



Cisco UCS Central Server Management Guide, Release 2.0

First Published: 2017-05-16

Last Modified: 2019-12-19

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

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

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

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

CHAPTER 1

Overview	1
Overview	1
Cisco UCS Central User Documentation Reference	1

CHAPTER 2

Cisco UCS Servers	3
Server Management	3
Replacing a Server	3
Unified KVM Launcher	4
Using the Unified KVM Launcher	4
Inband Policy	4
Create Inband Policy	4
About KVM Outband Configuration	5
Equipment Policies	6
Managing Equipment Policies	6
Managing Rack Discovery Policies	7
Physical and Logical Inventory	8
Fabric Interconnect	8
Fabric Interconnect Main View	8
Fabric Evacuation	16
Configuring Fabric Evacuation	17

Server Details	18
Servers Details Page	19
Launch Cisco UCS Manager Power Tab	23
NIC Mode and NIC Redundancy Settings	25
Launch Cisco UCS Manager SEL Logs	26
Launch Cisco UCS Manager Server Temperatures Tab	26
Launch Cisco UCS Manager VIF Paths Tab	29
Launch Cisco UCS Manager Adapter Interface Statistics	29
Launch Cisco UCS Manager Server Statistics Tab	32
Launch Cisco UCS Manager CIMC Sessions Tab	34
Launch Cisco UCS Manager Installed Host Firmware Package Tab	35
About End-to-End Diagnostics	36
Configuration Status	38
FlexFlash Configuration Status	40
Chassis Inventory	40
Chassis Main View	40
Storage Chassis View	52
FEX	53
FEX Main View	54
Domains Table View	57
Domain Group Details	57
Domains Main View	58
ID Universe	59
All Pools	60
Exporting Inventory Lists	60
Viewing Configuration Status	60
Inventory Faults	60
Toggling Locator LEDs	61
About End-to-End Diagnostics	61
Displaying the Results of an End-to-End Diagnostic Test	62
Dynamic Searches	63
Saving Dynamic Search Queries	63
Executing a Saved Search Query	63
Deleting a Saved Search Query	64

CHAPTER 3	Hardware Compatibility Report	65
	Hardware Compatibility Report	65
	Hardware Compatibility Page	66
	Create Hardware Compatibility Report	66
	Running the HCL on a Host Firmware Package Policy	67
	Running the HCL on a Service Profile or Service Profile Template	67
	Viewing Hardware Compatibility Report Results	68
	Hardware Compatibility Report Layout	69
	Hardware Compatibility Lists	70
	Scheduling Periodic Hardware Compatibility List Synchronization	70
	Running On Demand Hardware Compatibility List Synchronization	71
	Manually Downloading and Importing Compatibility Lists	72

CHAPTER 4	Service Profiles and Templates	73
	Service Profile Templates	73
	Creating or Editing a Service Profile Template	73
	Service Profile Template Detail View	75
	Service Profiles	75
	Creating a Service Profile from a Template	75
	Binding a Service Profile to a Template	76
	Unbinding a Service Profile from a Template	76
	Manually Assigning a Server to a Service Profile	77
	Configuring Interface Placement on a Service Profile or Service Profile Template	77
	Viewing Service Profile Configuration Status	78
	UUID Synchronization Behavior	78
	Configuring UUID Synchronization Behavior	79
	Using Static IDs	79
	Setting the Management VLAN	80
	Assigning Static IDs	80
	Pool IDs	81
	Resetting IDs	81
	Service Profile Views	82
	Service Profile Detail View	82

Creating or Editing an FC Zone Profile	84
Local Service Profile Detail View	85
Templates Table	86
Profiles Table	86
UCS Central Faults	86
Service Profile Server Faults	87
Service Profile Faults	87
Service Profile Event Logs	87
Service Profile Audit Logs	88

CHAPTER 5**Globalization of Local Service Profiles 89**

About Globalizing a Local Service Profile	89
Globalize Local Service Profiles View	91
Globalizing Local Service Profiles	93
Blocker Issues in Globalization	93
Globalization Tasks View	94
Resolving Pool Conflicts	95
Resolving Policy Conflicts	95
About Globalizing a VLAN/VSAN	96
Globalization of VLANs/VLANs View	97
Conflicts in Globalizing a VLAN/VSAN	98
Globalizing VSANs and VLANs	99
Resolving VLAN Conflicts	99
Resolving VSAN Conflicts	100
Resolving Multicast Policy Conflicts	100

CHAPTER 6**Server Pools 103**

Server Pools	103
Creating or Editing a Server Pool	103
Server Pool Qualification Policy	104
Creating or Editing a Server Pool Qualification Policy	105
IP Pools	105
Creating and Editing an IP Pool	106
Creating and Editing a Management IP Pool	107

Configuring Management IPs	108
IQN Pools	109
Creating and Editing an IQN Pool	109
UUID Suffix Pools	110
Creating and Editing a UUID Suffix Pool	110

CHAPTER 7
Server Boot 113

Boot Policy	113
Boot Order	114
UEFI Boot Mode	115
UEFI Secure Boot	116
Cautions and Guidelines for Downgrading a Boot Policy	116
Creating or Editing a Boot Policy	117
Configuring iSCSI Targets	118

CHAPTER 8
Server Policies 119

Server Policies	119
BIOS Policy	119
Creating or Editing a BIOS Policy	120
Default BIOS Settings	121
Basic BIOS Settings	121
Processor BIOS Settings	124
I/O BIOS Settings	137
RAS Memory BIOS Settings	138
USB BIOS Settings	140
PCI BIOS Settings	143
Graphics Configuration BIOS Settings	150
Boot Options BIOS Settings	151
Server Manager BIOS Settings	152
Console BIOS Settings	154
IPMI Access Profile	158
Creating and Editing an IPMI Access Profile	158
Serial over LAN Policy	158
Creating and Editing a Serial over LAN Policy	159

Hardware Change Discovery Policy	159
Create Hardware Change Discovery Policy	159
Host Firmware Package Policy	160
About Service Packs	161
Creating or Editing a Host Firmware Package Policy	162
iSCSI Adapter Policy	163
Creating or Editing an iSCSI Adapter Policy	163
iSCSI Authentication Profile	163
Creating or Editing an iSCSI Authentication Profile	163
Local Disk Policy	164
Creating or Editing a Local Disk Policy	164
Port Auto-Discovery Policy	165
Creating or Editing Port Auto-Discovery Policy	165
Graphics Card Policy	165
Creating and Editing a Graphics Card Policy	166
Statistics Threshold Policy	166
Creating a Statistics Threshold Policy	167
Scrub Policy	168
Creating or Editing a Scrub Policy	169
vMedia Policy	169
Creating or Editing a vMedia Policy	170



Preface

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

Audience

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

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

Conventions

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

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



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



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



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



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



Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

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

Documentation Feedback

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



CHAPTER 1

Overview

- [Overview, on page 1](#)
- [Cisco UCS Central User Documentation Reference, on page 1](#)

Overview

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

- UCS server hardware
- Service profile and templates
- Server boot
- Server policies

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.
Cisco UCS Central Authentication Guide	Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP.

Guide	Description
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

Cisco UCS Servers

- [Server Management, on page 3](#)
- [Replacing a Server, on page 3](#)
- [Unified KVM Launcher, on page 4](#)
- [Inband Policy, on page 4](#)
- [About KVM Outband Configuration, on page 5](#)
- [Equipment Policies, on page 6](#)
- [Physical and Logical Inventory, on page 8](#)
- [About End-to-End Diagnostics, on page 61](#)
- [Dynamic Searches, on page 63](#)

Server Management

With global policies, global server pools and firmware management in Cisco UCS Central, you can manage general and complex server deployments for the following servers in your registered UCS domains:

- Cisco UCS B-Series Blade Servers
- Cisco UCS C-Series Rack-Mount Servers
- Cisco UCS Mini

Replacing a Server

If you plan to replace a server registered in a Cisco UCS Domain, use the following instructions to prepare for the replacement:

1. Disassociate any service profiles associated with the server from Cisco UCS Central.
2. Decommission the server from Cisco UCS Central. If a motherboard replacement is required, delete the server from any of the associated pools and refresh inventory.
3. Perform the necessary maintenance actions and reacknowledge the server from Cisco UCS Central.
4. After the server is discovered, add it back to the server-pools as required.
5. Refresh the inventory if required, and reassociate the service profiles from Cisco UCS Central.

Unified KVM Launcher

The **Unified KVM Launcher** page allows you to connect to any server in the Cisco UCS domain, whether or not they are associated with a service profile.

Beginning with Release 1.4, you can create users with the KVM privilege, or use the new KVM role that only has the KVM privilege. When users that only have the KVM privilege log into the Cisco UCS Central HTML5 UI, they will only be able to view the unified KVM launcher page.

Using the Unified KVM Launcher

Procedure

- Step 1** On the **Unified KVM Launcher** page, select the server that you want to connect to.
Use the checkboxes in the **Filters** area to narrow down the selections.
- Step 2** Click **Launch KVM**.
-

Inband Policy

Cisco UCS Central lets you configure the Inband IP address on a server directly, or through an **Inband Policy**. This feature is supported on Cisco UCS Manager release 4.1 (3) and later. After you create an Inband policy, you can assign it to a domain group from **Domain Configuration Settings** in **Domains Main View**. The **Inband Policy** view displays details about the corresponding **VLAN Group**, the **Default Management VLAN**, and the **Management IP pool** associated with the policy.

Create Inband Policy

Procedure

- Step 1** In the **Actions** bar, type **Create Inband Policy** and press Enter.
- Step 2** In the **Create Inband Policy** dialog box, choose the **Domain Group Location** in which you want to create the policy and enter the **Name** and optional **Description**.
The name is case sensitive.
- Step 3** In **VLAN Group**, select the VLAN group from the **VLAN Group** drop-down list, and the VLAN ID from the **Default Management VLAN** drop-down list to associate with this policy.
- Step 4** In **IP Pool**, select **Management IP Pool** from the drop-down list to associate it with this policy.
- Step 5** Click **Create**.
- Step 6** (Optional) You can favorite this policy and pin it to the Cisco UCS Central dashboard to navigate to it directly.

After you create an Inband policy, you can assign it to a domain group from the **Domain Configuration Settings** in **Domains Main View**.

- Step 7** In the **Domain Configuration Settings** window, click **Inband Policy** in the **Management IP** tab, and select the policy you want to assign to the domain group.

About KVM Outband Configuration

Beginning Cisco UCS Central, you can create a KVM Outband IP pool on Cisco UCS Central and assign it to a domain directly. With a KVM Outband IP pool, you can automatically push down the IP addresses to available blade and rack servers by assigning them to a Cisco UCS domain through **Domain Configuration Settings**. The physical KVM Outband settings are independent from the KVM Outband configuration associated with a service profile. This feature is supported on Cisco UCS Manager 4.1(3) and later.

KVM Outband IP pools have the following features:

- An Outband pool pushed down to Cisco UCS Manager can override any local configuration on Cisco UCS Manager. However, a Cisco UCS Manager user can edit the Outband KVM configuration locally, and the option to edit the IP pool is not grayed out on the Cisco UCS Manager GUI.
- When an Outband configuration is altered locally on Cisco UCS Manager, the IP addresses associated with the pool are released and are available for other associations.
- If you are non-admin Cisco UCS Central user, you require Domain-Group-Management privileges to create, read, update, or delete a KVM Outband configuration.
- When you modify a Management IP pool to add, remove, or update a block, use the **Reapply Configuration** option from the **Domains Main View**. This option ensures that the pool is refreshed with the modified IP addresses before it is pushed down to Cisco UCS Manager. However, if you unassign a pool or switch the Management IP pools, you do not have to reapply the configuration settings.



Note A warning message displays when you use the **Reapply Configuration** option. When you accept the option to reapply the configuration, Cisco UCS Central reapplies the configuration of only the Management IP addresses.

- You can verify the assigned physical KVM Outband IP pool when you **Launch KVM** from the **Server Details** page. The drop-down menu on the KVM Console Launch displays the physical KVM Outband and the IPv4 Outband associated with a service profile.



Note IPv6 is not supported for KVM Outband.

- You can access the CIMC through an Outband or Inband address. In the case of an Outband address, traffic traverses the fabric interconnect (FI) via the management port to the network. Traffic to and from an Inband address traverses through the FI via the fabric uplink port.
- In Cisco UCS Central, KVM Outband support is managed through an IP pool and not with a static IP.

Equipment Policies

Equipment policies allow you to tune your servers and other equipment to suit your requirements. Equipment policies can only be set at the domain group level, and apply to all servers in that domain group.



Note Equipment policies are not included in service profiles.

Managing Equipment Policies

Procedure

-
- Step 1** Click the **Domain Group Navigation** icon and choose a domain group.
- Step 2** Click the **Configuration** icon and choose **System Policies**.
- Step 3** In **Equipment**, click **Basic** and complete the following fields:
- In **Rack Management Action**, select how server management is configured when a new rack server is discovered:
 - **Auto Acknowledged**—Cisco UCS automatically configures server management by domain based on the available server connections.
 - **User Acknowledged**—Cisco UCS does not automatically configure server management. It waits until acknowledged by the user.
 - In **MAC Address Table Aging Time**, select the length of time an idle MAC address remains in the MAC address table before it is removed:
 - **Mode Default**—System uses the default value. For end-host mode, the default is 14,500 seconds. For switching mode, the default is 300 seconds.
 - **Never**—Cisco UCS never removes MAC addresses from the table.
 - **Other**—Enter a custom value in the dd:hh:mm:ss field.
 - In **VLAN Port Count Optimization**, select whether Cisco UCS can logically group VLANs to optimize the use of ports and reduce the CPU load on the FI.
 - In **Firmware Auto Server Sync State**, select the firmware synchronization policy for recently discovered blade servers or rack servers:
 - **User Acknowledged**—Cisco UCS does not synchronize firmware until the administrator acknowledges the upgrade.
 - **No Actions**—Cisco UCS does not perform any firmware upgrade on the server.
 - In **Info Action**, select whether the information policy displays the uplink switches that are connected to the Cisco UCS domain.

- Step 4** Click **Discovery** and complete the fields to specify how you want the system to behave when you add a new chassis or FEX:
- In **Chassis/FEX Link Action**, select the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.
 - In **Chassis/FEX Link Grouping Preference**, select whether the links from the system IO controllers, IOMs, or FEXes to the fabric interconnects are grouped in a port channel.
 - In the **Multicast Hardware Hash**, click **Enable** to specify if Cisco UCS can use all of the links from the IOMs or FEXes to the fabric interconnects for multicast traffic.
 - In the **Backplane Speed Preference**, choose the speed that you want to use.
- Step 5** Click **Power** and complete the following fields:
- In **Power Redundancy**, select the power redundancy policy that you want to use:
 - **N+1**—The total number of power supplies, plus one additional power supply for redundancy, equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS sets them to a "turned-off" state.
 - **Grid**—Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails, the surviving power supplies continue to provide power to the chassis.
 - **Non-Redundant**—All installed power supplies are turned on and the load is evenly balanced. Only power small configurations (requiring less than 2500W) by a single power supply.
 - In **Power Allocation**, select the power allocation management mode used in the Cisco UCS domain:
 - **Policy Driven Chassis Group Cap**—Configures power allocation at the chassis level through power control policies included in the associated service profiles.
 - **Manual Blade Level Cap**—Configures power allocation on each individual blade server in all chassis.

Specifies how the power cap values of the servers are calculated. If it is enabled, the servers will be profiled during discovery through benchmarking. This policy applies when the Global Power Allocation Policy is set to Policy Driven Chassis Group Cap.
 - In **ID Soaking Interval**, specify the number of seconds Cisco UCS Central waits before reassigning a pool entity that Cisco UCS released. Enter an integer between 0 and 86400.
- Step 6** Click **Save**.

Managing Rack Discovery Policies

Procedure

- Step 1** Click the **Domain Group Navigation** icon and choose a domain group.
- Step 2** Click the **Configuration** icon and choose **System Policies**.
- Step 3** In **Rack Discovery**, click **Enabled**.
- Step 4** In **Basic**, for **Discovery Policy Action**, select how you want the system to behave when you add a new rack server.

- **Immediate**—Cisco UCS domain attempts to discover new servers automatically.
- **User Acknowledged**—Cisco UCS domain waits until the user tells it to search for new servers.

Step 5 Click **Policies** and select the scrub policy that you want to run on a newly discovered server.

The server must meet the criteria in the selected server pool policy qualification.

Step 6 Click **Save**.

Physical and Logical Inventory

Cisco UCS Central allows you to view all fabric interconnects, servers, chassis, and FEXes located in your Cisco UCS domains. You can also view individual components for each type of hardware, such as cartridges, fans, CPUs, IOMs, and ports.

You can also view the logical inventory details such as the server pools and ID pools in the registered UCS domains.

Fabric Interconnect

The **Fabric Interconnect (FI)** page displays the following information related to FIs associated with the registered Cisco UCS domain:

FI	Hardware	FW	Status
<p>This column displays the following information for a fabric interconnect:</p> <ul style="list-style-type: none"> • The associated domain name and FI ID • Domain group location • IP address of the domain 	<p>This column displays the following hardware information for a fabric interconnect:</p> <ul style="list-style-type: none"> • The model number and type of FI • Serial number • The number of fixed and expansion module ports • The number of ethernet and fabric channel ports 	<p>This column displays the following firmware details for a fabric interconnect:</p> <ul style="list-style-type: none"> • Firmware version • Firmware status 	<p>This column displays the following status for a fabric interconnect:</p> <ul style="list-style-type: none"> • Overall status • Worst fault level • Locator LED status

Fabric Interconnect Main View

The **Fabric Interconnect Main View** page displays the following information related to the selected Fabric Interconnect (FI) and its components within a registered Cisco UCS domain.

- **Basic**—Displays an overview of the FI within the domain, hardware details, firmware version, number of ports (Ethernet or FC) that are in use and available for use, management IP, and fault summary details.

- **Fixed Mod.**—Displays overall status, firmware, hardware, properties, and fault summary details of the fixed modules installed in the FI .
- **Exp. Mod.**—Displays overall status, firmware, hardware, properties, and fault summary details of the expansion modules installed in the FI.
- **Fans**—Displays overall status, and hardware details of the fan.
- **PSUs**—Displays overall status, fault summary, and hardware details of the PSU.
- **Ports**—Displays ports, port role, and port status for all ports in the FI.
- **Port Channels**—Displays all port channels in the FI and detailed information about each port channel.
- **Traffic Monitoring**—Displays traffic monitoring sessions for the Ethernet or FC ports.

You can also perform the following tasks:

- View configuration status.
- Turn on or off the Locator LED.
- Set the switching mode.
- Manage unified port configuration.
- Create port channels.
- Create Traffic Monitoring.
- Configure Evacuation.



Note You can configure the evacuation state by selecting one of these **Admin Evac Mode** options:

- **Enabled** - Stops the traffic on the IO module or the fabric interconnect
- **Disabled** - Restarts traffic on the IO module or the fabric interconnect

To evacuate a fabric interconnect regardless of its current evacuation state, you can select one of these **Force Evac** options:

- **Enabled** - To evacuate the FI regardless of the current evacuation state
- **Disabled** - Disables force evacuation of the FI regardless of the evacuation state



Note For more information about Fabric Evacuation, see [Fabric Evacuation, on page 16](#) and [Configuring Fabric Evacuation, on page 17](#).

-
- 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.

Launch Cisco UCS Manager Fabric Interconnect Statistics

You can launch Cisco UCS Manager **Fabric Interconnect (FI)** statistics from the **Tools** menu in Cisco UCS Central to view these details for the FI:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB. <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager Fabric Interconnect PSU Statistics

You can launch Cisco UCS Manager PSU statistics for a Fabric Interconnect (FI) from the **Tools** menu in Cisco UCS Central to view these details:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB. <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager Port Statistics

You can launch Cisco UCS Manager Port statistics from the **Tools** menu in Cisco UCS Central to view these details:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB. <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Fabric Evacuation

Cisco UCS Central enables Fabric Evacuation, which is the ability to evacuate all traffic that flows through a fabric interconnect (FI) from all servers attached to it through an IOM or FEX while upgrading a system. Upgrading the secondary FI in a system disrupts active traffic on the FI. This traffic fails over to the primary FI. Using Fabric Evacuation, you can stop all traffic that is active through an FI. After verifying that the traffic failed over completely, and upgrading the secondary FI, you can restart all the stopped flows after rebooting the secondary FI and all the connected IOMs. In a cluster configuration, you can change the cluster lead to the subordinate FI, stop all the flows, and upgrade the other FI in the same manner.

Cisco UCS Central 2.1 supports Fabric Evacuation during Firmware AutoInstall to ensure that the appropriate failover settings are configured for the firmware upgrade. Fabric Evacuation is now automatically turned on during an FI upgrade and reboot during an AutoInstall. Fabric Evacuation is automatically configured when there is an activation prior to reboot on any of the FIs during an AutoInstall. Fabric Evacuation also forces an immediate failover of Fabric-Failover vNICs and ensures that there are no active vNICs in the target FI. This feature avoids the disruption when a primary FI goes down for a short duration for activation, and the secondary FI takes over through the heartbeat loss detection mechanism.

During an upgrade, Fabric Evacuation goes through the following steps:

1. Stop all traffic that is active through an FI.
2. Upgrade the secondary FI.
3. Restart all stopped traffic flows.
4. Change the cluster lead to the secondary FI.
5. Repeat Steps 1 to 4 to upgrade the primary FI.



Note Fabric Evacuation is supported:

- At the FI level in Cisco UCS Manager release 2.2(4) and later.
- In AutoInstall only in Cisco UCS Manager release 4.1(3).
- Only on a subordinate FI.
- In a cluster configuration.

Fabric Evacuation has the following limitations:

- Evacuation on I/O modules is not supported.
- Evacuation of directly-attached rack servers is not supported. Evacuation on the FI is enabled by manually bringing down the server ports when there are directly-connected rack servers. For an IOM/FEX, the HIF ports must be brought down to enable evacuation.
- Downgrade from Cisco UCS Manager 2.2(4) to earlier releases places the FIs in the regular mode. However, server traffic flows through regardless of the configuration on the FI when you run the Cisco UCS Manager 2.2(4) image.
- If you use AutoInstall with Fabric Evacuation to downgrade to a Cisco UCS Manager release earlier than 4.1(3), Fabric Evacuation does not work as configured.
- When an FI is configured for evacuation, all blade and rack servers connected through the Fabric Extender are evacuated.

Configuring Fabric Evacuation

You can configure the fabric evacuation state of a fabric interconnect (FI) to enable or restart all traffic that flows through the FI. You can set the properties to turn Fabric Evacuation on automatically during an FI upgrade and reboot during Auto Install.

Procedure

-
- Step 1** From a **Cisco UCS Domain**, select the **Fabric Interconnects** *name* for which you want to view the fabric evacuation state.
- The **Fabric Interconnect** main view displays the key indicators for the FI, including the **Admin Evac Mode** and the **Oper Evac Mode** that indicate the current evacuation status of the FI.
- Step 2** From **Tools**, select **Configure Evacuation**.
- The **Configure Evacuation** dialog box displays.
- Step 3** To configure fabric evacuation on the specified Fabric Interconnect, select one of the following options under **Admin Evac Mode**:
- **Enabled**—Stops traffic on the IO module or the fabric interconnect
 - **Disabled**—Restarts traffic on the IO module or the fabric interconnect

Step 4 (Optional) To evacuate a Fabric Interconnect regardless of its current evacuation state, select one of the options under **Force**:

- **Enabled**—To evacuate the FI regardless of the current evacuation state
- **Disabled** —Disables force evacuation of the FI regardless of the evacuation state

Note

When you stop the server traffic and then enable traffic evacuation, the system moves to a NO-OP status. When you select the **Force (Enabled)** option, it ensures that the second command does not involve a NO-OP and the traffic is forced to shut down again.

Step 5 Click **OK**.

The following warning messages display when you choose Enabled or Disabled, respectively:

```
There are outstanding faults since last FI reboot. Please make sure all the data paths on
other
FI are working before proceeding with this FI Evacuation to avoid interruption to the data
traffic.
Are you sure you want to continue?
```

```
Disabling fabric evacuation will cause server traffic that failed over to the Primary Fabric
Interconnect to fail back to this Fabric Interconnect. Are you sure you want to continue?
```

Note

After triggering fabric evacuation, the backplane ports on the FEX/IOM are shutdown. You must reboot the fabric interconnect to restart the traffic flows.

Step 6 Click **OK** or **Cancel** on the warning messages as necessary.

On the Fabric Interconnect main view, check the values for **Admin Evac Mode** and **Oper Evac Mode**. These values display the current evacuation status.

Server Details

The **Server** page displays the following information related to the servers associated with the registered Cisco UCS domain:

Servers	Hardware	Configuration	Status
<p>This column displays the following information for a server:</p> <ul style="list-style-type: none"> The associated domain name, chassis ID, and slot ID Domain group location Management IP address 	<p>This column displays the following hardware information for a server:</p> <ul style="list-style-type: none"> Blade server model The number of cores the CPU has and the total RAM on the motherboard The serial number The number of CPUs and the speed 	<p>This column displays the following configuration for a server:</p> <ul style="list-style-type: none"> Service profile name Service profile organization location Firmware version Firmware status 	<p>This column displays the following status for a server:</p> <ul style="list-style-type: none"> Overall status Worst fault level Power status Decommissioned server. <p>You can recommit a decommissioned server. You can also remove a decommissioned rack server and delete all data about the server from the Delete option in the System Tools submenu.</p>

Servers Details Page

You can view the following information on the selected server and its components, and also perform various tasks:



Note Depending on the server type, the options may vary.

- **Basic**—Displays associated service profile, fault summary, hardware, and firmware details of the selected server. The server Asset tag is displayed as a read-only field in this page. Beginning Cisco UCS Central release 2.1, a server reboot log is also displayed with the top five reasons for the reset along with the time and source of power transition. To view the server reboot log, Cisco UCS Central 2.1 must be registered with Cisco UCS Manager 4.1(3) and later.

For servers that have a KMIP Certification policy configured at the domain scope, this tab displays additional details related to KMIP Certificate for the supported servers. For information on security-related remote operations, see Security-Related Operations in the *Cisco UCS Central Storage Management Guide*.

- **Motherboard**—Displays the overall status and the hardware details of the motherboard.
- **CIMC**— Displays the overall status of firmware version, server activity status, hardware specifications, and in-band policy.

- **CPUs**—Displays a list of all the CPUs in the server. Select a processor to view overall status and hardware and other details of the selected processor.
- **GPUs**—Displays a list of all graphics cards in the server. Select a graphics card to view the overall status and additional details.
- **Security**—Displays a list of all hardware security modules in the server, such as the Cisco Mezzanine Crypto Card.
- **Memory**—Displays a list of available memory in the selected server. Select a memory card to view the current overall status and other details.
- **Adapters**—Displays details of the adapter in the selected server. Select an adapter to view overall status, power status, and other product details. The **Interfaces** tab in the **Adapter Details** page displays details of the adapter interfaces that are added to a service profile. Select an interface to view admin state, operability status, MAC addresses, and other details of the interface. The following types of interfaces are displayed in the adapters **Inventory** after you assign them to the service profile:
 - DCE
 - NIC
 - HBA
 - ISCSI



Note Remote operations are not supported on ISCSI devices.

Cisco UCS Central lets you perform one of the following remote operations for the adapter interfaces: enable, disable, or reset connectivity of the devices. For an HBA interface, you can enable or disable the interface, or reset connectivity. In the case of a failover vNIC interface, you can enable, disable, or reset connectivity of the active or stand-by interfaces to the fabric interconnect. The **Configuration Status** window displays the Admin state of the interfaces when there is a change in the remote operations.

- **Controllers**—Displays the list of storage controllers, such as SAS or FlexFlash. Select a controller to view operability and other product details. For FlexFlash FX3S Controllers, you can view the **Configuration Status** of the controller, **Configure Auto-Sync** of the SD cards, **Format SD cards**, and **Reset the FlexFlash Controller** from the **Tools** menu. For all other controllers, these options will be non-operational.

You can perform these server actions for Storage controllers :



Note If you choose to pair or unpair the SD cards from **Configure Auto-Sync**, the contents of the SD cards are synced and the status displayed in the Operation State property. The FlexFlash controller view displays the Operation Status, Raid Pair syncing status and other properties consistent with Cisco UCS Manager. For more information about FlexFlash controller properties in Cisco UCS Manager, see *Cisco UCS Manager Storage Management Guide*.



Note The dual HBA Controllers on the Cisco S3260 servers are discovered and displayed on the server details page. This feature is supported from Cisco UCS Central 2.1 and Cisco UCS Manager 4.1(3) and later.

- **Storage Enclosures**—Displays a list of the storage enclosures in the selected server. You can view details on the enclosure or the individual slots.
- **Storage**—Displays list of the storage in the selected server. Select a disk to view the current overall status, hardware, and controller details.
- **LUNs**—Displays a list of the virtual drives created on the server. Select a virtual drive to view the status, configuration status, and other details. You can also perform virtual-drive related tasks.
- From the **Tools** menu, you can perform the following actions: View Configuration Status, Reset, Recover, Decommission a server, Re-Acknowledge, Reset Server to Factory Default, Configure Management IPs, Start Diagnostic test, Toggle the locator LED. For more information about Diagnostic test, see [About End-to-End Diagnostics, on page 36](#).



Note The **Reset Server to Factory Defaults** is shown only for the supported servers. This feature is supported on servers with CIMC version 2.2(7) and later.

You can perform the following server-related tasks:

- Launch the **KVM Console**. You can launch the HTML-5 based KVM client from Cisco UCS Central 2.1 and later.
- 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.

- Launch Cisco UCS Manager GUI for the selected Cisco UCS domain. Beginning Cisco UCS Central 2.1, you can sign on to a Cisco UCS Domain with the same user credentials that you provide for logging on to Cisco UCS Central. These credentials will provide the same roles/locales as Cisco UCS Central. For the Cisco UCS domains prior to 3.1(2), the existing functionality will continue to work as before. If you are not logged in the Cisco UCS domain with the same password, it prompts you to provide a new password. In order to log in as a remote user, you must authenticate the user role in the **Manage UCS Central Authentication** window. The single sign-on feature works for launching the UCS domain and KVM on any server, or a service profile using the Cisco UCS Central user credentials, roles, and locales.



Note Single sign-on is supported on Cisco UCS Manager release 4.1(3) and later.

- Launch corresponding Cisco UCS Manager Statistics pages for the following:
 - [Launch Cisco UCS Manager CIMC Sessions Tab, on page 34](#)
 - [Launch Cisco UCS Manager SEL Logs, on page 26](#)
 - [Launch Cisco UCS Manager VIF Paths Tab, on page 29](#)
 - [Launch Cisco UCS Manager Server Statistics Tab, on page 32](#)
 - [Launch Cisco UCS Manager Server Temperatures Tab, on page 26](#)
 - [Launch Cisco UCS Manager Power Tab, on page 23](#)
 - [Launch Cisco UCS Manager Installed Host Firmware Package Tab, on page 35](#)



Important To view Cisco UCS Manager content from Cisco UCS Central, ensure to log in to the Cisco UCS Central GUI with the same hostname, or IP address that was used to register Cisco UCS Manager with Cisco UCS Central.

Beginning Cisco UCS Central 2.1, you can launch the KVM HTML-5 based client from the sub-menu in the **Server** view. The HTML-5 based client launches only if your set up has Cisco UCS Manager 4.1(3) or later, and if you have installed CIMC version 3.1.22.x and higher. This feature is supported on the Cisco UCS B-Series server models or higher. If you run earlier versions of Cisco UCS Manager with the supported versions of firmware, **Launch KVM Client** launches the Java based client.

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.

Component	Remote Action	Action
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*.

Launch Cisco UCS Manager Power Tab

You can launch Cisco UCS Manager server power statistics from the **Tools** menu in Cisco UCS Central to view these details for the server:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB. <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

NIC Mode and NIC Redundancy Settings

Table 1: Valid NIC Redundancy Settings For Each NIC Mode

NIC Mode	Valid NIC Redundancy Settings
Shared LOM EXT	Active-active
Dedicated	None
Shared LOM	Active-active Active-standby
Cisco Card	Active-active Active-standby

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

- *Shared LOM EXT* (default)—This is the shared LOM extended mode, the factory-default setting. With this mode, the Shared LOM and Cisco Card interfaces are both enabled. You must select the default *Active-Active* NIC redundancy setting in the following step.

In this NIC mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco card are disabled. Use the Cisco Card NIC mode if you want to connect to Cisco IMC through a Cisco card in standalone mode.

- *Shared LOM*—The 1-Gb/10-Gb Ethernet ports are used to access Cisco IMC. You must select either the *Active-Active* or *Active-standby* NIC redundancy setting in the following step.
- *Dedicated*—The dedicated management port is used to access Cisco IMC. You must select the *None* NIC redundancy setting in the following step.

- *Cisco Card*—The ports on an installed Cisco UCS Virtual Interface Card (VIC) are used to access the Cisco IMC. You must select either the *Active-Active* or *Active-standby* NIC redundancy setting in the following step.

See also the required VIC Slot setting below.

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

- *None*—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.
- *Active-standby*—If an active Ethernet port fails, traffic fails over to a standby port. Shared LOM and Cisco Card modes can each use either Active-standby or Active-active settings.
- *Active-active* (default)—All Ethernet ports are utilized simultaneously. The Shared LOM EXT mode must use only this NIC redundancy setting. Shared LOM and Cisco Card modes can each use either Active-standby or Active-active settings.

Launch Cisco UCS Manager SEL Logs

You can launch the Cisco UCS Manager SEL Logs from Cisco UCS Central to view the system event log generated by the server.

It includes the following buttons below the log:

- **Export**—Exports the log to a text file.
- **Copy**—Copies the selected portion of the log to the clipboard.
- **Print**—Opens the **Print** dialog box so that you can print the log.
- **Refresh**—Displays any new messages that have been generated since the log was displayed.
- **Backup**—Backs up the log to the server specified in the SEL policy for this Cisco UCS domain.
- **Clear**—Clears the entries from the log.



Note This action triggers an automatic backup if **Clear** is enabled in the SEL policy **Action** option box.

Launch Cisco UCS Manager Server Temperatures Tab

Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.

Name	Description
Modify Collection Policy button	<p>Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter.</p> <p>Note This option is only available if a counter is selected.</p>
Name column	<p>A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart.</p> <p>System statistics for fabric interconnects and FEX are available. These include:</p> <ul style="list-style-type: none">• CPU usage• Memory usage, including low kernel memory <p>Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB.</p> <ul style="list-style-type: none">• ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager VIF Paths Tab

You can launch the Cisco UCS Manager VIF Paths table from Cisco UCS Central to view the following details about VIF Paths:

Name	Description
Name column	The name of the virtual interface path. Expand the name to view the virtual circuits contained in that path, if any.
Adapter Port column	The adapter port associated with this interface.
FEX Host Port column	The FEX port that serves as the host port for this interface.
FEX Network Port column	The FEX port that serves as the network port for this interface.
FI Server Port column	The fabric interconnect (FI) port information, in the form <i>fabric name/port ID/slot ID</i> .
vNIC column	The vNIC associated with the virtual circuit.
FI Uplink column	The uplink status for the FI.
Link State column	The link state for the interface.
State Qual column	The link quality for the interface.

Launch Cisco UCS Manager Adapter Interface Statistics

You can launch Cisco UCS Manager adapter interface statistics from the **Tools** menu in Cisco UCS Central to view these details about the following adapter interfaces:

- HBAs
- NICs
- iSCSI vNICs

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none">• CPU usage• Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB. <ul style="list-style-type: none">• ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager Server Statistics Tab

Statistics Subtab

You can launch the Cisco UCS Manager Server Statistics tab from Cisco UCS Central and view the statistical counters available for the selected component.

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.

Name	Description
<p>Name column</p>	<p>A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart.</p> <p>System statistics for fabric interconnects and FEX are available. These include:</p> <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory <p>Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB.</p> <ul style="list-style-type: none"> • ECC errors
<p>Value column</p>	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)

Name	Description
Avg column	The average value for the counter. Note For aggregated counters, this is the average delta within the reporting interval.
Max column	The maximum recorded value for the counter. Note For aggregated counters, this is the maximum delta within the reporting interval.
Min column	The minimum recorded value for the counter. Note For aggregated counters, this is the minimum delta within the reporting interval.
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager CIMC Sessions Tab

You can view the Cisco UCS Manager CIMC Sessions for a registered UCS domain from Cisco UCS Central. The following details are displayed for the active CIMC sessions:

Column	Description
Name	The name of the user who launched the session.
Session ID	The ID associated with the session.
Session Type	This can be one of the following: <ul style="list-style-type: none"> • KVM • Vmedia • SOL

Column	Description
CIMC Address	The Management IP address on which the session is established.
Login Time	The date and time the session started.
Last Update Time	The last time the session information was updated by CIMC.
Administrative State	This can be one of the following: <ul style="list-style-type: none"> • Active • Inactive
Privilege	The privilege level of the user. This can be one of the following: <ul style="list-style-type: none"> • Read-write (RW) • Read Only • Granted (vMedia)
Source Address	The IP address of the computer from which the session was opened.
Service Profile	The name of the service profile associated with the session. The value is displayed when a session is launched with the service profile IP address. Note This field is not displayed when you view CIMC Sessions from the Servers tab.
Server	The name of the server associated with the session. Note This field is not displayed when you view CIMC Sessions from the Equipment tab.

Launch Cisco UCS Manager Installed Host Firmware Package Tab

You can view the Cisco UCS Manager **Installed Host Firmware Package** tab from the list of Policies in the **Service Profile Details** view. This option is available only if you have an associated service profile. You can view the following details for the installed firmware pack items:

Name	Description
Update Firmware button	Click this button to update the firmware on one or more components.

Name	Description
Activate Firmware button	Click this button to activate the backup firmware version on one or more components.
Capability Catalog button	Click this button to open the Catalog Update Tasks Tab.
Management Extension button	Click this button to open the Management Extension General Tab..
Name column	A navigation tree that allows you to view a particular component and its subcomponents. You can right-click a component to view any actions available for that component.
Model column	The model number.
Running Version column	The firmware version used by the component.
Startup Version column	The version of the firmware that takes effect the next time that the component reboots.
Backup Version column	Displays the firmware version that exists in memory, but is not being used by the server.
Update Status column	This can be one of the following: <ul style="list-style-type: none"> • Ready—This firmware version is ready to activate. • Updating—This firmware version is being updated. • Failed—The firmware update failed. For more information, double-click the component to view the Status Details area on the General tab.
Activate Status column	This can be one of the following: <ul style="list-style-type: none"> • Ready—Activation succeeded and the component is running the new version. • Activating—The system is activating the new firmware version. • Failed—The firmware activation failed. For more information, double-click the failed component to view its status properties.

About End-to-End Diagnostics

With Cisco UCS Central, you can initiate end-to-end diagnostics in an integrated fashion with Cisco UCS Manager, in order to troubleshoot hardware issues and conduct burn-in tests on your environments.



Note Cisco UCS Central does not fully support end-to-end diagnostics. For task-based information on conducting end-to-end diagnostics refer to the Cisco UCS Manager documentation. This feature also excludes policies in Cisco UCS Central. Also, Cisco UCS Central does not report instances of bad memory.



Note Initiating the end-to-end diagnostic process causes a system reboot. Also, if the process should stop mid-execution, a fault message is captured and displays the stage in which the fault occurred. You can manually restart the diagnostic process.



Note The connectivity to a Cisco UCS Domain can temporarily show **Lost Connectivity** status. This happens when Cisco UCS Manager gets extremely busy processing the job at hand and may not be able to respond to HeartBeat messages from Cisco UCS Central. The system will recover to normal connectivity after the Cisco UCS Domain completes the job.

Feature	Functions
Remote diagnostic capability	Remotely diagnose your Cisco UCS Manager hardware components and environments.
Trigger the diagnostic process (start/stop) from Cisco UCS Central	Initiate the diagnostic process from within Cisco UCS Central and then let Cisco UCS Manager continue with the full diagnostic process.
Diagnoses multiple servers simultaneously	Cisco UCS Central can identify multiple servers to diagnose.
Dynamically assign diagnostic policy changes to Cisco UCS Manager	Policy changes can be pushed from Cisco UCS Central to Cisco UCS Manager.

Conducting End-to-End Diagnostics

With Cisco UCS Central, you can initiate end-to-end diagnostics in an integrated fashion with Cisco UCS Manager, in order to troubleshoot hardware issues and conduct burn-in tests on your environments.



Note You can run diagnostics on both servers and domains. However, initiating the diagnostic process causes a server reboot. Additionally, if the diagnostic test fails, an error is shown in the fail stage in the FSM and in the result session. If you manually stop the diagnostic process, no error is displayed. Consequently, if the process should stop mid-execution, a fault message is captured and displays the stage in which the fault occurred. You can also manually restart the diagnostic process.

Procedure

- Step 1** On the menu bar, click **Servers**.
- Step 2** Choose a server.
- Step 3** Click the **Tools** icon.
- Step 4** Choose **Start Diagnostics Test**.
- Step 5** Click **Yes**.

The diagnostics process begins.

Step 6 Click the **System Alerts** icon.

Step 7 Choose **Diagnostics Configuration Status**.

The **Configuration Status** page appears. The following information is displayed:

Option	Description
Server System (Management IP)	Displays the server system (as well as the Finite State Machine (FSM) stage, if present).
Server Domain	Displays the configuration status of the selected server domain.
Diagnostic Status	Displays the current diagnostics process of the selected server or domain.

Step 8 Once the process is complete click **Close**.

A pass or fail notice is displayed.

Configuration Status

You can view the FSM status for a server in the domain from the **Configuration Status** window. You can navigate to this window from **Tools > Configuration Status** on the following pages:

- **Server Details**
- **Service Profile Details**
- **Image Library Download Details**
- **Fabric Interconnect Details**
- **Infrastructure Firmware Management Details**
- **FlexFlash Controller**
- **Globalizing Service Profiles**

An FSM is a workflow model, similar to a flow chart, that is composed of the following:

- A finite number of stages
- Transition between those stages
- Operations

The current stage in an FSM is determined by past stages and the operations performed to transition between these stages. The transition between one stage to another is dependent on the success or failure of an operation. The **Configuration Status** window displays the following details for various components:

Launch pages in Cisco UCS Central	Configuration Status Details
------------------------------------------	------------------------------

Server Details	<ul style="list-style-type: none"> • Server System (Management IP) tab <ul style="list-style-type: none"> • System Status • FSM Stages • Server Domain tab <ul style="list-style-type: none"> • Discover Domain Status of the Current FSM • FSM Stages
Service Profile Details	<ul style="list-style-type: none"> • Service Profile System tab <ul style="list-style-type: none"> • Success System Status • FSM Stages • Service Profile Domain tab <ul style="list-style-type: none"> • Configure Domain Status • FSM Stages • Server tab <ul style="list-style-type: none"> • Associate Domain Status • FSM Stages
Image Library Download Details	<ul style="list-style-type: none"> • Download Success/Fail System Status • FSM Stages
Fabric Interconnect Details	<ul style="list-style-type: none"> • Configure Physical Domain Status • FSM Stages
Infrastructure Firmware Management Details	<ul style="list-style-type: none"> • Infrastructure Firmware Deploy Domain Status • FSM Stages

- The **System Status** section displays these details for all components: Status, Progress Status(percent), and FSM Details (button).
- Click **FSM Details** to view these details about the configuration status: Order of Operations, Name, Description, Time Stamp, Retries, and Status for the domain.
- You can favorite the **Configuration Status** window to navigate directly to the configuration status of a component from the Cisco UCS Central dashboard.

FlexFlash Configuration Status

You can view the following configuration status of the FlexFlash SD cards in the **FlexFlash Configuration Status** window:

- **Domain Status**—Shows the **Last Status** and the number of **Retries** for re-pairing the SD cards.
 - **Time Stamp**—Time when pairing completed
 - **Stage Completed**—Sync status completed
 - **Stage Description**—Description of the sync status
 - **Error Code**—Error code in the case of a failed pairing attempt
 - **Error Description**—Description of the error code
- **Domain Stages**—Shows the **Name**, **Time Stamp** of when the SD card re-pair was attempted, and the current status of the MOpsPair.
- **Configuration Stage**—Shows the **Configuration Status**, **Order and Retries**, **Stage Name**, **Time Stamp**, and **Stage Description** of the FlexFlash mirroring in progress.

Chassis Inventory

The **Chassis** page displays the following information related to the chassis associated with the registered Cisco UCS domain:

Chassis	Hardware	Configuration	Status
<p>This column displays the following information for a chassis:</p> <ul style="list-style-type: none"> • The associated domain name and chassis ID • Domain group location • Fabric side 	<p>This column displays the following hardware information for a chassis:</p> <ul style="list-style-type: none"> • Model number of the chassis • Serial number of the chassis • Number of blades 	<p>This column displays the following configuration for a Chassis:</p> <ul style="list-style-type: none"> • Configuration status • Configuration error count 	<p>This column displays the following status for a Chassis:</p> <ul style="list-style-type: none"> • Overall status • Worst fault level • Power status • Thermal status • Decommissioned chassis. <p>You can recommission the chassis by specifying a valid chassis ID.</p>

Chassis Main View

The **Chassis Main View** page allows you to manage and monitor all chassis in a Cisco UCS domain through Cisco UCS Central GUI.

You can view the following information on the selected chassis and its components within a registered Cisco UCS domain:

- **Basic**—Displays the overall status and, overview of all the components within the selected chassis, fault summary, configuration errors and hardware details.
- **IOM Left**—Displays overall status, hardware details and fault summary of the left IOM module.
- **IOM Right**—Displays overall status, hardware details and fault summary details of the right IOM module.
- **Servers**—Displays overall status, hardware, and firmware details of the server associated with this chassis. If you select a server, the page redirects to the server detail view page.
- **Fans**—Displays a list of fans in the chassis. Select a fan to view information related to its module, overall status and hardware details.
- **PSUs**— Displays a list of all the PSUs in the chassis. Select a PSU to view information related to its fault summary, overall status, and other property details.

You can also perform the following tasks:

- Acknowledge and decommission a chassis. You can also launch the chassis statistics tab on Cisco UCS Manager.
- Turn on or turn off the Locator LED for a chassis.
- Verify that that you are in a Single-Server Single SIOC or Single-Server Dual SIOC mode.
- 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.

Launch Cisco UCS Manager Chassis Statistics

You can launch Cisco UCS Manager Chassis statistics from the **Tools** menu in Cisco UCS Central to view these details for a chassis:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.

Name	Description
Modify Collection Policy button	<p>Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter.</p> <p>Note This option is only available if a counter is selected.</p>
Name column	<p>A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart.</p> <p>System statistics for fabric interconnects and FEX are available. These include:</p> <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory <p>Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB.</p> <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager Chassis FAN Statistics

You can launch Cisco UCS Manager Chassis FAN statistics from the **Tools** menu in Cisco UCS Central to view these details for a chassis:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click the + (plus sign) button at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)— Amperes • (babbles) • (bytes)— Number of bytes • (C)—Celsius • (collisions)— Number of times a network collision was encountered • (drops)— Number of times packets were dropped during the transfer • (errors)— Number of errors encountered • (lostCarrier)— Number of times the carrier was lost during transmission • (MB)— Megabytes • (noCarrier)— Number of times no carrier could be found • (packets)— Number of packets transferred • (pause)— Number of pauses encountered during data transmission • (resets)— Number or resets encountered during data transmission • (V)—Volts • (W)— Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>

Name	Description
Min column	The minimum recorded value for the counter. Note For aggregated counters, this is the minimum delta within the reporting interval.
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager PSU Statistics

You can launch Cisco UCS Manager PSU statistics for a chassis from the **Tools** menu in Cisco UCS Central to view these details for a chassis:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.

Name	Description
<p>Name column</p>	<p>A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart.</p> <p>System statistics for fabric interconnects and FEX are available. These include:</p> <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory <p>Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB.</p> <ul style="list-style-type: none"> • ECC errors
<p>Value column</p>	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)

Name	Description
Avg column	The average value for the counter. Note For aggregated counters, this is the average delta within the reporting interval.
Max column	The maximum recorded value for the counter. Note For aggregated counters, this is the maximum delta within the reporting interval.
Min column	The minimum recorded value for the counter. Note For aggregated counters, this is the minimum delta within the reporting interval.
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager Fabric Interconnect IO Module Left Statistics

You can launch Cisco UCS Manager **Fabric Interconnect IOM Left** statistics from the **Tools** menu in Cisco UCS Central to view these details for the IO module:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.

Name	Description
<p>Name column</p>	<p>A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart.</p> <p>System statistics for fabric interconnects and FEX are available. These include:</p> <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory <p>Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB.</p> <ul style="list-style-type: none"> • ECC errors
<p>Value column</p>	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)

Name	Description
Avg column	The average value for the counter. Note For aggregated counters, this is the average delta within the reporting interval.
Max column	The maximum recorded value for the counter. Note For aggregated counters, this is the maximum delta within the reporting interval.
Min column	The minimum recorded value for the counter. Note For aggregated counters, this is the minimum delta within the reporting interval.
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Launch Cisco UCS Manager Fabric Interconnect IO Module Right Statistics

You can launch Cisco UCS Manager **Fabric Interconnect IOM Right** statistics from the **Tools** menu in Cisco UCS Central to view these details for the IO module:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.

Name	Description
<p>Name column</p>	<p>A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart.</p> <p>System statistics for fabric interconnects and FEX are available. These include:</p> <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory <p>Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB.</p> <ul style="list-style-type: none"> • ECC errors
<p>Value column</p>	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)

Name	Description
Avg column	The average value for the counter. Note For aggregated counters, this is the average delta within the reporting interval.
Max column	The maximum recorded value for the counter. Note For aggregated counters, this is the maximum delta within the reporting interval.
Min column	The minimum recorded value for the counter. Note For aggregated counters, this is the minimum delta within the reporting interval.
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Storage Chassis View

The Storage Chassis page allows you to manage and monitor all Cisco UCS S3260 Storage Servers in a Cisco UCS domain.

You can view the following information on the selected chassis and its components:

- **Basic**—Displays the overall status and an overview of all the components within the selected chassis, fault summary, configuration errors and hardware details.
- **System IO Controllers**—Displays overall status and detailed information about the shared adapter.
- **Servers**—Displays overall status, hardware, and firmware details of the server associated with this chassis. If you select a server, the page redirects to the server detail view page.
- **SAS Expanders**—Displays the overall status, configuration, and hardware for each SAS expander associated with this chassis.

- **Storage Enclosures**—Displays the overall status and configuration of the storage enclosures associated with this chassis by enclosure or by slot.
- **Storage**—Displays list of the storage in the selected server. Select a disk to view the current overall status, hardware, and controller details.
- **Fans**—Displays a list of fans in the chassis. Select a fan to view information related to its module, overall status and hardware details.
- **PSUs**—Displays a list of all the PSUs in the chassis. Select a PSU to view information related to its fault summary, overall status, and other property details.

You can also perform the following tasks:

- Acknowledge and decommission a chassis.
- Turn on or turn off the Locator LED for a chassis.
- Modify the discovery policy for the selected 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.
-

FEX

The **All FEX** page displays the following information for each FEX associated with a registered Cisco UCS domains:

FEX	Hardware	Configuration	Status
<p>This column displays the following information for a FEX:</p> <ul style="list-style-type: none"> • The associated domain name and FEX ID • Domain group location • Fabric Side 	<p>This column displays the following hardware information for a FEX:</p> <ul style="list-style-type: none"> • Model number • Serial number • Number of ports available 	<p>This column displays the following configuration for a FEX:</p> <ul style="list-style-type: none"> • Configuration status • Configuration error count 	<p>This column displays the following status for a FEX:</p> <ul style="list-style-type: none"> • Overall status • Worst fault level • Power status • Thermal status • Decommissioned FEX. <p>You can recommission the FEX by specifying a valid FEX ID.</p> <p>You can also remove a decommissioned FEX and delete all data about the FEX from the Delete option in the System Tools submenu.</p>

FEX Main View

You can view the following information related to the FEX and its components within a registered Cisco UCS domain:

- **Basic**—Displays fault summary, overall status and hardware details of the FEX within UCS domain.
- **IOM**—Displays fault summary, overall status, and properties of the IOM.
- **Servers**—Displays number of rack servers connected to the FEX. Select a server to view more information on overall status, firmware and hardware details of the server.
- **Fans**—Displays a list of fans in the FEX. Select a fan to view more information related to the module number, overall status and hardware details.
- **PSUs**— Displays a list of all the PSUs in the FEX. Select a PSU to view details on fault summary, status, properties, and status of power supply units.

You can also perform the following tasks:

- Acknowledge, decommission, and recommission a FEX.
- Turn on or turn off Locator LED for FEXes.
- 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.

Launch Cisco UCS Manager FEX Statistics

You can launch Cisco UCS Manager FEX statistics from the **Tools** menu in Cisco UCS Central to view these details:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the History table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the History table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the General tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. Note This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click + (plus sign) at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: <ul style="list-style-type: none"> • CPU usage • Memory usage, including low kernel memory Note A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB. <ul style="list-style-type: none"> • ECC errors

Name	Description
Value column	<p>For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter.</p> <p>The unit the value is in can be determined by the code appended to the name of the counter:</p> <ul style="list-style-type: none"> • (A)—Amperes • (babbles) • (bytes)—Number of bytes • (°C)—Celsius • (collisions)—Number of times a network collision was encountered • (drops)—Number of times packets were dropped during the transfer • (errors)—Number of errors encountered • (lostCarrier)—Number of times the carrier was lost during transmission • (MB)—Megabytes • (noCarrier)—Number of times no carrier could be found • (packets)—Number of packets transferred • (pause)—Number of pauses encountered during data transmission • (resets)—Number or resets encountered during data transmission • (V)—Volts • (W)—Watts • (blank)
Avg column	<p>The average value for the counter.</p> <p>Note For aggregated counters, this is the average delta within the reporting interval.</p>
Max column	<p>The maximum recorded value for the counter.</p> <p>Note For aggregated counters, this is the maximum delta within the reporting interval.</p>
Min column	<p>The minimum recorded value for the counter.</p> <p>Note For aggregated counters, this is the minimum delta within the reporting interval.</p>

Name	Description
Delta column	The largest change recorded for the counter.

Chart Subtab

If you already created a chart during this session, the **Chart** tab displays that chart. Otherwise, when you navigate to the **Chart** tab, Cisco UCS Manager GUI displays the **Select Statistics** dialog box. This dialog box enables you to select one or two statistics to view as a line graph.

If you right-click the chart, you can access a pop-up menu with additional options. This menu enables you to:

- Change the appearance of the chart by selecting **Properties**
- Change the statistics displayed on the chart by selecting **Configure Chart**
- Print the chart by selecting **Print**

Domains Table View

The **Domains Table View** page displays the following information related to the domains registered with Cisco UCS Central:

Domain	Hardware	Configuration	Status
<p>This column displays the following information for a registered domain:</p> <ul style="list-style-type: none"> • The associated domain name and site • Domain group location • Management IP address • Owner 	<p>This column displays the following hardware information for a registered domain:</p> <ul style="list-style-type: none"> • Fabric interconnect model number and cluster state (HA or Standalone) • Number of chassis and FEX • Number of blade and rack servers • Number of blade servers available for storage 	<p>This column displays the following configuration for a registered domain:</p> <ul style="list-style-type: none"> • Platform family • Firmware version • Firmware status 	<p>This column displays the following status for a registered domain:</p> <ul style="list-style-type: none"> • Overall status • Worst fault level • Trial expiry or status

Domain Group Details

From the **Domain Group** page, you can view information about the entities associated with a domain group. This includes the following:

- **Backup**
- **Settings**

- **Inventory**
- **Domain IDs**
- **Policies**
- **VLANs**
- **VSANs**

If you click the **Settings** icon, you can perform the following tasks:

- Create a system profile or system policy.
- Manage users, authentication, SNMP, and Call Home settings.
- Edit the domain group, and delete any user-created domain group.



Note The domain group root cannot be deleted.

Domains Main View

The **Cisco UCS Domain** page displays the following information related to a selected Cisco UCS domain:

- **Basic**—Displays information related to the overall status, firmware, resources available, fault summary and management details of the selected Cisco UCS domain.

Also, you can suspend and acknowledge a Cisco UCS Central subscription, and re-evaluate the membership of the domain. The **Firmware Upgrade Validation Status** field displays Failure to indicate that upgrade has failed. You must resolve the faults before you use the **Force Deploy** option to continue with the upgrade.

- **FI**—Displays the number of Fabric Interconnects (FI) associated with a domain, overall status, hardware, and firmware details of the FI.

If you want to view more information on the status of the components in the FI, click on an FI from the list.

- **Chassis**—Displays the number of chassis associated with a domain, overall status, hardware, and configuration details of the chassis. For more information on the status of the components in the chassis, click on a chassis from the list.

- **FEX**—Displays the number of FEX associated with a domain, overall status, hardware, and configuration details of the FEX. For more information on the status of the components in the FEX, click on an FEX from the list.

- **Servers**—Displays the number of servers in a domain and the number of available servers. For more information on overall status, hardware, and configuration details of the server, click **Go to Servers Table**.

- **Pin Groups**—Displays the list of all pin groups in a domain and the details of each pin group.

- **FC Zone Profiles**—Displays list of FC Zone Profiles created in the Domain.

- **Diagnostics** — Launch Cisco UCS Central Diagnostic tests.

On the **Cisco UCS Domain** page, you can do the following:

- Launch Cisco UCS Manager GUI for the selected Cisco UCS Domain. Beginning Cisco UCS Central release 2.1, you can sign-on to a Cisco UCS Domain with the same user credentials that you provide for logging on to Cisco UCS Central. However, you will be prompted to specify the new password if the passwords are different. In order to log in as a remote user, you must authenticate the user role in the **Manage UCS Central Authentication** window. After you authenticate the user, you need not provide the credentials again to sign-on to the Cisco UCS Domain. You can also create local user roles and define permissions, authentication servers, locales, and domain groups and sign-on to the Cisco UCS Domain from Cisco UCS Central without specifying the credentials again.



Note Single sign-on is supported on Cisco UCS manager release 4.1(3) and later.

- Activate UCS Central subscription when the overall status of a domain is suspended.
- Re-evaluate membership
- Assign Domain to Domain Group
- Create Pin Group — Create a LAN or SAN Pin Group.
- Create FC Zone Profile
- Domain Configuration Settings
- Suspend UCS Central Subscription (when the overall status of a domain is OK).
- Reapply Configuration

ID Universe

The **ID Universe** displays the collections of identities, or physical or logical resources, that are available in the system. All pools increase the flexibility of service profiles and allow you to centrally manage your system resources. Pools that are defined in Cisco UCS Central are called Global Pools and can be shared between Cisco UCS domains. Global Pools allow centralized ID management across Cisco UCS domains that are registered with Cisco UCS Central. By allocating ID pools from Cisco UCS Central to Cisco UCS Manager, you can track how and where the IDs are used, prevent conflicts, and be notified if a conflict occurs. Pools that are defined locally in Cisco UCS Manager are called Domain Pools.



Note The same ID can exist in different pools, but can be assigned only once. Two blocks in the same pool cannot have the same ID.

You can pool identifying information, such as MAC addresses, to preassign ranges for servers that host specific applications. For example, you can configure all database servers across Cisco UCS domains within the same range of MAC addresses, UUIDs, and WWNs.

From the **ID Universe** page, you can view the total number IDs for each type of pool, and how many of the total are **Available**, **In Use**, or have a **Conflict**. If you click on a **Resource**, you can view detailed information about that ID and where it is used.

All Pools

Display a complete list of ID pools in the system. You can use filter to sort by **Utilization Status**, **Org** or **ID Type** to view availability and usage.

Exporting Inventory Lists

You can export data to CSV, XLS, and PDF formats from table views in Cisco UCS Central.

Procedure

-
- Step 1** In an inventory view, click the **CSV**, **XLS**, or **PDF** icon of your selected export format. This launches the **Opening report** dialog box.
 - Step 2** Click the **Open with** or **Save as** option to complete the export process.
-

Viewing Configuration Status

Procedure

-
- Step 1** Click on a server, chassis, FI, FEX, or firmware package.
 - Step 2** On the detailed view for your selection, click the Notification icon (bell icon representation) and select **Configuration Status**.
The **Configuration Status** page displays.
 - Step 3** Click **Close** to close the window.
-

Inventory Faults

You can view faults from each individual inventory page. Click the **Browse Tables** icon and choose a physical inventory type. Click your selection to open the inventory page, and then click the **Faults** icon to view the following information:

- **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.

Toggling Locator LEDs

You can toggle the locator LEDs on and off for servers, chassis, fabric interconnects, and FEXes.

Procedure

-
- Step 1** From the **All Servers**, **All Chassis**, **All Fabric Interconnects**, or **All FEX** page, click on a server, chassis, FI, or FEX.
 - Step 2** On the detailed view for the selected server, chassis, FI, or FEX, check the status of the Locator LED.
The Locator LED status is located at the top of the **Basic** tab.
 - Step 3** Click the **Operations** icon and select **Toggle Locator LED**.
-

About End-to-End Diagnostics

With Cisco UCS Central, you can initiate end-to-end diagnostics in an integrated fashion with Cisco UCS Manager, in order to troubleshoot hardware issues and conduct burn-in tests on your environments.



Note Cisco UCS Central does not fully support end-to-end diagnostics. For task-based information on conducting end-to-end diagnostics refer to the Cisco UCS Manager documentation. This feature also excludes policies in Cisco UCS Central. Also, Cisco UCS Central does not report instances of bad memory.



Note Initiating the end-to-end diagnostic process causes a system reboot. Also, if the process should stop mid-execution, a fault message is captured and displays the stage in which the fault occurred. You can manually restart the diagnostic process.



Note The connectivity to a Cisco UCS Domain can temporarily show **Lost Connectivity** status. This happens when Cisco UCS Manager gets extremely busy processing the job at hand and may not be able to respond to HeartBeat messages from Cisco UCS Central. The system will recover to normal connectivity after the Cisco UCS Domain completes the job.

Feature	Functions
Remote diagnostic capability	Remotely diagnose your Cisco UCS Manager hardware components and environments.
Trigger the diagnostic process (start/stop) from Cisco UCS Central	Initiate the diagnostic process from within Cisco UCS Central and then let Cisco UCS Manager continue with the full diagnostic process.
Diagnoses multiple servers simultaneously	Cisco UCS Central can identify multiple servers to diagnose.
Dynamically assign diagnostic policy changes to Cisco UCS Manager	Policy changes can be pushed from Cisco UCS Central to Cisco UCS Manager.

Displaying the Results of an End-to-End Diagnostic Test

Before you begin

Initiate the [About End-to-End Diagnostics, on page 36](#) process.

Procedure

	Command or Action	Purpose
Step 1	<code>UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/diag* # show detail server-name</code>	Shows the details of the server diagnostic process.
Step 2	<code>UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/diag* # show result</code>	Displays the server diagnostic results.
Step 3	<code>UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/diag* # scope result result-number</code>	Enters into the results information and assigns a number to the output.
Step 4	<code>UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/diag* # show detail</code>	Displays the server diagnostic results.

Example

The following example shows how to create a end-to-end diagnosis and display the operation's details:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server/diag* # show detail
```

```
Server Diagnostics:
Oper State: Failed
Error Descr: Diagnostic operation Failed
Diag Overall Progress: 100
Current Diag Policy Name: BBB
Scheduled Diag Policy Name:
Current Task:
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server/diag* # show result
```

```
Server Diag Results:
```

```

Id Status Descr Result Progress
-----
1 Completed Test passed Pass 100
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server/diag* # show result 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server/diag/result* # show detail

Server Diag Results:
Id: 1
Status: Completed
Descr: Test passed
Result: Pass
Progress: 100
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server/diag/result* #

```

Dynamic Searches

Cisco UCS Central enables you to save a dynamic search query that includes filters such as name, label, tag, ID, and PID. Unless you delete a query, it is retained when background processes are restarted or when the system is rebooted. Your search results are dynamically updated with current data when you select and execute a saved query.

Saving Dynamic Search Queries

Procedure

-
- Step 1** From the Task bar, select a view such as **Domains**, **Policies**, **Schedules** from the navigation menu.
 - Step 2** In the **Filters** panel, select parameters for your search such as Fault level status or Platform name. When you make selections, a save icon appears at the right of **Filters**.
 - Step 3** Click the save icon and enter a context-sensitive name for the search query you want to create.
 - Step 4** Click **Save this filter**.
The query you created is listed under **Saved Searches** in the **Filters** panel.
-

Executing a Saved Search Query

Procedure

-
- Step 1** In the **Filters** panel under **Saved Searches**, select a query that you previously saved.
 - Step 2** Verify that the filters you selected when you created the query are checked.
The search results are dynamically updated.
-

Deleting a Saved Search Query

Procedure

-
- Step 1** In the **Filters** panel under **Saved Searches**, select a query that you previously saved.
- Step 2** Click the trash can icon at the right of the query name.
The search query immediately disappears.
-



CHAPTER 3

Hardware Compatibility Report

- [Hardware Compatibility Report](#), on page 65
- [Hardware Compatibility Page](#), on page 66
- [Viewing Hardware Compatibility Report Results](#), on page 68
- [Hardware Compatibility Lists](#), on page 70

Hardware Compatibility Report

The Cisco UCS Hardware Compatibility Report allows you to check interoperability information for Cisco UCS components and configurations that have been tested and verified by Cisco, by Cisco partners, or both. You can run reports and check the status against your current software version or a target software version.

The hardware compatibility report checks the compatibility of the operating systems on the servers, and then checks the adapter drivers associated with that operating system.



Note If you run the hardware compatibility report using the Cisco UCS Platform Emulator, the servers can be checked, but not the adapter drivers. Therefore the overall status will always read Can Not Determine or Not Validated.

Running hardware compatibility reports requires the following:

- All servers that you want to run the hardware compatibility report against must be associated with a service profile.
- You must have a Cisco.com account with **Hardware Compatibility Catalog** selected to download or import updated versions of the hardware compatibility list. If you do not already have an account, see the procedure to set up an account in the [Cisco UCS Central Administration Guide](#).



Note Cisco UCS Central ships with a version of the hardware compatibility list, but we recommend that you update to the latest version before running the report.

You will no longer be able to download the Hardware Compatibility Catalog stored in `https://ucshclserver.cloudapps.cisco.com/fetch/current.tar.gz` from Cisco.com. Cisco recommends that you run the following command to download the catalog and then import it into Cisco UCS Central from the UI.

Before you run the command, ensure that you have internet connectivity.

```
curl -k -f --connect-timeout 30 --dump-header "hcl_download_header" -o current.tar.gz
https://ucshclserver.cloudapps.cisco.com/fetch/current.tar.gz -u CCUsername:CCOPassword'
```

Hardware Compatibility Page

The hardware compatibility page displays the existing hardware compatibility reports and catalog downloads. You can have up to 10 reports active at any one time.

From this page, you can:

- View reports or delete reports that are no longer in use on the **Reports** tab.
- View downloads or imports of hardware compatibility lists on the **Downloads** tab.
- Create hardware compatibility reports.
- Schedule periodic synchronization of hardware compatibility lists.
- Synchronize the hardware compatibility list.
- Import a hardware compatibility list.

Create Hardware Compatibility Report

Hardware compatibility reports are stored on the hardware compatibility page.

Procedure

-
- Step 1** Click the **System Tools** icon and choose **Hardware Compatibility**.
 - Step 2** On the Hardware Compatibility page, click the **Tools** icon and choose **Create Hardware Compatibility Report**.
 - Step 3** On the **Hardware Compatibility Report** dialog box, enter a name.
 - Step 4** Choose whether to run the report against the current firmware version of your software or a target firmware version.
 - Step 5** If you chose **Target Version**, select the firmware version for which you want to run the report.
 - Step 6** Choose where you want to run the report. This can be one of the following:
 - **All**—Runs the report on all servers associated with a service profile.

Note

If you have a large number of servers, we recommend that you limit the number of servers by choosing a different option.

- **Domain Group**—Runs the report against all servers in a selected domain group.
- **Domains**—Runs the report against all servers in one or more selected domains.
- **Servers**—Runs the report against one or more selected servers.

Step 7 Click **Create**.

Note

You can only create a maximum of 10 hardware compatibility lists. Creating additional reports causes an error when you click **Create**. You will need to delete one or more existing reports before you can create a new one.

Running the HCL on a Host Firmware Package Policy

You can run the hardware compatibility report in a host firmware package policy that meets the following criteria:

- The host firmware package policy must be assigned to a service profile or service profile template.
- The service profile or service profile template must be associated with a server.

Procedure

- Step 1** Click the **Browse Tables** icon and choose **Policies**.
- Step 2** Choose a host firmware package policy.
- Step 3** On the host firmware package policy page, click the **Edit** icon.
- Step 4** Click **Hardware Compatibility**.
- Step 5** In the hardware compatibility report, check the status of the operating systems and adapter drivers.
For more information, see [Viewing Hardware Compatibility Report Results, on page 68](#).
- Step 6** Click **Save** to save any changes that you have made to the hardware firmware package policy, or click **Edit** to return to edit mode.
-

Running the HCL on a Service Profile or Service Profile Template

You can run the hardware compatibility report in a global service profile or service profile template that is associated with a server.

Procedure

-
- Step 1** Click the **Browse Tables** icon and choose **Templates** or **Profiles**.
- Step 2** Choose a global service profile or service profile template.
- Step 3** On the service profile or service profile template page, click the **Edit** icon.
- Step 4** Click the **Policies** tab.
- Step 5** Click the **Host Firmware Package** policy.
- Step 6** Click the Host Firmware Package drop-down arrow and choose a policy.
- Step 7** Click **Hardware Compatibility**.
- Step 8** In the hardware compatibility report, check the status of the operating systems and adapter drivers.
For more information, see [Viewing Hardware Compatibility Report Results, on page 68](#).
- Step 9**
-

Viewing Hardware Compatibility Report Results

Procedure

-
- Step 1** Click the **System Tools** icon and choose **Hardware Compatibility**.
- Step 2** On the Hardware Compatibility page, in Reports, click the **View Results** icon for the report that you want to view.
- Step 3** On the Report page, check the overall status.
- **Can Not Determine**—Either the operating system or the adapter drivers have not been tagged.
 - **Not Validated**—The operating system and adapter drivers have not been tested and verified by Cisco, by Cisco partners, or both.
 - **Validated**—The operating system and all adapter drivers have been tested and verified.
- Step 4** If an operating system is not tagged, click **Add Tag** and complete the following:
- a) Choose the **Vendor** and **Version** of the operating system.
 - b) Click **Add**.
- Note**
Click **View compatible operating systems** to see a list of validated operating systems.
- Step 5** If an adapter driver is not tagged, click **Add Tag** and complete the following:
- a) Choose the **Vendor**, **Device Type**, and **Version**.
 - b) Click **Add**.
- Note**

Click **View compatible drivers** to see a list of validated adapter drivers.

Step 6 If the operating system or adapter drivers have not been validated, check the [UCS HCL tool](#).

Step 7 Click the **Refresh Report** icon to rerun the report.
The Report page displays.

Hardware Compatibility Report Layout

Field	Description
Report Summary	Lists the number of servers verified by the report. <ul style="list-style-type: none"> • Not Validated—The combination of the server model, firmware versions, OS and adapters is not a tested and validated configuration. • Cannot Determine—There is not enough information to determine if it is a validated configuration. This could be due to the OS or adapters not being tagged. • Validated—Both the OS and the adapters have been tagged and validated.
Overall Report Status	The overall status of the report.
Report Server Firmware Version	The firmware version of the server on which the report was run.
Hardware Compatibility List Version	The hardware compatibility list version on which the report was run.
Report Run On	The servers on which the report was run. <ul style="list-style-type: none"> • All—All servers associated with a service profile. • Domain Group—All servers in a selected domain group. • Domains—All servers in one or more selected domains. • Servers—One or more selected servers.
Report Date	The date and time on which the report was run.
Server	The server name, slot number, domain group, and model number.
Firmware	The current version of the firmware, and the version on which the report was run.

Field	Description
Configuration	The service profile applied to the server.
Operating System	If tagged, the operating system for the selected server.
Add Tag	Click to tag the operating system.
View compatible operating systems	If the operating system is not supported, displays the list of all validated operating systems.
Adapter	The model of the adapter.
Add Tag	Click to tag the adapter driver information.
Show Notes	Any additional information related to the OS or adapter driver.
View compatible drivers	If the adapter driver is not supported, displays the list of all validated drivers.
View supported adapter firmware	If the adapter firmware is not supported, displays the list of validated firmware.

Hardware Compatibility Lists

Hardware compatibility lists are stored in the hardware compatibility lists page under the **Downloads** tab. Cisco UCS Central ships with a version of the hardware compatibility list, but we recommend that you update to the latest version before running the report.

You can obtain updated hardware compatibility lists in one of the following ways:

Type	Description
Automatic synchronization from Cisco.com	After you set up a Cisco.com account, you can: <ul style="list-style-type: none"> • Schedule periodic hardware compatibility list synchronization. • Synchronize the hardware compatibility list on demand.
Manual download and import	If you don't want to use automatic synchronization to download the hardware compatibility lists inside of Cisco UCS Central, you can manually download the lists to an external machine and then import them.

All choices are available from the **Tools** icon on the hardware compatibility page.

Scheduling Periodic Hardware Compatibility List Synchronization

Schedule periodic hardware compatibility list syncs to automatically fetch updated hardware compatibility lists according to the frequency that you set.

Before you begin

You must have a Cisco.com account with **Hardware Compatibility Catalog** selected.

If you do not already have an account, see .

Procedure

-
- Step 1** Click the **System Tools** icon and choose **Hardware Compatibility**.
- Step 2** On the **Hardware Compatibility** page, click the **Tools** icon and choose **Schedule Periodic Hardware Compatibility List Syncs**.
- Step 3** Choose the frequency with which you want to synchronize the hardware compatibility list.
- This can be one of the following:
- **On Demand**—The hardware compatibility list is synced when you click the **Tools** icon and choose **Synchronize Hardware Compatibility List**.
 - **Daily**—The hardware compatibility list is synced once a day.
 - **Weekly**—The hardware compatibility list is synced once a week.
 - **Bi-Weekly**—The hardware compatibility list is synced every two weeks.
- Step 4** Click **Schedule**.
-

Running On Demand Hardware Compatibility List Synchronization

Use on demand hardware compatibility list syncs to fetch updated hardware compatibility lists when you need them.

Before you begin

You must have a Cisco.com account with **Hardware Compatibility Catalog** selected.

If you do not already have an account, see .

Procedure

-
- Step 1** Click the **System Tools** icon and choose **Hardware Compatibility**.
- Step 2** On the **Hardware Compatibility** page, click the **Tools** icon and choose **Synchronize Hardware Compatibility List**.
- The updated hardware compatibility list is downloaded.
-

Manually Downloading and Importing Compatibility Lists

If you do not want to use automatic synchronization you can manually download the hardware compatibility list to a local or remote location.

Before you begin

Download the hardware compatibility list from Cisco.com. The file is stored in the following location:
<https://ucshclserver.cloudapps.cisco.com/fetch/current.tar.gz>.

Procedure

-
- Step 1** Click the **System Tools** icon and choose **Hardware Compatibility**.
 - Step 2** On the **Hardware Compatibility** page, click the **Tools** icon and choose **Import Hardware Compatibility List**.
 - Step 3** Choose **Local** to import a local compatibility list and browse to the file location.
 - Step 4** Choose **Remote** if you want to import a remote file.
 - a) Choose the **Transfer Protocol** that you want to use.
 - b) Enter the **Absolute Remote Path** and the **Remote Server Host Name/IP Address**.
 - c) If you chose FTP, SFTP or SCP, enter the username and password for the remote server.
 - Step 5** Click **Import**.
-



CHAPTER 4

Service Profiles and Templates

- [Service Profile Templates](#), on page 73
- [Service Profiles](#), on page 75

Service Profile Templates

Service profile templates enable you to quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools. There are two types of service profile templates:

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

Creating or Editing a Service Profile Template

Service profile templates created in Cisco UCS Central can be used on any of your registered Cisco UCS domains.



Note When you edit an existing template, you should click **Evaluate** to estimate the impact of the changes, such as requiring a server reboot. Changes made to a service profile template affect all service profiles that are bound to that template.

Procedure

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

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

You can configure an **Asset Tag** to uniquely identify a server. This tag can be 16 characters long. You can specify the asset tag on the **Creating or Editing a Service Profile** dialog box. The asset tag is displayed in the **Servers Details** page as a read only field, and in the **Service Profile Detail** after you reboot.

- a) Enter a **Name** and optional **Description** and **User Label** to help identify the service profile template.
- b) Select the **Template Instantiation Mode** to determine whether service profiles created from this template will be updated when this template is updated.
- c) Set the **Desired Power State on Association** to **Power Off** if you want all servers to be powered down after being associated, otherwise, select **On**.
- d) Select whether to enable **Compatibility Check on Migration Using Server Pool**.

You must select a server pool on the **Servers** tab if you select **Enabled**.

Step 3 Click **Identifiers** to assign identifiers for this service profile.

Click each identifier that you want to use. On the right, click the drop-down to display available pools and choose the one you want to use for this service profile template.

Step 4 In **LAN**, click **Policy** to assign existing policies or click **Advanced** to create new vNICs or iSCSI vNICs for this service profile template.

To create a new vNIC, click on + and specify the vNIC name and select the following properties:

- **Basic**— Select the **Fabric Interconnect**, **Fabric Failover** option (Enabled or disabled), **MTU**, and the **CDN Source** (vNIC Name or User Defined Name for the CDN source).
- **MAC Address**— Select the MAC address from a pool.
- **VLANs**— Specify or search for the VLAN name. 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. You cannot set multiple native VLANs for a vNIC in a Service Profile. When you click on **Set as Native**, a **Configuration Error** results.
- **VLAN Groups**— Specify the VLAN Group name that you have created to group the VLANs.
- **Policies**— Click **SRIOV HPN** to add an existing SRIOV policy.

For more information on creating vNICs, see .

Note

We recommend that you choose existing policies for your LAN settings. Individual settings are not efficient for a scale environment.

Note

You can configure a Native VLAN on each VLAN Group, and also on the vNIC while selecting a specific VLAN. However, only one Native VLAN can be configured in the collective pool of individual VLANs and VLAN Groups selected for a particular vNIC. A configuration error results on the Service Profile upon association if more than one Native VLAN is configured .

Step 5 In **SAN**, click **Policy** to assign existing policies or click **Advanced** to create new vHBAs and assign WWPN pools for this service profile template.

For more information on creating vHBAs, see .

Note

We recommend that you choose existing policies for your SAN settings. Individual settings are not efficient for a scale environment.

Step 6 Click **Servers** to assign an existing server pool or server pool qualification policy.

You can click on the policies, use the drop-down option on the right, and select the server-related policies that you want to assign to this template.

Step 7 Click **Storage** to assign an existing local disk configuration policy or storage profile.

You can click on the policies, use the drop-down option on the right, and select the storage-related policies that you want to assign to this template.

Step 8 Click **Policies** to assign existing policies to the service profile template.

You can click on all service profile related policies, use the drop-down option on the right, and assign policies to this template.

Step 9 Click **Create**.

After you create a Service Profile, you can check the status of the deployment in the **Configuration Status** window from the **Service Profile Details** page.

Service Profile Template Detail View

The Service Profile Template page displays detailed information about a service profile template. From here, you can:

- View audit logs
- Delete, clone, or rename the service profile template
- Create a service profile from this service profile template
- Configure the host interface placement

Service Profiles

Service profiles in Cisco UCS Central define servers and their storage and networking characteristics.



Note You cannot create service profiles directly in Cisco UCS Central. You must create a service profile template first.

Creating a Service Profile from a Template

Procedure

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

Step 2 In **Basic**, select the **Service Profile Template to Instantiate**, and select the **Organization** where you want to create the service profile.

- Step 3** Determine the type of **Service Profile Naming Convention** that you want to use. This can be one of the following:
- **Simple**—Enter the number of service profiles that you want to create, and the naming prefix for each service profile.
The service profiles are created using the format prefixX. For example, three service profiles would be called prefix1, prefix2, and prefix3.
 - **Advanced**—Enter the prefix, suffix, number of service profiles, the first number, and the number of digits.
The service profiles are created using the format prefixXXsuffix. For example, three service profiles starting at 400 and using 4 digits would be called prefix0400suffix, prefix0401suffix, and prefix0402suffix.
 - **Manual Entry**—Enter the service profile names as comma separated values. A service profile will be created for each value entered.

Note

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

- Step 4** In **Servers**, select an existing server pool or server pool qualification policy.

Note

If the service profiles are created from an updating template, then after the service profile instances are created, making changes to the server pool or service pool qualification policy in the template will update the values that you selected here. This may potentially change the associated server to a different server if the server is rebooted.

- Step 5** Click **Create**.
-

Binding a Service Profile to a Template

Procedure

- Step 1** From the **Service Profile** page, click the **Tools** icon and choose **Bind to Template**.
- Step 2** In **Service Profile Template to Instantiate**, choose the service profile template from the available list.
- Step 3** Click **Bind**.
-

Unbinding a Service Profile from a Template

Procedure

- Step 1** From the **Service Profile** page, click the **Tools** icon and choose **Unbind from Template**.

- Step 2** In the Unbind from Template confirmation dialog, click **Yes**.
-

Manually Assigning a Server to a Service Profile

To watch a video manually assigning a server, see [Video: Assigning a Server to a Global Service Profile Manually](#).

Procedure

- Step 1** Click the **Browse Tables** icon and choose **Profiles**.
- Step 2** On the **Profiles** page, choose the service profile that you want to modify.
- Step 3** On the **Service Profile** page, click the **Tools** icon and choose **Assign Server Manually**.
- Step 4** Choose whether to enable **Compatibility Check On Migration Using Manual Assignment**.
- Step 5** Choose the server that you want to assign to the service profile.
- Step 6** Click **Assign**.
-

Configuring Interface Placement on a Service Profile or Service Profile Template

Procedure

- Step 1** Click the **Browse Tables** icon and choose **Profiles** or **Templates**.
- Step 2** Choose the service profile or service profile template that you want to edit.
- Step 3** Click the **Tools** icon and choose **Configure Interface Placement**.
- Step 4** In the **Configure Host Interface Placement** dialog box, in the **Placement** tab, choose whether to enable **Manual Interface Placement**.
- If you choose **Disabled**, the system automatically assigns interfaces based on their PCI order.
- Step 5** If you choose **Enabled**, add vHBAs or vNICs.
- You can associate each vNIC or vHBA with a vCON, and then choose how to assign the Admin Host Port:
- **Any**—Allows Cisco UCS Central to determine the host port to which the vNIC or vHBA is assigned.
 - **1**—Explicitly assigns the vNIC or vHBA to host port 1.
 - **2**—Explicitly assigns the vNIC or vHBA to host port 2.
- Step 6** In **Preference**, choose the **Virtual Slot Selection Preference** for each virtual slot.

Note

This field is only present on service profile templates.

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 7 In **PCI Order**, click the up and down arrows to arrange the order.

Note

If **Manual Interface Placement** is enabled, the PCI order is read-only.

Step 8 Click **Configure**.

Viewing Service Profile Configuration Status

Procedure

Step 1 On the service profile page, click the Notification icon (bell icon representation), and select **Configuration Status**.

The **Configuration Status** page for the selected service profile displays.

Step 2 Click **Close** to close the window.

UUID Synchronization Behavior

For Cisco UCS M3 and greater server models, the UUID that is configured in Cisco UCS Manager is not synchronized with the UUID that is seen by the operating systems running on those servers. UUID synchronization flips the prefix of the UUID in Cisco UCS Manager to match the UUID on the server operating system. By default, the UUIDs are unsynchronized.



Note Changing the UUID synchronization behavior may cause the server to reboot.

The following guidelines apply to UUID synchronization:

- UUID synchronization is supported only for global service profiles.
- UUID synchronization is supported only on the following Cisco UCS Manager releases:
 - Cisco UCS Manager release 2.2(7) and above

- Cisco UCS Manager release 4.1(3) and above
- UUID synchronization is not applicable on Cisco UCS M1 and M2 server models.
- If UUID synchronization is enabled, you must disable UUID synchronization before downgrading or upgrading to a Cisco UCS Manager version that does not support UUID synchronization.
- When changing the service profile to which a server is associated:
 - Cisco UCS M1 and M2 server models are automatically synchronized at association.
 - If synchronization is enabled, Cisco UCS M3 and greater server models are automatically synchronized at association
 - If synchronization is not enabled, Cisco UCS M3 and greater server models are not synchronized at association.

Configuring UUID Synchronization Behavior

Procedure

-
- | | |
|---------------|------------------------------------------------------------------------------------------------------------|
| Step 1 | Click the Browse Tables icon and choose Profiles . |
| Step 2 | Choose the service profile that you want to modify. |
| Step 3 | On the service profile page, click the Tools icon and choose UUID Synchronization Behavior . |
| Step 4 | Choose whether to enable or disable UUID synchronization. |
| Step 5 | Click Save . |
-

Using Static IDs

Cisco UCS Central centralizes ID sourcing with pools. Centralizing IDs makes it simple to move objects between Cisco UCS domains.

Previously, you could only set static IDs by using a script. Now, you can still use a script if you choose to, but the UI provides an easier method. You can now manually create and enter, or copy and paste, static IDs into the UI static ID fields. You can set static IDs for the following addresses:

- MAC
- IP, both IPv4 and IPv6
- IQN
- WWPN
- WWNN
- UUID
- iSCSI Initiator IP

Setting the Management VLAN

When using static IDs for In-Band IPv4 and IPv6 addresses, you must first set the management VLAN.

Procedure

-
- Step 1** Click the **Browse Tables** icon and choose **Profiles**.
 - Step 2** Choose the global service profile for which you want to add static IDs.
 - Step 3** From the **Service Profile** page, click the **Edit** icon.
 - Step 4** Click the **LAN** icon.
 - Step 5** Click **Connectivity** and choose **Management VLAN**.
 - Step 6** Click the Management VLAN drop-down and select a VLAN.
 - Step 7** Click **Save**.
-

Assigning Static IDs

Before you begin

- Unbind the global service profile from the service profile template, if using an updating template.
- If using static IDs for In-Band IPv4 and IPv6 addresses, you must first set the management VLAN.

Procedure

-
- Step 1** Click the **Browse Tables** icon and choose **Profiles**.
 - Step 2** Choose the global service profile for which you want to add static IDs.
 - Step 3** From the **Service Profile** page, click the **Tools** icon and choose **Configure Static IDs**.
 - Step 4** In the various **Identifier** fields, enter the static IDs.

Static ID for WWNN or WWPN must be in the ranges from 20:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF.

Note

You can access the IQN from both the Identifier section and the Interface section. If you set the IQN through the identifier, and then set it through the interface, the last ID overwrites the first, so be careful to only enter the IQN once. Conversely, if you set it in the interface first, setting it again through the identifier overwrites it.

- Step 5** Click **Check Utilization** to check if the ID is available or in use.
Check the utilization every time you enter a static ID.
- Step 6** Click **Clear Static ID** to erase the ID, when necessary.
- Step 7** Click **Interfaces**.
- Step 8** Click on an interface to activate the static ID field.

- Step 9** Enter the static IDs in the various interface fields.
- Step 10** Click **Save**.
Changing the UUID, WWNN, IQN or interface IDs causes the server to reboot.
-

Pool IDs

After setting static IDs, if you decide that you want to return to obtaining IDs from an ID pool, you can do it through editing the global service profile.

Switching Back to Pool IDs

Procedure

- Step 1** Click the **Browse Tables** icon and choose **Profiles**.
- Step 2** Choose the relevant global service profile.
- Step 3** From the **Service Profile** page, click the **Edit** icon.
- Step 4** Click **LAN**, select the appropriate fields, and select the drop-down arrow to select a pool from which to obtain IDs.
- Step 5** Click **SAN**, select the appropriate fields and select the drop-down arrow to select a pool from which to obtain IDs.
- Step 6** Click **Save**.
-

Resetting IDs

Cisco UCS Central updates the following addresses immediately, when you switch them back to the obtaining IDs from a pool.

- In-Band Management IP
- Out-of-Band Management IP
- iSCSI Initiator

The following IDs are not updated immediately. Therefore, you must reset the IDs manually.

- UUID
- IQN
- MAC
- WWNN
- WWPN

Resetting IDs Manually to Resolve IDs to a Global Pool

Procedure

-
- Step 1** Click the **Browse Tables** icon and choose **Profiles**.
- Step 2** Choose the global service profile for which you want to resolve the IDs.
- Step 3** From the **Service Profile** page, click the **Identifiers** icon.
- Step 4** In the assigned ID column, click the **Reset** icon for each identity.
- Step 5** In the Reset ID from pool dialog, click **Reset** to confirm resetting the ID and resolving the statically assigned ID to a pool.
- This step can take up to 10 seconds.
- Step 6** Repeat for all identities that you want to manually reset.
- Step 7** Click the **Connectivity** icon.
- Step 8** In the Interfaces column, select the interface to manually reset.
- Step 9** In the details column, find the assigned ID and click the **Reset** icon.
- Step 10** In the Reset ID from pool dialog, click **Reset** to confirm resetting the IDs.
- Step 11** Repeat for all valid interfaces.
-

Service Profile Views

From the **Service Profiles** page you can view a list of all service profiles in Cisco UCS Central, and filter which service profiles are displayed.

Service Profile Detail View

The Service Profile page displays detailed information about a service profile. You can view the following information on the selected service profile and its components:

- **Basic**—Displays the overall status and an overview of all the components within the selected service profile. You can configure an **Asset Tag** such as a serial number, to uniquely identify a server. This tag can be 32 characters long. You can specify the asset tag on the **Creating or Editing a Service Profile** dialog box. The asset tag is displayed in the **Servers Details** page as a read only field, and in the **Service Profile Detail** after you reboot.



Note Asset tags are configurable directly on a service profile, and only on the associated servers. Consider the following points when you configure the asset tags:

- Because the new asset tag needs to be picked up by the BIOS, configuring the asset tag will require a host reboot. The new tag will not take effect on the host OS until the next reboot.
- Cisco UCS Manager will not automatically reboot the host when the asset tag is changed if the service profile is already associated. You must manually reboot the host (either through Cisco UCS Manager or through the host) in order for the new asset tag to take effect in BIOS.
- On a standalone service profile or on a service profile derived from a template without a pool, you can set the asset tag before the association so that the tag can be applied directly on the BIOS. But if a template has a server pool mentioned, the association process could already complete before you configure the asset tag. In such cases, you have to manually reboot the server to view the asset tag.

-
- **Identifiers**—Displays a list of entities used to identify the service profile.
 - **Connectivity**—Displays a list of connectivity-related information. Shows the list of VLANs and Network Groups associated with the Service Profile under **Interfaces**.
 - **FC Zones**—Displays a list of Fibre Channel zones included in the service profile. To create an FC Zone Profile, see [Creating or Editing an FC Zone Profile, on page 84](#).
 - **Server**—Displays a list of the storage-related policies and profiles included in the service profile.
 - **Storage**—Displays a list of the storage-related policies and profiles included in the service profile.
 - **Policies**—Displays a list of all the policies included in the service profile.

You can also perform the following tasks:

- View logs and configuration status.
- Create a service profile template from this service profile.
- Delete, clone, or rename the service profile.
- Assign or unassign a server.
- Reapply the configuration to the associated server.
- Configure the host interface placement.
- Configure zoning.
- Configure iSCSI targets.
- Configure Static IDs.
- Configure UUID synchronization behavior.
- Bind or unbind from the service profile template.

- Shut down or reset server.

If you want to shutdown the server from a service profile, you can select one of the following **Graceful Shutdown** options to trigger a shutdown and reboot. If you choose **Enabled**, and if there is a maintenance policy assigned to the service profile, Cisco UCS Manager waits for the **Hard Shutdown Timer** value specified in Cisco UCS Central (Maintenance Policy) before it triggers a shutdown and reboot.



Note The **Hard Shutdown Timer** specifies time in seconds (150, 300, or 600) that Cisco UCS Manager waits before it triggers a shutdown and reboot. You can set this timer value in the global maintenance policy in the **Creating a Maintenance Policy** dialog box. If you choose **Enable** and there is no maintenance policy assigned, Cisco UCS Central waits for 150 seconds by default before triggering a shutdown. Otherwise, it will immediately shutdown and reboot. If you choose **Graceful Shutdown Disabled**, Cisco UCS Manager immediately triggers a shutdown and reboot.

- 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.

Creating or Editing an FC Zone Profile

FC Zone profile is a logical representation of all zoning needs for a VM, to represent a single data replication solution between a few storage arrays. An FC Zone Profile contains a collection of all member WWPNs along with their VSAN and FC Zoning enabled. You can create an FC Zone profile and directly deploy it. On Cisco UCS Manager, the **Admin State** appears as **Enabled**.

Before you begin

- FC Zone Active option must be enabled.
- The fabric interconnects on Cisco UCS Manager must have FC switching mode turned on.
- FC Zoning must be enabled on the VSANs. The FC Zone profiles will not deploy if FC Zoning is disabled.
- All FC Zones must have members associated with it and configured. They do not appear as deployed on the fabric interconnect, and their status is shown as inactive if no members are configured.

Procedure

-
- Step 1** In the **Navigation** pane, expand **UCS Domains**.
- Step 2** Click on a **Domain**, and then click the **Tools** icon and select **Create FC Zone Profile**.
- Step 3** In the create **FC Zone Profile** dialog box, enter the **Name** and optional **Description** for the FC Zone Profile.
- Step 4** In the **FC Zone Active** options, click **Enable** to create the zone set. This option is disabled by default.
- Step 5** Click **Save**.
- Step 6** In the **FC Zones** group, do the following:
- Provide a name for the zone set you want to create, and select fabric interconnect **A** or **B** to make the zone set accessible.
 - Add the **VSAN** information for the zone set and ensure that it has FC zoning enabled.
 - Enter the **Member WWPN Address** for the zone set. You can add multiple WWPN addresses for a zone set.
- Step 7** Click **Save** to create the zone profile. You can also edit to delete the zone profile you have created from the **Domain** dashboard.
-

Local Service Profile Detail View

The Local Service Profile page displays detailed information about a local service profile. Local service profiles are managed by Cisco UCS Manager.

You can perform the following tasks on the local service profile page:

- View fault logs.
- Shut down or reset server.
- Launch KVM.
- Launch Cisco UCS Manager Host Firmware Package tab to view the pack items. This option is available under **Policies** when there is an associated Service Profile.
- 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.
-

Templates Table

The **Templates** page allows you to view all templates in Cisco UCS Central. You can filter to view the following types of template:

- Chassis profile template
- Service profile template
- vHBA template
- vNIC template

From this page, you can:

- Add tags to one or more templates.
- Delete one or more templates.
- Click on a selected template to view the details page for that template.

Profiles Table

The **Profiles** page allows you to view all service profiles or all chassis profiles in Cisco UCS Central. Select either **Service Profiles** or **Chassis Profiles** from the top of the page.

From this page, you can:

- Filter which service profiles or chassis profiles are displayed.
- Add tags to one or more service profiles or chassis profiles.
- Delete one or more service profiles or chassis profiles.
- Click on a selected service profile or chassis profile to view the details page for that profile.

UCS Central Faults

Cisco UCS Central collects and displays all the Cisco UCS Central service profile and chassis profile faults on the **Fault Logs** page. To view these faults, click the **Faults** icon in the **Fault Summary** section of a service profile or 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 system faults.

The faults table includes the following information for each fault:

- **Code**—The ID associated with the fault
- **Timestamp**—Date and time at which the fault occurred
- **Type**—Origin of the fault
- **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

To manage the information that is collected, see .

Service Profile Server Faults

Cisco UCS Central collects and displays all the server faults associated with a service profile. To view server faults, click the **Faults** icon in the **Server Fault Summary** section of a **Service 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.

The faults table includes the following information for each fault:

- **Filters**—Filter the data in the table by severity, fault type, and timestamp.
- **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

Service Profile Faults

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

- **Filters**—Filter the data in the table by severity, fault type, and timestamp.
- **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

Service Profile Event Logs

Displays event logs for the selected service profile. This can include the following:

- **ID**—Unique identifier associated with the event that caused the fault
- **Timestamp**—Date and time at which the event occurred
- **Trig. By**—Type of user associated with the event

- **Affected Object**—The component that is affected by the event

Service Profile Audit Logs

Displays the audit logs for the selected service profile. This includes the following:

- Resources that were accessed
- Day and time at which the event occurred
- Unique identifier associated with the log message
- The user who triggered an action to generate the audit log. This can be an internal session or an external user who made a modification using the Cisco UCS Central GUI or the Cisco UCS Central CLI.
- The source that triggered the action
- The component that is affected



CHAPTER 5

Globalization of Local Service Profiles

- [About Globalizing a Local Service Profile, on page 89](#)
- [About Globalizing a VLAN/VSAN, on page 96](#)

About Globalizing a Local Service Profile

You can globalize Local Service Profiles (LSP) from Cisco UCS Manager into Cisco UCS Central so you can deploy and use Cisco UCS Central in a legacy (brownfield) software environment. You can globalize a standalone service profile created from updating a template, or an initial template. This feature is supported from Cisco UCS Manager, release 2.2(8) and higher.

To globalize an LSP, select a domain and then a local service profile to globalize, evaluate, remove blockers, and resolve conflicts. There could be policy conflicts, advance policy conflicts, and identifier conflicts. If there are blockers, resolve the blocking issues, and restart globalization. If there are no blockers, resolve other conflicts if any, and then globalize the LSP. These blockers must be fixed outside of the globalization operation and re-evaluated once complete. For more information about how to globalize an LSP, see [Globalizing Local Service Profiles, on page 93](#).

You can fix policy or advanced policy conflicts by cloning the policy with a new name, by referencing an existing policy from Cisco UCS Central, or by selecting an existing pool from Cisco UCS Central. A global-default is used instead of default policies after globalization, and a default policy is never globalized.



Note You have to first create a new pool outside the globalization operation.

A globalization operation comprises the following stages and potential outcomes:

- Not Evaluated - The globalization request is created and operation is not started.
- Fetching Data from Domain - When the local service profile and other data is retrieved from the domain.
- Evaluating - Evaluating the local service profile and related policies or identifiers against the Cisco UCS Central definition.
- Evaluated with Blocking Issues - One or more blocking issues are found during globalization.
- Evaluated with Conflicts - One or more conflicts are found during evaluation.
- Evaluated with Success - No blocking issues or conflicts found during evaluation.

- Globalizing - When in Evaluated with success status, you can start to globalize the service profile, which may globalize some local policies, and move the local service profile to Cisco UCS Central.
- Globalized With Error - The system experiences an error during the globalization process.
- Globalized with Success- The system succeeds in globalizing the local service profile.

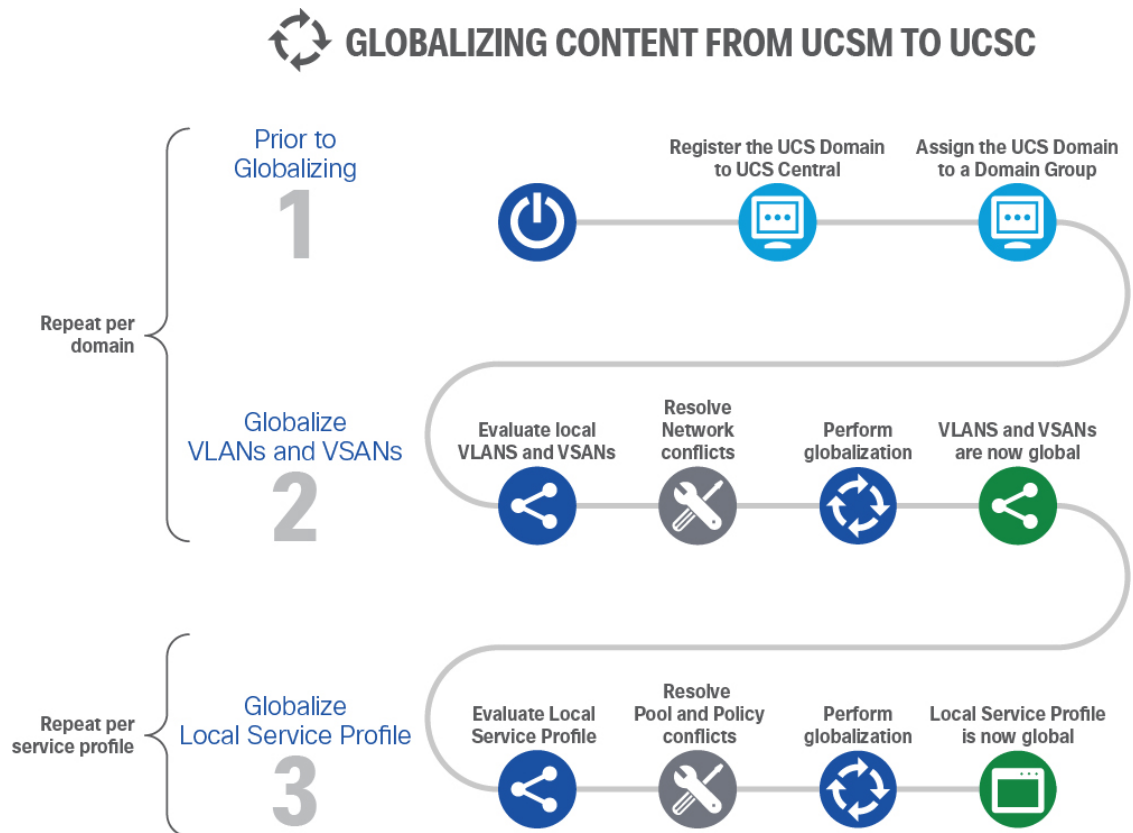


Important

- Cisco recommends that you initiate a globalization operation during a maintenance window in order to avoid any impact on existing configuration settings. You cannot make any configuration changes in Cisco UCS Central and the Cisco UCS domains during a globalization operation.
 - You can globalize only one service profile at a given time.
 - If you have to change any configuration settings in Cisco UCS Central or any Cisco UCS domain, restart the globalization operation after the changes.
 - If an LSP references one or more VLANs or VSANs, globalize the VLANs and VSANs before you globalize the service profile.
 - After globalization, a service profile is not bound to any service profile template in Cisco UCS Central.
 - Org permissions are created automatically for VLANs (except primary VLANs) used by a service profile, if the permissions are not already created.
-

The Globalization workflow is illustrated below:

Figure 1: Globalization Workflow



Globalize Local Service Profiles View

The status of a globalization request is displayed in the **Globalize Local Service Profile** view. When a Local Service Profile (LSP) is evaluated prior to being globalized, this view displays the following details:

- **Globalization Status**—Shows the status of an LSP in the globalization operation. **Status** includes Evaluating, Evaluated with Success, Evaluated with Conflicts, Globalized with Success.
- **Number of Blockers**—Displays the number of issues, or blockers, that cannot be resolved through the globalization process. A description of the issue and a recommendation for resolving the issue are also displayed. A description of the blocker **Issue** and a **Recommendation** to resolve that issue are also displayed in the Globalize Local Service Profile view.

For more information about blocking issues, see [Blocker Issues in Globalization](#).

When there are no blockers, the **Globalize Local Service Profile** view displays the following details about a local service profile being evaluated for globalization.

- **Pools** tab—Displays the server pool or identifier conflicts, and details such as name, pool ID, status of the globalization request. For more information about pool conflicts and how to resolve them, see [Resolving Pool Conflicts, on page 95](#).

- **Policies** tab—Displays the number of simple policy conflicts and details such as same policy name, or an empty policy name, or references to a global policy. For more information about policy conflicts and how to resolve them, see [Resolving Policy Conflicts, on page 95](#).
- **Advanced Policies** tab—Displays the number of advanced policy conflicts. For more information about Advanced Policy Conflicts, and how to resolve a conflict, see [Resolving Policy Conflicts, on page 95](#).

Click the **Pools** tab to view these details about the globalization operation.

- **Name**—Name of the pool associated with the LSP
- **Assigned ID**—The assigned pool ID
- **Pool Type**—The type of pools associated with the LSP (MAC pool, server pools, IPv4 pools)
- **Assigned Pool**—The new pool of the globalized LSP.
- **Status**—Result of the evaluation and if it is successful or not, and a recommendation to resolve a conflict if there is one. Cisco UCS Central also displays details of the conflict and an option to **Change Resolution** or **Edit Resolution**.



Note

- If the globalization request is inactive, the option to **Change** or **Edit Resolution** is not available. You can **Edit Resolution** if the evaluation is successful or **Change Resolution** if evaluation results in a conflict.
 - A service profile cannot be globalized if there is a conflict. Resolve the conflict first and then globalize the service profile.
 - After you resolve a pool or policy conflict, you can choose to **Re-evaluate** or **Start Globalization** from the **Tools** menu.
 - After evaluating an LSP, you cannot change any configuration settings in Cisco UCS Manager before the globalization is complete.
-

Click the **Policies** tab to view these details about the globalization operation.

- **Name**—Name of the policy associated with the LSP.
- **Type**—Type of the policy referenced by the LSP.
- **Assigned Policy**—The new policy used for globalizing an LSP. This policy can be cloned, or referenced from another global policy.
- **Status**—Result of the evaluation and if it is successful or not, and a recommendation to resolve a conflict if there is one. Cisco UCS Central also displays details of the conflict and an option to **Change Resolution** or **Edit Resolution**.
- (Available only in the Advanced Policies tab) **Referenced Pools and Policies**—A table listing the pools and other policies referenced by a policy.

Globalizing Local Service Profiles

You can move or globalize Local Service Profiles (LSP) from Cisco UCS Manager into Cisco UCS Central so you can deploy and use Cisco UCS Central in a legacy (brownfield) software environment. You can globalize a standalone service profile that is bound to a service profile template, or a service profile created from updating a template, or an initial template.

Before you begin

- Your Cisco UCS Manager domain must be registered and exist under a domain group.
- Ensure that the service profiles are associated.
- All VLANs and VSANs referenced by the Service Profile must be global.
- Maintenance Policy must be user acknowledgment enabled.

Procedure

-
- Step 1** In the **Actions** bar, type **Globalize Local Service Profile** and press Enter.
- Step 2** In the **Globalize Local Service Profile** dialog box, in the **Domain** drop-down list, select the Cisco UCS Central domain you want to globalize.
- The following details are displayed:
- **Profile**—Displays the name of the local service profile, the organization it is present in, the status, and the Cisco UCS Domain ID it is present in.
 - **Template**—The name of the template based on which the service template has been created.
 - **Server**—The server associated with the service profile.
 - **Status**—The status of the profile. Also displays whether faults are cleared.
- Step 3** Choose a profile.
- Step 4** Click **Evaluate**. If you want to prioritize a globalization request over another, Delete the request from the **Globalize Local Service Profile** view.

The **Globalize Local Service Profile** view displays. This view shows the status of the globalization and the conflicts if any. For more information, see [Globalize Local Service Profiles View, on page 91](#).

Blocker Issues in Globalization

Issues that cannot be resolved through the globalization operation are considered Blocker issues. You have to resolve them either in the Cisco UCS domain (for example, by unbinding an initial Vnic template) or in Cisco UCS Central (for example, by globalizing the Cisco UCS Domain VLANs). After you resolve the blockers, you must restart the globalization operation by re-evaluating the globalization operation. The following is a list of all blockers you can encounter during the globalization process:

- The Cisco UCS domain is in suspended state. To resolve this issue, acknowledge the Cisco UCS domain to move out of the suspended state before you attempt to globalize again.
- A global service profile (GSP) with the same name exists in the same org. To resolve this issue, rename the local service profile (LSP) in Cisco UCS Manager before you attempt to globalize the service profile.
- The Cisco UCS Manager domain is not under any domain group.
- When a local service profile is not in assigned state.
- A local service profile is not in config-applied state.
- A local service profile is not in associated state.
- A local service profile does not have a Maintenance policy or the Maintenance policy is not User-Acknowledged.
- A local service profile has a pending-reboot request.
- A local service profile references storage profile policy.
- A local service profile has vMedia defined inline. Cisco UCS Central does not support this configuration.
- A local service profile has inline storage profile configured. Cisco UCS Central does not support this configuration.
- A local service profile has inline boot policy configured. Cisco UCS Central does not support this configuration.
- A local service profile resolves to an initial vNIC template. To resolve this issue, unbind the LSP from the initial vNIC template from Cisco UCS Manager.
- A local service profile resolves to an initial vHBA template. To resolve this issue, unbind the LSP from the initial vHBA template from Cisco UCS Manager.
- The local service profile has a vNIC template pairing configured.
- Cisco UCS Central does not support the Storage Connection feature for the specified Cisco UCS Manager domain software version.
- Any ID referenced by a local service profile has already been assigned to another object. To resolve this issue, change the service profile ID, or un-assign the ID from the other object.
- The VLAN/VSAN referenced by a local service profile is not global. To resolve this issue, try to globalize the VLAN/VSAN. If globalization fails, define a new VLAN/VSAN with the same definition in Cisco UCS Manager, and change the service profile to reference the newly created VLAN/VSAN. Globalize the new VLAN/VSAN and then globalize the service profile again.

Globalization Tasks View

The **Globalization Tasks** view displays a list of the globalization tasks in progress. The following details are displayed in this view:

- **Name**—Name of the service profile in the globalization workflow.
- **Globalization Type**—The service profile type.

- **Status**—Evaluation or globalization status of the service profile. Select a service profile from this list to view details about globalization.



Note If you want to cancel a globalization request, you can select request from the table and **Delete**.

Resolving Pool Conflicts

A globalization request evaluates a local service profile (LSP) to determine the impact of globalization. A pool conflict is created when either a local service profile has a local server pool assigned to it, or when the local service profile references a local domain ID pool. In such cases, one server pool/ID pool conflict is created for each ID pool reference, or when the LSP references a local domain ID pool.

To resolve a Pool conflict, click **Change Resolution** from **Status** in the **Globalize Local Service Profile** view and follow these steps:

Procedure

-
- Step 1** Click **Change Resolution** in the **Status** column. The **Resolve Conflict** window opens.
- Step 2** From the **Pool** drop down (for a MAC, UUID, IPv4, or server pool), select one of the following options as required:
- Select and assign a global server pool that contains the same server that is assigned to the LSP.
 - Select and assign a non-qualified global server pool that does not include the server in the pool. This server is automatically added to the global server pool during the globalization process.
 - Reference a global ID pool that contains the ID acquired by the local service profile.
 - Reference a global non-qualified ID pool that does not contain the ID acquired by the LSP. The ID is added to the global ID pool during the globalization process.
- Note**
UUID and IQN pool IDs must have the same prefix as that in the global ID pool. A conflict results if the prefixes are different.
- Step 3** Click **Resolve Conflict**.
- When a local service profile references a global pool, no pool ID conflict is created. If the service profile uses a global pool already, the same pools are used. You can change the pool in all cases except IQN pools.
-

Resolving Policy Conflicts

A globalization request evaluates a local service profile (LSP) to determine if a referenced local policy can be globalized. A policy conflict results in the following scenarios:

- If a policy has the same name as a global policy but with different definitions under the same org.
- If a policy has a potential to affect other global service profiles after globalization.

A policy conflict could be for a Simple or an Advanced policy:

- A simple policy does not contain any reference to a policy or ID pool.
- An Advanced policy contains one or more references to another policy, or ID pool. For example, a vNIC template object may contain references to a MAC pool, QoS policy, Network Control policy, Pin Group policy, Stats Threshold policy, etc. To resolve an advanced policy conflict, resolve the underlying pool and policy conflicts and then resolve the top-level policy conflict.
- IPMI, vMedia, and iSCSI Authentication profile policies require that you enter the password after globalizing the service profile or cloning a policy.
- Any change in the iSCSI Authentication profile triggers Pending Reboots.
- usNIC Connection Policy and Adapter Policy appear in different orgs in the hierarchy.

Procedure

-
- Step 1** Click **Change Resolution** in the **Status** column.
- Step 2** On the **Resolve Conflict** window, select **Clone with new name** or **Reference existing policy**. To reference an existing policy, select the appropriate policy from the Policy drop-down list.
- Step 3** Click **Resolve Conflict**.
- Step 4** To resolve **Advanced Policies** conflict, click on the policy **Type** in the **Advanced Policies** tab. The **Referenced Pools and Policies** table displays the list of policies referenced by the **Advanced Policy**. If there is a conflict in the referenced pool or policies, resolve them before you globalize.

Important

If you want to resolve a local advanced policy (For example, Lan Connectivity Policy) conflict by referencing an advanced global policy (For example, vNIC template) in Cisco UCS Central, you must ensure that the policy name referenced by the local advanced policy matches the policy name referenced by the global policy. You can reference an existing policy while resolving the policy conflict for the local advanced policy (Lan Connectivity Policy here, as stated in example above). While resolving conflicts, Cisco UCS Central makes sure that the original advanced policy and its referenced policies match the definitions of those global policies you choose when you resolve the conflict. If there is any difference between the policy definitions, the advanced local policy still shows conflict.

About Globalizing a VLAN/VSAN

Starting Cisco UCS Central release 2.0, you can move or globalize a VLAN/VSAN created in a Cisco UCS Domain. Globalization of VLAN/VSAN is supported on Cisco UCS Manager, release 2.2(8) and higher. When you initiate a globalization request, an evaluation of the VLANs/VSANs and the Multicast Policy is set off by default. The evaluation operation determines if the VLANs/VSANs and the Multicast policy getting globalized from a specific Cisco UCS domain are in conflict with the existing VLANs/VSANs, and Multicast Policy in Cisco UCS Central.

If there is a conflict on the Multicast policy, the associated VLAN appears in conflict. On the contrary, if there is a conflict on the VLAN, the Multicast policy does not appear in conflict. You can choose to set a desired

domain group at the domain level, or set it per VLAN/VSAN after evaluation. This desired domain group is used to globalize a VLAN/VSAN and Multicast policy if there are no conflicts on any of them.

After evaluation, you can see the list of VLANs/VSANs and the Multicast policy with their globalization status as **Conflict**, or **No Conflict**, or **Not-Evaluated** in the **Globalization of VLANs/VSANs** view. If there is a conflict, an error message with the corresponding conflicting VLAN/VSAN information along with the suggestion to resolve the conflict is displayed in the **Status** column. Select or change the desired domain group for the conflicting VLAN/VSAN in the **Edit Resolution** window. In such cases, the suggested domain name is set to that domain group and **Status** shows **Conflict Resolved**. You can either change a desired domain group and/or re-evaluate again.

During re-evaluation, Cisco UCS Central fetches the Cisco UCS VLANs/VSANs, and any VLANs/VSANs created in the Cisco UCS domain after the first evaluation are also evaluated. If Cisco UCS Central does not find a domain group to globalize a VLAN/VSAN without any impact, the suggested domain name remains empty. After the initial evaluation, you can choose to globalize a VLAN/VSAN from that domain. If you do not want to globalize a particular VLAN/VSAN, you can delete it from the list of VLANs/VSANs before proceeding to globalize others.

Cisco UCS Central does not block the globalization operation if there is a conflict. If you attempt to globalize VLANs/VSANs without resolving a conflict, only those VLANs/VSANs without a conflict will be globalized. For more information about conflicts in globalizing a VLAN/VSAN, see [Conflicts in Globalizing a VLAN/VSAN, on page 98](#).

Globalization of VLANs/VSANs in Cisco UCS Central has the following limitations:

- A globalization operation supports only one domain in a single request.
- A VLAN/VSAN not supported by Cisco UCS Central will not be considered for globalization. For example, Fabric specific VLANs created in Fabric A or Fabric B, common VSANs and default VLANs/VSANs are excluded from globalization operations.
- Only such VLANs/VSANs without conflict, and with an actual or suggested domain group placement are considered for globalization.
- During globalization, you cannot migrate a domain that has an in progress globalization, or any other domain registered with Cisco UCS Central.

Globalization of VLANs/VLANs View

Cisco UCS Central 2.0 lets you globalize VSANs, and VLANs from a domain and place them in a desired domain group location. During the evaluation step, you can view the status of the evaluation in the **Configuration Settings** window. The Globalization of VLANs/VSANs view displays these details: number of **VLAN Conflicts**, **VSAN Conflicts**, **Policy Conflicts**, the **Desired Domain Group**, and **Permitted Org for VLANs**.

The **VLANs** and **VSANS** tabs contain information gathered by the evaluation operation that may help in troubleshooting a particular conflict. The **Policies** tab contains information regarding the policies that are evaluated for globalization impact.

The following details are displayed for each of these tabs:

- **Name**—Name of the VSAN/VLAN associated with the conflict.
- **VnetID**—The Vnet ID associated with the VLAN/VSAN.
- Only in the **Policies** tab, **Type**—The Multicast policy associated with the VLAN/VSAN.

- **Domain Group Placement**—The domain group to which the VLAN/VSAN is assigned.
- **Status**—Status of the VLAN/VSAN. If there is a conflict, a description of the conflict and options to **Change** or **Edit Resolution** are also displayed.

Click **Start Globalization** after all conflicts are resolved.



Note When you select a VLAN Org permit, it is set at the domain level and you cannot modify it later. To reset the Org permit, delete the globalization request and recreate another one.

Conflicts in Globalizing a VLAN/VSAN

A VLAN/VSAN in a Cisco UCS domain cannot be globalized if the evaluation reports a conflict. Before you globalize, resolve the conflicts by completing the suggested actions in the **Status** column in the **Globalizing VLAN/VSAN** view. If there are no suggested actions, the conflicting VLAN cannot be globalized. A VLAN/VSAN conflict occurs in the following cases:

- When any configurable property of a VLAN/VSAN being globalized is different from an existing VLAN/VSAN with the same name in path in the current domain group where the domain is located.
- While globalizing the VLAN/VSAN from a domain makes any other domain re-resolve to this VLAN/VSAN.
- When a VLAN refers to a Multicast policy, Cisco UCS Central also evaluates the policy for conflict. If there is no conflict, the Multicast policy is globalized as well. A Multicast policy conflict occurs in the following cases:
 - When a Multicast policy is different from an existing Multicast policy with same name in path from the current domain group where the domain is located.
 - When any other VLAN in a search from the context of a domain, has the same Multicast policy name reference.
 - If a Multicast policy in Cisco UCS Central is referenced by any VLAN in Cisco UCS Central which is in turn consumed by other domains, then the Multicast policy will be in conflict.
- A global Multicast policy is supported from Cisco UCS Manager 3.1(3) and higher. A Multicast policy is based on the context domain name of a domain. If a Multicast policy is in unresolved conflict state, all VLANs that refer to that Multicast policy will also be in conflict, and will not be globalized.



Note Cisco UCS Central does not support globalization if you try to globalize VLANs or PVLANS from a domain that run versions prior to Cisco UCS Manager 3.1(3). Cisco UCS Central globalizes PVLANS from a domain only if a global PVLAN is supported on that domain. If a primary VLAN in a PVLAN is in unresolved conflict state, all the secondary VLANs will also be in conflict and will not be globalized.

- If a Cisco UCS Manager 3.1(3) domain refers to a Multicast policy, and another domain uses the same name for a Multicat policy locally, that policy cannot be globalized.

Globalizing VSANs and VLANs

Cisco UCS Central lets you globalize VSANs and VLANs from a domain group and place them in a desired group location after they are globalized, and if there are no conflicts encountered. If there is a conflict, Cisco UCS Central automatically places them in a different domain group in the hierarchy to resolve any conflict.



Note Cisco UCS Central can globalize only common VLANs and fabric-specific VSANs.

Before you begin

Your Cisco UCS Manager domain must be registered and exist under a domain group.

Procedure

-
- Step 1** In the **Actions** bar, type **Globalize VLANs and VSANs** and press Enter.
- Step 2** In the **Globalize VLANs and VSANs** window, select the Cisco UCS Central domain you want to globalize.
- Step 3** In the **Desired Domain Group Location** drop-down list, select the domain group in the hierarchy that you want to move the VLANs and VSANs into.
- Cisco UCS Central places the VLANs and VSANs at this location after they are globalized, and if there are no conflicts. To resolve any conflict, Cisco UCS Central automatically places them in the domain group of any of the parent domain groups in the direct hierarchy.
- Step 4** In the **Permitted Org for VLAN** drop-down list, select the appropriate permission for the VLANs.
- Step 5** Click **Evaluate**.
- Step 6** If the evaluation results in no conflicts, the VLAN/VSANs get globalized successfully and the results are displayed in the **Globalization of VLANs/VSANs** view. For more information, see [Globalization of VLANs/VSANs View, on page 97](#).
- All VSAN/VLAN conflicts have to be resolved before beginning globalization.
- Step 7** After the conflicts are resolved, click **Start Globalization**.
-

Resolving VLAN Conflicts

When you find a VLAN in conflict after evaluation in a globalization operation, you must resolve the conflict before proceeding to globalize or re-evaluate. For more information on VLAN conflicts, see [Conflicts in Globalizing a VLAN/VSAN, on page 98](#).

Procedure

-
- Step 1** From **Status** in the **Globalization of VLANs/VSANs** window, click **Change Resolution**.
- Step 2** In the **Resolve Conflict** window, select the **Desired Domain Group Location** from the drop down list.

This domain group location is where the VLAN is placed after conflict resolution. The desired domain name must be either of a domain group or an ancestor in the same org. You can **Edit** your resolution after you re-evaluate. However, you cannot edit a resolution after a VLAN/VSAN is globalized..

Step 3 Click **Resolve Conflict**.

A conflict resolution success or error message appears.

Resolving VSAN Conflicts

When you find a VSAN in conflict after evaluation in a globalization operation, resolve the conflict before proceeding to globalize or reevaluate. For more information on VSAN conflicts, see [Conflicts in Globalizing a VLAN/VSAN, on page 98](#).

Procedure

Step 1 From **Status** in the **Globalization of VLANs/VSANs** window, click **Change Resolution**.

Step 2 In the **Resolve Conflict** window, select the **Desired Domain Group Location** from the drop-down list.

This domain group location is where you want to place the VSAN after conflict resolution. The desired domain name must be either of a domain group or an ancestor in the same org. You can **Edit** your resolution after you reevaluate. However, you cannot edit a resolution after a VLAN/VSAN is globalized.

Step 3 Click **Resolve Conflict**.

A conflict resolution success or error message appears.

Resolving Multicast Policy Conflicts

When you find a Multicast policy in conflict after evaluation in a globalization operation, resolve the conflict before proceeding to globalize or reevaluate. For more information on Multicast policy conflicts, see [Conflicts in Globalizing a VLAN/VSAN, on page 98](#).

Procedure

Step 1 From **Status** in the **Globalization of VLANs/VSANs** window, click **Change Resolution**.

Step 2 In the **Resolve Conflict** window, select the **Desired Domain Group Location** from the drop-down list.

This domain group location is where you want to place the Multicast policy after conflict resolution. The desired domain name must be either of a domain group or an ancestor in the same org. You can **Edit** your resolution after you reevaluate. However, you cannot edit a resolution after a VLAN/VSAN is globalized.

Step 3 Click **Resolve Conflict**.

A conflict resolution success or error message appears.



CHAPTER 6

Server Pools

- [Server Pools](#), on page 103
- [Server Pool Qualification Policy](#), on page 104
- [IP Pools](#), on page 105
- [IQN Pools](#), on page 109
- [UUID Suffix Pools](#), on page 110

Server Pools

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

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

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

When you select a specific server pool, you can view the individual details for that pool, including the number of servers included in the pool, and the associated qualification policies.

Creating or Editing a Server Pool

To watch a video on creating a server pool, see [Video: Creating a Server Pool](#).

After you create the server pool, you can assign it to a service profile template. See [Video: Assigning a Server Pool to a Global Service Profile Template](#).

Procedure

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

- Step 2** In **Basic**, click **Organization** and select the location in which you want to create the server pool.
- Step 3** Enter a **Name** and optional **Description**.
- Step 4** Required: In **Qualification**, click **Add** to add new qualification policies, or **Delete** to remove existing ones.
For more information, see [Creating or Editing a Server Pool Qualification Policy, on page 105](#).
- Step 5** In **Servers**, add the servers to be included in the pool.
- Step 6** Click **Create**.
-

Server Pool Qualification Policy

The server pool qualification policy qualifies servers based on the server inventory conducted during the discovery process. You can configure these qualifications or individual rules in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it. You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model or server type
- Owner
- Site
- Address
- Domain group
- Domain name
- Product family

Creating or Editing a Server Pool Qualification Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Server Pool Qualification Policy** and press Enter.
- Step 2** In the **Server Pool Qualification 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** and **Server Model/PID**.
- Step 4** (Optional) In **Domain**, click the plus sign to add the **Domain Qualifier**.
When you click **Domain Qualifier** the system displays available domain qualification options in tabs on the right pane. Click the appropriate tabs and add the qualification.
- Step 5** In **Hardware**, select the appropriate qualification if you enable the processor, memory, storage, or adapter options.
- Step 6** Click **Create**.
-

IP Pools

IP pools are a collection of IP IPv4 or IPv6 addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

- For external management of Cisco UCS Managerservers.
- For iSCSI boot initiators.
- For both external management and iSCSI boot initiators in Cisco UCS Manager.



Note The IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

A fault is raised if the same IP address is assigned to two different Cisco UCS domains. If you want to use the same IP address, you can use the **scope** property to specify whether the IP addresses in the block are public or private:

- **public**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.
- **private**—You can assign the IP addresses in the block to one and only one registered Cisco UCS domain.

Cisco UCS Central creates public IP pools by default.

Global IP pools should be used for similar geographic locations. If the IP addressing schemes are different, the same IP pool cannot be used for those sites.

Cisco UCS Central supports creating and deleting IPv4 and IPv6 blocks in IP pools. However, iSCSI boot initiators support only IPv4 blocks.

Creating and Editing an IP Pool

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

Procedure

- Step 1** In the Task bar, type **Create IP Pool** and press **Enter**.
This launches the **Create IP Pool** dialog box.
- Step 2** In **Basic**, complete the following:
- From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IP pool.
 - Enter the name and description of the pool.
- Step 3** Click the respective IP blocks to create a block of IP addresses (IPv4 or IPv6) and complete the following:
- Click the **Plus** sign to create one or more blocks of IP addresses in the selected pool.
 - In the respective IP block start column, enter the first IPv4 or IPv6 addresses in the block.
 - In the **Size** column, enter the total number of IP addresses in the pool.
- Step 4** Click the **Apply** icon.
The page displays additional fields.
- Step 5** In **Basic**, complete the following fields:
- Enter the subnet mask associated with the IPv4 or IPv6 address in the block.
 - Enter the default gateway associated with the IPv4 or IPv6 address in the block.
 - Enter the primary DNS server that this block of IPv4 or IPv6 address should access.
 - Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.
 - Select whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following:
 - **Public**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.
 - **Private**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.
- Note**
The scope for an IP address within the block cannot be changed after the block has been saved.
- Step 6** In **IPv4** or **IPv6** addresses, you can view a graphical representation of the number of IP addresses in the pool, the number of assigned IP addresses and the number of duplicated IP addresses.
- Step 7** In **Access Control**, select a policy to associate with this IP address block from the **ID Range Access Control Policy** drop-down list

Step 8 Click **Create**.

Creating and Editing a Management IP Pool

You can create a Management IP Pool and assign it to an Inband policy or use it as KVM Outband Pool from **Domain Configuration Settings** in the **Domains Main View**.

Procedure

Step 1 In the **Actions** bar, type **Create Management IP Pool** and press **Enter**.

Step 2 In the **Create Management IP Pool** dialog box, click **Basic** and choose the **Domain Group** in which you want to create the Management IP pool, and enter the **Name** and optional **Description**.

The name is case sensitive.

Step 3 In **IPv4 Blocks**, select an IPv4 block from the list or click + to enter the IPv4 address and the pool size for the block.

The pool size must range between 1- 1024.

Step 4 In **IPv6 Blocks**, select an IPv6 block from the list or click + to enter the IPv6 address and the pool size for the block. The pool size must range between 1- 1024.

Complete the following details for both the IPv4 and IPv6 blocks:

- a. Enter the subnet mask associated with the IPv4 or IPv6 address in the block.
- b. Enter the default gateway associated with the IPv4 or IPv6 address in the block.
- c. Enter the primary DNS server that this block of IPv4 or IPv6 address should access.
- d. Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.
- e. Select whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following:
 - **Public**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.
 - **Private**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.

Note

1. IPv6 is not supported for Outband KVM.
2. You cannot change the scope for an IP address within the block after you save the block.

Step 5 Click **Create**.

Step 6 After creating a Management IP pool, you can edit it by selecting the **Edit** icon on the summary page of the selected Management IP Pool. Repeat steps 2-4 and then click **Save**.

Step 7 (Optional) You can favorite this screen and pin it to the Cisco UCS Central dashboard to navigate to it directly.

Configuring Management IPs

You can set Management IPs for KVM in the **Configure Management IPs** window. You can navigate to the **Configure Management IPs** window from the **Tools** menu on the **Server Details** page. To assign the management IPs through an Inband policy, see [Creating an Inband Policy](#) . You can set the Management IPs for KVM Outband from **Domains View > Domain Configuration Settings > Management IP > Outband Pool**.

Before you begin

Before you configure management IPs, you must:

- Create a **Management IP Pool** and specify the IPv4 and IPv6 blocks.
- Assign the Inband Policy or Outband Pool to a domain from the **Domain Configurations Settings** window.
- Set the VLAN Group in the Inband Policy assigned to the domain. The VLAN you select for Inband management network for manual assignment must belong to the VLAN Group you set.

Procedure

-
- Step 1** In **Inband Management**, select the VLAN you want to manually assign from the **Inband Management Network** drop-down list. This list displays all VLANs added to the VLAN Group that you assigned in the Inband policy.
 - Step 2** Select the IPv4 pool that you want to manually assign from the **Inband Management IP Pool (IPv4)** drop-down list.
 - Step 3** Select the IPv6 pool that you want to manually assign from the **Inband Management IP Pool (IPv6)** drop-down list.
 - Step 4** Click **Save**.
 - Step 5** From the **Server Details** page, select **Launch KVM Console** from the **Configuration Settings** menu and select the **Physical IPv4 Inband address** and **Physical IPv6 Inband address** for the KVM.
-

- The server inherits the configuration settings after you assign the parameters to complete the configuration. You can verify the management IP details from the **CIMC** configuration settings in the **Server Details** page. However, the manually configured servers supersede the configuration settings deployed through the Inband policy. To make them inherit the configuration settings defined in the Inband policy, you must unassign the parameters of the Inband policy and associate them with the Inband policy. To unassign and reassign policy parameters, see [Creating an Inband Policy](#) .
- The Inband configurations that are part of a service profile do not impact any of the assignments made through the Inband policy or the manual assignment.
- When you deploy a global Inband policy from Cisco UCS Central to Cisco UCS Manager, it supersedes the local Inband profile in Cisco UCS Manager, and does not allow you to edit the VLAN Group, Network, and IP Pool Name fields under the **Inband Profile** in the **LAN** tab. These fields are grayed out. You can edit them only if you Localize them by clicking the **Use Local for InBand Profile** in the Actions area. For more information about localizing a global policy pushed down from Cisco UCS Central, see Cisco UCS Manager documentation.

- You can verify the status of Management IP pools by clicking **Error Details**.
- When you move a domain across domain groups, the Inband configuration settings are retained. You can click **Reapply Configuration** from the **Domain** tab when you move a domain across domain groups.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pools created in Cisco UCS Central can be shared between Cisco UCS domains.

IQN pool members are of the form *prefix:suffix:number*, where you can specify the prefix, suffix, and a block (range) of numbers.

An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but share the same prefix.

Creating and Editing an IQN Pool



Note In most cases, the maximum iSCSI Qualified Name (IQN) size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

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

Procedure

-
- Step 1** In the Actions bar, type **Create IQN Pool** and press **Enter**.
This launches the **Create IQN Pool** dialog box.
 - Step 2** In **Basic**, complete the following:
 - From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IQN pool.
 - Enter name and description of the IQN pool.
 - Enter the prefix for any IQN blocks created for this pool.
 - Step 3** In **Suffix Blocks**, complete the following:
 - Click the **Plus** icon to create one or more blocks of IQN suffixes in the selected pool.
 - In the **Suffix Block** column, enter the suffix for this block of IQNs.
 - In the **Start** column, enter the first IQN suffix in the block.
 - In the **Size** column, enter the total number of IQN suffixes in the block.
 - Step 4** Click the **Apply** icon.
 - Step 5** Click **Create**.
-

What to do next

Include the IQN suffix pool in a service profile or a service profile template.

UUID Suffix Pools

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

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile. Assigning global UUID suffix pools from Cisco UCS Central to service profiles in Cisco UCS Central or Cisco UCS Manager allows them to be shared across Cisco UCS domains.

Creating and Editing a UUID Suffix Pool

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

Procedure

-
- Step 1** In the Actions bar, type **Create UUID Pool** and press **Enter**.
This launches the **Create UUID Pool** dialog box.
- Step 2** In **Basic**, complete the following:
- From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an UUID pool.
 - Enter name and description of the pool.
 - Enter the suffix for any UUID blocks created for this pool.
- Step 3** In **Suffix Blocks**, complete the following:
- Click the **Create** icon.
 - In the **Suffix Block** column, enter the suffix for this block of UUIDs.
 - In the **Start** column, enter the first UUID suffix in the block.
 - In the **Size** column, enter the total number of UUIDs in the block.
 - Click the **Apply** icon.
Additional fields related to UUID pools are displayed.
 - In **UUIDs**, you can view a graphical representation of the number of UUID addresses in the pool, the number of assigned UUID addresses, duplicate UUID addresses, and UUID summary.
 - 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**.

What to do next

Include the UUID suffix pool in a service profile or service profile template.



CHAPTER 7

Server Boot

This chapter includes the following sections:

- [Boot Policy, on page 113](#)
- [Boot Order, on page 114](#)
- [UEFI Boot Mode, on page 115](#)
- [UEFI Secure Boot, on page 116](#)
- [Cautions and Guidelines for Downgrading a Boot Policy, on page 116](#)
- [Creating or Editing a Boot Policy, on page 117](#)

Boot Policy

Boot policy overrides the boot order in the BIOS setup menu, and determines the following:

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

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

You can either create a named boot policy that can be associated with one or more service profiles, or create a boot policy for a specific service profile. A boot policy must be included in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the UCS domain applies the default boot policy.



Note Changes to a boot policy will be propagated to all service profiles created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is automatically triggered.

Boot Order

Cisco UCS Central enables you to use standard or enhanced boot order for the global boot policies you create in Cisco UCS Central.

- Standard boot order is supported for all Cisco UCS servers, and allows a limited selection of boot order choices. You can add a local device, such as a local disk, CD-ROM, or floppy, or you can add SAN, LAN, or iSCSI boot.
- Enhanced boot order allows you greater control over the boot devices that you select for your boot policy. Enhanced boot order is supported for all Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers at release 2.2(1b) or greater.

The following boot order devices are supported for standard boot order, but can be used with both:

- **Local LUN/Local Disk**—Enables standard boot from a local hard disk. Do not enter a primary or secondary LUN name. Those are reserved for enhanced boot order only.
- **CD/DVD ROM Boot**—Enables standard boot from local CD/DVD ROM drive.
- **Floppy**—Enables standard boot from local floppy drive.
- **LAN Boot**—Enables standard boot from a specified vNIC.
- **SAN Boot**—Enables standard boot from a specified vHBA.
- **iSCSI Boot**—Enables standard boot from a specified iSCSI vNIC.

The following boot order devices are supported only for enhanced boot order:

- **Local LUN/Local Disk**—Enables boot from local hard disk, or local LUN.
- **Local CD/DVD**—Enables boot from local CD/DVD drive.
- **Local Floppy**—Enables boot from local floppy drive.
- **SD Card**—Enables boot from SD Card.
- **Internal USB**—Enables boot from Internal USB.
- **External USB**—Enables boot from External USB.
- **Embedded Local Disk**—Enables booting from the embedded local disk on the Cisco UCS C240 M4SX and C240 M4L servers.



Note You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.

- **Embedded Local LUN**—Enables boot from the embedded local LUN on the Cisco UCS C240 M4SX and C240 M4L servers.



Note You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.

- **Local JBOD**—Enables boot from a local disk.
- **KVM Mapped CD/DVD**—Enables boot from KVM mapped ISO images.
- **KVM Mapped Floppy**—Enables boot from KVM mapped image files.
- **CIMC Mapped HDD**—Enables boot from CIMC mapped vMedia drives.
- **CIMC MAPPED CD/DVD**—Enables boot from CIMC mapped vMedia CDs and DVDs.
- **LAN Boot**—Enables you to select a specific vNIC from which to boot.
- **SAN Boot**—Enables you to select a specific vHBA from which to boot.
- **iSCSI Boot**—Enables you to select a specific iSCSI vNIC from which to boot.
- **Remote Virtual Drive**—Enables boot from a remote virtual drive.



-
- Note**
- If a boot policy with enhanced boot order is applied to Cisco UCS M1 and M2 blade and rack servers, or to Cisco UCS M3 blade and rack servers with a release prior to Release 2.2(1b) installed, the association fails with configuration errors.
 - You must enable USB for Virtual Media. If you modify the BIOS settings, that in turn affects the Virtual media. The following USB BIOS default settings are recommended for best performance:
 - **Make Device Non Bootable**—set to disabled
 - **USB Idle Power Optimizing Setting**—set to high-performance
-

UEFI Boot Mode

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

You can choose either legacy or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported on Cisco UCS B-Series , Cisco UCS C-Series Rack Servers, and Cisco UCS X-Series and allows you to enable UEFI secure boot mode.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is not supported on Cisco UCS B-Series M1 and M2 Blade Servers and Cisco UCS C-Series M1 and M2 Rack Servers.
- UEFI boot mode is not supported with the following combinations:

- Gen-3 Emulex & QLogic adapters on Cisco UCS blade & rack servers integrated with Cisco UCS domain.
- PXE boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS domain.
- iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS domain.
- You cannot mix UEFI and legacy boot mode on the same server.
- Make sure an UEFI-aware operating system is installed in the device. The server will boot correctly in UEFI mode only if the boot devices configured in the boot policy have UEFI-aware OS installed. If a compatible OS is not present, the boot device is not displayed on the **Boot Policies** page.
- In some corner cases, the UEFI boot may not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation could occur in the following situations:
 - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is manually powered on using the **Server** page or the front panel.
 - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.
 - If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

UEFI Secure Boot

Cisco UCS Central supports UEFI secure boot on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and Rack Servers. When UEFI secure boot is enabled, all executables, such as boot loaders and adapter drivers, are authenticated by the BIOS before they can be loaded. To be authenticated, the images must be signed by either the Cisco Certificate Authority (CA) or a Microsoft CA.

The following limitations apply to UEFI secure boot:

- UEFI boot mode must be enabled in the boot policy.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.
- User-generated encryption keys are not supported.
- UEFI secure boot can only be controlled by Cisco UCS Manager or Cisco UCS Central.
- If you want to downgrade to an earlier version of Cisco UCS Manager, and you have a blade server in secure boot mode, you must disassociate and reassociate the blade server before downgrading. Otherwise, the blade will not be discovered successfully.

Cautions and Guidelines for Downgrading a Boot Policy

You cannot downgrade to an earlier version of Cisco UCS Manager if:

- An associated server has a boot policy with UEFI boot mode enabled.

- An associated server has a boot policy with UEFI secure boot enabled.
- An associated server has a boot policy with enhanced boot order. For example, if an associated server has a boot policy which contains any of the following:
 - SD card
 - Internal USB
 - External USB
- An associated server has a boot policy that includes both SAN and local LUN.

Creating or Editing a Boot Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Boot Policy** and press Enter.
- Step 2** Choose the organization from the drop-down list, and then enter a unique name and optional description for the policy.
- Step 3** Required: Click **Enabled** for **Reboot on Boot Order Change** to reboot all servers that use this boot policy after you make changes to the boot order.
- For boot policies applied to a server with a non-Cisco VIC adapter, even if Reboot on Boot Order Change is disabled, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.
- Step 4** Required: Click **Enabled** for **Enforce Interface Name** to receive a configuration error if any of the vNICs, vHBAs or iSCSI vNICs in the Boot Order section match the server configuration in the service profile.
- Step 5** In **Boot Mode**, click **Legacy** or **Unified Extensible Firmware Interface (UEFI)**.
- Step 6** If you selected **Unified Extensible Firmware Interface (UEFI)**, choose if you want to enable UEFI secure boot.
- Step 7** Click **Boot Order** and perform the following:
- a) Click the **Add** button to add boot options.
For information on each option, see [Boot Order, on page 114](#).
 - b) Update the required properties for the boot option.
 - c) Use the up and down arrows to arrange the boot order.
- Note**
If you create a boot policy for iSCSI boot in the HTML5 GUI, you can only update that boot policy in the HTML5 GUI.
- Step 8** Click **Save**.
-

Configuring iSCSI Targets



Note This dialog box is read-only unless you configured the iSCSI targets directly under the service profile or service profile template using the Cisco UCS Central CLI or the Flash-based GUI.

Procedure

-
- Step 1** Click **Primary** or **Secondary** and enter the iSCSI vNIC.
- Step 2** Select the **iSCSI Target Definition Mode** and complete the necessary fields:
- **Static**—Specify a static target interface for the iSCSI vNIC.
 - **Auto**—Allow the system to select an interface automatically using DHCP.
 - **Decide Later**—Allows the system to ignore the iSCSI boot until you configure the iSCSI targets. You can also use this to delete a target you no longer want to use.
- Step 3** Click **Save** .
-



CHAPTER 8

Server Policies

- [Server Policies](#), on page 119
- [BIOS Policy](#), on page 119
- [IPMI Access Profile](#), on page 158
- [Serial over LAN Policy](#), on page 158
- [Hardware Change Discovery Policy](#), on page 159
- [Host Firmware Package Policy](#), on page 160
- [iSCSI Adapter Policy](#), on page 163
- [iSCSI Authentication Profile](#), on page 163
- [Local Disk Policy](#), on page 164
- [Port Auto-Discovery Policy](#), on page 165
- [Graphics Card Policy](#), on page 165
- [Statistics Threshold Policy](#), on page 166
- [Scrub Policy](#), on page 168
- [vMedia Policy](#), on page 169

Server Policies

Server policies allow you to apply changes globally to your Cisco UCS servers.



Note You must include policies in a service profile and associate them with a server before Cisco UCS Central can apply them.

BIOS Policy

The BIOS policy automates the configuration of BIOS settings for a server or group of servers. You can create global BIOS policies available to all servers in the root organization, or you can create BIOS policies in sub-organizations that are only available to that hierarchy.

To use a BIOS policy:

1. Create the BIOS policy in Cisco UCS Central.

2. Assign the BIOS policy to one or more service profiles.
3. Associate the service profile with a server.

During service profile association, Cisco UCS Central modifies the BIOS settings on the server to match the configuration in the BIOS policy. If you do not create and assign a BIOS policy to a service profile, the server uses the default BIOS settings for that server platform.

Creating or Editing a BIOS Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create BIOS Policy** and press Enter.
- Step 2** In the **BIOS Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
- a) Enter a **Name** and optional **Description**.
The policy name is case sensitive.
 - b) (Optional) Complete the other fields as necessary.
For more information, see [Basic BIOS Settings, on page 121](#).
- Step 3** In **Processor**, complete the fields as necessary.
For more information, see [Processor BIOS Settings, on page 124](#).
- Step 4** In **I/O**, complete the fields as necessary.
For more information, see [I/O BIOS Settings, on page 137](#).
- Step 5** In **RAS Memory**, complete the fields as necessary.
For more information, see [RAS Memory BIOS Settings, on page 138](#).
- Step 6** In **USB**, complete the fields as necessary.
For more information, see [USB BIOS Settings, on page 140](#).
- Step 7** In **PCI**, complete the fields as necessary.
For more information, see [#unique_158](#).
- Step 8** In **Graphics Configuration**, complete the fields as necessary.
For more information, see [Graphics Configuration BIOS Settings, on page 150](#).
- Step 9** In **Boot Options**, complete the fields as necessary.
For more information, see [Boot Options BIOS Settings, on page 151](#).
- Step 10** In **Server Manager**, complete the fields as necessary.
For more information, see [Server Manager BIOS Settings, on page 152](#).
- Step 11** In **Console**, complete the fields as necessary.

For more information, see [Console BIOS Settings, on page 154](#).

Step 12 Click **Create**.

Default BIOS Settings

Cisco UCS Central includes a set of default BIOS settings for each type of server supported by Cisco UCS. The default BIOS settings are available only in the root organization and are global. Only one set of default BIOS settings can exist for each server platform supported by Cisco UCS. You can modify the default BIOS settings, but you cannot create an additional set of default BIOS settings.

Each set of default BIOS settings are designed for a particular type of supported server and are applied to all servers of that specific type which do not have a BIOS policy included in their service profiles.

Unless a Cisco UCS implementation has specific needs that are not met by the server-specific settings, we recommend that you use the default BIOS settings that are designed for each type of server in the Cisco UCS domain.

Cisco UCS Central applies these server platform-specific BIOS settings as follows:

- The service profile associated with a server does not include a BIOS policy.
- The BIOS policy is configured with the platform-default option for a specific setting.

You can modify the default BIOS settings provided by Cisco UCS Central. However, any changes to the default BIOS settings apply to all servers of that particular type or platform. If you want to modify the BIOS settings for only certain servers, we recommend that you use a BIOS policy.

Basic BIOS Settings

The following table lists the main server BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Organization	Select an organization.
Name	Enter a name between 1 and 16 alphanumeric characters.
Description	Enter up to 256 characters. you can use any characters or spaces except ' (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

Name	Description
Reboot on BIOS Settings Change	<p>When the server is rebooted after you change one or more BIOS settings.</p> <p>—If you enable this setting, the server is rebooted according to the maintenance policy in the server's service profile. For example, if the maintenance policy requires user acknowledgment, the server is not rebooted and the BIOS changes are not applied until a user acknowledges the pending activity.</p> <p>—If you do not enable this setting, the BIOS changes are not applied until the next time the server is rebooted, whether as a result of another server configuration change or a manual reboot.</p>
Serial Port A	<p>Whether serial port A is enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The serial port is disabled. • —The serial port is enabled.
Quiet Boot	<p>What the BIOS displays during Power On Self-Test (POST). This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS displays all messages and Option ROM information during boot. • —The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.
Post Error Pause	<p>What happens when the server encounters a critical error during POST. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS continues to attempt to boot the server. • —The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.

Name	Description
Front Panel Lockout	<p>Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The power and reset buttons on the front panel are active and can be used to affect the server. • —The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.
Consistent Device Naming (CDN)	<p>Whether Consistent Device Naming (CDN) is enabled. CDN allows Ethernet interfaces to be named in a consistent manner, making Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made.</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —CDN is disabled for this BIOS policy. • —CDN is enabled for this BIOS policy.
Resume AC On Power Loss	<p>How the server behaves when power is restored after an unexpected power loss. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server is powered on and the system attempts to restore its last state. • —The server is powered on and automatically reset. • —The server remains off until manually powered on.
QuickPath Interconnect (QPI) Link Frequency	<p>The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s). This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • 6400 • 7200 • 8000 • 9600 • —The CPU determines the QPI link frequency.

Name	Description
QuickPath Interconnect (QPI) Snoop Mode	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • —This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads. • —The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized.
Trusted Platform Module (TPM)	<p>Whether TPM is used to securely store artifacts that are used to authenticate the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —TPM is used for authentication. • —TPM is not used for authentication.
Intel Trusted Execution Technology (TXT)	<p>Whether TXT is used for data protection. TXT can be enabled only after TPM, Intel Virtualization technology (VT) and Intel Virtualization Technology for Directed I/O (VTDio) are enabled. If you only enable TXT, it implicitly enables TPM, VT, and VTDio also. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —TXT is used for extra security. • —TXT is not used for extra security.

Processor BIOS Settings

The following tables list the processor BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Table 2: Basic Tab

Name	Description
Execute Disabled Bit	<p>Classifies memory areas on the server to specify where the application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not classify memory areas. • —The processor classifies memory areas. <p>We recommend that you contact your operating system vendor to make sure your operating system supports this feature.</p>
Direct Cache Access	<p>Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Data from I/O devices is not placed directly into the processor cache. • —Data from I/O devices is placed directly into the processor cache.
Local X2 Application Policy Infrastructure Controller (APIC)	<p>Allows you to set the type of Application Policy Infrastructure Controller (APIC) architecture. This can be one of the following:</p> <ul style="list-style-type: none"> • xAPIC—Uses the standard xAPIC architecture. • x2APIC—Uses the enhanced x2APIC architecture to support 32 bit addressability of processors. • —Automatically uses the xAPIC architecture that is detected. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Frequency Floor Override	<p>Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:</p> <ul style="list-style-type: none"> • —The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • — The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
P-STATE Coordination	<p>Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.</p> <ul style="list-style-type: none"> • HW_ALL—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • SW_ALL—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • SW_ANY—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note must be set to Custom or the server ignores the setting for this parameter.</p>

Name	Description
DRAM Clock Throttling	<p>Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Balanced— DRAM clock throttling is reduced, providing a balance between performance and power. • Performance—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • —DRAM clock throttling is increased to improve energy efficiency. • —The CPU determines the level.
Channel Interleaving	<p>Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following:</p> <ul style="list-style-type: none"> • —The CPU determines what interleaving is done. • 1 Way—Some channel interleaving is used. • 2 Way • 3 Way • 4 Way—The maximum amount of channel interleaving is used. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Rank Interleaving	<p>Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • —The CPU determines what interleaving is done. • 1 Way—Some rank interleaving is used. • 2 Way • 4 Way • 8 Way—The maximum amount of rank interleaving is used. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Altitude	<p>The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:</p> <ul style="list-style-type: none"> • —The CPU determines the physical elevation. • —The server is approximately 300 meters above sea level. • —The server is approximately 900 meters above sea level. • —The server is approximately 1500 meters above sea level. • —The server is approximately 3000 meters above sea level. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
CPU Hardware Power Management	<p>Manages the CPU power functions.</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not classify memory areas. • —The processor classifies memory areas.
Energy Performance Tuning	<p>This item selects whether the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS.</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not use energy performance management. • —The processor uses energy performance management.
Workload Configuration	<p>The BIOS uses values that are default for the server type and vendor. Balanced is selected for workload optimization. This is the recommended setting.</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The workload configuration optimizations are disabled. • —The workload configuration optimizations are enabled.

Table 3: Prefetchers Tab

Name	Description
Hardware Prefetcher	<p>Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The hardware prefetcher is not used. • —The processor uses the hardware prefetcher when cache issues are detected. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note must be set to Custom in order to specify this value. For any value other than Custom, this option is overridden by the setting in the selected CPU performance profile.</p>
Adjacent Cache Line Prefetcher	<p>Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following:</p> <ul style="list-style-type: none"> • —The processor only fetches the required line. • —The processor fetches both the required line and its paired line. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note must be set to Custom in order to specify this value. For any value other than Custom, this option is overridden by the setting in the selected CPU performance profile.</p>
Data Cache Unit (DCU) Streamer Prefetcher	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none"> • —The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • —The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Data Cache Unit (DCU) IP Prefetcher	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none"> • —The processor does not preload any cache data. • —The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Table 4: Technology Tab

Name	Description
Turbo Boost	<p>Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not increase its frequency automatically. • —The processor uses Turbo Boost Technology if required.
Enhanced Intel Speed Step	<p>Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor never dynamically adjusts its voltage or frequency. • —The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. <p>We recommend that you contact your operating system vendor to make sure your operating system supports this feature.</p>

Name	Description
Hyper Threading	<p>Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not permit hyperthreading. • —The processor allows for the parallel execution of multiple threads. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Core Multi-Processing	<p>Sets the state of logical processor cores per CPU in a package. If you disable this setting, Intel Hyper Threading technology is also disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • All—Enables multiprocessing on all logical processor cores. • 1 through <i>n</i>—Specifies the number of logical processor cores per CPU that can run on the server. To disable multiprocessing and have only one logical processor core per CPU running on the server, choose 1. <p>We recommend that you contact your operating system vendor to make sure your operating system supports this feature.</p>
Virtualization Technology (VT)	<p>Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not permit virtualization. • —The processor allows multiple operating systems in independent partitions. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>

Table 5: Power Tab

Name	Description
Power Management	<p>Enables you to configure the CPU power management settings for the following options:</p> <ul style="list-style-type: none"> • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 <p>Power Technology can be one of the following:</p> <ul style="list-style-type: none"> • —The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • —The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters. • —The server automatically optimizes the performance for the BIOS parameters mentioned above. • —The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Energy Performance	<p>Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following:</p> <ul style="list-style-type: none"> • • • • • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note must be set to Custom or the server ignores the setting for this parameter.</p>

Name	Description
Processor C State	<p>Whether the system can enter a power savings mode during idle periods. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The system remains in a high-performance state even when idle. • —The system can reduce power to system components such as the DIMMs and CPUs. <p>We recommend that you contact your operating system vendor to make sure your operating system supports this feature.</p>
Processor C1E	<p>Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU continues to run at its maximum frequency in the C1 state. • —The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state.
CPU Performance	<p>Sets the CPU performance profile for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —For M3 servers, all prefetchers and data reuse are enabled. For M1 and M2 servers, data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • —Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • —All prefetchers are enabled and data reuse is disabled. This setting is also known as high-performance computing. • Custom

Name	Description
Package C State Limit	<p>The amount of power available to the server components when they are idle. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU determines the available power. • —The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • —When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • —When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • —When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves more power than C7, but it also requires the longest time for the server to return to high performance mode. • —The server may enter any available C state.

Table 6: Errors and Reporting Tab

Name	Description
Processor C3 Report	<p>Whether the processor sends the C3 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not send the C3 report. • —The processor sends the C3 report. • —The processor sends the C3 report using the advanced configuration and power interface (ACPI) C2 format. • —The processor sends the C3 report using the ACPI C3 format. <p>On the Cisco UCS B440 Server, the BIOS Setup menu uses enabled and disabled for these options. If you specify <code>acpi-c2</code> or <code>acpi-c3</code>, the server sets the BIOS value for that option to enabled.</p>
Processor C6 Report	<p>Whether the processor sends the C6 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not send the C6 report. • —The processor sends the C6 report.
Processor C7 Report	<p>Whether the processor sends the C7 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not send the C7 report. • —The processor sends the C7 report. • —The processor sends the C7 report. • —The processor sends the C7s report. <p>Note The selections vary depending on the server and operating system.</p>

Name	Description
Processor CMCI	<p>The BIOS uses values that are default for the server type and vendor.</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • — Corrected Machine Check Interrupt is not generated. • — Corrected Machine Check Interrupt is generated.
Max Variable MTRR Setting	<p>Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —BIOS uses the default value for the processor. • 8—BIOS uses the number specified for the variable MTRR.
Demand Scrub	<p>Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • — Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. • — Single bit memory errors are not corrected.
Patrol Scrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Enabled—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running. • —The system checks for memory ECC errors only when the CPU reads or writes a memory address.

Name	Description
CPU Hardware Power Management	<p>Enables processor Hardware Power Management (HWPM). This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —HWPM is disabled. • —HWPM native mode is enabled. • —HWPM Out-Of-Box mode is enabled.

I/O BIOS Settings

The following table lists the I/O BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Virtualization Technology (VT) for Directed IO	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). You can select one of the following options:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor uses virtualization technology. • —The processor does not use virtualization technology. <p>Note This option must be set to enabled if you want to change any of the other Intel Directed I/O BIOS settings.</p>
Interrupt Re-map	<p>Whether the processor supports Intel VT-d Interrupt Remapping. You can select one of the following options:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor uses VT-d Interrupt Remapping as required. • —The processor does not support remapping.
Coherency Support	<p>Whether the processor supports Intel VT-d Coherency. You can select one of the following options:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor uses VT-d Coherency as required. • —The processor does not support coherency.

Name	Description
Address Translation Services (ATS) Support	<p>Whether the processor supports Intel VT-d Address Translation Services (ATS). You can select one of the following options:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor uses VT-d ATS as required. • —The processor does not support ATS.
Pass Through DMA Support	<p>Whether the processor supports Intel VT-d Pass-through DMA. You can select one of the following options:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor uses VT-d Pass-through DMA as required. • —The processor does not support pass-through DMA.

RAS Memory BIOS Settings

The following table lists the RAS memory BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
NUMA	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • —The BIOS does not support NUMA.

Name	Description
LV DDR Mode	<p>Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • —The system prioritizes high frequency operations over low voltage operations. • —The CPU determines the priority.
DRAM Refresh Rate	<p>The refresh interval rate for internal memory. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • 1x • 2x • 3x • 4x •
Memory RAS Configuration Mode	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —System performance is optimized. • —System reliability is optimized by using half the system memory as backup. • —If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers. • —Enables sparing mode.

Name	Description
Sparing Mode	<p>Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population.</p> <p>This option is only available if you choose the sparing option for the Memory RAS Config parameter. It can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • —A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank.
DDR3 Voltage Selection	<p>The voltage to be used by the dual-voltage RAM. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • •

USB BIOS Settings

The following tables list the USB BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Basic Tab

Name	Description
Make Device Non Bootable	<p>Whether the server can boot from a USB device. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server can boot from a USB device. • —The server cannot boot from a USB device.

Name	Description
USB Front Panel Access Lock	<p>USB front panel lock is configured to enable or disable the front panel access to USB ports. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • •
Legacy USB Support	<p>Whether the system supports legacy USB devices. This can be one of the following:</p> <ul style="list-style-type: none"> • —Disables legacy USB support if no USB devices are connected. • —USB devices are only available to EFI applications. • —Legacy USB support is always available. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Idle Power Optimizing Setting	<p>Whether the USB System Idle Power Optimizing setting is used to reduce USB EHCI idle power consumption. Depending upon the value you choose, this setting can have an impact on performance. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The USB System Idle Power Optimizing setting is disabled, because optimal performance is preferred over power savings. <p>Selecting this option can significantly improve performance. We recommend you select this option unless your site has server power restrictions.</p> <ul style="list-style-type: none"> • —The USB System Idle Power Optimizing setting is enabled, because power savings are preferred over optimal performance.
Port 60h/64h Emulation Support	<p>Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —60h/64 emulation is not supported. • —60h/64 emulation is supported. <p>You should select this option if you are using a non-USB aware operating system on the server.</p>

Name	Description
xHCI Mode Support	<p>How onboard USB 3.0 ports behave. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Onboard USB 3.0 ports function as USB 2.0 ports. • —Onboard USB 3.0 ports function as USB 3.0 ports.

Device Management Tab

Name	Description
Front Panel USB Ports	<p>Whether the front panel USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • —Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
Rear Panel USB Ports	<p>Whether the rear panel USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • —Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
Internal USB Ports	<p>Whether the internal USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • —Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
KVM I/O	<p>Whether the vKVM ports are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • —Enables the KVM keyboard and/or mouse devices.
SD Card Drives	<p>Whether the SD card drives are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • —Enables the SD card drives.
vMedia Devices	<p>Whether the virtual media devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the vMedia devices. • —Enables the vMedia devices.
All USB Devices	<p>Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —All USB devices are disabled. • —All USB devices are enabled.

PCI BIOS Settings

The following tables list the PCI configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Table 7: Basic Tab

Name	Description
Max Memory Below 4G	<p>Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Does not maximize memory usage. Choose this option for all operating systems with PAE support. • —Maximizes memory usage below 4GB for an operating system without PAE support.
Memory Mapped IO Above 4Gb Configuration	<p>Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • —Maps I/O of 64-bit PCI devices to 4GB or greater address space.

Name	Description
VGA Priority	<p>Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following:</p> <ul style="list-style-type: none"> • —Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • —Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • —Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. <p>Note The vKVM does not function when the onboard VGA is disabled.</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note Only onboard VGA devices are supported with Cisco UCS B-Series servers.</p>
PCIe OptionROMs	<p>Whether Option ROM is available on all expansion ports. This can be one of the following:</p> <ul style="list-style-type: none"> • —The expansion slots are not available. • —The expansion slots are available. • —The expansion slots are available for UEFI only. • —The expansion slots are available for legacy only. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Mezz OptionRom	<p>Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —All LOM ports are enabled. • —All LOM ports are disabled.

Name	Description
PCIe 10G LOM 2 Link	<p>Whether Option ROM is available on the 10G LOM port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is available. • —The expansion slot is not available.
ASPM Support	<p>Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU determines the power state. • —ASPM support is disabled in the BIOS. • —Force all links to L0 standby (L0s) state.

Table 8: PCIe Slot Link Speed Tab

Name	Description
Slot <i>n</i> Link Speed	<p>This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot <i>n</i>. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —2.5GT/s (gigatransfers per second) is the maximum speed allowed. • —5GT/s is the maximum speed allowed. • —8GT/s is the maximum speed allowed. • —The maximum speed is set automatically. • —The maximum speed is not restricted.

Table 9: PCIe Slot OptionROM Tab

Name	Description
Slot <i>n</i> OptionROM	<p>Whether Option ROM is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot SAS	<p>Whether is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot HBA	<p>Whether is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.

Name	Description
Slot MLOM	<p>Whether Option ROM is available on the PCIe slot connected to the MLOM available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot N1	<p>Whether is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot N2	<p>Whether is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
PCI ROM CLPset pci-rom-clp-support pci-rom-clp-config	<p>The following options are available for PCI ROM CLP.</p> <ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. .

Name	Description
SIOC1 Option ROMset sloc1-optionrom-config sloc1-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.
SB Mezz1 Option ROMset sbmezz1-optionrom-config sbmezz1-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.
IOE Slot1 Option ROMset ioeslot1-option-config ioeslot1-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.
IOE Mezz1 Option ROMset ioemezz1-optionrom-config ioemezz1-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.

Name	Description
IOE Slot2 Option ROMset ioeslot2-optionrom-config ioeslot2-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.
IO ENVMe1 Option ROMset ioenvme1-optionrom-config ioenvme1-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.
IO ENVMe2 Option ROMset ioenvme2-optionrom-config ioenvme2-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.
SBNVMe1 Option ROMset ioenvme1-optionrom-config ioenvme1-optionrom	<ul style="list-style-type: none"> • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • Legacy-only—The expansion slot is available for legacy only. • UEFI-only—The expansion slot is available for UEFI only.

Graphics Configuration BIOS Settings

The following tables list the graphics configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Integrated Graphics	Enables integrated graphics. This can be one of the following: <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Integrated graphic is enabled. • —Integrated graphics is disabled.
Integrated Graphics Aperture Size	Allows you to set the size of mapped memory for the integrated graphics controller. This can be one of the following: <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • • • • • •
Onboard Graphics	Enables onboard graphics (KVM). This can be one of the following: <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Onboard graphics is enabled. • —Onboard graphics is disabled.

Boot Options BIOS Settings

The following table lists the boot options BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Waits for user input before retrying NON-EFI based boot options. • —Continually retries NON-EFI based boot options without waiting for user input.

Name	Description
Onboard SCU Storage Support	<p>Whether the onboard software RAID controller is available to the server. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The software RAID controller is not available. • —The software RAID controller is available.
Intel Entry SAS RAID	<p>Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The Intel SAS Entry RAID Module is disabled. • —The Intel SAS Entry RAID Module is enabled.
Intel Entry SAS RAID Module	<p>How the Intel SAS Entry RAID Module is configured. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Configures the RAID module to use Intel IT/IR RAID. • —Configures the RAID module to use Intel Embedded Server RAID Technology II.

Server Manager BIOS Settings

The following tables list the server management BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Assert NMI on SERR	<p>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS does not generate an NMI or log an error when a SERR occurs. • —The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable Assert Nmi on Perr.

Name	Description
Assert NMI on PERR	<p>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS does not generate an NMI or log an error when a PERR occurs. • —The BIOS generates an NMI and logs an error when a PERR occurs. You must enable Assert Nmi on Serr to use this setting.
OS Boot Watchdog Timer	<p>Whether the BIOS programs the watchdog timer with a predefined timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The watchdog timer is not used to track how long the server takes to boot. • —The watchdog timer tracks how long the server takes to boot. If the server does not boot within the predefined length of time, the CIMC resets the system and logs an error. <p>This feature requires either operating system support or Intel Management software.</p>
FRB-2 Timer	<p>Whether the FRB-2 timer is used to recover the system if it hangs during POST. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The FRB-2 timer is not used. • —The FRB-2 timer is started during POST and used to recover the system if necessary.
Out of Band Management	<p>This is used for the Windows Special Administration Control (SAC).</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The option to use the Windows Special Administration Control (SAC) is disabled. • —The option to use the Windows Special Administration Control (SAC) is enabled.

Name	Description
OS Boot Watchdog Timer Timeout	<p>What action the system takes if the watchdog timer expires. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server is powered off if the watchdog timer expires during OS boot. • —The server is powered off if the watchdog timer expires during OS boot. <p>This option is only available if you enable the OS Boot Watchdog Timer.</p>
OS Boot Watchdog Timer Timeout	<p>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The watchdog timer expires 5 minutes after the OS begins to boot. • —The watchdog timer expires 10 minutes after the OS begins to boot. • —The watchdog timer expires 15 minutes after the OS begins to boot. • —The watchdog timer expires 20 minutes after the OS begins to boot. <p>This option is only available if you enable the OS Boot Watchdog Timer.</p>
Redirection After BIOS POST	<ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The option to redirect is disabled. • —The option to redirect is disabled.

Console BIOS Settings

The following table lists the Console BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Legacy OS Redirect	<p>Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The serial port enabled for console redirection is hidden from the legacy operating system. • — The serial port enabled for console redirection is visible to the legacy operating system.
Console Redirection	<p>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —No console redirection occurs during POST. • —Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • —Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • —Console redirection occurs during POST. • —Enables console redirection of BIOS POST messages to server COM port 0. <p>Note If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.</p>

Name	Description
BAUD Rate	<p>What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • 9600—A 9600 BAUD rate is used. • 19200—A 19200 BAUD rate is used. • 38400—A 38400 BAUD rate is used. • 57600—A 57600 BAUD rate is used. • 115200—A 115200 BAUD rate is used. <p>Note This setting must match the setting on the remote terminal application.</p>
Terminal Type	<p>What type of character formatting is used for console redirection. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • pc-ansi—The PC-ANSI terminal font is used. • vt100—A supported vt100 video terminal and its character set are used. • vt100-plus—A supported vt100-plus video terminal and its character set are used. • vt-utf8—A video terminal with the UTF-8 character set is used. <p>Note This setting must match the setting on the remote terminal application.</p>

Name	Description
Flow Control	<p>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • None—No flow control is used. • —RTS/CTS is used for flow control. <p>Note This setting must match the setting on the remote terminal application.</p>
Putty Keypad	<p>Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following:</p> <ul style="list-style-type: none"> • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • ESCN—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • LINUX—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • SCO—The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • vt100—The function keys generate ESC OP through ESC O [. • VT400—The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS. • XTERMR6—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate ESC OP through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals.

IPMI Access Profile

The IPMI access profile policy allows you to determine whether you can send the IPMI commands directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the Cisco IMC. This policy defines the IPMI access, including a username and password, that can be authenticated locally on the server, and whether the access is read-only or read-write.

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

Creating and Editing an IPMI Access Profile

IPMI access profiles require IPMI users. You can create IPMI users at the same time you create the IPMI access profile, or you can add them to an existing IPMI access profile.

To modify the parameters of an IPMI access profile policy, select the policy from the **All policies** page, and click the **Edit** icon.

Procedure

-
- Step 1** In the **Actions** bar, type **Create IPMI Access Profile Policy** and press Enter.
 - Step 2** In the **IPMI Access Profile Policy** dialog box, click **Basic** and choose the **Domain Group Location** in which you want to create the domain group.
 - Step 3** In **Basic**, click **Organization** and select the location in which you want to create the policy.
 - Step 4** Enter a **Name** and optional **Description**.
The policy name is case sensitive.
 - Step 5** Select whether to allow **IPMI over LAN** remote connectivity.
 - Step 6** (Optional) In **IPMI Users**, select an IPMI user name, enter a password, and confirm the password.
 - Step 7** Select whether to allow read only or admin **Serial over LAN Access**.
 - Step 8** Click **Create**.
-

What to do next

Include the IPMI profile in a service profile or a service profile template.

Serial over LAN Policy

The serial over LAN policy (SOL) configures a serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

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

Creating and Editing a Serial over LAN Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Serial Over LAN (SOL) Policy** and press Enter.
 - Step 2** In the **Serial Over LAN (SOL) Policy** dialog box, choose the **Organization** in which you want to create the policy.
 - Step 3** Enter the **Name** and optional **Description** for the policy.
 - Step 4** Select a value for a **Baud Rate**.
 - Step 5** Click **Enabled** to allow the serial over LAN connection.
 - Step 6** Click **Create**.
-

Hardware Change Discovery Policy

When Cisco UCS Manager detects a change in the server hardware components, such as adapter insertion, adapter replacement, storage controller replacement, etc., an automatic deep-discovery of hardware changes is triggered. In some cases, this deep-discovery could erroneously report on new hardware, suggest steps to clean up inventories information about a removed or replaced component, or apply service profile changes. To prevent triggering an automatic deep-discovery of hardware changes, the **Hardware Change Discovery** Policy in Cisco UCS Central raises a critical hardware mismatch fault on the server and the changed hardware component.

- You must manually acknowledge the blade servers and clear faults to complete a hardware inventory. The deep-discovery and deep-association is initiated after you acknowledge the server.
- You must decommission rack servers when there is a hardware replacement, and then recommission them to clear all the hardware mismatch faults to initiate deep-discovery.



Note The **Hardware Change Discovery** Policy is supported on Cisco UCS Manager release 4.1(3) and later. **Hardware Change Discovery** Policy appears grayed out on Cisco UCS Manager when it is pushed down from Cisco UCS Central and the local Cisco UCS Manager user cannot edit the global policy. Cisco UCS Manager downgrade to prior releases is interrupted when any of the associated servers has a hardware inventory mismatch fault. However, you can upgrade to any release when there is a hardware mismatch fault. When the server has a hardware mismatch fault, service profile changes may not get applied correctly. You cannot change the **Hardware Change Discovery** Policy to **Auto-acknowledged** if the setup has servers with hardware inventory mismatch faults. You must acknowledge the server, or decommission/recommission rack servers, to clear all the hardware inventory mismatch faults before making any changes to the policy.

Create Hardware Change Discovery Policy

You can create a **Hardware Change Discovery** policy in a domain group in Cisco UCS Central.

Procedure

-
- Step 1** In the **Actions** bar, type **Hardware Change Discovery** and press Enter.
- Step 2** In the **Hardware Change Discovery** dialog box, choose the **Domain Group Location** in which you want to create the policy and enter a **Name** and optional **Description**.
- Step 3** In **Desired Action after a hardware component change**, select one of the following options to trigger hardware deep-discovery.
- **Auto Acknowledged**: Select this option to continue to use the current behavior. In this case, automatic deep-discovery is triggered.
 - **User Acknowledged** (default option): Select this option to trigger deep discovery after you acknowledge the server and clear the fault.
- Step 4** Click **Create**.
- Step 5** (Optional) You can favorite this policy and pin it to the Cisco UCS Central dashboard to navigate to it directly. After you create a Hardware Change Discovery policy, you can assign it to a domain group from the **Domain Configuration Settings** in **Domains Main View**.
- Step 6** In the **Domain Configuration Settings** window, click **Hardware Change Discovery Policy** in the **Policies** tab, and select the policy you want to assign to the domain group, and click **Save**.
- Step 7** Verify the assigned policy from the **Domains** view and check if there are any **Critical** faults associated with the server.
- Step 8** Click **Faults Summary** to view details of the fault in the **Fault Logs** window. From the Server main view, select **Re-Acknowledge** to acknowledge the server to clear the fault.
- Step 9** Verify that deep-discovery is triggered from the **Configuration Status** window.
-

Host Firmware Package Policy

The host firmware package policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). After you select the firmware bundle, you can choose to exclude different components. This allows you to prevent sensitive devices in your data center from being upgraded.



Note Excluding components is only supported in Cisco UCS Manager release 2.2.7 and above.

When excluding components, you should be aware of the following:

- The global-default host firmware package policy includes all components, but if you create a new custom host firmware package policy, the local disk component is automatically excluded.
- Host firmware package policies created in Cisco UCS Central 1.3 or previous do not support excluding components. These policies are not changed when you upgrade to Cisco UCS Central release 1.4 or above.

- If you create your own custom host firmware package policy with excluded components, including the local disk component that is excluded by default, you cannot include that host firmware package policy in a service profile associated with a server running a Cisco UCS Manager version prior to 2.2.7. If you do, you will see the following error during service profile association:

```
ucs domain does not have the matching server capabilities for this service-profile
```

You can either remove all excluded components in the host firmware package policy, or upgrade your version of Cisco UCS Manager to release 2.2.7 or above.

Cisco UCS Central release 2.1 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 4.1(3) and above. You can choose the firmware to be updated by using a service pack. For more information about service packs, see [About Service Packs](#), on page 161.

About Service Packs

Service packs are patches that you can use to apply security updates to Cisco UCS Manager infrastructure and server components. Service packs are specific to a base release. A service pack is provided as a single bundle for infrastructure and server components.

The following guidelines apply to service pack versions:

- A service pack can be applied only on its base bundle. You cannot install the service pack independently. For example, service pack 3.1(3)SP2 can be applied only on a 3.1(3) release. It is not compatible with a 3.1(4) or later release.
- Service packs are cumulative. You can use the latest service pack version with any patch version within the same maintenance release. For example, 3.1(3)SP3 will contain all the fixes that went into 3.1(3)SP2 and 3.1(3)SP1. You can apply 3.1(3)SP3 on any 3.1(3) release.
- Service pack version numbering in separate maintenance releases are unrelated. For example, service packs 3.1(3)SP2 and 3.1(4)SP2 are separate and unrelated.
- The same fix can be made available for separate maintenance releases through separate service packs. For example, the same fix can be made available in 3.1(3)SP2 and 3.1(4)SP3.
- You cannot downgrade service packs to versions below the default service pack version for a maintenance release. For example:
 - Base Bundle Version: 3.1(3b)
 - Default Service Pack Version: 3.1(3)SP2(Default)
 - Running Service Pack Version: 3.1(3)SP3
 - Service pack cannot be downgraded below 3.1(3)SP2
- When an upgrade or downgrade of a service pack fails, the default service pack version for that maintenance release becomes the running service pack version.
- You can roll back a service pack that was applied to a base release by removing the service pack selection.

The following table lists the Cisco UCS Manager release versions and the running version deployed in different situations when a service pack is applied:

Update Scenario	Bundle Version	Service Pack Version
Update to a service pack within the same maintenance release	No change is made to the bundle version	Service pack is updated to the specified version
Remove Service Pack	No change is made to the bundle version	Service pack is the default version that comes with the bundle
Update base bundle to another maintenance release	Base bundle changes to the version of the specified maintenance release	Current service pack is removed and is updated to the default version for the base bundle
Update to another maintenance release, and service pack	Base bundle changes to the version of the specified maintenance release	Service pack is updated to the specified version

For more information about selecting the compatible service packs for a firmware upgrade, see *Host Firmware Package Policy*, *Scheduling Firmware Infrastructure Update*, and *Chassis Firmware Package Policy*.

Creating or Editing a Host Firmware Package Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Host Firmware Package Policy** and press Enter.
- Step 2** In the **Host Firmware Package Policy** dialog box, click **Basic** and choose the **Organization** where you want to create the policy.
- Step 3** Enter a **Name** and optional **Description**.
The policy name is case-sensitive.
- Step 4** Select the **Blade Version** and **Rack Version** of the firmware, as required for your environment.
- Step 5** Select the required **Service Pack Version** of the firmware.
A Service pack can be applied only to the base version of a release and it should be compatible with that version. If the service pack is incompatible with the base version, the following error message is displayed:
Package Version of all bundles in the pack must match.
For more information about applicable service packs, see [About Service Packs](#), on page 161. The service pack version rolls back to the default setting when you remove the selection from the drop-down. 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.
- Step 7** To exclude all components, click **Excluded Components**.
- Step 8** To remove an excluded component, select it and click **Delete**.

Step 9 Click **Create**.

Note

To understand the impact of the policy, click **Evaluate**.

After you create a Host Firmware Package policy and associate it with a service profile template, the Service Pack images take precedence and when it is resolved, the firmware image is applied to the components accordingly.

iSCSI Adapter Policy

Creating or Editing an iSCSI Adapter Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create iSCSI Adapter Policy** and press Enter.
 - Step 2** In the **iSCSI Adapter Policy** dialog box, 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** Enter values for the **Connection Timeout**, **LUN Busy Retry Count**, and **DHCP Timeout**.
 - Step 5** Choose whether to enable **TCP Timestamp**, **HBA Mode**, and **Boot To Target**.
 - Step 6** Click **Create**.
-

iSCSI Authentication Profile

When you configure an adapter or blade in Cisco UCS to iSCSI boot from a LUN target, you should create an iSCSI Adapter Policy and configure the authentication profiles to be used by the initiator and the target.

Creating or Editing an iSCSI Authentication Profile

Procedure

-
- Step 1** In the **Actions** bar, type **Create iSCSI Authentication Profile** and press Enter.
 - Step 2** In the **iSCSI Authentication Profile** dialog box, 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** Enter the **User ID**.
 - Step 5** Type and confirm the password.
 - Step 6** Click **Create**.
-

Local Disk Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **Any Configuration**
- **No Local Storage**
- **No RAID**
- **RAID 1 Mirrored**
- **RAID 10 Mirrored and Striped**
- **RAID 0 Striped**
- **RAID 6 Striped Dual Parity**
- **RAID 60 Striped Dual Parity Striped**
- **RAID 5 Striped Parity**
- **RAID 50 Striped Parity Striped**

Creating or Editing a Local Disk Policy

Procedure

- Step 1** In the **Actions** bar, type **Create Local Disk Policy** and press Enter.
- Step 2** In the **Local Disk 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 **Mode**, select the configuration mode for the local disks.
- Step 5** Choose whether to enable or disable **Configuration Protection**, **FlexFlash**, and **FlexFlash RAID Reporting**.

Step 6 Click **Create**.

Port Auto-Discovery Policy

The **Port Auto-Discovery** policy enables automatic discovery of the type of device connected to a switch port, and configures it as a server port. When you choose to enable automatic port-discovery as part of the Port Auto-Discovery policy, Cisco UCS can automatically detect the port type if it is connected to a VIC, fabric extender, or an IOM, and configure it as an Fabric Interconnect (FI) server port. You can create a **Port Auto-Discovery** policy on a domain group and assign it to a domain profile from **Domain Configuration Settings** in the **Tools** menu.



Note The Port Auto-Discovery policy cannot be deployed onto Cisco UCS Manager if the domain is not part of a domain group.

Creating or Editing Port Auto-Discovery Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Port Auto-Discovery Policy** and press Enter.
- Step 2** In the **Create Port Auto-Discovery Policy** dialog box, choose the **Domain Group Location** in which you want to create the policy and enter the **Name** and optional **Description**.
- The name is case sensitive.
- Step 3** Select one of the options under **Auto Configure Server Port** to configure server port automatically:
- **Enabled**—Detects the FI ports and configures them as server ports if the ports are connected to a VIC, Fabric Extender, or chassis.
 - **Disabled**—Prevents auto-discovery and configuration of the ports as server ports.
- Step 4** Click **Create**.
- Click **Evaluate** to estimate the impact of the changes before saving the **Create Port Auto-Discovery** Policy.
- Step 5** (Optional) You can favorite this policy and pin it to the Cisco UCS Central dashboard to navigate to it directly.
- Step 6** (Optional) If a server port is already configured, you must first unconfigure it before you reapply the configuration through the server Port Auto-Discovery policy.
-

Graphics Card Policy

You can create a Graphics Card Policy to configure an NVIDIA GPU card and assign it to a service profile. This policy facilitates Cisco UCS Manager support to NVIDIA GPU cards for blade servers. The GPU cards

are integrated with the ability to upgrade device firmware through service profiles. The **Service Profile Details** page displays Graphics Card Policy details with the present mode of the GPU in the inventory.



Note The Graphics Card Policy is configured in the **Any Configuration** mode by default. If you configure the Graphics Card Policy in any mode except **Any Configuration**, associate it with a service profile, and the server does not have a GPU card, a configuration warning displays on the domain. If you configure the Graphics Card Policy in any mode except **Any Configuration**, associate it with a service profile, and the server has a GPU that does not support the mode-setting feature, a configuration error results.

However, if a server has a combination of graphics cards and one of them supports the mode-setting feature, then you must change the mode of the supported card.

Creating and Editing a Graphics Card Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Graphics Card Policy** and press Enter.
- Step 2** In the **Graphics Card Policy** dialog box, select the **Organization** in which you want to create the policy.
- Step 3** Enter a **Name** for the Graphics Card Policy, and add an optional **Description**.
The name is case sensitive.
- Step 4** In **Graphics Card Mode**, select one of these configuration modes for the graphics card:
- **Compute**
 - **Graphics**
 - **Any Configuration (default)**
- Step 5** Click **Create**.
- Step 6** To edit a Graphics Card policy, click **Edit** on the policy and change the Description and the graphics card mode.
Click **Evaluate** to estimate the impact of the changes before saving the Graphics Card Policy.
-

Statistics Threshold Policy

Cisco UCS Central lets you create a Statistics Threshold Policy that provides statistics about aspects of the system and generates an event if a threshold is crossed. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value. However, the threshold policies do not control the hardware or the device-level thresholds enforced by endpoints, such as the CIMC. The thresholds are built into the hardware components at manufacture. You can establish both minimum and maximum thresholds.

Creating a Statistics Threshold Policy

The Statistics Threshold Policy monitors statistics about aspects of the system and generates an event if a threshold is crossed. You can establish both minimum and maximum thresholds.

Procedure

-
- Step 1** In the **Actions** bar, type **Statistics Threshold Policy** and press Enter.
- Step 2** In the **Statistics Threshold Policy** dialog box (in **Basic**), choose the organization where you want to create the statistics threshold policy.
- Step 3** In the **Statistics Threshold Policy** dialog box, complete the following fields:
- **Name**—The name of the class. 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 class. Cisco recommends that you include information about where and when the policy can be used. Enter up to 256 characters.
- Step 4** Click **Create** to create a Basic Threshold class, or to create extra classes, choose a different policy category (for example, Adaptor Classes).
- Important**
You cannot clone a Statistics Threshold Policy.
- Step 5** (Optional) To create an Adaptor Class, click **Adaptor Classes** and click +.
- Step 6** Click the corresponding check boxes (classes) you want to include in your policy and click **Select**.
- Step 7** Click + in the Thresholds Definitions column and select the corresponding check boxes for the threshold definitions that you want to include in your class. In the Threshold Definitions column, do the following:
- a) In the **Normal Value** field, enter the desired value for the property type (in packets).
 - b) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:
 - **Critical**
 - **Major**
 - **Minor**
 - **Warning**
 - **Condition**
 - **Info**
 - c) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes:
 - **Condition**
 - **Info**
 - **Warning**
 - **Minor**

- **Major**
- **Critical**

Step 8 Click **Select** and **Create**.

Step 9 To create extra classes, repeat steps 5 to 9.

Scrub Policy

From Cisco UCS Central you can create scrub policy to determine what happens to local data and to the BIOS settings on a server during the discovery process, when the server is reacknowledged, or when the server is disassociated from a service profile.



Note Local disk scrub policies only apply to hard drives that are managed by Cisco UCS Manager and do not apply to other devices such as USB drives.

Depending upon how you configure a scrub policy, the following can occur at those times:

Disk scrub

One of the following occurs to the data on any local drives on disassociation:

- If enabled, destroys all data on any local drives.
- If disabled, preserves all data on any local drives, including local storage configuration.

BIOS Settings Scrub

One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:

- If enabled, erases all BIOS settings for the server and resets them to the BIOS defaults for that server type and vendor.
- If disabled, preserves the existing BIOS settings on the server.

FlexFlash Scrub

FlexFlash Scrub enables you to pair new or degraded SD cards, resolve FlexFlash metadata configuration failures, and migrate older SD cards with 4 partitions to single partition SD cards. One of the following occurs to the SD card when a service profile containing the scrub policy is disassociated from a server, or when the server is reacknowledged:

- If enabled, the HV partition on the SD card is formatted using the PNUOS formatting utility. If two SD cards are present, the cards are RAID-1 paired, and the HV partitions in both cards are marked as valid. The card in slot 1 is marked as primary, and the card in slot 2 is marked as secondary.
- If disabled, preserves the existing SD card settings.



- Note**
- Because the FlexFlash scrub erases the HV partition on the SD cards, we recommend that you take a full backup of the SD card(s) using your preferred host operating system utilities before performing the FlexFlash Scrub.
 - To resolve metadata config failures in a service profile, you need to disable FlexFlash in the local disk config policy before you run the FlexFlash scrub, then enable FlexFlash after the server is reacknowledged.
 - Disable the scrub policy as soon as the pairing is complete or the metadata failures are resolved.

Creating or Editing a Scrub Policy

Procedure

- Step 1** In the **Actions** bar, type **Create Scrub Policy** and press Enter.
- Step 2** In the **Scrub 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** Choose the scrub policies that you want to enable.
- Step 5** Click **Create**.

vMedia Policy

A vMedia policy is used to configure the mapping information for remote vMedia devices. Two vMedia devices and mappings for CD and HDD are allowed in a vMedia policy. You can configure one ISO and one IMG at a time. ISO configurations map to a CD drive. IMG configurations map to a HDD device.



- Note** If you want to map a device to a remote folder, you must create an IMG and map it as a HDD device.

From Cisco UCS Central you can provision vMedia devices ISO images for remote UCS servers. Using Scriptable vMedia, you can programmatically mount IMG and ISO images on a remote server. CIMC mounted vMedia provides communications between other mounted media inside your datacenter with no additional requirements for media connection. Scriptable vMedia allows you to control virtual media devices without using a browser to manually map each Cisco UCS server individually.

Scriptable vMedia supports multiple share types including NFS, CIFS, HTTP, and HTTPS shares. Scriptable vMedia is enabled through BIOS configuration and configured through a Web GUI and CLI interface. You can do the following in the registered Cisco UCS domains using scriptable vMedia:

- Boot from a specific vMedia device

- Copy files from a mounted share to local disk
- Install and update OS drivers



Note Support for Scriptable vMedia is applicable for CIMC mapped devices only. Existing-KVM based vMedia devices are not supported.

Creating or Editing a vMedia Policy

You can create a vMedia policy and associate the policy with a service profile.

Procedure

-
- Step 1** In the **Actions** bar, type **Create vMedia Policy** and press Enter.
- Step 2** In the **vMedia Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
- Enter a **Name** and optional **Description**.
Policy name is case sensitive.
 - (Optional) Select **Enabled** or **Disabled** for Retry on Mount Failure.
If enabled, the vMedia will continue mounting when a mount failure occurs.
- Step 3** (Optional) Click **HDD**, and do the following:
- Enter the **Mount Name**.
 - Select the **Protocol** and fill in required protocol information.
 - In **Generate File name from Service Profile Name**, click **Enabled** or **Disabled**.
Enabled will automatically use the Service profile name as IMG name. The IMG file with the same name as the service profile must be available at the required path. If you select **Disabled**, fill in remote IMG file name that the policy must use.
- Step 4** (Optional) Click **CDD** and do the following:
- Enter the **Mount Name**.
 - Select the **Protocol** and fill in required protocol information.
 - In **Generate File name from Service Profile Name**, click **Enabled** or **Disabled**.
Enabled will automatically use the Service profile name as ISO name. The ISO file with the same name as the service profile must be available at the required path. If you select **Disabled**, fill in remote ISO file name that the policy must use.
- Step 5** Click **Create**.
-

What to do next

Associate the vMedia policy with a service profile.

