Cisco UCS Central Storage Management Guide, Release 2.0

First Published: 2017-05-16

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

Audience

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

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

Conventions

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

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

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

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

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: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

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

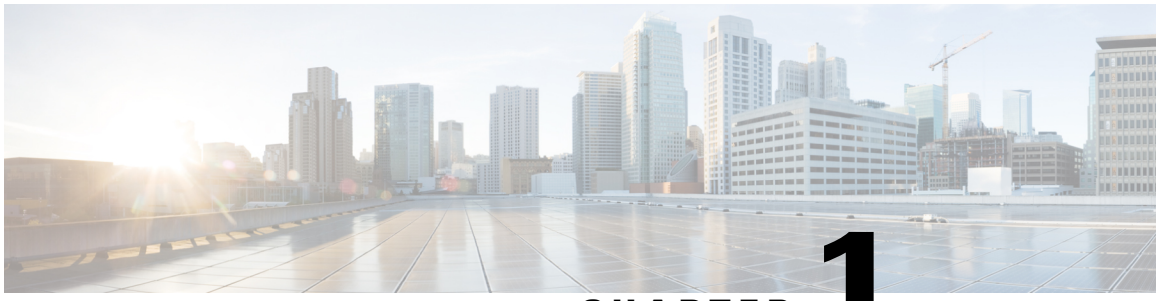
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

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



CHAPTER 1

Overview

Overview

This guide contains conceptual and procedural information on the following components that are intrinsic to Cisco UCS Central storage management:

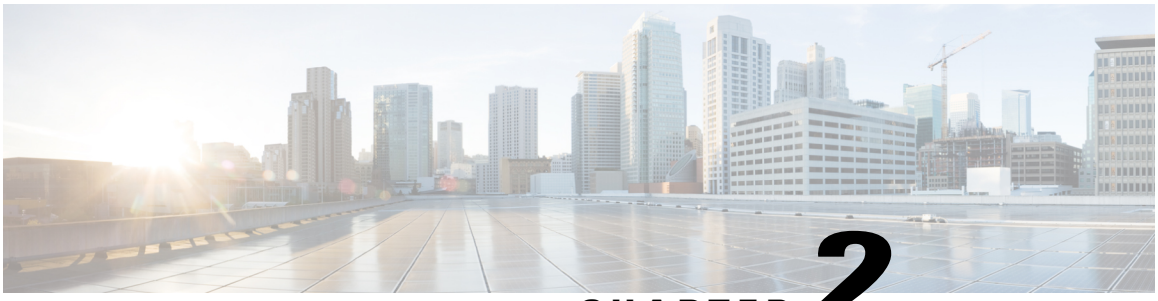
- Ports and port channels
- SAN and VSAN
- vHBA
- Storage Pools
- Storage Policies
- Storage Profiles

Cisco UCS Central User Documentation Reference

The Cisco UCS Central following use case-based documents to understand and configure Cisco UCS Central:

Guide	Description
Cisco UCS Central Getting Started Guide	Provides a brief introduction to the Cisco UCS infrastructure, Cisco UCS Manager, and Cisco UCS Central. Includes an overview of the HTML5 UI, how to register Cisco UCS domains in Cisco UCS Central, and how to activate licenses.
Cisco UCS Central Administration Guide	Provides information on administrative tasks, such as user management, communication, firmware management, backup management, and Smart Call Home.

Guide	Description
Cisco UCS Central Authentication Guide	Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP.
Cisco UCS Central Server Management Guide	Provides information on server management, such as equipment policies, physical inventory, service profiles and templates, server pools, server boot, and server policies.
Cisco UCS Central Storage Management Guide	Provides information on storage management, such as ports and port channels, VSAN and vHBA management, storage pools, storage policies, storage profiles, disk groups, and disk group configuration.
Cisco UCS Central Network Management Guide	Provides information on network management, such as ports and port channels, VLAN and vNIC management, network pools, and network policies.
Cisco UCS Central Operations Guide	Best practices for setting up, configuring, and managing domain groups for small, medium and large deployments.
Cisco UCS Central Troubleshooting Guide	Provides help for common issues in Cisco UCS Central.



CHAPTER 2

Ports and Port Channels

Server and Uplink Ports

Each fabric interconnect can include the following port types:

Server Ports

Server ports handle data traffic between the fabric interconnect and the adapter cards on the servers.

Uplink Ethernet Ports

Uplink Ethernet ports handle Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports.

By default, Ethernet ports are unconfigured. However, you can configure them to function in the following ways:

- Uplink
- FCoE
- Appliance

You can configure uplink Ethernet ports on either the fixed module or an expansion module.

Uplink Fibre Channel Ports

Uplink Fibre Channel ports handle FCoE traffic between the fabric interconnect and the next layer of the storage area network. All network-bound FCoE traffic is pinned to one of these ports.

By default, Fibre Channel ports are uplink. However, you can configure them to function as Fibre Channel storage ports. This is useful in cases where Cisco UCS requires a connection to a Direct-Attached Storage (DAS) device.

You can only configure uplink Fibre Channel ports on an expansion module. The fixed module does not include uplink Fibre Channel ports.

Unified Ports

Unified ports can be configured to carry either Ethernet or Fibre Channel traffic. These ports are not reserved. A Cisco UCS domain cannot use these ports until you configure them.

All ports on the following fabric interconnects are unified:

- Cisco UCS 6248 UP Fabric Interconnect
- Cisco UCS 6296 UP Fabric Interconnect
- Cisco UCS 6324 Fabric Interconnect
- Cisco UCS 6332-16UP Fabric Interconnect

Note When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. If the port is connected to another device, this may cause traffic disruption. You can disable the port after configuring it.

Unified Storage Ports

Unified storage is configuring the same physical port as an Ethernet storage interface and FCoE storage interface. You can configure any appliance port or FCoE storage port as a unified storage port on either a

fixed module or an expansion module. To configure a unified storage port, the fabric interconnect must be in Fibre Channel switching mode.

In a unified storage port, you can enable/disable individual FCoE storage or appliance interfaces.

- In an unified storage port, if you do not specify a non default VLAN for the appliance port the fcoe-storage-native-vlan will be assigned as the native VLAN on the unified storage port. If the appliance port has a non default native VLAN specified as native VLAN, this will be assigned as the native VLAN for unified storage port.
- When you enable or disable the appliance interface, the corresponding physical port is enabled/disabled. So when you disable the appliance interface in a unified storage, even if the FCoE storage is enabled, it goes down with the physical port.
- When you enable or disable FCoE storage interface, the corresponding VFC is enabled or disabled. So when the FCoE storage interface is disabled in a unified storage port, the appliance interface will continue to function normally.

Unified Uplink Ports

When you configure an Ethernet uplink and an FCoE uplink on the same physical Ethernet port, it is called the unified uplink port. You can individually enable or disable either FCoE or Ethernet interfaces independently.

- Enabling or disabling the FCoE uplink results in corresponding VFC being enabled or disabled.
- Enabling or disabling an Ethernet uplink results in corresponding physical port being enabled or disabled.

If you disable an Ethernet uplink, it disables the underlying physical port in an unified uplink. So, even if the FCoE uplink is enabled, the FCoE uplink also goes down. But if you disable an FCoE uplink, only the VFC goes down. If the Ethernet uplink is enabled, it can still function properly in the unified uplink port.

Ports on the Cisco UCS 6300 Series Fabric Interconnects

The Cisco UCS 6300 Series Fabric Interconnect includes the Cisco UCS 6324 Fabric Interconnect for UCS Mini (Cisco UCS Manager Release 3.0), and the Cisco UCS 6332 and 6332-16UP Fabric Interconnects (Cisco UCS Manager Release 3.1).

The following table summarizes the port usage for the Cisco UCS 6300 Series Fabric Interconnects:

Fabric Interconnect Name:	Cisco UCS 6324 (Cisco UCS Mini)	Cisco UCS 6332	Cisco UCS 6332-16UP
Description:	Fabric Interconnect with 4 unified ports and 1 scalability port	32–Port Fabric Interconnect	40–Port Fabric Interconnect
Number of fixed 40 GB Interfaces:	—	6 (ports 17-32)	6 (ports 35-40)
Number of 1GB/10GB Interfaces (depending on the SFP module installed)	All	Ports 5–26 using breakout cable	Ports 17–34 using breakout cable

Fabric Interconnect Name:	Cisco UCS 6324 (Cisco UCS Mini)	Cisco UCS 6332	Cisco UCS 6332-16UP
Unified Ports (8 Gb/s, FC, FCoE)	4	None	Ports 1–16

Note Cisco UCS 6300 Series Fabric Interconnects support breakout capability for ports. For more information on how the 40G ports can be converted into four 10G ports, see Scalability and Breakout Ports, on page 16.

Port Modes

The port mode determines whether a unified port on the fabric interconnect is configured to carry Ethernet or Fibre Channel traffic. The fabric interconnect does not automatically discover the port mode. You configure the port mode in Cisco UCS Central.

Changing the port mode deletes the existing port configuration and replaces it by a new logical port. Any objects associated with that port configuration, such as VLANs and VSANS, are removed. There is no restriction on the number of times you can change the port mode for a unified port.

Effect of Port Mode Changes on Data Traffic

Port mode changes can cause an interruption to the data traffic for the Cisco UCS domain. The length of the interruption and the traffic that is affected depend upon the configuration of the Cisco UCS domain and the module on which you made the port mode changes.

Tip To minimize the traffic disruption during system changes, form a Fibre Channel uplink port-channel across the fixed and expansion modules.

Impact of Port Mode Changes on an Expansion Module

After you make port mode changes on an expansion module, the module reboots. All traffic through ports on the expansion module is interrupted for approximately one minute while the module reboots.

Impact of Port Mode Changes on the Fixed Module in a Cluster Configuration

A cluster configuration has two fabric interconnects. After you make port changes to the fixed module, the fabric interconnect reboots. The impact on the data traffic depends upon whether or not you have configured the server vNICs to failover to the other fabric interconnect when one fails.

If you change the port modes on the expansion module of one fabric interconnect and then wait for that to reboot before changing the port modes on the second fabric interconnect, the following occurs:

- With server vNIC failover, traffic fails over to the other fabric interconnect and no interruption occurs.

- Without server vNIC failover, all data traffic through the fabric interconnect on which you changed the port modes is interrupted for approximately eight minutes while the fabric interconnect reboots.

If you change the port modes on the fixed modules of both fabric interconnects simultaneously, all data traffic through the fabric interconnects are interrupted for approximately eight minutes while the fabric interconnects reboot.

Impact of Port Mode Changes on the Fixed Module in a Standalone Configuration

A standalone configuration has only one fabric interconnect. After you make port changes to the fixed module, the fabric interconnect reboots. All data traffic through the fabric interconnect is interrupted for approximately eight minutes while the fabric interconnect reboots.

Port Roles

The port role defines the type of traffic carried over a unified port connection.

All of the port roles listed are configurable on both the fixed and expansion module, including server ports, which are configurable on the 6200 and later series fabric interconnect expansion modules.

By default, unified ports changed to Ethernet port mode are set to the uplink Ethernet port role. Unified ports changed to Fibre Channel (FC) port mode are set to the FC uplink port role. You cannot unconfigure FC ports.

Changing the port role does not require a reboot.

When you set the port mode to Ethernet, you can configure the following port roles:

- Server ports
- Ethernet uplink ports
- FCoE storage ports
- FCoE uplink ports
- Appliance ports

When you set the port mode to FC, you can configure the following port roles:

- FC uplink ports
- FC storage ports

Guidelines for Configuring Unified Ports

Consider the following guidelines and restrictions when configuring unified ports:

Hardware and Software Requirements

Unified ports are not supported on 6100 series fabric interconnects.

Port Mode Placement

Because the Cisco UCS Central GUI interface uses a slider to configure the port mode for unified ports on a fixed or expansion module, it automatically enforces the following restrictions which limits how port modes

can be assigned to unified ports. When using the Cisco UCS Central CLI interface, these restrictions are enforced when you commit the transaction to the system configuration. If the port mode configuration violates any of the following restrictions, the Cisco UCS Central CLI displays an error:

- Ethernet ports must be grouped together in a block. For each module (fixed or expansion), the Ethernet port block must start with the first port and end with an even numbered port.
- Fibre Channel ports must be grouped together in a block. For each module (fixed or expansion), the first port in the Fibre Channel port block must follow the last Ethernet port and extend to include the rest of the ports in the module. For configurations that include only Fibre Channel ports, the Fibre Channel block must start with the first port on the fixed or expansion module.
- Alternating Ethernet and Fibre Channel ports is not supported on a single module.

Example of a valid configuration— Might include unified ports 1–16 on the fixed module configured in Ethernet port mode and ports 17–32 in Fibre Channel port mode. On the expansion module you could configure ports 1–4 in Ethernet port mode and then configure ports 5–16 in Fibre Channel mode. The rule about alternating Ethernet and Fibre Channel port types is not violated because this port arrangement complies with the rules on each individual module.

Example of an invalid configuration— Might include a block of Fibre Channel ports starting with port 16. Because each block of ports has to start with an odd-numbered port, you would have to start the block with port 17.

Note The total number of uplink Ethernet ports and uplink Ethernet port channel members that can be configured on each fabric interconnect is limited to 31. This limitation includes uplink Ethernet ports and uplink Ethernet port channel members configured on the expansion module.

The 40GB ports on the 6300 series fabric interconnects do not support expansion module configuration.

Cautions and Guidelines for Configuring Unified Uplink Ports and Unified Storage Ports

The following are cautions and guidelines to follow while working with unified uplink ports and unified storage ports:

- You must configure a non default native VLAN on FCoE and unified uplink ports. This VLAN is not used for any traffic. Cisco UCS Central will reuse an existing fcoe-storage-native-vlan for this purpose. This fcoe-storage-native-vlan will be used as a native VLAN on FCoE and unified uplinks.
- In an unified uplink port, if you do not specify a non default VLAN for the Ethernet uplink port the fcoe-storage-native-vlan will be assigned as the native VLAN on the unified uplink port. If the Ethernet port has a non default native VLAN specified as native VLAN, this will be assigned as the native VLAN for unified uplink port.
- When you create or delete a member port under an Ethernet port channel, Cisco UCS Central automatically creates or deletes the member port under FCoE port channel. The same happens when you create or delete a member port in FCoE port channel.

- When you configure an Ethernet port as a standalone port, such as server port, Ethernet uplink, FCoE uplink or FCoE storage and make it as a member port for an Ethernet or FCOE port channel, Cisco UCS Central automatically makes this port as a member of both Ethernet and FCoE port channels.
- When you remove the membership for a member port from being a member of server uplink, Ethernet uplink, FCoE uplink or FCoE storage, Cisco UCS Central deletes the corresponding members ports from Ethernet port channel and FCoE port channel and creates a new standalone port.
- For unified uplink ports and unified storage ports, when you create two interfaces, only one license is checked out. As long as either interface is enabled, the license remains checked out. The license will be released only if both the interfaces are disabled for a unified uplink port or a unified storage port.
- Cisco UCS 6100 series fabric interconnect switch can only support 1VF or 1VF-PO facing same downstream NPV switch.

Configuring Unified Ports

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click the **Tools** icon and choose **Unified Port Configuration**.

Step 4 Use your mouse to drag the slider along the bar until the displays shows the port mode configuration that you want to use.
The ports are displayed as follows:

- Ethernet ports are displayed in green.
- FC ports are displayed in purple.
- Disabled ports are displayed in faded green or purple.

Note Depending on the server, the Ethernet and FC port slider may be reversed.

Step 5 Click **Configure**.

Note Configuring unified ports reboots the FI, and can cause an interruption to the data traffic for the Cisco UCS domain.

Configuring Ports

Note Ports configured for Cisco UCS Manager releases prior to 3.1 were supported in Cisco UCS Central release 1.3, but are not supported in later releases of Cisco UCS Central. Any additional configuration of those ports must be done in Cisco UCS Manager.

Before You Begin

- You must be running Cisco UCS Manager release 3.1 or above.
- All Cisco UCS Manager domains must be included in a Cisco UCS Central domain group.
- Port Configuration must be set to Global on the Policy Resolution Control page in Cisco UCS Manager.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.

Step 6 Select the **Role** for the port.
For Ethernet ports, this can be one of the following:

- Appliance
- FCoE Storage
- FCoE Uplink
- Server
- Uplink

For FC ports, this can be one of the following:

- FC Uplink
- FC Storage

Step 7 Complete the fields as required for your selection.

Step 8 Click **Save**.

Configuring an Appliance Port

Appliance ports are used to connect fabric interconnects to directly attached NFS storage.

Note If you are changing the configuration from an FCoE storage port to an appliance port, admin users have the option to make the port appliance only or unified storage.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **Appliance**.

Step 7 On the **Basic** tab, do the following:

a) Enter the **Interface User Label**.
b) Select the port speed.
c) Select the quality of service setting associated with this interface. This can be one of the following:

- **Platinum—**Use this priority for vNIC traffic only.
- **Gold—**Use this priority for vNIC traffic only.
- **Silver—**Use this priority for vNIC traffic only.
- **Bronze—**Use this priority for vNIC traffic only.
- **Best Effort—**Do not use this priority. It is reserved for the Basic Ethernet traffic lane.
- **Fibre Channel—**Use this priority for vHBA traffic only.

Step 8 On the **Policies** tab, select the flow control policy, pin group, and network control policy.
Note Only network control policies of type Appliance are supported and available for appliance port configuration.

Step 9 On the **VLANs** tab, choose whether the port will be a **Truck** or **Access** port, and select the VLANs that you want to assign to the ports.
You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

- Trunk ports can have multiple VLANs and allow the VLANs to transport between switches over the trunk link.
- Access ports have one VLAN and is connected to an end point. If the VLAN is a primary VLAN, secondary VLANs are required.

The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

Note Only VLANs of type Appliance are supported and available for appliance port configuration.

Step 10 On the **Ethernet Target Endpoint** tab, click **Enabled** to enter the **Name** and **MAC Address** for the endpoint.
The Ethernet target endpoint is disabled by default.

Step 11 Click **Save**.

Configuring an FCoE Storage Port

Fibre Channel over Ethernet (FCoE) Storage ports allow storage consolidation from two separate links to a single storage that carries both Fibre Channel (FC) and Ethernet traffic.

Note If you are changing the configuration from an appliance port to an FCoE storage port, admin users have the option to make the port FCoE storage only or unified storage.

Before You Begin

The Fibre Channel switching mode must be set to Switching for these ports to be valid. The storage ports cannot function in end-host mode.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FCoE Storage**.

Step 7 On the **Basic** tab, enter the **Interface User Label**.

Step 8 On the **VSAN** tab, select the VSANs that you want to assign to the ports.
The VSANs that you select are displayed in the **VSAN** column. VSANs that were created in Cisco UCS Manager are displayed in the **VSAN on Domain** column.

Note Only VSANs of type Storage are supported and available for FCoE storage port configuration.

Step 9 Click **Save**.

Configuring an FCoE Uplink Port

FCoE Uplink ports are physical Ethernet interfaces between the fabric interconnects and the upstream Ethernet switch, used for carrying FCoE traffic. With this support, the same physical Ethernet port can carry both Ethernet traffic and Fibre Channel traffic.

Note If you are changing the configuration from an uplink port to an FCoE uplink port, admin users have the option to make the port FCoE uplink only or unified uplink.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.
Step 2 Click on a Fabric Interconnect to open it for editing.
Step 3 Click **Ports**.
Step 4 Choose the port that you want to configure.
Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.
Step 6 In the **Role** drop-down, select **FCoE Uplink**.
Step 7 On the **Basic** tab, enter the **Interface User Label**.
Step 8 On the **Policies** tab, select the link profile policy that you want to assign to the port.
Step 9 Click **Save**.

Configuring a Server Port

Server Ports handle data traffic between the Fabric Interconnect and the adapter cards on the servers. Server ports are only configurable on the 6200 series and 6300 series fabric interconnect expansion modules.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.
Step 2 Click on a Fabric Interconnect to open it for editing.
Step 3 Click **Ports**.
Step 4 Choose the port that you want to configure.
Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.
Step 6 In the **Role** drop-down, choose **Server**.
Step 7 In the **Server** field, enter the **Interface User Label**.
Step 8 Click **Save**.

Configuring an Uplink Port

Ethernet Uplink Ports connect to external LAN Switches. Network bound Ethernet traffic is pinned to one of these ports.

Note If you are changing the configuration from an FCoE uplink port to an uplink port, admin users have the option to make the port uplink only or unified uplink.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **Uplink**.

Step 7 On the **Basic** tab, do the following:

a) Enter the **Interface User Label**.

b) Select the port speed.

Step 8 On the **VLANs** tab, select the VLANs that you want to assign to the ports.
The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

Note Only VLANs of type LAN are supported and available for uplink port configuration.

Step 9 From the **VLAN Groups** tab, select the VLAN groups you want to assign to the ports.
The VLAN Groups that you select are displayed in the **VLAN Groups from System** column. VLAN groups that were configured on the port in Cisco UCS Manager are displayed in the **VLAN Groups Configured on Domain** column.
Note Only LAN type VLAN groups are created and available in Cisco UCS Central.

Step 10 On the **Policies** tab, select the flow control policy and link profile.

Step 11 Click **Save**.

Configuring an FC Storage Port

FC Storage ports allow you to directly attach an FC storage device to a port on the FI.

Before You Begin

The Fibre Channel switching mode must be set to Switching for these ports to be valid. The storage ports cannot function in end-host mode.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FC Storage**.

Step 7 On the **Basic** tab, enter the **Interface User Label** and select a fill pattern.

Step 8 On the **VSAN** tab, select the VSANs that you want to assign to the ports.
The VSANs that you select are displayed in the **VSAN** column. VSANs that were created in Cisco UCS Manager are displayed in the **VSAN on Domain** column.

Note Only VSANs of type Storage are supported and available for FC storage port configuration.

Step 9 Click **Save**.

Configuring an FC Uplink Port

FC uplink ports allow you to connect to external SAN switches.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.
The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FC Uplink**.

Step 7 On the **Basic** tab, enter the **Interface User Label** and select a fill pattern.

Step 8 On the **VSAN** tab, select the VSANs that you want to assign to the ports.
The VSANs that you select are displayed in the **VSAN from System** column. VSANs that were created in Cisco UCS Manager are displayed in the **VSAN Configured on Domain** column.

Note Only VSANs of type SAN are supported and available for FC uplink port configuration.

Step 9 Click **Save**.

Scalability and Breakout Ports

The Cisco UCS 6300 Series Fabric Interconnects contain scalability ports that can be broken out into groups of 4 10-Gigabit Ethernet ports. The configuration requires a Small Form-Factor Pluggable adapter (SPF) that has one 40GB QSFP+ on one end to connect to the Fabric Interconnect, and four 10 GB ports to connect to different end points supporting 10 GB connectivity.

- The Cisco UCS 6324 Fabric Interconnect contains one scalability port that can be used as a licensed server port for supported Cisco UCS rack servers, an appliance port, or a FCoE storage port.
- The Cisco UCS 6332 and Cisco UCS 6332-16 UP fabric interconnects contain multiple 40-Gigabet Ethernet ports that can be broken out into 10-Gigabit Ethernet ports.

Caution Configuring breakout ports requires rebooting the Fabric Interconnect. Any existing configuration on a port is erased. It is recommended to break out all required ports in a single transaction.

Once you configure a breakout port, you can configure each 10 GB sub-port as server, uplink, FCoE uplink, FCoE storage or appliance port as required.

The following table summarizes the constraints for breakout functionality for the Cisco UCS 6332 and 6332-16UP fabric interconnects:

Fabric Interconnect	Breakout Configurable Ports	Normal Ports with no Breakout Support
UCS-FI-6332	1-12,15-26	13-14,27-32 **Note** • Auto-negotiate behavior is not supported on ports 27–32. • A maximum of four ports are allowed as breakout ports if using QoS jumbo frames.
UCS-FI-6332-16UP	17-34	1-16,35-40 **Note** • Auto-negotiate behavior is not supported on ports 35-40. • A maximum of four ports are allowed as breakout ports if using QoS jumbo frames.

Managing Configured Ports

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 Click the Port **Tools** icon on the far right.

Step 6 Select one of the following:

- **Configuration Status—**Displays the status of the port.
- **Configure Port—**Enables you to change the configuration of the port.
- **Unconfigure Port—**Deletes the port configuration information. If you unconfigure a port, all traffic using the port will stop.
- **Enable Port—**Sets the administrative state of the port to Enabled. Only visible when the port is Disabled.
- **Disable Port—**Sets the administrative state of the port to Disabled. Only visible when the port is Enabled.
- **Unconfigure Breakout Port—**Combines the four 10GbE ports into a single 40GbE port.
- **Configure as Breakout Port—**Turns the port into a scalability port that can be broken out into four 10GbE ports.

Step 7 Complete the fields as required.

Creating a Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select the type of port channel that you want to create.
This can be one of the following:

Step 5 Complete the fields as required for your selection.

Step 6 Click **Save**.

Creating or Editing an Ethernet Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select **Ethernet** and complete the following:

a) Enter the **Port ID**, **Name**, and optional **Description**.

b) Select the admin speed and whether to enable auto negotiation.

Step 5 Click **Policies** and select the flow control and LACP policy that you want to assign to the ports.

Step 6 Click **VLANs** and select the VLANs that you want to assign to the ports.
The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

Step 7 Click **Ports** and click the **Add** icon to add ports to the port channel.

Step 8 Click **Save**.

Creating or Editing an FC Port Channel

Note For Cisco UCS Manager release 3.1(2) and above, FC port channels must be disabled before you can delete them.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select **FC** and complete the following:

a) Enter the **Port ID**, **Name**, and optional **Description**.

b) Select the **Admin Speed** for the port channel.

Step 5 Click **VLAN** and select the VLANs that you want to assign to the ports.
You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

The VLANs that you select are displayed in the **VLAN from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLAN Configured on Domain** column.

Step 6 Click **Ports** and click the **Add** icon to add ports to the port channel.

Step 7 Click **Save**.

Creating or Editing an FCoE Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select **FCoE**.

Step 5 Enter the **Port Channel ID**, **Name**, and optional **Description**.

Step 6 Click **Policies** and select the LACP policy that you want to assign to the ports.

Step 7 Click **Ports** and click the Plus icon to add ports to the port channel.

Step 8 Click **Save**.

Creating or Editing an Appliance Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 **Basic**, select **Appliance** and complete the following:

a) Enter the **Port Channel ID**, **Name**, and optional **Description**.

b) Select the admin speed and whether to use **Static** mode or dynamic **LACP**.

c) Select the quality of service **Priority** associated with this interface. This can be one of the following:

- **Platinum—**Use this priority for vNIC traffic only.
- **Gold—**Use this priority for vNIC traffic only.
- **Silver—**Use this priority for vNIC traffic only.
- **Bronze—**Use this priority for vNIC traffic only.
- **Best Effort—**Do not use this priority. It is reserved for the Basic Ethernet traffic lane.
- **Fibre Channel—**Use this priority for vHBA traffic only.

Step 5 Click **Policies** and select the flow control policy, network control policy, and the pin group that you want to assign to the ports.

Step 6 Click **VLANs** and select the VLANs that you want to assign to the ports.
The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

Step 7 Click **Ethernet Target Endpoint** and click **Enabled** to enter the **Name** and **MAC Address** for the endpoint.
The Ethernet target endpoint is disabled by default.

Step 8 Click **Ports** and click the **Add** icon to add ports to the port channel.

Step 9 Click **Save**.

Pin Groups

LAN Pin Groups

Cisco UCS uses LAN pin groups to pin Ethernet traffic from a vNIC on a server to an uplink Ethernet port or port channel on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

To configure pinning for a server, you must include the LAN pin group in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server. All traffic from the vNIC travels through the I/O module to the specified uplink Ethernet port.

Note If you do not assign a pin group to a server interface through a vNIC policy, Cisco UCS Central chooses an uplink Ethernet port or port channel for traffic from that server interface dynamically. This choice is not permanent. A different uplink Ethernet port or port channel may be used for traffic from that server interface after an interface flap or a server reboot.

If an uplink is part of a LAN pin group, the uplink is not necessarily reserved for only that LAN pin group. Other vNIC's policies that do not specify a LAN pin group can use the uplink as a dynamic uplink.

SAN Pin Groups

Cisco UCS uses SAN pin groups to pin Fibre Channel traffic from a vHBA on a server to an uplink Fibre Channel port on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups will be ignored.

To configure pinning for a server, you must include the SAN pin group in a vHBA policy. The vHBA policy is then included in the service profile assigned to that server. All traffic from the vHBA will travel through the I/O module to the specified uplink Fibre Channel port.

You can assign the same pin group to multiple vHBA policies. As a result, you do not need to manually pin the traffic for each vHBA.

Important Changing the target interface for an existing SAN pin group disrupts traffic for all vHBAs which use that pin group. The fabric interconnect performs a log in and log out for the Fibre Channel protocols to re-pin the traffic.

Creating a Pin Group

You can create a pin group for either LAN or SAN.

Step 1 Click the **Browse Tables** icon and choose **Domains**.

Step 2 Click the domain in which you want to create a pin group.

Step 3 On the domain page, click the **Tools** icon and select **Create Pin Group**.

Step 4 In the **Create Pin Group** dialog box, click **Basic** and choose whether you want to create a LAN or a SAN pin group.

Step 5 Enter the **Name** and optional **Description**.

Step 6 In **Fabric A Target**, choose whether you want to manually select a port, or select an existing port channel.

Step 7 If you selected **Manual**, select the port.
For LAN pin groups, only ethernet uplink ports are shown. For SAN pin groups, only FC and FCoE uplink ports are shown.

Step 8 If you selected **Port Channel**, select an existing port channel.
For LAN pin groups, only ethernet port channels are shown. For SAN pin groups, only FC and FCoE port channels are shown.

Step 9 In **Fabric B Target**, select a port or a port channel.

Step 10 Click **Save**.

Fibre Channel Switching Mode

The Fibre Channel switching mode determines how the fabric interconnect behaves as a switching device between the servers and storage devices. The fabric interconnect operates in either of the following Fibre Channel switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the connected fibre channel networks, representing all servers (hosts) connected to it through virtual host bus adapters (vHBAs). This behavior is achieved by pinning (either dynamically pinned or hard pinned) vHBAs to Fibre Channel uplink ports, which makes the Fibre Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the fabric interconnect avoids loops by denying uplink ports from receiving traffic from one another.

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching mode.

Note When you enable end-host mode, if a vHBA is hard pinned to an uplink Fibre Channel port and this uplink port goes down, the system cannot repin the vHBA, and the vHBA remains down.

Switch Mode

Switch mode is the traditional Fibre Channel switching mode. Switch mode allows the fabric interconnect to connect directly to a storage device. Enabling Fibre Channel switch mode is useful in Pod models where there is no SAN (for example, a single Cisco UCS domain that is connected directly to storage), or where a SAN exists (with an upstream MDS).

Switch mode is not the default Fibre Channel switching mode.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

Configuring Fibre Channel Switching Mode

You can configure your fabric interconnect to use either FC End-Host Mode or FC Switch Mode. By default, the FI is set to end-host mode.

Note When you change the Fibre Channel switching mode, Cisco UCS Central logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Central restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system ready.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 On the fabric interconnect page, click the **Tools** icon and select the **FC switching mode**.
If you are using end-host mode, **Set FC Switching Mode** displays. If you are using FC switching mode, **Set FC End-Host Mode** displays.

Step 4 Click **Yes** on the warning page to change the configuration and restart the FI.

Viewing Port Configuration Status

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

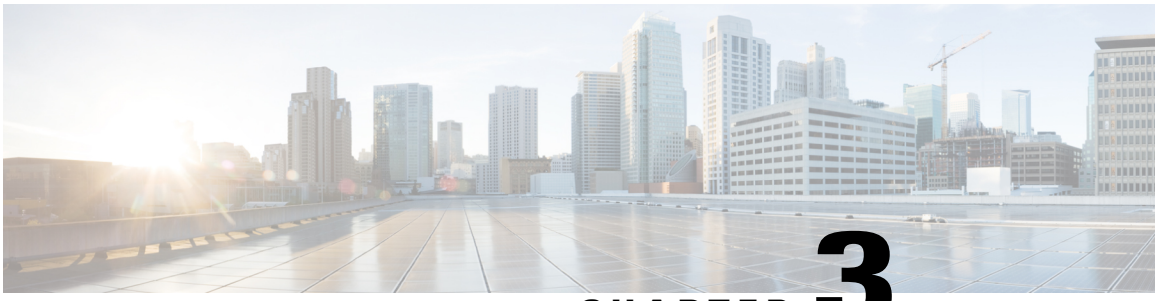
Step 3 Click the Tools icon on the far right and select **Configuration Status**.
The Configuration Status page for the selected port displays.

Step 4 Click **Close** to close the window.

Port Configuration Faults

The port faults page displays the following information for each fault:

- **Code—**The ID associated with the fault
- **Timestamp—**Date and time at which the fault occurred
- **Cause—**Cause of the fault
- **Affected Object—**The component that is affected by this fault
- **Fault Details—**The details of the fault.
- **Severity—**The severity of the fault
- **Action—**Any action required by the fault



CHAPTER 3

Global VSAN

Global VSANs

Cisco UCS Central enables you to define global VSAN in the SAN cloud or the Storage cloud. The global VSANs created in Cisco UCS Central are specific to the fabric interconnect where you create them. You can assign a VSAN to either Fabric A or Fabric B, or to both Fabric A and B. Global VSANs are not common VSANs in Cisco UCS Central.

Resolution of global VSANs takes place in Cisco UCS Central prior to deployment of global service profiles that reference them to Cisco UCS Manager. If a global service profile references a global VSAN, and that VSAN does not exist, deployment of the global service profile to Cisco UCS Manager will fail due to insufficient resources. All global VSANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VSANs are available and can be used in Cisco UCS Manager, even if no global service profile with reference to a global VSAN is deployed in that UCS domain. A global VSAN is not deleted when a global service profile that references it is deleted.

Global VSANs that are referenced by a global service profile available to a Cisco UCS Manager instance remain available unless they are specifically deleted for use from the domain group. Global VSANs can be localized in Cisco UCS Manager, in which case they act as local VSANs. Unless a global VSAN is localized, it cannot be deleted from Cisco UCS Manager.

Creating or Editing a VSAN

You can create a VSAN with IDs from 1 to 4093, except for those in the following reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.
- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

Important FCoE VLANs in the SAN cloud and vLANs in the LAN cloud must have different IDs. Using the same ID for an FCoE vLAN in a VSAN and for a vLAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE vLAN ID.

You can create a VSAN at the domain group root or in a specific domain. You can also assign the VSAN to either fabric A or fabric B, or to both fabric A and B. When you assign the VSAN to both fabrics, both of them must have different VSAN ID and FCoE VLAN ID.

Step 1 In the **Actions** bar, type **Create VSAN** and press Enter.

Step 2 In the VSAN dialog box, choose the type of VSAN that you want to create.
This can be one of the following:

- **SAN—**Connects your fabric interconnect to external switches.
- **Storage—**Directly connects your storage to the fabric interconnect.

Step 3 Click **Domain Group Location** and select the location in which you want to create this VSAN.

Step 4 Enter a **Name**.
The VSAN name is case sensitive.

Important Do not use the name **default** when you create a VSAN in Cisco UCS Central. If you want to create a global default VSAN, you may use **globalDefault** for the name.

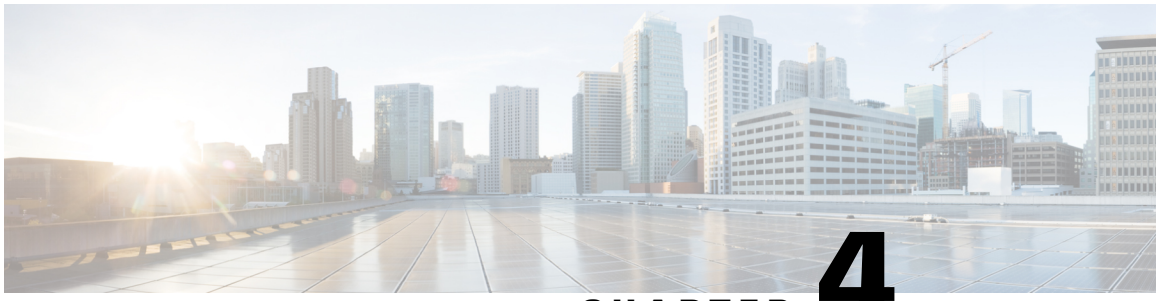
Step 5 Choose whether to enable Fibre Channel zoning.
FC zoning can be one of the following:

- Enabled—Cisco UCS Manager will configure and control Fibre Channel zoning when the VSAN is deployed.
- Disabled—The upstream switch configures and controls the Fibre Channel zoning, or Fibre Channel zoning is not implemented on this VSAN.

Note Fibre Channel zoning is disabled by default.

Step 6 Select the Fabric where you want to assign this VSAN.
If you assign the VSAN to both fabrics, enter the VSAN ID and FCoE VLAN ID for both fabrics. If not, assign the IDs for the selected VSAN.

Step 7 Click **Create**.



CHAPTER 4

vHBA Management

vHBA Templates

Use vHBA templates to define how a vHBA on a server connects to the SAN. You can view all existing vHBA templates on the **Templates** page.

vHBA Redundancy Template Pairs

Creating vHBA template pairs enables you to group vHBAs that belong to a specific server. For example, you can create a vHBA template and specify it as the primary template, then create a different vHBA template and specify it as the secondary template. You can link the two templates to create a pair that share attributes that you define in the primary template. The secondary template inherits the attributes from the primary template. If you select **Updating Template**, any changes made to the primary template are propagated to the secondary template in the template pair. You can also modify any non-shared configurations on each individual template in the pair.

When creating the pair, you can assign one template to each fabric. For example you could assign the primary template to fabric A, and the secondary template to fabric B. This eliminates the need to configure vHBA pairs independently using one or more templates. The number of vHBA pairs that can be created using a template pair is only limited by the adapter's maximum capabilities.

The following configurations are shared when using template pairs:

- VSANs
- Template Type
- Maximum Data Field Size
- QoS Policy
- Statistics Threshold Policy

The following configurations are not shared when using template pairs:

- Fabric ID
- WWPN Pool
- Description
- Pin Group Policy

Note If you plan to use a global vHBA redundancy template pair in a local service profile in Cisco UCS Manager, you cannot assign the vHBA template for the primary and the secondary of the redundancy template pair at the same time. You will need to assign the vHBA template for the primary vHBA and set the peer name for the second vHBA, then modify the secondary vHBA and manually assign the secondary vHBA template.

Creating or Editing a vHBA Template

Note Global vHBAs can be used in local service profiles created in Cisco UCS Manager.

Step 1 In the **Actions** bar, type **Create vHBA Template** and press Enter.

Step 2 In the **vHBA Template** dialog box, click **Basic** and complete the following:

a) Choose the **Organization** where you want to create the vHBA template.
b) Enter a **Name** and **Description**.
c) Choose the **Redundancy Type** to enable vHBA pairing.
This can be one of the following:

- **None—**Creates a standard vHBA template without vHBA pairing.
- **Primary—**Creates the primary vHBA template.
- **Secondary—**Creates the secondary vHBA template.

d) Select the options for **Type**, **Fabric ID**, **Fabric Failover** and enter the the **Max Data Field Size(Bytes)**.

Step 3 If you enabled vHBA pairing, click **Peer Redundancy Template** and choose the primary or secondary vHBA template.

Step 4 In **Basic**, select the **Organization** where you want to create the vHBA template.

a) Enter a **Name** and **Description**.
b) Select the options for **Type**, **Fabric ID**, and enter **Max Data Field Size(Bytes).**

Step 5 Click **WWN Address Pool** and select the WWN addresses.
If you do not assign a WWN address pool, the system assigns the default.

Step 6 Click **VSAN** and add the VSANs you want to use for this vHBA template.

Step 7 Click **Policies** and assign the policies that you want to use for this vHBA template.
If the policies are not assigned, click on each of the policies and pin group. On the right, click the drop-down to display related policies and pin group and select the one you want for this vHBA template.

Step 8 Click **Create**.

Host Interface Placement Policy

The host interface placement policy enables you to determine the user-specified virtual network interface connection (vCon) placement for vNICs and vHBAs.

To create a host interface placement policy, see Creating or Editing a Host Interface Placement Policy, on page 29. Details for existing policies are displayed on the **Host Interface Placement Policy** page.

Creating or Editing a Host Interface Placement Policy

Step 1 In the **Actions** bar, type **Create Host Interface Placement Policy** and press Enter.

Step 2 In the **Create Host Interface Placement Policy** dialog box, click **Organization** and chose the organization in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.
The policy name is case sensitive.

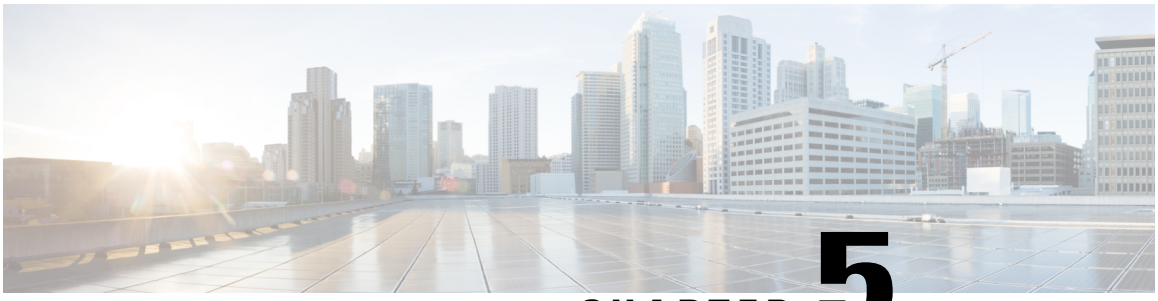
Step 4 Select the **Virtual Slot Mapping Scheme**.
This can be one of the following:

- **Linear Ordered—**The virtual slots are assigned in order.
- **Round Robin—**The virtual slots are assigned sequentially.

Step 5 Select the **Virtual Slot Selection Preference** for each virtual slot.
This can be one of the following:

- **all—**All configured vNICs and vHBAs can be assigned. This is the default.
- **assigned-only—**vNICs and vHBAs must be explicitly assigned.
- **exclude-dynamic—**Dynamic vNICs and vHBAs cannot be assigned.
- **exclude-unassigned—**Unassigned vNICs and vHBAs cannot be assigned.
- **exclude-usnic—**usNIC vNICs cannot be assigned.

Step 6 Click **Create**.



CHAPTER 5

Storage Pools

This chapter includes the following sections:

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS domain. WWN pools created in Cisco UCS Central can be shared between Cisco UCS domains. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA
- Both WW node names and WW port names

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks.

WWNN Pools

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

WWxN Pools

A WWxN pool is a WWN pool that contains both WW node names and WW port names. You can specify how many ports per node are created with WWxN pools. The pool size for WWxN pools must be a multiple of ports-per-node + 1. For example, if there are 7 ports per node, the pool size must be a multiple of 8. If there are 63 ports per node, the pool size must be a multiple of 64.

Creating and Editing a WWN Pool

After creating a WWN pool you can edit by selecting the **Edit** icon on the overall summary page of the selected WWN pool. To select a WWN pool, go to **All Pools** page and select the WWN pool that you want to edit. The page redirects you to the overall summary page of the selected WWN pool.

Step 1 In the Actions bar, type **Create WWN Pool** and press **Enter**.
This launches the **Create WWN Pool** dialog box.

Step 2 In **Basic**, complete the following:

a) Click **Organization** and select the location in which you want to create the pool.
b) Enter name and description of the WWN pool.
c) In the **World Wide Name (WWN) Used For** area, select one of the following:

- **Port (WWPN)—**The pool is used for both WWNNs and WWPNs.
- **Node (WWNN)—**The pool is used for WWNNs.
- **Both (WWxN)—**The pool is used for WWNNs.

Step 3 In **WWN Blocks**, complete the following:

a) Click the **Create** icon.
b) In the **WWN Block Start** column, enter the first WWN initiator in the block.
c) In the **Size** column, enter the total number of WWN initiators in the pool.
d) Click the **Apply** icon.
Additional fields related to WWN pools are displayed.
e) Click the **WWNs** tab, you can view a graphical representation of the number if WWN addresses in the pool, the number of assigned WWN addresses, and the duplicate MAC addresses and WWN summary.
f) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.

Note You must wait a minimum of 5 seconds before you create another pool.

What to Do Next

- Include the WWPN pool in a vHBA template.
- Include the WWNN pool in a service profile or service profile template.
- Include the WWxN pool in a service profile or service profile template.

Deleting a Pool

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

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

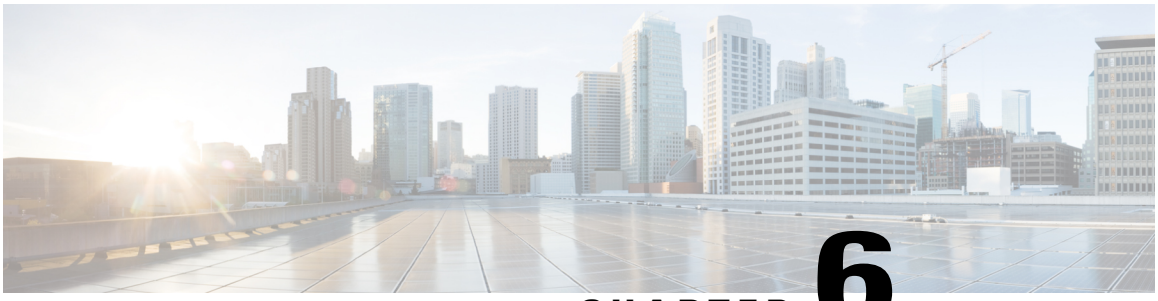
Step 1 Click the **Browse Tables** icon and choose **Pools**.

Step 2 In the **Pool Name** column, locate the pool that you want to delete.
You can search for the pool in one of the following ways:

- Browse through the list of pools.
- Click the **Search** icon and enter the pool name.
- Select a pool type from the **Filters** column.

Step 3 Click the pool.
This launches the overall summary page of the selected pool.

Step 4 Click the **Delete** icon.
If Cisco UCS Central displays a confirmation dialog box, click **Delete**.



CHAPTER 6

Storage Policies

This chapter includes the following sections:

Fibre Channel Adapter Policy

Fibre channel adapter policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by Cisco UCS Central may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in possible mismatch between SANsurfer and Cisco UCS Central:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Central supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Central, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Central displays as 5 s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Central allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Central displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Fibre channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Note We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

Creating or Editing a Fibre Channel Adapter Policy

Step 1 In the **Actions** bar, type **Create Fibre Channel Adapter Policy** and press Enter.

Step 2 In the **Fibre Channel Adapter Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create this policy.

Step 3 Enter a **Name** and optional **Description**
The policy name is case sensitive.

Step 4 In **Resources**, complete the fields as necessary.

Step 5 In **Settings**, complete the fields as necessary.

Step 6 Click **Create**.

SAN Connectivity Policy

SAN connectivity policies determine the connections and the network communication resources between the server and the SAN on the network. These policies use pools to assign WWNs, and WWPNs to servers and to identify the vHBAs that the servers use to communicate with the network.

Note These policies are included in service profiles and service profile templates, and can be used to configure multiple servers. So, using static IDs in connectivity policies is not recommended.

Creating or Editing a SAN Connectivity Policy

Step 1 In the **Actions** bar, type **Create SAN Connectivity Policy** and press Enter.

Step 2 In the **SAN Connectivity Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.
The name is case sensitive.

Step 4 In **Identifiers**, choose the WWNN pool.
For more information, see Creating and Editing a WWN Pool, on page 32.

Step 5 In **vHBAs**, create one or more vHBAs and select the properties.
You can manually create the vHBA, use a vHBA template, or create a redundancy template pair. For more information, see Creating or Editing a vHBA Template, on page 28.

Step 6 Click **Create**.

Storage Connection Policy

The storage connection policy contains a collection of target storage ports on storage array that you use to configure fibre channel zoning.

From Cisco UCS Central you can create a storage connection policy in an organization.

Creating or Editing a Storage Connection Policy

Step 1 In the **Actions** bar, type **Create Storage Connection Policy** and press Enter.

Step 2 In the **Storage Connection Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

a) Enter a **Name** and an optional **Description** for this policy.
b) Select a **Zoning Type**. This can be one of the following:

- **None—**FC zoning is not configured.
- **Single Initiator Single Target—**The system automatically creates one zone for each vHBA and storage port pair. Each zone has two members. We recommend that you configure this type of zoning unless you expect the number of zones to exceed the maximum supported.

  This is the default.
- **Single Initiator Multiple Targets—**The system automatically creates one zone for each vHBA. We recommend that you configure this type of zoning if you expect the number of zones to reach or exceed the maximum supported.

Step 3 Click **Endpoints** and click the plus sign to add a **WWPN**.
The WWPN is assigned to the physical target port on the Fibre Channel or FCoE storage array that the server uses to access the LUNs configured on the storage array.

a) In the **FC Target Endpoints** > **Basic** tab, enter an optional description and select the fabric interconnect in the **Path** field.
   By default, fabric interconnect A is used for communications with the target endpoint.
b) In the **FC Target Endpoints** > **VSAN** tab, select the VSAN associated with the FI port and target endpoint.

Step 4 Click **Create**.

Fibre Channel Zoning

Fibre Channel (FC) zoning allows you to partition the Fibre Channel fabric into one or more zones. Each zone defines the set of FC initiators and FC targets that can communicate with each other in a VSAN.

The access and data traffic control provided by zoning does the following:

- Enhances SAN network security
- Helps prevent data loss or corruption
- Reduces performance issues

Cisco UCS Central FC zoning combines direct attach storage with local zoning. Fibre Channel or FCoE storage is directly connected to the fabric interconnects, and zoning is performed in Cisco UCS Central, using Cisco UCS local zoning.

Configuring Zoning

Note This dialog box is read-only if the global service profile or service profile template you select already has a SAN connectivity policy associated with it.

Step 1 From the **Service Profile** or **Service Profile Template** page, click the **Tools** icon and choose **Configuring Zoning**.

Step 2 In the **Configure Zoning** dialog box, click the plus icon to add a new vHBA Initiator Group, and type the name that you want to use for the group.

Step 3 In **Basic**, enter the optional description.

Step 4 In **vHBA Initiators**, select the vHBA initiators that you want to add.

Step 5 In **Storage Connection Policy**, select the policy that you want to use.

Step 6 Click **Save**.

Direct-Attached Storage

Direct-attached storage (DAS) uses FC storage ports to connect an FC storage device to a port on the fabric interconnect.

Configuring Direct-Attached Storage

Step 1 Ensure that the FI is configured in FC Switch Mode.

Step 2 Create a VSAN in the Storage cloud.

Step 3 Set the port role to FC Switch Mode.

Step 4 Perform the following steps to confirm that the storage port WWPN is logged into the fabric interconnect.

a) Log in through the secure shell (SSH), or establish a Telnet connection to the UCS Virtual IP (VIP) on the primary FI.

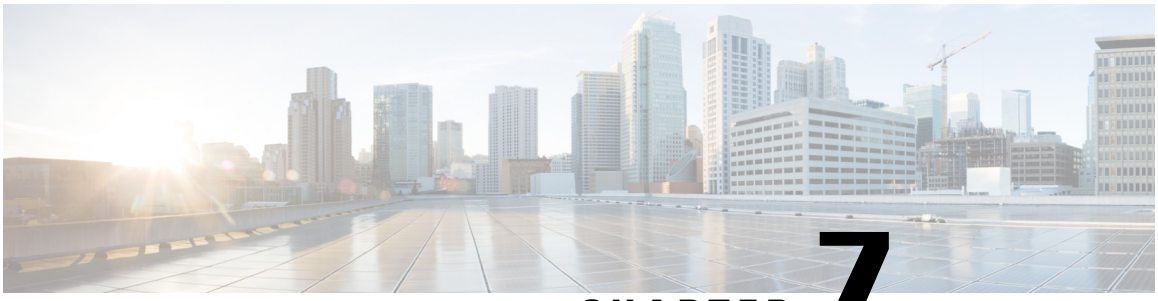
b) Enter the connect nxos { a | b } command, where a | b represents FI A or FI B.

c) Enter the **show flogi database vsan** *vsan ID* command, where *vsan ID* is the identifier for the VSAN.

Step 5 Create a storage connection policy.

Step 6 Create a service profile that uses the storage connection policy you just created.

Step 7 Associate the service profile with the server.



CHAPTER 7

SED Management

Security Policies for Self Encrypting Drives

Self-Encrypting Drives (SEDs) have special hardware that encrypts incoming data and decrypts outgoing data in real-time. The data on the disk is always encrypted in the disk and stored in the encrypted form. The encrypted data is always decrypted on the way out of the disk. A media encryption key controls this encryption and decryption. This key is never stored in the processor or memory. Cisco UCS Manager supports SEDs on Cisco UCS C-Series and S-Series servers.

SEDs are locked using a security key. The security key, which is also known as Key-Encryption Key or an authentication passphrase, is used to encrypt the media encryption key. If the disk is not locked, no key is required to fetch the data.

Cisco UCS Central enables you to configure security keys locally or remotely. When you configure the key locally, you must remember the key. In case you forget the key, it cannot be retrieved and the data is lost. You can configure the key remotely by using a key management server (also known as KMIP server). This method addresses the issues related to safe-keeping and retrieval of the keys in the local management.

The encryption and decryption for SEDs is done through the hardware. Thus, it does not affect the overall system performance. SEDs reduce the disk retirement and redeployment costs through instantaneous cryptographic erasure. Cryptographic erasure will render all data on the SED unreadable when the encryption key is destroyed.

Security Guidelines and Limitations for SED Management

The following security guidelines and limitations apply to SED management from Cisco UCS Central:

- Storage operations get applied only when the server is powered on, and they do not trigger a server reboot.
- A global service profile (GSP) with a security policy gets pushed to Cisco UCS Manager releases prior to 3.1(3), and the security policies related operations are cleaned up and an unsecured LUN is created.
- A Cisco UCS Manager downgrade fails if a storage controller with **Drive Security Enable** is present in the domain.

- A GSP association fails with a `config-failure` status/message if it is associated with an unsupported server, or a supported server with unsupported firmware.
- A GSP association fails with a `config-failure` status/message if LUN security is set to **Enabled** in the Disk Configuration Policy but if the Security policy is not created in the storage profile.
- A GSP association fails if the Security policy is deleted from the storage profile after the Storage Controller is set to **Drive Security Enable**.

Security Flags for Controller and Disk

Security flags indicate the current security status of the storage controller and disks.

The storage controller and disks have the following security flags:

- **Security Capable—**Indicates that the controller, LUN, or disk is capable of supporting SED management.
- **Security Enable—**Indicates that the security key is programmed on the controller, disk, or LUN, and security is enabled on the device. This flag is set when you configure a security policy and associate it to a server, making the controller and disk secure. This flag is not set on a Cisco HyperFlex device.
- **Secured—**Indicates that the security key is programmed on the disk, and security is enabled on the Cisco HyperFlex device.

The following security flags are exclusive to storage disks:

- **Locked—**Indicates that the disk key does not match the key on the controller. This happens when you move disks across servers that are programmed with different keys. The data on a locked disk is inaccessible and the operating system cannot use the disk. To use this disk, you must either unlock the disk or secure erase the foreign configuration.
- **Foreign Secured—**Indicates that a secure disk is in foreign configuration. This happens when you unlock a locked disk with the right key, but the disk is in a foreign configuration state and the data on it is encrypted. To use this disk, you can either import or clear the foreign configuration.

Security Related Operations

You can create security policies for Self-Encrypting Drives (SEDs) through a Storage Profile in Cisco UCS Central. In addition to creating security policies, you can perform additional operations on the supported servers. The following table lists the remote operations and their descriptions:

Component	Remote Action	Action
Controller	Unlock Disk	Unlocks ForeignSecured and Locked Disks encrypted using a Local Policy.
	Modify Remote Key	Modifies the Key in the KMIP Server and fetches the new Key for Encryption.
	Disable Security	Disables Security on the Controller when no Secured Disks are present on Controller.
	Unlock for Remote	Unlocks ForeignSecured and Locked Disks encrypted using a Remote Policy.
Virtual Disk	Secure Virtual Drive	Secures LUNs comprised only of SEDs when the Controller is Security Enabled.
Physical Disk	Enable Encryption	Used to Secure JBOD Self-Encrypting Drive(SED) when Controller is Security Enabled.
	Secure Erase	Erases disk cryptographically to make it Unsecured and Reusable.
	Secure Erase Foreign Configuration	Erases ForeignSecured and Locked disks cryptographically to make them Unsecured and Unconfigured Good

For more information about SED Management and security policies, see *Cisco UCS Manager Storage Management Guide*.

KMIP Certification Policy

Cisco UCS Central lets you create a **KMIP Certification** policy to enable communication with the KMIP server for remote management of Self-Encrypting Disks (SED). This policy creates a certificate signing request for the server CIMC. The KMIP Certification policy is supported on Cisco UCS Manager release 3.1(3) and later, Cisco S3260M4 with MegaRAID controllers, and Cisco UCS M4 Blade Servers (C220 and C240M4).

You can create a KMIP Certification policy in the domain scope. Any modification of the certificate in this scope does not result in the regeneration of the certificate. If you want to regenerate a certificate, you must create a KMIP Certification Policy in the **Server** tab in Cisco UCS Manager.

After you create a KMIP Client Certification policy, do one of the following:

- Copy the generated certificate to the KMIP Server.
- Use the generated Certificate Signing Request to get a CA-signed certificate from the KMIP Server and navigate to the **Configure KMIP Certificate** in the Server details page to configure the CA-signed certificate.

Creating or Editing a KMIP Certification Policy

KMIP Certification Policy enables using SEDs through key management servers. This policy aims to generate a certificate that is used by CIMC to communicate with KMIP server to get the key. You can create a KMIP Certification policy from the domain scope.

Step 1 In the **Actions** bar, type **KMIP Certification Policy** and press Enter.

Step 2 In the Create **KMIP Certification Policy** dialog box, select the **Domain Group Location** in which you want to create the policy.

Step 3 Enter a **Name** for the **KMIP Certification Policy**, and add an optional **Description**.
The name is case-sensitive.

Step 4 Fill in appropriate details in the following fields:

- **E-Mail Address—**(Optional) The email address associated with the request. This information is optional.
- **Org Name—**The organization requesting the certificate.
- **Organizational Unit—**(Optional) The organization division that holds the certificate. This field is mandatory if you are using SafeNet KMIP server.
- **Locality—**Locality or city where your organization is located.
- **State—**State or province name.
- **Country Code—**Country name in two upper case letters. For example, US.
- **Validity—**Validity period for the certificate, in number of days.

Step 5 Click **Create**.

Step 6 To edit a KMIP Certification policy, click **Edit** on the policy and change the **Description** and the other details.

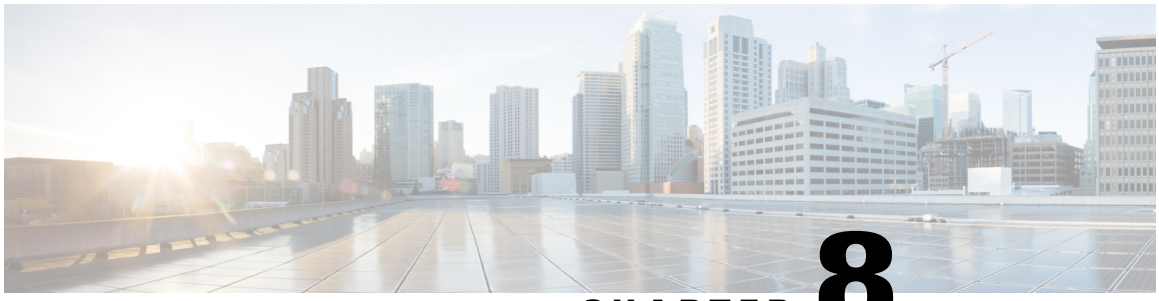
Configuring a KMIP Certification Policy

Before You Begin

- Configure the domain in a domain group to refer to the KMIP policy.

Step 1 To configure the policy for the domain scope, select **Domain Configuration Settings** > **Policies** > **KMIP Certification Policy**.

Step 2 In **Policies**, select the KMIP Certification Policy from the drop-down, and click **Save**.
The KMIP Certification policy is configured on the server and you can view the details of the key on the **Server Details** page.



CHAPTER 8

Chassis Profiles and Templates

About the Cisco UCS S3260 Storage Server

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

The Cisco UCS S3260 Storage Server is designed to operate in a standalone environment and as part of the Cisco Unified Computing System with Cisco UCS Manager integration. It assumes almost the same characteristics of its predecessors, the Cisco UCS C3160 Rack Server, but with the following additional features:

- System IO Controllers (SIOC).
- Support of up to two server modules.
- Capability to operate in a standalone mode.
- Chassis level functionality in the standalone mode—Shared components such as storage adapters, fans and power supply units are configured at the chassis level.

- Data Center Ethernet connectivity to a server host through a shared dual virtual interface card (VIC).
- 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 Storage Server 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.

For more information, see the *Cisco UCS 3260 Quick Reference Guide*.

Chassis Profiles

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

A chassis profile includes four types of 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. Cisco UCS Central 2.0(1a) introduces delivery of critical fixes and security updates through service packs. In addition to the Blade and Rack server bundles for firmware updates, you must also download the service pack bundles to complete the firmware upgrade. Service packs are specific and cumulative to a maintenance release and are supported for Cisco UCS Manager version 3.1(3) and above. You can choose the firmware to be updated by using a service pack.
- **Disk zoning policy—**Includes the zoning policy to be applied to the storage disks.

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 chassis can be associated with only one chassis profile. Similarly, each chassis profile can be associated with only one chassis at a time.
- Chassis profiles are supported only on the Cisco UCS S3260 Storage Server.
- C bundles earlier than Cisco UCS Manager Release 3.1(2) are not supported on the Cisco UCS S3260 Storage Server.

Creating or Editing a Chassis Profile Template

Step 1 In the **Actions** bar, type **Create Chassis Profile Template** and press enter.

Step 2 In **Basic**, select the **Organization** where you want to create the chassis profile template.

a) Enter a **Name** and optional **Description** and **User Label** to help identify the chassis profile template.

b) Choose a **Template Instantiation Mode**:

- **Initial—**Chassis profiles created from this template inherit all the properties of the template, but will not be updated when this template is updated.
- **Updating—**Chassis profiles created from this template remain connected and are automatically updated when this template is updated.

Step 3 Click the **Policies** tab to assign existing policies to the chassis profile template.
You can click on a policy and use the drop-down option on the right to assign the policy to the template.

Step 4 Click **Create**.

Creating a Chassis Profile from a Template

Step 1 In the **Actions** bar, type **Create Chassis Profile from Template** and press Enter.

Step 2 Choose the chassis profile template that you want to use from the **Chassis Profile Template to Instantiate**, and select the **Organization** where you want to create the chassis profile.

Step 3 Determine the type of **Chassis Profile Naming Convention** that you want to use. This can be one of the following:

- **Manual Entry—**Enter the chassis profile names as comma separated values. A chassis profile will be created for each value entered.
- **Advanced—**Enter the prefix, suffix, number of chassis profiles, the first number, and the number of digits.

  The chassis profiles are created using the format prefixXXsuffix. For example, three chassis profiles starting at 400 and using 4 digits would be called prefix0400suffix, prefix0401suffix, and prefix0402suffix.

Note You can create up to 99 chassis profiles at one time from a single template.

Step 4 Click **Create**.

Manually Assigning a Chassis to a Chassis Profile

Step 1 Click **Browse Tables** and choose **Profiles**.

Step 2 On the **Profiles** page, choose the chassis profile that you want to modify.

Step 3 On the **Chassis Profile** page, click the **Tools** icon and choose **Assign Chassis Manually**.

Step 4 Choose the chassis that you want to assign to the chassis profile.

Step 5 Click **Assign**.

Chassis Profile Template Details

The Chassis Profile Template details page displays detailed information on the chassis profile template. From here you can:

- View audit logs.
- Create a chassis profile from this chassis profile template.
- Delete, clone, or rename the chassis profile template.

Chassis Profile Details

The Chassis Profile details page displays detailed information on the chassis profile. From here you can:

- View logs and configuration status.
- Create a chassis profile template from this chassis profile.
- Bind or unbind from the chassis profile template.
- Assign or unassign a chassis.
- Reapply the configuration to the associated chassis.
- Delete, clone, or rename the chassis profile.
- Acknowledge and decommission a chassis.
- Turn on or turn off the Locator LED for a chassis.
- Launch Cisco UCS Manager for the specific Cisco UCS domain.

Note

- Your browser must have pop-ups enabled.
- For Cisco UCS Manager release 3.1(2) or later, this launches the HTML5 GUI. If the Cisco UCS Manager credentials match the credentials for your Cisco UCS Central login, then the system will automatically log in to the Cisco UCS Manager GUI without prompting for the login information.
- For Cisco UCS Manager release 3.1(1) or previous, this launches the Java-based GUI.

Editing a Chassis Profile

Step 1 From the **Chassis Profile Details** view, select **Edit** and press Enter.

Step 2 In **Basic**, enter a **Description** and **User Label** to help identify the chassis profile.

Step 3 Click the **Policies** tab to assign the existing policies to the chassis profile.
You can click on a policy and use the drop-down list on the right to assign the Chassis Firmware Package policy to the profile.

Step 4 Click **Create**.

Local Chassis Profiles

The Local Chassis Profile details page displays detailed information on a local chassis profile. Local chassis profiles are managed by Cisco UCS Manager.

From here you can:

- View logs.
- Acknowledge and decommission a chassis.
- Turn on or turn off the Locator LED for a chassis.
- Launch Cisco UCS Manager for the specific Cisco UCS domain.

Note

- Your browser must have pop-ups enabled.
- For Cisco UCS Manager release 3.1(2) or later, this launches the HTML5 GUI. If the Cisco UCS Manager credentials match the credentials for your Cisco UCS Central login, then the system will automatically log in to the Cisco UCS Manager GUI without prompting for the login information.
- For Cisco UCS Manager release 3.1(1) or previous, this launches the Java-based GUI.

Viewing Chassis Profile Configuration Status

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Click **Chassis Profiles**.

Step 3 Select the chassis profile for which you want to view configuration status.

Step 4 On the detailed view for your selection, click the **Alerts** icon and choose **Configuration Status**. The **Configuration Status** page displays.

Step 5 Click **Close** to close the window.

Chassis Profile Faults

To view consolidated faults of both the chassis profile and associated chassis, click the **Alerts** icon on the chassis profile page and choose **Faults**. The following information is displayed:

- **Filters—**Filter the data in the table by severity, fault type, and timestamp.
- **Code—**Unique identifier associated with the fault.
- **Timestamp—**Day and time at which the fault occurred.
- **Cause—**Brief description of what caused the fault.
- **Affected Object—**The name and location of the component that this issue affects, and the domain name where it is found.
- **Fault Details—**More information about the log message.
- **Severity—**Displays an icon denoting the fault severity. The icon key displays below the table.
- **Action—**Any action required by the fault.

Chassis Profile Inventory Faults

You can view faults from each chassis associated with a chassis profile. To view chassis faults, click the **Faults** icon in the **Chassis Fault Summary** section of a **Chassis Profile** details page. The **Faults Logs** page displays information on the type and severity level of the fault and allows you to monitor and acknowledge the faults.

- **Filters—**Filter the data in the table by severity, fault type, and timestamp.
- **Code—**Unique identifier associated with the fault.
- **Timestamp—**Day and time at which the fault occurred.
- **Cause—**Brief description of what caused the fault.
- **Affected Object—**The name and location of the component that this issue affects, and the domain name where it is found.
- **Fault Details—**More information about the log message.
- **Severity—**Displays an icon denoting the fault severity. The icon key displays below the table.
- **Action—**Whether user acknowledgment is required.

Chassis Discovery Policy

The chassis discovery policy determines whether a specific chassis is included in a fabric port channel after chassis discovery. This allows for different chassis connectivity modes per fabric interconnect. By default, the chassis discovery policy is set to global. This means that connectivity control is configured when the chassis is newly discovered, using the settings configured for Chassis/FEX Link Grouping Policy on the domain group system policy. Depending on the domain group equipment policy setting, the chassis links are either all set to port channel or single links.

When you set the chassis discovery policy manually for a chassis, you have the following options:

- **None—**All links functions as single links.
- **Port Channel—**All links functions as a port channel.
- **Global—**All links use the settings in the Equipment policy for the entire domain group.

  For more information, see .

Note The chassis discovery policy is applicable only when the hardware configuration supports fabric port channels, and the chassis is directly connected to a fabric interconnect.

Configuring a Chassis Discovery Policy

Step 1 Click the **Browse Tables** icon and choose **Chassis**.

Step 2 Click a chassis.

Step 3 On the chassis page, click the **Tasks** icon and choose **Discovery Policy**.

Step 4 Choose whether to use the global domain group policy, force all links to function as a port channel, or force all links to function as single links.

Step 5 Click **Save**.

Chassis Maintenance Policy

A chassis maintenance policy determines when a chassis is rebooted when changes are made to the chassis profile. By default, the chassis maintenance policy always requires that a user acknowledges the changes before the reboot occurs.

Creating or Editing a Chassis Maintenance Policy

All chassis maintenance policies require user acknowledgment before any maintenance-related configuration can be applied to the chassis.

Step 1 In the **Actions** bar, type **Create Maintenance Policy** and press Enter.

Step 2 In the **Maintenance Policy Create** dialog box, choose **Chassis**.

Step 3 Choose the **Organization** where you want to create the policy, and enter the **Name** and optional **Description**. The name is case sensitive.

Step 4 Click **Evaluate** to view the impact of the policy.

Step 5 Click **Create**.

Chassis Firmware Package Policy

The Chassis Firmware Package Policy page displays details about an individual chassis firmware package policy. From this page, you can edit the policy or view the chassis to which the policy is associated.

Creating or Editing a Chassis Firmware Package Policy

Step 1 In the **Actions** bar, type **Create Chassis Firmware Package Policy** and press Enter.

Step 2 In the **Chassis Firmware Package Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.
The policy name is case-sensitive.

Step 4 Select the **Chassis Version** of the firmware, as required for your environment.
Note Only Cisco UCS Manager version 3.1(2) and above C bundles are supported.

Step 5 Select the applicable **Service Pack Version** for the firmware.
If the service pack version you select is for Cisco UCS Manager release earlier than 3.1(3), the following Warning message displays:
Package Version of all bundles in the pack must match
Ensure that the service pack you download is compatible with the supported Cisco UCS Manager version. For more information about applicable service packs, see *About Service Packs* in the *Cisco UCS Central Administration Guide*.

For more information on downloading images, see *Downloading Firmware from Cisco.com* in the *Cisco UCS Central Administration Guide*.

Step 6 In the **Components** tab, click **Add** to select any components that want to exclude from the firmware update.
The included and excluded components display. The following components can be excluded:

- Chassis adapter
- Chassis board controller
- Chassis management controller
- Local disk
- SAS expander
- Storage controller

a) To exclude all components, click **Excluded Components**.
b) To remove an excluded component, select it and click **Delete**.

Step 7 Click **Create**.
Note To understand the impact of the policy, click **Evaluate**.

Step 8 The **Configuration Settings** window displays the images of the service pack bundles that get updated.

Disk Zoning Policies

Disk zoning policies allow you to manage the disks on your chassis servers when associated in a chassis profile.

Depending on the storage controller, the disk-sharing modes that are supported for your disk zoning policy may vary. For more information about disk-sharing modes supported on the storage controllers, see the Storage Server Features and Components Overview section in the *Cisco UCS Manager Storage Management Guide*.

Creating or Editing a Disk Zoning Policy

Step 1 In the **Actions** bar, type **Create Disk Zoning Policy** and press Enter.

Step 2 In the **Basic** tab, enter the **Name** and optional **Description**.

Step 3 Choose whether to enable **Preserve Configuration**.
If enabled, any disk zoning that is configured on the chassis remains as is when the chassis is associated to a chassis profile. If disabled, enter your disk zoning preferences in the **Disk Slots** tab.

Step 4 In **Disk Slots**, assign the disks as follows:

- **Unassigned—**The disks are not visible to any server, and can be allocated as dedicated, shared, or chassis hot spare. Specify a **Slot Range** for the unassigned disks.
- **Dedicated—**Disks are assigned to the specified controller, and are not visible to any other controllers in the chassis. Specify the **Slot Range** for disks to assign to a server and a controller and choose the **Server ID** and **Controller ID** from the drop-down. For HBA controllers, you can assign the disks to a combination of either server and controller.

  Note Beginning Cisco UCS Central 2.0 and Cisco UCS Manager release 3.1(3), disk zoning supports a second RAID controller (1 or 2) on Cisco S3260 Storage servers.

  For the RAID controllers, you can select only one server per combination of the controllers 1 or 2. An Unsupported Hardware Configuration message displays if you select an unsupported server.
- **Shared—**Disks are visible to multiple servers and controllers, and can be used for disk failover. When you specify a slot range, these disks are seen by all controllers in the Cisco C3260 chassis.

  Note Cisco UCS Central 2.0 and Cisco UCS Manager 3.1(3) do not support selection of server and controller for shared mode.
- **Chassis Global Hot Spares—**Disks will be made available to a controller if no hot spares on that controller are available. You can the select disk slot you want to reserve as hot spare. An error displays when you select an unsupported configuration.

Step 5 Click **Create**.

Compute Connect Policy

Starting with Cisco UCS Central release 2.0, you can create a Compute Connect Policy that lets you utilize a Cisco UCS C3260 chassis' second Cisco Storage I/O Control (SIOC). Cisco SIOCs allow prioritization of storage resources during periods of contention. The Compute Connect Policy is applied to a Cisco UCS C3260 chassis through a chassis profile and depends on infrastructure, CMC, and server firmware. When the policy is successfully applied to a chassis, the CMC performs a reboot and the server receives two adapter instances.

Note The Compute Connect Policy is supported on Cisco UCS Manager 3.1(3) and later.

Cisco produces the Cisco UCS C3260 chassis in two configurations:

- Single Server
- Dual Server

Before Cisco UCS Central release 2.0, the data path was only through a single SIOC. The CIMC firmware now supports using both SIOCs to process data. There are two single-server configurations for the Cisco UCS C3260 chassis:

- Single Server—Uses an HDD expansion tray in the second slot to provide four more disk slots.
- Single Server with IO Expander Tray—Provides an extra mezzanine storage controller and two PCI slots.

The Compute Connect Policy introduces two new values available during the policy creation process:

- Single-Server Single SIOC (legacy mode)
- Single-Server Dual SIOC

Note An attempt to push the policy to any chassis models other than a Cisco UCS C3260 chassis results in an error message. For Cisco UCS Manager releases prior to 3.1(3), Cisco recommends that you maintain this policy as unassigned in the **Global Chassis Profile** before associating it to the chassis.

Creating a Compute Connect Policy

Before You Begin

- Cisco C3260 Chassis should be in Single Server Configuration
- The chassis, server, and Cisco UCS Manager firmware should be release 3.1(3) or later

Step 1 In the **Actions** bar, type **Create Compute Connect Policy** and press Enter.

Step 2 In the **Compute Connect Policy** dialog box, choose the organization where you want to create the Compute Connect Policy.

Step 3 In the **Compute Connect Policy** dialog box, complete the following fields:

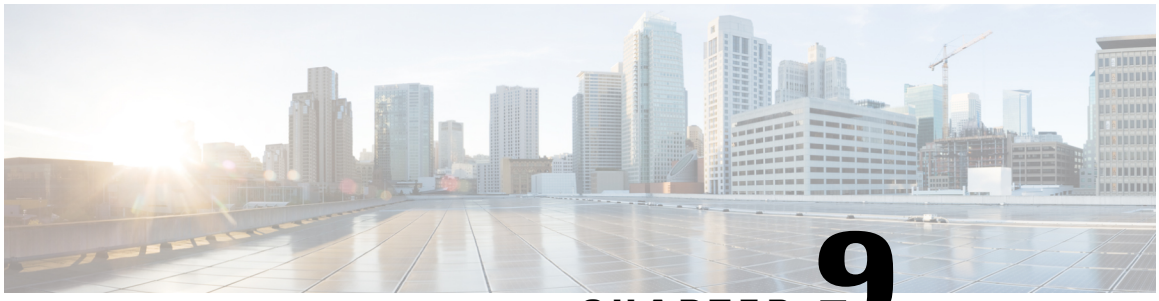
- **Name—**The name of the policy. This name can be between 1 and 16 alphanumeric characters other than □(hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
- **Description—**A description of the policy. Cisco recommends that you include information about where and when the policy can be used. Enter up to 256 characters.

- **Server SIOC Connectivity—**Choose a connectivity mode:
- **Single Server Single SIOC**
- **Single Server Dual SIOC**

Step 4 Click **Create** to create the new policy.

Viewing System IO Configuration Status

Step 1 Click the **Browse Tables** icon and choose **Chassis**.
Step 2 Click a storage chassis.
Step 3 On the storage chassis page, click **System IO Controller**.
Step 4 Click a system IO controller to expand it.
Step 5 Click the **Tools** icon and choose **Configuration Status**.
Step 6 On the storage chassis page, click **System IO Controller**.
On the **System IO Controller** dialog box, you can view the SIOC, the CMC, and the chassis discovery configuration status.
Step 7 Click **Close**.



CHAPTER 9

Storage Profiles

This chapter includes the following sections:

Storage Profiles

To allow flexibility in defining the number of storage disks, roles and usage of these disks, and other storage parameters, you can create and use storage profiles. A storage profile encapsulates the storage requirements for one or more service profiles. LUNs configured in a storage profile can be used as boot LUNs or data LUNs, and can be dedicated to a specific server. You can also specify a local LUN as a boot device.

Note Storage profiles on Cisco UCS rack and blade servers are supported on Cisco UCS Manager release 2.2.7 and above, and Cisco UCS Manager release 3.1.1 and above.

Because Cisco UCS M-series Modular Servers have been deprecated, storage profiles with boot orders created in Cisco UCS Central release 1.4 are not supported in Cisco UCS Central release 1.5 and later.

Storage profiles allow you to do the following:

- Configure multiple virtual drives and select the physical drives that are used by a virtual drive.
- Configure the storage capacity of a virtual drive.
- Configure the number, type and role of disks in a disk group.
- Associate a storage profile with a service profile.

Note LUN resizing is not supported.

Virtual Drives

A disk group can be partitioned into virtual drives. Each virtual drive appears as an individual physical device to the Operating System.

All virtual drives in a disk group must be managed by using a single disk group policy.

Configuration States

Indicates the configuration states of a virtual drive. Virtual drives can have the following configuration states:

- Applying—Creation of the virtual drive is in progress.
- Applied—Creation of the virtual drive is complete, or virtual disk policy changes are configured and applied successfully.
- Failed to apply—Creation, deletion, or renaming of a virtual drive has failed due to errors in the underlying storage subsystem.
- Orphaned—The service profile that contained this virtual drive is deleted or the service profile is no longer associated with a storage profile.
- Not in use—The service profile that contained this virtual drive is in the disassociated state.

Deployment States

Indicates the actions that you are performing on virtual drives. Virtual drives can have the following deployment states:

- No action—No pending work items for the virtual drive.
- Creating—Creation of the virtual drive is in progress.
- Deleting—Deletion of the virtual drive is in progress.
- Modifying—Modification of the virtual drive is in progress.
- Apply-Failed—Creation or modification of the virtual drive has failed.

Operability States

Indicates the operating condition of a virtual drive. Virtual drives can have the following operability states:

- Optimal—The virtual drive operating condition is good. All configured drives are online.
- Degraded—The virtual drive operating condition is not optimal. One of the configured drives has failed or is offline.
- Cache-degraded—The virtual drive has been created with a write cache policy of Write Back Good BBU mode, but the BBU has failed, or there is no BBU.

  Note This state does not occur if you select Always Write Back mode.

- Partially degraded—The operating condition in a RAID 6 virtual drive is not optimal. One of the configured drives has failed or is offline. RAID 6 can tolerate up to two drive failures.

- Offline—The virtual drive is not available to the RAID controller. This is essentially a failed state.
- Unknown—The state of the virtual drive is not known.

Presence States

Indicates the presence of virtual drive components. Virtual drives have the following presence states:

- Equipped—The virtual drive is available.
- Mismatched—A virtual drive deployed state is different from its configured state.
- Missing—Virtual drive is missing.

Virtual Drive Naming

When you use Cisco UCS Central to create a virtual drive, Cisco UCS Central assigns a unique ID that can be used to reliably identify the virtual drive for further operations. Cisco UCS Central also provides the flexibility to provide a name to the virtual drive at the time of service profile association. Any virtual drive without a service profile or a server reference is marked as an orphan virtual drive.

In addition to a unique ID, a name is assigned to the drive. Names can be assigned in two ways:

- When configuring a virtual drive, you can explicitly assign a name that can be referenced in storage profiles.
- If you have not preprovisioned a name for the virtual drive, Cisco UCS Central generates a unique name for the virtual drive.

You can rename virtual drives that are not referenced by any service profile or server.

RAID Levels

The RAID level of a disk group describes how the data is organized on the disk group for the purpose of ensuring availability, redundancy of data, and I/O performance.

The following are features provided by RAID:

- Striping—Segmenting data across multiple physical devices. This improves performance by increasing throughput due to simultaneous device access.
- Mirroring—Writing the same data to multiple devices to accomplish data redundancy.
- Parity—Storing of redundant data on an additional device for the purpose of error correction in the event of device failure. Parity does not provide full redundancy, but it allows for error recovery in some scenarios.
- Spanning—Allows multiple drives to function like a larger one. For example, four 20 GB drives can be combined to appear as a single 80 GB drive.

The supported RAID levels include the following:

- RAID 0 Striped—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails. A minimum of one disk is required for RAID 0.

- RAID 1 Mirrored—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives. A minimum of two disks are required for RAID 1.
- RAID 5 Striped Parity—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.

  RAID 5 distributes parity data blocks among the disks that are part of a RAID-5 group and requires a minimum of three disks.
- RAID 6 Striped Dual Parity—Data is striped across all disks in the array and two sets of parity data are used to provide protection against failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.

  Other than addition of a second parity block, RAID 6 is identical to RAID 5 . A minimum of four disks are required for RAID 6.
- RAID 10 Mirrored and Striped—RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates through block-level striping. RAID 10 is mirroring without parity and block-level striping. A minimum of four disks are required for RAID 10.
- RAID 50 Striped Parity and Striped—Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance. A minimum of six disks are required for RAID 50.
- RAID 60 Striped Dual Parity and Striped—Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance. A minimum of eight disks are required for RAID 60.

Supported LUN Modifications

Some modifications that are made to the LUN configuration when LUNs are already deployed on an associated server are supported.

The following are the types of modifications that can be performed:

- Creation of a new virtual drive.
- Deletion of an existing virtual drive, which is in the orphaned state.
- Non-disruptive changes to an existing virtual drive. These changes can be made on an existing virtual drive without loss of data, and without performance degradation:
  - Policy changes. For example, changing the write cache policy.
  - Modification of boot parameters

The removal of a LUN will cause a warning to be displayed. Ensure that you take action to avoid loss of data.

Unsupported LUN Modifications

Some modifications to existing LUNs are not possible without destroying the original virtual drive and creating a new one. All data is lost in these types of modification, and these modifications are not supported.

Disruptive modifications to an existing virtual drive are not supported. The following are unsupported disruptive changes:

- Any supported RAID level change that can be handled through reconstruction. For example, RAID0 to RAID1.
- Increasing the size of a virtual drive through reconstruction.
- Addition and removal of disks through reconstruction.

Destructive modifications are also not supported. The following are unsupported destructive modifications:

- RAID-level changes that do not support reconstruction. For example, RAID5 to RAID1.
- Shrinking the size of a virtual drive.
- RAID-level changes that support reconstruction, but where there are other virtual drives present on the same drive group.
- Disk removal when there is not enough space left on the disk group to accommodate the virtual drive.
- Explicit change in the set of disks used by the virtual drive.

LUN Dereferencing

A LUN is dereferenced when it is no longer used by any service profile. This can occur as part of the following scenarios:

- The LUN is no longer referenced from the storage profile
- The storage profile is no longer referenced from the service profile
- The server is disassociated from the service profile
- The server is decommissioned

When the LUN is no longer referenced, but the server is still associated, re-association occurs. When the service profile that contained the LUN is disassociated, the LUN state is changed to Not in Use. When the service profile that contained the LUN is deleted, the LUN state is changed to Orphaned. When decommissioning the server, the state of all the LUNs associated with the server is changed to Not in use or Orphaned. However, no action is taken to delete the actual LUNs.

Note When LUNs are orphaned, the LUNs stay in the shared storage and the content is preserved. You can reclaim the orphan LUN to retrieve the data and attach the LUN to a new service profile.

Creating or Editing a Storage Profile

Step 1 In the **Actions** bar, type **Create Storage Profile** and press Enter.

Step 2 In the **Storage Profile** dialog box, click **Basic**, then select the **Organization** in which you want to create the storage profile.

Step 3 Enter the **Name** and optional **Description**.
The name is case sensitive.

Step 4 Select the server type where you plan to apply the storage profile.

Step 5 In **Local LUNs**, click **Add** to add a new local LUN.

Step 6 Click **Basic** to add a new LUN, or **Claim Mode** to reclaim a previously orphaned LUN.
Creating a local LUN in Claim Mode will claim an orphaned LUN when the storage profile is applied to an associated service profile.

Step 7 In the **Basic** tab, do the following:

a) Enter the size in GB.
The size must be between 1 GB and 10240 GB.

b) Choose whether to enable automatic deployment for the local LUN.

c) Choose whether this LUN can be expanded to use the entire available disk group. For each service profile, only one LUN can use this option.

Step 8 In the **Disk Group** tab, select the **Disk Group Configuration Policy** that you want to apply. If you want to encrypt a disk, select the Disk Group with Security enabled.

Step 9 In **Controller Defs**, click **Add**.

Step 10 Enable configuration protection in order to prevent a service profile using this local disk policy from being associated to a server with a different physical disk configuration.
If the service profile includes a local disk policy with configuration protection enabled, and there is an attempt to associate that service profile to a server that includes disks with a different local disk configuration, the association will immediately fail with a configuration mismatch error.

Caution We recommend that you enable configuration protection to preserve any data that may exist on local disks. If disabled, any existing volume that does not match the local disk configuration policy will be deleted.

Step 11 Set the RAID level.
See RAID Levels, on page 61 for detailed information about the different levels.

Step 12 In **Security Policy**, click the **Local** tab, and enter 32 character alphanumeric character key in the **Key** field.

Attention Use the instructions in Step 12 and later only if you want to enable security for the drives. You can choose to enable a Local or Remote security policy. If you do not want to enable security for the drives, select **None** in the **Security Policy** tab and proceed.

This key is used to encrypt the data in the disks. You can create a local security policy on a new or existing Storage profile.

Step 13 (Optional) To edit or modify the **Local Security** policy, enter the current security key for the database in **Deployed Key**.

Step 14 In **Security Policy**, click the **Remote** tab, and enter the following details:

Important Before you create a Remote Security policy, you must have created a KMIP Client Certificate policy. You can create a remote policy on a new or existing storage profile.

a) Enter the **Primary Server IP Address/Hostname**. These credentials are used for accessing the KMIP server to fetch the key.
b) (Optional) Enter the **Secondary Server IP Address/Hostname**.
c) Enter the port number of the server in **Port**.
d) Enter seconds in number in **Timeout**.
e) Enter the contents of KMIP certificate in **KMIP Server Public Certificate**.
Save this certificate from the browser in base-64 format.

a) Select **Enable** to enter **Username** and **Password** to enable SED management through manual key configuration.

Step 15 Click **Create**.

Step 16 To modify a **Remote Security** policy and make it a **Local Security** policy, select the policy you want to modify and repeat the procedure in Step 14, and follow these steps:

a) Click **Local Policy** option and enter a new security key for the controller in the **Key** field.

- The key created is associated to the storage profile and is deployed under the storage controller. To verify, navigate to **Server** > **Controller**.
- After you configure the key from the KMIP server, navigate to the **Custom Attributes** column in the **Secure Key Management Console** page and add the serial number of the controller. You can obtain the serial number of the controller from the **Server** inventory.
- Verify that the **Security** field shows **Drive Security Enabled**. For more information on Enabling/Disabling security on disks, see Creating or Editing a Disk Group Configuration Policy, on page 66.
- You can check the status of the storage configuration in **Configuration Status**.

Disk Groups and Disk Group Configuration Policies

Servers in a chassis can use storage that is centralized in that chassis. You can select and configure the disks to be used for storage. A logical collection of these physical disks is called a disk group. Disk groups allow you to organize local disks. The storage controller controls the creation and configuration of disk groups.

A disk group configuration policy defines how a disk group is created and configured. The policy specifies the RAID level to be used for the disk group. It also specifies either a manual or an automatic selection of disks for the disk group, and roles for disks. You can use a disk group policy to manage multiple disk groups. However, a single disk group can be managed only by one disk group policy.

Creating or Editing a Disk Group Configuration Policy

Step 1 In the **Actions** bar, type, **Create Disk Group Configuration Policy** and press Enter.

Step 2 In the **Disk Group Configuration Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the disk group configuration policy.

Step 3 Enter the **Name** and optional **Description**.
The name is case sensitive.

Step 4 Select the **Raid Level**.
This can be one of the following:

- **RAID 0 Striped**
- **RAID 1 Mirrored**
- **RAID 5 Striped Parity**
- **RAID 6 Striped Dual Parity**
- **RAID 10 Mirrored & Striped**
- **RAID 50 Striped Parity & Striped**
- **RAID 60 Striped Dual Parity & Striped**

Step 5 In **Disk Group**, choose one of the following:

- **Auto—**Choose the **Drive Type**, type values for the drive information, and choose whether to use the remaining disks.
- **Manual—**Add a disk slot ID, and select the Span and disk role for the slots.

You can create a policy with SEDs and enter the **Disk Slot ID** in the **Configuration** details.

Step 6 In **Virtual Drive** icon, complete the fields as necessary.

Step 7 In **Security** select **Enable** or **Disable** to automatically scan the disk for the SED capable disks and pick them.

Step 8 Click **Create**.

The **Security** field in the **Controller** details displays DriveSecurityCapable, Enabled after you enable security.

Monitoring the Health of SSDs

Cisco UCS Central lets you monitor the following SSD conditions (statistics) as reported by Cisco UCS Manager:

- Wear status (displayed in days)
- Percentage of disk life remaining
- Power cycle count

- Power on hours

Step 1 Click the **Dashboard** icon and choose **Servers**.
Step 2 Choose the server that contains the SSD.
Step 3 Click the **Controller** icon.
Step 4 Choose the controller managing the SSD.
Step 5 Click the **Launch** icon and from the drop-down list choose **Statistics**.