- **RAID 50 Striped Parity and Striped**
- **RAID 60 Striped Dual Parity and Striped**

**Note**

Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Manager associates a service profile containing this local disk policy with a server, Cisco UCS Manager verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Manager displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the Hardware Installation Guide for that server.
### Protect Configuration check box

If checked, the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile.

**Caution** Protect Configuration becomes non-functional if one or more disks in the server are defective or faulty.

This property is checked by default.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

With this option enabled, the data on the disk is protected even after the server is decommissioned and then recommissioned. Hence, reassociation of the server with a service profile fails.

**Note** If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

### FlexFlash State radio button

To enable or disable the FlexFlash controller on the SD card, click the appropriate button.

**Note** This parameter only applies to a server with an SD card module.

### FlexFlash RAID Reporting State radio button

To enable or disable RAID reporting, click the appropriate button. When RAID reporting is enabled, the RAID status is monitored and faults are enabled.

**Note** If only one SD card is installed, the RAID state will be displayed as Disabled and the RAID health as NA even if RAID reporting is enabled.

### FlexFlash Removable State radio button

To select the removable state of the FlexFlash SD card, click the appropriate button.

- **Yes**—Use this option to define the SD card as removable.
- **No**—Use this option to define the SD card as fixed or non-removable.
- **No Change**—Use this option if the hypervisor does not require a preset state for the SD card.

**Step 6** Click OK.
Changing a Local Disk Configuration Policy

This procedure describes how to change a local disk configuration policy from an associated service profile. You can also change a local disk configuration policy from the Policies node from Servers.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Expand Servers &gt; Service Profiles.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Expand the organization that includes the service profile with the local disk configuration policy you want to change. If the system does not include multitenancy, expand the root node.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click the service profile that contains the local disk configuration policy you want to change.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the Work pane, click the Storage tab.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>In the Actions area, click Change Local Disk Configuration Policy.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>In the Change Local Disk Configuration Policy dialog box, choose one of the following options from the Select the Local Disk Configuration Policy drop-down list.</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Use a Disk Policy</td>
<td>Select an existing local disk configuration policy from the list below this option. Cisco UCS Manager assigns this policy to the service profile.</td>
</tr>
<tr>
<td>Create a Local Disk Policy</td>
<td>Enables you to create a local disk configuration policy that can only be accessed by the selected service profile.</td>
</tr>
<tr>
<td>No Disk Policy</td>
<td>Selects the default local disk policy. &lt;br&gt;<strong>Note</strong> If a UCS server is attached to the Cisco UCS Manager, selecting the No Disk Policy can erase and replace the RAID with individual RAID 0 disks if the default RAID configuration is not supported on the attached server.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Click OK.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>(Optional) Expand the Local Disk Configuration Policy area to confirm that the change has been made.</td>
</tr>
</tbody>
</table>

Deleting a Local Disk Configuration Policy

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Expand Servers &gt; Policies &gt; Organization_Name.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Expand the Local Disk Config Policies node.</td>
</tr>
</tbody>
</table>
Step 4: Right-click the policy you want to delete and select **Delete**.

Step 5: If a confirmation dialog box displays, click **Yes**.

---

**FlexFlash Support**

**Overview**

Cisco UCS B-Series, C-Series M3 and higher, and S-Series M4 servers support internal Secure Digital (SD) memory cards. The SD cards are hosted by the Cisco Flexible Flash storage controller, a PCI-based controller which has two slots for SD cards. The cards contain a single partition called HV. When FlexFlash is enabled, Cisco UCS Manager displays the HV partition as a USB drive to both the BIOS and the host operating system.

You can populate one or both the SD card slots that are provided. If two SD cards are populated, you can use them in a mirrored mode.

---

**Note**

Do not mix different capacity cards in the same server.

---

The SD cards can be used to store operating system boot images or other information. The following figure illustrates the SD card slots.

*Figure 1: SD Card Slots*
FlexFlash is disabled by default. You can enable FlexFlash in a local disk policy used in a service profile. When FlexFlash is enabled in a local disk policy, and the server is capable of supporting SD cards, the FlexFlash controller is enabled during service profile association. If a server is not capable of supporting SD cards or has an older CIMC version, a config failure message is displayed.

If you disable FlexFlash in a supported server, the Hypervisor or HV partition is immediately disconnected from the host. The FlexFlash controller will also be disabled as part of a related service profile disassociation.

The FlexFlash controller supports RAID-1 for dual SD cards. The FlexFlash scrub policy erases the HV partition in both cards, and brings the cards to a healthy RAID state.

You can configure new SD cards in a RAID pair and format them using one of the following methods:

- Format the SD cards. Formatting the SD Cards, on page 262 provides detailed information.
- Disassociate the service profile from the server. Re-acknowledge the server after modifying the default scrub policy and then associate the server profile back to the server.

The Scrub Policy Settings section in the Cisco UCS Manager Server Management Guide provides more details about the usage of the scrub policy.

Note

Disable the scrub policy as soon as the pairing is complete.

To boot from the HV partition, the SD card must be present in the boot policy used in the service profile.

FlexFlash Firmware Management

The FlexFlash controller firmware is bundled as part of the CIMC image. When you upgrade the CIMC, if a newer firmware version is available for the FlexFlash controller, the controller can no longer be managed, and the FlexFlash inventory displays the Controller State as Waiting For User Action and the Controller Health as Old Firmware Running. To upgrade the FlexFlash controller firmware, you need to perform a board controller update. For more information, see the appropriate Cisco UCS B-Series Firmware Management Guide, available at the following URL:

Limitations for the Cisco Flexible Flash Storage Controller:

- The Cisco Flexible Flash storage controller only supports 16 GB, 32 GB, and 64 GB SD cards.

**Note**

16 GB and 32 GB cards are supported only on the M3 blade servers, and the 64 GB SD cards are supported only on the M4 blade servers.

- We do not recommend using an SD card from a rack server in a blade server, or using an SD card from a blade server in a rack server. Switching SD cards between server types might result in data loss from the SD card.

- Some Cisco UCS C-Series rack-mount servers have SD cards with four partitions: HV, HUU, SCU, and Drivers. Only the HV partition is visible in Cisco UCS Manager. You can migrate a four-partition SD card to a single HV partition card with a FlexFlash scrub policy but there may be data loss.

- The FlexFlash controller does not support RAID-1 sync (mirror rebuild). If the SD cards are in a degraded RAID state, or if any metadata errors are reported by the controller, you must run the FlexFlash scrub policy to pair the cards for RAID. For more information about the FlexFlash scrub policy, see Server-Related Policies. The following conditions might result in degraded RAID or metadata errors:
  - Inserting a new or used SD card in one slot, when the server already has an SD card populated in the second slot.
  - Inserting two SD cards from different servers.

- The server firmware version must be at 2.2(1a) or higher.

**FlexFlash FX3S Support**

Beginning with Release 2.2(3), Cisco UCS Manager allows additional FlexFlash support with the FX3S controller. The FX3S controller is present on the following servers:

- Cisco UCS B200 M4 blade server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4 rack server

FlexFlash operations with the FX3S control are similar to those with the Cisco Flexible Flash storage controller. FlexFlash is disabled by default, and is enabled using a local disk policy. You can also reset the controller, format the SD cards, and enable automatic synchronization of your paired SD cards.

The SD cards for the FX3S controller contain a single partition called Hypervisor.

Limitations for the Cisco FX3S Controller:

- The FX3S controller supports only 32 GB and 64 GB SD cards. 16 GB cards are not supported.

- We do not recommend using an SD card from a rack server in a blade server, or using an SD card from a blade server in a rack server. Switching SD cards between server types might result in data loss from the SD card.

- The server firmware version must be at 2.2(3a) or higher.
Starting Up Blade Servers with FlexFlash SD Cards

Use this procedure to start up blade servers using FlexFlash cards 16 GB and larger. This procedure requires that you know how to setup the blade server, software, and the associated infrastructure, and ensure that they are working. This Cisco UCS Manager controlled procedure is applicable to all blade servers, running any version of firmware. This procedure does not apply to rack servers. Follow this procedure before you enable FlexFlash cards in a working environment.

Caution

If you use the following procedure with FlexFlash cards already in use, you will lose all data from the cards.

Note

This procedure does not cover FlexFlash card usage or other functions of the FlexFlash system.

Procedure

Step 1
Expand Equipment > Chassis > Chassis Number > Servers.

Step 2
In the Work pane, check the details of the FlexFlash cards in the FlexFlash Controller window.

Step 3
Expand Servers > Service Profiles.

Step 4
Expand the node for the organization containing the pool.

Step 5
Expand the node for the organization containing the service profile and click Storage.

Step 6
In the Work pane, click Change Local Disk Configuration Policy in the Actions area and expand Create Local Disk Configuration Policy link. Follow the procedure in Creating a Local Disk Configuration Policy, on page 253 to create a Local Disk Configuration Policy.

The FlexFlash policy name must not contain empty spaces or special characters.

Step 7
Expand Change Disk Local Configuration Policy, and select the policy you just created and click OK.

Step 8
Expand Servers > Policies.

Step 9
Follow the procedure in Creating a Scrub Policy, on page 263 and create a policy with a name such as Scrub-FF-name and click OK.

The Scrub policy name must not contain empty spaces or special characters.

Step 10
Select the policy you created from the drop-down box.

Step 11
Expand Equipment > Chassis > Chassis Number > Servers.

Step 12
In the Work pane, click the General tab and select Server Maintenance from the Actions area.

Step 13
In the Maintenance Server dialogue box, click on the Re-acknowledge radio button, and then click OK.

Step 14
Click Server Maintenance in the Action area and click on the Re-acknowledge radio button again.

Step 15
From the Inventory tab, select the Storage sub-tab.

You can verify details of the enabled FlexFlash cards from the FlexFlash Controller window in the Work area.
Step 16  Launch KVM Manager and log on to the operating system. Verify details of the Hypervisor partition from the Devices and drives folder. Depending on the card size, the HV partition displays details of 32GB, 64GB, or 128 GB. The FlexFlash cards are now synced and ready to use.

---

Enabling FlexFlash SD Card Support

**Procedure**

**Step 1**  In the Navigation pane, click Servers.

**Step 2**  Expand Servers > Policies.

**Step 3**  Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the root node.

**Step 4**  Expand Local Disk Config Policies and choose the local disk config policy for which you want to enable FlexFlash support.

**Step 5**  In the Work pane, click the General tab.

**Step 6**  In the FlexFlash State field, click the Enable radio button.

**Step 7**  In the FlexFlash RAID Reporting State field, click the Enable radio button.

**Step 8**  Click Save Changes.

---

Enabling Auto-Sync

**Procedure**

**Step 1**  In the Navigation pane, click Equipment.

**Step 2**  Expand Equipment > Chassis > Chassis Number > Servers.

**Step 3**  Click the server for which you want to enable auto-sync.

**Step 4**  In the Work pane, click the Inventory tab.

**Step 5**  Click the Storage subtab.

**Step 6**  In the Actions area, click Enable Auto-sync.

**Step 7**  In the Enable Auto-sync dialog box, choose the Admin Slot Number for the SD card that you want to use as the primary.

**Step 8**  Click OK.
Formatting the SD Cards

**Procedure**

- **Step 1** In the Navigation pane, click Equipment.
- **Step 2** Expand Equipment > Chassis > Chassis Number > Servers.
- **Step 3** Click the server for which you want to format the SD cards.
- **Step 4** In the Work pane, click the Inventory tab.
- **Step 5** Click the Storage subtab.
- **Step 6** In the Actions area, click Format SD Cards.
- **Step 7** Click Yes to format the SD cards.

Resetting the FlexFlash Controller

**Procedure**

- **Step 1** In the Navigation pane, click Equipment.
- **Step 2** Expand Equipment > Chassis > Chassis Number > Servers.
- **Step 3** Click the server for which you want to reset the FlexFlash controller.
- **Step 4** In the Work pane, click the Inventory tab.
- **Step 5** Click the Storage subtab.
- **Step 6** In the Actions area, click Reset FlexFlash Controller.
- **Step 7** Click Yes to reset the FlexFlash controller.

Scrub Policy

**Scrub Policy Settings**

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process, when the server is re-acknowledged, or when the server is disassociated from a service profile.

**Note**

Local disk scrub policies only apply to hard drives that are managed by Cisco UCS Manager and do not apply to other devices such as USB drives.

Depending upon how you configure a scrub policy, the following can occur at those times:
Disk scrub

One of the following occurs to the data on any local drives on disassociation:

- If enabled, destroys all data on any local drives.
- If disabled (default), preserves all data on any local drives, including local storage configuration.

Scrub policies are supported on all B-Series platforms and only on the following C-Series platforms:

BIOS Settings Scrub

One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:

- If enabled, erases all BIOS settings for the server and resets them to the BIOS defaults for that server type and vendor.
- If disabled (default), preserves the existing BIOS settings on the server.

FlexFlash Scrub

FlexFlash Scrub enables you to pair new or degraded SD cards, resolve FlexFlash metadata configuration failures, and migrate older SD cards with 4 partitions to single partition SD cards. One of the following occurs to the SD card when a service profile containing the scrub policy is disassociated from a server, or when the server is reacknowledged:

- If enabled, the HV partition on the SD card is formatted using the PNUOS formatting utility. If two SD cards are present, the cards are RAID-1 paired, and the HV partitions in both cards are marked as valid. The card in slot 1 is marked as primary, and the card in slot 2 is marked as secondary.
- If disabled (default), preserves the existing SD card settings.

Because the FlexFlash scrub erases the HV partition on the SD cards, we recommend that you take a full backup of the SD card(s) using your preferred host operating system utilities before performing the FlexFlash scrub.

To resolve metadata config failures in a service profile, you need to disable FlexFlash in the local disk config policy before you run the FlexFlash scrub, then enable FlexFlash after the server is reacknowledged.

Disable the scrub policy as soon as the pairing is complete or the metadata failures are resolved.

FlexFlash scrub is not supported for Cisco UCS S3260 Storage Server.

Creating a Scrub Policy

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies.
Deleting a Scrub Policy

**Step 3** Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

**Step 4** Right-click **Scrub Policies** and select **Create Scrub Policy**.

**Step 5** In the **Create Scrub Policy** wizard, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except `'(accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ' (single quote).</td>
</tr>
<tr>
<td>Disk Scrub field</td>
<td>If this field is set to <strong>Yes</strong>, when a service profile containing this scrub policy is disassociated from a server, all data on the server local drives is completely erased. If this field is set to <strong>No</strong>, the data on the local drives is preserved, including all local storage configuration.</td>
</tr>
<tr>
<td>BIOS Settings Scrub field</td>
<td>If the field is set to <strong>Yes</strong>, when a service profile containing this scrub policy is disassociated from a server, the BIOS settings for that server are erased and reset to the defaults for that server type and vendor. If this field is set to <strong>No</strong>, the BIOS settings are preserved.</td>
</tr>
<tr>
<td>FlexFlash Scrub field</td>
<td>If the field is set to <strong>Yes</strong>, the HV partition on the SD card is formatted using the PNUOS formatting utility when the server is reacknowledged. If this field is set to <strong>No</strong>, the SD card is preserved.</td>
</tr>
</tbody>
</table>

**Step 6** Click **OK**.

**Note** Disk scrub and FlexFlash Scrub options are not supported for Cisco UCS S3260 Storage Server.

---

**Deleting a Scrub Policy**

**Procedure**

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Servers > Policies > Organization_Name**.

**Step 3** Expand the **Scrub Policies** node.

**Step 4** Right-click the policy you want to delete and select **Delete**.
DIMM Error Management

DIMM Correctable Error Handling

In Cisco UCS Manager, when a DIMM encounters a significant correctable error in a given predefined window, it is stated as degraded and considered as a non-functional device.

The DIMM correctable error handling feature enables you to reset all the correctable and uncorrectable memory errors on all the DIMMs in a server. When you reset the error configuration, the error count of a given DIMM is cleared, the status changes to operable, and it resets the sensor state of the given DIMM.

Resetting Memory Errors

Use this procedure to reset all correctable and uncorrectable memory errors encountered by Cisco UCS Manager and the baseboard management controller (BMC).

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Chassis Number > Servers.
Step 3 Right-click on the server for which you want to reset the error configuration, and select Reset All Memory Errors. You can also select Reset All Memory Errors from the Actions area.
Step 4 If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes.

DIMM Blacklisting

In Cisco UCS Manager, the state of the Dual In-line Memory Module (DIMM) is based on SEL event records. When the BIOS encounters a noncorrectable memory error during memory test execution, the DIMM is marked as faulty. A faulty DIMM is a considered a nonfunctional device.

If you enable DIMM blacklisting, Cisco UCS Manager monitors the memory test execution messages and blacklists any DIMMs that encounter memory errors in the DIMM SPD data. To allow the host to map out any DIMMs that encounter uncorrectable ECC errors.

Enabling DIMM Blacklisting

The memory policy is a global policy that you can apply to existing servers on a Cisco UCS domain and also to the servers that are added after you set the memory policy.
Enabling DIMM Blacklisting

Note

- This feature is supported both on the Cisco UCS B-Series blade servers and UCS C-Series rack servers.

Note

Cisco UCS C-Series 420 M3 rack servers do not support this feature.

Note

- This global policy cannot be added to a service profile.

Before you begin

- For Cisco B-Series blade server, the server firmware must be at Release 2.2(1) or a later release.
- For Cisco C-Series and S-Series rack server, the server firmware must be at Release 2.2(3).
- You must be logged in with one of the following privileges:
  - Admin
  - Server policy
  - Server profile server policy

Procedure

Step 1
In the Navigation pane, click Servers.

Step 2
Expand Servers > Policies.

Step 3
Expand the node for the organization where you want to enable the blacklisting. If the system does not include multitenancy, expand the root node.

Step 4
Expand Memory Policy and choose default.

Step 5
In the Blacklisting area, click the Enabled radio button.

The DIMM blacklisting is enabled for the domain level policy and these changes apply to all the servers on that particular domain.

Note

If the Cisco IMC of a server does not support DIMM blacklisting, an information level fault is generated.
Serial over LAN Policy Settings

Serial over LAN Policy Overview

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating a Serial over LAN Policy

Procedure

Step 1. In the Navigation pane, click Servers.

Step 2. Expand Servers > Policies.

Step 3. Expand the node for the organization where you want to create the policy.

   If the system does not include multitenancy, expand the root node.

Step 4. Right-click Serial over LAN Policies and select Create Serial over LAN Policy.

Step 5. In the Create Serial over LAN Policy wizard, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
</tbody>
</table>
| Serial over LAN State field | This can be one of the following:  
  • Disable—Serial over LAN access is blocked.  
  • Enable—Serial over LAN access is permitted. |
Deleting a Serial over LAN Policy

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies > Organization_Name.
Step 3 Expand the Serial over LAN Policies node.
Step 4 Right-click the policy you want to delete and select Delete.
Step 5 If a confirmation dialog box displays, click Yes.

Server Autoconfiguration Policies

Server Autoconfiguration Policy Overview

Cisco UCS Manager uses this policy to determine how to configure a new server. If you create a server autoconfiguration policy, the following occurs when a new server starts:

1. The qualification in the server autoconfiguration policy is executed against the server.
2. If the server meets the required qualifications, the server is associated with a service profile created from the service profile template configured in the server autoconfiguration policy. The name of that service profile is based on the name given to the server by Cisco UCS Manager.
3. The service profile is assigned to the organization configured in the server autoconfiguration policy.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed drop-down list</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 9600</td>
</tr>
<tr>
<td></td>
<td>• 19200</td>
</tr>
<tr>
<td></td>
<td>• 38400</td>
</tr>
<tr>
<td></td>
<td>• 57600</td>
</tr>
<tr>
<td></td>
<td>• 115200</td>
</tr>
</tbody>
</table>
Creating an Autoconfiguration Policy

Before you begin

This policy requires that one or more of the following resources already exist in the system:

- Server pool policy qualifications
- Service profile template
- Organizations, if a system implements multitenancy

Procedure

Step 1
In the Navigation pane, click Equipment.

Step 2
Click the Equipment node.

Step 3
In the Work pane, click the Policies tab.

Step 4
Click the Autoconfig Policies subtab.

Step 5
On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 6
In the Create Autoconfiguration Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ’ (single quote).</td>
</tr>
<tr>
<td>Qualification drop-down list</td>
<td>The server pool policy qualification associated with this auto-configuration policy. If a new server is discovered that matches the criteria specified in the server pool policy qualification, Cisco UCS automatically creates a service profile based on the service profile template selected in the Service Profile Template Name drop-down list and associates the newly created service profile with the server.</td>
</tr>
</tbody>
</table>
Deleting an Autoconfiguration Policy

**Procedure**

Step 1  In the **Navigation** pane, click **Equipment**.

Step 2  Click the **Equipment** node.

Step 3  In the **Work** pane, click the **Policies** tab.

Step 4  Click the **Autoconfig Policies** subtab.

Step 5  Right-click the autoconfiguration policy that you want to delete and choose **Delete**.

Step 6  If a confirmation dialog box displays, click **Yes**.

Server Discovery Policy Settings

**Server Discovery Policy Overview**

The server discovery policy determines how the UCS Manager reacts when you add a new UCS Blade Server and UCS Mini. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

If you create a server discovery policy, the following occurs when a new server starts:

1. The server discovery policy qualification is executed against the server.

2. If the server meets the required qualifications, Cisco UCS Manager applies the following to the server:
   - Depending on the option that you select for the action, UCS Manager discovers the new server immediately, or waits for a user acknowledgment of the new server
   - Applies the scrub policy to the server
If automatic deep discovery is triggered by any hardware insertion, removal, or replacement, the following occurs:

1. The server is moved to a “pending activities” list.
2. A critical hardware mismatch fault is raised on the server, indicating that UCSM has detected a hardware mismatch.
3. User must explicitly acknowledge the server to trigger the deep discovery.

Important

In Cisco UCS Manager Release 2.2 (4), blade servers do not support drives with a block size of 4K, but rack-mount servers support such drives. If a drive with a block size of 4K is inserted into a blade server, discovery fails and the following error message appears:

Unable to get Scsi Device Information from the system

If this error occurs, do the following:

1. Remove the 4K drive.
2. Reacknowledge the server.

Reacknowledging the server causes the server to reboot and results in loss of service.

Creating a Server Discovery Policy

Before you begin

If you plan to associate this policy with a server pool, create server pool policy qualifications.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 In the Work pane, click the Policies tab.
Step 3 Click the Server Discovery Policies subtab.
Step 4 Click the + icon on the table icon bar to open the Create Server Discovery Policy dialog box.
Step 5 In the Description field, enter a description for the discovery policy.
Step 6 In the Action field, select one of the following options:
   • Immediate—Cisco UCS Manager attempts to discover new servers automatically
   • User Acknowledged—Cisco UCS Manager waits until the user tells it to search for new servers
Step 7 (Optional) To associate this policy with a server pool, select server pool policy qualifications from the Qualification drop-down list.
Step 8 (Optional) To include a scrub policy, select a policy from the Scrub Policy drop-down list.
Step 9 Click OK.
What to do next
Include the server discovery policy in a service profile and/or template.

Deleting a Server Discovery Policy

Procedure

Step 1
In the Navigation pane, click Equipment.

Step 2
In the Work pane, click the Policies tab.

Step 3
Click the Server Discovery Policies subtab.

Step 4
Right-click the server discover policy that you want to delete and choose Delete.

Step 5
If a confirmation dialog box displays, click Yes.

Hardware Change Discovery Policy

The Hardware Change Discovery is a global policy used to set the how Cisco UCS Manager behaves when there is a hardware component change. The policy has two values:

• User Acknowledged: You must acknowledge the server to clear all the hardware inventory mismatch faults.

• Auto Acknowledged: Triggers automatic deep discovery when a hardware component change is detected.

When UCSM detects any change in the server hardware component, a critical hardware inventory mismatch fault is raised on the server. You must manually acknowledge the server to clear the fault and complete the hardware inventory. Once you have acknowledged the server, deep discovery and deep association is triggered.

For rack servers, you must decommision and recomission the server to clear the fault and complete the hardware inventory.

You cannot make changes to the policy if there is a hardware inventory mismatch fault.

Configuring Hardware Change Discovery Policy

Procedure

Step 1
Navigate to Equipment > Policies > Global Policies

Step 2
Under Hardware Change Discovery Policy, choose one of the following:

• User Acknowledged: You must acknowledge the server to clear all the hardware inventory mismatch faults.

• Auto Acknowledged: Triggers automatic deep discovery when a hardware component change is detected.
Server Inheritance Policy Settings

Server Inheritance Policy Overview

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Creating a Server Inheritance Policy

A blade server or rack-mount server with a VIC adapter, such as the Cisco UCS M81KR Virtual Interface Card, does not have server identity values burned into the server hardware at manufacture. As a result, the identity of the adapter must be derived from default pools. If the default pools do not include sufficient entries for one to be assigned to the server, service profile association fails with a configuration error.

Procedure

Step 1  In the Navigation pane, click Equipment.
Step 2  In the Work pane, click the Policies tab.
Step 3  Click the Server Inheritance Policies subtab.
Step 4  On the icon bar at the bottom of the table, click + Add.
         If + Add is disabled, click an entry in the table to enable it.
Step 5  In the Create Server Inheritance Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
</tbody>
</table>
Deleting a Server Inheritance Policy

**Procedure**

**Step 1**  In the **Navigation** pane, click **Equipment**.
**Step 2**  In the **Work** pane, click the **Policies** tab.
**Step 3**  Click the **Server Inheritance Policies** subtab.
**Step 4**  Right-click the server inheritance policy that you want to delete and choose **Delete**.
**Step 5**  If a confirmation dialog box displays, click **Yes**.

Server Pool Policy Settings

**Server Pool Policy Overview**

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

**Creating a Server Pool Policy**

**Before you begin**

This policy requires that one or more of the following resources already exist in the system:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong> field</td>
<td>A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except <code>\</code> (accent mark), <code>\</code> (backslash), <code>^</code> (carat), <code>&quot;</code> (double quote), <code>=</code> (equal sign), <code>&gt;</code> (greater than), <code>&lt;</code> (less than), or <code>'</code> (single quote).</td>
</tr>
<tr>
<td><strong>Qualification</strong> drop-down list</td>
<td>To associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools.</td>
</tr>
<tr>
<td><strong>Org</strong> drop-down list</td>
<td>If you want to associate an organization with this policy, or if you want to change the current association, choose the organization from the drop-down list.</td>
</tr>
</tbody>
</table>
• A minimum of one server pool
• Server pool policy qualifications, if you choose to have servers automatically added to pools

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Policies.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization where you want to create the policy. If the system does not include multitenancy, expand the root node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click Server Pool Policies and select Create Server Pool Policy.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Create Server Pool Policy dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the policy.Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ' (accent mark), \ (backslash), ^ (carat), &quot; (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ' (single quote).</td>
</tr>
<tr>
<td>Target Pool drop-down list</td>
<td>If you want to associate this policy with a server pool, select that pool from the drop-down list.</td>
</tr>
<tr>
<td>Qualification drop-down list</td>
<td>To associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools.</td>
</tr>
</tbody>
</table>

| Step 6 | Click OK. |

Deleting a Server Pool Policy

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Policies &gt; Organization_Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the Server Pool Policies node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the policy you want to delete and select Delete.</td>
</tr>
</tbody>
</table>
Step 5 If a confirmation dialog box displays, click **Yes**.

### Server Pool Policy Qualifications Settings

#### Server Pool Policy Qualification Overview

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you might need to configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

### Creating Server Pool Policy Qualifications

#### Procedure

**Step 1** In the **Navigation** pane, click **Servers**.

**Step 2** Expand **Servers > Policies**.
Step 3
Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the root node.

Step 4
Right-click the Server Pool Policy Qualifications node and select Create Server Pool Policy Qualification.

Step 5
In the Create Server Pool Policy Qualification dialog box, enter a unique name and description for the policy.

Step 6
(Optional) To use this policy to qualify servers according to their adapter configuration, do the following:

a) Click Create Adapter Qualifications.
b) In the Create Adapter Qualifications dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type drop-down list</td>
<td>The adapter type.</td>
</tr>
<tr>
<td></td>
<td>Once you save the adapter qualification, this type cannot be changed.</td>
</tr>
<tr>
<td>PID field</td>
<td>A regular expression that the adapter PID must match.</td>
</tr>
<tr>
<td>Maximum Capacity field</td>
<td>The maximum capacity for the selected type.</td>
</tr>
<tr>
<td></td>
<td>To specify a capacity, choose select and enter the desired maximum capacity.</td>
</tr>
<tr>
<td></td>
<td>You can enter an integer between 1 and 65535.</td>
</tr>
</tbody>
</table>

c) Click OK.

Step 7
(Optional) To use this policy to qualify servers according to the chassis in which they physically reside, do the following:

a) Click Create Chassis/Server Qualifications.
b) In the Chassis Qualifications area of the Create Chassis and Server Qualifications dialog box, complete the following fields to specify the range of chassis you want to use:

- **First Chassis ID** field—The first chassis ID from which server pools associated with this policy can draw.
- **Number of Chassis** field—The total number of chassis to include in the pool, starting with the chassis identified in the First Chassis ID field.

Example:
For example, if you want to use chassis 5, 6, 7, and 8, enter 5 in the First Chassis ID field and 4 in the Number of Chassis field. If you want to use only chassis 3, enter 3 in the First Chassis ID field and 1 in the Number of Chassis field.

Tip
If you want to use chassis 5, 6, and 9, create a chassis/server qualification for the range 5-6 and another qualification for chassis 9. You can add as many chassis/server qualifications as needed.
c) Click Finish.

Step 8
(Optional) To use this policy to qualify servers according to both the chassis and slot in which they physically reside, do the following:

a) Click Create Chassis/Server Qualifications.
b) In the Chassis Qualifications area of the Create Chassis and Server Qualifications dialog box, complete the following fields to specify the range of chassis you want to use:
Creating Server Pool Policy Qualifications

- **First Chassis ID** field—The first chassis ID from which server pools associated with this policy can draw.

- **Number of Chassis** field—The total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.

c) In the **Server Qualifications** table, click **Add**.
d) In the **Create Server Qualifications** dialog box, complete the following fields to specify the range of server locations you want to use:

  - **First Slot ID** field—The first slot ID from which server pools associated with this policy can draw.
  - **Number of Slots** field—The total number of slots from which server pools associated with this policy can draw.

e) Click **Finish Stage**.
f) To add another range of slots, click **Add** and repeat steps d and e.
g) When you have finished specifying the slot ranges, click **Finish**.

**Step 9**

(Optional) To use this policy to qualify servers according to their memory configuration, do the following:

a) Click **Create Memory Qualifications**.
b) In the **Create Memory Qualifications** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock field</td>
<td>The minimum clock speed required, in megahertz.</td>
</tr>
<tr>
<td>Latency field</td>
<td>The maximum latency allowed, in nanoseconds.</td>
</tr>
<tr>
<td>Min Cap field</td>
<td>The minimum memory capacity required, in megabytes.</td>
</tr>
<tr>
<td>Max Cap field</td>
<td>The maximum memory capacity allowed, in megabytes.</td>
</tr>
<tr>
<td>Width field</td>
<td>The minimum width of the data bus.</td>
</tr>
<tr>
<td>Units field</td>
<td>The unit of measure to associate with the value in the <strong>Width</strong> field.</td>
</tr>
</tbody>
</table>

c) Click **OK**.

**Step 10**

(Optional) To use this policy to qualify servers according to their CPU/Cores configuration, do the following:

a) Click **Create CPU/Cores Qualifications**.
b) In the **Create CPU/Cores Qualifications** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Architecture drop-down list</td>
<td>The CPU architecture to which this policy applies.</td>
</tr>
<tr>
<td>PID field</td>
<td>A regular expression that the processor PID must match.</td>
</tr>
<tr>
<td>Min Number of Cores field</td>
<td>The minimum number of CPU cores required. To specify a capacity, choose select and enter an integer between 1 and 65535 in the associated text field.</td>
</tr>
</tbody>
</table>
### Server-Related Policies

#### Creating Server Pool Policy Qualifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max Number of Cores</strong> field</td>
<td>The maximum number of CPU cores allowed. To specify a capacity, choose select and enter an integer between 1 and 65535 in the associated text field.</td>
</tr>
<tr>
<td><strong>Min Number of Threads</strong> field</td>
<td>The minimum number of CPU threads required. To specify a capacity, choose select and enter an integer between 1 and 65535 in the associated text field.</td>
</tr>
<tr>
<td><strong>Max Number of Threads</strong> field</td>
<td>The maximum number of CPU threads allowed. To specify a capacity, choose select and enter an integer between 1 and 65535 in the associated text field.</td>
</tr>
<tr>
<td><strong>CPU Speed</strong> field</td>
<td>The minimum CPU speed required. To specify a capacity, choose select and enter the minimum CPU speed.</td>
</tr>
<tr>
<td><strong>CPU Stepping</strong> field</td>
<td>The minimum CPU version required. To specify a capacity, choose select and enter the maximum CPU speed.</td>
</tr>
</tbody>
</table>

**c)** Click **OK**.

**Step 11** *(Optional)* To use this policy to qualify servers according to their storage configuration and capacity, do the following:

a) Click **Create Storage Qualifications**.

b) In the **Create Storage Qualifications** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Diskless** field | Whether the available storage must be diskless. This can be one of the following:  
  • Unspecified—Either storage type is acceptable.  
  • Yes—The storage must be diskless.  
  • No—The storage cannot be diskless. |
| **Number of Blocks** field | The minimum number of blocks required. To specify a capacity, choose select and enter the number of blocks. |
| **Block Size** field | The minimum block size required, in bytes. To specify a capacity, choose select and enter the block size. |
| **Min Cap** field | The minimum storage capacity across all disks in the server, in megabytes. To specify a capacity, choose select and enter the minimum storage capacity. |
### Name | Description
--- | ---
Max Cap field | The maximum storage capacity allowed, in megabytes. To specify a capacity, choose select and enter the maximum storage capacity.
Per Disk Cap field | The minimum storage capacity per disk required, in gigabytes. To specify a capacity, choose select and enter the minimum capacity on each disk.
Units field | The number of units. To specify a capacity, choose select and enter the desired units.
Number of Flex Flash Cards field | The number of FlexFlash Cards. To specify a capacity, choose select and enter the desired units.
Disk Type field | The disk type. This can be one of the following:
  - Unspecified — Either disk type is acceptable.
  - HDD — The disk must be HDD.
  - SSD — The disk must be SSD (SATA or SAS).

---

**Step 12** (Optional) To use this policy to qualify servers according to the model of the server, do the following:

a) Click Create Server Model Qualifications.
b) In the Create Server Model Qualifications dialog box, enter a regular expression that the server model must match in the Model field.
c) Click OK.

**Step 13** (Optional) To use this policy to qualify servers according to power group, do the following:

a) Click Create Power Group Qualifications.
b) In the Create Power Group Qualifications dialog box, choose a power group from the Power Group drop-down list.
c) Click OK.

**Step 14** (Optional) To use this policy to qualify the rack-mount servers that can be added to the associated server pool, do the following:

a) Click Create Rack Qualifications.
b) In the Create Rack Qualifications dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Slot ID field</td>
<td>The first rack-mount server slot ID from which server pools associated with this policy can draw.</td>
</tr>
<tr>
<td>Number of Slots field</td>
<td>The total number of rack-mount server slots from which server pools associated with this policy can draw.</td>
</tr>
</tbody>
</table>
Step 15 Verify the qualifications in the table and correct if necessary.
Step 16 Click OK.

Deleting Server Pool Policy Qualifications

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies > Organization_Name.
Step 3 Expand the Server Pool Policy Qualifications node.
Step 4 Right-click the policy qualifications you want to delete and select Delete.
Step 5 If a confirmation dialog box displays, click Yes.

Deleting Qualifications from Server Pool Policy Qualifications

Use this procedure to modify Server Pool Policy Qualifications by deleting one or more sets of qualifications.

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies > Organization_Name.
Step 3 Expand the Server Pool Policy Qualifications node.
Step 4 Choose the policy you want to modify.
Step 5 In the Work pane, choose the Qualifications tab.
Step 6 To delete a set of qualifications:
   a) In the table, choose the row that represents the set of qualifications.
   b) Right-click the row and select Delete.
Step 7 Click Save Changes.

vNIC/vHBA Placement Policy Settings

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine the following:

- How the virtual network interface connections (vCons) are mapped to the physical adapters on a server.
• What types of vNICs or vHBAs can be assigned to each vCon.

Each vNIC/vHBA placement policy contains four vCons that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters and the vNICs and vHBAs are assigned to those vCons.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the type of server and the selected virtual slot mapping scheme, which can be Round Robin or Linear Ordered. For details about the available mapping schemes, see vCon to Adapter Placement, on page 282.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the Selection Preference for each vCon. This can be one of the following:

- **All**—All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- **Assigned Only**—vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- **Exclude Dynamic**—Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- **Exclude Unassigned**—Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.
- **Exclude usNIC**—Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

Note

- An SRIOV usNIC that is explicitly assigned to a vCon set to Exclude usNIC will remain assigned to that vCon.

If you do not include a vNIC/vHBA placement policy in the service profile, Cisco UCS Manager defaults to the Round Robin vCon mapping scheme and the All vNIC/vHBA selection preference, distributing the vNICs and vHBAs between the adapters based on the capabilities and relative capacities of each adapter.

**vCon to Adapter Placement**

Cisco UCS maps every vCon in a service profile to a physical adapter on the server. How that mapping occurs and how the vCons are assigned to a specific adapter in a server depends on the following:
vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers

In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme:

- **Round Robin**—Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default.
- **Linear Ordered**—Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.

vCon to Adapter Placement for All Other Supported Servers

For all other servers supported by Cisco UCS in addition to the N20-B6620-2 and N20-B6625-2 blade servers, the vCon assignment depends on the number of adapters in the server and the virtual slot mapping scheme.

<table>
<thead>
<tr>
<th>Number of Adapters</th>
<th>vCon1 Assignment</th>
<th>vCon2 Assignment</th>
<th>vCon3 Assignment</th>
<th>vCon4 Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adapter1</td>
<td>Adapter1</td>
<td>Adapter1</td>
<td>Adapter1</td>
</tr>
<tr>
<td>2</td>
<td>Adapter1</td>
<td>Adapter2</td>
<td>Adapter1</td>
<td>Adapter2</td>
</tr>
<tr>
<td>3</td>
<td>Adapter1</td>
<td>Adapter2</td>
<td>Adapter3</td>
<td>Adapter2</td>
</tr>
<tr>
<td>4</td>
<td>Adapter1</td>
<td>Adapter2</td>
<td>Adapter3</td>
<td>Adapter4</td>
</tr>
</tbody>
</table>

Round Robin is the default mapping scheme.
Table 3: vCon to Adapter Placement Using the Linear Ordered Mapping Scheme

<table>
<thead>
<tr>
<th>Number of Adapters</th>
<th>vCon1 Assignment</th>
<th>vCon2 Assignment</th>
<th>vCon3 Assignment</th>
<th>vCon4 Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adapter1</td>
<td>Adapter1</td>
<td>Adapter1</td>
<td>Adapter1</td>
</tr>
<tr>
<td>2</td>
<td>Adapter1</td>
<td>Adapter1</td>
<td>Adapter2</td>
<td>Adapter2</td>
</tr>
<tr>
<td>3</td>
<td>Adapter1</td>
<td>Adapter2</td>
<td>Adapter3</td>
<td>Adapter3</td>
</tr>
<tr>
<td>4</td>
<td>Adapter1</td>
<td>Adapter2</td>
<td>Adapter3</td>
<td>Adapter4</td>
</tr>
</tbody>
</table>

If you are using a vCon policy with two adapters in the Cisco UCS B440 M2 Blade Server, be aware of the following mapping:

- vCon 2 to adapter 1 maps first
- vCon 1 to adapter 2 maps second

vNIC/vHBA to vCon Assignment

Cisco UCS Manager provides two options for assigning vNICs and vHBAs to vCons through the vNIC/vHBA placement policy: explicit assignment and implicit assignment.

Explicit Assignment of vNICs and vHBAs

With explicit assignment, you specify the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned. Use this assignment option when you need to determine how the vNICs and vHBAs are distributed between the adapters on a server.

To configure a vCon and the associated vNICs and vHBAs for explicit assignment, do the following:

- Set the vCon configuration to any of the available options. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server. If a vCon is configured for All, you can still explicitly assign a vNIC or vHBA to that vCon.
- Assign the vNICs and vHBAs to a vCon. You can make this assignment through the virtual host interface placement properties of the vNIC or vHBA or in the service profile associated with the server.

If you attempt to assign a vNIC or vHBA to a vCon that is not configured for that type of vNIC or vHBA, Cisco UCS Manager displays a message advising you of the configuration error.

During service profile association, Cisco UCS Manager validates the configured placement of the vNICs and vHBAs against the number and capabilities of the physical adapters in the server before assigning the vNICs and vHBAs according to the configuration in the policy. Load distribution is based upon the explicit assignments to the vCons and adapters configured in this policy.

If the adapters do not support the assignment of one or more vNICs or vHBAs, Cisco UCS Manager raises a fault against the service profile.
You can specify the PCI order for the vHBA; however, the desired order works within a class of devices, such as vNICs or vHBAs and not across them. Within an adapter, vNICs are always placed ahead of the vHBAs.

**Implicit Assignment of vNICs and vHBAs**

With implicit assignment, Cisco UCS Manager determines the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned according to the capability of the adapters and their relative capacity. Use this assignment option if the adapter to which a vNIC or vHBA is assigned is not important to your system configuration.

To configure a vCon for implicit assignment, do the following:

- Set the vCon configuration to **All, Exclude Dynamic**, or **Exclude Unassigned**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server.
- Do not set the vCon configuration to **Assigned Only**. Implicit assignment cannot be performed with this setting.
- Do not assign any vNICs or vHBAs to a vCon.

During service profile association, Cisco UCS Manager verifies the number and capabilities of the physical adapters in the server and assigns the vNICs and vHBAs accordingly. Load distribution is based upon the capabilities of the adapters, and placement of the vNICs and vHBAs is performed according to the actual order determined by the system. For example, if one adapter can accommodate more vNICs than another, that adapter is assigned more vNICs.

If the adapters cannot support the number of vNICs and vHBAs configured for that server, Cisco UCS Manager raises a fault against the service profile.

**Implicit Assignment of vNICs in a Dual Adapter Environment**

When you use implicit vNIC assignment for a dual slot server with an adapter card in each slot, Cisco UCS Manager typically assigns the vNICs/vHBAs as follows:

- If the server has the same adapter in both slots, Cisco UCS Manager assigns half the vNICs and half the vHBAs to each adapter.
- If the server has one non-VIC adapter and one VIC adapter, Cisco UCS Manager assigns two vNICs and two vHBAs to the non-VIC adapter and the remaining vNICs and vHBAs to the VIC adapter.
- If the server has two different VIC adapters, Cisco UCS Manager assigns the vNICs and vHBAs proportionally, based on the relative capabilities of the two adapters.

The following examples show how Cisco UCS Manager would typically assign the vNICs and vHBAs with different combinations of supported adapter cards:

- If you want to configure four vNICs and the server contains two Cisco UCS M51KR-B Broadcom BCM57711 adapters (with two vNICs each), Cisco UCS Manager assigns two vNICs to each adapter.
- If you want to configure 50 vNICs and the server contains a Cisco UCS CNA M72KR-E adapter (2 vNICs) and a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs), Cisco UCS Manager assigns two vNICs to the Cisco UCS CNA M72KR-E adapter and 48 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter.
• If you want to configure 150 vNICs and the server contains a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs) and a Cisco UCS VIC-1240 Virtual Interface Card adapter (256 vNICs), Cisco UCS Manager assigns 50 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter and 100 vNICs to the Cisco UCS VIC-1240 Virtual Interface Card adapter.

 Exceptions to this implicit assignment occur if you configure the vNICs for fabric failover and if you configure dynamic vNICs for the server.

For a configuration that includes vNIC fabric failover where one adapter does not support vNIC failover, Cisco UCS Manager implicitly assigns all vNICs that have fabric failover enabled to the adapter that supports them. If the configuration includes only vNICs that are configured for fabric failover, no vNICs are implicitly assigned to the adapter that does not support them. If some vNICs are configured for fabric failover and some are not, Cisco UCS Manager assigns all failover vNICs to the adapter that supports them and a minimum of one nonfailover vNIC to the adapter that does not support them, according to the ratio above.

For a configuration that includes dynamic vNICs, the same implicit assignment would occur. Cisco UCS Manager assigns all dynamic vNICs to the adapter that supports them. However, with a combination of dynamic vNICs and static vNICs, at least one static vNIC is assigned to the adapter that does not support dynamic vNICs.

Creating a vNIC/vHBA Placement Policy

Procedure

Step 1  In the Navigation pane, click Servers.
Step 2  Expand Servers > Policies.
Step 3  Expand the node for the organization where you want to create the policy.
        If the system does not include multitenancy, expand the root node.
Step 4  Right-click vNIC/vHBA Placement Policies and choose Create Placement Policy.
Step 5  In the Create Placement Policy dialog box, do the following:
        a)  Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name for this placement policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td>
</tr>
</tbody>
</table>
Cisco UCS assigns virtual network interface connections (vCons) to the PCIe adapter cards in the server. Each vCon is a virtual representation of a physical adapter that can be assigned vNICs and vHBAs.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the selected virtual slot mapping scheme. This can be one of the following:

- **Round Robin** — In a server with two adapter cards, Cisco UCS assigns vCon1 and vCon3 to Adapter1, then assigns vCon2 and vCon4 to Adapter2.

  In a server with three adapter cards, Cisco UCS assigns vCon1 to Adapter1, vCon2 and vCon4 to Adapter2, and vCon3 to Adapter3.

  This is the default scheme.

- **Linear Ordered** — In a server with two adapter cards, Cisco UCS assigns vCon1 and vCon2 to Adapter1, then assigns vCon3 and vCon4 to Adapter2.

  In a server with three adapter cards, Cisco UCS assigns vCon1 to Adapter1 and vCon2 to Adapter2, then assigns vCon3 and vCon4 to Adapter3.

**Note**  
In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme:

- **Round Robin** — Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default.

- **Linear Ordered** — Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the Selection Preference for each vCon.

b) In the Selection Preference column for each Virtual Slot, choose one of the following from the drop-down list:
Deleting a vNIC/vHBA Placement Policy

Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Servers > Policies > Organization_Name.
Step 3 Expand the vNIC/vHBA Placement Policies node.
Step 4 Right-click the policy you want to delete and choose Delete.
Step 5 If a confirmation dialog box displays, click Yes.

Explicitly Assigning a vNIC to a vCon

Before you begin
Configure the vCons through a vNIC/vHBA placement policy or in the service profile with one of the following values:

- Assigned Only
- Exclude Dynamic
- Exclude Unassigned

If a vCon is configured for All, you can explicitly assign a vNIC or vHBA to that vCon. However, there is less control with this configuration.

Note An SRIOV usNIC that is explicitly assigned to a vCon set to Exclude usNIC will remain assigned to that vCon.

c) Click OK.
Procedure

**Step 1** In the Navigation pane, click Servers.

**Step 2** Expand Servers > Service Profiles.

**Step 3** Expand the node for the organization which contains the service profile whose vNICs you want to explicitly assign to a vCon.

If the system does not include multitenancy, expand the root node.

**Step 4** Expand Service_Profile_Name > vNICs.

**Step 5** Click on the vNIC that you want to explicitly assign to a vCon.

**Step 6** In the Work pane, click the General tab.

**Step 7** In the Virtual Host Interface Placement section, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Desired Placement drop-down list | The user-specified virtual network interface connection (vCon) placement for the vNIC. This can be one of the following:  
  • Any—Allows Cisco UCS Manager to determine the vCon to which the vNIC is assigned.  
  • 1—Explicitly assigns the vNIC to vCon1.  
  • 2—Explicitly assigns the vNIC to vCon2.  
  • 3—Explicitly assigns the vNIC to vCon3.  
  • 4—Explicitly assigns the vNIC to vCon4. |
| Actual Assignment field     | The actual vCon assignment of the vNIC on the server.                       |

If you attempt to assign a vNIC to a vCon that is not configured for that type of vNIC, Cisco UCS Manager displays a message box to advise you of the configuration error. You must either assign the vNIC to another vCon or change the vCon configuration in the service profile.

**Step 8** In the Order section, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Desired Order field   | The user-specified PCI order for the vNIC.  
  Enter an integer between 0 and 128. You cannot create more than 128 vNICs for a server. |
| Actual Order field    | The actual PCI order of the vNIC on the server.                              |

**Step 9** Click Save Changes.
Explicitly Assigning a vHBA to a vCon

Before you begin

Configure the vCons through a vNIC/vHBA placement policy or in the service profile with one of the following values:

- Assigned Only
- Exclude Dynamic
- Exclude Unassigned

If a vCon is configured for All, you can explicitly assign a vNIC or vHBA to that vCon. However, there is less control with this configuration.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Servers.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Expand Servers &gt; Service Profiles.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand the node for the organization which contains the service profile whose vHBAs you want to explicitly assign to a vCon. If the system does not include multitenancy, expand the root node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand Service_Profile_Name &gt; vHBAs.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click on the vHBA that you want to explicitly assign to a vCon.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Virtual Host Interface Placement section, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Desired Placement field | The user-specified virtual network interface connection (vCon) placement for the vHBA. This can be one of the following:  
  - Any—Allows Cisco UCS Manager to determine the vCon to which the vHBA is assigned.  
  - 1—Explicitly assigns the vHBA to vCon1.  
  - 2—Explicitly assigns the vHBA to vCon2.  
  - 3—Explicitly assigns the vHBA to vCon3.  
  - 4—Explicitly assigns the vHBA to vCon4. |
| Actual Assignment field | The actual vCon assignment of the vHBA on the server. |

If you attempt to assign a vHBA to a vCon that is not configured for that type of vHBA, Cisco UCS Manager displays a message box to advise you of the configuration error. You must either assign the vHBA to another vCon or change the vCon configuration in the service profile.
Step 8  
In the **Order** section, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desired Order</strong> field</td>
<td>The user-specified PCI order for the vHBA. Enter an integer between 0 and 128. You cannot create more than 128 vHBAs for a server.</td>
</tr>
<tr>
<td><strong>Actual Order</strong> field</td>
<td>The actual PCI order of the vHBA on the server.</td>
</tr>
</tbody>
</table>

Step 9  
Click **Save Changes**.

---

**Placing Static vNICs Before Dynamic vNICs**

For optimal performance, static vNICs and vHBAs should be placed before dynamic vNICs on the PCIe bus. Static vNICs refer to both static vNICs and vHBAs. Cisco UCS Manager Release 2.1 provides the following functionality regarding the order of static and dynamic vNICs:

- After upgrading to Cisco UCS Manager Release 2.1, if no change is made to existing service profiles (profiles that are defined in releases prior to Cisco UCS Manager Release 2.1), the vNIC order does not change.

- After an upgrade to Cisco UCS Manager Release 2.1, any vNIC-related change would reorder the vNIC map. As a result, all dynamic vNICs would be placed after the static vNICs.

- For newly created service profiles in Cisco UCS Manager Release 2.1, static vNICs are always ordered before dynamic vNICs.

- The above behavior is independent of the sequence of creating or deleting static or dynamic vNICs.

- For SRIOV-enabled service profiles, UCSM places the vNIC Physical Function(PF) before the corresponding Virtual Functions (VFs). This scheme guarantees that the VFs are placed close to the parent PF vNIC on the PCIe bus and BDFs are in successive incremental order for the VFs.

**Example**

**Beginning Device Order in Cisco UCS Manager Release 2.0:**
```
dyn-vNIC-1 1
dyn-vNIC-2 2
```

**New Device Order in Cisco UCS Manager Release 2.0 (Add 2 static vNICs):**
```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

**After upgrading to Cisco UCS Manager Release 2.1, (Before any vNIC-related change is made to the service profile.**)
```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```
New Device Order in Cisco UCS Manager Release 2.1 (Add 2 dynamic vNICs by changing the policy count from 2 to 4.)

\[
\begin{align*}
dyn\text{-vNIC-1} & \quad 3 \\
dyn\text{-vNIC-2} & \quad 4 \\
eth\text{-vNIC-1} & \quad 1 \\
eth\text{-vNIC-2} & \quad 2 \\
dyn\text{-vNIC-3} & \quad 5 \\
dyn\text{-vNIC-4} & \quad 6
\end{align*}
\]

**Dynamic vNICs as Multifunction PCIe Devices**

Cisco UCS Manager Version 2.1 provisions static vNICs as 0-function devices (new BUS for every static vNIC). Multifunction dynamic vNICs are placed from the new Bus-slot after the last static vNIC/vHBA.

---

**Note**

Cisco UCS Manager Version 2.1 supports the new StaticZero mode.

#### Table 4: Version Compatibility

<table>
<thead>
<tr>
<th>Cisco UCS Manager</th>
<th>Version 2.0</th>
<th>Version 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.4</td>
<td>Scheme: ZeroFunction / MultiFunction</td>
<td>Scheme: ZeroFunction / MultiFunction / StaticZero</td>
</tr>
<tr>
<td>Scheme: ZeroFunction</td>
<td>Static vNICs and Dynamic vNICs are on Bus [0-57], Function [0-7]. Bus 0, Function 0</td>
<td></td>
</tr>
<tr>
<td>Static and Dynamic vNICs are all on Bus [0-57], Function [0]</td>
<td>Bus 1, Function 0</td>
<td></td>
</tr>
<tr>
<td>&lt; ZeroFunction Mode &gt;</td>
<td>&lt; MultiFunction Mode &gt;</td>
<td></td>
</tr>
<tr>
<td>Upgrade from Balboa will not renumber BDFs (remain in ZeroFunction mode) until Bus &lt;= 57. Once devices exceed 58, switch to MultiFunction mode.</td>
<td>Upgrade from Cisco UCS Manager Version 2.0 will not renumber BDFs (remain in ZeroFunction / MultiFunction mode). Once devices exceed 58 or Platform specific maximum PCIe Bus number OR Change to SRIOV configuration, switch to StaticZero mode.</td>
<td></td>
</tr>
</tbody>
</table>
vNIC/vHBA Host Port Placement

After a vNIC/vHBA is assigned to a vCON, it can be placed on one of the host ports of specific adapters. You can either explicitly specify the host port for placement, or allow Cisco UCS Manager to automatically assign vNICs/vHBAs to host ports.

Note
You can perform vNIC/vHBA host port placement on servers that support Cisco UCS VIC 1340, and VIC 1380 adapters.

The host port placement of the vNIC/vHBA determines the order of the vNIC/vHBA on the adapter. The vNICs/vHBAs placed on the first host port will be enumerated first, followed by the vNICs/vHBAs on the second host port.

Configuring Host Port Placement

You can configure host port placement for vNICs on servers that support Cisco UCS VIC 1340 and VIC 1380 adapters, and the Cisco UCS VIC 1385 and Cisco UCS VIC 1387 adapters.

Procedure

Step 1
In the Navigation pane, click Servers.

Step 2
Expand Servers > Service Profiles.

Step 3
Select the service profile which is associated with the vNIC that you want to place on a host port.

Step 4
Expand Service_Profile_Name > vNICs

Step 5
Under the vNICs summary table, double-click the Admin Host Port value of the vNIC which you want to configure and select one of the following:
- Any—Allows Cisco UCS Manager to determine the host port to which the vNIC is assigned.
- 1—Explicitly assigns the vNIC to host port 1.
- 2—Explicitly assigns the vNIC to host port 2.

Actual Host Port displays the actual assignment of the vNIC on a host port. When this feature is not supported, this will appear as None.

Step 6
Click Save Changes.

CIMC Mounted vMedia

Using Scriptable vMedia

Cisco UCS Manager allows provisioning of vMedia devices iso images for remote UCS servers. Using Scriptable vMedia, you can programmatically mount an IMG or an ISO image on a remote server. CIMC mounted vMedia provide communications between other mounted media inside your datacenter with no
Creating a vMedia Policy

A vMedia policy is used to configure the mapping information for remote vMedia devices. Two vMedia devices and mappings for CD and HDD are allowed in a vMedia policy. You can configure one ISO and one IMG at a time. ISO configurations maps to a CD drive and IMG configurations maps to a HDD device.

Note
If you want to map a device to a remote folder, you must create an IMG and map it as a HDD device.

Before you begin
Make sure that you have access to the following:

• Remote vMedia Server
• vMedia Devices
Procedure

Step 1  In the Navigation pane, click Servers.

Step 2  Expand Servers > Policies.

Step 3  Expand the node for the organization where you want to create the policy.
       If the system does not include multitenancy, expand the root node.

Step 4  Right-click vMedia Policies and select Create vMedia Policy.

Step 5  In the Create vMedia Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the vMedia policy.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot</td>
</tr>
<tr>
<td></td>
<td>use spaces or any special characters other than - (hyphen), _ (underscore),</td>
</tr>
<tr>
<td></td>
<td>: (colon), and . (period), and you cannot change this name after the object</td>
</tr>
<tr>
<td></td>
<td>is saved.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the policy. We recommend including information about where</td>
</tr>
<tr>
<td></td>
<td>and when the policy should be used. Maximum 115 characters.</td>
</tr>
<tr>
<td>Retry on Mount Failure</td>
<td>Designates if the vMedia will continue mounting when a mount failure</td>
</tr>
<tr>
<td></td>
<td>occurs. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
</tbody>
</table>

   Note  The default setting is Yes. When Yes is selected the remote server will continue to try to mount the vMedia mount process until it is successful or you disable this option. If you select No, a warning message will appear indicating retry on mount failure will not work in case of mount failure.

Step 6  On the icon bar to the right of the table, click +.

Step 7  In the Create vMedia Mount dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the vMedia Mount policy.</td>
</tr>
<tr>
<td></td>
<td>This name can be between 1 and 16 alphanumeric characters. You cannot</td>
</tr>
<tr>
<td></td>
<td>use spaces or any special characters other than - (hyphen), _ (underscore),</td>
</tr>
<tr>
<td></td>
<td>: (colon), and . (period), and you cannot change this name after the object</td>
</tr>
<tr>
<td></td>
<td>is saved.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of remote vMedia you plan to mount. This can be:</td>
</tr>
<tr>
<td></td>
<td>• CDD—Scriptable vMedia CD.</td>
</tr>
<tr>
<td></td>
<td>• HDD—Scriptable vMedia HDD.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol to use when communicating with the remote server. Click one of the following radio buttons to indicate the protocol you want to use to communicate with the mounted remote server. This can be:  • NFS - Network Files System.  • CIFS - Common Internet File System.  • HTTP - Hypertext Transfer Protocol.  • HTTPS - Hypertext Transfer Protocol over Secure.</td>
</tr>
</tbody>
</table>
| Authentication Protocol | The protocol to use for authentication when you use CIFS as the protocol for communicating with the remote server. When you use any protocol other than CIFS, this field is not available. Select one of the following from the drop-down list to specify the authentication protocol.  • Default—NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2.  • None—No authentication is used  • Ntlm—NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2.  • Ntlmi—NTLMi security protocol. Use this option only when you enable Digital Signing in the CIFS Windows server.  • Ntlmssp—NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2.  • Ntlmsspi—NTLMSSP i protocol. Use this option only when you enable Digital Signing in the CIFS Windows server.  • Ntlmv2—NTLMv2 security protocol. Use this option only with Samba Linux.  • Ntlmv2i—NTLMv2i security protocol. Use this option only with Samba Linux.  

**Note** The authentication protocol options are available only when you select CIFS as the protocol. For all other protocols, the Authentication Protocol field is disabled.  

| Hostname/IPAddress   | Enter the IP address or hostname of the location where the backup file is to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.  

If you use a hostname, you must configure Cisco UCS Manager to use a DNS server. The hostname (DNS) can be used when **Inband** network is configured for that server.  

---

**Creating a vMedia Policy**
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Name Variable</strong></td>
<td>The name to be used for the image. This can be:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—Filename must be entered in the Remote File field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Service Profile Name</strong>—Filename automatically becomes the name of the service profile that the vMedia Policy is associated with.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• If you select <strong>Service Profile Name</strong> as the Image Name variable, the Remote File field is disabled.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Service Profile Name</strong> as the Image Name variable, do not rename the service profile. Renaming the service profile can result in vMedia mount failure.</td>
</tr>
<tr>
<td><strong>Remote File</strong></td>
<td>Enter the full path to the ISO or other image file.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Ensure that the full path to the file begins with “/” after the share name.</td>
</tr>
<tr>
<td></td>
<td>This field can contain the filename [with the file extension] only.</td>
</tr>
<tr>
<td><strong>Remote Path</strong></td>
<td>Enter the share name on the remote server, for example “Share”.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username that Cisco UCS Manager should use to log in to the remote server.</td>
</tr>
<tr>
<td></td>
<td>This field does not apply if the protocol is NFS. This field is optional if the protocol is HTTP.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password associated with the username.</td>
</tr>
<tr>
<td></td>
<td>This field does not apply if the protocol is NFS. This field is optional if the protocol is HTTP.</td>
</tr>
</tbody>
</table>

**Step 8**

Click **OK**.

The remote server details are listed in the **vMedia Mounts** area of the **Create vMedia Mount** dialog box.

---

**What to do next**

Create a vMedia boot policy.

**Adding a vMedia Policy to a Service Profile**

Before you can use Scriptable vMedia, you must add the vMedia and Boot Policies to a Service Profile. After the vMedia and Boot Policies are added to a service profile you can associate the service profile with a Cisco UCS server. The following procedure describes how to add a vMedia policy to a Service Profile.

**Before you begin**

Configure the vMedia Policy you want to add to a service profile.
**Procedure**

**Step 1**  
In the Navigation pane, click Servers.

**Step 2**  
Expand Servers > Service Profiles.

**Step 3**  
Expand the node for the organization where you want to create the service profile.  
If the system does not include multitenancy, expand the root node.

**Step 4**  
Right-click the organization and select Create Service Profile (expert).  
The Unified Computing System Manager pane displays.

**Step 5**  
In the Name field, enter a unique name that you can use to identify the service profile.  
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.  
This name must be unique within the organization or sub-organization in which you are creating the service profile.

**Step 6**  
From the UUID Assignment drop-down list, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Select (pool default used by default)** | Assigns a UUID from the default UUID Suffix pool.  
Continue with Step 8.                                                                                                                                                           |
| **Hardware Default**                | Uses the UUID assigned to the server by the manufacturer.  
If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.  
Continue with Step 8.                                                                                                                                                           |
| **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX** | Uses the UUID that you manually assign.  
Continue with Step 7.                                                                                                                                                           |
| **Pools Pool_Name**                 | Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list.  
Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.  
If you do not want use any of the existing pools, but instead want to create a pool that all |
**Viewing CIMC vMedia Policy**

**Before you begin**

vMedia Policies are configured.
Procedure

Step 1 In the Navigation pane, click Servers.
Step 2 Expand Policies > vMedia Policies.
Step 3 Expand the vMedia Policies node to view the list of vMedia Policies.
Step 4 Double-click the name of a vMedia policy to view the properties for the selected vMedia Mount.
On the Properties page, you can modify the properties used for the vMedia Mounts.
Firmware Upgrades

Beginning with Cisco UCS Manager Release 3.1, Cisco is releasing unified Cisco UCS Manager software and firmware upgrades for each of the following platforms with every release of Cisco UCS Manager:

- Cisco UCS 6300 Series Fabric Interconnect with Cisco UCS B-Series, C-Series, and S-Series Servers
- Cisco UCS 6200 Series Fabric Interconnect with Cisco UCS B-Series, C-Series, and S-Series
- Cisco UCS 6324 Fabric Interconnect with Cisco UCS B-Series Servers and C-Series Servers, which is also known as UCS Mini

You can upgrade the firmware through Auto Install, packages in service profiles, using the firmware automatic synchronization server policy, and directly at endpoints. For more information on guidelines and installing firmware, see the Cisco UCS Firmware Management Guide.

Verifying Firmware Versions on Components

Procedure

1. In the Navigation pane, click Equipment.
2. In the Work pane, click the Firmware Management tab.
3. On the Installed Firmware tab, review the firmware versions listed for each component.

For more information on guidelines and installing firmware, see the Cisco UCS Firmware Management Guide.
Overview of Cisco UCS Manager Diagnostics

The Cisco UCS Manager diagnostics tool enables you to verify the health of the hardware components on your servers. The diagnostics tool provides a variety of tests to exercise and stress the various hardware subsystems on the servers, such as memory and CPU. You can use the tool to run a sanity check on the state of your servers after you fix or replace a hardware component. You can also use this tool to run comprehensive burn-in tests before you deploy a new server in your production environment.

When a system is new, a default diagnostics policy is created in org scope. This default policy is named default and it cannot be deleted. The user will receive an error message if they try to delete it. The default diagnostic policy is the preferred way to execute the same set of tests across all servers. Any diagnostic policy, including the default can be customized.

The default policy only has one memory test. The default parameters of the memory test can be modified. In addition, the memory test within the default diagnostics policy can be deleted. If it does not have a memory test, the diagnostic policy will not run.

Creating a Diagnostics Policy

Before you begin

You must have admin privileges to perform this task.

Procedure

Step 1 Navigate to Servers > Policies > Diagnostics Policies.
Step 2 Click Add.

Step 3 Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the diagnostics policy. The character limit is 16.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the diagnostics policy. This is optional.</td>
</tr>
</tbody>
</table>

Step 4 Click Next.

Step 5 Click Add.

Step 6 Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>The order in which the tests will be executed.</td>
</tr>
<tr>
<td>CPU Filter</td>
<td>Sets the CPU filter to all CPUs or to a specified CPU.</td>
</tr>
<tr>
<td>Loop Count</td>
<td>Sets the loop count to the specified iterations. The range is from 1-1000.</td>
</tr>
<tr>
<td>Memory Chunk Size</td>
<td>Sets the memory chunk to 5mb-chunk or big-chunk.</td>
</tr>
<tr>
<td>Memory Size</td>
<td>Sets the memory size to a specific value.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Sets the memory test to butterfly, killer, prbs, prbs-addr, or prbs-killer.</td>
</tr>
</tbody>
</table>

Step 7 Click OK.

Step 8 Click Finish.

---

**Diagnostics Test on a Blade Server**

**Starting a Diagnostics Test on a Blade Server**

**Before you begin**

You must have admin privileges to perform this task.

**Procedure**

Step 1 Navigate to Equipment > Chassis > Server.

Step 2 Choose the server for which you want to start the diagnostics test.

Step 3 Click on the Diagnostics tab.
Stopping a Diagnostics Test on a Blade Server

Procedure

Step 1 Navigate to Equipment > Chassis > Server.
Step 2 Choose the server for which you want to stop the diagnostics test.
Step 3 Click on the Diagnostics tab.
Step 4 Click Stop. Once the diagnostic text has stopped, the button will be grayed out.

Starting a Diagnostics Tests on All Servers

Note
Starting diagnostics testing all servers will cause a reboot of each individual server.

Before you begin
You must have admin privileges to perform this task.

Procedure

Step 1 Navigate to Equipment > Diagnostics.
Step 2 Click Start. Once the diagnostics test has started, the link will be grayed out.
In the Diagnostic Result table, you can view the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The system-defined server name.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The unique identifier for the chassis. This numeric identifier is assigned based on the location of the chassis within the system.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not applicable for rack servers.</td>
</tr>
<tr>
<td>PID</td>
<td>The server model PID.</td>
</tr>
<tr>
<td>Overall Progress Percentage</td>
<td>A description of the overall progress percentage of the diagnostics test on the server.</td>
</tr>
</tbody>
</table>
Stopping a Diagnostics Tests on All Servers

Before you begin
You must have admin privileges to perform this task.

Procedure

Step 1 Navigate to Equipment > Diagnostics.
Step 2 Click Stop. Once the diagnostics test has stopped, the link will be grayed out.

Viewing the Server Diagnostics Status/Result

Before you begin
You can run the diagnostic test on individual servers through CLI and view the status on this page.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 Expand Equipment > Chassis > Servers.
Step 3 Choose the server for which you want to view the diagnostic status and then click the Diagnostics tab.

You can view the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic Policies</td>
<td>Enables the user to select a diagnostics policy and apply it to a specific server.</td>
</tr>
<tr>
<td>Start/Stop</td>
<td>Enables the user to start or stop a diagnostics test on a specific server.</td>
</tr>
<tr>
<td>Operation State</td>
<td>The server's diagnostics operation status. Possible values are Idle, In-Progress, Completed, Failed, and Cancelled.</td>
</tr>
</tbody>
</table>
### Table 5: Diagnostic Result

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSM Status Descr</td>
<td>A brief description of the current task in the server's diagnostics operation.</td>
</tr>
<tr>
<td>FSM Progress</td>
<td>The overall progress of the diagnostics operation being executed on the server.</td>
</tr>
<tr>
<td>Test Overall Progress</td>
<td>The overall progress of the diagnostics test.</td>
</tr>
<tr>
<td>Error Description</td>
<td>A description of the error returned from the diagnostics operation.</td>
</tr>
</tbody>
</table>

### Diagnostics Troubleshooting

<table>
<thead>
<tr>
<th>Issue</th>
<th>Steps to Debug</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the BIOS detects a bad DIMM, the DIMM is disabled and is not visible to the Diagnostics operation.</td>
<td>Refer to memory-related faults in addition to the diagnostics operation results.</td>
</tr>
<tr>
<td>If the DIMM blacklisting feature is enabled and a DIMM is blacklisted, it is not visible to the Diagnostics operation.</td>
<td>Refer to memory-related faults in addition to the diagnostics operation results.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>The Diagnostics operation may not execute successfully, if the server has bad DIMMs which prevent the server from booting.</td>
<td>NA</td>
</tr>
<tr>
<td>The Diagnostics operation can fail, if an uncorrectable error causes a server reboot.</td>
<td>NA</td>
</tr>
<tr>
<td>A Diagnostics operation failure can occur if there are memory errors that cause the Diagnostics operation to hang.</td>
<td>NA</td>
</tr>
<tr>
<td>The Diagnostics operation can be interrupted by external events, such as a managed endpoint failover or a critical UCSM process restart. In these cases, the Diagnostics operation is cancelled and the Memory Tests are marked as failed.</td>
<td>The failure is triggered by external events. Retry the Diagnostics operation.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| **A Memory test fails with the error: Uncorrectable errors detected.** | **Check for server faults under the Chassis/Server/Faults tab.**  
See the SEL logs for the DIMM errors under the Chassis/Server/SEL Logs tab. |
| **A Memory test failure needs further analysis.** | **See the diagnostics operation logs in following log file archive on the primary FI in the /workspace path:**  
diagnostics/diag_log_<system-name>_<timestamp>_<chassis-id>_<blade-id>  
**See the analysis file:** tmp/ServerDiags/MemoryPmem2.<id>/MemoryPmem2.analysis  
**Use the following command to find the diagnostics logs with the analysis files:**  
```bash  
# for file in `ls /workspace/diagnostics/*diag*`; do tar -tzvf $file | grep analysis & echo "IN " $file; done  
``` |