Configuring Server-Related Policies

This chapter includes the following sections:

- Configuring BIOS Settings, page 1
- CIMC Security Policies, page 50
- Configuring Local Disk Configuration Policies, page 55
- Configuring Scrub Policies, page 66
- Configuring DIMM Error Management, page 69
- Configuring Serial over LAN Policies, page 71
- Configuring Server Autoconfiguration Policies, page 74
- Configuring Server Discovery Policies, page 76
- Configuring Server Inheritance Policies, page 78
- Configuring Server Pool Policies, page 80
- Configuring Server Pool Policy Qualifications, page 82
- Configuring vNIC/vHBA Placement Policies, page 95
- CIMC Mounted vMedia, page 105

Configuring BIOS Settings

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in an Cisco UCS domain. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enable you to fine tune the BIOS settings for a server managed by Cisco UCS Manager.

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS domain, or you can use only one of them. You can also use Cisco UCS Manager to view the actual BIOS settings on a server and determine whether they are meeting current needs.

Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Main 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 **set reboot-on-update**	When the server is rebooted after you change one or more BIOS settings. **yes—**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. **no—**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.
Quiet Boot **set quiet-boot-config quiet-boot**	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Post Error Pause **set post-error-pause-config post-error-pause**	What happens when the server encounters a critical error during POST. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Resume Ac On Power Loss **set resume-ac-on-power-loss-config resume-action**	How the server behaves when power is restored after an unexpected power loss. This can be one of the following: • **stay-off—**The server remains off until manually powered on. • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Front Panel Lockout **set front-panel-lockout-config 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: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Consistent Device Naming **set consistent-device-name-control cdn-name**	Consistent Device Naming allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made. Whether consistent device naming is enabled or not. This can be one of the following: • **disabled—**Consistent device naming is disabled for the BIOS policy. • **enabled—**Consistent device naming is enabled for the BIOS policy. This enables Ethernet interfaces to be named consistently. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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 **set intel-turbo-boost-config 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 **set enhanced-intel-speedstep-config 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: • **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 **set hyper-threading-config 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 **set core-multi-processing-config 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 **set execute-disable 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) **set intel-vt-config 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
Hardware Pre-fetcher **set processor-prefetch-config hardware-prefetch**	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** **CPUPerformance** 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.
Adjacent Cache Line Pre-fetcher **set processor-prefetch-config adjacent-cache-line-prefetch**	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** **CPUPerformance** 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.
DCU Streamer Pre-fetch **set processor-prefetch-config dcu-streamer-prefetch**	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.

Name	Description
DCU IP Pre-fetcher **set processor-prefetch-config dcu-ip-prefetch**	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.
Direct Cache Access **set direct-cache-access-config 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 **set processor-c-state-config 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.

Name	Description
Processor C1E **set processor-c1e-config 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.
Processor C3 Report **set processor-c3-report-config 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 **set processor-c6-report-config 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.

Name	Description
Processor C7 Report **set processor-c7-report-config 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.
CPU Performance **set cpu-performance-config 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.
Max Variable MTRR Setting **set max-variable-mtrr-setting-config processor-mtrr**	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.
Local X2 APIC **set local-x2-apic-config**	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.

Name	Description
Power Technology **set processor-energy-config cpu-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 **set processor-energy-config 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** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Frequency Floor Override **set frequency-floor-override-config cpu-frequency**	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.
P-STATE Coordination **set p-state-coordination-config p-state**	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** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
DRAM Clock Throttling **set dram-clock-throttling-config dram-clock-throttling**	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Channel Interleaving **set interleave-config channel-interleave**	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 **set interleave-config rank-interleave**	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
Demand Scrub **set set scrub-policies config 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: • **Disabled—** Single bit memory errors are not corrected. • **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Patrol Scrub **set scrub-policies config 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: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Altitude **set altitude altitude-config**	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.

Name	Description
Package C State Limit **set package-c-state-limit-config package-c-state-limit**	The amount of power available to the server components when they are idle. This can be one of the following: • **no-limit—**The server may enter any available C state. • **c0—**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—**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. • **c3—**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—**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. • **c2—**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. • **c7—**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—**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. • **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
VT for Directed IO **set intel-vt-directed-io-config vtd**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **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 **set intel-vt-directed-io-config interrupt-remapping**	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **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 **set intel-vt-directed-io-config coherency-support**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **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.
ATS Support **set intel-vt-directed-io-config ats-support**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **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 **set intel-vt-directed-io-config passthrough-dma**	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **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
Memory RAS Config **set memory-ras-config 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.

Name	Description
NUMA **set numa-config numa-optimization**	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.
Mirroring Mode **set memory-mirroring-mode mirroring-mode**	Memory mirroring enhances system reliability by keeping two identical data images in memory. This option is only available if you choose the **mirroring** option for **Memory RAS Config**. It can be one of the following: • **inter-socket—**Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • **intra-socket—**One IMC is mirrored with another IMC in the same socket. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Sparing Mode **set memory-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 **sparing** option for **Memory RAS Config**. It can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
LV DDR Mode **set lv-dimm-support-config 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.
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.
DDR3 Voltage Selection **set Ddr3VoltageSelection**	The voltage to be used by the dual-voltage RAM. This can be one of the following: • **DDR3-1500mv** • **DDR3-1350mv** • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Serial Port BIOS Settings

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

Name	Description
Serial Port A **set serial-port-a-config serial-port-a**	Whether serial port A is enabled or disabled. This can be one of the following: • **disabled—**The serial port is disabled. • **enabled—**The serial port is enabled. • **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 **set usb-boot-config make-device-non-bootable**	Whether the server can boot from a USB device. This can be one of the following: • **disabled—**The server can boot from a USB device. • **enabled—**The server cannot boot from a USB device. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Legacy USB Support **set LegacyUSBSupport**	Whether the system supports legacy USB devices. This can be one of the following: • **disabled—**USB devices are only available to EFI applications. • **enabled—**Legacy USB support is always available. • **auto—**Disables legacy USB support if no USB devices are connected. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
USB System Idle Power Optimizing Setting **set usb-system-idle-power-optimizing-setting-config usb-idle-power-optimizing**	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: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Front Panel Access Lock **set usb-front-panel-access-lock-config usb-front-panel-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: • **disabled** • **enabled** • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Port 60/64 Emulation **set UsbEmul6064**	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
USB Port:Front **set UsbPortFront**	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Port:Internal **set UsbPortInt**	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Port:KVM **set UsbPortKVM**	Whether the KVM ports are enabled or disabled. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
USB Port:Rear **set UsbPortRear**	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Port:SD Card **set UsbPortSdCard**	Whether the SD card drives are enabled or disabled. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Port:VMedia **set UsbPortVMedia**	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the vMedia devices. • **Enabled—**Enables the vMedia devices. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
All USB Devices **set AllUsbDevices**	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled—**All USB devices are disabled. • **Enabled—**All USB devices are enabled. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

PCI Configuration BIOS Settings

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

Name	Description
Max Memory Below 4G **set max-memory-below-4gb-config max-memory**	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: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory Mapped IO Above 4Gb Config **set memory-mapped-io-above-4gb-config memory-mapped-io**	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: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
VGA Priority **set VGAPriority**	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.
ASPM Support **set ASPMSupport**	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **disabled—**ASPM support is disabled in the BIOS. • **auto—**The CPU determines the power state. • **force l0—**Force all links to L0 standby (L0s) state. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

QPI BIOS Settings

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

Name	Description
QPI Link Frequency **set qpi-link-frequency-select-config qpi-link-freqency-mt-per-sec**	The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s). This can be one of the following: • **6400** • **7200** • **8000** • **Auto—**The CPU determines the QPI link frequency. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
QPI Snoop Mode **set vfqpisnoopmode vpqpisnoopmode**	This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

LOM and PCIe Slots 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
PCIe Slot:SAS OptionROM **set slot-option-rom-enable-config pcie-sas**	Whether Option ROM is available on the SAS port. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Slot:*n* Link Speed **set slot-link-speed config pcie-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: • **gen1—**2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **gen2—**5GT/s is the maximum speed allowed. • **gen3—**8GT/s is the maximum speed allowed. • **auto—**The maximum speed is set automatically. • **disabled—**The maximum speed is not restricted. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Slot:*n* OptionROM **set slot-option-rom-enable-config slot*n*-option-rom-enable**	Whether Option ROM is available on the port. This can be one of the following: • **Disabled—**The slot is not available. • **Enabled—**The slot is available. • **UEFI_Only—**The slot is available for UEFI only. • **Legacy_Only—**The slot is 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.

Name	Description
PCIe Slot:HBA OptionROM **set slot-option-rom-enable-config pcie-hba**	Whether Option ROM is available on the HBA port. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Slot:MLOM OptionROM **set slot-option-rom-enable-config mlom**	Whether Option ROM is available on the MLOM port. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Slot:N1 OptionROM **set slot-option-rom-enable-config n1**	Whether Option ROM is available on the port. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
PCIe Slot:N2 OptionROM **set slot-option-rom-enable-config n2**	Whether Option ROM is available on the port. This can be one of the following: • **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. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe OptionROMs **set option-rom-enable-config option-rom-enable**	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 **set slot-option-rom-enable-config mezz-slot-option-rom-enable**	Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
All PCI Onboard LOM Ports **set lom-ports-config all-lom-ports**	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe 1G LOM 1 Link **set pcie-lom1-link**	Whether Option ROM is available on the 1G LOM port. This can be one of the following: • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe 10G LOM 2 Link **set pcie-lom2-link**	Whether Option ROM is available on the 10G LOM port. This can be one of the following: • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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 **set boot-option-retry-config 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 for this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID **set intel-entry-sas-raid-config 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 for this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID Module **set intel-entry-sas-raid-config 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 for this attribute contained in the BIOS defaults for the server type and vendor.
Onboard SCU Storage Support **set onboard-sas-storage-config onboard-sas-ctrl**	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 for this attribute contained in the BIOS defaults for the server type and vendor.

Server Management BIOS Settings

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

General Settings

Name	Description
Assert Nmi on Serr **set assert-nmi-on-serr-config assertion**	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 **set assert-nmi-on-perr-config assertion**	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 **set os-boot-watchdog-timer-config 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 Policy **set os-boot-watchdog-timer-policy-config os-boot-watchdog-timer-policy**	What action the system takes if the watchdog timer expires. This can be one of the following: • **power-off—**The server is powered off if the watchdog timer expires during OS boot. • **reset—**The server is reset if the watchdog timer expires during OS 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.

Name	Description
OS Boot Watchdog Timer Timeout **set os-boot-watchdog-timer-timeout-config 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.
FRB-2 Timer **set FRB-2**	Whether the FRB-2 timer is used to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB-2 timer is not used. • **Enabled—**The FRB-2 timer is started during POST and used to recover the system if necessary. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Console Redirection Settings

Name	Description
Console Redirection **set console-redir-config console-redir**	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.
Flow Control **set console-redir-config 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.

Name	Description
BAUD Rate **set console-redir-config 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 **set console-redir-config 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.
Legacy OS Redirect **set console-redir-config legacy-os-redir**	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.

Name	Description
Putty KeyPad **set PuttyFunctionKeyPad**	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: • **VT100—**The function keys generate ESC OP through ESC O[. • **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. • **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. • **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 [{. • **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~. • **VT400—**The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS. • **platform-default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

BIOS Policy

The BIOS policy is a policy that 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 Manager.

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 Manager 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.

Default BIOS Settings

Cisco UCS Manager 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 Manager 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 Manager. 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.

Creating a BIOS Policy

Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters org mode for the specified organization. To enter the default org mode, type / as the *org-name* .
Step 2	UCS-A /org # **create bios-policy** *policy-name*	Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.
Step 3	Configure the BIOS settings.	For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topics: • **Main** page: Main BIOS Settings, on page 2 • **Processor** page: Processor BIOS Settings, on page 4

	Command or Action	Purpose
		• **Intel Directed IO** page: Intel Directed I/O BIOS Settings, on page 15 • **RAS Memory** page: RAS Memory BIOS Settings, on page 17 • **Serial Port** page: Serial Port BIOS Settings, on page 19 • **USB** page: USB BIOS Settings, on page 20 • **PCI Configuration** page: PCI Configuration BIOS Settings, on page 24 • **Boot Options** page: Boot Options BIOS Settings, on page 30 • **Server Management** page: Server Management BIOS Settings, on page 32
Step 4	UCS-A /org/bios-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a BIOS policy under the root organization and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create bios-policy biosPolicy3
UCS-A /org/bios-policy* # set numa-config numa-optimization enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org/bios-policy #
```

Modifying BIOS Defaults

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

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.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope server-defaults**	Enters server defaults mode.
Step 3	UCS-A /system/server-defaults # **show platform**	(Optional) Displays platform descriptions for all servers.
Step 4	UCS-A /system/server-defaults # **scope platform** *platform-description*	Enters server defaults mode for the server specified. For the *platform-description* argument, enter the server description displayed by the **show platform**

	Command or Action	Purpose
		command using the following format: "*vendor*" *model revision*. **Tip** You must enter the vendor exactly as shown in the **show platform** command, including all punctuation marks.
Step 5	UCS-A /system/server-defaults/platform # **scope bios-settings**	Enters server defaults BIOS settings mode for the server.
Step 6	Reconfigure the BIOS settings.	For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topics: • **Main** page: Main BIOS Settings, on page 2 • **Processor** page: Processor BIOS Settings, on page 4 • **Intel Directed IO** page: Intel Directed I/O BIOS Settings, on page 15 • **RAS Memory** page: RAS Memory BIOS Settings, on page 17 • **Serial Port** page: Serial Port BIOS Settings, on page 19 • **USB** page: USB BIOS Settings, on page 20 • **PCI Configuration** page: PCI Configuration BIOS Settings, on page 24 • **Boot Options** page: Boot Options BIOS Settings, on page 30 • **Server Management** page: Server Management BIOS Settings, on page 32
Step 7	UCS-A /system/server-defaults/platform/bios-settings # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to change the NUMA default BIOS setting for a platform and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope server-defaults
UCS-A /system/server-defaults # show platform

Platform:
    Product Name Vendor     Model      Revision
    ------------ ---------- ---------- --------
    Cisco B200-M1
                 Cisco Systems, Inc.
                            N20-B6620-1
```

```
                                                0

UCS-A /system/server-defaults # scope platform "Cisco Systems, Inc." N20-B6620-1 0
UCS-A /system/server-defaults/platform # scope bios-settings
UCS-A /system/server-defaults/platform/bios-settings # set numa-config numa-optimization
disabled
UCS-A /system/server-defaults/platform/bios-settings* # commit-buffer
UCS-A /system/server-defaults/platform/bios-settings #
```

Viewing the Actual BIOS Settings for a Server

Follow this procedure to see the actual BIOS settings on a server.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope bios**	Enters BIOS mode for the specified server.
Step 3	UCS-A /chassis/server/bios # **scope bios-settings**	Enters BIOS settings mode for the specified server.
Step 4	UCS-A /chassis/server/bios/bios-settings # **show** *setting*	Displays the BIOS setting. Enter **show ?** to display a list of allowed values for *setting* .

The following example displays a BIOS setting for blade 3 in chassis 1:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope bios
UCS-A /chassis/server/bios # scope  bios-settings
UCS-A /chassis/server/bios/bios-settings # show intel-vt-config

Intel Vt Config:
    Vt
    --
    Enabled

UCS-A /chassis/server/bios/bios-settings #
```

Configuring Trusted Platform Module

Trusted Platform Module

The Trusted Platform Module (TPM) is a component that can securely store artifacts that are used to authenticate the server. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. It is a requirement for the Intel Trusted Execution Technology (TXT) security feature, which

must be enabled in the BIOS settings for a server equipped with a TPM. Cisco UCS M4 blade and rack-mount servers include support for TPM. TPM is enabled by default on these servers.

Important

- If you upgrade Cisco UCS Manager to Release 2.2(4), TPM is enabled.
- When TPM is enabled and you downgrade Cisco UCS Manager from Release 2.2(4), TPM is disabled.

Intel Trusted Execution Technology

Intel Trusted Execution Technology (TXT) provides greater protection for information that is used and stored on the business server. A key aspect of that protection is the provision of an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data, invisible to the rest of the system. Intel TXT provides for a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code. Cisco UCS M4 blade and rack-mount servers include support for TXT. TXT is disabled by default on these servers.

TXT can be enabled only after TPM, Intel Virtualization technology (VT) and Intel Virtualization Technology for Directed I/O (VTDio) are enabled. When you only enable TXT, it implicitly enables TPM, VT, and VTDio also.

Configuring Trusted Platform

Cisco UCS M4 blade and rack-mount servers include support for TPM and TXT. UCS Manager Release 2.2(4) allows you to perform the following operations on TPM and TXT:

- Enabling or Disabling TPM, on page 42
- Enabling or Disabling TXT, on page 43
- Clearing TPM for a Blade Server or Clearing TPM for a Rack-Mount Server

Note For Cisco UCS M3 blade servers, press **F2** to enter the BIOS setup menu and change the settings.

Enabling or Disabling TPM

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **create bios-policy** *policy-name*	Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.

	Command or Action	Purpose
Step 3	UCS-A /org/bios-policy* # **set trusted-platform-module-config tpm-support** {**enabled** | **disabled** | **platform-default**}	Specifies whether TPM is **enabled** or **disabled**. **platform-default** is TPM enabled.
Step 4	UCS-A /org/bios-policy* # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /org # **create service-profile** *sp-name*}	Creates the service profile specified and enters service profile configuration mode.
Step 6	UCS-A /org/service-profile* # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile.
Step 7	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.
Step 8	UCS-A /org/service-profile # **associate server** *chassis-id / slot-id*	Associates the service profile with a single server.

The following example shows how to enable TPM:

```
UCS-A # scope org
UCS-A /org # create bios-policy bp1
UCS-A /org/bios-policy* # set trusted-platform-module-config tpm-support enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org # create service-profile sp1
UCS-A /org/service-profile* # set bios-policy bp1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # associate server 1/2
```

Enabling or Disabling TXT

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **create bios-policy** *policy-name*	Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.
Step 3	UCS-A /org/bios-policy* # **set intel-trusted-execution-technology-config txt-support** {**enabled** | **disabled** | **platform-default**}	Specifies whether TXT is **enabled** or **disabled**. **platform-default** is TXT disabled.

	Command or Action	Purpose
Step 4	UCS-A /org/bios-policy* # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /org # **create service-profile** *sp-name*}	Creates the service profile specified and enters service profile configuration mode.
Step 6	UCS-A /org/service-profile* # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile.
Step 7	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.
Step 8	UCS-A /org/service-profile # **associate server** *chassis-id / slot-id*	Associates the service profile with a single server.

The following example shows how to enable TXT:

```
UCS-A # scope org
UCS-A /org # create bios-policy bp1
UCS-A /org/bios-policy* # set intel-trusted-execution-technology-config txt-support enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org # create service-profile sp1
UCS-A /org/service-profile* # set bios-policy bp1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # associate server 1/2
```

Consistent Device Naming

When there is no mechanism for the Operating System to label Ethernet interfaces in a consistent manner, it becomes difficult to manage network connections with server configuration changes. Consistent Device Naming (CDN), introduced in Cisco UCS Manager Release 2.2(4), allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more persistent when adapter or other configuration changes are made.

To configure CDN for a vNIC, do the following:

- Enable consistent device naming in the BIOS policy.
- Associate the BIOS policy with a service profile.
- Configure consistent naming for a vNIC.

Guidelines and Limitations for Consistent Device Naming

- CDN is supported only on Windows 2012 R2. It is not supported on any other Operating System.
- Consistent device naming (CDN) is supported on all M3 and higher blade and rack-mount servers.
- BIOS and adapter firmware must be part of the Release 2.2(4) bundle to support CDN.

- In Cisco UCS Manager Release 2.2(4), CDN is supported only on the following adapters:
  - Cisco UCS VIC 1225 (UCSC-PCIE-CSC-02)
  - Cisco UCS MLOM 1227 (UCSC-MLOM-CSC-02)
  - Cisco UCS VIC 1225T (UCSC-PCIE-C10T-02)
  - Cisco UCS MLOM 1227T (UCSC-MLOM-C10T-02)
  - Cisco UCS VIC 1240 (UCSB-MLOM-40G-01)
  - Cisco UCS VIC 1280 (UCS-VIC-M82-8P)
  - Cisco UCS VIC 1340 (UCSB-MLOM-40G-03)
  - Cisco UCS VIC 1380 (UCSB-VIC-M83-8P)
- CDN is not supported for vNIC template and dynamic vNIC.
- Multiple vNICs within the same service profile cannot have the same CDN name.
- When a CDN name is not specified for a vNIC, the vNIC name is used as the CDN name.
- The CDN name that you configure for a vNIC appears as **Admin CDN Name**. The CDN name that is finally applied to the vNIC appears as **Oper CDN Name**. For example, if the **Admin CDN Name** for a vNIC called "vnic0" is cdn0, then the **Oper CDN Name** for this vNIC will be cdn0, but if the **Admin CDN Name** for the same vNIC is not specified, the **Oper CDN Name** will be vnic0.
- In Cisco UCS Manager Release 2.2(4), downgrade of Cisco UCS Manager is prevented if CDN is enabled in a BIOS policy that is assigned to an associated server.
- In Cisco UCS Manager Release 2.2(4), downgrade of the BIOS firmware is prevented if a CDN-enabled BIOS policy is assigned to a server.
- In Cisco UCS Manager Release 2.2(4), downgrade of the adapter firmware is prevented if a CDN-enabled BIOS policy is assigned to a server.
- When the applied BIOS policy is changed from CDN-disabled to CDN-enabled or from CDN-enabled to CDN-disabled, the host reboots with a warning, irrespective of whether reboot on BIOS update is enabled or not.
- It is recommended that you enable CDN in the BIOS policy and add CDN names to the vNICS before the Windows Operating System is installed.
- If the Windows Operating System is already installed on the server and CDN is then enabled in the BIOS policy, do the following:

  1. Uninstall the network drivers.
  2. Scan the system for hidden devices and uninstall them.
  3. Rescan the system for new hardware and install the network drivers again.

  If this is not done, the vNICs will not come up with the configured CDN names.
- When the applied BIOS policy is changed from CDN-disabled to CDN-enabled or from CDN-enabled to CDN-disabled on a service profile, do the following:

  1. Uninstall the network drivers.
  2. Scan the system for hidden devices and delete them.

3 Rescan the system for new hardware and install the network drivers again.

Note When the BIOS policy is changed from CDN-enabled to CDN-disabled, ensure that the CDN names are removed from all the vNICs on the system.

- If any change is made to the vNICs, the BDF of all the devices on the system also changes. Following are some of the scenarios that trigger a change in the BDF of all the vNICs present on the system:
  - When a vNIC is added or deleted
  - When a vNIC is moved from one adapter on the system to another adapter on the system

  When these changes are made to the system, do the following:

  1 Uninstall the network driver from all the present network interfaces.

  2 Scan the system for hidden devices and uninstall them.

  3 Rescan the system for new hardware and install the network driver on the network controllers again.

  If the hidden devices are not deleted, the CDN names of the network adapters will not appear as configured on Cisco UCS Manager.

CDN with a Mixed Set of Adapters

When a CDN name is configured for a vNIC in a system with a mixed set of CDN-supported adapters and CDN-unsupported adapters, then system placement may not place CDN-configured vNICs on adapters that support CDN.

If CDN is enabled in the BIOS policy, and system placement places a CDN-configured vNIC (Admin CDN configured) on an adapter that does not support CDN, an info fault will be raised, but the configuration issue for the service profile will be ignored.

If CDN is enabled in the BIOS policy, and system placement places a vNIC (Admin CDN not configured) on an adapter that does not support CDN, an info fault will be raised, but the configuration issue for the service profile will be ignored. The **Oper CDN Name** in this case will be empty and will not be derived from the vNIC name.

If you want to deploy the CDN name as the host network interface name for a server, you must manually place a vNIC on a supported adapter.

Enabling Consistent Device Naming in a BIOS Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.

	Command or Action	Purpose
Step 2	UCS-A /org # **create bios-policy** *policy-name*	Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.
Step 3	UCS-A /org/bios-policy* # **set consistent-device-name-control cdn-name** {**enabled** | **disabled** | **platform-default**}	Specifies whether consistent device naming (CDN) is **enabled** or **disabled**.
Step 4	UCS-A /org/bios-policy* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to enable CDN in a BIOS policy:

```
UCS-A # scope org
UCS-A /org # create bios-policy cdn-bios-policy
UCS-A /org/bios-policy* # set consistent-device-name-control cdn-name enabled
UCS-A /org/bios-policy* # commit-buffer
```

Associating a BIOS Policy with a Service Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope service-profile** *sp-name*}	Enters service profile configuration mode for the specified service profile.
Step 3	UCS-A /org/service-profile # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile.
Step 4	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to associate a CDN-enabled BIOS policy with a service profile:

```
UCS-A # scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # set bios-policy cdn-bios-policy
UCS-A /org/service-profile* # commit-buffer
```

Configuring Consistent Device Naming for a vNIC

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope service-profile** *sp-name*	Enters service profile configuration mode for the specified service profile.
Step 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	Enters vNIC configuration mode for the specified vNIC.
Step 4	UCS-A /org/service-profile/vnic # **set cdn-name** *cdn-name*	Specifies the CDN name for the vNIC.
Step 5	UCS-A /org/service-profile/vnic* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to configure CDN for a vNIC:

```
UCS-A # scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # scope vnic vn1
UCS-A /org/service-profile/vnic # set cdn-name eth0
UCS-A /org/service-profile/vnic* # commit-buffer
```

Displaying the CDN Name of a vNIC

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *server-num*	Enters server mode for the specified server.
Step 2	UCS-A /server # **scope adapter** *adapter-id*	Enters adapter mode for the specified adapter.
Step 3	UCS-A /server/adapter # **show host-eth-if** [**detail**] [**expand**]	Displays the details of the host Ethernet interface for the specified adapter.

The following example shows how to display the CDN name of a vNIC:

```
UCS-A # scope server 3
UCS-A /server # scope adapter 1
UCS-A /server/adapter # show host-eth-if detail expand
```

```
Eth Interface:
    ID: 1
    Dynamic MAC Address: 00:25:B5:00:00:99
    Burned-In MAC Address: 00:00:00:00:00:00
    Model: UCSC-PCIE-CSC-02
    Name: vnic1
    Cdn Name: cdn0
    Admin State: Enabled
    Operability: Operable
    Order: 1
```

Displaying the Status of a vNIC

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope service-profile** *sp-name*	Enters service profile configuration mode for the specified service profile.
Step 3	UCS-A /org/service-profile # **show vnic** [**detail**] [**expand**]	Displays the details of the vNIC in the specified service profile.

This example shows how to display the status of a vNIC.

Note The CDN name that you configured for the vNIC appears as the **Admin CDN Name**. The CDN name that is finally applied to the BIOS policy appears as the **Oper CDN Name**.

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # show vnic detail expand

vNIC:
    Name: vnic1
    Fabric ID: B
    Dynamic MAC Addr: 00:25:B5:17:47:01
    Desired Order: Unspecified
    Actual Order: 1
    Desired VCon Placement: 2
    Actual VCon Placement: 2
    Desired Host Port: ANY
    Actual Host Port: NONE
    Equipment: sys/chassis-2/blade-5/adaptor-3/host-eth-2
    Host Interface Ethernet MTU: 1500
    Ethernet Interface Admin CDN Name:cdn0
    Ethernet Interface Oper CDN Name:cdn0
    Template Name:
```

CIMC Security Policies

Cisco UCS Manager provides the following policies to increase security:

- KVM Management Policy
- IPMI Access Profile

IPMI Access Profile

This policy allows you to determine whether 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 CIMC. 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 can also restrict remote connectivity by disabling or enabling IPMI over LAN in the IPMI access profile. IPMI over LAN is disabled by default on all unassociated servers, and on all servers without an IPMI access policy. When an IPMI access policy is created, the IPMI over LAN is set to enabled by default. If you do not change the value to disabled, IPMI over LAN will be enabled on all associated servers.

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

Configuring an IPMI Access Profile

Before You Begin

Obtain the following:

- Username with appropriate permissions that can be authenticated by the operating system of the server
- Password for the username
- Permissions associated with the username

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create ipmi-access-profile** *profile-name*	Creates the specified IPMI access profile and enters organization IPMI access profile mode.
Step 3	UCS-A /org/ipmi-access-profile # **set ipmi-over-lan** {**disable** | **enable**}	Determines whether remote connectivity can be established.

	Command or Action	Purpose
		Note IPMI over LAN is disabled by default on all unassociated servers, and on all servers without an IPMI access policy. When an IPMI access policy is created, the IPMI over LAN is set to enabled by default. If you do not change the value to disabled, IPMI over LAN will be enabled on all associated servers.
Step 4	UCS-A /org/ipmi-access-profile # **create ipmi-user** *ipmi-user-name*	Creates the specified endpoint user and enters organization IPMI access profile endpoint user mode. **Note** More than one endpoint user can be created within an IPMI access profile, with each endpoint user having its own password and privileges.
Step 5	UCS-A /org/ipmi-access-profile/ipmi-user # **set password**	Sets the password for the endpoint user. After entering the **set password** command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI.
Step 6	UCS-A /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	Specifies whether the endpoint user has administrative or read-only privileges.
Step 7	UCS-A /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates an IPMI access profile named ReadOnly, creates an endpoint user named bob, sets the password and the privileges for bob, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # create ipmi-user bob
UCS-A /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user #
```

What to Do Next

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

Deleting an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **delete ipmi-access-profile** *profile-name*	Deletes the specified IPMI access profile.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the IPMI access profile named ReadOnly and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete ipmi-access-profile ReadOnly
UCS-A /org* # commit-buffer
UCS-A /org #
```

Adding an Endpoint User to an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	Enters organization IPMI access profile mode for the specified IPMI access profile.
Step 3	UCS-A /org/ipmi-access-profile # **create ipmi-user** *ipmi-user-name*	Creates the specified endpoint user and enters organization IPMI access profile endpoint user mode. **Note** More than one endpoint user can be created within an IPMI access profile, with each endpoint user having its own password and privileges.
Step 4	UCS-A /org/ipmi-access-profile/ipmi-user # **set password**	Sets the password for the endpoint user. After entering the **set password** command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI.

	Command or Action	Purpose
Step 5	UCS-A /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	Specifies whether the endpoint user has administrative or read-only privileges.
Step 6	UCS-A /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

The following example adds an endpoint user named alice to the IPMI access profile named ReadOnly and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # create ipmi-user alice
UCS-A /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user #
```

Deleting an Endpoint User from an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	Enters organization IPMI access profile mode for the specified IPMI access profile.
Step 3	UCS-A /org/ipmi-access-profile # **delete ipmi-user** *epuser-name*	Deletes the specified endpoint user from the IPMI access profile.
Step 4	UCS-A /org/ipmi-access-profile # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the endpoint user named alice from the IPMI access profile named ReadOnly and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile # delete ipmi-user alice
UCS-A /org/ipmi-access-profile* # commit-buffer
UCS-A /org/ipmi-access-profile #
```

KVM Management Policy

This policy allows you to determine whether vMedia encryption is enabled when you access a server via KVM.

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

Note After a KVM vMedia session is mapped, if you change the KVM management policy, it will result in a loss of the vMedia session. You must re-map the KVM vMedia session again.

Configuring a KVM Management Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create kvm-mgmt-policy** *policy-name*	Creates the specified KVM management policy and enters organization KVM management policy mode.
Step 3	UCS-A /org/kvm-mgmt-policy # **set descr** *description*	(Optional) Provides a description for the policy.
Step 4	UCS-A /org/kvm-mgmt-policy # **set vmedia-encryption** {**disable** | **enable**}	Specifies vMedia encryption is enabled or disabled.
Step 5	UCS-A /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a KVM management policy named KVM_Policy1, enable vMedia encryption, and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # create kvm-mgmt-policy KVM_Policy1
UCS-A /org/kvm-mgmt-policy* # set vmedia-encryption enable
UCS-A /org/kvm-mgmt-policy* # commit-buffer
UCS-A /org/kvm-mgmt-policy #
```

Configuring Local Disk Configuration Policies

Local Disk Configuration 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:

- **No Local Storage—**For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Striped—**Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored—**Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration—**For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID—**For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

  If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

  To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.
- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

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

Note For a Cisco UCS C-Series server integrated with Cisco UCS Manager, with an embedded on-board RAID controller, the local disk mode should always be **Any Configuration**, and the RAID must be configured directly on the controller.

Guidelines for all Local Disk Configuration Policies

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single server or RAID configuration.

Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or re-assign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes those with Any Configuration or JBOD configuration.

JBOD Mode Support

Note Only B200 M1, B200 M2, B200 M3, B250 M1, B250 M2 and B22 M3 blade servers support the JBOD mode for local disks.

Guidelines for Local Disk Configuration Policies Configured for RAID

Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server. You can do this either by configuring the local disk configuration policy in the service profile using one of the defined RAID modes for that server, or you can use the **Any Configuration** mode with the LSI Utilities toolset to create the RAID volumes.

If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

Server May Not Boot After RAID1 Cluster Migration if Any Configuration Mode Specified in Service Profile

After RAID1 clusters are migrated, you need to associate a service profile with the server. If the local disk configuration policy in the service profile is configured with **Any Configuration** mode rather than **RAID1**, the RAID LUN remains in "inactive" state during and after association. As a result, the server cannot boot.

To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the **Any Configuration** mode.

Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with a MegaRAID storage controllers. JBOD mode and operations are not intended for nor are they fully functional on these servers.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

Maximum of One RAID Volume and One RAID Controller in Blade Servers

A blade server can have a maximum of one RAID volume irrespective of how many drives are present in the server. All the local hard drives must be connected to only one RAID controller. For example, a B200 M3 server has an LSI controller and an Intel Patsburg controller, but only the LSI controller can be used as a RAID controller.

In addition, do not use third party tools to create multiple RAID LUNs on blade servers. Cisco UCS Manager does not support that configuration.

Number of Disks Selected in Mirrored RAID Should Not Exceed Two

If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

License Required for Certain RAID Configuration Options on Some Servers

Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Manager associates a service profile containing this local disk policy with a server, Cisco UCS Manager verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Manager displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

B420 M3 Server Does Not Support All Configuration Modes

The B420 M3 server does not support the following configuration modes in a local disk configuration policy:

- No RAID
- RAID 6 Striped Dual Parity

In addition, the B420 M3 does not support JBOD modes or operations.

Single-Disk RAID 0 Configurations Not Supported on Some Blade Servers

A single-disk RAID 0 configuration is not supported in the following blade servers:

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

Creating a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create local-disk-config-policy** *policy-name*	Creates a local disk configuration policy and enters local disk configuration policy mode.
Step 3	UCS-A /org/local-disk-config-policy # **set descr** *description*	(Optional) Provides a description for the local disk configuration policy.
Step 4	UCS-A /org/local-disk-config-policy # **set mode** {**any-configuration** | **no-local-storage** | **no-raid** | **raid-0-striped** | **raid-1-mirrored** | **raid-5-striped-parity** | **raid-6-striped-dual-parity** | **raid-10-mirrored-and-striped**}	Specifies the mode for the local disk configuration policy.
Step 5	UCS-A /org/local-disk-config-policy # **set protect** {**yes** | **no**}	Specifies whether the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile. **Caution** Protect Configuration becomes non-functional if one or more disks in the server are defective or faulty. When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile. With this option enabled, the data on the disk is protected even after the server is decommissioned and then recommissioned. Hence, reassociation of the server with a service profile fails.

	Command or Action	Purpose
		Note If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.
Step 6	UCS-A /org/local-disk-config-policy # **set flexflash-state** {**enable** | **disable**}	Specifies whether FlexFlash SD card support is enabled.
Step 7	UCS-A /org/local-disk-config-policy # **set flexflash-raid-reporting-state** {**enable** | **disable**}	Specifies whether FlexFlash RAID reporting support is enabled. **Note** If only one SD card is installed, the FlexFlash inventory displays the RAID State as Disabled and the RAID Health as NA.
Step 8	UCS-A /org/local-disk-config-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a local disk configuration policy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create local-disk-config-policy DiskPolicy7
UCS-A /org/local-disk-config-policy* # set mode raid-1-mirrored
UCS-A /org/local-disk-config-policy* # set protect yes
UCS-A /org/local-disk-config-policy* # commit-buffer
UCS-A /org/local-disk-config-policy #
```

Viewing a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **show local-disk-config-policy** *policy-name*	Displays the local disk policy. If you have not configured a local disk policy, the local disk configuration (created by the create local-disk-config command) displays. Displays the local disk definition (set by the create local-disk-config command). If the serial over LAN definition is not set, and if a policy is set (using the set local-disk-config-policy command), then the policy will be displayed.

The following example shows how to display local disk policy information for a local disk configuration policy called DiskPolicy7:

```
UCS-A# scope org /
UCS-A /org # show local-disk-config-policy DiskPolicy7

Local Disk Config Policy:
Name: DiskPolicy7
Mode: Raid 1 Mirrored
Description:
Protect Configuration: Yes
```

Deleting a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **delete local-disk-config-policy** *policy-name*	Deletes the specified local disk configuration policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the local disk configuration policy named DiskPolicy7 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete local-disk-config-policy DiskPolicy7
UCS-A /org* # commit-buffer
UCS-A /org #
```

FlexFlash Support

Overview

Cisco UCS B-Series and C-Series M3 and M4 servers support internal Secure Digital (SD) memory cards. The SD cards are hosted by the Cisco Flexible Flash storage controller, a PCI-based controller which has two slots for SD cards. The cards contain a single partition called HV. When FlexFlash is enabled, Cisco UCS Manager displays the HV partition as a USB drive to both the BIOS and the host operating system.

FlexFlash is disabled by default. You can enable FlexFlash in a local disk policy used in a service profile. When FlexFlash is enabled in a local disk policy, and the server is capable of supporting SD cards, the FlexFlash controller is enabled during service profile association. If a server is not capable of supporting SD cards or has an older CIMC version, a config failure message is displayed.

If you disable FlexFlash in a supported server, the Hypervisor or HV partition is immediately disconnected from the host. The FlexFlash controller will also be disabled as part of a related service profile disassociation.

The FlexFlash controller supports RAID-1 for dual SD cards. You can configure new SD cards in a RAID pair by creating a FlexFlash scrub policy and reacknowledging the server. The FlexFlash scrub policy erases the HV partition in both cards, and brings the cards to a healthy RAID state.

Note Disable the scrub policy as soon as the pairing is complete.

To boot from the HV partition, the SD card must be present in the boot policy used in the service profile.

FlexFlash Firmware Management

The FlexFlash controller firmware is bundled as part of the CIMC image. When you upgrade the CIMC, if a newer firmware version is available for the FlexFlash controller, the controller can no longer be managed, and the FlexFlash inventory displays the **Controller State** as **Waiting For User Action** and the **Controller Health** as **Old Firmware Running**. To upgrade the FlexFlash controller firmware, you need to perform a board controller update. For more information, see the appropriate *Cisco UCS B-Series Firmware Management Guide*, available at the following URL: http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html.

Limitations for the Cisco Flexible Flash Storage Controller:

- The Cisco Flexible Flash storage controller only supports 16 GB, 32 GB, and 64 GB SD cards.

  Note 16 GB and 32 GB cards are supported only on the B200-M3 blade servers, and the 64 GB SD cards are supported only on the B200-M4 blade servers.

- We do not recommend using an SD card from a rack server in a blade server, or using an SD card from a blade server in a rack server. Switching SD cards between server types might result in data loss from the SD card.
- Some Cisco UCS C-Series rack-mount servers have SD cards with four partitions: HV, HUU, SCU, and Drivers. Only the HV partition is visible in Cisco UCS Manager. You can migrate a four-partition SD card to a single HV partition card with a FlexFlash scrub policy.
- The FlexFlash controller does not support RAID-1 sync (mirror rebuild). If the SD cards are in a degraded RAID state, or if any metadata errors are reported by the controller, you must run the FlexFlash scrub policy to pair the cards for RAID. For more information about the FlexFlash scrub policy, see Scrub Policy, on page 66. The following conditions might result in degraded RAID or metadata errors:
  - Inserting a new or used SD card in one slot, when the server already has an SD card populated in the second slot.
  - Inserting two SD cards from different servers.
- The server firmware version must be at 2.2(1a) or higher.

FlexFlash FX3S Support

Beginning with Release 2.2(3), Cisco UCS Manager allows additional FlexFlash support with the FX3S controller. The FX3S controller is present on the following servers:

- Cisco UCS B200 M4 blade server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4 rack server

FlexFlash operations with the FX3S control are similar to those with the Cisco Flexible Flash storage controller. FlexFlash is disabled by default, and is enabled using a local disk policy. You can also reset the controller, format the SD cards, and enable automatic synchronization of your paired SD cards.

The SD cards for the FX3S controller contain a single partition called Hypervisor.

Limitations for the Cisco FX3S Controller:

- The FX3S controller supports only 32 GB and 64 GB SD cards. 16 GB cards are not supported.
- We do not recommend using an SD card from a rack server in a blade server, or using an SD card from a blade server in a rack server. Switching SD cards between server types might result in data loss from the SD card.
- The server firmware version must be at 2.2(3a) or higher.

Enabling or Disabling FlexFlash SD Card Support

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope local-disk-config-policy** *policy-name*	Enters the specified local disk configuration policy mode.
Step 3	UCS-A /org/local-disk-config-policy # **set flexflash-state** {**enable** | **disable**}	Specifies whether FlexFlash SD card support is enabled.
Step 4	UCS-A /org/local-disk-config-policy # **set flexflash-raid-reporting-state** {**enable** | **disable**}	Specifies whether FlexFlash RAID reporting support is enabled. **Note** If only one SD card is installed, the FlexFlash inventory displays the RAID State as Disabled and the RAID Health as NA.
Step 5	UCS-A /org/local-disk-config-policy # **commit-buffer**	Commits the transaction to the system.

The following example shows how to enable FlexFlash SD card support and FlexFlash RAID reporting state on the local disk config policy default, and commits the transaction to the system:

```
UCS-A# scope org/
UCS-A /org # scope local-disk-config-policy default
```

```
UCS-A /org/local-disk-config-policy #set flexflash-state enable
UCS-A /org/local-disk-config-policy# #set flexflash-raid-reporting-state enable
UCS-A /org/local-disk-config-policy* # commit-buffer
UCS-A /org/local-disk-config-policy #
```

Enabling Auto-Sync

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope server** *server-num*	Enters server chassis mode.
Step 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	Enters flexflash controller server chassis mode.
Step 4	UCS-A /chassis/server/flexflash-controller # **pair** *primary_slot_number*	Resyncs the SD cards if they are out of sync, using the card in the selected slot number as the primary. This can be one of the following: • **1—**The SD card in slot 1 will be used as the primary. • **2—**The SD card in slot 2 will be used as the primary.
Step 5	UCS-A /chassis/server/flexflash-controller # **commit-buffer**	Commits the transaction to the system configuration.

The following example resyncs the SD cards using the SD card in slot 2 as the primary:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # pair 2
UCS-A /chassis/server/flexflash-controller* # commit-buffer
UCS-A /chassis/server/flexflash-controller #
```

Formatting the FlexFlash Cards

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope server** *server-num*	Enters server chassis mode.

	Command or Action	Purpose
Step 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	Enters flexflash controller server chassis mode.
Step 4	UCS-A /chassis/server/flexflash-controller # **format**	Formats the SD cards.
Step 5	UCS-A /chassis/server/flexflash-controller # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to format the FlexFlash controller:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # format
Warning: When commited, UCSM will format the SD Cards.
This will completely erase the data on the SD Cards!!

UCS-A /chassis/server/flexflash-controller* # commit-buffer
UCS-A /chassis/server/flexflash-controller #
```

Resetting the FlexFlash Controller

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope server** *server-num*	Enters server chassis mode.
Step 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	Enters flexflash controller server chassis mode.
Step 4	UCS-A /chassis/server/flexflash-controller # **reset**	Resets the specified FlexFlash controller.
Step 5	UCS-A /chassis/server/flexflash-controller # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to reset the FlexFlash controller:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # reset
Warning: When commited, UCSM will reset the FlexFlash Controller.
This will cause the host OS to lose connectivity to the SD Cards.

UCS-A /chassis/server/flexflash-controller* # commit-buffer
UCS-A /chassis/server/flexflash-controller #
```

Viewing the FlexFlash Controller Status

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope server** *server-num*	Enters server chassis mode.
Step 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	Enters flexflash controller server chassis mode.
Step 4	UCS-A /chassis/server/flexflash-controller # **show detail expand**	Displays the detailed FlexFlash controller properties.

The following example shows the status of the FlexFlash controller and SD cards:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # show detail expand

FlexFlash Controller:
    ID: 1
    Type: SD
    FlexFlash Type: FX3S
    Vendor: Cypress
    Model: FX3S
    Serial: NA
    Firmware Version: 1.3.2 build 158
    Controller State: Connected Partition Over USB To Host
    Controller Health: Old Firmware Running
    RAID State: Enabled Paired
    RAID Health: OK
    Physical Drive Count: 2
    Virtual Drive Count: 1
    RAID Sync Support: Supported
    Operability: Operable
    Oper Qualifier Reason:
    Presence: Equipped
    Current Task:

    FlexFlash Card:
        Controller Index: 1
        Slot Number: 1
        Vendor: SE32G
        Model: SE32G
        HW Rev: 8.0
        Serial: 0xa2140794
        Manufacturer ID: 3
        OEM ID: SD
        Manufacturer Date: 2/14
        Size (MB): 30436
        Block Size: 512
        Card Type: FX3S configured
        Write Enabled: Not Write Protected
        Card Health: OK
        Card Mode: Secondary Active
        Operation State: Raid Partition
        Card State: Active
        Write IO Error Count: 0
```

```
            Read IO Error Count: 0
            Operability: Operable
            Oper Qualifier Reason:
            Presence: Equipped

            FlexFlash Card Drive:
                Name: Hypervisor
                Size (MB): 30432
                Removable: Yes
                Operability: Operable
                Operation State: Raid Partition

            Controller Index: 1
            Slot Number: 2
            Vendor: SE32G
            Model: SE32G
            HW Rev: 8.0
            Serial: 0xa2140742
            Manufacturer ID: 3
            OEM ID: SD
            Manufacturer Date: 2/14
            Size (MB): 30436
            Block Size: 512
            Card Type: FX3S configured
            Write Enabled: Not Write Protected
            Card Health: OK
            Card Mode: Primary
            Operation State: Raid Partition
            Card State: Active
            Write IO Error Count: 0
            Read IO Error Count: 0
            Operability: Operable
            Oper Qualifier Reason:
            Presence: Equipped

            FlexFlash Card Drive:
                Name: Hypervisor
                Size (MB): 30432
                Removable: Yes
                Operability: Operable
                Operation State: Raid Partition

        Local Disk Config Definition:
            Mode: Any Configuration
            Description:
            Protect Configuration: Yes

UCS-A /chassis/server/flexflash-controller #
```

Configuring Scrub Policies

Scrub Policy

This policy determines 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 a Scrub Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .

	Command or Action	Purpose
Step 2	UCS-A /org # **create scrub-policy** *policy-name*	Creates a scrub policy with the specified policy name, and enters organization scrub policy mode.
Step 3	UCS-A /org/scrub-policy # **set descr** *description*	(Optional) Provides a description for the scrub policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A /org/scrub-policy # **set disk-scrub** {**no** | **yes**}	Disables or enables disk scrubbing on servers using this scrub policy as follows: • If enabled, destroys all data on any local drives. • If disabled, preserves all data on any local drives, including local storage configuration.
Step 5	UCS-A /org/scrub-policy # **set bios-settings-scrub** {**no** | **yes**}	Disables or enables BIOS settings scrubbing on servers using this scrub policy as follows: • 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.
Step 6	UCS-A /org/scrub-policy # **set flexflash-scrub** {**no** | **yes**}	Disables or enables flexflash scrubbing on servers using this scrub policy as follows: • 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.
Step 7	UCS-A /org/scrub-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a scrub policy named ScrubPolicy2, enables disk scrubbing on servers using the scrub policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create scrub-policy ScrubPolicy2
UCS-A /org/scrub-policy* # set descr "Scrub disk but not BIOS."
UCS-A /org/scrub-policy* # set disk-scrub yes
UCS-A /org/scrub-policy* # set bios-settings-scrub no
UCS-A /org/scrub-policy* # set flexflash-scrub no
```

```
UCS-A /org/scrub-policy* # commit-buffer
UCS-A /org/scrub-policy #
```

Deleting a Scrub Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **delete scrub-policy** *policy-name*	Deletes the specified scrub policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the scrub policy named ScrubPolicy2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete scrub-policy ScrubPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring DIMM Error Management

DIMM Correctable Error Handling

In Cisco UCS Manager, when a DIMM encounters a significant correctable error in a given predefined window, it is stated as degraded and considered as a non-functional device.

The DIMM correctable error handling feature enables you to reset all the correctable and uncorrectable memory errors on all the DIMMs in a server. When you reset the error configuration, the error count of a given DIMM is cleared, the status changes to operable, and it resets the sensor state of the given DIMM.

Resetting Memory Errors

Use this procedure to reset all correctable and uncorrectable memory errors encountered by Cisco UCS Manager and the baseboard management controller (BMC).

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A/chassis # **scope server** *server-num*	Enters server mode for the specified server.

	Command or Action	Purpose
Step 3	UCS-A/chassis/server # **reset-all-memory-errors**	Resets the correctable and uncorrectable errors on all the DIMMs in a server.
Step 4	UCS-A /chassis/server* # **commit-buffer**	Commits any pending transactions.

This example shows how to reset the memory errors for the selected memory unit(s):

```
UCS-A# scope chassis 1
UCS-A/chassis # scope server 1
UCS-A/chassis/server # reset-all-memory-errors
UCS-A/chassis/server* # commit-buffer
UCS-A/chassis/server #
```

DIMM Blacklisting

In Cisco UCS Manager, the state of the Dual In-line Memory Module (DIMM) is based on SEL event records. When the BIOS encounters a noncorrectable memory error during memory test execution, the DIMM is marked as faulty. A faulty DIMM is a considered a nonfunctional device.

If you enable DIMM blacklisting, Cisco UCS Manager monitors the memory test execution messages and blacklists any DIMMs that encounter memory errors in the DIMM SPD data. To allow the host to map out any DIMMs that encounter uncorrectable ECC errors.

Enabling DIMM Blacklisting

The memory policy is a global policy that you can apply to existing servers on a Cisco UCS domain and also to the servers that are added after you set the memory policy.

Note

- This feature is supported both on the Cisco UCS B-Series blade servers and UCS C-Series rack servers.

  Note Cisco UCS C-Series 420 M3 rack server do not support this feature.

- This global policy cannot be added to a service profile.

Before You Begin

- For Cisco B-Series blade server, the server firmware must be at Release 2.2(1) or a later release.
- For Cisco C-Series rack server, the server firmware must be at Release 2.2(3).
- You must be logged in with one of the following privileges:
  - Admin
  - Server policy
  - Server profile server policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** /	Enters root organization mode.
Step 2	UCS-A /org # **memory-config-policy default**	Enters memory policy mode for the global memory policy.
Step 3	UCS-A /org/memory-config-policy # **set blacklisting enabled**	Enables DIMM blacklisting for the domain level policy and these changes applies to all the servers on that particular domain. **Note** If the Cisco IMC of a server does not support DIMM blacklisting, an information level fault is generated.
Step 4	UCS-A /org/memory-config-policy* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to enable DIMM blacklisting:

```
UCS-A# scope org /
UCS-A /chassis/org # scope memory-config-policy default
UCS-A /chassis/org/memory-config-policy # set blacklisting enabled
UCS-A /chassis/org/memory-config-policy* # commit-buffer
UCS-A /chassis/org/memory-config-policy #
UCS-A /chassis/org/memory-config-policy # show detail

Memory Config Policy:
    Blacklisting: enabled
```

Configuring Serial over LAN Policies

Serial over LAN Policy

This policy sets the configuration for the 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.

Configuring a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create sol-policy** *policy-name*	Creates a serial over LAN policy and enters organization serial over LAN policy mode.
Step 3	UCS-A /org/sol-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A /org/sol-policy # **set speed** {**115200** | **19200** | **38400** | **57600** | **9600**}	Specifies the serial baud rate.
Step 5	UCS-A /org/sol-policy # {**disable** | **enable**}	Disables or enables the serial over LAN policy. By default, the serial over LAN policy is disabled; you must enable it before it can be applied.
Step 6	UCS-A /org/sol-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a serial over LAN policy named Sol9600, provides a description for the policy, sets the speed to 9,600 baud, enables the policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create sol-policy Sol9600
UCS-A /org/sol-policy* # set descr "Sets serial over LAN policy to 9600 baud."
UCS-A /org/sol-policy* # set speed 9600
UCS-A /org/sol-policy* # enable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy #
```

Viewing a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **show sol-policy** *policy-name*	Displays the serial over LAN definition (set by the create sol-config command). If the serial over LAN definition is not set, and if a policy is set (using the set sol-policy command), then the policy will be displayed.

The following example shows how to display serial over LAN information for a serial over LAN policy called Sol9600:

```
UCS-A# scope org /
UCS-A /org # show sol-policy Sol9600

SOL Policy:
Full Name: Sol9600
SOL State: Enable
Speed: 9600
Description:
```

Deleting a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **delete sol-policy** *policy-name*	Deletes the specified serial over LAN policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the serial over LAN policy named Sol9600 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete sol-policy Sol9600
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Autoconfiguration Policies

Server Autoconfiguration Policy

Cisco UCS Manager uses this policy to determine how to configure a new server. If you create a server autoconfiguration policy, the following occurs when a new server starts:

1. The qualification in the server autoconfiguration policy is executed against the server.
2. If the server meets the required qualifications, the server is associated with a service profile created from the service profile template configured in the server autoconfiguration policy. The name of that service profile is based on the name given to the server by Cisco UCS Manager.
3. The service profile is assigned to the organization configured in the server autoconfiguration policy.

Configuring a Server Autoconfiguration Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create server-autoconfig-policy** *policy-name*	Creates a server autoconfiguration policy with the specified policy name, and enters organization server autoconfiguration policy mode.
Step 3	UCS-A /org/server-autoconfig-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A /org/server-autoconfig-policy # **set destination org** *org-name*	(Optional) Specifies the organization for which the server is to be used.
Step 5	UCS-A /org/server-autoconfig-policy # **set qualifier** *server-qual-name*	(Optional) Specifies server pool policy qualification to use for qualifying the server.

	Command or Action	Purpose
Step 6	UCS-A /org/server-autoconfig-policy # **set template** *profile-name*	(Optional) Specifies a service profile template to use for creating a service profile instance for the server.
Step 7	UCS-A /org/server-autoconfig-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server autoconfiguration policy named AutoConfigFinance, provides a description for the policy, specifies finance as the destination organization, ServPoolQual22 as the server pool policy qualification, and ServTemp2 as the service profile template, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create server-autoconfig-policy AutoConfigFinance
UCS-A /org/server-autoconfig-policy* # set descr "Server Autoconfiguration Policy for
Finance"
UCS-A /org/server-autoconfig-policy* # set destination org finance
UCS-A /org/server-autoconfig-policy* # set qualifier ServPoolQual22
UCS-A /org/server-autoconfig-policy* # set template ServTemp2
UCS-A /org/server-autoconfig-policy* # commit-buffer
UCS-A /org/server-autoconfig-policy #
```

Deleting a Server Autoconfiguration Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **delete server-autoconfig-policy** *policy-name*	Deletes the specified server autoconfiguration policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the server autoconfiguration policy named AutoConfigFinance and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete server-autoconfig-policy AutoConfigFinance
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Discovery Policies

Server Discovery Policy

This discovery policy determines how the system reacts when you add a new server. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

If you create a server discovery policy, the following occurs when a new server starts:

1. The qualification in the server discovery policy is executed against the server.
2. If the server meets the required qualifications, Cisco UCS Manager applies the following to the server:
   - Depending upon the option selected for the action, either discovers the new server immediately or waits for a user to acknowledge the new server
   - Applies the scrub policy to the server

Important In Cisco UCS Manager Release 2.2(4), blade servers do not support drives with a block size of 4K, but rack-mount servers support such drives. If a drive with a block size of 4K is inserted into a blade server, discovery fails and the following error message appears:

```
Unable to get Scsi Device Information from the system
```

If this error occurs, do the following:

1. Remove the 4K drive.
2. Reacknowledge the server.

Note: Reacknowledging the server causes the server to reboot and results in loss of service.

Configuring a Server Discovery Policy

Before You Begin

If you plan to associate this policy with a server pool, create server pool policy qualifications.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org /**	Enters the root organization mode. **Note** Chassis discovery policies can only be accessed from the root organization.

	Command or Action	Purpose
Step 2	UCS-A /org # **create server-disc-policy** *policy-name*	Creates a server discovery policy with the specified policy name, and enters org server discovery policy mode.
Step 3	UCS-A /org/server-disc-policy # **set action** {**diag** | **immediate** | **user-acknowledged**}	Specifies when the system will attempt to discover new servers.
Step 4	UCS-A /org/chassis-disc-policy # **set descr** *description*	(Optional) Provides a description for the server discovery policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCS-A /org/server-disc-policy # **set qualifier** *qualifier*	(Optional) Uses the specified server pool policy qualifications to associates this policy with a server pool.
Step 6	UCS-A /org/server-disc-policy # **set scrub-policy**	Specifies the scrub policy to be used by this policy. The scrub policy defines whether the disk drive on a server should be scrubbed clean upon discovery.
Step 7	UCS-A /org/server-disc-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server discovery policy named ServDiscPolExample, sets it to immediately discover new servers, provides a description for the policy, specifies the server pool policy qualifications and scrub policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create server-disc-policy ServDiscPolExample
UCS-A /org/server-disc-policy* # set action immediate
UCS-A /org/server-disc-policy* # set descr "This is an example server discovery policy."
UCS-A /org/server-disc-policy* # set qualifier ExampleQual
UCS-A /org/server-disc-policy* # set scrub-policy NoScrub
UCS-A /org/server-disc-policy # commit-buffer
```

What to Do Next

Include the server discovery policy in a service profile and/or template.

Deleting a Server Discovery Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **Delete server-disc-policy** *policy-name*	Deletes the specified server discovery policy.
Step 3	UCS-A /org/server-disc-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the server discovery policy named ServDiscPolExample and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete server-disc-policy ServDiscPolExample
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Inheritance Policies

Server Inheritance Policy

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Configuring a Server Inheritance Policy

A blade server or rack-mount server with a VIC adapter, such as the Cisco UCS M81KR Virtual Interface Card, does not have server identity values burned into the server hardware at manufacture. As a result, the identity of the adapter must be derived from default pools. If the default pools do not include sufficient entries for one to be assigned to the server, service profile association fails with a configuration error.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create server-inherit-policy** *policy-name*	Creates a server inheritance policy with the specified policy name, and enters organization server inheritance policy mode.
Step 3	UCS-A /org/server-inherit-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A /org/server-inherit-policy # **set destination org** *org-name*	(Optional) Specifies the organization for which the server is to be used.
Step 5	UCS-A /org/server-inherit-policy # **set qualifier** *server-qual-name*	(Optional) Specifies server pool policy qualification to use for qualifying the server.
Step 6	UCS-A /org/server-inherit-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server inheritance policy named InheritEngineering, provides a description for the policy, specifies engineering as the destination organization and ServPoolQual22 as the server pool policy qualification, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create server-inherit-policy InheritEngineering
UCS-A /org/server-inherit-policy* # set descr "Server Inheritance Policy for Engineering"
UCS-A /org/server-inherit-policy* # set destination org engineering
UCS-A /org/server-inherit-policy* # set qualifier ServPoolQual22
UCS-A /org/server-inherit-policy* # commit-buffer
UCS-A /org/server-inherit-policy #
```

Deleting a Server Inheritance Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **delete server-inherit-policy** *policy-name*	Deletes the specified server inheritance policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the server inheritance policy named InheritEngineering and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete server-inherit-policy InheritEngineering
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Pool Policies

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Configuring a Server Pool Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create pooling-policy** *policy-name*	Creates a server pool policy with the specified name, and enters organization pooling policy mode.

	Command or Action	Purpose
Step 3	UCS-A /org/pooling-policy # **set descr** *description*	(Optional) Provides a description for the server pool policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A /org/pooling-policy # **set pool** *pool-distinguished-name*	Specifies the server pool to use with the server pool policy. You must specify the full distinguished name for the pool.
Step 5	UCS-A /org/pooling-policy # **set qualifier** *qualifier-name*	Specifies the server pool qualifier to use with the server pool policy.
Step 6	UCS-A /org/pooling-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server pool policy named ServerPoolPolicy4 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create pooling-policy ServerPoolPolicy4
UCS-A /org/pooling-policy* # set pool org-root/compute-pool-pool3
UCS-A /org/pooling-policy* # set qualifier ServPoolQual8
UCS-A /org/pooling-policy* # commit-buffer
UCS-A /org/pooling-policy #
```

Deleting a Server Pool Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **delete pooling-policy** *policy-name*	Deletes the specified server pool policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the server pool policy named ServerPoolPolicy4 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete pooling-policy ServerPoolPolicy4
UCS-A /org/pooling-policy* # commit-buffer
UCS-A /org/pooling-policy #
```

Configuring Server Pool Policy Qualifications

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure 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

Depending upon the implementation, you might need to configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating a Server Pool Policy Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .

	Command or Action	Purpose
Step 2	UCS-A /org # **create server-qual** *server-qual-name*	Creates a server pool qualification with the specified name, and enters organization server qualification mode.
Step 3	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server pool qualification named ServPoolQual22 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create server-qual ServPoolQual22
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

What to Do Next

Configure one or more of the following server component qualifications:

- Adapter qualification
- Chassis qualification
- Memory qualification
- Power group qualification
- Processor qualification
- Storage qualification

Deleting a Server Pool Policy Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **delete server-qual** *server-qual-name*	Deletes the specified server pool qualification.
Step 3	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the server pool qualification named ServPoolQual22 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete server-qual ServPoolQual22
```

```
UCS-A /org* # commit-buffer
UCS-A /org #
```

Creating an Adapter Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create adapter**	Creates an adapter qualification and enters organization server qualification adapter mode.
Step 4	UCS-A /org/server-qual/adapter # **create cap-qual** *adapter-type*	Creates an adapter capacity qualification for the specified adapter type and enters organization server qualification adapter capacity qualification mode. The *adapter-type* argument can be any of the following values: • **fcoe —**Fibre Channel over Ethernet • **non-virtualized-eth-if —**Non-virtualized Ethernet interface • **non-virtualized-fc-if —**Non-virtualized Fibre Channel interface • **path-encap-consolidated —**Path encapsulation consolidated • **path-encap-virtual —**Path encapsulation virtual • **protected-eth-if —**Protected Ethernet interface • **protected-fc-if —**Protected Fibre Channel interface • **protected-fcoe —**Protected Fibre Channel over Ethernet • **virtualized-eth-if —**Virtualized Ethernet interface • **virtualized-fc-if —**Virtualized Fibre Channel interface • **virtualized-scsi-if —**Virtualized SCSI interface
Step 5	UCS-A /org/server-qual/adapter/cap-qual # **set maximum** {*max-cap* | **unspecified**}	Specifies the maximum capacity for the selected adapter type.

	Command or Action	Purpose
Step 6	UCS-A /org/server-qual/adapter/cap-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates and configures an adapter qualification for a non-virtualized Ethernet interface and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create adapter
UCS-A /org/server-qual/adapter* # create cap-qual non-virtualized-eth-if
UCS-A /org/server-qual/adapter/cap-qual* # set maximum 2500000000
UCS-A /org/server-qual/adapter/cap-qual* # commit-buffer
UCS-A /org/server-qual/adapter/cap-qual #
```

Deleting an Adapter Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete adapter**	Deletes the adapter qualification from the server pool policy qualification.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the adapter qualification from the server pool policy qualification named ServPoolQual22 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete adapter
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Configuring a Chassis Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create chassis** *min-chassis-num max-chassis-num*	Creates a chassis qualification for the specified chassis range and enters organization server qualification chassis mode.
Step 4	UCS-A /org/server-qual/chassis # **create slot** *min-slot-num max-slot-num*	Creates a chassis slot qualification for the specified slot range and enters organization server qualification chassis slot mode.
Step 5	UCS-A /org/server-qual/chassis/slot # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a chassis qualification for slots 1 to 4 on chassis 1 and 2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope server-qual ServPoolQual22
UCS-A /org/server-qual* # create chassis 1 2
UCS-A /org/server-qual/chassis* # create slot 1 4
UCS-A /org/server-qual/chassis/slot* # commit-buffer
UCS-A /org/server-qual/chassis/slot #
```

Deleting a Chassis Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete chassis** *min-chassis-num max-chassis-num*	Deletes the chassis qualification for the specified chassis range.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the chassis qualification for chassis 1 and 2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete chassis 1 2
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a CPU Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create cpu**	Creates a CPU qualification and enters organization server qualification processor mode.
Step 4	UCS-A /org/server-qual/cpu # **set arch** {**any** | **dual-core-opteron** | **intel-p4-c** | **opteron** | **pentium-4** | **turion-64** | **xeon** | **xeon-mp**}	Specifies the processor architecture type.
Step 5	UCS-A /org/server-qual/cpu # **set maxcores** {*max-core-num* | **unspecified**}	Specifies the maximum number of processor cores.
Step 6	UCS-A /org/server-qual/cpu # **set mincores** {*min-core-num* | **unspecified**}	Specifies the minimum number of processor cores.
Step 7	UCS-A /org/server-qual/cpu # **set maxprocs** {*max-proc-num* | **unspecified**}	Specifies the maximum number of processors.
Step 8	UCS-A /org/server-qual/cpu # **set minprocs** {*min-proc-num* | **unspecified**}	Specifies the minimum number of processors.
Step 9	UCS-A /org/server-qual/cpu # **set maxthreads** {*max-thread-num* | **unspecified**}	Specifies the maximum number of threads.
Step 10	UCS-A /org/server-qual/cpu # **set minthreads** {*min-thread-num* | **unspecified**}	Specifies the minimum number of threads.
Step 11	UCS-A /org/server-qual/cpu # **set stepping** {*step-num* | **unspecified**}	Specifies the processor stepping number.

	Command or Action	Purpose
Step 12	UCS-A /org/server-qual/cpu # **set model-regex** *regex*	Specifies a regular expression that the processor name must match.
Step 13	UCS-A /org/server-qual/cpu # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates and configures a CPU qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create processor
UCS-A /org/server-qual/cpu* # set arch xeon
UCS-A /org/server-qual/cpu* # set maxcores 8
UCS-A /org/server-qual/cpu* # set mincores 4
UCS-A /org/server-qual/cpu* # set maxprocs 2
UCS-A /org/server-qual/cpu* # set minprocs 1
UCS-A /org/server-qual/cpu* # set maxthreads 16
UCS-A /org/server-qual/cpu* # set minthreads 8
UCS-A /org/server-qual/cpu* # set stepping 5
UCS-A /org/server-qual/cpu* # commit-buffer
UCS-A /org/server-qual/cpu #
```

Deleting a CPU Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete cpu**	Deletes the processor qualification.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the processor qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete cpu
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Power Group Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create power-group** *power-group-name*	Creates a power group qualification for the specified power group name.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a power group qualification for a power group called powergroup1 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create power-group powergroup1
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Deleting a Power Group Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete power-group** *power-group-name*	Deletes the specified power group qualification.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes a power group qualification for a power group called powergroup1 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete power-group powergroup1
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Memory Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create memory**	Creates a memory qualification and enters organization server qualification memory mode.
Step 4	UCS-A /org/server-qual/memory # **set clock** {*clock-num* | **unspec**}	Specifies the memory clock speed.
Step 5	UCS-A /org/server-qual/memory # **set maxcap** {*max-cap-num* | **unspec**}	Specifies the maximum capacity of the memory array.
Step 6	UCS-A /org/server-qual/memory # **set mincap** {*min-cap-num* | **unspec**}	Specifies the minimum capacity of the memory array.
Step 7	UCS-A /org/server-qual/memory # **set speed** {*speed-num* | **unspec**}	Specifies the memory data rate.
Step 8	UCS-A /org/server-qual/memory # **set units** {*unit-num* | **unspec**}	Specifies the number of memory units (DRAM chips mounted to the memory board).
Step 9	UCS-A /org/server-qual/memory # **set width** {*width-num* | **unspec**}	Specifies the bit width of the data bus.
Step 10	UCS-A /org/server-qual/memory # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates and configures a memory qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create memory
UCS-A /org/server-qual/memory* # set clock 1067
UCS-A /org/server-qual/memory* # set maxcap 4096
UCS-A /org/server-qual/memory* # set mincap 2048
UCS-A /org/server-qual/memory* # set speed unspec
UCS-A /org/server-qual/memory* # set units 16
UCS-A /org/server-qual/memory* # set width 64
UCS-A /org/server-qual/memory* # commit-buffer
UCS-A /org/server-qual/memory #
```

Deleting a Memory Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete memory**	Deletes the memory qualification.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the memory qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete memory
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Physical Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create physical-qual**	Creates a physical qualification and enters organization server qualification physical mode.
Step 4	UCS-A /org/server-qual/physical-qual # **set model-regex** *regex*	Specifies a regular expression that the model name must match.
Step 5	UCS-A /org/server-qual/physical-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates and configures a physical qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create physical-qual
UCS-A /org/server-qual/physical-qual* # set model-regex
UCS-A /org/server-qual/physical-qual* # commit-buffer
UCS-A /org/server-qual/physical-qual #
```

Deleting a Physical Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete physical-qual**	Deletes the physical qualification.
Step 4	UCS-A /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes a physical qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
```

```
UCS-A /org/server-qual # delete physical-qual
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Storage Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **create storage**	Creates a storage qualification and enters organization server qualification storage mode.
Step 4	UCS-A /org/server-qual/storage # **set blocksize** {*block-size-num* | **unknown**}	Specifies the storage block size.
Step 5	UCS-A /org/server-qual/storage # **set diskless** {**no** | **unspecified** | **yes** }	Specifies whether the available storage must be diskless.
Step 6	UCS-A /org/server-qual/storage # **set disktype** {**hdd** | **ssd** | **unspecified**}	Specifies the type of disk that can be used. The options are: • **Unspecified—**Either disk type is acceptable. • **HDD—**The disk must be HDD. • **SSD—**The disk must be SSD (SATA or SAS).
Step 7	UCS-A /org/server-qual/storage # **set flexflash-num-cards** {*ff_card-num* | **unknown**}	Specifies the number of FlexFlash cards.
Step 8	UCS-A /org/server-qual/storage # **set maxcap** {*max-cap-num* | **unknown**}	Specifies the maximum capacity of the storage array.
Step 9	UCS-A /org/server-qual/storage # **set mincap** {*min-cap-num* | **unknown**}	Specifies the minimum capacity of the storage array.
Step 10	UCS-A /org/server-qual/storage # **set numberofblocks** {*block-num* | **unknown**}	Specifies the number of blocks.

	Command or Action	Purpose
Step 11	UCS-A /org/server-qual/storage # **set perdiskcap** {*disk-cap-num* | **unknown**}	Specifies the per-disk capacity.
Step 12	UCS-A /org/server-qual/storage # **set units** {*unit-num* | **unspecified**}	Specifies the number of storage units.
Step 13	UCS-A /org/server-qual/storage # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create and configure a storage qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create storage
UCS-A /org/server-qual/storage* # set blocksize 512
UCS-A /org/server-qual/storage* # set disktype hdd
UCS-A /org/server-qual/storage* # set maxcap 420000
UCS-A /org/server-qual/storage* # set mincap 140000
UCS-A /org/server-qual/storage* # set numberofblocks 287277984
UCS-A /org/server-qual/storage* # set perdiskcap 140000
UCS-A /org/server-qual/storage* # set units 1
UCS-A /org/server-qual/storage* # set flexflash-num-cards 2
UCS-A /org/server-qual/storage* # commit-buffer
UCS-A /org/server-qual/storage #
```

Deleting a Storage Qualification

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope server-qual** *server-qual-name*	Enters organization server qualification mode for the specified server pool policy qualification.
Step 3	UCS-A /org/server-qual # **delete storage**	Deletes the storage qualification.
Step 4	UCS-A /org/server-qual/ # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the storage qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete storage
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Configuring vNIC/vHBA Placement Policies

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine the following:

- How the virtual network interface connections (vCons) are mapped to the physical adapters on a server.
- What types of vNICs or vHBAs can be assigned to each vCon.

Each vNIC/vHBA placement policy contains four vCons that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters and the vNICs and vHBAs are assigned to those vCons.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the type of server and the selected virtual slot mapping scheme, which can be **Round Robin** or **Linear Ordered**. For details about the available mapping schemes, see vCon to Adapter Placement, on page 96.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the **Selection Preference** for each vCon. This can be one of the following:

- **all—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- **assigned-only—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- **exclude-dynamic—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- **exclude-unassigned—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.
- **exclude-usnic—**Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

Note An SRIOV usNIC that is explicitly assigned to a vCon set to **exclude-usnic** will remain assigned to that vCon.

If you do not include a vNIC/vHBA placement policy in the service profile, Cisco UCS Manager defaults to the **Round Robin** vCon mapping scheme and the **All** vNIC/vHBA selection preference, distributing the vNICs and vHBAs between the adapters based on the capabilities and relative capacities of each adapter.

vCon to Adapter Placement

Cisco UCS maps every vCon in a service profile to a physical adapter on the server. How that mapping occurs and how the vCons are assigned to a specific adapter in a server depends on the following:

- The type of server. N20-B6620-2 and N20-B6625-2 blade servers with two adapter cards use a different mapping scheme than other supported rack or blade servers.
- The number of adapters in the server.
- The setting of the virtual slot mapping scheme in the vNIC/vHBA placement policy, if applicable.

You must consider this placement when you configure the vNIC/vHBA selection preference to assign vNICs and vHBAs to vCons.

Note vCon to adapter placement is not dependent upon the PCIE slot number of the adapter. The adapter numbers used for the purpose of vCon placement are not the PCIE slot numbers of the adapters, but the ID assigned to them during server discovery.

vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers

In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme:

- **round-robin—**Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default.
- **linear-ordered—**Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.

vCon to Adapter Placement for All Other Supported Servers

For all other servers supported by Cisco UCS in addition to the N20-B6620-2 and N20-B6625-2 blade servers, the vCon assignment depends on the number of adapters in the server and the virtual slot mapping scheme.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the selected virtual slot mapping scheme: Round Robin or Linear Ordered.

Table 1: vCon to Adapter Placement Using the Round - Robin Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
2	Adapter1	Adapter2	Adapter1	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter2
4	Adapter1	Adapter2	Adapter3	Adapter4

Round Robin is the default mapping scheme.

Table 2: vCon to Adapter Placement Using the Linear Ordered Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter1	Adapter2	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter3
4	Adapter1	Adapter2	Adapter3	Adapter4

Note If you are using a vCon policy with two adapters in the Cisco UCS B440 M2 Blade Server, be aware of the following mapping.

- vCon 2 to adapter 1 maps first
- vCon 1 to adapter 2 maps second ZXA Q

vNIC/vHBA to vCon Assignment

Cisco UCS Manager provides two options for assigning vNICs and vHBAs to vCons through the vNIC/vHBA placement policy: explicit assignment and implicit assignment.

Explicit Assignment of vNICs and vHBAs

With explicit assignment, you specify the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned. Use this assignment option when you need to determine how the vNICs and vHBAs are distributed between the adapters on a server.

To configure a vCon and the associated vNICs and vHBAs for explicit assignment, do the following:

- Set the vCon configuration to any of the available options. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server. If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon.

- Assign the vNICs and vHBAs to a vCon. You can make this assignment through the virtual host interface placement properties of the vNIC or vHBA or in the service profile associated with the server.

If you attempt to assign a vNIC or vHBA to a vCon that is not configured for that type of vNIC or vHBA, Cisco UCS Manager displays a message advising you of the configuration error.

During service profile association, Cisco UCS Manager validates the configured placement of the vNICs and vHBAs against the number and capabilities of the physical adapters in the server before assigning the vNICs and vHBAs according to the configuration in the policy. Load distribution is based upon the explicit assignments to the vCons and adapters configured in this policy.

If the adapters do not support the assignment of one or more vNICs or vHBAs, Cisco UCS Manager raises a fault against the service profile.

Implicit Assignment of vNICs and vHBAs

With implicit assignment, Cisco UCS Manager determines the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned according to the capability of the adapters and their relative capacity. Use this assignment option if the adapter to which a vNIC or vHBA is assigned is not important to your system configuration.

To configure a vCon for implicit assignment, do the following:

- Set the vCon configuration to **All**, **Exclude Dynamic**, or **Exclude Unassigned**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server.
- Do not set the vCon configuration to **Assigned Only**. Implicit assignment cannot be performed with this setting.
- Do not assign any vNICs or vHBAs to a vCon.

During service profile association, Cisco UCS Manager verifies the number and capabilities of the physical adapters in the server and assigns the vNICs and vHBAs accordingly. Load distribution is based upon the capabilities of the adapters, and placement of the vNICs and vHBAs is performed according to the actual order determined by the system. For example, if one adapter can accommodate more vNICs than another, that adapter is assigned more vNICs.

If the adapters cannot support the number of vNICs and vHBAs configured for that server, Cisco UCS Manager raises a fault against the service profile.

Implicit Assignment of vNICs in a Dual Adapter Environment

When you use implicit vNIC assignment for a dual slot server with an adapter card in each slot, Cisco UCS Manager typically assigns the vNICs/vHBAs as follows:

- If the server has the same adapter in both slots, Cisco UCS Manager assigns half the vNICs and half the vHBAs to each adapter.
- If the server has one non-VIC adapter and one VIC adapter, Cisco UCS Manager assigns two vNICs and two vHBAs to the non-VIC adapter and the remaining vNICs and vHBAs to the VIC adapter.
- If the server has two different VIC adapters, Cisco UCS Manager assigns the vNICs and vHBAs proportionally, based on the relative capabilities of the two adapters.

The following examples show how Cisco UCS Manager would typically assign the vNICs and vHBAs with different combinations of supported adapter cards:

- If you want to configure four vNICs and the server contains two Cisco UCS M51KR-B Broadcom BCM57711 adapters (with two vNICs each), Cisco UCS Manager assigns two vNICs to each adapter.
- If you want to configure 50 vNICs and the server contains a Cisco UCS CNA M72KR-E adapter (2 vNICs) and a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs), Cisco UCS Manager assigns two vNICs to the Cisco UCS CNA M72KR-E adapter and 48 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter.
- If you want to configure 150 vNICs and the server contains a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs) and a Cisco UCS VIC-1240 Virtual Interface Card adapter (256 vNICs), Cisco UCS Manager assigns 50 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter and 100 vNICs to the Cisco UCS VIC-1240 Virtual Interface Card adapter.

Note Exceptions to this implicit assignment occur if you configure the vNICs for fabric failover and if you configure dynamic vNICs for the server.

For a configuration that includes vNIC fabric failover where one adapter does not support vNIC failover, Cisco UCS Manager implicitly assigns all vNICs that have fabric failover enabled to the adapter that supports them. If the configuration includes only vNICs that are configured for fabric failover, no vNICs are implicitly assigned to the adapter that does not support them. If some vNICs are configured for fabric failover and some are not, Cisco UCS Manager assigns all failover vNICs to the adapter that supports them and a minimum of one nonfailover vNIC to the adapter that does not support them, according to the ratio above.

For a configuration that includes dynamic vNICs, the same implicit assignment would occur. Cisco UCS Manager assigns all dynamic vNICs to the adapter that supports them. However, with a combination of dynamic vNICs and static vNICs, at least one static vNIC is assigned to the adapter that does not support dynamic vNICs.

Configuring a vNIC/vHBA Placement Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **create vcon-policy** *policy-name*	Creates the specified vNIC/vHBA placement profile and enters organization vcon policy mode.
Step 3	UCS-A /org/vcon-policy # **set descr** *description*	(Optional) Provides a description for the vNIC/vHBA Placement Profile. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote). **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.

	Command or Action	Purpose
Step 4	UCS-A /org/vcon-policy # **set mapping-scheme** {**round-robin** | **linear-ordered**}	(Optional) For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4. For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the selected virtual slot mapping scheme. This can be one of the following: • **round-robin—** In a server with two adapter cards, Cisco UCS assigns vCon1 and vCon3 to Adapter1, then assigns vCon2 and vCon4 to Adapter2. In a server with three adapter cards, Cisco UCS assigns vCon1 to Adapter1, vCon2 and vCon4 to Adapter2, and vCon3 to Adapter3. This is the default scheme. • **linear-ordered—** In a server with two adapter cards, Cisco UCS assigns vCon1 and vCon2 to Adapter1, then assigns vCon3 and vCon4 to Adapter2. In a server with three adapter cards, Cisco UCS assigns vCon1 to Adapter1 and vCon2 to Adapter2, then assigns vCon3 and vCon4 to Adapter3. In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme: • **round-robin—**Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default. • **linear-ordered—**Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.
Step 5	UCS-A /org/vcon-policy # **set vcon** {**1** | **2** | **3** | **4**} **selection** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	Specifies the selection preference for the specified vCon. The options are: • **all—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default. • **assigned-only—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA. • **exclude-dynamic—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.

	Command or Action	Purpose
		• **exclude-unassigned—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it. • **exclude-usnic—**Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic. **Note** An SRIOV usNIC that is explicitly assigned to a vCon set to **exclude-usnic** will remain assigned to that vCon.
Step 6	UCS-A /org/vcon-policy # **commit-buffer**	Commits the transaction.

The following example creates a vNIC/vHBA placement policy named Adapter1All, sets the vCon mapping scheme to Linear Ordered, specifies that only assigned vNICs and vHBAs can be placed on adapter 1, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create vcon-policy Adapter1
UCS-A /org/vcon-policy* # set descr "This profile places all vNICs and vHBAs on adapter 1."
UCS-A /org/vcon-policy* # set mapping-scheme linear-ordered
UCS-A /org/vcon-policy* # set vcon 1 selection assigned-only
UCS-A /org/vcon-policy* # commit-buffer
UCS-A /org/vcon-policy* #
UCS-A /org #
```

Deleting a vNIC/vHBA Placement Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **delete vcon-policy** *policy-name*	Deletes the specified vNIC/vHBA placement profile.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction.

The following example deletes the vNIC/vHBA placement profile named Adapter1All and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete vcon-policy Adapter1All
UCS-A /org* # commit-buffer
UCS-A /org #
```

Explicitly Assigning a vNIC to a vCon

Before You Begin

Configure the vCons through a vNIC/vHBA placement policy or in the service profile with one of the following values:

- **Assigned Only**
- **Exclude Dynamic**
- **Exclude Unassigned**

If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon. However, you have less control with this configuration.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the organization which contains the service profile whose vNICs you want to explicitly assign to a vCon. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope service-profile** *profile-name*	Enters organization service profile mode for the specified service.
Step 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	Enters organization service profile mode for the specified vnic.
Step 4	UCS-A /org/service-profile/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	Sets the virtual network interface connection (vCon) placement for the specified vNIC. Entering a value of any allows Cisco UCS Manager to determine the vCon to which the vNIC is assigned.
Step 5	UCS-A /org/service-profile/vnic # **set order** {*order-num* | **unspecified**}	Specifies the desired PCI order for the vNIC. Valid values include 0-128 and unspecified.
Step 6	UCS-A /org/service-profile/vnic # **commit-buffer**	Commits the transaction to the system configuration.

The following example sets the vCon placement for a vNIC called vnic3 to 2, sets the desired order to 10, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope vnic vnic3
UCS-A /org/service-profile/vnic # set vcon 2
UCS-A /org/service-profile/vnic* # set order 10
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

Explicitly Assigning a vHBA to a vCon

Before You Begin

Configure the vCons through a vNIC/vHBA placement policy or in the service profile with one of the following values:

- **Assigned Only**
- **Exclude Dynamic**
- **Exclude Unassigned**

If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon. However, you have less control with this configuration.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the organization which contains the service profile whose vHBAs you want to explicitly assign to a vCon. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope service-profile** *profile-name*	Enters organization service profile mode for the specified service.
Step 3	UCS-A /org/service-profile # **scope vhba** *vhba-name*	Enters organization service profile mode for the specified vHBA.
Step 4	UCS-A /org/service-profile/vhba # **set vcon** {**1** | **2** | **3** | **4** | **any**}	Sets the virtual network interface connection (vCon) placement for the specified vHBA. Entering a value of any allows Cisco UCS Manager to determine the vCon to which the vHBA is assigned.
Step 5	UCS-A /org/service-profile/vhba # **set order** {*order-num* | **unspecified**}	Specifies the desired PCI order for the vHBA. Valid desired order number values include 0-128 and unspecified.
Step 6	UCS-A /org/service-profile/vhba # **commit-buffer**	Commits the transaction to the system configuration.

The following example sets the vCon placement for a vHBA called vhba3 to 2, sets the desired order to 10, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope vhba vhba3
UCS-A /org/service-profile/vhba # set vcon 2
UCS-A /org/service-profile/vhba* # set order 10
UCS-A /org/service-profile/vhba* # commit-buffer
UCS-A /org/service-profile/vhba #
```

Placing Static vNICs Before Dynamic vNICs

For optimal performance, static vNICs and vHBAs should be placed before dynamic vNICs on the PCIe bus. Static vNICs refer to both static vNICs and vHBAs. Cisco UCS Manager Release 2.1 provides the following functionality regarding the order of static and dynamic vNICs:

- After upgrading to Cisco UCS Manager Release 2.1, if no change is made to existing service profiles (profiles that are defined in releases prior to Cisco UCS Manager Release 2.1), the vNIC order does not change.
- After an upgrade to Cisco UCS Manager Release 2.1, any vNIC-related change would reorder the vNIC map. As a result, all dynamic vNICs would be placed after the static vNICs.
- For newly created service profiles in Cisco UCS Manager Release 2.1, static vNICs are always ordered before dynamic vNICs.
- The above behavior is independent of the sequence of creating or deleting static or dynamic vNICs.
- For SRIOV-enabled service profiles, UCSM places the vNIC Physical Function(PF) before the corresponding Virtual Functions (VFs). This scheme guarantees that the VFs are placed close to the parent PF vNIC on the PCIe bus and BDFs are in successive incremental order for the VFs.

Example

Beginning Device Order in Cisco UCS Manager Release 2.0:

```
dyn-vNIC-1 1
dyn-vNIC-2 2
```

New Device Order in Cisco UCS Manager Release 2.0 (Add 2 static vNICs):

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

After upgrading to Cisco UCS Manager Release 2.1, (Before any vNIC-related change is made to the service profile.)

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

New Device Order in Cisco UCS Manager Release 2.1 (Add 2 dynamic vNICs by changing the policy count from 2 to 4.)

```
dyn-vNIC-1 3
dyn-vNIC-2 4
eth-vNIC-1 1
eth-vNIC-2 2
dyn-vNIC-3 5
dyn-vNIC-4 6
```

Dynamic vNICs as Multifunction PCIe Devices

Cisco UCS Manager Version 2.1 provisions static vNICs as 0-function devices (new BUS for every static vNIC). Multifunction dynamic vNICs are placed from the new Bus-slot after the last static vNIC/vHBA.

Note Cisco UCS Manager Version 2.1 supports the new StaticZero mode.

Table 3: Version Compatibility

Cisco UCS Manager		
Version 1.4 **Scheme: ZeroFunction**	**Version 2.0** **Scheme: ZeroFunction / MultiFunction**	**Version 2.1** **Scheme: ZeroFunction / MultiFunction / StaticZero**
Static and Dynamic vNICs are all on Bus [0-57], Function [0] < ZeroFunction Mode >	Static vNICs and Dynamic vNICs are on Bus [0-57], Function [0-7]. Bus 0, Function 0 Bus 0, Function 7 Bus 1, Function 0 < MultiFunction Mode >	Static vNICs or PFs will be on Bus [0-57], Function [0]. SRIOV: Corresponding VFs will be on the same Bus and Functions [1-255] No-SRIOV: Dynamic vNICs are on Bus [0-57], Function [0-7] < StaticZero Mode >
	Upgrade from Balboa will not renumber BDFs (remain in ZeroFunction mode) until Bus <= 57. Once devices exceed 58, switch to MultiFunction mode.	Upgrade from Balboa will not renumber BDFs (remain in ZeroFunction mode) until Bus <=57. Once devices exceed 58 or Platform specific maximum PCIe Bus number or change to SRIOV configuration, switch to StaticZero mode.
		Upgrade from Cisco UCS Manager Version 2.0 will not renumber BDFs (remain in ZeroFunction / MultiFunction mode). Once devices exceed 58 or Platfor specific maximum PCIe Bus number OR Change to SRIOV configuration, switch to StaticZero mode.

CIMC Mounted vMedia

Using Scriptable vMedia

Cisco UCS Manager allows provisioning of vMedia devices iso images for remote UCS servers. Using Scriptable vMedia, you can programmatically mount an IMG or an ISO image on a remote server. CIMC mounted vMedia provide communications between other mounted media inside your datacenter with no additional requirements media connection. Scriptable vMedia allows you to control virtual media devices without using a browser to manually map each 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.

Cisco UCS Manager Scriptable vMedia supports the following functionality:

- Booting from a specific vMedia device

- Copying files from a mounted share to a local disk
- Installation and updating OS drivers

Note Cisco UCS Manager support for Scriptable vMedia is applicable for CIMC mapped devices only. Existing KVM based vMedia devices are not supported.

vMedia mount fails when the following conditions are met:

1 The remote vMedia image filename in the vMedia policy is set to **Service-Profile-Name**.

2 The service profile is renamed.

This is because the change in the name of the service profile does not change the remote vMedia image filename in the vMedia policy. The image filename still points to the older image on the remote device, which cannot be found.

Creating a CIMC vMedia Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **create vmedia-policy** *policy-name*	Creates a vMedia policy with the specified policy name.
Step 3	UCS-A /org/vmedia-policy* # **create vmedia-mapping** *mapping -name*	Creates a vMedia policy sub-directory with the specified mapping name.
Step 4	UCS-A /org/vmedia-policy/vmedia-mapping # **set descr** *description*	(Optional) Provides a description for the vMedia policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCS-A /org/vmedia-policy/vmedia-mapping* # **set device type** *device-type*	Specifies the remote vMedia image type you wish to mount. Options are: • **CDD** • **HDD**
Step 6	UCS-A /org/vmedia-policy/vmedia-mapping* # **set image-file** *image-file-name*	Specifies the type of remote vMedia image file name.

	Command or Action	Purpose
Step 7	UCS-A /org/vmedia-policy/vmedia-mapping* # **set image-path** *image-path*	Specifies the remote vMedia image path.
Step 8	UCS-A /org/vmedia-policy/vmedia-mapping* # **set image-variable-name** {**none** | **service-profile-name**}	Specifies the name to be used for the image. Options are: • **none—**Enter the filename manually. • **service-profile-name—**Automatically uses the name of the service profile that the policy is associated with. **Note** If you specify the **image-variable-name** as the **service-profile-name**, do not rename the service profile. Renaming the service profile can result in vMedia mount failure.
Step 9	UCS-A /org/vmedia-policy/vmedia-mapping* # **set mount-protocol** *mount-protocol*	Specifies the remote vMedia mount protocol. Options are: • **CIFS** • **NFS** • **HTTP** • **HTTPS**
Step 10	UCS-A /org/vmedia-policy/vmedia-mapping* # **set auth-option** { **default** | **none** | **ntlm** | **ntlmi** | **ntlmssp** | **ntlmsspi** | **ntlmv2** | **ntlmv2i**}	Specifies the CIFS authentication options. This command is available only when you specify CIFS as the remote vMedia mount protocol. It is not available when you select any other remote vMedia mount protocol. The CIFS authentication options are: • **default—**NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **none—**No authentication is used. • **ntlm—**NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **ntlmi—**NTLMi security protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **ntlmssp—**NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **ntlmsspi—**Use this option only when you enable Digital Signing in the CIFS Windows server.

	Command or Action	Purpose
		• **ntlmv2—**NTLMv2 security protocol. Use this option only with Samba Linux. • **ntlmv2i—**NTLMv2i security protocol. Use this option only with Samba Linux.
Step 11	UCS-A /org/vmedia-policy/vmedia-mapping* # **set password**	Specifies the remote vMedia image password.
Step 12	UCS-A /org/vmedia-policy/vmedia-mapping* # **set remote-ip** *remote-ip*	Specifies the remote vMedia image IP address.
Step 13	UCS-A /org/vmedia-policy/vmedia-mapping* # **set user-id** *user-id*	Specifies the user id for mounting the vMedia device.
Step 14	UCS-A /org/vmedia-policy/vmedia-mapping* # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a vMedia policy named vMediaPolicy2, selects remote vMedia device type, mount protocol, image location, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create vmedia-policy vmediapolicy2
UCS-A /org/vmedia-policy* # create vmedia-mapping map1
UCS-A /org/vmedia-policy/vmedia-mapping* # set descr vmedia-map
UCS-A /org/vmedia-policy/vmedia-mapping* # set device-type cdd
UCS-A /org/vmedia-policy/vmedia-mapping* # set image-file-name win2011.iso
UCS-A /org/vmedia-policy/vmedia-mapping* # set image-path cifs
UCS-A /org/vmedia-policy/vmedia-mapping* # set image-variable-name service-profile-name
UCS-A /org/vmedia-policy/vmedia-mapping* # set mount-protocol cifs
UCS-A /org/vmedia-policy/vmedia-mapping* # set auth-option default
UCS-A /org/vmedia-policy/vmedia-mapping* # set password Password:
UCS-A /org/vmedia-policy/vmedia-mapping* # set remote-ip 172.41.1.158
UCS-A /org/vmedia-policy/vmedia-mapping* # set user-id Adminstrator
UCS-A /org/vmedia-policy/vmedia-mapping* # commit-buffer
```

Note When vMedia policy is created the **Retry on Mount Fail** option is set to **Yes**. The following example changes the **Retry on Mount Fail** option to **No** .

```
UCS-A# scope org /
UCS-A /org # create vmedia-policy vmediapolicy2
UCS-A /org/vmedia-policy* # set retry-on-mount-fail No
UCS-A /org/vmedia-policy* # commit-buffer
```

When you set the **Retry on Mount Fail** option to **No**, a warning message appears stating: **This will disable automatic retry of mount in case of any vMedia mount failure**.