



Cisco UCS S3260 Server Integration with Cisco UCS Manager, Release 4.3

First Published: 2023-08-16

Last Modified: 2023-11-14

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

PREFACE

Preface	ix
Audience	ix
Conventions	ix
Related Cisco UCS Documentation	xi
Documentation Feedback	xi

CHAPTER 1

New and Changed Information	1
New and Changed Information for This Release	1

CHAPTER 2

Overview	3
About the Cisco UCS S3260 System	3
How to Use This Guide	5
Cisco UCS S3260 System Architectural Overview	7
Connectivity Matrix	8
Deployment Options	9
Management Through Cisco UCS Manager	11
Server SIOC Connectivity Functionality	12
New SIOC with PCIe Slots	14

CHAPTER 3

Migration to UCSM-Managed Cisco UCS S3260	19
Migration to UCSM Managed Cisco UCS S3260	19
Migrating Standalone 3260 to UCSM Managed 3260	20
Prerequisites for Migrating Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260	20
Booting From Chassis HDD	20
Migrating from Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260	21

Migrating from Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260 [2.0(13) or later version] 22

System IP Addresses 23

Configuring Server Ports Using Cisco UCS Manager 24

Migrating from UCSM Managed Cisco UCS S3260 to Standalone Cisco UCS S3260 25

CHAPTER 4

Equipment Related Policies 27

Chassis Discovery Policy 27

 Configuring the Chassis/FEX Discovery Policy 28

Chassis Connectivity Policy 29

 Configuring a Chassis Connectivity Policy 31

CHAPTER 5

Chassis Profiles 33

Chassis Profiles in Cisco UCS Manager 33

Guidelines and Recommendations for Chassis Profiles 34

Creating a Chassis Profile with the Wizard 34

Renaming a Chassis Profile 35

Cloning a Chassis Profile 36

Deleting a Chassis Profile 37

Chassis Profile Association 37

 Associating a Chassis Profile with a Chassis 37

 Disassociating a Chassis Profile from a Chassis 38

Chassis Profile Template 38

 Chassis Profile Templates 38

 Creating a Chassis Profile Template 39

 Creating One or More Chassis Profiles from a Chassis Profile Template 40

 Creating a Chassis Profile Template from a Chassis Profile 40

 Cloning a Chassis Template Profile 41

 Changing the Maintenance Policy for a Chassis Profile Template 42

 Binding a Chassis Profile to a Chassis Profile Template 42

 Unbinding a Chassis Profile from a Chassis Profile Template 43

Chassis Maintenance Policy 43

 Creating a Chassis Maintenance Policy 43

 Changing the Maintenance Policy for a Chassis Profile 44

Deleting a Chassis Maintenance Policy	45
Compute Connection Policy	45
Creating a Compute Connection Policy	45
Associating a Compute Connection Policy to Chassis Profile	46

CHAPTER 6**Storage 47**

Storage Server Features and Components Overview	47
Cisco UCS S3260 Storage Management Operations	54
Disk Sharing for High Availability	55
Disk Zoning Policies	55
Creating a Disk Zoning Policy	56
Creating Disk Slots and Assigning Ownership	59
Associating Disk Zoning Policies to Chassis Profile	60
Disk Migration	61
Storage Enclosure Operations	62
Removing Chassis Level Storage Enclosures	62
Sas Expander Configuration Policy	63
Creating Sas Expander Configuration Policy	63
Deleting a Sas Expander Configuration Policy	65

CHAPTER 7**Firmware Management 67**

Firmware Management for Cisco UCS S3260 Systems	67
Chassis Firmware Upgrade through Auto Install	68
Upgrading the Chassis Firmware with Auto Install	68
Firmware Upgrades through Chassis Firmware Packages in Chassis Profiles	71
Chassis Firmware Package	71
Stages of a Firmware Upgrade through Chassis Firmware Packages in Chassis Profiles	72
Effect of Updates to Firmware Packages in Chassis Profiles	73
Creating a Chassis Firmware Package	74
Updating a Chassis Firmware Package	75
Adding Chassis Firmware Packages to an Existing Chassis Profile	76
Upgrading a UCS Domain with Cisco UCS S3260 Servers	76
Direct Firmware Upgrade on S3260 Chassis and Server Endpoints	77
Direct Firmware Upgrade on Chassis Endpoints	78

Updating the CMC Firmware on a S3260 Chassis	78
Updating the Chassis Adapter Firmware on a S3260 Chassis	79
Updating the SAS Expander Firmware on a S3260 Chassis	79
Activating the SAS Expander Firmware on a S3260 Chassis	80
Activating the CMC Firmware on a S3260 Chassis	81
Activating the Chassis Adapter Firmware on a S3260 Chassis	81
Activating the Chassis Board Controller Firmware on a S3260 Chassis	81
Direct Firmware Upgrade on Server Endpoints	82
Updating the CIMC Firmware on a Cisco UCS S3260 Server Node	82
Activating the CIMC Firmware on a Cisco UCS S3260 Server Node	83
Updating the BIOS Firmware on a Cisco UCS S3260 Server Node	83
Activating the BIOS Firmware on a Cisco UCS S3260 Server Node	84
Activating the Board Controller Firmware on a Cisco UCS S3260 Server Node	85
Activating the Storage Controller Firmware on a Cisco UCS S3260 Server Node	85

CHAPTER 8

Chassis Management 87

The Cisco UCS S3260 Chassis	87
Acknowledging a Chassis	88
Decommissioning a Chassis	88
Removing a Chassis	89
Turning on the Locator LED for a Chassis	89
Turning off the Locator LED for a Chassis	89
Creating a Zoning Policy from Inventory	90
Viewing the POST Results for a Chassis	90

CHAPTER 9

Server Management 93

Cisco UCS S3260 Server Node Management	93
Booting a Cisco UCS S3260 Server Node	94
Booting a Cisco UCS S3260 Server Node from the Service Profile	94
Determining the Boot Order of a Cisco UCS S3260 Server Node	95
Shutting Down a Cisco UCS S3260 Server Node	95
Shutting Down a Cisco UCS S3260 Server Node from the Service Profile	96
Resetting a Cisco UCS S3260 Server Node	96
Resetting a Cisco UCS S3260 Server Node to Factory Default Settings	97

Reacknowledging a Cisco UCS S3260 Server Node	98
Removing a Cisco UCS S3260 Server Node from a Chassis	98
Deleting the Inband Configuration from a Cisco UCS S3260 Server Node	99
Decommissioning a Cisco UCS S3260 Server Node	99
Recommissioning a Cisco UCS S3260 Server Node	100
Reacknowledging a Server Slot in a S3260 Chassis	100
Removing a Non-Existent Cisco UCS S3260 Server Node from the Configuration Database	101
Turning the Locator LED for a Cisco UCS S3260 Server Node On and Off	102
Turning the Local Disk Locator LED on a Cisco UCS S3260 Server Node On and Off	102
Resetting the CIMC for a Cisco UCS S3260 Server Node	103
Resetting the CMOS for a Cisco UCS S3260 Server Node	103
Resetting the BIOS Password for a S3X60 Server	104
Issuing an NMI from a Cisco UCS S3260 Server Node	104
Viewing the POST Results for a Cisco UCS S3260 Server Node	104
Viewing Health Events for a Cisco UCS S3260 Server Node	105
Health LED Alarms	107
Viewing Health LED Alarms	107

CHAPTER 10
SIOC Management 109

SIOC Management in Cisco UCS Manager	109
SIOC Removal or Replacement	109
Acknowledging an SIOC	110
Migrating to SIOC with PCIe Support	111
Resetting the CMC	111
CMC Secure Boot	111
Guidelines and Limitations for CMC Secure Boot	112
Enabling CMC Secure Boot	112



Preface

- [Audience, on page ix](#)
- [Conventions, on page ix](#)
- [Related Cisco UCS Documentation, on page xi](#)
- [Documentation Feedback, on page xi](#)

Audience

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

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in this font . Main titles such as window, dialog box, and wizard titles appear in this font .
Document titles	Document titles appear in <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <code>this font</code> .
System output	Terminal sessions and information that the system displays appear in <code>this font</code> .
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	Elements in square brackets are optional.

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



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



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



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](#).

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.



CHAPTER 1

New and Changed Information

- [New and Changed Information for This Release, on page 1](#)

New and Changed Information for This Release

This section provides information on new features and changed behavior in Cisco UCS Manager, Release 4.3.

Table 1: New Features and Changed Behavior in Cisco UCS Manager, 4.3(2c)

Feature	Description	Where Documented
Support Cisco UCS X-Series Server	Cisco UCS Manager supports Cisco UCS X410c M7 Compute Node. Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers.	—

The following table provides an overview of the significant changes to this guide for this current release.

Table 2: New Features and Changed Behavior in Cisco UCS Manager, 4.3(2b)

Feature	Description	Where Documented
Deprecated support for Cisco UCS S3260 M4 server.	Cisco UCS Manager support for Cisco UCS S3260 M4 server is deprecated.	—
Deprecated support for Cisco UCS 6200 series Fabric Interconnect.	Cisco UCS Manager support for Cisco UCS 6200 Series Fabric Interconnect is deprecated.	—



CHAPTER 2

Overview

- [About the Cisco UCS S3260 System, on page 3](#)
- [How to Use This Guide, on page 5](#)
- [Cisco UCS S3260 System Architectural Overview, on page 7](#)
- [Connectivity Matrix , on page 8](#)
- [Deployment Options, on page 9](#)
- [Management Through Cisco UCS Manager, on page 11](#)
- [Server SIOC Connectivity Functionality, on page 12](#)
- [New SIOC with PCIe Slots, on page 14](#)

About the Cisco UCS S3260 System

The Cisco UCS S3260 is a dense storage rack server with dual server nodes, optimized for large data sets used in environments such as Big data, cloud, object storage, and content delivery. It belongs to the Cisco UCS S-Series rack-mount servers product family.

Beginning with Cisco UCS Manager Release 3.1(3), Cisco UCS C3260/C3X60 is renamed to Cisco UCS S3260. You may still see certain components in the system labeled as C3260/C3X60. For this release, the terms S3260 and C3260/C3X60 are used interchangeably. Both, S3260 and C3260/C3X60, refer to the same hardware component.

Cisco UCS Manager Release 3.2(3) introduces Cisco UCS S3260 M5 server. Cisco UCS S3260 M5 server integrates with Cisco UCS Manager the same way Cisco UCS S3260 does. The information and procedures in this document can be used for Cisco UCS S3260 M5 servers.

The Cisco UCS S3260 system is designed to operate in a non-cluster environment and as part of the Cisco Unified Computing System with Cisco UCS Manager integration. It assumes almost the same characteristics of its predecessor, Cisco UCS C3160, but with the following additional features:

- System IO Controllers (SIOC) with Cisco VIC 1300 and 1400 Series Embedded Chip supporting 10/25/40/100G speeds.
- Support of up to two server modules
- Capability to operate in a non-cluster setup and with Cisco UCS Manager
- Individual hard disk drives (HDD) can be assigned to either server in the dedicated or shared mode

In addition, one of the server slots in the Cisco UCS S3260 system can be utilized by a storage expansion module for an additional four 3.5" drives. The server modules can also accommodate two solid state drives (SSD) for internal storage dedicated to that module. The chassis supports Serial Attached SCSI (SAS) expanders that can be configured to assign the 3.5" drives to individual server modules.

Beginning with release 3.1(3), Cisco UCS S3260 system supports the following:

- Server SIOC Connectivity functionality
- Second RAID controller in the optional I/O expander module
- Dual HBA Controller



Note If a Cisco UCS S3260 system has Dual HBA Controller then you cannot downgrade Cisco UCS Manager to any release earlier than 3.1(3).

In a Cisco UCS S3260 system, both servers should have either dual RAID controllers or dual HBA controllers. Mixing the controller types is not supported.

Cisco UCS S3260 system supports Server SIOC Connectivity functionality. Using this functionality, you can configure the data path through both the primary and auxiliary SIOCs when the chassis has single server and dual SIOCs set up. For more details, see [Server SIOC Connectivity Functionality, on page 12](#).

Cisco UCS S3260 system supports Second RAID controller in the optional I/O expander module that attaches to the top of the server node. You cannot downgrade Cisco UCS Manager, BMC, CMC, and BIOS to any release earlier than 3.1(3) depending on the number of disk zoned to the controllers :

Controller Configuration	Is Downgrade Possible?
Two controllers in the server (one in optional I/O expander) or one controller in the server (in optional I/O expander) and at least one disk is zoned to the controller in the optional I/O expander.	No
Two controllers in the server (one in optional I/O expander) or one controller in the server (in optional I/O expander) and at least one disk is pre-provisioned to controller in the optional I/O expander.	No
Two controllers in the server (one in optional I/O expander) or one controller in the server (in any slot) and disk are not zoned or pre-provisioned to the controller in optional I/O expander.	Yes

License Requirement

Beginning with release 4.2(3b), for Cisco UCS 6536 Fabric Interconnect (UCS-FI-6536), all ports are enabled using a term-based subscription license (Supported license term: 36-60 months).



Note Licensing for FI 6536 is not a port-based license like in previous FI generations.

ETH_PORT_ACTIVATION_PKG (/6400 FI series), 40G_ETH_PORT_ACTIVATION_PKG (for 6400 and 6300 FI - 6332), 10G_PORT_ACTIVATION_PKG (for 6300 FI - 6332-16UP), licenses are used when S3260 system is connected to FI as appliance (appliance port) or Cisco UCS Manager managed node (server port).

For more information on license requirement, refer *Server License Management* chapter in *Cisco UCS Manager Server Management Guide*.

How to Use This Guide

Cisco UCS S3260 systems managed through Cisco UCS Manager support most of the features that are supported by other S-Series Rack Servers managed through Cisco UCS Manager. Cisco UCS S3260 systems also introduce some new features and management capabilities to Cisco UCS Manager. These features and management capabilities are detailed in the following chapters of this guide:

- **Overview**—Provides detailed information about the architecture of the Cisco UCS S3260 system and its connectivity when managed through Cisco UCS Manager.
- **System Related Policies**—Describes the chassis discovery policy and chassis connectivity policy that are applicable to Cisco UCS S3260 systems.
- **Chassis Profiles**—Provides detailed information about Chassis Profiles and Chassis Profile Templates, which can now be used to define the storage, firmware and maintenance characteristics of a Cisco UCS S3260 chassis.
- **Storage Management**—Describes the new storage components in a Cisco UCS S3260 system, and how to manage them.
- **Firmware Management**—Provides detailed information about Chassis Firmware Packages and the endpoints of Cisco UCS S3260 on which firmware can be updated manually.
- **Chassis Management**—Provides detailed information about the management of the Cisco UCS S3260 chassis.
- **Server Management**—Provides detailed information about the management of the Cisco UCS S3260 Server Node.
- **SIOC Management**—Provides detailed information about the management of the System Input/Output controllers (SIOCs) that are part of a Cisco UCS S3260 chassis.

All features and configuration tasks that are supported by Cisco UCS Manager Release 3.1 and later releases are described in the configuration guides that are listed in the following table. These guides must be used with this quick reference guide for Cisco UCS S3260 systems.

Guide	Description
Cisco UCS Manager Getting Started Guide	Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration and configuration best practices.

Guide	Description
Cisco UCS Manager Administration Guide	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.
Cisco UCS Manager Infrastructure Management Guide	Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.
Cisco UCS Manager Firmware Management Guide	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.
Cisco UCS Manager Server Management Guide	Discusses the new licenses, registering Cisco UCS domain with Cisco UCS Central, power capping, server boot, server profiles, and server-related policies.
Cisco UCS Manager Storage Management Guide	Discusses all aspects of storage management, such as SAN and VSAN in Cisco UCS Manager.
Cisco UCS Manager Network Management Guide	Discusses all aspects of network management, such as LAN and VLAN connectivity in Cisco UCS Manager.
Cisco UCS Manager System Monitoring Guide	Discusses all aspects of system and health monitoring, including system statistics in Cisco UCS Manager.
Cisco UCS S3260 Server Integration with Cisco UCS Manager	Discusses all aspects of management of UCS S-Series servers that are managed through Cisco UCS Manager.

The [Release Notes for Cisco UCS Manager, Release 4.1](#) has detailed information about new features, resolved caveats, open caveats, and workarounds for Cisco UCS Manager, Release 4.1.

Cisco UCS S3260 System Architectural Overview

Architectural Overview

Figure 1: Cisco UCS S3260 System Overall Architecture Diagram

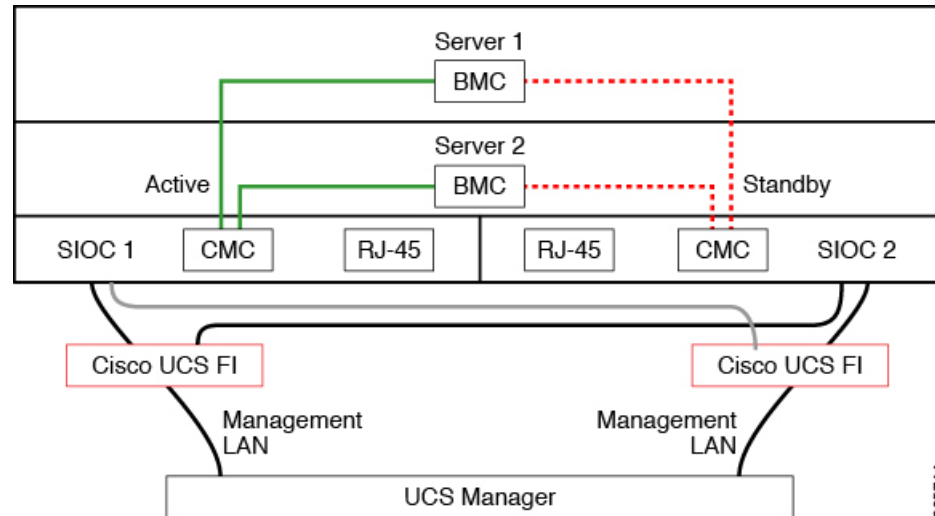
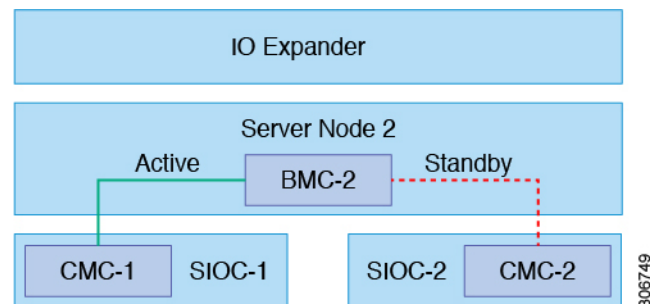


Figure 2: Cisco UCS S3260 System (with Single node Dual SIOC) Overall Architecture Diagram



The system uses a chassis management controller (CMC) to manage the server nodes. Each system I/O controller (SIOC) module contains an onboard CMC. If you have two SIOCs, the two CMCs act in an active/standby organization. The CMC in the SIOC that you log into with the Cisco IMC interface becomes the active CMC and it allows you to manage the BMCs in both server nodes.

All user interfaces run only on the active CMC. Configuration changes are automatically synchronized between the active and the standby CMCs.

When you power-cycle the system, the CMC in SIOC 1 is the active CMC by default. The active CMC will fail over to the standby CMC when any of the following conditions occur:

- The active CMC is rebooted or fails.
- The SIOC with active CMC is removed.
- Network connectivity is lost on the active CMC.

Building Blocks and Connectivity

The Cisco UCS S3260 chassis has a modular architecture consisting of the following modules:

Base Chassis

Contains four power supplies, eight fans, and a rail kit.

Server Node

One or two server nodes, each with two CPUs, 128, 256, or 512 GB of DIMM memory, and a RAID card in pass-through mode or a RAID card with a 1 GB or 4 GB cache.

System I/O Controller (SIOC) (Release 4.0(1) onwards)

Beginning with release 4.0(1), Cisco UCS S3260 system supports a new server SIOC UCS-S3260-PCISIOC with S3260 M5 servers. This SIOC has PCIe slots to replace the network adapters.

System I/O Controller (SIOC) (Release 3.2(3) and earlier)

One or two System I/O Controllers, each of which includes a 1300 series VIC. The Cisco UCS S3260 SIOC has an integrated Cisco UCS VIC 1300 Series chip onboard, so there is no removable adapter card.

Optional Drive Expansion Node

Choice of either 4 x 4 TB drives (total capacity: 16TB), 4 x 6 TB drives (total capacity: 24 TB), or 4 x 10 TB drives (total capacity: 40TB).

Solid-State Boot Drives

Up to two SSDs per server node.

Cisco UCS Fabric Connectivity

The Cisco UCS S3260 chassis can be connected in one of the following ways:

- Direct connection to the fabric interconnects.
- Connectivity using FEX.

Direct Connection to Cisco UCS Fabric Interconnects

1. **Cisco UCS 6300 Series Fabric Interconnects:** The SIOC uplink can be connected directly to a 6300 Series FI port through a single 40G connection.
2. **Cisco UCS 6400 Series Fabric Interconnect:** The SIOC uplink can be connected directly to a Cisco UCS 6400 Series Fabric Interconnect port through a single 25G connection.
3. **Cisco UCS 6536 Fabric Interconnect:** The SIOC uplink can be connected directly to a Cisco UCS 6536 Fabric Interconnect port through a single 25G connection.

Connectivity Matrix

New Cisco VIC Card

Beginning with release 4.0(2a), Cisco UCS S3260 system supports the following new Cisco VIC card:

- Cisco UCS VIC 1495

Beginning with release 4.0(1a), Cisco UCS S3260 system supports the following new Cisco VIC card:

- Cisco UCS VIC 1455

Table 3: Connectivity Matrix

	Cable	Link Aggregation	Connection Speed	FEX Support	6300 Series FI Support	6400 Series FI Support	6500 Series (6536) FI Support
VIC 1495 (with new generation SIOC)	QSFP	Non Port-Channel	40G	No	Yes	No	Yes
VIC 1455 (with new generation SIOC)	SPF+	Port-Channel	2x10G	Yes	Yes	Yes	Yes
	Breakout Cable	Port-Channel	2x10G	No	Yes	No	Yes
	SFP28	Port-Channel	2x25G	No	No	Yes	Yes
SIOC	QSA (SFP+)	Non Port-Channel	10G	Yes	No	Yes	Yes
	QSFP	Non Port-Channel	40G	No	Yes	No	Yes
	Breakout Cable	Port-Channel	4x10G	No	No	Yes	Yes



Note With VIC 1455 (with new generation SIOC), there are 4 ports for integration to UCS fabric interconnects. Ports 1 and 2 should be connected to FI-A, and Ports 3 and 4 should be connected to FI-B, otherwise the server discovery fails. (For example, if Port 1 is connected to FI-A and Port 2 is connected to FI-B, the server discovery fails.)

Deployment Options

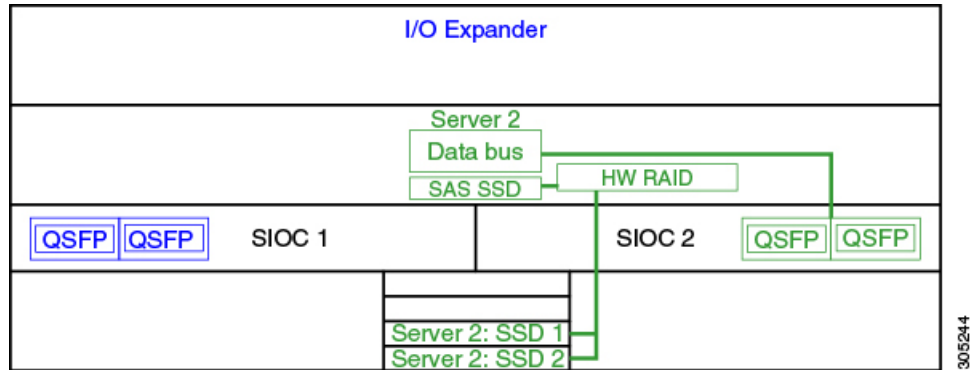
The following sections describe the three main deployment options for Cisco UCS S3260 systems—single and dual server connectivity.

Single Server Connectivity

The following illustration shows the associations for a single-server system:

- The data bus in server node 2 connects through SIOC 2.
- Server 2 SSDs 1 and 2 can be controlled by a RAID controller card in server node 2.

Figure 3: Single Server with I/O Expander



Single Server Connectivity (with Server SIOC Connectivity Functionality)

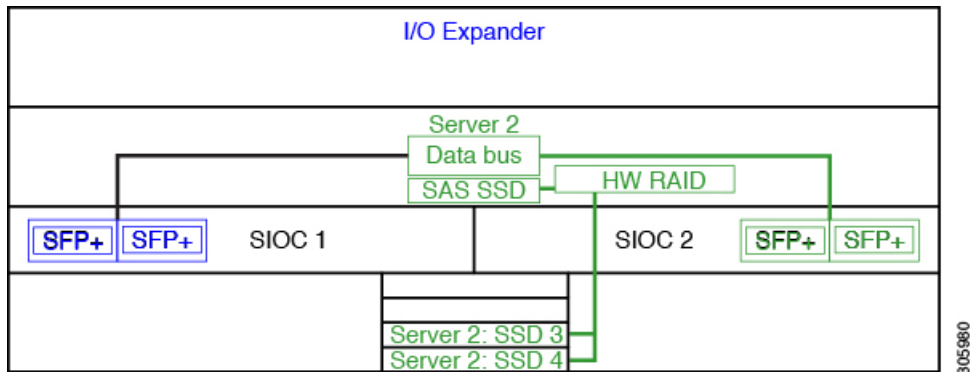
When a Cisco UCS S3260 system has single server and dual SIOCs, users can enable the Server SIOC Connectivity functionality. The following illustration shows the associations for a single-server system with Server SIOC Connectivity functionality enabled:

- The data bus in server node 2 connects through both the primary and auxiliary SIOCs.



Note Primary SIOC for server 1 is SIOC 1 and for Server 2 is SIOC 2. Auxiliary SIOC for server 1 is SIOC 2 and for server 2 is SIOC 1.

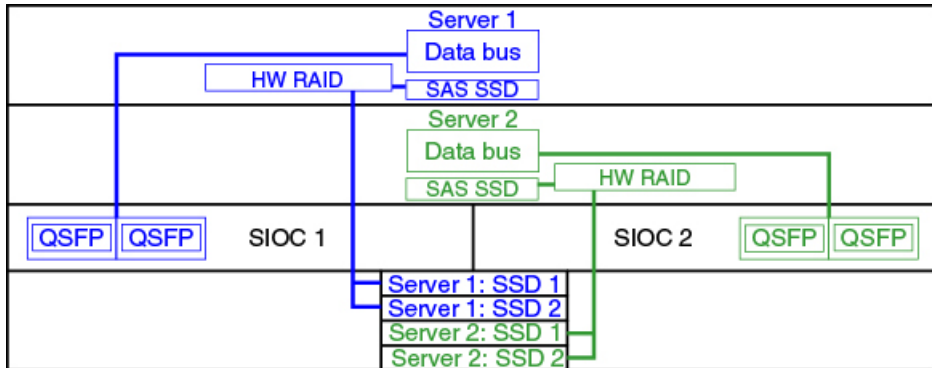
Figure 4: Single Server Single SIOC with Server SIOC Connectivity Functionality



Dual Server Connectivity

In this mode of deployment, each server slot contains an independent server blade. The redundant server nodes along with the various components such as SAS SSDs provide high availability.

Figure 5: Dual Server System



305403



Important

For detailed information on storage controller considerations for a Cisco UCS S3260 system such as storage controllers supported for the various server nodes and the associated service notes, please refer to the "Storage Controllers" section in the *Cisco UCS S3260 Storage Server Installation and Service Guide*.

Management Through Cisco UCS Manager

The Cisco UCS S3260 system can operate in either standalone mode or can be managed by Cisco UCS Manager.



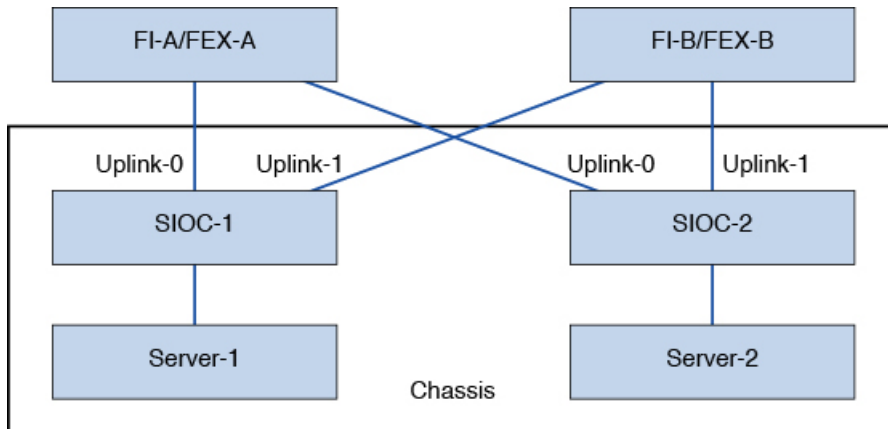
Note

UCS mini 6324 does not support Cisco UCS Manager integration of Cisco UCS S3260.

Dual Server Connectivity

The following illustration describes the connectivity for a Cisco UCS S3260 system with dual servers managed by Cisco UCS Manager:

Figure 6: Cisco UCS S3260 System with Cisco UCS Manager



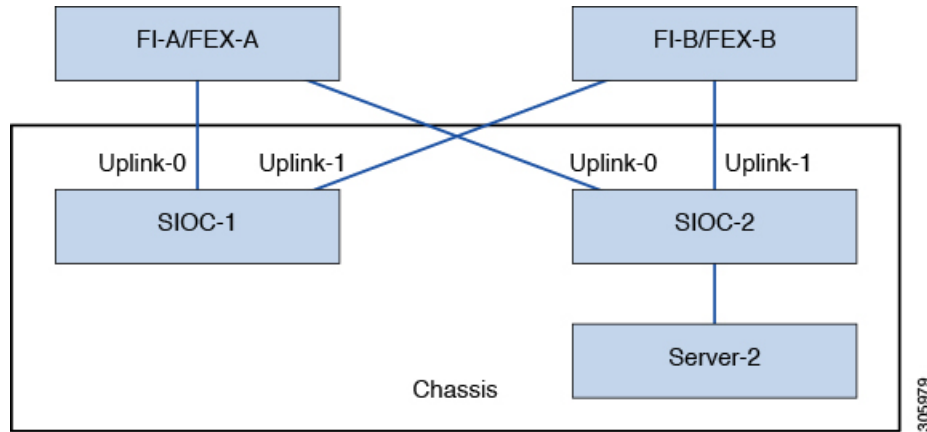
305305

The 40G ports on the SIOCs can be connected to either a fabric interconnects or a FEX module. On each SIOC, one port can be connected to the primary fabric interconnect/FEX and the other port can be connected to the subordinate fabric interconnect/FEX. Traffic from each SIOC can reach fabric interconnects and FEXs.

Single Server and Single SIOC Connectivity

The following illustration describes the connectivity for a Cisco UCS S3260 system with single server and single SIOC managed by Cisco UCS Manager without Server SIOC Connectivity functionality :

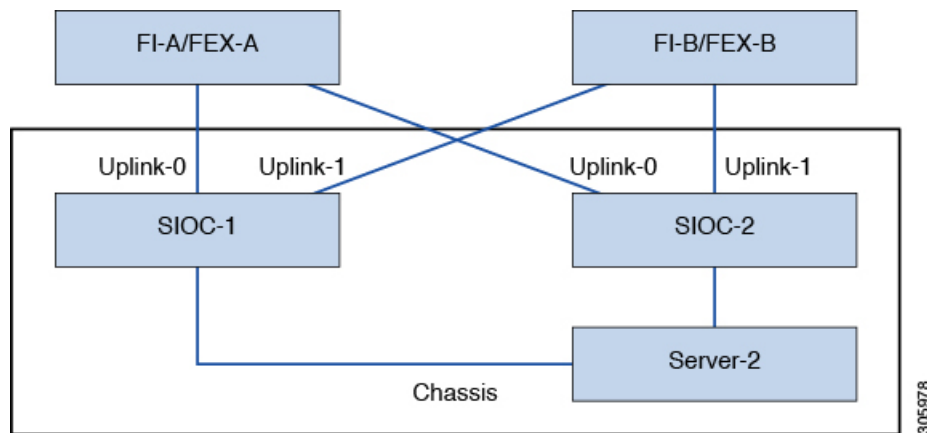
Figure 7: Cisco UCS S3260 System with Cisco UCS Manager (Single Server Single SIOC without Server SIOC Connectivity Functionality)



Single Server and Dual SIOC Connectivity (with Server SIOC Connectivity Functionality)

The following illustration describes the connectivity for a Cisco UCS S3260 system with single server and dual SIOCs managed by Cisco UCS Manager with the Server SIOC Connectivity functionality:

Figure 8: Cisco UCS S3260 System with Cisco UCS Manager (Single Server Single SIOC with Server SIOC Connectivity Feature)



Server SIOC Connectivity Functionality

Beginning with release 3.1(3), Cisco UCS S3260 system supports Server SIOC Connectivity functionality. Using this functionality, you can configure the data path through both the primary and auxiliary SIOCs when the chassis has single server and dual SIOCs set up.



Note Primary SIOC for server 1 is SIOC 1 and for Server 2 is SIOC 2. Auxiliary SIOC for server 1 is SIOC 2 and for server 2 is SIOC 1.

You can configure Server SIOC Connectivity functionality through chassis profile using **Compute Conn Policy** by selecting **single-server-dual-sioc** option.

Prerequisites for Server SIOC Connectivity Functionality

This functionality works only under the following conditions:

- Cisco UCS S3260 system is running release 3.1(3) or later.
- Associated BIOS, BMC and CMC firmware are running 3.1(3) or later.
- Chassis has single server and dual SIOCs.

Workflow - Cisco UCS Manager Upgrade

After Cisco UCS Manager is upgraded to release 3.1(3) or later release, chassis discovery is triggered and UCSM gets the operational state of Server SIOC Connectivity feature. User can now enable the feature using the **single-server-dual-sioc** option available for **Compute Conn Policy** under chassis profile.



Note Any change to Compute Connection Policy settings raises a pending-event. Chassis profile association starts automatically only after you acknowledge the pending-event.

In GUI, once **Compute Conn Policy** property is set to **single-server-dual-sioc**, then Cisco UCS Manager displays a message, warning that this operation causes server reboot. After acknowledging the message, chassis association is triggered. When Server SIOC Connectivity configuration is successfully deployed, Cisco UCS Manager automatically triggers server deep discovery.

In CLI, once **Compute Conn Policy** property is set to **single-server-dual-sioc**, run the **apply pending-changes immediate** command to start association.

Once **Compute Conn Policy** is set to **single-server-dual-sioc**, you cannot downgrade Cisco UCS Manager to any release earlier than 3.1(3). Similarly, Cisco UCS Manager prevents BMC, CMC, and BIOS downgrade to any release earlier than 3.1(3).

Conditions Impacting the Functionality when single-server-dual-sioc Option is Enabled

- Server Replacement - When the server is replaced, the blade slot mismatch is detected. When you acknowledge the slot, server deep discovery is triggered followed by service profile association. When service profile association is triggered, then there can be the following two situations:
 1. When BIOS/BMC firmware is specified in the host firmware. If the BIOS/BMC firmware support Single Server Dual SIOC connectivity, then the service profile association process continues. If the BIOS/BMC firmware do not support Single Server Dual SIOC connectivity, then the association raises a config-issue.

- When BIOS/BMC firmware is not specified in the host firmware. Cisco UCS Manager checks if the running BIOS/BMC version support Single Server Dual SIOC connectivity. If the feature is not supported, then a config-issue is raised.

- SIOC Replacement - If the replaced SIOC is running 3.1(3) or later, then a user acknowledgment message is displayed when one of the SIOC is seated. Once you acknowledge SIOC action, then Cisco UCS Manager establishes the connectivity between the FI and the SIOC. In addition to that Cisco UCS Manager re-acknowledges the server that has the data path connectivity through this SIOC. The VNICs configured for the server are also re-acknowledged. See [SIOC Removal or Replacement, on page 109](#) for more information.

If the replaced SIOC is running an earlier firmware version, then Cisco UCS Manager automatically changes the **Server SIOC Connectivity** operational state to **single-server-single-sioc**. You may update the firmware of the replaced SIOC by re-triggering chassis profile association.

- SIOC Removal - When any SIOC is removed, Cisco UCS Manager marks the SIOC and the corresponding adapter unit created under the server as missing.
- Adding Server in Chassis - When a new server is added in the chassis with this functionality enabled, then server discovery fails.
- Chassis/Server Disassociation - Server SIOC Connectivity functionality is not disabled if a server or chassis is disassociated.

New SIOC with PCIe Slots

Beginning with Cisco UCS Manager release 4.0(1a), Cisco UCS S3260 systems support a new server SIOC, UCS-S3260-PCISIOC, with S3260 M5 servers. This SIOC has PCIe slots to replace the network adapters (See [Table 4: Supported Cisco VIC and Third-party Adapters, on page 15](#) for supported adapters). These slots support both Cisco VIC and third-party adapters. In addition, the new SIOC has two NVME slots.

Beginning with Cisco UCS Manager release 4.0(2a), NVMe OOB is supported.

Figure 9: FI Connectivity with New SIOC

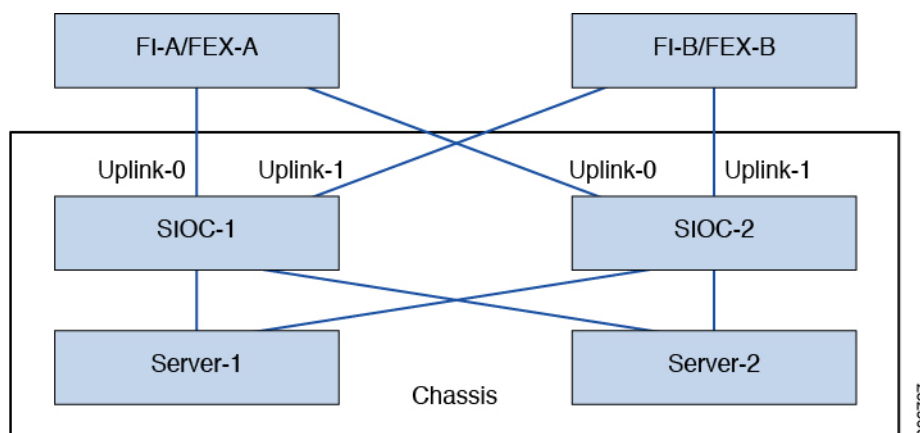


Table 4: Supported Cisco VIC and Third-party Adapters

PID	Description
UCSC-PCIE-C25Q-04	Cisco VIC 1455 Quad port – 25G
UCSC-PCIE-ID10GC	Intel X550 dual-port 10GB Base-T
UCSC-PCIE-ID25GF	Intel XXV710 dual-port 25G SFP28
UCSC-PCIE-ID40GF	Intel XL710 dual-port 40GB QSFP+ NIC
UCSC-PCIE-QD16GF	Qlogic QLE2692 dual-port 16G Fibre Channel HBA

Table 5: Supported NVMe Disks

PID	Description
UCS-S3260-NVG25	UCS S3260 500GB NVMe for M5 Server Node based on Intel 4501
UCS-S3260-NVG210	UCS S3260 1TB NVMe for M5 Server Node based on Intel 4501
UCS-S3260-NVG220	UCS S3260 2TB NVMe for M5 Server Node based on Intel 4501

Prerequisites for Installing New SIOC

- BMC firmware version should be 4.0(1a) or higher.
- CMC firmware version should be 4.0(1a) or higher.

Limitations for Cisco VIC Cards, Third-party Adapters, and NVMe Disks

- The SIOC with the third-party adapter can be set only as standby.
- If you reboot the active SIOC, it does not cause the SIOC attached to the third-party adapter to become active.
- Cisco UCS Manager does not support a setup with mixed SIOCs. You cannot mix new gen SIOCs and old SIOCs in a setup.
- Cisco UCS Manager does not manage the SIOC that has a third-party adapter in it.
- Cisco UCS Manager does not update or activate the CMC image of the SIOC that has a third-party adapter.
- Hot insertion and removal of NVMe disks are not supported.
- For more details on Cisco and third-party adapters support, see [Cisco UCS Manager Management for Mixed Adapter Set-up, on page 16](#).

Cisco UCS Manager Management for Mixed Adapter Set-up

Table 6: Cisco UCS Manager Management

Slot 1	Slot 2	Server SIOC Connection	Cisco UCS Manager Management
Cisco VIC	Cisco VIC	Single Server Dual VIC	Cisco UCS Manager provides full support
Cisco VIC	Cisco VIC	Dual Server Mode	Cisco UCS Manager provides full support
Cisco VIC	Third-party Adapter	Single Server Dual VIC	Cisco UCS Manager provides partial support: <ul style="list-style-type: none"> • Discovery and firmware management for third-party adapter • CMC redundancy is not supported in case of SIOC/VIC failure
Cisco VIC	Third-party Adapter	Dual Server	Cisco UCS Manager provides partial support: <ul style="list-style-type: none"> • Discovery of server in slot 1 • CMC redundancy is not supported in case of SIOC/VIC failure • Discovery of server in slot 2 is not supported in Cisco UCS Manager mode. If there is a server in slot 2, Cisco UCS Manager discovery fails with the No Connected Adapters error.

Slot 1	Slot 2	Server SIOC Connection	Cisco UCS Manager Management
Third-party Adapter	Cisco VIC	Single Server Dual VIC	Cisco UCS Manager provides partial support: <ul style="list-style-type: none"> Discovery and firmware management for third-party adapter CMC redundancy is not supported in case of SIOC/VIC failure
Third-party Adapter	Cisco VIC	Dual Server	Cisco UCS Manager provides partial support: <ul style="list-style-type: none"> Discovery of server in slot 2 CMC redundancy is not supported in case of SIOC/VIC failure Discovery of server in slot 1 is not supported in Cisco UCS Manager mode. If there is a server in slot 1, Cisco UCS Manager discovery fails with the No Connected Adapters error.
Third-party Adapter	Third-party Adapter	Single Server Dual VIC	Not supported
Third-party Adapter	Third-party Adapter	Dual Server	Not supported

SIOC Removal or Replacement

You can remove or replace an SIOC from a chassis. Removal or replacement of an SIOC is a service-affecting operation, which requires you to power down the entire chassis. See [SIOC Removal or Replacement, on page 109](#) for more information.

Migrating to New SIOC with PCIe Support

See [Migrating to SIOC with PCIe Support, on page 111](#) for more information. Once you migrate to new SIOC, the following downgrade restrictions are applied:

- You cannot downgrade Cisco UCS Manager to any release below 4.0(1a)
- You cannot downgrade BMC firmware to any release below 4.0(1a)

Server SIOC Connectivity Functionality

Cisco UCS Manager continues to support single server dual VIC functionality with the new SIOC with the following exceptions:

- The support is extended to third-party adapters connected to the new SIOC
- Once you change the **Compute Connection Policy** property to **single-server-dual-sioc**, the server is powered down before the policy is applied.
- Single server dual SIOC only decides the allocation of the adapter in the SIOC, it does not allocate the NVME disk slots in the SIOC. One NVMe disk is allocated per server and SIOC NVME connections to the servers are fixed.



CHAPTER 3

Migration to UCSM-Managed Cisco UCS S3260

- [Migration to UCSM Managed Cisco UCS S3260, on page 19](#)
- [Migrating Standalone 3260 to UCSM Managed 3260, on page 20](#)
- [Migrating from UCSM Managed Cisco UCS S3260 to Standalone Cisco UCS S3260, on page 25](#)

Migration to UCSM Managed Cisco UCS S3260



Note Direct migration of Cisco UCS C3160 to UCSM managed Cisco UCS S3260 is not supported. First migrate standalone Cisco UCS C3160 to standalone Cisco UCS S3260 and then to UCSM managed Cisco UCS S3260.

Migrating Standalone Cisco UCS C3160 to UCSM Managed Cisco UCS S3260

To migrate standalone Cisco UCS C3160 to UCSM Managed Cisco UCS S3260:

1. Standalone Cisco UCS C3160 to Standalone Cisco UCS Cisco UCS S3260
2. Standalone Cisco UCS Cisco UCS S3260 to UCSM managed Cisco UCS S3260
3. Configure Server Ports Using Cisco UCS Manager

Migrating Standalone Cisco UCS Cisco UCS S3260 to UCSM Managed Cisco UCS S3260

To migrate standalone Cisco UCS Cisco UCS S3260 to UCSM Managed Cisco UCS S3260:

1. Standalone Cisco UCS Cisco UCS S3260 to UCSM managed Cisco UCS S3260
2. Configure Server Ports Using Cisco UCS Manager

Migrating Standalone 3260 to UCSM Managed 3260

Prerequisites for Migrating Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260

Ensure that the following conditions are met before starting the migrating procedure:

- For M5 server, download and run the Cisco UCS S3260 Host Upgrade Utility (HUU) for release 3.2(3) or later. Use the Host Upgrade Utility User Guide for release 3.2(3) or later for instructions on downloading and using the utility, see the instructions in the guide for your release: [HUU Guides](#).
- Up to five IP addresses, either configured in your DHCP server or manually entered for static IP addresses. See [System IP Addresses, on page 23](#) for more information.
- It is recommended to make a note of the existing system configurations before migrating to UCSM managed Cisco UCS S3260. These configurations can include the following:
 - Server UUID
 - Storage configuration
 - Network configuration
 - Boot policy
 - Number of vNICs
 - vNIC placements
 - MAC addresses
 - MTU

You can create these configurations again using Cisco UCS Manager after the migration.

- If the system boot volume is created out of chassis HDD, then perform [Booting From Chassis HDD, on page 20](#).

Booting From Chassis HDD

Before you begin

Before migrating to UCSM Managed Cisco UCS S3260, perform this procedure only if the system boot volume is created out of chassis HDD.

Procedure

-
- Step 1** Associate the chassis with a chassis profile in which **Disk Zoning Policy** is set to **Preserve Config**.

For more information, see *Creating a Chassis Profile with the Wizard* for GUI procedure or *Creating a Chassis Profile* for CLI procedure.

Step 2 Within the service profile for the server, create a storage profile with a LUN using the **Prepare Claim Local LUN** option.

Note the name of the LUN. For more information on storage profiles, see http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/3-1/b_UCSM_GUI_Storage_Management_Guide_3_1/b_UCSM_GUI_Storage_Management_Guide_3_1_chapter_010000.html#d1049e1627a1635.

Step 3 After associating the service profile, go to the storage profile on the service profile and select **Reclaim orphaned LUN** and choose the LUN (LUN on the chassis HDDs) for reclaim.

Step 4 In the boot policy, define the local LUN with the same name as noted in step 2.

What to do next

Proceed to [Migrating from Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260, on page 21](#).

Migrating from Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260



Important If the system is running an earlier version than 2.0(13), perform the following procedure to migrate standalone Cisco UCS S3260 to UCSM managed Cisco UCS S3260.

Procedure

- Step 1** Use the Cisco UCS S3260 HUU for 2.0(13) to upgrade the entire system to Cisco IMC release 2.0(13). Run the HUU for all the server nodes in Cisco UCS S3260 system.
- Step 2** Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
- Step 3** Connect a keyboard and monitor to the system:
- Connect a KVM cable (Cisco PID N20-BKVM) to the external KVM connector on the server node at the rear of the system.
 - Connect a VGA monitor and a USB keyboard to the connectors on the KVM cable.
- Step 4** Connect power cords and then power on the system. Watch for the prompt to press F8.
- Step 5** When prompted, press **F8** to enter the Cisco IMC Configuration Utility.
- Step 6** Configure the networking properties for your desired IP addresses, NIC mode, and NIC redundancy.
- Be aware of the Cisco UCS S3260 system requirement to set as many as five IP addresses. See [System IP Addresses, on page 23](#) for more information. At this point in the procedure, the system requires three addresses:
 - One management IP address

- One CMC address for the each SIOC
- One BMC address for each server nodes

Note If you use a DHCP server, the addresses are defined by the DHCP server. If you disable DHCP, you must set your own static management IP addresses and network settings.

- Make networking settings using the Cisco IMC Configuration Utility, which you opened by pressing F8 during boot. See *Setting Up the System Using the Cisco IMC Configuration Utility* at http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/s/hw/S3260/install/S3260.html.
- If you want to set static IP addresses for the CMC and BMC controllers, you will be directed to use the Cisco IMC management interface. See *Setting Static CMC and BMC Internal IP Addresses* at http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/s/hw/S3260/install/S3260.html.

Step 7 Upgrade the remaining system components to Cisco IMC release 2.0(13) or later by using the Cisco UCS Host Upgrade Utility.

Use the Host Upgrade Utility User Guide for release 2.0(13) or later for instructions on downloading and using the utility: [HUU Guides](#)

After the upgrade completes, Cisco UCS S3260 system is ready for UCSM integration.

Step 8 Watch for the prompt to press F8 and when prompted, press **F8** to enter the Cisco IMC Configuration Utility.

Step 9 Refer [Resetting Cisco IMC to Factory Defaults](#) to set the server to factory defaults or perform the following steps to use the utility to set the server controller to factory defaults:

- Press **F1** to go to the second screen of the utility.
- Select the **Chassis Controller Configuration** option under Factory Default. **Do not** select **Server Controller Configuration**.
- Press **F10** to save changes and reboot the BMC.
- Wait for the reboot to complete (approximately five minutes).

Step 10 Connect the 40G ports on the SIOCs to either a fabric Interconnect or a FEX module.

On each SIOC, one port is attached to FI-A/FEX-A and the other port is attached to FI-B/FEX-B. Traffic from each SIOC can reach both FIs/FEXs. Refer [Cisco UCS S3260 System Architectural Overview, on page 7](#).

What to do next

Configure the server ports. Refer [Configuring Server Ports Using Cisco UCS Manager, on page 24](#).

Migrating from Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260 [2.0(13) or later version]



Important

If the system is already running 2.0(13) or later version, perform the following procedure to migrate standalone Cisco UCS S3260 to UCSM managed Cisco UCS S3260.

Procedure

- Step 1** Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
- Step 2** Connect a keyboard and monitor to the system:
- Connect a KVM cable (Cisco PID N20-BKVM) to the external KVM connector on the server node at the rear of the system.
 - Connect a VGA monitor and a USB keyboard to the connectors on the KVM cable.
- Step 3** Connect power cords and then power on the system. Watch for the prompt to press F8.
- Step 4** When prompted, press **F8** to enter the Cisco IMC Configuration Utility.
- Step 5** Refer [Resetting Cisco IMC to Factory Defaults](#) to set the server to factory defaults or perform the following steps to use the utility to set the server controller to factory defaults:
- Press **F1** to go to the second screen of the utility.
 - Select the **Chassis Controller Configuration** option under Factory Default. **Do not** select **Server Controller Configuration**.
 - Press **F10** to save changes and reboot the BMC.
 - Wait for the reboot to complete (approximately five minutes).
- Step 6** Connect the 40G ports on the SIOCs to either a fabric Interconnect or a FEX module.
- On each SIOC, one port is attached to FI-A/FEX-A and the other port is attached to FI-B/FEX-B. Traffic from each SIOC can reach both FIs/FEXs. Refer [Cisco UCS S3260 System Architectural Overview](#), on page 7.
-

What to do next

Configure the server ports. Refer [Configuring Server Ports Using Cisco UCS Manager](#), on page 24.

System IP Addresses

A Cisco UCS S3260 system can have up to five IP addresses:



- Note** All controllers present in the system must have IP addresses assigned in order to communicate with each other. All IP addresses can be assigned by your DHCP server, or you can assign static IP addresses.
- Management IP—This is the overall system virtual IP address. You log into this address when you access the system's Cisco IMC interface through your LAN connection to the active chassis management controller in SIOC 1 or SIOC 2.
 - SIOC 1 CMC IP—This is the internal address for the chassis management controller (CMC) in SIOC 1. This address can be assigned by your DHCP server or you can set a static address by using the Cisco IMC interface.

- SIOC 2 CMC IP—This is the internal address for the CMC in SIOC 2 (if installed). This address can be assigned by your DHCP server or you can set a static address by using the Cisco IMC interface.
- Server 1 BMC IP—This is the internal address for the board management controller (BMC) in server node 1. This address can be assigned by your DHCP server or you can set a static address by using the Cisco IMC interface.
- Server 2 BMC IP—This is the internal address for the BMC in server node 2 (if installed). This address can be assigned by your DHCP server or you can set a static address by using the Cisco IMC interface.

Configuring Server Ports Using Cisco UCS Manager

Perform the following procedure to configure Ethernet ports as server ports. After the ports are configured as server ports, the migration process is complete.



Note If the Ethernet ports connected to standalone Cisco UCS S3260 were already configured as appliance ports, then re-configure them as server ports.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment** > **Fabric Interconnects** > *Fabric_Interconnect_Name* > **Fixed Module** > **Ethernet Ports**.
 - Step 3** Click a port under the **Ethernet Ports** node.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Actions** area, click **Reconfigure**.
 - Step 6** From the drop-down list, choose **Configure as Server Port**.
-

What to do next

This completes the migration process. Cisco UCS Manager automatically discovers the S3260 Chassis. [Chassis Discovery Policy, on page 27](#) provides more information about chassis discovery. [Server Management](#) provides more information how to use the Cisco UCS Manager to manage the server.

You can recreate configurations that existed in the standalone Cisco UCS S3260 by using Cisco UCS Manager. Cisco UCS Manager configuration guides listed under [How to Use This Guide, on page 5](#) provide detailed information.

Migrating from UCSM Managed Cisco UCS S3260 to Standalone Cisco UCS S3260

Procedure

- Step 1** Decommission the chassis. See *Decommissioning a Chassis* procedure in *Chassis Management* chapter.
- Step 2** Disconnect the SIOC cables.
-

What to do next

This completes the migration process. The chassis can now be used in standalone mode. For further configuration, see the Configuration guides for Cisco UCS S3260 system to manage the server. Cisco UCS S3260 system configuration guides are located at: <http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html>.



CHAPTER 4

Equipment Related Policies

- [Chassis Discovery Policy, on page 27](#)
- [Chassis Connectivity Policy, on page 29](#)

Chassis Discovery Policy

The chassis discovery policy determines how the system reacts when you add a new Cisco UCS S3260 chassis or an existing standalone Cisco UCS S3260 chassis to a Cisco UCS system. [Cisco UCS S3260 System Architectural Overview, on page 7](#) describes the connectivity for a Cisco UCS S3260 system managed by Cisco UCS Manager. Cisco UCS Manager uses the settings in the chassis discovery policy to determine whether to group links from the system I/O controllers (SIOCs) to the fabric interconnects in fabric port channels.

To add a previously standalone Cisco UCS S3260 chassis to a Cisco UCS system, you must first configure it to factory default. You can then connect both SIOCs on the chassis to both fabric interconnects. After you connect the SIOCs on the chassis to the fabric interconnects, and mark the ports as server ports, chassis discovery begins.



Note Chassis/IOM acknowledgement after chassis/FEX discovery policy changes is not applicable for S3260 chassis.

Server Discovery

Cisco UCS Manager automatically discovers the Cisco UCS S3260 server nodes after the Cisco UCS S3260 chassis is discovered.



Note Server discovery fails if the SIOC corresponding to the server is not present.

Link Grouping

In release 4.0(1a), **Link Group Preference** is automatically set to **Port Channel** when using new SIOC with PCIe slots.



Note For the Cisco UCS 6400 Series Fabric Interconnect, and Cisco UCS 6536 Fabric Interconnect, the **Link Group Preference** is always set to **Port Channel**.

When you connect a Cisco UCS S3260 chassis through a FEX to directly to a Cisco UCS 6300 Series fabric interconnect, or Cisco UCS 6400 Series Fabric Interconnect, and Cisco UCS 6536 Fabric Interconnect, Cisco UCS Manager ignores the **Port Channel** preference and the SIOCs operate in the non-port channel mode.

Set the link grouping preference to **None** if the Cisco UCS S3260 chassis is connected to a fabric interconnect through a single 10G cable.

After changing the **Link Group Preference** value in the Cisco UCS Manager GUI, Decommission and then Recommission the Cisco UCS S3260 chassis for the change to take effect.

In the Cisco UCS domain, if there are other chassis operating in **Port Channel** mode, do the following:

1. Discover the chassis in the Cisco UCS system with the **Link Group Preference** set to **Port Channel**
2. Change the link aggregation preference for the Cisco UCS S3260 chassis through Chassis Connectivity Policy
3. Decommission the chassis
4. Recommission the chassis

Configuring the Chassis/FEX Discovery 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 **Chassis/FEX Discovery Policy** area, specify the action and the link grouping preference.
 - a. From the **Action** drop-down list, select the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.
 - b. For the **Link Grouping Preference** radio button, select whether the links from the IOMs or FEXes to the fabric interconnects are grouped in a port channel.

In release 4.0(1a), **Link Group Preference** is automatically set to **Port Channel** when using new SIOC with PCIe slots.

Note In a setup with Cisco UCS 6400 Series Fabric Interconnect, and Cisco UCS 6500 Series Fabric Interconnect, the **Link Grouping Preference** value for Chassis/FEX Discovery Policy is not user configurable. The value is set to **Port Channel**.
 - c. For the **Backplane Speed Preference** radio button, select the speed preference. The 40G backplane setting is not applicable for 22xx IOMs.

Step 6 Click **Save Changes**.

What to do next

To customize fabric port channel connectivity for a specific chassis, configure the chassis connectivity policy.

Chassis Connectivity Policy

The chassis connectivity policy determines whether a specific chassis is included in a fabric port channel after chassis discovery. This policy is helpful for users who want to configure one or more chassis differently from what is specified in the global chassis discovery policy.

By default, the chassis connectivity policy is set to global. This means that connectivity control is configured when the chassis is newly discovered, using the settings configured in the chassis discovery policy. Once the chassis is discovered, the chassis connectivity policy controls whether the connectivity control is set to none or port channel.



Note The chassis connectivity policy is created by Cisco UCS Manager only when the hardware configuration supports fabric port channels.

The following table displays the various connectivity and media type support for FC/FCoE.

Table 7: Connectivity and Media Type Support for FC/FCoE

FI	Connectivity	Supported	Port-Channel	FC/FCoE
Cisco UCS 6536 Fabric Interconnect	Direct Connect– 25 GB – QSA28	Yes	¹ SIOC (Non Port-Channel) ² New gen SIOC - No	Yes
Cisco UCS 6536 Fabric Interconnect	93180YC-FX3 (25G server ports)	Yes	SIOC - No New gen SIOC (Port-Channel)	Yes
Cisco UCS 6536 Fabric Interconnect	2348 UPQ (10G server ports)	Yes	SIOC - No New gen SIOC (Port-Channel)	Yes
Cisco UCS 6400 Series Fabric Interconnect	Direct Connect– 10 GB – QSA	Yes Not using Breakout	³ SIOC (Non Port-Channel) ⁴ New gen SIOC - No	Yes

FI	Connectivity	Supported	Port-Channel	FC/FCoE
Cisco UCS 6400 Series Fabric Interconnect	Direct Connect– 25G SFP 28	Yes Not using Breakout	SIOC - No New gen SIOC (Port-Channel)	Yes
Cisco UCS 6400 Series Fabric Interconnect	2232 FEX - 10 GB - QSA	Yes	SIOC (Non Port-Channel) New gen SIOC (Port-Channel)	Yes
Cisco UCS 6400 Series Fabric Interconnect	2232xx - 4x10 GB - Breakout Cable	Yes	SIOC (Port-Channel) New gen SIOC -No	No
Cisco UCS 6300 Series Fabric Interconnect	Direct Connect 40 GB	Yes	SIOC (Non Port-Channel) New gen SIOC -No	Yes
Cisco UCS 6300 Series Fabric Interconnect	Direct Connect– 10 GB – QSA	Yes Not using Breakout	SIOC - No New gen SIOC (Port-Channel)	No
Cisco UCS 6300 Series Fabric Interconnect	Direct Connect 4x10 GB – Breakout	No	N/A	N/A
Cisco UCS 6300 Series Fabric Interconnect	Direct Connect 2x10 GB – Reverse Breakout	Yes	SIOC - No New gen SIOC (Port-Channel)	No
Cisco UCS 6300 Series Fabric Interconnect	2348UPQ FEX - 10 GB – QSA	Yes	SIOC (Non Port-Channel) New gen SIOC (Port-Channel)	Yes
Cisco UCS 6300 Series Fabric Interconnect	2348UPQ FEX - 4x10 GB - Breakout	No	N/A	N/A
Cisco UCS 6324 Fabric Interconnect	Direct Connect - 40 GB	No	N/A	N/A
Cisco UCS 6324 Fabric Interconnect	Direct Connect - 10 GB – QSA	No	N/A	N/A

¹ SIOC without PCIe slots used in release 3.2 and earlier

² New SIOC with PCIe slots used in release 4.0 and higher

³ SIOC without PCIe slots used in release 3.2 and earlier

⁴ New SIOC with PCIe slots used in release 4.0 and higher

Configuring a Chassis Connectivity Policy



Caution Changing the connectivity mode for a chassis results in decommissioning and recommissioning the chassis. Traffic will be disrupted during this time.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis**.
- Step 3** Click the chassis for which you want to configure the connectivity between the SIOCs and fabric interconnects.
- Step 4** In the **Work** pane, click the **Connectivity Policy** tab.
- Step 5** For each SIOC in the chassis, choose one of the following values in the **Admin State** field for the chassis and fabric connectivity:
- **None**—No links are grouped in a port channel
 - **Port Channel**—All links from an IOM to a fabric interconnect are grouped in a port channel.
- Note** Cisco UCS 6400 Series Fabric Interconnects , and Cisco UCS 6536 Fabric Interconnect support only Port Channel mode.
- **Global**—The chassis inherits this configuration from the chassis discovery policy. This is the default value.
- Step 6** Click **Save Changes**.
-



CHAPTER 5

Chassis Profiles

- [Chassis Profiles in Cisco UCS Manager, on page 33](#)
- [Guidelines and Recommendations for Chassis Profiles, on page 34](#)
- [Creating a Chassis Profile with the Wizard, on page 34](#)
- [Renaming a Chassis Profile, on page 35](#)
- [Cloning a Chassis Profile, on page 36](#)
- [Deleting a Chassis Profile, on page 37](#)
- [Chassis Profile Association, on page 37](#)
- [Chassis Profile Template, on page 38](#)
- [Chassis Maintenance Policy, on page 43](#)
- [Compute Connection Policy, on page 45](#)

Chassis Profiles in Cisco UCS Manager

A chassis profile defines the storage, firmware, and maintenance characteristics of a chassis. You can create a chassis profile for the Cisco UCS S3260 chassis. When a chassis profile is associated to a chassis, Cisco UCS Manager automatically configures the chassis to match the configuration specified in the chassis profile.



Important At any given time, each S3260 chassis can be associated with only one chassis profile. Similarly, each chassis profile can be associated with only one S3260 chassis at a time.

A chassis profile includes the following information:

- **Chassis definition**—Defines the specific chassis to which the profile is assigned.
- **Maintenance policy**—Includes the maintenance policy to be applied to the profile.
- **Firmware specifications**—Defines the chassis firmware package that can be applied to a chassis through this profile.
- **Disk zoning policy**—Includes the zoning policy to be applied to the storage disks.
- **Compute Connection policy** — Defines the data path between the primary, auxiliary SIOC, and server.

Guidelines and Recommendations for Chassis Profiles

In addition to any guidelines or recommendations that are specific to the policies included in chassis profiles and chassis profile templates, such as the disk zoning policy, adhere to the following guidelines and recommendations that impact the ability to associate a chassis profile with a chassis:

- Each S3260 chassis can be associated with only one chassis profile. Similarly, each chassis profile can be associated with only one S3260 chassis at a time.
- Chassis profiles are supported only on the Cisco UCS S3260 chassis. The Cisco UCS 5108 blade server chassis does not support chassis profiles and cannot be associated to a chassis profile.
- For Cisco UCS S3260 chassis, S-Series server software bundles earlier than Cisco UCS Manager Release 3.1(2) are not supported.

Creating a Chassis Profile with the Wizard

Procedure

-
- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization where you want to create the chassis profile.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the organization and select **Create Chassis Profile**.
- Step 5** In the **Identify Chassis Profile** panel, specify the chassis profile **Name** and click **Next**.
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.
You can provide an optional description for this chassis profile.
- Note** To create a chassis profile quickly, you can click **Finish** after specifying the name. Cisco UCS Manager creates a new chassis profile with the specified name and all system default values.
- Step 6** (Optional) In the **Chassis Maintenance Policy** panel, specify the maintenance policy, then click **Next**.
You can create a new maintenance policy from this panel. [Creating a Chassis Maintenance Policy, on page 43](#) provides more information about creating a chassis maintenance policy.
- Step 7** (Optional) In the **Chassis Assignment** panel, specify the following, and then click **Next**.
- a) Specify the **Chassis Assignment** from the drop-down list.
You can specify **Chassis Assignment** as one of the following:
 - **Assign Later**—Allows you to assign a chassis after you have created and configured the chassis profile.

- **Select existing Chassis**—Displays a table of available, unassociated chassis that you can use to select the chassis which will be assigned to the chassis profile.

To restrict the migration of the chassis profile after it has been associated with a chassis, 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 chassis before migrating the existing chassis profile. If the chassis types are not similar, the association might fail.

- b) To associate a **Chassis Firmware Package** with this chassis profile, expand the **Chassis Firmware Package** area and specify a chassis firmware package.
You can create a chassis firmware package from this panel. [Creating a Chassis Firmware Package, on page 74](#) provides more information about creating a chassis firmware package.
- c) To associate a **Compute Connection Policy** with this chassis profile, expand the **Compute Connection Policy** area and specify a compute connection policy. See [Server SIOC Connectivity Functionality, on page 12](#) for more details on **Compute Connection Policy** and Server SIOC Connectivity functionality.
You can create a compute connection policy from this panel. [Creating a Compute Connection Policy, on page 45](#) provides more information about creating a compute connection policy.

Step 8 (Optional) In the **Disk Zoning Policy** panel, specify the disk zoning policy, then click **Next**.

You can create a disk zoning policy from this panel. [Creating a Disk Zoning Policy, on page 56](#) provides more information about creating a disk zoning policy.

Note If you do not select a disk zoning policy, the default disk zoning policy is used. **Preserve Config** is selected by default in the default disk zoning policy.

Step 9 (Optional) In the **Sas Expander Configuration Policy** panel, specify the SAS Expander Configuration policy, then click **Next**.

You can create a Sas Expander Configuration policy from this panel. [Creating Sas Expander Configuration Policy, on page 63](#) provides more information about creating a Sas Expander Configuration policy.

Note If you do not select a Sas Expander Configuration policy, the default Sas Expander Configuration policy is used. **No Change** is selected by default in the default Sas Expander Configuration policy.

Step 10 Click **Finish**.

Renaming a Chassis Profile

When you rename a chassis profile, the following occurs:

- Event logs and audit logs that reference the previous name for the chassis profile are retained under that name.
- A new audit record is created to log the rename operation.
- All records of faults against the chassis profile under its previous name are transferred to the new chassis profile name.



Note You cannot rename a chassis profile with pending changes.

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that includes the chassis profile you want to rename.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Click the chassis profile you want to rename.
- Step 5** In the **Work** pane, click the **General** tab.
- Step 6** In the **Actions** area, click **Rename Chassis Profile**.
- Step 7** In the **Rename Chassis Profile** dialog box, enter the new name for the chassis profile in the **New Name** field.
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 8** Click **OK**.
-

Cloning a Chassis Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that includes the chassis profile you want to clone.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis profile you want to clone and select **Create a Clone**.
- Step 5** In the **Create Clone From Chassis Profile** dialog box:
- Enter the name you want to use for the new profile in the **Clone Name** field.
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.
This name must be unique within the organization or sub-organization in which you are creating the chassis profile.
 - (Optional) Select the organization or sub-organization in which you want to create the chassis profile.
 - Click **OK**.

- Step 6** Navigate to the chassis profile you just created and make sure that all options are correct.
-

Deleting a Chassis Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Right-click the chassis profile that you want to delete and select **Delete**.
- Step 4** If a confirmation dialog box displays, click **Yes**.
- Step 5** Click **OK**.
-

Chassis Profile Association

Associating a Chassis Profile with a Chassis

Follow this procedure if you did not associate the chassis profile with a chassis when you created it or to change the chassis with which a chassis profile is associated.

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that contains the chassis profile that you want to associate with a new chassis.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis profile that you want to associate with a chassis and select **Change Chassis Profile Association**.
- Step 5** In the **Associate Chassis Profile** dialog box, select the **Select existing Chassis** option from the drop-down list.
- This displays a table of available, unassociated chassis that you can use to select the chassis which will be assigned to the chassis profile.
- Step 6** In the **Select** column of the table of available chassis, click the radio button for the chassis that you want to associate with this chassis profile.
- Step 7** (Optional) To restrict the migration of the chassis profile after it has been associated with a chassis, 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 chassis before migrating the existing chassis profile. If the hardware of both chassis are not similar, the association might fail.

Step 8 Click OK.

Disassociating a Chassis Profile from a Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that contains the chassis profile that you want to disassociate from a chassis.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis profile you want to disassociate from a chassis and select **Disassociate Chassis Profile**.
- Step 5** In the **Disassociate Chassis Profile** dialog box, click **Yes** to confirm.
- Step 6** (Optional) Monitor the status and FSM for the chassis to confirm that the disassociation is complete.
-

Chassis Profile Template

Chassis Profile Templates

With a chassis profile template, you can quickly create several chassis profiles with the same basic parameters, such as the maintenance policy and the disk zoning policy.



Tip If you need only one chassis profile with similar values to an existing chassis profile, you can clone a chassis profile in the Cisco UCS Manager GUI.

For example, if you need several chassis profiles with similar values, you can create a chassis profile template, either manually or from an existing chassis profile. You can then use the template to create the chassis profiles.

Cisco UCS supports the following types of chassis profile templates:

Initial template

Chassis profiles created from an initial template inherit all the properties of the template. Chassis profiles created from an initial chassis profile template are bound to the template. However, changes to the initial template do not automatically propagate to the bound chassis profiles. If you want to propagate changes to bound chassis profiles, unbind and rebind the chassis profile to the initial template.

Updating template

Chassis 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 chassis profiles created from the template.

Creating a Chassis Profile Template

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profile Templates**.
- Step 3** Expand the node for the organization where you want to create the chassis profile template.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the organization and choose **Create Chassis Profile Template**.
- Step 5** In the **Identify Chassis Profile Template** panel, specify the chassis profile **Name** and **Type**, and then click **Next**.
You can provide an optional description for this chassis profile template.
- Note** To create a chassis profile template quickly, you can click **Finish** after specifying the name. Cisco UCS Manager creates a new chassis profile template with the specified name and all system default values.
- Step 6** (Optional) In the **Chassis Maintenance Policy** panel, specify the chassis maintenance policy, then click **Next**.
You can create a new chassis maintenance policy from this panel.
- Step 7** (Optional) In the **Policies** panel, specify the following, then click **Next**.
- To associate a **Chassis Firmware Package**, expand the **Chassis Firmware Package** area and specify a chassis firmware package.
You can create a chassis firmware package from this panel. [Creating a Chassis Firmware Package, on page 74](#) provides more information about creating a chassis firmware package.
 - To associate a **Compute Connection Policy**, expand the **Compute Connection Policy** area and specify a compute connection policy. See [Server SIOC Connectivity Functionality, on page 12](#) for more details on **Compute Connection Policy** and Server SIOC Connectivity functionality.
You can create a compute connection policy from this panel. [Creating a Compute Connection Policy, on page 45](#) provides more information about creating a compute connection policy.
- Step 8** (Optional) In the **Disk Zoning Policy** panel, specify the disk zoning policy, then click **Next**.
You can create a disk zoning policy from this panel.
- Step 9** Click **Finish**.
-

Creating One or More Chassis Profiles from a Chassis Profile Template

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profile Templates**.
- Step 3** Expand the node for the organization that contains the chassis profile template that you want to use as the basis for your chassis profiles.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis profile template from which you want to create the profiles and select **Create Chassis Profiles From Template**.
- Step 5** In the **Create Chassis Profiles From Template** dialog box, complete the following fields:

Name	Description
Naming Prefix field	The prefix to use for the template name. When the system creates the chassis profile, it appends a unique numeric identifier to this prefix. This number begins with the number specified in the Name Suffix Starting Number field. Enter between 1 and 29 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period).
Name Suffix Starting Number field	The first unique numeric identifier that is assigned as a suffix to a chassis profile Naming Prefix .
Number of Instances field	The number of chassis profiles to create. Enter a number between 1 and 255. For example, if you specify the Naming Prefix as MyProfile , the Name Suffix Starting Number as 1, and the Number of Instances as 2, the first chassis profile would be called MyProfile1 and the second would be MyProfile2.
Chassis Profile Template field	The name of the chassis profile template.

- Step 6** Click **OK**.

Creating a Chassis Profile Template from a Chassis Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.

- Step 3** Expand the node for the organization that contains the chassis profile that you want to use as the basis for your template.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis profile from which you want to create the template and select **Create a Chassis Profile Template**.
- Step 5** In the **Create Template From Chassis Profile** dialog box, complete the following fields:

Name	Description
Template Name field	The name of the chassis profile template
Org drop-down list	Select the organization that you want this template to be associated with.
Type field	The type of template. This can be one of the following: <ul style="list-style-type: none"> • Initial Template—Any chassis profiles created from this template are not updated if the template changes. • Updating Template—Any chassis profiles created from this template are updated if the template changes.

- Step 6** Click **OK**.

Cloning a Chassis Template Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profile Templates**.
- Step 3** Expand the node for the organization that includes the chassis template profile you want to clone.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis template profile you want to clone and select **Create a Clone**.
- Step 5** In the **Create Clone From Chassis Template Profile** dialog box:
- Enter the name you want to use for the new profile in the **Clone Name** field.

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.

This name must be unique within the organization or sub-organization in which you are creating the chassis template profile.
 - (Optional) Select the organization or sub-organization in which you want to create the chassis template profile.
 - Click **OK**.

- Step 6** Navigate to the chassis template profile you just created and make sure that all options are correct.
-

Changing the Maintenance Policy for a Chassis Profile Template

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profile Templates**.
- Step 3** Expand the node for the organization that includes the chassis profile template whose chassis maintenance policy you want to change.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Click the chassis profile template you want to modify.
- Step 5** In the **Work** pane click the **General** tab.
- Step 6** In the **Actions** area, click **Change Chassis Maintenance Policy**
- Step 7** In the **Change Chassis Maintenance Policy** dialog box, specify the chassis maintenance policy from the **Chassis Maintenance Policy** drop-down list, then click **OK**.
- You can create a new maintenance policy from this panel.
-

Binding a Chassis Profile to a Chassis Profile Template

You can bind a chassis profile to a chassis profile template. When you bind the chassis profile to a template, Cisco UCS Manager configures the chassis profile with the values defined in the chassis profile template. If the existing chassis profile configuration does not match the template, Cisco UCS Manager reconfigures the chassis profile. You can only change the configuration of a bound chassis profile through the associated template.

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that includes the chassis profile that you want to bind.
- If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Click the chassis profile that 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 Chassis Profile Template** dialog box, do the following:
- From the **Chassis Profile Template** drop-down list, choose the template to which you want to bind the chassis profile.

- b) Click **OK**.

Unbinding a Chassis Profile from a Chassis Profile Template

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that includes the chassis profile that you want to unbind.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Click the chassis profile that you want to unbind.
- Step 5** In the **Work** pane, click the **General** tab.
- Step 6** In the **Actions** area, click **Unbind from the Template**.
- Step 7** If a confirmation dialog box displays, click **Yes**.

Chassis Maintenance Policy

Creating a Chassis Maintenance Policy

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click **Chassis Maintenance Policies** and choose **Create Chassis Maintenance Policy**.
- Step 5** In the **Create Chassis Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	<p>The name of the policy.</p> <p>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.</p>

Name	Description
Description field	<p>A description of the policy. Cisco recommends including information about where and when to use the policy.</p> <p>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).</p>
Reboot Policy field	<p>When a chassis profile is associated with a chassis, or when changes are made to a chassis profile that is already associated with a chassis, you must power cycle the chassis to complete the process. The Reboot Policy field determines when the power cycle occurs for chassis associated with any chassis profiles that include this chassis maintenance policy. Chassis profiles and chassis profile templates support only one reboot policy:</p> <p>User Ack—The user must power cycle the chassis manually after the chassis profile association is complete or changes are made.</p>

Step 6 Click **OK**.

What to do next

Include the policy in a chassis profile or chassis profile template.

Changing the Maintenance Policy for a Chassis Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that includes the chassis profile whose maintenance policy you want to change.
- If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the chassis profile you want to modify and select **Change Chassis Maintenance Policy**.
- Step 5** In the **Change Chassis Maintenance Policy** dialog box, specify the chassis maintenance policy from the **Chassis Maintenance Policy** drop-down list, then click **OK**.
- You can create a new chassis maintenance policy from this panel.

Note The chassis profile will immediately reboot when disruptive changes are applied.

Deleting a Chassis Maintenance Policy

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
 - Step 2** Expand **Chassis > Policies > Organization_Name**.
 - Step 3** Expand **Chassis Maintenance Policies**.
 - Step 4** Right-click the chassis maintenance policy you want to delete and choose **Delete**.
 - Step 5** If a confirmation dialog box displays, click **Yes**.
-

Compute Connection Policy

Compute Connection Policy is used to store the user configuration of the server SIOC connectivity. The configuration settings are done using the property **Server SIOC Connectivity**, which can be set to:

- **single-server-single-sioc** (default) - The data path is configured through one SIOC when the chassis has single server and single SIOC or dual server and dual SIOCs.
- **single-server-dual-sioc** - When enabled, you can configure the data path through both the primary and auxiliary SIOCs when the chassis has single server and dual SIOCs. See [Server SIOC Connectivity Functionality, on page 12](#) for more details.

Creating a Compute Connection Policy

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Policies > Organization_Name**.
- Step 3** Right-click **Compute Connection Policies** and select **Create Compute Connection Policy**.
- Step 4** In the **Create Compute Connection Policy** pane, enter the following:
 - **Name** - Enter a name for the policy.
 - **Description** - A brief description of the policy.
 - **Server SIOC Connectivity** - Select one of the following:
 - **single-server-single-sioc** (default) - The data path is configured through one SIOC when the chassis has single server and single SIOC or dual server and dual SIOCs.

- **single-server-dual-sioc** - When enabled, you can configure the data path through both the primary and auxiliary SIOCs when the chassis has single server and dual SIOCs. See [Server SIOC Connectivity Functionality, on page 12](#) for more details.

Step 5 Click **OK**.

Note In GUI, once **Compute Conn Policy** property is set to **single-server-dual-sioc**, then Cisco UCS Manager displays a message, warning that this operation causes server reboot. After acknowledging the message, chassis association is triggered. When Server SIOC Connectivity configuration is successfully deployed, Cisco UCS Manager automatically triggers server deep discovery.

Associating a Compute Connection Policy to Chassis Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles > Chassis_Profile_Name**.
- Step 3** Select the **Policies** tab.
- Step 4** Expand **Compute Connection Policies** area.
- Step 5** Select a policy from the **Compute Connection Policies** drop-down list.
- Step 6** Click **Save Changes**.
-



CHAPTER 6

Storage

- [Storage Server Features and Components Overview](#), on page 47
- [Cisco UCS S3260 Storage Management Operations](#), on page 54
- [Disk Sharing for High Availability](#), on page 55
- [Storage Enclosure Operations](#), on page 62
- [Sas Expander Configuration Policy](#), on page 63

Storage Server Features and Components Overview

Storage Server Features

The following table summarizes the Cisco UCS S3260 system features:

Table 8: Cisco UCS S3260 System Features

Feature	Description
Chassis	Four rack unit (4RU) chassis
Processors	<ul style="list-style-type: none">• Cisco UCS S3260 M5 server nodes: Two Intel Skylake 2S-EP processors inside each server node.
Memory	Up to 16 DIMMs inside each server node.
Multi-bit error protection	This system supports multi-bit error protection.

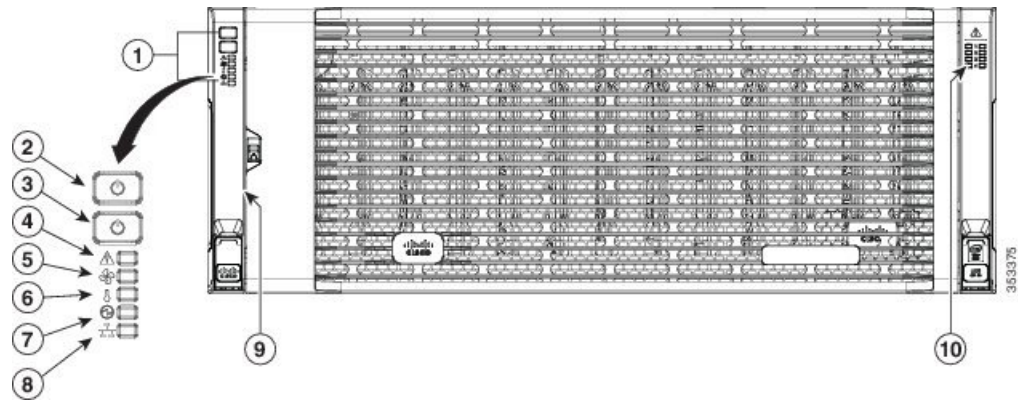
Feature	Description
Storage	<p>The system has the following storage options:</p> <ul style="list-style-type: none"> • Up to 56 top-loading 3.5-inch drives • Up to four 3.5-inch, rear-loading drives in the optional drive expander module • Up to four 2.5-inch, rear-loading SAS solid state drives (SSDs) • Two 7 mm NVMe drive inside the server node <p>Note This is applicable for S3260 M5 servers only.</p> <ul style="list-style-type: none"> • Two 15 mm NVMe drive supported for IO Expander
Disk Management	<p>The system supports up to two storage controllers:</p> <ul style="list-style-type: none"> • One dedicated mezzanine-style socket for a Cisco storage controller card inside each server node
RAID Backup	<p>The supercap power module (SCPM) mounts to the RAID controller card.</p>
PCIe I/O	<p>The optional I/O expander provides two 8x Gen 3 PCIe expansion slots.</p> <p>Release 3.2(3) and later supports the following for S3260 M5 servers:</p> <ul style="list-style-type: none"> • Intel X550 dual-port 10GBase-T • Qlogic QLE2692 dual-port 16G Fiber Channel HBA • N2XX-AIPCI01 Intel X520 Dual Port 10Gb SFP+ Adapter
Network and Management I/O	<p>The system can have one or two system I/O controllers (SIOC). These provide rear-panel management and data connectivity.</p> <ul style="list-style-type: none"> • Two SFP+ 40 Gb ports each SIOC. • One 10/100/1000 Ethernet dedicated management port on each SIOC. <p>The server nodes each have one rear-panel KVM connector that can be used with a KVM cable, which provides two USB, one VGA DB-15, and one serial DB-9 connector.</p>

Feature	Description
Power	Two or four power supplies, 1050 W each (hot-swappable and redundant as 2+2).
Cooling	Four internal fan modules that pull front-to-rear cooling, hot-swappable. Each fan module contains two fans. In addition, there is one fan in each power supply.

Front Panel Features

The following image shows the front panel features for the Cisco UCS S3260 system:

Figure 10: Front Panel Features

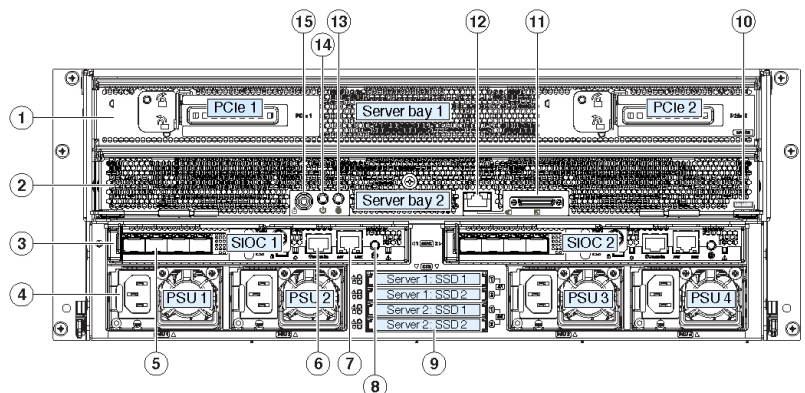


1	Operations panel	6	Temperature status LED
2	System Power button/LED	7	Power supply status LED
3	System unit identification button/LED	8	Network link activity LED
4	System status LED	9	Pull-out asset tag (not visible under front bezel)
5	Fan status LED	10	Internal-drive status LEDs

Rear Panel Features

The following image shows the rear panel features for the Cisco UCS S3260 system:

Figure 11: Front Panel Features



Disk Slots

1	<p>Server bay 1</p> <ul style="list-style-type: none"> • (Optional) I/O expander, as shown (with Cisco UCS S3260 M5 server node only) • (Optional) server node • (Optional) drive expansion module 	8	Not used at this time
2	<p>Server bay 2</p> <ul style="list-style-type: none"> • (Optional) server node (Cisco UCS S3260 M5 shown) (Optional) drive expansion module 	9	Not used at this time

3	System I/O controller (SIOC) <ul style="list-style-type: none"> • SIOC 1 is required if you have a server node in server bay 1 • SIOC 2 is required if you have server node in server bay 2 	10	Solid state drive bays (up to four 2.5-inch SAS SSDs) <ul style="list-style-type: none"> • SSDs in bays 1 and 2 require a server node in server bay 1 • SSDs in bays 3 and 4 require a server node in server bay 2
4	Power supplies (four, redundant as 2+2)	11	Note This label identifies a Cisco UCS S3260 M5 server node.
5	40-Gb SFP+ ports (two on each SIOC)	12	KVM console connector (one each server node). Used with a KVM cable that provides two USB, one VGA, and one serial connector
6	Chassis Management Controller (CMS) Debug Firmware Utility port (one each SIOC)	13	Server node unit identification button/LED
7	10/100/1000 dedicated management port, RJ-45 connector (one each SIOC)	14	Server node power button
		15	Server node reset button (resets chipset in the server node)

Storage Server Components

Server Nodes

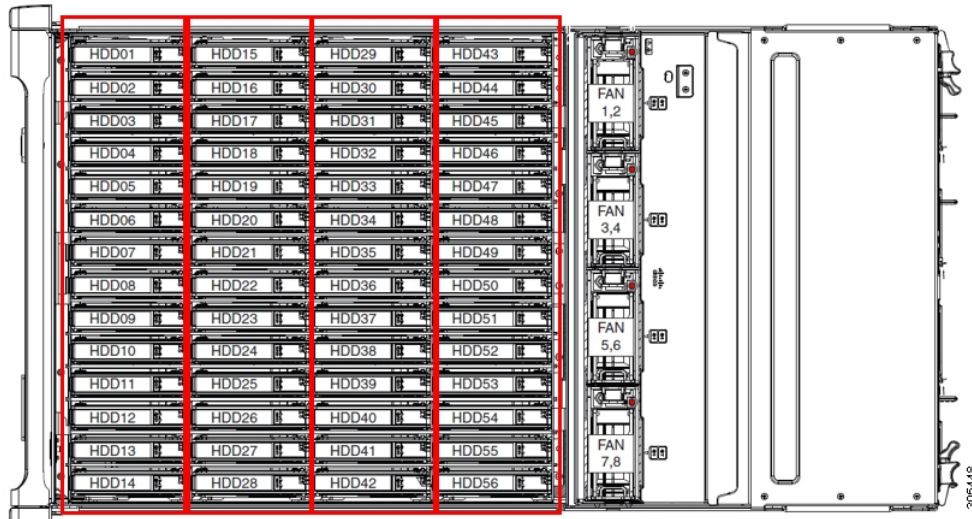
The Cisco UCS S3260 system consists of one or two server nodes, each with two CPUs, DIMM memory of 128, 256, or 512 GB, and a RAID card up to 4 GB cache or a pass-through controller. The server nodes can be one of the following:

- Cisco UCS S3260 M5 Server Node—This node might include an optional I/O expander module that attaches to the top of the server node.

Disk Slots

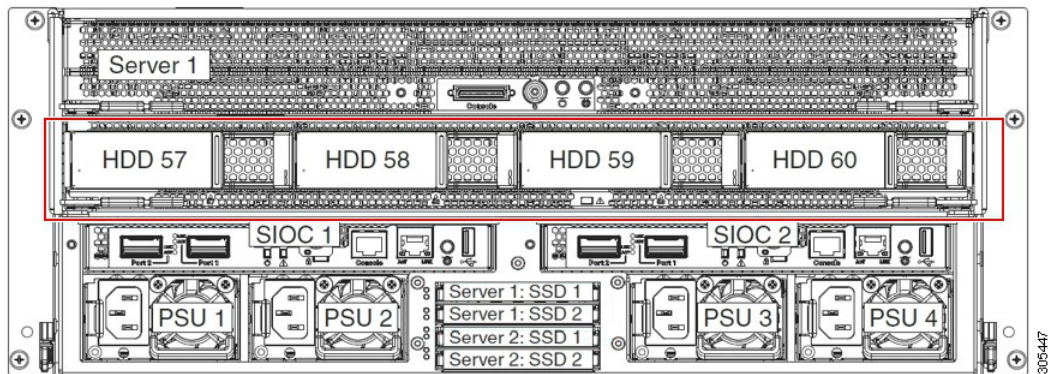
The Cisco UCS S3260 chassis has 4 rows of 14 disk slots on the HDD motherboard and 4 additional disk slots on the HDD expansion tray. The following image shows the disk arrangement for the 56 top-accessible, hot swappable 3.5-inch 6 TB or 4 TB 7200 rpm NL-SAS HDD drives. A disk slot has two SAS ports and each is connected a SAS expander in the chassis.

Figure 12: Cisco UCS S3260 Top View



The following image shows the Cisco UCS S3260 chassis with the 4 additional disk slots on the HDD expansion tray.

Figure 13: Cisco UCS 3260 with the HDD expansion tray (Rear View)



If you have two server nodes with two SIOC, you will have the following functionality:

1. The top server node works with the left SIOC (Server Slot1 with SIOC1).
2. The bottom server works with the right SIOC (Sever Slot 2 with SIOC2).

If you have one server node with two SIOC, you can enable Server SIOC Connectivity functionality. Beginning with release 3.1(3), Cisco UCS S3260 system supports Server SIOC Connectivity functionality. Using this functionality, you can configure the data path through both the primary and auxiliary SIOC when the chassis has single server and dual SIOC set up.

SAS Expanders

The Cisco UCS S3260 system has two SAS expanders that run in redundant mode and connect the disks at the chassis level to storage controllers on the servers. The SAS expanders provide two paths between a storage controller, and hence enable high availability. They provide the following functionality:

- Manage the pool of hard drives.
- Disk zone configuration of the hard drives to storage controllers on the servers.

Beginning with release 3.2(3a), Cisco UCS Manager can enable single path access to disk by configuring single DiskPort per disk slot. This ensures that the server discovers only a single device and avoid a multi-path configuration.

The following table describes how the ports in each SAS expander are connected to the disks based on the type of deployment.

Port range	Connectivity
1-56	Top accessible disks
57-60	Disks in the HDD expansion tray.



Note The number of SAS uplinks between storage controller and SAS expander can vary based on the type of controller equipped in the server.

Storage Enclosures

A Cisco UCS S3260 system has the following types of storage enclosures:

Chassis Level Storage Enclosures

- **HDD motherboard enclosure**—The 56 dual port disk slots in the chassis comprise the HDD motherboard enclosure.
- **HDD expansion tray**—The 4 additional dual disk slots in the Cisco UCS S3260 system comprise the HDD expansion tray.



Note The HDD expansion tray is a field replaceable unit (FRU). The disks will remain unassigned upon insertion, and can be assigned to storage controllers. For detailed steps on how to perform disk zoning, see [Disk Zoning Policies, on page 55](#)

Server level Storage Enclosures

Server level storage enclosures are pre-assigned dedicated enclosures to the server. These can be one of the following:

- **Rear Boot SSD enclosure**—This enclosure contains two 2.5 inch disk slots on the rear panel of the Cisco UCS S3260 system. Each server has two dedicated disk slots. These disk slots support SATA SSDs.
- **Server board NVMe enclosure**—This enclosure contains one PCIe NVMe controller.



Note In the Cisco UCS S3260 system, even though disks can be physically present on the two types of enclosures described above, from the host OS all the disks are viewed as part of one SCSI enclosure. They are connected to SAS expanders that are configured to run as single SES enclosure.

Storage Controllers

Mezzanine Storage Controllers

The following table lists the storage controller type, firmware type, modes, sharing and OOB support for the various storage controllers.

Table 9:

Storage Controller Type	Firmware type	Modes	Sharing	OOB Support
UCSC-S3X60-R1GB	Mega RAID	HW RAID, JBOD	No	Yes
UCSC-S3X60-HBA	Initiator Target	Pass through	Yes	Yes
UCS-S3260-DHBA	Initiator Target	Pass through	Yes	Yes
UCS-S3260-DRAID	Mega RAID	HW RAID, JBOD	No	Yes

Other storage controllers

SW RAID Controller—The servers in the Cisco UCS S3260 system support two dedicated internal SSDs embedded into the PCIe riser that is connected to the SW RAID Controller.

NVMe Controller—This controller is used by servers in the Cisco UCS S3260 system for inventory and firmware updates of NVMe disks.

For more details about the storage controllers supported in the various server nodes, see the related service note:

- [Cisco UCS S3260 M5 Server Node For Cisco UCS S3260 Storage Server Service Note](#)

Cisco UCS S3260 Storage Management Operations

The following table summarizes the various storage management operations that you can perform with the Cisco UCS Manager integrated Cisco UCS S3260 system.

Operation	Description	See:
Disk Sharing for High Availability	The SAS expanders in the Cisco UCS S3260 system can manage the pool of drives at the chassis level. To share disks for high availability, perform the following: <ol style="list-style-type: none"> 1. Creating disk zoning policies. 2. Creating disk slots and assigning ownership. 3. Associating disks to chassis profile. 	"Disk Zoning Policies" section in this guide.
Storage Profiles, Disk Groups and Disk Group Configuration Policies	You can utilize Cisco UCS Manager's Storage Profile and Disk Group Policies for defining storage disks, disk allocation and management in the Cisco UCS S3260 system.	"Storage Profiles" section in the <i>Cisco UCS Manager Storage Management Guide, Release 3.2</i> .
Storage Enclosure Operations	You can swap the HDD expansion tray with a server, or remove the tray if it was previously inserted.	"Removing Chassis Level Storage Enclosures" section in this guide.

Disk Sharing for High Availability

Disk Zoning Policies

You can assign disk drives to the server nodes using disk zoning. Disk zoning can be performed on the controllers in the same server or on the controllers on different servers. Disk ownership can be one of the following:

Unassigned

Unassigned disks are those not visible to the server nodes.

Dedicated

If this option is selected, you will need to set the values for the **Server**, **Controller**, **Drive Path**, and **Slot Range** for the disk slot.



Note A disk is visible only to the assigned controller.

Beginning with release 3.2(3a), Cisco UCS Manager can enable single path access to disk by configuring single DiskPort per disk slot for Cisco UCS S3260 M5 and higher servers. Setting single path configuration ensures that the server discovers the disk drive only through a single drive path chosen in the configuration. Single path access is supported only for **Cisco UCS S3260 Dual Pass Through Controller** (UCS-S3260-DHBA)

Once single path access is enabled, you cannot downgrade to any release earlier than 3.2(3a). To downgrade, disable this feature and assign all the disk slots to both the disk ports by configuring disk path of the disk slots to **Path Both** in disk zoning policy.

Shared

Shared disks are those assigned to more than one controller. They are specifically used when the servers are running in a cluster configuration, and each server has its storage controllers in HBA mode.



Note Shared mode cannot be used under certain conditions when dual HBA controllers are used.

Chassis Global Hot Spare

If this option is selected, you will need to set the value for the **Slot Range** for the disk.



Important Disk migration and claiming orphan LUNs: To migrate a disk zoned to a server (Server 1) to another server (Server 2), you must mark the virtual drive (LUN) as transport ready or perform a hide virtual drive operation. You can then change the disk zoning policy assigned for that disk. For more information on virtual drive management, see the *Disk Groups and Disk Configuration Policies* section of the [Cisco UCS Manager Storage Management Guide](#).

Creating a Disk Zoning Policy

Procedure

- Step 1** In the Navigation pane, click **Chassis**.
- Step 2** Expand **Policies > root**.
- Step 3** Right-click **Disk Zoning Policies** and choose **Create Disk Zoning Policy**.
- Step 4** In the **Create Disk Zoning Policy** dialog box, complete the following:

Name	Description
Name field	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.

Name	Description
Description field	<p>A description of the policy. Cisco recommends including information about where and when to use the policy.</p> <p>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).</p>
Preserve Config check box	<p>If this check box is selected, it preserves all configuration related information for the disks such as slot number, ownership, server assigned, controller assigned, and controller type.</p> <p>Note By default the Preserve Config check box remains unchecked.</p>

In the **Disk Zoning Information** area, complete the following:

Name	Field
Name column	The name for the disk slot.
Slot Number column	The slot number for the disk.

Name	Field
Ownership column	<p>The slot ownership value. This can be one of the following:</p> <ul style="list-style-type: none"> • Unassigned—This option is selected by default. You can set the slot number in the Slot Range field. • Dedicated—If this option is selected, you will need to set the values for the Server, Controller, Drive Path, and Slot Range for the disk slot. Beginning with release 3.2(3a), Cisco UCS Manager can enable single path access to disk by configuring single DiskPort per disk slot. This ensures that the server discovers only a single device and avoid a multi-path configuration. Drive Path options are: <ul style="list-style-type: none"> • Path Both (Default) - Drive path is zoned to both the SAS expanders. • Path 0 - Drive path is zoned to SAS expander 1. • Path 1 - Drive path is zoned to SAS expander 2. • Shared—If this option is selected, you will need to set the values for the Slot Range and controller information such as server assigned, controller assigned, and controller type for the disk slot. Note Shared mode cannot be used under certain conditions when dual HBA controllers are used. To view the conditions for Shared mode for Dual HBA controller, see Table 10: Limitations for Shared Mode for Dual HBA Controller, on page 59. • Chassis Global Hot Spare—If this option is selected, you will need to set the value for the Slot Range for the disk.
Assigned to Server column	The ID of the server that the disk is assigned.

Name	Field
Assigned to Controller column	The ID of the controller that the disk is assigned. Note In a Dual RAID setup, to migrate the disk from first controller to second, change the Assigned to Controller to the second controller.
Controller Type column	The type for the controller. If the disk is either dedicated or shared, the controller type is always SAS.

Table 10: Limitations for Shared Mode for Dual HBA Controller

Server	HDD Tray	Controller	Shared mode Support
Cisco UCS S3260	No	Dual HBA	Not Supported
Cisco UCS S3260	HDD Tray	Dual HBA	Not Supported
Pre-Provisioned	HDD Tray	Dual HBA	Not Supported

Creating Disk Slots and Assigning Ownership

After you create a disk zoning policy, you must create the disk slots, and assign ownership.

Procedure

- Step 1** In the Navigation pane, click **Chassis**.
- Step 2** Expand **Policies > root > Disk Zoning Policies**, and select the disk zoning policy that you want to add disk slots.
- Step 3** In the Work pane, under **Actions**, click **Add Slots to Policy**.
- Step 4** In the **Add Slots to Policy** dialog box, complete the following:

Name	Description
Ownership check box	<p>The ownership for the disk slot. This can be one of the following:</p> <ul style="list-style-type: none"> • Unassigned—This option is selected by default. You can set the slot number in the Slot Range field. • Dedicated—If this option is selected, you will need to set the values for the Server, Controller, and Slot Range for the disk slot. • Shared—If this option is selected, you will need to set the values for the Slot Range and controller information such as server assigned, controller assigned, and controller type for the disk slot. <p>Note Shared mode cannot be used under certain conditions when dual HBA controllers are used. To view the conditions for Shared mode for Dual HBA controller, see Table 10: Limitations for Shared Mode for Dual HBA Controller, on page 59.</p> <ul style="list-style-type: none"> • Chassis Global Hot Spare—If this option is selected, you will need to set the value for the Slot Range for the disk.

Step 5 Click **OK**.

Associating Disk Zoning Policies to Chassis Profile

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization where you want to create the chassis profile.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click the organization and select **Create Chassis Profile**.
- Step 5** In the **Identify Chassis Profile** page, specify the name for the chassis profile, and click **Next**.
- Step 6** (Optional) In the **Maintenance Policy** page, specify the name for the maintenance policy, and click **Next**.
- Step 7** In the **Chassis Assignment** page, select **Select existing Chassis** under **Chassis Assignment**, and then select the chassis that you want to associate with this chassis profile. Click **Next**.
- Step 8** In the **Disk Zoning** page, specify the disk zoning policy that you want to associate with this chassis profile.
- Step 9** Click **Finish**.

Disk Migration

Before you can migrate a disk zoned from one server to another, you must mark the virtual drive(LUN) as transport ready or perform a hide virtual drive operation. This will ensure that all references from the service profile have been removed prior to disk migration. For more information on virtual drives, please refer to the "virtual drives" section in the *Cisco UCS Manager Storage Management Guide, Release 3.2*



Note In a Dual RAID setup, to migrate the disk from first controller to second change the **Assigned to Controller** to the second controller in the disk zoning policy. Refer [Creating a Disk Zoning Policy, on page 56](#).

Procedure

- Step 1** In the Navigation pane, click **Equipment > Chassis > Servers**.
- Step 2** Choose the Sever where you want to perform disk migration.
- Step 3** In the Work pane, click the **Inventory** tab.
- Step 4** Click the **Storage** subtab.
- Step 5** Click the **LUNs** subtab.
- Step 6** Choose the storage controller where you want to prepare the virtual drives for migration to another server.
- Step 7** Choose the disk that you want to migrate.
- Step 8** In the **Actions** area, choose one of the following:

Name	Description
Rename	Click on this link to rename your disk.
Delete	Click on this link to delete your disk.
Set Transportation Ready	Click on this link for the safe migration of the virtual drive from one server to another. Note All virtual drives on a disk group must be marked as hidden before migrating or unassigning the disks from a server node.
Clear Transportation Ready	Click on this link to set the state of the virtual drive to no longer be transport ready.

Name	Description
Hide Virtual Drive	<p>Click on this option for the safe migration of the virtual drive from one server to another.</p> <p>Note All virtual drives on a disk group must be marked as hidden before migrating or unassigning the disks from a server node.</p>
Unhide Virtual Drive	<p>Click on this link to unhide the virtual drive and enable IO operations.</p>

Storage Enclosure Operations

Removing Chassis Level Storage Enclosures

You can remove the storage enclosure corresponding to HDD expansion tray in Cisco UCS Manager after it is physically removed. You cannot remove server level or any other chassis level storage enclosures.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Chassis > Servers > Storage Enclosures**.
- Step 3** Choose the storage enclosure that you want to remove.
- Step 4** In the **Actions** area, click **Remove Enclosure**.

Sas Expander Configuration Policy

Creating Sas Expander Configuration Policy

Procedure

	Command or Action	Purpose						
Step 1	In the Navigation pane, click Chassis .							
Step 2	Expand Chassis > Policies .							
Step 3	Expand the node for the organization where you want to create the policy.	If the system does not include multi tenancy, expand the root node.						
Step 4	Right-click Sas Expander Configuration Policies and choose Create Sas Expander Configuration Policy .							
Step 5	In the Create Sas Expander Configuration Policy dialog box, complete the following fields:	<table border="1"> <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), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).</td> </tr> </tbody> </table>	Name	Description	Name field	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.	Description field	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).
Name	Description							
Name field	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.							
Description field	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).							

	Command or Action	Purpose	
		Name	Description
		6G-12G Mixed Mode field	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Connection Management is disabled in this policy and the Sas Expander uses only 6G speeds even if 12G is available. • Enabled—Connection Management is enabled in this policy and it intelligently shifts between 6G and 12 G speeds based on availability. <p>After 6G-12G Mixed Mode is enabled, you cannot downgrade to any release earlier than 3.2(3a). To downgrade, disable this mode.</p> <ul style="list-style-type: none"> • No Change (Default) —Pre-existing configuration is retained. <p>Note Enabling or disabling 6G-12G Mixed Mode causes system reboot.</p> <p>6G-12G Mixed Mode field is available only for Cisco UCS S3260 M5 and higher servers.</p>
Step 6	Click OK .		

Deleting a Sas Expander Configuration Policy

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Policies**.
- Step 3** Expand the node for the organization containing the pool.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Expand **Sas Expander Configuration Policies**.
- Step 5** Right-click the Sas Expander Configuration policy you want to delete and choose **Delete**.
- Step 6** If a confirmation dialog box displays, click **Yes**.
-



CHAPTER 7

Firmware Management

- [Firmware Management for Cisco UCS S3260 Systems, on page 67](#)
- [Chassis Firmware Upgrade through Auto Install, on page 68](#)
- [Firmware Upgrades through Chassis Firmware Packages in Chassis Profiles , on page 71](#)
- [Direct Firmware Upgrade on S3260 Chassis and Server Endpoints, on page 77](#)

Firmware Management for Cisco UCS S3260 Systems

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS domain. Each endpoint is a component in the Cisco UCS domain that requires firmware to function.

Cisco UCS Manager Firmware Management Guide, Release 3.2 provides detailed information about the complete firmware management process. Additionally, beginning with Cisco UCS Manager Release 3.1(2), you can upgrade the firmware of Cisco UCS S3260 chassis components by defining a chassis firmware policy and including it in the chassis profile associated with a Cisco UCS S3260 chassis.

You can upgrade a Cisco UCS domain with a S3260 chassis and servers through Cisco UCS Manager in the following ways:

- Upgrade infrastructure components through Auto Install—You can upgrade the infrastructure components, such as the Cisco UCS Manager software and the fabric interconnects, in a single step by using Auto Install. *Cisco UCS Manager Firmware Management Guide, Release 3.2* provides detailed information about the Auto Install process.
- Upgrade chassis through one of the following:
 - Upgrade chassis components through Auto Install—Beginning with Cisco UCS Manager Release 3.2(3), you can upgrade the firmware of Cisco UCS S3260 chassis components in a single step by using Auto Install.
 - Upgrade chassis through chassis firmware packages in chassis profiles—This option enables you to upgrade all chassis endpoints in a single step. The chassis endpoints that you can upgrade through a chassis firmware package are:
 - Chassis Adapter
 - Chassis Management Controller
 - Chassis Board Controller
 - Local Disk



Note You can upgrade local disks in the chassis through a chassis firmware package. Upgrade the local disks in a server through a host firmware package.

- SAS Expander

- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows. The server endpoints that you can upgrade through a host firmware package are:
 - CIMC
 - BIOS
 - Board Controller
 - Storage Controller
 - Local Disk
 - NVMe in SIOC
 - Third-party adapter in SIOC

Cisco UCS Manager Firmware Management Guide, Release 3.2 provides detailed information about upgrading server endpoints through host firmware packages.

You can also directly upgrade the firmware at each infrastructure, chassis, and server endpoint. This option enables you to upgrade many infrastructure, chassis, and server endpoints directly, including the fabric interconnects, SAS expanders, CMCs, chassis adapters, storage controllers, and board controllers. However, direct upgrade is not available for all endpoints, including the storage controller, HBA firmware, HBA option ROM and local disk.

This chapter explains the following newly introduced firmware management capabilities for the Cisco UCS S3260 system:

- Upgrading firmware through chassis firmware packages in chassis profiles
- Directly upgrading firmware on Cisco UCS S3260 chassis and server endpoints

Chassis Firmware Upgrade through Auto Install

Cisco UCS Manager Release 3.2(3) introduces support for upgrading chassis firmware through Auto Install on Cisco UCS S3260 chassis. This ability enables you to upgrade all chassis components in a Cisco UCS domain through a single chassis firmware package.

Upgrading the Chassis Firmware with Auto Install

You can upgrade chassis firmware by specifying a Chassis Firmware package.

If you staged the chassis firmware through **Prepare for Firmware Install**, and that backup version is the same as the selected chassis firmware version in this procedure, the backup version is set as the startup version.

If you did not set the backup version earlier, the selected firmware version is set as the backup version. This version is then set as the startup version.

Completing this stage will result in a reboot.



Note You cannot use Auto Install to upgrade the chassis in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS Manager 3.2(3). For more information, see the *Cautions and Guidelines for Upgrading with Auto Install* section in the *Cisco UCS Manager Firmware Management Guide, Release 3.2*.

You cannot cancel a chassis firmware upgrade process after you complete the configuration in the **Install Chassis Firmware** wizard. Cisco UCS Manager applies the changes immediately.

Before you begin

- Complete all prerequisites listed in the *Prerequisites for Upgrading and Downgrading Firmware* section of the *Cisco UCS Manager Firmware Management Guide, Release 3.2*.
- Stage the Chassis firmware if using Cisco UCS Manager Release 3.2(3) or later releases. The *Preparing for Firmware Install* section of the *Cisco UCS Manager Firmware Management Guide, Release 3.2*, provides detailed information about staging the chassis firmware.



Note Although this is optional, it is also recommended.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** In the **Work** pane, click the **Firmware Auto Install** tab.
- Step 5** In the **Actions** area, click **Install Chassis Firmware**.
- Step 6** On the **Prerequisites** page of the **Install Chassis Firmware** wizard, carefully review the prerequisites and guidelines listed on this page and then do one of the following:
- If you have completed all of the prerequisites, click **Next**.
 - If you have not completed all of the prerequisites, click **Cancel** and complete the prerequisites before you upgrade the chassis firmware.
- Step 7** On the **Select Package Versions** page of the **Install Chassis Firmware** wizard, do the following:
- a) Choose the software bundle to which you want to upgrade these chassis from the **New Version** drop-down list in the **Chassis Firmware** area.
 - b) To upgrade the chassis to a service pack firmware version, choose the service pack to which you want to upgrade these chassis from the **New Version** drop-down list in the **Service-Pack Firmware** area.

- c) Click **Next**.

Step 8

On the **Select Firmware Packages** page of the **Install Chassis Firmware** wizard, do the following:

- a) Expand the node for each organization that contains a chassis firmware package you want to update with the selected software.

If the firmware version for a chassis firmware package is staged, it appears as the **Backup Version** along with the name of the chassis firmware package.

- b) Check the check box next to the name of each chassis firmware package that you want to update.

This step updates the selected chassis firmware package with the new version of firmware. You must choose the chassis firmware packages included in the chassis profiles associated with all chassis in the Cisco UCS domain to update all chassis.

- c) Click **Next**.

Step 9

On the **Firmware Package Dependencies** page of the **Install Chassis Firmware** wizard, do the following:

- a) Expand the node for each chassis firmware package listed in the table.
b) Review the list of chassis profiles that include the chassis firmware package.
c) If desired, click a link in one of the following columns:

- **Chassis Pack DN** column—Opens the navigator for the chassis firmware package.
- **Chassis Profile DN** column—Opens the navigator for the chassis profile.

- d) Do one of the following:

- If you want to change one or more of the selected chassis firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate chassis firmware packages and want to review the impact of the chassis firmware upgrade on the endpoints, click **Next**.
- If you want to start the chassis upgrade immediately, click **Install**.

Step 10

On the **Impacted Endpoints Summary** page of the **Install Chassis Firmware** wizard, do the following:

- a) Click the appropriate check boxes to filter the results in the **Impacted Endpoints** table.

You can filter the results by the type of endpoint and by whether the impact of the upgrade is disruptive or not.

- b) Review the list of impacted endpoints.
c) If desired, click the link in the **Maintenance Policy** column to open the navigator for that policy.
d) Do one of the following:

- If you want to change one or more of the selected chassis firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate chassis firmware packages and want to start the chassis upgrade, click **Install**.

Step 11

(Optional) To check on the progress of the chassis firmware upgrade, check the **FSM** tab for each chassis that you are upgrading.

The **Firmware Installer** field on the **Firmware Auto Install** tab shows only the status of an infrastructure firmware upgrade.

Firmware Upgrades through Chassis Firmware Packages in Chassis Profiles

Cisco UCS Manager Release 3.1(2) introduces support for chassis profiles and chassis firmware packages on Cisco UCS S3260 chassis. You can upgrade the firmware of Cisco UCS S3260 chassis endpoints by defining a chassis firmware package and including it in the chassis profile associated with a chassis. You cannot manually upgrade the firmware of a chassis that is associated with a chassis profile.



Note If any chassis component is in the failed state, chassis profile association fails. Cisco recommends bringing the chassis component back up before continuing with chassis profile association. To continue association without bringing the chassis component back up, exclude the component before association.

You cannot upgrade the firmware on a server through chassis profiles. Upgrade the firmware on servers through service profiles.

Servers in a chassis are automatically powered down before the chassis upgrade process begins.

Chassis Firmware Package

This policy enables you to specify a set of firmware versions that make up the chassis firmware package (also known as the chassis firmware pack). The chassis firmware package includes the following firmware for chassis endpoints:

- **Chassis Adapter**
- **Chassis Management Controller**
- **Chassis Board Controller**
- **Local Disk**



Note **Local Disk** is excluded by default from the chassis firmware package.

- **SAS Expander**



Tip You can include more than one type of firmware in the same chassis firmware package. For example, a chassis firmware package can include both board controller firmware and chassis adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a chassis firmware package either when creating a new chassis firmware package or when modifying an existing chassis firmware package. For example, if you do not want to upgrade the board controller firmware through the chassis firmware package, you can exclude board controller firmware from the list of firmware package components.



Important Each chassis firmware package is associated with one list of excluded components.

The chassis firmware package is pushed to all chassis associated with chassis profiles that include this policy.

This policy ensures that the chassis firmware is identical on all chassis associated with chassis profiles that use the same policy. Therefore, if you move the chassis profile from one chassis to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the chassis firmware package, new versions are applied to all the affected chassis profiles immediately.

For a chassis firmware package to take effect, include this policy in a chassis profile, and associate that chassis profile with a chassis.

This policy is not dependent upon any other policies. Ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a chassis with a chassis profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Stages of a Firmware Upgrade through Chassis Firmware Packages in Chassis Profiles

You can use the chassis firmware package policies in chassis profiles to upgrade chassis firmware.



Caution If you modify a chassis firmware package by adding an endpoint or changing firmware versions for an existing endpoint, Cisco UCS Manager upgrades the endpoints after you acknowledge the change by clicking **Pending Activities**. This process disrupts data traffic to and from the chassis.

New Chassis Profile

For a new chassis profile, this upgrade takes place over the following stages:

Chassis Firmware Package Policy Creation

During this stage, you create the chassis firmware package.

Chassis Profile Association

During this stage, you include the chassis firmware package in a chassis profile, and then associate the chassis profile with a chassis. The system pushes the selected firmware versions to the endpoints. The

chassis must be reacknowledged to ensure that the endpoints are running the versions specified in the firmware package.

Existing Chassis Profile

For chassis profiles that are associated with a chassis, Cisco UCS Manager upgrades the firmware after you acknowledge the change by clicking **Pending Activities**.

Effect of Updates to Firmware Packages in Chassis Profiles

To update firmware through a chassis firmware package in a chassis profile, you need to update the firmware in the package. What happens after you save the changes to a firmware package depends upon how the Cisco UCS domain is configured.

The following table describes the most common option for upgrading chassis with a firmware package in a chassis profile.

Chassis Profile	Maintenance Policy	Upgrade Actions
<p>The chassis firmware package is included in one or more chassis profiles, and each chassis profile is associated with one chassis.</p> <p>OR</p> <p>The chassis firmware package is included in an updating chassis profile template, and the chassis profile created from that template is associated with one chassis.</p>	Configured for user acknowledgment	<p>The following occurs when you update the chassis firmware package:</p> <ol style="list-style-type: none"> 1. Cisco UCS asks you to confirm your change and advises that a user-acknowledgement of the chassis is required. 2. Click the flashing Pending Activities button to select the chassis you want to reacknowledge, and apply the new firmware. 3. Cisco UCS verifies the model numbers and vendor against all chassis associated with chassis profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reacknowledges the chassis and updates the firmware. <p>A manual reacknowledgment of the chassis does not cause Cisco UCS to apply the chassis firmware package, nor does it cancel the pending activities. You must acknowledge or cancel the pending activity through the Pending Activities button.</p>

Creating a Chassis Firmware Package



Tip You can include more than one type of firmware in the same chassis firmware package. For example, a chassis firmware package can include both board controller firmware and chassis adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a chassis firmware package either when creating a new chassis firmware package or when modifying an existing chassis firmware package.

Before you begin

Ensure that the appropriate firmware was downloaded to the fabric interconnect.

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Right-click **Chassis Firmware Packages** and choose **Create Chassis Firmware Package**.
- Step 5** In the **Create Chassis Firmware Package** dialog box, enter a unique name and description for the package.
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** From each drop-down list, **Chassis Package**, and **Service Pack**, select the firmware package.
The images from **Service Pack** will take precedence over the images from **Chassis Package**.
- Step 7** In the **Excluded Components** area, check the check boxes corresponding to the components that you want to exclude from this chassis firmware package.
If you do not check any component check boxes, all the listed components are included in the chassis firmware package.
Note Local Disk is excluded by default from the chassis firmware pack.
- Step 8** Click **OK**.

What to do next

Include the policy in a chassis profile or chassis profile template

Updating a Chassis Firmware Package

You can include more than one type of firmware in the same chassis firmware package. For example, a chassis firmware package can include both board controller firmware and chassis adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a chassis firmware package either when creating a new chassis firmware package or when modifying an existing chassis firmware package.



Important Each chassis firmware package is associated with one list of excluded components.

Before you begin

Ensure that the appropriate firmware was downloaded to the fabric interconnect.

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Policies**.
- Step 3** Expand the node for the organization that includes the policy you want to update.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Expand **Chassis Firmware Packages** and choose the policy you want to update.
- Step 5** In the **Work** pane, click the **General** tab.
- Step 6** To modify the components in the chassis firmware package, click **Modify Package Versions**.
The **Modify Package Versions** window appears.
- Step 7** To modify the chassis package, from the **Chassis Package** drop-down list, select the chassis package version.
- Step 8** To modify the service pack, from the **Service Pack** drop-down list, select the service pack version.
To remove the service pack, select **<not set>**.
- Step 9** In the **Excluded Components** area, check the check boxes corresponding to the components that you want to exclude from this chassis firmware package.
If you do not check any component check boxes, all the listed components are included in the chassis firmware package.
- Note** **Local Disk** is excluded by default from the chassis firmware pack.
- Step 10** Click **OK**.
-

Adding Chassis Firmware Packages to an Existing Chassis Profile

If the chassis profile is associated with a chassis, Cisco UCS Manager updates and activates the firmware in the chassis with the new versions after a user acknowledgment.

Procedure

- Step 1** In the **Navigation** pane, click **Chassis**.
- Step 2** Expand **Chassis > Chassis Profiles**.
- Step 3** Expand the node for the organization that includes the chassis profile that you want to update.
If the system does not include multi tenancy, expand the **root** node.
- Step 4** Click the chassis profile to which you want to add the chassis firmware package.
- Step 5** In the **Work** pane, click the **Policies** tab.
- Step 6** Click the down arrows to expand the **Chassis Firmware Package** section.
- Step 7** To add a chassis firmware package, select the desired policy from the **Chassis Firmware Package** drop-down list.
- Step 8** Click **Save Changes**.
-

Upgrading a UCS Domain with Cisco UCS S3260 Servers

Before you begin

- Ensure that all the servers nodes are shut down.
- Ensure that the UCS domain has an assigned chassis policy that references a chassis firmware package policy and a chassis maintenance policy.

Procedure

- Step 1** Upgrade infrastructure firmware through Auto Install. See [Upgrading the Infrastructure Firmware with Auto Install](#).
- Step 2** Update the chassis firmware package policy.
- If you are using the default chassis firmware package policy, update the **default** chassis firmware package policy with the new package version. See [Updating a Chassis Firmware Package, on page 75](#).
 - You can create a new chassis firmware package policy using the new chassis package version, and configure the existing or assigned chassis profile (accept any UserAck). See [Creating a Chassis Firmware Package, on page 74](#) to create a new chassis firmware package policy.

This process may take 1-2 hours. You can monitor the status in the chassis FSM tab.

- Step 3** Update the host firmware. See [Upgrading the Server Firmware with Auto Install](#).
-

Direct Firmware Upgrade on S3260 Chassis and Server Endpoints

The following sections provide detailed information about upgrading S3260 Chassis and Server endpoints.

S3260 Chassis Endpoints

To trigger firmware upgrade on S3260 Chassis components, use the following order:

1. Update CMC 1 firmware
2. Update CMC 2 firmware
3. Update Chassis Adapter 1 firmware
4. Update Chassis Adapter 2 firmware
5. Update SAS Expander 1 firmware
6. Update SAS Expander 2 firmware
7. Activate SAS Expander 1 firmware
8. Activate SAS Expander 2 firmware
9. Activate CMC 1 firmware
10. Activate CMC 2 firmware
11. Activate Chassis Adapter 1 firmware
12. Activate Chassis Adapter 2 firmware
13. Activate Chassis Board Controller



Note You cannot manually update the firmware for local disk in a chassis. The local disk firmware is updated when you explicitly include it in a chassis firmware package.

Cisco UCS S3260 Server Node Endpoints

To trigger firmware upgrade on server endpoints, use the following order:

1. Update CIMC
2. Activate CIMC
3. Update BIOS
4. Activate BIOS
5. Activate Board Controller
6. Activate Storage Controller

While upgrading firmware, Cisco recommends that you use the following order:

1. Upgrade infrastructure—Cisco UCS Manager software and the fabric interconnects
2. Upgrade chassis and server endpoints

While downgrading firmware, Cisco recommends that you use the following order:

1. Downgrade chassis and server endpoints
2. Downgrade infrastructure—Cisco UCS Manager software and the fabric interconnects

Direct Firmware Upgrade on Chassis Endpoints

Updating the CMC Firmware on a S3260 Chassis



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis** > *Chassis Number*
- Step 3** In the **Work** pane, click the **Installed Firmware** tab, select **Chassis Management Controller**, and then click **Update Firmware**.
- Step 4** In the **Update Firmware** dialog box, do the following:
- a) From the **Version** drop-down list, select the firmware version to update the endpoint.
 - b) Click **OK**.

If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

- Step 5** (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Installed Firmware** tab.

What to do next

Activate the firmware.

Updating the Chassis Adapter Firmware on a S3260 Chassis

If the adapter connectivity to both fabric interconnects is down, upgrade is skipped.



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

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

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

Step 3 In the **Installed Firmware** tab, select **Chassis Adapter** and click **Update Firmware**.

Note For Cisco UCS S3260 Chassis with blade servers, the firmware details of Cisco UCS VIC adapters are not displayed in the **Installed Firmware** tab.

Step 4 In the **Update Firmware** dialog box, do the following:

- a) From the **Version** drop-down list, select the firmware version to update the endpoint.
- b) Click **OK**.

If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

Step 5 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Installed Firmware** tab.

What to do next

Activate the firmware.

Updating the SAS Expander Firmware on a S3260 Chassis



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number**
- Step 3** In the **Installed Firmware** tab, select the SAS expander that you want to update and click **Update Firmware**.
- Step 4** In the **Update Firmware** dialog box, do the following:
- From the **Version** drop-down list, select the firmware version to update the endpoint.
 - Click **OK**.

If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

- Step 5** (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Installed Firmware** tab.

What to do next

Activate the firmware.

Activating the SAS Expander Firmware on a S3260 Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number**
- Step 3** In the **Installed Firmware** tab, select the SAS Expander that you want to update and click **Activate Firmware**.
- Step 4** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

- Click **OK**.
-

Activating the CMC Firmware on a S3260 Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number**
- Step 3** In the **Installed Firmware** tab, select **Chassis Management Controller** and then click **Activate Firmware**.
- Step 4** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - Click **OK**.
-

Activating the Chassis Adapter Firmware on a S3260 Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number**
- Step 3** In the **Installed Firmware** tab, select **Chassis Adapter** and then click **Activate Firmware**.
- Step 4** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - Click **OK**.
-

Activating the Chassis Board Controller Firmware on a S3260 Chassis



Note Cisco UCS Manager does not support activation of chassis board controller firmware to earlier versions.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number**

Step 3 In the **Installed Firmware** tab, select **Board Controller** and then click **Activate Firmware**.

Step 4 In the **Activate Firmware** dialog box, do the following:

- a) Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

- b) Click **OK**.
-

Direct Firmware Upgrade on Server Endpoints

Updating the CIMC Firmware on a Cisco UCS S3260 Server Node



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

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

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

Step 3 Expand the node for the server for which you want to update the CIMC.

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

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Update Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

- a) From the **Version** drop-down list, select the firmware version to update the endpoint.
- b) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

Step 8 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to do next

Activate the firmware.

Activating the CIMC Firmware on a Cisco UCS S3260 Server Node

The activation of firmware for a CIMC does not disrupt data traffic. However, it will interrupt all KVM sessions and disconnect any vMedia attached to the server.



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.
- Step 4** On the **Work** pane, click the **Inventory** tab.
- Step 5** Click the **CIMC** tab.
- Step 6** In the **Actions** area, click **Activate Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:
 - a) Select the appropriate version from the **Version To Be Activated** drop-down list.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.

If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.
 - c) Click **OK**.

Updating the BIOS Firmware on a Cisco UCS S3260 Server Node



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server for which you want to update the BIOS firmware.
- Step 4** In the **Work** pane, click the **Inventory** tab.
- Step 5** Click the **Motherboard** tab.
- Step 6** In the **Actions** area, click **Update BIOS Firmware**.
- Step 7** In the **Update Firmware** dialog box, do the following:
- From the **Version** drop-down list, select the firmware version to which you want to update the server BIOS.
 - (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Force** check box.
 - Click **OK**.
- Cisco UCS Manager copies the selected server BIOS firmware package to the backup memory slot, where it remains until you explicitly activate it.
- The update is complete when the **BIOS** area of the **Motherboard** tab displays **Ready** in the **Update Status** column for the **Backup Version**.
-

What to do next

Activate the firmware.

Activating the BIOS Firmware on 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** Expand the node for the server for which you want to activate the updated BIOS firmware.
- Step 4** In the **Work** pane, click the **Inventory** tab.
- Step 5** Click the **Motherboard** tab.
- Step 6** In the **Actions** area, click **Activate BIOS Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate server BIOS version from the **Version To Be Activated** drop-down list.
 - If you want to set the startup version and not change the version running on the server, check the **Set Startup Version Only** check box.
- If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the server is not immediately rebooted. The activated firmware does not become the running version of firmware until the server is rebooted.

- c) Click **OK**.

Activating the Board Controller Firmware on a Cisco UCS S3260 Server Node



Note This activation procedure causes the server to reboot. Depending upon whether the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. Cisco recommends that you upgrade the board controller firmware through the host firmware package in the service profile as the last step of upgrading a Cisco UCS domain, along with upgrading the server BIOS. This reduces the number of times a server needs to reboot during the upgrade process.

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
- Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**. Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.
- Step 6** For the board controller you want to update, select a version from the **Startup Version** drop-down list.
- Step 7** Click **OK**.
- Step 8** (Optional) You can also use the **Force Board Controller Activation** option to update the firmware version when you upgrade CPUs with different architectures.

Activating the Storage Controller Firmware on 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** Select the server on which you want to activate the storage controller.
- Step 4** In the **Installed Firmware** tab, select **Storage Controller** and then click **Activate Firmware**.
- Step 5** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

- b) Click **OK**.
-



CHAPTER 8

Chassis Management

- [The Cisco UCS S3260 Chassis, on page 87](#)
- [Acknowledging a Chassis, on page 88](#)
- [Decommissioning a Chassis, on page 88](#)
- [Removing a Chassis, on page 89](#)
- [Turning on the Locator LED for a Chassis, on page 89](#)
- [Turning off the Locator LED for a Chassis, on page 89](#)
- [Creating a Zoning Policy from Inventory, on page 90](#)
- [Viewing the POST Results for a Chassis, on page 90](#)

The Cisco UCS S3260 Chassis

Cisco UCS Manager Release 4.2(3) introduces support for the Cisco UCS S3260 chassis on Cisco UCS 6536 Fabric Interconnect.

Cisco UCS Manager Release 4.1(1) introduces support for the Cisco UCS S3260 chassis on Cisco UCS 64108 Fabric Interconnect.

Cisco UCS Manager Release 4.0(1) introduces support for the Cisco UCS S3260 chassis on Cisco UCS 6454 Fabric Interconnect.

Cisco UCS Manager Release 3.1(2) introduces support for the Cisco UCS S3260 chassis on Cisco UCS 6300 Series fabric interconnect setups.

The Cisco UCS S3260 chassis is a 4U chassis that is designed to operate in a standalone environment and also as part of the Cisco Unified Computing System. It has the following main components:

- Four 1050 Watt AC modular power supplies (2 + 2 shared and redundant mode of operation)
- Two System IO Controller (SIOC) slots
- Two storage server slots out of which one can be used for storage expansion



Note The second server slot in the chassis can be utilized by an HDD expansion tray module for an additional four 3.5” drives.

- 56 3.5” drive bays with an optional 4 x 3.5” HDD expansion tray module instead of the second server

- Up to 360 TB storage capacity by using 6 TB HDDs
- Serial Attached SCSI (SAS) expanders that can be configured to assign the 3.5” drives to individual server modules
- The two servers in the chassis can be replaced by a single, dual-height server with an IO expander

Acknowledging a Chassis

Perform the following procedure if you change the port that connects the chassis to the fabric interconnect. Acknowledging the chassis ensures that Cisco UCS Manager is aware of the change in the port.

After you change the port that connects the chassis to the fabric interconnect, wait for at least 1 minute before you reacknowledge the chassis.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis**.
- Step 3** Choose the chassis that you want to acknowledge.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Actions** area, click **Acknowledge Chassis**.
- Step 6** If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Cisco UCS Manager disconnects the chassis and then rebuilds the connections between the chassis and the fabric interconnect or fabric interconnects in the system.

Decommissioning a Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis**.
- Step 3** Choose the chassis that you want to decommission.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Actions** area, click **Decommission Chassis**.
- Step 6** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The decommission process may take several minutes to complete.

Removing a Chassis

Before you begin

Physically remove the chassis before performing the following procedure.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment > Chassis**.
 - Step 3** Choose the chassis that you want to remove.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Actions** area, click **Remove Chassis**.
 - Step 6** If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
- The removal may take several minutes to complete.
-

Turning on the Locator LED for a Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment > Chassis**.
 - Step 3** Click the chassis that you need to locate.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Actions** area, click **Turn on Locator LED**.
- This action is not available if the locator LED is already turned on.
- The LED on the chassis starts flashing.
-

Turning off the Locator LED for a Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis**.

Step 3 Choose the chassis for which you want to turn off the locator LED.

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

Step 5 In the **Actions** area, click **Turn off Locator LED**.

This action is not available if the locator LED is already turned off.

The LED on the chassis stops flashing.

Creating a Zoning Policy from Inventory

You can create a disk zoning policy from the existing inventory and disk ownership.



Note Creating a disk zoning policy from the existing inventory is supported only on Cisco UCS S3260 chassis.

Procedure

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

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

Step 3 Choose the chassis for which you want to create a zoning policy.

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

Step 5 In the **Actions** area, click **Create Zoning Policy from Inventory**.

Step 6 In the **Create Zoning Policy from Inventory** dialog box that appears, do the following:

- a) Enter the **Disk Zoning Policy Name**.
- b) Select the organization where you want to create the policy.
- c) Click **OK**.

Step 7 In the confirmation dialog box that appears, click **OK**.

Viewing the POST Results for a Chassis

You can view any errors collected during the Power On Self-Test process for all servers and adapters in a chassis.

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 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 each server in the chassis 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.



CHAPTER 9

Server Management

- [Cisco UCS S3260 Server Node Management, on page 93](#)
- [Booting a Cisco UCS S3260 Server Node, on page 94](#)
- [Booting a Cisco UCS S3260 Server Node from the Service Profile , on page 94](#)
- [Determining the Boot Order of a Cisco UCS S3260 Server Node, on page 95](#)
- [Shutting Down a Cisco UCS S3260 Server Node, on page 95](#)
- [Shutting Down a Cisco UCS S3260 Server Node from the Service Profile , on page 96](#)
- [Resetting a Cisco UCS S3260 Server Node, on page 96](#)
- [Resetting a Cisco UCS S3260 Server Node to Factory Default Settings, on page 97](#)
- [Reacknowledging a Cisco UCS S3260 Server Node, on page 98](#)
- [Removing a Cisco UCS S3260 Server Node from a Chassis, on page 98](#)
- [Deleting the Inband Configuration from a Cisco UCS S3260 Server Node, on page 99](#)
- [Decommissioning a Cisco UCS S3260 Server Node, on page 99](#)
- [Recommissioning a Cisco UCS S3260 Server Node, on page 100](#)
- [Reacknowledging a Server Slot in a S3260 Chassis, on page 100](#)
- [Removing a Non-Existent Cisco UCS S3260 Server Node from the Configuration Database, on page 101](#)
- [Turning the Locator LED for a Cisco UCS S3260 Server Node On and Off, on page 102](#)
- [Turning the Local Disk Locator LED on a Cisco UCS S3260 Server Node On and Off, on page 102](#)
- [Resetting the CIMC for a Cisco UCS S3260 Server Node, on page 103](#)
- [Resetting the CMOS for a Cisco UCS S3260 Server Node, on page 103](#)
- [Resetting the BIOS Password for a S3X60 Server, on page 104](#)
- [Issuing an NMI from a Cisco UCS S3260 Server Node, on page 104](#)
- [Viewing the POST Results for a Cisco UCS S3260 Server Node, on page 104](#)
- [Viewing Health Events for a Cisco UCS S3260 Server Node, on page 105](#)
- [Health LED Alarms, on page 107](#)

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:
- Click the **Power Cycle** option.
 - (Optional) Check the check box if you want Cisco UCS Manager to complete all management operations that are pending on this server.
 - 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:
- Click **Reset to Factory Default**.
 - 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.

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

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

- 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.
- 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.

Removing a Cisco UCS S3260 Server Node 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 **Decommission**, 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 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

- Step 1** In the **Navigation** pane, click **Servers**.
- 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 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 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:
- Click **Decommission**.
 - 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 for Cisco UCS Manager to rediscover the server.
- After decommissioning the Cisco UCS S3260 server, you must wait for few minutes to initiate the recommissioning of the server.

For more information, see [Recommissioning a Cisco UCS S3260 Server Node, on page 100](#)

Recommissioning a Cisco UCS S3260 Server Node

Before you begin

In case of recommissioning the server after decommission, you should wait for few minutes to initiate the recommission of the server.

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 reactnowledge.
- Step 4** If Cisco UCS Manager displays a **Resolve Slot Issue** dialog box, do one of the following:

Option	Description
The here link in the Situation area	Click this link and then click Yes in the confirmation dialog box. Cisco UCS Manager reactnowledges the slot and discovers the server in the slot.
OK	Click this button if you want to proceed to the General tab. You can use the Reactnowledge Slot link in the Actions area to have Cisco UCS Manager reactnowledge the slot and discover the server in the slot.

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 98](#).

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 the management controller of the blade 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**.
-

Resetting the BIOS Password for a S3X60 Server

This option allows you to reset the BIOS password without using the F2 BIOS configuration prompt. Resetting the BIOS password is not part of the normal maintenance of a server. After BIOS password reset, the server is rebooted immediately and the new BIOS password gets updated.

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 BIOS password.
 - 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 BIOS Password**, 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:

Name	Description
Health Summary area	
Health Qualifier field	Comma-separated names of all the health events that are triggered for the component.

Name	Description
Health Severity field	<p>Highest severity of all the health events that are triggered for the component. This can be one of the following:</p> <ul style="list-style-type: none"> • critical • major • minor • warning • info • cleared <p>Note The severity levels listed here are from highest to lowest severity.</p>
Health Details area	
Severity column	<p>Severity of the health event. This can be one of the following:</p> <ul style="list-style-type: none"> • critical • major • minor • warning • info • cleared <p>Note The severity levels listed here are from highest to lowest severity.</p>
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.

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:

Name	Description
Severity column	The severity of the alarm. This can be one of the following: <ul style="list-style-type: none"> • Critical - The server health LED blinks amber. This is indicated with a red dot. • Minor - The server health LED is amber. This is indicated with an orange dot.
Description column	A brief description of the alarm.
Sensor ID column	The ID of the sensor that triggered the alarm.
Sensor Name column	The name of the sensor that triggered the alarm.

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.
-



CHAPTER 10

SIOC Management

- [SIOC Management in Cisco UCS Manager](#) , on page 109
- [Acknowledging an SIOC](#), on page 110
- [Migrating to SIOC with PCIe Support](#), on page 111
- [Resetting the CMC](#), on page 111
- [CMC Secure Boot](#), on page 111

SIOC Management in Cisco UCS Manager

You can manage and monitor all System Input/Output Controllers (SIOC) in a Cisco UCS domain through Cisco UCS Manager.

SIOC Removal or Replacement

You can remove or replace an SIOC from a chassis. Removal or replacement of an SIOC is a service-affecting operation, which requires you to power down the entire chassis.

Guidelines for SIOC Removal

- To remove the active SIOC, or both SIOCs, shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
- Removal of SIOCs from a chassis results in the entire chassis being disconnected from Cisco UCS Manager.

SIOC Removal

Do the following to remove an SIOC from the system:

1. Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
2. Disconnect the cables connecting the SIOC to the system.
3. Remove the SIOC from the system.

SIOC Replacement

Do the following to remove an SIOC from the system and replace it with another SIOC:

1. Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
2. Disconnect the cables connecting the SIOC to the system.
3. Remove the SIOC from the system.
4. Connect the new SIOC to the system.
5. Connect the cables to the SIOC.
6. Connect power cords and then power on the system.
7. Acknowledge the new SIOC.

The server connected to the replaced SIOC is rediscovered.



Note If the firmware of the replaced SIOC is not the same version as the peer SIOC, then it is recommended to update the firmware of the replaced SIOC by re-triggering chassis profile association.

Acknowledging an SIOC

Cisco UCS Manager has the ability to acknowledge a specific SIOC in a chassis. Perform the following procedure when you replace an SIOC in a chassis.



Caution This operation rebuilds the network connectivity between the SIOC and the fabric interconnects to which it is connected. The server corresponding to this SIOC becomes unreachable, and traffic is disrupted.

NVMe slot-1 in SIOC is mapped to server 1 and NVMe slot-2 to server 2. Cisco UCS Manager triggers rediscovery on both the servers since SIOC has NVMe mapped to both the servers.

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **SIOC**
 - Step 3** Choose the SIOC that you want to acknowledge.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Actions** area, click **Acknowledge SIOC**.
 - Step 6** In the **Acknowledge SIOC** confirmation box, click **Yes**.
-

Migrating to SIOC with PCIe Support

Before you begin

Ensure that the Cisco UCS Manager is at release 4.0(1a) or higher.

Procedure

- Step 1** Update the chassis and server firmware to 4.0(1) release.
 - Step 2** Decommission the chassis.
 - Step 3** Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
 - Step 4** Disconnect the cables connecting the SIOC to the system.
 - Step 5** Remove the SIOC from the system.
 - Step 6** Connect the new SIOC to the system.
 - Step 7** Connect the cables to the SIOC.
 - Step 8** Connect power cords and then power on the system.
 - Step 9** Acknowledge the new SIOC.
-

Resetting the CMC

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **SIOC** > *SIOC Number*
 - Step 3** In the **Work** pane, click the **Chassis Management Controller** tab.
 - Step 4** In the **Actions** area, click **Reset CMC**.
 - Step 5** In the **Reset CMC** confirmation box, click **Yes**.
-

CMC Secure Boot

With Chassis Management Controller (CMC) secure boot, only Cisco-signed firmware images can be installed and run on the CMC. When the CMC 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 CMC firmware.

Guidelines and Limitations for CMC Secure Boot

- CMC secure boot is supported only on the Cisco UCS S3260 chassis.
- When chassis association is in progress, enabling secure boot on one of the SIOCs will result in a failed operation.
- After CMC secure boot is enabled, it cannot be disabled.
- CMC secure boot is specific to the SIOC on which it is enabled. If you replace the SIOC on which CMC secure boot is enabled, the **Secure boot operational state** field will now display the secure boot status of the new SIOC.
- After CMC secure boot is enabled on a chassis, you cannot move the chassis back to non-cluster setup and downgrade the firmware to a CMC firmware image earlier than Cisco IMC Release 2.0(13).
- The **Secure boot operational state** field shows the secure boot status. This can be one of the following:
 - **Disabled**—When CMC secure boot is not enabled. This is the default state.
 - **Enabling**—When CMC secure boot is being enabled.
 - **Enabled**—When CMC secure boot is enabled.
- Beginning with 4.0(1), **Secure boot operational state** is **Enabled** by default and is not user configurable. The option is grayed out.

Enabling CMC Secure Boot

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **SIOC**
- Step 3** Choose the SIOC on which you want to enable CMC secure boot.
- Step 4** In the **Work** pane, click the **Chassis Management Controller** tab.
- Step 5** In the **Actions** area, click **Enable Secure Boot**.

The **Enable Secure Boot** confirmation box appears with the following warning:

When committed, CMC secure boot and installation will be enabled. This is an irreversible operation. Are you sure you want to enable secure boot.

- Step 6** Click **Yes**.
-