Policies

This chapter includes the following sections:

Policies in Cisco UCS Central and Cisco UCS Domains

You can create and manage global policies in Cisco UCS Central and include them in service profiles or service profile templates for one or more Cisco UCS domains. The service profiles and service profile templates that include global policies can be either of the following:

- Local service profiles or service profile templates that are created and managed by Cisco UCS Manager in one Cisco UCS domain. You can only associate local service profiles with servers in that domain. When you include a global policy in a local service profile, Cisco UCS Manager makes a local read-only copy of that policy.
- Global service profiles or service profile templates that are created and managed by Cisco UCS Central. You can associate global service profiles with servers in one or more registered Cisco UCS domains.

You can only make changes to global policies in Cisco UCS Central. Those changes affect all service profiles and service profile templates that include the global policy. All global policies are read-only in Cisco UCS Manager.

You can configure all operational policies under a domain group using IPv6 addresses. These policies are located in the **Operations Management** tab of the Cisco UCS Central GUI.

This feature helps the Cisco UCS Manager to use an IPv6 address while importing these policies from Cisco UCS Central.

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

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

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

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

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

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

Name	Description
Infrastructure & Catalog Firmware	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Time Zone Management	Determines whether the date and time is defined locally or comes from Cisco UCS Central.
Communication Services	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Global Fault Policy	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
DNS Management	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy	Determines whether managed endpoints are defined locally or in Cisco UCS Central.
Power Management	Determines whether the power management is defined locally or in Cisco UCS Central.
Power Supply Unit	Determines whether power supply units are defined locally or in Cisco UCS Central.

Consequences of Policy Resolution Changes

When you register a Cisco UCS domain, you configure policies for local or global resolution. The behavior that occurs when the Cisco UCS domain is registered or when that registration or configuration changes, depends upon several factors, including whether a domain group has been assigned or not.

The following table describes the policy resolution behavior you can expect for each type of policy.

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Call Home	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SNMP configuration	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
HTTP	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Telnet	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
CIM XML	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Management interfaces monitoring policy	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Power allocation policy	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Power policy (also known as the PSU policy)	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SEL policy	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Authentication Domains	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
LDAP	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
LDAP provider groups and group maps	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
TACACS, including provider groups	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
RADIUS, including provider groups	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SSH (Read-only)	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
DNS	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Time zone	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Web Sessions	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Fault	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Core Export	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Syslog	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Global Backup/Export Policy	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Default Authentication	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Console Authentication	Domain group root	Assigned domain group	Local	Can be local or remote	Retains last known policy state	Converted to a local policy
Roles	Domain group root	Assigned domain group	Local	Local/Combine (Remote replacing Local)	Deletes remote policies	Converted to a local policy
Locales - Org Locales	Domain group root	Assigned domain group	Local	Local/Combine (Remote replacing Local)	Deletes remote policies	Converted to a local policy
Trust Points	Domain group root	Assigned domain group	Local	Local/Combine (Remote replacing Local)	Deletes remote policies	Converted to a local policy
Firmware Download Policy	Domain group root	N/A	N/A	N/A	N/A	N/A
ID Soaking Policy	Domain group root	N/A	N/A	N/A	N/A	N/A
Locales - Domain Group Locales	Domain group root	N/A	N/A	N/A	N/A	N/A
Infrastructure Firmware Packs	N/A	Assigned domain group	Local	Local/Remote (if Remote exists)	Retains last known policy state	Converted to a local policy
Catalog	N/A	Assigned domain group	Local	Local/Remote (if Remote exists)	Retains last known policy state	Converted to a local policy

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 6	See Consequences of Service Profile Changes on Policy Resolution, on page 6	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 6	See Consequences of Service Profile Changes on Policy Resolution, on page 6	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 6	See Consequences of Service Profile Changes on Policy Resolution, on page 6	Deletes remote policies	Converted to a local policy

Consequences of Service Profile Changes on Policy Resolution

For certain policies, the policy resolution behavior is also affected by whether or not one or more service profiles that include that policy have been updated.

The following table describes the policy resolution behavior you can expect for those policies.

Policy	Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Domain Group Assigned after Registration with Cisco UCS Central
	Domain Group Unassigned / Domain Group Assigned		
	Service Profile not Modified	Service Profile Modified	
Maintenance Policy **Note** If you are using a global maintenance policy in a local service profile, all pending activities must be acknowledged on the Cisco UCS Central **Pending Activities** page.	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Schedule	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Host Firmware Packages	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

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.

Creating or Editing a Boot Policy

Step 1 In the Task bar, type **Create Boot Policy** and press Enter.
This launches the **Create Boot Policy** dialog box.

Step 2 Choose the organization from the drop-down list, and then enter a unique name and optional description for the policy.

Step 3 (Optional) 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 (Optional) 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 Click the **Boot Order** icon and perform the following:

a) Click the **Add** button to add boot options.
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 7 Click **Save**.

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, do the following:

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.

Related Topics

Basic BIOS Settings, on page 10
Processor BIOS Settings, on page 12
Intel Directed I/O BIOS Settings, on page 17
RAS Memory BIOS Settings, on page 19
USB BIOS Settings, on page 20
PCI BIOS Settings, on page 22
Boot Options BIOS Settings, on page 28
Server Manager, on page 30
Console , on page 32
Default BIOS Settings, on page 10
Basic BIOS Settings, on page 10
Boot Options BIOS Settings, on page 28
Console , on page 32
Intel Directed I/O BIOS Settings, on page 17
PCI BIOS Settings, on page 23
Processor BIOS Settings, on page 12
RAS Memory BIOS Settings, on page 19
Server Manager, on page 30
USB BIOS Settings, on page 20

Creating or Editing a BIOS Policy

Step 1 In the Task bar, type **Create BIOS Policy** and press Enter.
This launches the **Create BIOS Policy** dialog box.

Step 2 In **Basic**, click **Organization** and select the location in which you want to create the BIOS 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 10.

Step 3 In **Processor**, complete the fields as necessary.
For more information, see Processor BIOS Settings, on page 12.

Step 4 In **I/O**, complete the fields as necessary.
For more information, see Intel Directed I/O BIOS Settings, on page 17.

Step 5 In **RAS Memory**, complete the fields as necessary.
For more information, see RAS Memory BIOS Settings, on page 19.

Step 6 In **USB**, complete the fields as necessary.

For more information, see USB BIOS Settings, on page 20.

Step 7 In **PCI**, complete the fields as necessary.
For more information, see PCI BIOS Settings, on page 23.

Step 8 In **Boot Options**, complete the fields as necessary.
For more information, see Boot Options BIOS Settings, on page 28.

Step 9 In **Server Manager**, complete the fields as necessary.
For more information, see Server Manager, on page 30.

Step 10 In **Console**, complete the fields as necessary.
For more information, see Console , on page 32.

Step 11 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.
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.

Name	Description
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.
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.

Processor BIOS Settings

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

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: • **disabled—**The processor does not increase its frequency automatically. • **enabled—**The processor uses Turbo Boost Technology if required. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Enhanced Intel Speedstep	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **disabled—**The processor never dynamically adjusts its voltage or frequency. • **enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
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: • **disabled—**The processor does not permit hyperthreading. • **enabled—**The processor allows for the parallel execution of multiple threads. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

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

Name	Description
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: • **disabled—**Data from I/O devices is not placed directly into the processor cache. • **enabled—**Data from I/O devices is placed directly into the processor cache. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Processor C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Processor C1E	Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server. This can be one of the following: • **disabled—**The CPU continues to run at its maximum frequency in the C1 state. • **enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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

Name	Description
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Max Variable MTRR Setting	Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following: • **auto-max—**BIOS uses the default value for the processor. • **8—**BIOS uses the number specified for the variable MTRR. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Intel Directed I/O BIOS Settings

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

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

Name	Description
Pass Through DMA Support	Whether the processor supports Intel VT-d Pass-through DMA. You can select one of the following options: • **disabled**—The processor does not support pass-through DMA. • **enabled**—The processor uses VT-d Pass-through DMA as required. • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

RAS Memory BIOS Settings

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

Name	Description
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **disabled**—The BIOS does not support NUMA. • **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. • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **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. • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
DRAM Refresh Rate	The refresh interval rate for internal memory. This can be one of the following: • **1x** • **2x** • **3x** • **4x** • **auto** • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory RAS Config	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **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. • **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

USB BIOS Settings

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

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**
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.

Name	Description
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.

PCI BIOS Settings

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

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.

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 1: 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 2: 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 3: 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.

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: • **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. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **disabled—**The software RAID controller is not available. • **enabled—**The software RAID controller is available. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID	Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following: • **disabled—**The Intel SAS Entry RAID Module is disabled. • **enabled—**The Intel SAS Entry RAID Module is enabled. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID Module	How the Intel SAS Entry RAID Module is configured. This can be one of the following: • **it-ir-raid—**Configures the RAID module to use Intel IT/IR RAID. • **intel-esrtii—**Configures the RAID module to use Intel Embedded Server RAID Technology II. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.

Server Manager

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: • **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**. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
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: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This feature requires either operating system support or Intel Management software.
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This option is only available if you enable the OS Boot Watchdog Timer.

Console

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: • **disabled—**The serial port enabled for console redirection is hidden from the legacy operating system. • **enabled—** The serial port enabled for console redirection is visible to the legacy operating system. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **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: • **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. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **pc-ansi—**The PC-ANSI terminal font is used. • **vt100—**A supported vt100 video terminal and its character set are used. • **vt100-plus—**A supported vt100-plus video terminal and its character set are used. • **vt-utf8—**A video terminal with the UTF-8 character set is used. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.

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: • **none—**No flow control is used. • **rts-cts—**RTS/CTS is used for flow control. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.

Ethernet Adapter Policy

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

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

Operating System Specific Adapter Policies

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

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

If you are creating an Ethernet adapter policy (instead of using the default Windows adapter policy) for a Windows operating system, you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues
Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9

Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating and Editing an Ethernet Adapter Policy

Step 1 In the Task bar, type **Create Ethernet Adapter Policy** and press Enter.
This launches the **Create Ethernet Adapter Policy** dialog box.

Step 2 In **Basic**, from the **Organization** drop-down list, select the location in which you want to create the ethernet adapter policy.

Step 3 Enter the **Name** and optional **Description**.

Step 4 In **Resources**, complete the following:

a) In **Transmit Queues**, enter the number of transmit queue resources to allocate.
b) In **Transmit Queue Ring Size**, enter the number of descriptors in each transmit queue.
c) In **Receive Queues**, enter the number of receive queue resources to allocate.
d) In **Receive Queues Ring Size**, enter the number of descriptors in each receive queue.
e) In **Completion Queues**, enter the number of completion queue resources to allocate. In general, the number of completion queue resources you allocate should be equal to the number of transmit queue resources, plus the number of receive queue resources.
f) In **Interrupts**, enter the number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources.

Step 5 In **Settings**, complete the following:

a) Choose whether to enable **Transmit Checksum Offloading**, **Receive Checksum Offloading**, **TCP Segmentation Offloading**, and **Large TCP Receive Offloading**.
b) Select an **Interrupt Mode**.
c) Enter the **Interrupt Timer** value in microseconds.
d) Select the **Interrupt Coalescing Type**.
e) Enter the **Failback Timeout** in seconds.

Step 6 Click **Create**.

IPMI Access Profile

The IPMI access profile policy allows you to determine whether the IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the 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.

Step 1 In the Task bar, type **Create IPMI Access Profile Policy** and press Enter.
This launches the **Create IPMI Access Profile Policy** dialog box.

Step 2 In **Basic**, click **Organization** and select the location in which you want to create the policy.

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

Step 4 (Optional) In **IPMI Users**, select an IPMI user name, enter a password, and confirm the password.

Step 5 Select whether to allow read only or admin **Serial over LAN Access**.

Step 6 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

Step 1 In the Task bar, type **Create Serial Over LAN (SOL) Policy** and press Enter.
This launches the **Create Serial Over LAN (SOL) Policy** dialog box.

Step 2 Click **Organization** and select the location 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 **Enable** to allow the serial over LAN connection.

Step 6 Click **Create**.

Deleting a Serial over LAN Policy

Before You Begin

Step 1 On the **show search tables** bar, click **Policies**.
You can view the polices at an organization or sub-organization level from the **Show Org Navigation** bar by expanding the root node until you reach the applicable organization name. Click **Go to All Policies Table** from the **root organization** page.

This launches the **All Policies** page.

Step 2 Search the policy that you want to delete.
You can search for the policy in one of the following ways:

- Browse through the list of policies.
- Click **Search** icon and enter the policy name.
- Select **Serial Over LAN** from the **Filter** column.

Step 3 In the **Org** column, click the policy.
This launches the selected **SOL policy** page.

Step 4 On the **SOL policy** page, click the **Delete** icon.
A dialog box prompting you to confirm the deletion of the policy appears.

Step 5 Click **Delete**.

What to Do Next

Dynamic vNIC Connection Policy

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Note Server Migration:

- If you migrate a server that is configured with dynamic vNICs or another migration tool, the dynamic interface used by the vNICs fails and Cisco UCS Central notifies you of that failure.
- When the server comes back up, Cisco UCS Central assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating or Editing a Dynamic vNIC Connection Policy

Step 1 In the Task bar, type **Create Dynamic vNIC Connection Policy** and press Enter.
This launches the **Create Dynamic vNIC Connection Policy** dialog box.

Step 2 Click **Organization** and select the location in which you want to create the dynamic vNIC connection policy.

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

Step 4 Enter the number of dynamic vNICS that you want to create.

Step 5 Select the protection mode that you want to use.

Step 6 Select the adapter profile to be associated with this policy.
The profile must already exist to be included in the **Ethernet Adapter** drop-down list.

Step 7 Click **Create**.

Fibre Channel Adapter Policy

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

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

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

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

Operating System Specific Adapter Policies

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

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

Creating or Editing a Fibre Channel Adapter Policy

Step 1 In the Task bar, type **Create Fibre Channel Adapter Policy** and press Enter.
This launches the **Create Fibre Channel Adapter Policy** dialog box.

Step 2 In **Basic**, click **Organization** and select the location in which you want to create this policy.

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

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

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

Step 6 Click **Create**.

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).

Creating or Editing a Host Firmware Package Policy

Step 1 In the Task bar, type **Create Host Firmware Package Policy** and press Enter.
This launches the **Create Host Firmware Package Policy** dialog box.

Step 2 Click **Organization** and select the location in which you want to create the policy.

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

Step 4 Select the **Blade Version**, **Rack Version**, and/or **Modular Version**, as required for your environment.

Step 5 Click **Create**.

Host Interface Placement Policy

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

To create a host interface placement policy, see Creating or Editing a Host Interface Placement Policy, on page 40. Details for existing policies are displayed on the **Host Interface Placement Policy** page.

Creating or Editing a Host Interface Placement Policy

Step 1 In the Task bar, type **Create Host Interface Placement Policy** and press Enter.
This launches the **Create Host Interface Placement Policy** dialog box.

Step 2 Click **Organization** and select the location in which you want to create the policy.

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

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

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

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

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

Step 6 Click **Create**.

iSCSI Adapter Policy

Creating or Editing an iSCSI Adapter Policy

Step 1 In the Task bar, type **Create iSCSI Adapter Policy** and press Enter.
This launches the **Create iSCSI Adapter Policy** dialog box.

Step 2 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 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

Step 1 In the Task bar, type **Create iSCSI Authentication Profile** and press Enter.
This launches the **Create iSCSI Authentication Profile** dialog box.

Step 2 In **Basic**, 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 Enter the **User ID**.

Step 5 Type and confirm the password.

Step 6 Click **Create**.

LAN Connectivity Policy

LAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

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

Creating or Editing a LAN Connectivity Policy

Step 1 In the Task bar, type **Create LAN Connectivity Policy** and press Enter.
This launches the **Create LAN Connectivity Policy** dialog box.

Step 2 In **Basic**, 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 In **vNICs**, enter the **vNIC** and enter the appropriate properties values.

Step 5 In **iSCSI vNICs**, enter the **iSCSI vNIC** and enter the appropriate properties values.

Note If you create a LAN Connectivity Policy in the HTML5 GUI, any iSCSI vNIC parameters that you set on the iSCSI vNICS in the policy can only be updated in the HTML5 GUI.

Step 6 Click **Create**.

Local Disk Policy

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

The local disk modes include the following:

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

Creating or Editing a Local Disk Policy

Step 1 In the Task bar, type **Create Local Disk Policy** and press Enter.

This launches the **Create Local Disk Policy** dialog box.

Step 2 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 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**.

Maintenance Policy

When you make any change to a service profile that is associated with servers in the registered domains, the change may require a server reboot. The maintenance policy determines how Cisco UCS Central reacts to the reboot request.

You can create a maintenance policy and specify the reboot requirements to make sure the server is not automatically rebooted with any changes to the service profiles. You can specify one of the following options for a maintenance policy:

- **Immediately**: Whenever you make a change to the service profile, apply the changes immediately.
- **User Acknowledgment**: Apply the changes after a user with administrative privileges acknowledges the changes in the system.
- **Schedule**: Apply the changes based on the day and time you specify in the schedule.

When you create the maintenance policy if you specify a schedule, the schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

Creating or Editing a Maintenance Policy

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

This launches the **Create Maintenance Policy** dialog box.

Step 2 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 when to apply the changes that require a reboot.
This can be one of the following:

- **User Acknowledgement**—Configuration changes must be acknowledged by the user, and reboots must be confirmed.
- **Schedule**—Configuration changes are applied depending on the schedule you select. To add a new schedule to the list of values, see Creating or Editing a Schedule, on page 44.
- **Save**—Configuration changes are applied immediately on save and cause a reboot.

Step 5 Click **Create**.

Creating or Editing a Schedule

Note Simple schedules, whether recurring or a one time occurrence, do not have the option to require user acknowledgment. If you want to require user acknowledgment, you must choose an advanced schedule.

Step 1 In the Task bar, type **Create Schedule** and press Enter.
This launches the **Create Schedule** dialog box.

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

Step 3 Choose whether the schedule should be **Recurring**, **One Time**, or **Advanced**.
If **Advanced**, choose whether to require user acknowledgment.

Step 4 In **Schedule**, complete the following:

a) For **Recurring** schedules, select the start date, frequency, time, and other properties.
b) For **One Time** schedules, select the start date, time, and other properties.
c) For **Advanced** schedules, enter a name for the schedule, choose whether to use a one time or recurring schedule, and select values for the other properties.

Step 5 Click **Create**.

Network Control Policy

This policy configures the network control settings for the Cisco UCS domain, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the virtual interface (VIF) behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Central takes on the remote Ethernet interface, vEthernet interface , or vFibre Channel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Central to bring the vEthernet or vFibre Channel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default behavior directs Cisco UCS Central to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibre Channel interfaces that are bound to the remote Ethernet interface are brought down as well.

Note if your implementation includes those types of non-VM-FEX capable converged network adapters mentioned in this section and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Note that this configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

MAC addresses are installed only on the native VLAN by default, which maximizes the VLAN port count in most implementations.

Note If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating or Editing a Network Control Policy

Step 1 In the Task bar, type **Create Network Control Policy** and press Enter.
This launches the **Create Network Control Policy** dialog box.

Step 2 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 Choose whether to enable **Cisco Discovery Protocol (CDP)**.

Step 5 Select values for **Action on Uplink Failure**, **MAC Address Registration**, and **MAC Address Forging**.

Step 6 Click **Create**.

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

Step 1 In the Task bar, type **Create Power Control Policy** and press Enter.
This launches the **Create Power Control Policy** dialog box.

Step 2 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 Choose whether to enable **Power Capping**.

Step 5 If **Enabled**, use the slider to select 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 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

Step 1 In the Task bar, type **Create Quality of Service (QOS) Policy** and press Enter.
This launches the **Create Quality of Service (QOS) Policy** dialog box.

Step 2 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.

- In the Egress area, choose a Priority, enter the Burst(Bytes) and Rate(Kbps), and choose the Host Control.

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**.

SAN Connectivity Policy

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

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

Creating or Editing a SAN Connectivity Policy

Step 1 In the Task bar, type **Create SAN Connectivity Policy** and press Enter.
This launches the **Create SAN Connectivity Policy** dialog box.

Step 2 In **Basic**, 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 In **Identifiers**, choose the WWNN pool.
For more information, see Creating and Editing a WWN Pool.

Step 5 In **vHBAs**, create one or more vHBAs and select the properties.
You can manually create the vHBA or use a vHBA template.

Step 6 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

Step 1 In the Task bar, type **Create Scrub Policy** and press Enter.
This launches the **Create Scurb Policy** dialog box.

Step 2 In **Basic**, 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 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.

Step 1 In the Task bar, type **Create vMedia Policy** and press Enter.
This launches the **Create vMedia Policy** dialog box.

Step 2 In **Basic**, click **Organization** and select the location in which you want to create this vMedia 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.

Call Home Policies

Cisco UCS Central supports global call home policies for notifying all email recipients defined in call home profiles to specific Cisco UCS Manager events. (There is no call home support for Cisco UCS Central in this release.) Profiles define lists of email recipients that receive alert notifications (to a maximum defined message size in full text, short text, or XML format) and alert criteria for triggering notifications.

Alert notifications are sent with predefined content based on alert levels (including major, minor, normal, notification and warning) and selected alert groups identifying events that trigger notification (such as diagnostic, environmental, inventory, license and other predefined events). Individual email recipients may be individually added to existing profiles. Registered Cisco UCS domains choosing to define security policies globally within that client's policy resolution control will defer all call home policies to its registration with Cisco UCS Central.

Configuring Call Home

A call home policy is created from a domain group under the domain group root. Call home policies under the Domain Groups root were already created by the system and ready to configure.

SUMMARY STEPS

1. Navigate to the **Domain Group** page.
2. Click the **Settings** icon and select **Call Home Settings**.
3. In **Basic**, click Enabled to enable the Call Home feature, and complete the necessary information.
4. In **Profiles**, click **Add** to create a new profile, or edit an existing profile.
5. In **Alerts**, click **Add** or **Delete** to manage the events that trigger alerts to be sent.
6. Click **Save**.

DETAILED STEPS

Step 1 Navigate to the **Domain Group** page.

Step 2 Click the **Settings** icon and select **Call Home Settings**.

Step 3 In **Basic**, click Enabled to enable the Call Home feature, and complete the necessary information.

Step 4 In **Profiles**, click **Add** to create a new profile, or edit an existing profile.

Step 5 In **Alerts**, click **Add** or **Delete** to manage the events that trigger alerts to be sent.

Step 6 Click **Save**.