Cisco UCS Central Server Management Guide, Release 1.5

First Published: July 29, 2016

Last Modified: August 11, 2016

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

CONTENTS

Preface

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

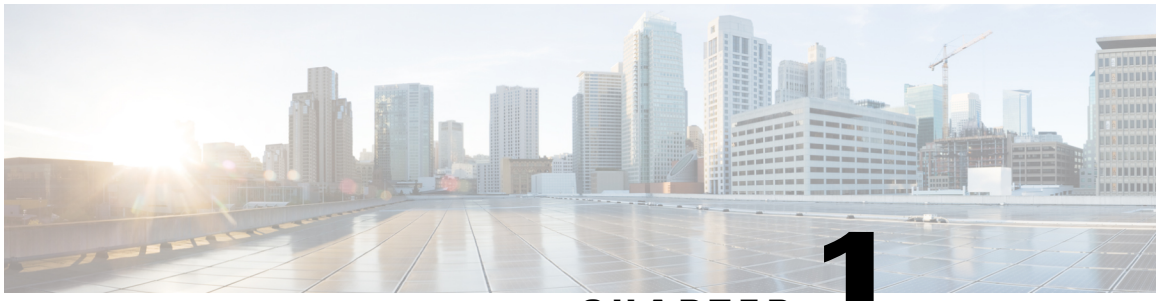
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

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



CHAPTER 1

Overview

Overview

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

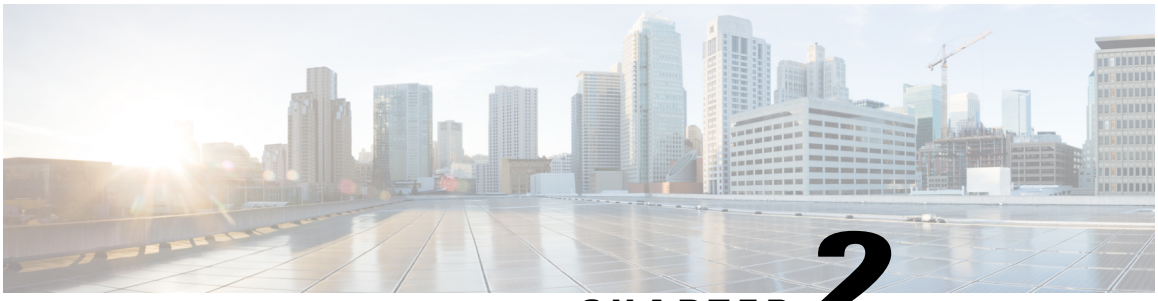
- UCS server hardware
- Service profile and templates
- Server boot
- Server policies

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.

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



CHAPTER 2

Cisco UCS Servers

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

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.

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 menu bar, click the **System Tools** icon and choose **Unified KVM Launcher**.

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

Step 3 Click **Launch KVM**.

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:

a) 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.

b) 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.

c) 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.

d) 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.

e) 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:

a) In **Chassis/FEX Link Action**, select the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.

b) 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.

c) 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.

d) In the **Backplane Speed Preference**, choose the speed that you want to use.

Step 5 Click **Power** and complete the following fields:

a) 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.

b) 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.

c) 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**.

Power Control Policy

You can create a power control policy in Cisco UCS Central and include it in the service profile to enable the system to manage the power allocation control for the blade servers in the registered Cisco UCS domains.

Cisco UCS uses the priority set in the power control policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis.

During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies. Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

For mission-critical application a special priority called no-cap is also available. Setting the priority to no-cap prevents Cisco UCS from leveraging unused power from a particular server. With this setting, the server is allocated the maximum amount of power possible for that type of server.

Creating or Editing a Power Control Policy

Procedure

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

Step 2 In the **Power ControlPolicy** 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 Choose the **Fan Speed**.
This can be one of the following:

- **Low Power—**The fan runs at the minimum speed required to keep the server cool.
- **Balanced—**The fan runs faster when needed based on the heat generated by the server. When possible, the fan returns to the minium required speed.
- **Performance—**The fan is kept at the speed needed for better server performance. This draws more power but means the fan is already at speed if the server begins to heat up.
- **High Power—**The fan is kept at an even higher speed that emphasizes performance over power consumption.
- **Max Power—**The fan is kept at the maximum speed at all times. This option provides the most cooling and uses the most power.
- **Any—**The server determines the optimal fan speed.

Step 5 Choose whether to enable **Power Capping**.

Step 6 If **Enabled**, choose the **Power Group Priority**.
Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

Step 7 Click **Create**.

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
This column displays the following information for a fabric interconnect: • The associated domain name and FI ID • Domain group location • IP address of the domain	This column displays the following hardware information for a fabric interconnect: • 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	This column displays the following firmware details for a fabric interconnect: • Firmware version • Firmware status	This column displays the following status for a fabric interconnect: • 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:

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

- 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.

Server Details

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

Servers	Hardware	Configuration	Status
This column displays the following information for a server: • The associated domain name, chassis ID, and slot ID • Domain group location • Management IP address	This column displays the following hardware information for a server: • 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	This column displays the following configuration for a server: • Service profile name • Service profile organization location • Firmware version • Firmware status	This column displays the following status for a server: • Overall status • Worst fault level • Power status • Decommissioned server. You can recommission a decommissioned server.

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.

- **Motherboard—**Displays the overall status and the hardware details of the motherboard.
- **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.
- **Controllers—**Displays the list of storage controllers, such as SAS or FlexFlash. Select a controller to view operability and other product details.
- **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.

You can also perform the following server-related tasks:

- 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 the **KVM Console**.
- Reset, recover, reacknowledge, or decommission a server.
- Toggle the locator LED.

Chassis Inventory

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

Chassis	Hardware	Configuration	Status
This column displays the following information for a chassis: • The associated domain name and chassis ID • Domain group location • Fabric side	This column displays the following hardware information for a chassis: • Model number of the chassis • Serial number of the chassis • Number of blades	This column displays the following configuration for a Chassis: • Configuration status • Configuration error count	This column displays the following status for a Chassis: • Overall status • Worst fault level • Power status • Thermal status • Decommissioned chassis. You can recommission the chassis by specifying a valid chassis ID.

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.
- Turn on or turn off the Locator LED for a chassis.
- Launch Cisco UCS Manager for the specific Cisco UCS domain.

Note

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

Storage Chassis View

The Storage Chassis page allows you to manage and monitor all Cisco UCS C3260 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
This column displays the following information for a FEX: • The associated domain name and FEX ID • Domain group location • Fabric Side	This column displays the following hardware information for a FEX: • Model number • Serial number • Number of ports available	This column displays the following configuration for a FEX: • Configuration status • Configuration error count	This column displays the following status for a FEX: • Overall status • Worst fault level • Power status • Thermal status • Decommissioned FEX. You can recommission the FEX by specifying a valid FEX ID.

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.

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
This column displays the following information for a registered domain: • The associated domain name and site • Domain group location • Management IP address • Owner	This column displays the following hardware information for a registered domain: • 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	This column displays the following configuration for a registered domain: • Platform family • Firmware version • Firmware status	This column displays the following status for a registered domain: • 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 UCS Central subscription, and re-evaluate the membership of the domain.

- **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.

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

- Launch Cisco UCS Manager GUI for the selected Cisco UCS domain.
- Suspend UCS Central subscription when the overall status of a domain is OK.
- Activate UCS Central subscription when the overall status of a domain is suspended.
- Re-evaluate membership
- Create a LAN or SAN pin group.

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 Click the **Browse Tables** icon and choose an inventory view, for example **Domains**, **Servers**, or **Templates**.
Note This does not apply to **ID Universe**.

Step 2 In an inventory view, click the icon that corresponds to your selected export format.
If there are more than 500 rows to be exported, you are given the opportunity to filter your results before downloading.

Viewing Configuration Status

Procedure

Step 1 Click the **Browse Tables** icon and choose a hardware option such as: **Servers**, **Chassis**, **Fabric Interconnects**, or **FEX**.

Step 2 Click on an object to select it.

Step 3 On the detail view page, click the **Tools** icon and select **Configuration Status**.
The **Configuration Status** page displays.

Step 4 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 Click the **Browse Tables** icon and choose a hardware option such as: **Servers**, **Chassis**, **Fabric Interconnects**, or **FEX**.

Step 2 Click on an object to select it.

Step 3 On the detail view page, click the **Tools** icon and select **Toggle Locator LED**.
The Locator LED status is located at the top of the **Basic** tab.

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 Click the **Browse Tables** icon and choose 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.

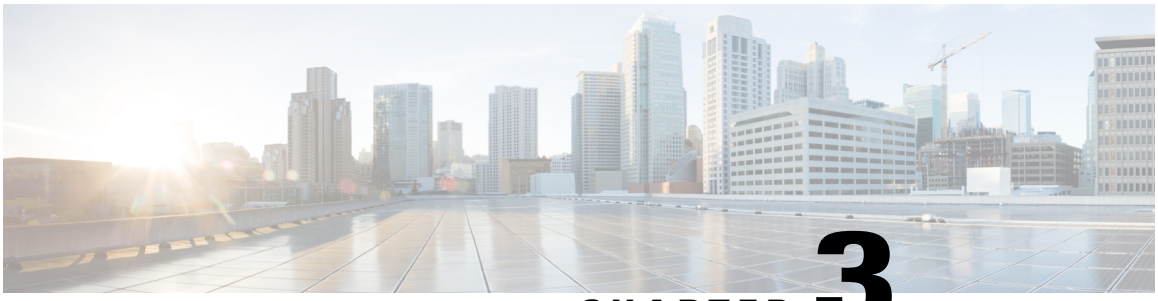
Step 2 Verify that the filters you selected when you created the query are checked.
The search results are dynamically updated.

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

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 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.

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 24.

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 24.

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. • **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. • **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.
Configuration	The service profile applied to the server.
Operating System	If tagged, the operating system for the selected server.

Field	Description
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: • 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 the Cisco UCS Central Administration Guide.

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 the Cisco UCS Central Administration Guide.

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 **Sychronize 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**.

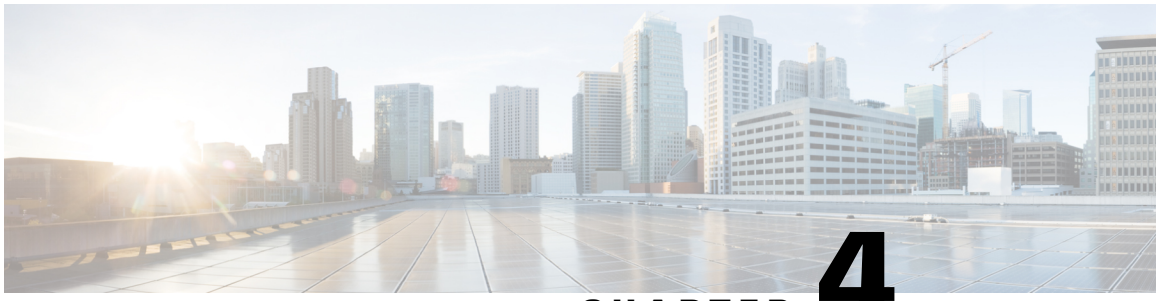
Step 2 On the **Hardware Compatibility** page, click the **Tools** icon and choose **Import Hardware Compatibility List**.

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

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.

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 **Compatability 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.
For more information on creating vNICs, see the Cisco UCS Central Network Management Guide.

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

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 the Cisco UCS Central Storage Management Guide.

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**.

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 that you want to use 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**.

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 3.1(2) 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

Note the following circumstances in which you **cannot** set a static ID:

- If you created the global service profile from a service profile updating template, and the service profile is bound to that template.

Note You can set static IDs if you unbind the service profile from the template. You can also set them if you created the service profile from an initial template.

- If you created the global service profile using an LCP (LAN connectivity policy) for iSCSI MAC addresses, iSCSI initiator IP addresses and iSCSI IQN addresses.
- If you created the global service profile using an SCP (SAN connectivity policy) for WWNN and WWPN addresses.

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 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF.

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.
- **Identifiers—**Displays a list of entities used to identify the service profile.
- **Connectivity—**Displays a list of connectivity-related information.
- **FC Zones—**Displays a list of Fibre Channel zones included in the service profile.
- **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.
- 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.

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 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 the Cisco UCS Central Administration Guide.

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

Viewing Service Profile Configuration Status

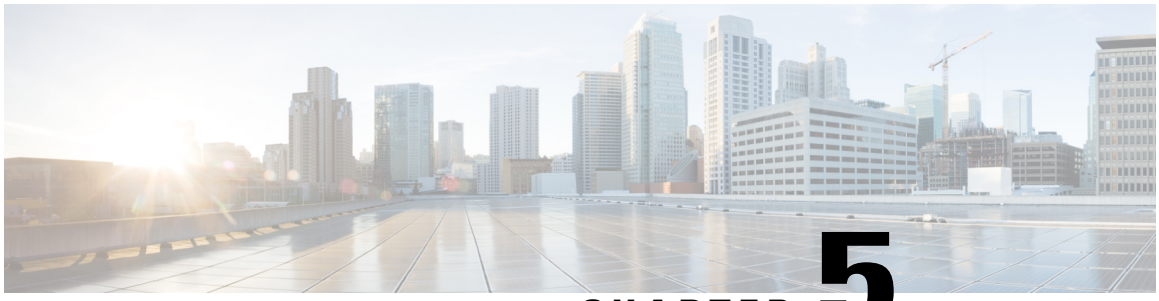
Procedure

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

Step 2 Click on a service profile to select it.

Step 3 On the service profile page, click the **Alerts** icon on the far right and select **Configuration Status**. The Configuration Status page for the selected service profile displays.

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



CHAPTER 5

Server Pools

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 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 45.

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—**You can assign the IP addresses in the block 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:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IP pool.
b) 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:

a) Click the **Plus** sign to create one or more blocks of IP addresses in the selected pool.
b) In the respective IP block start column, enter the first IPv4 or IPv6 addresses in the block.
c) 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:

1 Enter the subnet mask associated with the IPv4 or IPv6 address in the block.

2 Enter the default gateway associated with the IPv4 or IPv6 address in the block.

3 Enter the primary DNS server that this block of IPv4 or IPv6 address should access.

4 Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.

5 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 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**.

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:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IQN pool.
b) Enter name and description of the IQN pool.
c) Enter the prefix for any IQN blocks created for this pool.

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

a) Click the **Plus** icon to create one or more blocks of IQN suffixes in the selected pool.
b) In the **Suffix Block** column, enter the suffix for this block of IQNs.
c) In the **Start** column, enter the first IQN suffix in the block.
d) 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:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an UUID pool.
b) Enter name and description of the pool.
c) Enter the sufix for any UUID blocks created for this pool.

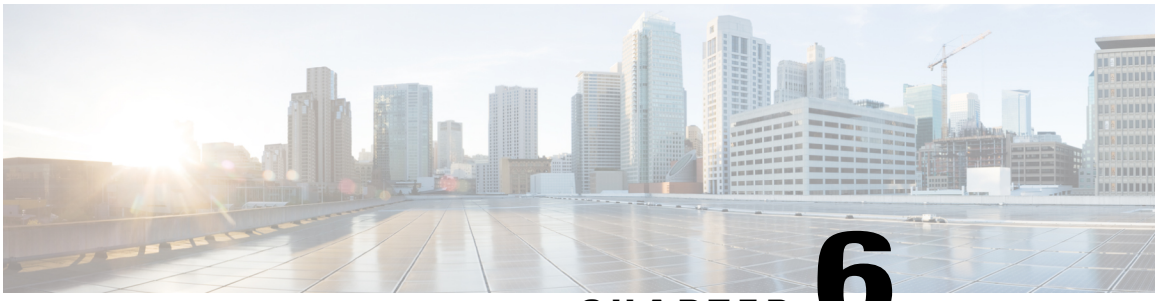
Step 3 In **Suffix Blocks**, complete the following:

a) Click the **Create** icon.
b) In the **Suffix Block** column, enter the suffix for this block of UUIDs.
c) In the **Start** column, enter the first UUID suffix in the block.
d) In the **Size** column, enter the total number of UUIDs in the block.
e) Click the **Apply** icon.
Additional fields related to UUID pools are displayed.
f) In **UUIDs**, you can view a graphical representation of the number if UUID addresses in the pool, the number of assigned UUID addresses, duplicate UUID addresses, and UUID summary.
g) 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 6

Server Boot

This chapter includes the following sections:

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 M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers, 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 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 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 50.

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

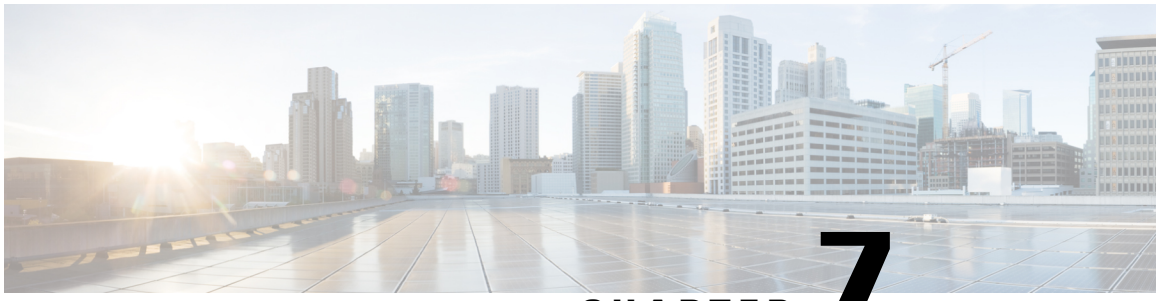
Step 1 From the **Service Profile** or **Service Profile Template** page, click the **Tools** icon and choose **Configure iSCSI Targets**.

Step 2 In the **Configure iSCSI Targets** dialog box, click **Primary** or **Secondary** and enter the iSCSI vNIC.

Step 3 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 4 Click **Save**.



CHAPTER 7

Server Policies

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 57.

Step 3 In **Processor**, complete the fields as necessary.
For more information, see Processor BIOS Settings, on page 61.

Step 4 In **I/O**, complete the fields as necessary.
For more information, see I/O BIOS Settings, on page 74.

Step 5 In **RAS Memory**, complete the fields as necessary.
For more information, see RAS Memory BIOS Settings, on page 75.

Step 6 In **USB**, complete the fields as necessary.
For more information, see USB BIOS Settings, on page 78.

Step 7 In **PCI**, complete the fields as necessary.
For more information, see PCI BIOS Settings, on page 82.

Step 8 In **Graphics Configuration**, complete the fields as necessary.
For more information, see Graphics Configuration BIOS Settings, on page 87.

Step 9 In **Boot Options**, complete the fields as necessary.
For more information, see Boot Options BIOS Settings, on page 88.

Step 10 In **Server Manager**, complete the fields as necessary.
For more information, see Server Manager BIOS Settings, on page 89.

Step 11 In **Console**, complete the fields as necessary.
For more information, see Console BIOS Settings, on page 91.

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
Reboot on BIOS Settings Change	When the server is rebooted after you change one or more BIOS settings. **Enabled—**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. **Disabled—**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.

Name	Description
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The serial port is disabled. • **Enabled—**The serial port is enabled.
Quiet Boot	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The BIOS displays all messages and Option ROM information during boot. • **Enabled—**The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The BIOS continues to attempt to boot the server. • **Enabled—**The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.
Front Panel Lockout	Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The power and reset buttons on the front panel are active and can be used to affect the server. • **Enabled—**The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.

Name	Description
Consistent Device Naming (CDN)	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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**CDN is disabled for this BIOS policy. • **Enabled—**CDN is enabled for this BIOS policy.
Resume AC On Power Loss	How the server behaves when power is restored after an unexpected power loss. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Last State—**The server is powered on and the system attempts to restore its last state. • **Reset—**The server is powered on and automatically reset. • **Stay Off—**The server remains off until manually powered on.
QuickPath Interconnect (QPI) Link Frequency	The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s). This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **6400** • **7200** • **8000** • **9600** • **Auto—**The CPU determines the QPI link frequency.

Name	Description
QuickPath Interconnect (QPI) Snoop Mode	This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Home Snoop—**The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Cluster On Die—**This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads. • **Early Snoop—**The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized.
Trusted Platform Module (TPM)	Whether TPM is used to securely store artifacts that are used to authenticate the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**TPM is used for authentication. • **Disabled—**TPM is not used for authentication.
Intel Trusted Execution Technology (TXT)	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**TXT is used for extra security. • **Disabled—**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 1: Basic Tab

Name	Description
Execute Disabled Bit	Classifies memory areas on the server to specify where the application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.

Name	Description
Local X2 Application Policy Infrastructure Controller (APIC)	Allows you to set the type of Application Policy Infrastructure Controller (APIC) architecture. This can be one of the following: • **xAPIC—**Uses the standard xAPIC architecture. • **x2APIC—**Uses the enhanced x2APIC architecture to support 32 bit addressability of processors. • **Auto—**Automatically uses the xAPIC architecture that is detected. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled—**The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled—** The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
P-STATE Coordination	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. • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **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. • **Energy Efficient—**DRAM clock throttling is increased to improve energy efficiency. • **Auto—**The CPU determines the level.

Name	Description
Channel Interleaving	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: • **Auto—**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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Rank Interleaving	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: • **Auto—**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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **Auto—**The CPU determines the physical elevation. • **300 M—**The server is approximately 300 meters above sea level. • **900 M—**The server is approximately 900 meters above sea level. • **1500 M—**The server is approximately 1500 meters above sea level. • **3000 M—**The server is approximately 3000 meters above sea level. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Table 2: Prefetchers Tab

Name	Description
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled—**The hardware prefetcher is not used. • **Enabled—**The processor uses the hardware prefetcher when cache issues are detected. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** **CPU Performance** must be set to **Custom** in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.

Name	Description
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled—**The processor only fetches the required line. • **Enabled—**The processor fetches both the required line and its paired line. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** **CPU Performance** must be set to **Custom** in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
Data Cache Unit (DCU) Streamer Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled—**The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Data Cache Unit (DCU) IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not preload any cache data. • **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Table 3: Technology Tab

Name	Description
Turbo Boost	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor uses Turbo Boost Technology if required.
Enhanced Intel Speed Step	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor never dynamically adjusts its voltage or frequency. • **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.

Name	Description
Hyper Threading	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Core Multi-Processing	Sets the state of logical processor cores per CPU in a package. If you disable this setting, Intel Hyper Threading technology is also disabled. This can be one of the following: • **Platform Default—**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 ***n*—**Specifies the number of logical processor cores per CPU that can run on the server. To disable multiprocessing and have only one logical processor core per CPU running on the server, choose 1. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Virtualization Technology (VT)	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.

Table 4: Power Tab

Name	Description
Power Management	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Disabled—**The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient—**The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters. • **Performance—**The server automatically optimizes the performance for the BIOS parameters mentioned above. • **Custom—**The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Performance** • **Balanced Performance** • **Balanced Energy** • **Energy Efficient** • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Processor C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The system remains in a high-performance state even when idle. • **Enabled—**The system can reduce power to system components such as the DIMMs and CPUs. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Processor C1E	Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The CPU continues to run at its maximum frequency in the C1 state. • **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state.
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enterprise—**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. • **High Throughput—**Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • **HPC—**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	The amount of power available to the server components when they are idle. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Auto—**The CPU determines the available power. • **C0 State—**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. • **C1 State—**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. • **C2 State—**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. • **C3 State—**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. • **C6 State—**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. • **C7 State—**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. • **C7s State—**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. • **No Limit—**The server may enter any available C state.

Table 5: Errors and Reporting Tab

Name	Description
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not send the C3 report. • **Enabled—**The processor sends the C3 report. • **ACPI-C2—**The processor sends the C3 report using the advanced configuration and power interface (ACPI) C2 format. • **ACPI-C3—**The processor sends the C3 report using the ACPI C3 format. On the Cisco UCS B440 Server, the BIOS Setup menu uses enabled and disabled for these options. If you specify acpi-c2 or acpi-c3, the server sets the BIOS value for that option to enabled.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not send the C6 report. • **Enabled—**The processor sends the C6 report.
Processor C7 Report	Whether the processor sends the C7 report to the operating system. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The processor does not send the C7 report. • **Enabled—**The processor sends the C7 report. • **C7—**The processor sends the C7 report. • **C7s—**The processor sends the C7s report. **Note** The selections vary depending on the server and operating system.

Name	Description
Max Variable MTRR Setting	Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Auto-Max—**BIOS uses the default value for the processor. • **8—**BIOS uses the number specified for the variable MTRR.
Demand Scrub	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. • **Disabled—** Single bit memory errors are not corrected.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **EnabledEnabled—**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. • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address.

Name	Description
CPU Hardware Power Management	Enables processor Hardware Power Management (HWPM). This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**HWPM is disabled. • **HWPM Native Mode—**HWPM native mode is enabled. • **HWPM OOB Mode—**HWPM Out-Of-Box mode is enabled.

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	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). You can select one of the following options: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The processor uses virtualization technology. • **Disabled—**The processor does not use virtualization technology. **Note** This option must be set to enabled if you want to change any of the other Intel Directed I/O BIOS settings.
Interrupt Re-map	Whether the processor supports Intel VT-d Interrupt Remapping. You can select one of the following options: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The processor uses VT-d Interrupt Remapping as required. • **Disabled—**The processor does not support remapping.

Name	Description
Coherency Support	Whether the processor supports Intel VT-d Coherency. You can select one of the following options: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The processor uses VT-d Coherency as required. • **Disabled—**The processor does not support coherency.
Address Translation Services (ATS) Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). You can select one of the following options: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The processor uses VT-d ATS as required. • **Disabled—**The processor does not support ATS.
Pass Through DMA Support	Whether the processor supports Intel VT-d Pass-through DMA. You can select one of the following options: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The processor uses VT-d Pass-through DMA as required. • **Disabled—**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	Whether the BIOS supports NUMA. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • **Disabled—**The BIOS does not support NUMA.
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Power Saving Mode—**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. • **Performance Mode—**The system prioritizes high frequency operations over low voltage operations. • **Auto—**The CPU determines the priority.
DRAM Refresh Rate	The refresh interval rate for internal memory. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **1x** • **2x** • **3x** • **4x** • **Auto**

Name	Description
Memory RAS Configuration Mode	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Maximum Performance—**System performance is optimized. • **Mirroring—**System reliability is optimized by using half the system memory as backup. • **Lockstep—**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. • **Sparing—**Enables sparing mode.
Sparing Mode	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. This option is only available if you choose the sparing option for the Memory RAS Config parameter. It can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **DIMM Sparing—**One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • **Rank Sparing—**A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank.

Name	Description
DDR3 Voltage Selection	The voltage to be used by the dual-voltage RAM. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **1500 MV** • **1350 MV**

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	Whether the server can boot from a USB device. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The server can boot from a USB device. • **Enabled—**The server cannot boot from a USB device.
USB Front Panel Access Lock	USB front panel lock is configured to enable or disable the front panel access to USB ports. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled** • **Enabled**

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Auto—**Disables legacy USB support if no USB devices are connected. • **Disabled—**USB devices are only available to EFI applications. • **Enabled—**Legacy USB support is always available. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Idle Power Optimizing Setting	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **High Performance—**The USB System Idle Power Optimizing setting is disabled, because optimal performance is preferred over power savings. Selecting this option can significantly improve performance. We recommend you select this option unless your site has server power restrictions. • **Lower Idle Power—**The USB System Idle Power Optimizing setting is enabled, because power savings are preferred over optimal performance.
Port 60h/64h Emulation Support	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**60h/64 emulation is not supported. • **Enabled—**60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.

Name	Description
xHCI Mode Support	How onboard USB 3.0 ports behave. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Onboard USB 3.0 ports function as USB 2.0 ports. • **Enabled—**Onboard USB 3.0 ports function as USB 3.0 ports.

Device Management Tab

Name	Description
Front Panel USB Ports	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
Rear Panel USB Ports	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
Internal USB Ports	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
KVM I/O	Whether the KVM ports are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled—**Enables the KVM keyboard and/or mouse devices.
SD Card Drives	Whether the SD card drives are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • **Enabled—**Enables the SD card drives.
vMedia Devices	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Disables the vMedia devices. • **Enabled—**Enables the vMedia devices.

Name	Description
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**All USB devices are disabled. • **Enabled—**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 6: Basic Tab

Name	Description
Max Memory Below 4G	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Does not maximize memory usage. Choose this option for all operating systems with PAE support. • **Enabled—**Maximizes memory usage below 4GB for an operating system without PAE support.

Name	Description
Memory Mapped IO Above 4Gb Configuration	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**Maps I/O of 64-bit PCI devices to 4GB or greater address space.
VGA Priority	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: • **Onboard—**Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard—**Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled—**Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** Only onboard VGA devices are supported with Cisco UCS B-Series servers.

Name	Description
PCIe OptionROMs	Whether Option ROM is available on all expansion ports. This can be one of the following: • **Disabled—**The expansion slots are not available. • **Enabled—**The expansion slots are available. • **UEFI-Only—**The expansion slots are available for UEFI only. • **Legacy Only—**The expansion slots are available for legacy only. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Mezz OptionRom	Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**All LOM ports are enabled. • **Disabled—**All LOM ports are disabled.
PCIe 10G LOM 2 Link	Whether Option ROM is available on the 10G LOM port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The expansion slot is available. • **Disabled—**The expansion slot is not available.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Auto—**The CPU determines the power state. • **Disabled—**ASPM support is disabled in the BIOS. • **Force L0—**Force all links to L0 standby (L0s) state.

Table 7: PCIe Slot Link Speed Tab

Name	Description
Slot *n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **gen1 - 2.5 GT/s—**2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **gen2 - 5 GT/s—**5GT/s is the maximum speed allowed. • **gen3 - 8 GT/s—**8GT/s is the maximum speed allowed. • **Auto—**The maximum speed is set automatically. • **Disabled—**The maximum speed is not restricted.

Table 8: PCIe Slot OptionROM Tab

Name	Description
Slot *n* OptionROM	Whether Option ROM is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.

Name	Description
Slot SAS	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.
Slot HBA	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.
Slot MLOM	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.

Name	Description
Slot N1	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.
Slot N2	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.

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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**Integrated graphic is enabled. • **Disabled—**Integrated graphics is disabled.

Name	Description
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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **128 MB** • **256 MB** • **512 MB** • **1024 MB** • **2048 MB** • **4096 MB**
Onboard Graphics	Enables onboard graphics (KVM). This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**Onboard graphics is enabled. • **Disabled—**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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Waits for user input before retrying NON-EFI based boot options. • **Enabled—**Continually retries NON-EFI based boot options without waiting for user input.

Name	Description
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The software RAID controller is not available. • **Enabled—**The software RAID controller is available.
Intel Entry SAS RAID	Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The Intel SAS Entry RAID Module is disabled. • **Enabled—**The Intel SAS Entry RAID Module is enabled.
Intel Entry SAS RAID Module	How the Intel SAS Entry RAID Module is configured. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Intel IT/IR RAID—**Configures the RAID module to use Intel IT/IR RAID. • **Intel Embedded Server RAID Technology II—**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	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The BIOS does not generate an NMI or log an error when a SERR occurs. • **Enabled—**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**.
Assert NMI on PERR	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The BIOS does not generate an NMI or log an error when a PERR occurs. • **Enabled—**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	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**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. This feature requires either operating system support or Intel Management software.

Name	Description
OS Boot Watchdog Timer Timeout Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Power Off—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is powered off if the watchdog timer expires during OS boot. This option is only available if you enable the OS Boot Watchdog Timer.
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **5 Minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10 Minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15 Minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20 Minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. This option is only available if you enable the OS Boot Watchdog Timer.

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	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The serial port enabled for console redirection is hidden from the legacy operating system. • **Enabled—** The serial port enabled for console redirection is visible to the legacy operating system.
Console Redirection	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: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**No console redirection occurs during POST. • **Serial Port A—**Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • **Serial Port B—**Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • **Enabled—**Console redirection occurs during POST. • **Com 0—**Enables console redirection of BIOS POST messages to server COM port 0. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.

Name	Description
BAUD Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **Platform Default—**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. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **Platform Default—**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. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Flow Control	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: • **Platform Default—**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—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **Platform Default—**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**.

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.

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 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 6 To exclude all components, click **Excluded Components**.

Step 7 To remove an excluded component, select it and click **Delete**.

Step 8 Click **Create**.

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

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**.

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**.

ID Range Access Control Policy

Use the ID range access control policy to limit what pools can be utilized in a specific domain group. When you apply the access control policy to a pool, only the domain groups selected can access those pools.

Creating or Editing an ID Range Access Control Policy

Procedure

Step 1 In the **Actions** bar, type **Create ID Range Access Control Policy** and press Enter.

Step 2 In the **ID Range Access Control 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 **Domain Groups**, click **Add** to select the **Permitted Domain Groups** associated with this policy.

Step 5 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**.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters, you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Creating or Editing a Quality of Service Policy

Procedure

Step 1 In the **Actions** bar, type **Create Quality of Service (QoS) Policy** and press Enter.

Step 2 In the **Create Quality of Service (QoS) Policy** dialog box, click **Organization** and select the location in which you want to create the policy.

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

Step 4 Select an **Egress Priority**.

Step 5 Choose whether to enable **Host Control Class of Service (CoS)**.

Step 6 Enter an **Egress Burst Size**, and select the egress average traffic rate.

Step 7 Click **Create**.

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.

a) Enter a **Name** and optional **Description**.
Policy name is case sensitive.

b) (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:

a) Enter the **Mount Name**.
b) Select the **Protocol** and fill in required protocol information.
c) 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:

a) Enter the **Mount Name**.

b) Select the **Protocol** and fill in required protocol information.
c) 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.