Server Policies

Server Policies

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

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

BIOS Policy

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

To use a BIOS policy:

1. Create the BIOS policy in Cisco UCS Central.
2. Assign the BIOS policy to one or more service profiles.
3. Associate the service profile with a server.

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

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in a 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. Alternatively, 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 Central.

Depending on 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 Central to view the actual BIOS settings on a server and determine whether they are meeting current needs.

Note Cisco UCS Central 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.

Creating a BIOS Policy

Procedure

Step 1 UCSC# **connect policy-mgr**

Enters policy manager mode.

Step 2 UCSC(policy-mgr)# **scope org** *org-name*

Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .

Step 3 UCSC(policy-mgr) /org # **create bios-policy** *BIOS policy name*

Creates the BIOS policy and enters BIOS policy mode.

Step 4 UCSC(policy-mgr) /org/bios-policy # **set** *BIOS settings*

Configure the BIOS settings. For descriptions and information about the options for each CLI BIOS setting, see the following topics:

- Basic BIOS Settings
- Processor BIOS Settings
- I/O BIOS Settings
- RAS Memory BIOS Settings
- USB BIOS Settings
- PCI BIOS Settings
- Boot Options BIOS Settings
- Server Manager BIOS Settings
- Console BIOS Settings

Step 5 UCSC(policy-mgr) /org/bios-policy # **commit-buffer**

Commits the transaction to the system configuration.

Example

The following example shows how to create a BIOS policy under the root organization, and set the NUMA configuration:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/ org #create bios-policy biosPolicy3
UCSC(policy-mgr) /org/bios-policy* # set numa-config numa-optimization enabled
UCSC(policy-mgr) /org/bios-policy* # commit-buffer
UCSC(policy-mgr) /org/bios-policy #
```

Deleting a BIOS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete bios-policy** *policy-name*	Deletes the specified BIOS policy.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete a BIOS policy in the root organization:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/ org #delete bios-policy biosPolicy3
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Default BIOS Settings

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

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

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

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

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

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

Basic BIOS Settings

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

Name	Description
Organization	Select an organization.
Name	Enter a name between 1 and 16 alphanumeric characters.

Name	Description
Description	Enter up to 256 characters. you can use any characters or spaces except ' (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Reboot on BIOS Settings Change	When the server is rebooted after you change one or more BIOS settings. —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. —If you do not enable this setting, the BIOS changes are not applied until the next time the server is rebooted, whether as a result of another server configuration change or a manual reboot.
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The serial port is disabled. • —The serial port is enabled.
Quiet Boot	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS displays all messages and Option ROM information during boot. • —The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS continues to attempt to boot the server. • —The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.

Name	Description
Front Panel Lockout	Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The power and reset buttons on the front panel are active and can be used to affect the server. • —The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.
Consistent Device Naming (CDN)	Whether Consistent Device Naming (CDN) is enabled. CDN allows Ethernet interfaces to be named in a consistent manner, making Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —CDN is disabled for this BIOS policy. • —CDN is enabled for this BIOS policy.
Resume AC On Power Loss	How the server behaves when power is restored after an unexpected power loss. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server is powered on and the system attempts to restore its last state. • —The server is powered on and automatically reset. • —The server remains off until manually powered on.
QuickPath Interconnect (QPI) Link Frequency	The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **6400** • **7200** • **8000** • **9600** • —The CPU determines the QPI link frequency.

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

Processor BIOS Settings

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

Table 1: Basic Tab

Name	Description
Execute Disabled Bit	Classifies memory areas on the server to specify where the application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not classify memory areas. • —The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Data from I/O devices is not placed directly into the processor cache. • —Data from I/O devices is placed directly into the processor cache.
Local X2 Application Policy Infrastructure Controller (APIC)	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. • —Automatically uses the xAPIC architecture that is detected. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • —The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • — The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
P-STATE Coordination	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. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Balanced**— DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance**—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • —DRAM clock throttling is increased to improve energy efficiency. • —The CPU determines the level.
Channel Interleaving	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: • —The CPU determines what interleaving is done. • **1 Way**—Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way**—The maximum amount of channel interleaving is used. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Rank Interleaving	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: • —The CPU determines what interleaving is done. • **1 Way**—Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way**—The maximum amount of rank interleaving is used. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • —The CPU determines the physical elevation. • —The server is approximately 300 meters above sea level. • —The server is approximately 900 meters above sea level. • —The server is approximately 1500 meters above sea level. • —The server is approximately 3000 meters above sea level. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
CPU Hardware Power Management	Manages the CPU power functions. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not classify memory areas. • —The processor classifies memory areas.
Energy Performance Tuning	This item selects whether the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not use energy performance management. • —The processor uses energy performance management.
Workload Configuration	The BIOS uses values that are default for the server type and vendor. Balanced is selected for workload optimization. This is the recommended setting. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The workload configuration optimazations are disabled. • —The workload configuration optimazations are enabled.

Table 2: Prefetchers Tab

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

Name	Description
Data Cache Unit (DCU) IP Prefetcher	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: • —The processor does not preload any cache data. • —The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Table 3: Technology Tab

Name	Description
Turbo Boost	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not increase its frequency automatically. • —The processor uses Turbo Boost Technology if required.
Enhanced Intel Speed Step	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor never dynamically adjusts its voltage or frequency. • —The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.

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

Table 4: Power Tab

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

Name	Description
Processor C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The system remains in a high-performance state even when idle. • —The system can reduce power to system components such as the DIMMs and CPUs. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Processor C1E	Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU continues to run at its maximum frequency in the C1 state. • —The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state.
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —For M3 servers, all prefetchers and data reuse are enabled. For M1 and M2 servers, data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • —Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • —All prefetchers are enabled and data reuse is disabled. This setting is also known as high-performance computing. • **Custom**

Name	Description
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU determines the available power. • —The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • —When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • —When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • —When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves more power than C7, but it also requires the longest time for the server to return to high performance mode. • —The server may enter any available C state.

Table 5: Errors and Reporting Tab

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

Name	Description
Processor CMCI	The BIOS uses values that are default for the server type and vendor. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • — Corrected Machine Check Interrupt is not generated. • — Corrected Machine Check Interrupt is generated.
Max Variable MTRR Setting	Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —BIOS uses the default value for the processor. • **8**—BIOS uses the number specified for the variable MTRR.
Demand Scrub	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • — Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. • — Single bit memory errors are not corrected.
Patrol Scrub	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running. • —The system checks for memory ECC errors only when the CPU reads or writes a memory address.

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

I/O BIOS Settings

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

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

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

RAS Memory BIOS Settings

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

Name	Description
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • —The BIOS does not support NUMA.

Name	Description
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • —The system prioritizes high frequency operations over low voltage operations. • —The CPU determines the priority.
DRAM Refresh Rate	The refresh interval rate for internal memory. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **1x** • **2x** • **3x** • **4x** •
Memory RAS Configuration Mode	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —System performance is optimized. • —System reliability is optimized by using half the system memory as backup. • —If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers. • —Enables sparing mode.

Name	Description
Sparing Mode	Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population. This option is only available if you choose the sparing option for the Memory RAS Config parameter. It can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • —A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank.
DDR3 Voltage Selection	The voltage to be used by the dual-voltage RAM. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • •

USB BIOS Settings

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

Basic Tab

Name	Description
Make Device Non Bootable	Whether the server can boot from a USB device. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server can boot from a USB device. • —The server cannot boot from a USB device.

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

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

Device Management Tab

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

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

PCI BIOS Settings

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

Table 6: Basic Tab

Name	Description
Max Memory Below 4G	Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Does not maximize memory usage. Choose this option for all operating systems with PAE support. • —Maximizes memory usage below 4GB for an operating system without PAE support.
Memory Mapped IO Above 4Gb Configuration	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • —Maps I/O of 64-bit PCI devices to 4GB or greater address space.

Name	Description
VGA Priority	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: • —Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • —Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • —Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled. • —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.
PCIe OptionROMs	Whether Option ROM is available on all expansion ports. This can be one of the following: • —The expansion slots are not available. • —The expansion slots are available. • —The expansion slots are available for UEFI only. • —The expansion slots are available for legacy only. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Mezz OptionRom	Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —All LOM ports are enabled. • —All LOM ports are disabled.

Name	Description
PCIe 10G LOM 2 Link	Whether Option ROM is available on the 10G LOM port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is available. • —The expansion slot is not available.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU determines the power state. • —ASPM support is disabled in the BIOS. • —Force all links to L0 standby (L0s) state.

Table 7: PCIe Slot Link Speed Tab

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

Table 8: PCIe Slot OptionROM Tab

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

Name	Description
Slot MLOM	Whether Option ROM is available on the PCIe slot connected to the MLOM available on the specified port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot N1	Whether is available on the specified port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot N2	Whether is available on the specified port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
PCI ROM CLPset pci-rom-clp-support pci-rom-clp-config	The following options are available for PCI ROM CLP. • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. .

Name	Description
SIOC1 Option ROMset sloc1-option rom-config sloc1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
SB Mezz1 Option ROMset sbmezz1 -optionrom-config sbmezz1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IOE Slot1 Option ROMset ioeslot1-option-config ioeslot1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IOE Mezz1 Option ROMset ioemezz1-optionrom-config ioemezz1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.

Name	Description
IOE Slot2 Option ROMset ioeslot2-optionrom-config ioeslot2-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IO ENVMe1 Option ROMset ioenvme1-optionrom-config ioenvme1 -optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IO ENVMe2 Option ROMset ioenvme2-optionrom-config ioenvme2 -optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
SBNVMe1 Option ROMset ioenvme1-optionrom-config ioenvme1 -optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.

Graphics Configuration BIOS Settings

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

Name	Description
Integrated Graphics	Enables integrated graphics. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Integrated graphic is enabled. • —Integrated graphics is disabled.
Integrated Graphics Aperture Size	Allows you to set the size of mapped memory for the integrated graphics controller. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • • • • • •
Onboard Graphics	Enables onboard graphics (KVM). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Onboard graphics is enabled. • —Onboard graphics is disabled.

Boot Options BIOS Settings

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

Name	Description
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Waits for user input before retrying NON-EFI based boot options. • —Continually retries NON-EFI based boot options without waiting for user input.

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

Server Manager BIOS Settings

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

Name	Description
Assert NMI on SERR	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS does not generate an NMI or log an error when a SERR occurs. • —The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert Nmi on Perr**.

Name	Description
Assert NMI on PERR	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS does not generate an NMI or log an error when a PERR occurs. • —The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert Nmi on Serr** to use this setting.
OS Boot Watchdog Timer	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The watchdog timer is not used to track how long the server takes to boot. • —The watchdog timer tracks how long the server takes to boot. If the server does not boot within the predefined length of time, the CIMC resets the system and logs an error. This feature requires either operating system support or Intel Management software.
FRB-2 Timer	Whether the FRB-2 timer is used to recover the system if it hangs during POST. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The FRB-2 timer is not used. • —The FRB-2 timer is started during POST and used to recover the system if necessary.
Out of Band Management	This is used for the Windows Special Administration Control (SAC). • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The option to use the Windows Special Administration Control (SAC) is disabled. • —The option to use the Windows Special Administration Control (SAC) is enabled.

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

Console BIOS Settings

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

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

Name	Description
BAUD Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **9600**—A 9600 BAUD rate is used. • **19200**—A 19200 BAUD rate is used. • **38400**—A 38400 BAUD rate is used. • **57600**—A 57600 BAUD rate is used. • **115200**—A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **pc-ansi**—The PC-ANSI terminal font is used. • **vt100**—A supported vt100 video terminal and its character set are used. • **vt100-plus**—A supported vt100-plus video terminal and its character set are used. • **vt-utf8**—A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **None**—No flow control is used. • —RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **ESCN**—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as **ESC [11~** and **ESC [12~**. • **LINUX**—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate **ESC [[A** through **ESC [[E**. • **SCO**—The function keys F1 to F12 generate **ESC [M** through **ESC [X**. The function and shift keys generate **ESC [Y** through **ESC [j**. The control and function keys generate **ESC [k** through **ESC [v**. The shift, control and function keys generate **ESC [w** through **ESC [{**. • **vt100**—The function keys generate **ESC OP** through **ESC O[.** • **VT400**—The function keys behave like the default mode. The top row of the numeric keypad generates **ESC OP** through **ESC OS**. • **XTERMR6**—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals.

IPMI Access Profile

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

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

Configuring an IPMI Access Profile

Before you begin

Obtain the following:

- Username that the operating system of the server can authenticate

- Password for the username
- Permissions associated with the username

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create ipmi-access-profile** *profile-name*	Creates the specified IPMI access profile and enters organization IPMI access profile mode.
Step 4	UCSC(policy-mgr) /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	UCSC(policy-mgr) /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	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	Specifies whether the endpoint user has administrative or read-only privileges.
Step 7	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create an IPMI access profile named ReadOnly
- Create an endpoint user named bob
- Set the password and the privileges for bob

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
```

```
UCSC(policy-mgr) /org # create ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org/ipmi-access-profile* # create ipmi-user bob
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCSC(policy-mgr) /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	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete ipmi-access-profile** *profile-name*	Deletes the specified IPMI access profile.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes the IPMI access profile named ReadOnly:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Adding an Endpoint User to an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **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 3	UCSC(policy-mgr) /org # **scope ipmi-access-profile** *profile-name*	Enters organization IPMI access profile mode for the specified IPMI access profile.
Step 4	UCSC(policy-mgr) /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	UCSC(policy-mgr) /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	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	Specifies whether the endpoint user has administrative or read-only privileges.
Step 7	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org/ipmi-access-profile* # create ipmi-user alice
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user #
```

Deleting an Endpoint User from an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope ipmi-access-profile** *profile-name*	Enters organization IPMI access profile mode for the specified IPMI access profile.
Step 4	UCSC(policy-mgr) /org/ipmi-access-profile # **delete ipmi-user** *epuser-name*	Deletes the specified endpoint user from the IPMI access profile.
Step 5	UCSC(policy-mgr) /org/ipmi-access-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org/ipmi-access-profile # delete ipmi-user alice
UCSC(policy-mgr) /org/ipmi-access-profile* # commit-buffer
UCSC(policy-mgr) /org/ipmi-access-profile #
```

Serial over LAN Policy

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

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

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

Configuring a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create sol-policy** *policy-name*	Creates a serial over LAN policy and enters organization serial over LAN policy mode.

	Command or Action	Purpose
Step 4	(Optional) UCSC(policy-mgr) /org/sol-policy # **set descr** *description*	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 5	UCSC(policy-mgr) /org/sol-policy # **set speed** {**115200** | **19200** | **38400** | **57600** | **9600**}	Specifies the serial baud rate.
Step 6	UCSC(policy-mgr) /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 7	UCSC(policy-mgr) /org/sol-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create a serial over LAN policy named Sol9600
- Provide a description for the policy
- Set the speed to 9,600 baud
- Enable the policy

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create sol-policy Sol9600
UCSC(policy-mgr) /org/sol-policy* # set descr "Sets serial over LAN policy to 9600 baud."
UCSC(policy-mgr) /org/sol-policy* # set speed 9600
UCSC(policy-mgr) /org/sol-policy* # enable
UCSC(policy-mgr) /org/sol-policy* # commit-buffer
UCSC(policy-mgr) /org/sol-policy #
```

Viewing a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /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.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # show sol-policy Sol9600

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

iSCSI Adapter Policy

Creating an iSCSI Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create iscsi-policy** *policy-name*	Creates the iSCSI adapter policy.
Step 4	(Optional) UCSC(policy-mgr) /org/iscsi-policy # **set descr** "*description*"	Provides a description for the iSCSI adapter policy.
Step 5	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item connection-timeout** *timeout-secs*	The number of seconds until Cisco UCS Central assumes that the initial login has failed and the iSCSI adapter is unavailable.

	Command or Action	Purpose
		Enter an integer between 0 and 255. If you enter 0, Cisco UCS Central uses the value set in the adapter firmware (default: 15 seconds).
Step 6	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item dhcp-timeout** *timeout-secs*	The number of seconds to wait before the initiator assumes that the DHCP server in unavailable. Enter an integer between 60 and 300 (default: 60 seconds).
Step 7	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item lun-busy-retry-count** *num*	The number of times to retry the connection in case of a failure during iSCSI LUN discovery. Enter an integer between 0 and 60. If you enter 0, Cisco UCS Central uses the value set in the adapter firmware (default: 15 seconds).
Step 8	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item tcp-time-stamp** {**no** | **yes**}	Specifies whether to apply a TCP timestamp. With this setting, transmitted packets are given a time stamp of when the packet was sent so that the packet's round-trip time can be calculated, when needed. This setting applies only to Cisco UCS M51KR-B Broadcom BCM57711 adapters.
Step 9	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item hbamode** {**no** | **yes**}	Specifies whether to enable HBA mode. This option should only be enabled for servers with the Cisco UCS NIC M51KR-B adapter running the Windows operating system.
Step 10	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item boottotarget** {**no** | **yes**}	Specifies whether to boot from the iSCSI target. This option only applies to servers with the Cisco UCS NIC M51KR-B adapter. It should be disabled until you have installed an operating system on the server.
Step 11	Required: UCSC(policy-mgr) /org/iscsi-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create an iSCSI adapter policy called iscsiboot
- Set the connection timeout
- DHCP timeout

- LUN busy retry count
- Apply a TCP timestamp

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCS-AUCSC(policy-mgr)UCS-A /org # create iscsi-policy iscsiboot
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item connection-timeout 60
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item dhcp-timeout 200
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item lun-busy-retry-count 5
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item tcp-time-stamp yes
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item hbamode yes
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item boottotarget yes
UCSC(policy-mgr) /org/iscsi-policy* # commit-buffer
UCSC(policy-mgr) /org/iscsi-policy #
```

What to do next

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

Deleting an iSCSI Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete iscsi-policy** *policy-name*	Deletes the iSCSI adapter policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete an iSCSI adapter policy named iscsi-adapter-pol:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete iscsi-policy iscsi-adapter-pol
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Creating an iSCSI Authentication Profile

If you use authentication for iSCSI boot, you need to create an authentication profile for both the initiator and target.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create auth-profile** *profile-name*	Creates an authentication profile with the specified name. The name can be up to 16 alphanumeric characters.
Step 4	UCSC(policy-mgr) /org/auth-profile # **set user-id** *id-name*	Creates a log in for authentication.
Step 5	UCSC(policy-mgr) /org/auth-profile # **set password**	Creates a password for authentication.
Step 6	UCSC(policy-mgr) /org/auth-profile # **commit-buffer**	Commits the transaction to the system configuration.
Step 7	UCSC(policy-mgr) /org/auth-profile # **exit**	Exits the current mode.
Step 8	Repeat steps 3 through 7 to create an authentication profile for the target.	
Step 9	Required: UCSC(policy-mgr) /org/auth-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create an authentication profile for an initiator and a target:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create auth-profile InitAuth
UCSC(policy-mgr) /org/auth-profile* # set user-id init
UCSC(policy-mgr) /org/auth-profile* # set  password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/auth-profile* # commit-buffer
UCSC(policy-mgr) /org/auth-profile # exit
UCSC(policy-mgr) /org # create auth-profile TargetAuth
UCSC(policy-mgr) /org/auth-profile* # set user-id target
UCSC(policy-mgr) /org/auth-profile* # set  password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/auth-profile* # commit-buffer
UCSC(policy-mgr) /org/auth-profile # exit
```

What to do next

Create an Ethernet vNIC for use as the overlay vNIC for the iSCSI device. Then create an iSCSI vNIC.

Deleting an iSCSI Authentication Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete auth-profile** *profile-name*	Deletes the specified iSCSI authentication profile.
Step 4	Required: UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete an iSCSI authentication profile and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # delete auth-profile InitAuth
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Local Disk Policy

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

The local disk modes include the following:

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

- **RAID 5 Striped Parity**
- **RAID 50 Striped Parity Striped**

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

The B200 M3 server supports JBOD mode for local disks.

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. 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 associates a service profile containing this local disk policy with a server, verifies that the selected RAID option is properly licensed. If there are issues, 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	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create local-disk-config-policy** *policy-name*	Creates a local disk configuration policy and enters local disk configuration policy mode.
Step 4	(Optional) UCSC(policy-mgr) /org/local-disk-config-policy # **set descr** *description*	Provides a description for the local disk configuration policy.
Step 5	UCSC(policy-mgr) /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-50-striped-parity-and-striped** | **raid-6-striped-dual-parity** | **raid-60-striped-parity-and-striped** | **raid-10-mirrored-and-striped**}	Specifies the mode for the local disk configuration policy.
Step 6	UCSC(policy-mgr) /org/local-disk-config-policy # **set protect** {**yes** | **no**}	Set configuration protection to yes in order to prevent a service profile using this local disk policy from being associated to a server with a different physical disk configuration. If the service profile includes a local disk policy with configuration protection enabled, and there is an attempt to associate that service profile to a server that includes disks with a different local disk configuration, the association immediately fails and produces a configuration mismatch error.

	Command or Action	Purpose
		Caution We recommend that you enable configuration protection to preserve any data that may exist on local disks. If disabled, any existing volume that does not match the local disk configuration policy will be deleted.
Step 7	UCSC(policy-mgr) /org/local-disk-config-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example configures a local disk configuration policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create local-disk-config-policy DiskPolicy7
UCSC(policy-mgr) /org/local-disk-config-policy* # set mode raid-1-mirrored
UCSC(policy-mgr) /org/local-disk-config-policy* # set protect yes
UCSC(policy-mgr) /org/local-disk-config-policy* # commit-buffer
UCSC(policy-mgr) /org/local-disk-config-policy #
```

Viewing a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /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.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /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	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete local-disk-config-policy** *policy-name*	Deletes the specified local disk configuration policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete local-disk-config-policy DiskPolicy7
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Scrub Policy

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

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

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

Disk scrub

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

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

BIOS Settings Scrub

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

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

FlexFlash Scrub

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

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

Note

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

Creating a Scrub Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create scrub-policy** *policy-name*	Creates a scrub policy with the specified policy name, and enters organization scrub policy mode.
Step 4	(Optional) UCSC(policy-mgr) /org/scrub-policy # **set descr** *description*	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 5	UCSC(policy-mgr) /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 6	UCSC(policy-mgr) /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 7	UCSC(policy-mgr) /org/scrub-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates and enables a scrub policy named ScrubPolicy2 on servers using the scrub policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create scrub-policy ScrubPolicy2
UCSC(policy-mgr) /org/scrub-policy* # set descr "Scrub disk but not BIOS."
UCSC(policy-mgr) /org/scrub-policy* # set disk-scrub yes
UCSC(policy-mgr) /org/scrub-policy* # set bios-settings-scrub no
UCSC(policy-mgr) /org/scrub-policy* # commit-buffer
UCSC(policy-mgr) /org/scrub-policy #
```

Deleting a Scrub Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete scrub-policy** *policy-name*	Deletes the specified scrub policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete scrub-policy ScrubPolicy2
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

vMedia Policy

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

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

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

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

- Boot from a specific vMedia device
- Copy files from a mounted share to local disk
- Install and update OS drivers

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

Creating a vMedia Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create vmedia-policy** *policy-name*	Creates the specified vMedia policy and enters organization vMedia policy mode.
Step 4	UCSC(policy-mgr) /org/vmedia-policy # **set retry-on-mount-fail** {**yes** | **no**}	Select whether the vMedia will continue mounting when a mount failure occurs.
Step 5	UCSC(policy-mgr) /org/vmedia-policy # **create vmedia-mapping** *name*	Creates a vMedia policy sub-directory with the specified mapping name.
Step 6	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set device-type** {**cdd** | **hdd**}	Specifies the remote vMedia image type that you wish to mount.
Step 7	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set image-file-name** *filename*	Specifies the image file name.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set image-path** *path*	Specifies the image path.
Step 9	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set image-variable-name** {**none** | **service-profile-name**}	Specifies the name to be used for the image. This can be one of the following: • **none**—Enter the name manually. • **service-profile-name**—Automatically uses the name of the service profile that the policy is associated with. **Note** The service profile must be available at the required path, and you cannot change the name of the service profile.
Step 10	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set mount-protocol** {**cifs** | **http** | **https** | **nfs**}	Specifies the remote vMedia protocol.
Step 11	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set auth-option** {**default** | **none** | **ntlm** | **ntlmi** | **ntlmssp** | **ntlmsspi** | **ntlmv2** | **ntlmv2i**}	Specifies the remote authentication options.
Step 12	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set password** *password*	Specifies the password.
Step 13	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set remote-ip** *ip-address*	Specifies the remote IP address.
Step 14	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set user-id** *name*	Specifies the user ID for mounting the vMedia device.
Step 15	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create a vMedia policy named vMediaPol2
- Create a mapping directory called MapDir
- Specify the device type and other criteria

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create vmedia-policy vmediaPol2
UCSC(policy-mgr) /org/vmedia-policy* # create vmedia-mapping MapDir
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set device-type hdd
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set image-file-name win2011.iso
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set image-path /home/vMedia
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set password MyPass
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set remote-ip 10.0.0.0
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set user-id VMediaAdmin
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # commit-buffer
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping #
```

Creating or Editing Power Sync Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create power-sync-policy***name*	Creates power-sync policy for the specified organization.
Step 4	UCSC(policy-mgr) /org/power-sync policy* # **commit-buffer**	Commits the transaction to the system.
Step 5	UCSC(policy-mgr) /org/power-sync policy # **set**	
Step 6	UCSC(policy-mgr) /org/power-sync policy* # **set syncoption**	Displays the power sync policy options. They can be one of the following : • always-sync - During shallow association, this option will always sync desired power state to the physical server even if the physical server power state is on and the desired power state is off. • default-sync - During shallow association, this option will sync desired power state to the physical server if the physical server power state is off and the desired power state is on. • initial-only-sync - This option only syncs power to the server during deep association, the first time we associate the service profile to a new server. During shallow association, this option does not

	Command or Action	Purpose
		sync power. When the user resets or cycles physical server power and this option is enabled, we will not set the desired power state for the service profile.
Step 7	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 8	UCSC(resource-mgr) /org # **scope service-profile** *profile-name*	Enters service profile organization mode for the service profile.
Step 9	UCSC(resource-mgr) /org/ service-profile # **set power-sync-policy** *name*	

Example

The following example shows how to create a power-sync policy and assign it to a service profile:

```
 UCSC(policy-mgr)# scope org
 UCSC(policy-mgr) /org # create power-sync-policy PowerSync
 UCSC(policy-mgr) /org/power-sync-policy* # set syncoption initial-only-sync
 UCSC(policy-mgr) /org/power-sync-policy* # commit-buffer
 UCSC(policy-mgr) /org/power-sync-policy # end
 UCSC(policy-mgr)# exit

UCSC(resource-mgr)# scope org
UCSC(policy-mgr)(resource-mgr) /org # scope service-profile AAA
UCSC(policy-mgr)(resource-mgr) /org/service-profile # set power-sync-policy PowerSync
UCSC(policy-mgr)(resource-mgr) /org/service-profile* # commit-buffer
```

Creating a Statistics Threshold Policy

Cisco UCS Central lets you create a statistics threshold policy that monitors statistics about certain aspects of the system and generates an event if the threshold is crossed.

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr) # **connect policy-mgr**	Enters the policy-manager mode.
Step 2	UCSC(policy-mgr)/org # **create stats-threshold-policy** *policy-name*	Creates statistics threshold policy and assigns a name to the policy.
Step 3	UCSC(policy-mgr)/org/stats-threshold-policy* # **create class nvme-stats**	Creates a class for the policy.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr)/org/stats-threshold-policy # **create property temperature**	Creates a property (temperature) for the policy.
Step 5	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **set normal value** *number-value*	Sets a normal value.
Step 6	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **create threshold d-value above-normal warning**	Creates above normal warning range.
Step 7	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **set escalating** *number-value*	Sets the escalating value of the property.
Step 8	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **set deescalating** *number-value*	Sets the deescalating value of the property
Step 9	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how Cisco UCS Central creates a statistical threshold policy called test:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org

UCSC(policy-mgr) /org # create stats-threshold-policy test
UCSC(policy-mgr) /org/stats-threshold-policy* # create class nvme-stats
UCSC(policy-mgr) /org/stats-threshold-policy/class* #create property  temperature
UCSC(policy-mgr) /org/stats-threshold-policy/class/property* # set normal-value    100
UCSC(policy-mgr) /org/stats-threshold-policy/class/property* # create threshol d-value
above-normal warning
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* # set escalating
 104
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* #  set
deescalating 101
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value # show
configuration
enter threshold-value above-normal warning
     set deescalating 101.000000
     set escalating 104.000000
exit
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value # exit
UCSC(policy-mgr) /org/stats-threshold-policy/class/property # exit
UCSC(policy-mgr) /org/stats-threshold-policy/class # exit
UCSC(policy-mgr) /org/stats-threshold-policy # show configuration
enter stats-threshold-policy test
     enter class nvme-stats
         enter property temperature
             enter threshold-value above-normal warning
                 set deescalating 101.000000
                 set escalating 104.000000
             exit
             set normal-value 100.000000
         exit
     exit
```

```
     set descr ""
exit
UCSC(policy-mgr) /org/stats-threshold-policy #
```

Monitoring Threshold Statistics

Cisco UCS Central lets you monitor statistics about aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds which are enforced by endpoints, such as the CIMC.

Note The thresholds are burned into the hardware components at manufacture.

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr) # **scope system**	Enters into the system.
Step 2	UCSC(resource-mgr) /system # **show stats**	

Example

The following example shows how Cisco UCS Central displays threshold statistics:

```
UCSC(resource-mgr) /system # scope server
UCS-A /chassis/server # show stats

Mb Power Stats:
    Time Collected: 2010-04-20T08:45:31.209
    Monitored Object: sys/chassis-2/blade-4/board
    Suspect: No
    Consumed Power (W): 116.653679
    Input Voltage (V): 12.051000
    Input Current (A): 9.680000
    Thresholded: Input Voltage Min

Mb Temp Stats:
    Time Collected: 2010-04-20T08:45:31.209
    Monitored Object: sys/chassis-2/blade-4/board
    Suspect: No
    Fm Temp Sen Io (C): 19.000000
    Fm Temp Sen Rear (C): 18.000000
    Fm Temp Sen Rear L (C):: N/A
    Fm Temp Sen Rear R (C): N/A
    Thresholded: 0

UCS-A /chassis/server #
```

Creating or Editing a Hardware Change Discovery Policy

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

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group# **create server-hwchange-disc-policy** *name*	Creates a Hardware Change Discovery policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy *# **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy # **show detail**	Displays details of the Hardware Change Discovery policy .
Step 6	(Optional) UCSC(policy-mgr) /domain-group# **scope server-hwchange-disc-policy** *name*	Enters the specific Hardware Change Discovery Policy.
Step 7	(Optional) UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy *# **show detail**	Displays details of the Hardware Change Discovery policy .
Step 8	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy # **set action user-acknowledged**	Sets the status of the Hardware Change Discovery policy to user acknowledged. This option would trigger a deep-discovery of hardware change after you acknowledge the server and clear the fault.
Step 9	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy *# **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a Hardware Change Discovery policy, show details of the policy, and how to set (edit) the policy.

```
UCSC(policy-mgr)connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create server-hwchange-disc-policy hwdp1
UCSC(policy-mgr) /domain-group/server-hwchange-disc-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/server-hwchange-disc-policy # show detail

Server Hardware Change Discovery Policy:
```

```
Name: hwdp1
Description:
Action: User Acknowledged

UCSC(policy-mgr) /domain-group/server-hwchange-disc-policy # exit
UCSC(policy-mgr) /domain-group # show server-hwchange-disc-policy
Server Hardware Change Discovery Policy:
Name Description Action
---------- ----------- ------
hcd-2 User Acknowledged
hd-test1 User Acknowledged
HW_CDP_DG2 User Ack on DG2
User Acknowledged
HwCDP-AutoAck
Auto Acknowledged
HWCDP-Demo1
User Acknowledged
HwCDP-UserAck
Auto Acknowledged
hwdp1 User Acknowledged
Editing a Policy

UCSC(policy-mgr)(policy-mgr) /domain-group/server-hwchange-disc-policy # set action
auto-acknowledged
UCSC(policy-mgr)(policy-mgr) /domain-group/server-hwchange-disc-policy* # commit-buffer
UCSC(policy-mgr)(policy-mgr) /domain-group/server-hwchange-disc-policy # show detail

Server Hardware Change Discovery Policy:
Name: hwdp1
Description:
Action: Auto Acknowledged
```

Deleting a Hardware Change Discovery Policy

Before you begin

You must have created a Hardware Change Discovery policy and assigned it to a domain.

Note If you delete this policy from Cisco UCS Central, the domain profile retains the policy name and automatically associates it with the policy when you create it later with the same name. When you delete a Hardware Change Discovery Policy from Cisco UCS Central, it becomes locally editable on Cisco UCS Manager.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **delete server-hw-change-disc-policy***name*	Deletes the Hardware Change Discovery policy in the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group *# **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group # **show server-hwchange-disc-policy**	Displays the existing Hardware Change Discovery policies in the system.

Example

This example displays the status of the existing Hardware Change Discovery policies in the system. The policy hwd2 is deleted and does not appear in the list of policies.

```
UCSC(policy-mgr)connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr)/domain-group # delete server-hwchange-disc-policy hwd2
UCSC(policy-mgr)/domain-group* # commit-buffer
UCSC(policy-mgr)/domain-group # show server-hwchange-disc-policy
Server Hardware Change Discovery Policy:
Name Description    Action
 ---   --------       ------
hwd-1 from Central User Acknowledged

test1            User Acknowledged
```

Assigning a Hardware Change Discovery Policy to a Domain

You can assign a **Hardware Change Discovery** policy in a domain group to a domain profile.

Before you begin

You must have created a **Hardware Change Discovery** policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile # **set hwchange-disc-policy-name** *name*	Assigns the Hardware Change Discovery policy to the domain profile .

	Command or Action	Purpose
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .
Step 7	(Optional) UCSC(resource-mgr) /fabric/domain/ domain-profile # **show detail**	Displays details of the domain profile and the Hardware Change Discovery Policy name assigned to this domain .

Example

This example shows how to assign a Hardware Discovery Policy hwd1 to a domain profile.

```
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr)/fabric # scope domain 1009
UCSC(resource-mgr)/fabric/domain # scope domain-profile default
UCSC(resource-mgr)/fabric/domain/domain-profile # set
descr hw-change-disc-policy-name inband-policy-name kmip-certificate-policy-name
outband-management-pool
port-disc-policy-name qos-class-policy-name
UCSC(resource-mgr)/fabric/domain/domain-profile # set hw-change-disc-policy-name hwdp1
UCSC(resource-mgr)/fabric/domain/domain-profile* # commit-buffer
UCSC(resource-mgr)/fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: hwdp1
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
```

Unassigning a Hardware Change Discovery Policy

You can un-assign a **Hardware Change Discovery** policy from a domain profile.

Before you begin

You must have assigned a Hardware Change Discovery policy to a domain profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.

	Command or Action	Purpose
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile # **set hw-change-disc-policy ''**	Un-assigns the Hardware Change Discovery policy from the domain profile. The empty string value indicates that no policy is associated with the domain. This prevents the policy from getting pushed down to Cisco UCS Manager.
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .

Example

This example shows how to un-assign a Hardware Change Discovery Policy from a domain profile.

```
UCSC(resource-mgr) /fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: hwdp1 <<< Before unassigned
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
UCSC(resource-mgr) /fabric/domain/domain-profile # set hw-change-disc-policy-name ''
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
UCSC(resource-mgr) /fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: << After Unassigned
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
```

Creating a Port Auto-Discovery Policy

You can create a Port Auto-Discovery Policy and assign it to a domain through the domain profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group# **create port-disc-policy** *name*	Creates a Port Auto-Discovery policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ port-disc-policy *# **set server-auto-disc enabled**	Sets the Port Auto-Discovery policy to automatically enabled status.
Step 5	UCSC(policy-mgr) /domain-group/ port-disc-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a Port Auto-Discovery Policy and set enable port auto discovery.

```
--------------------------------------------------------------------------------------------
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr)/domain-group # create port-disc-policy-p1
UCSC(policy-mgr)/domain-group/create port-disc-policy* # set server-auto-disc enabled
UCSC(policy-mgr)/domain-group/inband-policy* # commit-buffer
```

Assigning Port Auto-Discovery Policy to a Domain Profile

You can assign a **Port Auto-Discovery** policy in a domain group to a domain profile.

Before you begin

You must have created a port Auto-Discovery policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile *# **set port-policy***name*	Assigns the Port Auto-Discovery policy to the domain profile .

	Command or Action	Purpose
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .

Example

This example shows how to assign a Port Auto-Discovery Policy p1 to a domain profile.

```
UCSC # scope resource-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr)/fabric# scope domain 1009
UCSC(resource-mgr)/fabric/domain# scope domain-profile default
UCSC(resource-mgr) /fabric/domain/domain-profile # set port-policy p1
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
```

Unassigning a Port Auto-Discovery Policy from a Domain

Before you begin

You must have assigned a port Auto-Discovery policy to a domain profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile *# **set port-policy″ ″**	Un-assigns the Port Auto-Discovery policy from the domain profile. The empty string value indicates that no policy is associated with the domain profile and it will not be pushed down to Cisco UCS Manager.
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .

Example

This example shows how to un-assign a Port Auto-Discovery Policy from a domain profile.

```
UCSC # scope resource-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr)/fabric# scope domain 1009
UCSC(resource-mgr)/fabric/domain# scope domain-profile default
UCSC(resource-mgr) /fabric/domain/domain-profile # set port-policy " "
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
```

Creating a Graphics Card Policy

You can create a Graphics Card Policy to configure an NVIDIA GPU card and assign it to a service profile. This policy facilitates Cisco UCS Manager's support to NVIDIA GPU cards for blade servers. The GPU cards are integrated with the ability to upgrade device firmware through service profiles. Follow this procedure to create or edit or delete a graphics card policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create graphics-card-policy** *name*	Creates graphics card policy for the specified organization.
Step 4	UCSC(policy-mgr) /org/graphics-card-policy* # **commit-buffer**	Commits the pending transaction.

Example

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org
UCSC(policy-mgr) /org # create graphics-card-policy GPUName
UCSC(policy-mgr) /org/graphics-card-policy* # set
descr             graphicscardmode
```

Deleting a Graphics Card Policy

Before you begin

You must have created a Graphics card policy and assigned it to a service profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete graphics-card-policy***name*	Deletes the graphics-card-policy for the specified organization.
Step 4	UCSC* # **commit-buffer**	Commits any pending transactions.

Deleting a Graphics Card Policy

```
UCSC(policy-mgr)/org # delete graphics-card-policy GPU1
UCSC(policy-mgr)* # commit buffer
```

Associating a Service Profile to GPU card

Before you begin

You must have created a Graphics Card policy and assigned it to a service profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr) /org # **scope service-profile** *profile-name*	Enters service profile organization mode for the service profile.
Step 4	UCSC(resource-mgr) /org /service-profile # **set graphics-card-policy** *mode*	Specifies the GPU mode. It can be graphics, compute or any configuration.
Step 5	UCSC(resource-mgr) /org /service-profile* # **commit-buffer**	Commits the transaction to the system.

Example

This example shows how to associate a service profile to a GPU policy with no mode set.

```
UCSC # connect resource-mgr
```

```
UCSC (resource-mgr)# scope org
UCSC(resource-mgr) /org # scope service-profile GSP_1
UCSC(resource-mgr) /org/service-profile # set graphicscard-policy GPUNone
UCSC(resource-mgr) /org/service-profile* # commit-buffer
```

Inband Policy

Cisco UCS Central lets you configure the Inband IP address on a server directly, or through an **Inband Policy**. This feature is supported on Cisco UCS Manager release 3.1 (3) and later. After you create an Inband policy, you can assign it to a domain group from the **Domain Configuration Settings**. The **Inband Policy** displays details about the corresponding **VLAN Group**, the **Default Management VLAN**, and the **Management IP pool** associated with the policy.

Creating or Editing an Inband Policy

You can create an inband policy and assign it to a domain through the domain profile. You can manually configure the KVM inband IP on the domain servers or through the Inband policy. When you manually change the server's inband configuration, the domain's inband policy remains unchanged.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group# **create inband-policy** *name*	Creates an Inband policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ inband-policy *# **set net-group name** *name*	Assigns the netgroup to the inband-policy.
Step 5	UCSC(policy-mgr) /domain-group/ inband-policy *# **set default-ip-pool name**	Assigns the Management IP Pool to the Inband policy.
Step 6	UCSC(policy-mgr) /domain-group/ inband-policy *# **set default-net-name** *name*	Assigns the network (VLAN) to the Inband policy.
Step 7	UCSC(policy-mgr) /domain-group/ inband-policy *# **set default-net-group-name**	Assigns the netgroup to the Inband policy.
Step 8	UCSC(policy-mgr) /domain-group/ inband-policy* # **commit-buffer**	

Example

This example shows how to create an Inband Policy.

```
-------------------------------------------------------------------------------------------------
UCSC(policy-mgr)/domain-group # create inband-policy inband-123
UCSC(policy-mgr)/domain-group/inband-policy* # set net-group-name netgroup-123
UCSC(policy-mgr)/domain-group/inband-policy* # set default-net-name vlan-123
UCSC(policy-mgr)/domain-group/inband-policy* # set default-ip-pool ip-pool-123
UCSC(policy-mgr)/domain-group/inband-policy* # commit-buffer
UCSC(policy-mgr)/domain-group/inband-policy # show detail

Inband Policy:
Name: inband-123
Net Group Name: netgroup-123
Default Network: vlan-123
Default IP Pool: ip-pool-123
Name: inband-pol-1
Net Group Name:
Default Network:
Default IP Pool: pool-abc
UCSC(policy-mgr) /domain-group/inband-policy # exit
UCSC(policy-mgr) /domain-group # show inband-policy

Inband Policy:
Name Net Group Name Default Network Default IP Pool
---------- -------------- --------------- ---------------
inband-123 netgroup-123 vlan-123 ip-pool-123
```

Creating a Management IP Pool

You can create a Management IP Pool comprising IPv4 and IPv6 blocks and assign them to an Inband policy or use it as an Outband Pool.

Note IPv6 is not supported for Outband KVM management.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group# **create ip-pool** *pool-name*	Creates an IPv4 pool for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ ip-pool* # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group/ ip-pool# **create block** *IP from IP to Default Gateway Subnet Mask*	Creates an IPv4 pool block.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/ ip-pool/block* # **commit-buffer**	Commits the transaction to the system configuration.
Step 7	UCSC(policy-mgr) /domain-group/ ip-pool/block # **show detail**	Displays details of the IPv4 block.
Step 8	UCSC(policy-mgr) /domain-group/ ip-pool/block # **exit**	Exits the IP pool block.
Step 9	UCSC(policy-mgr) /domain-group/ ip-pool # **create IPv6-block** *IP from IP to prefix block qualifier*	Creates an IPv6 block.
Step 10	UCSC(policy-mgr) /domain-group/ ip-pool/ ipv6-block* # **commit-buffer**	Commits the transaction to the system configuration.
Step 11	UCSC(policy-mgr) /domain-group/ ip-pool/ ipv6-block* # **show detail**	Displays the block of IPv6 addresses.

Example

This example shows how to create an IP Pool and add block addresses.

```
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create ip-pool test
UCSC(policy-mgr) /domain-group/ip-pool* # commit buffer
UCSC(policy-mgr) /domain-group/ip-pool # create block 1.2.3.4 1.2.3.8 1.2.3.254 255.255.255.0

UCSC(policy-mgr) /domain-group/ip-pool/block* # commit buffer
UCSC(policy-mgr) /domain-group/ip-pool/block # show detail
Block of IP Addresses:
    From: 1.2.3.4
    To: 1.2.3.8
    Default Gateway: 1.2.3.254
    Subnet Mask: 255.255.255.0
    Primary DNS: 0.0.0.0
    Secondary DNS: 0.0.0.0
    Scope: Public
    Config Scope: Public
    Block Qualifier:
USCS(policy-mgr) /domain-group/ip-pool/block # exit
UCSC(policy-mgr) /domain-group/ip-pool*# create ipv6-block
UCSC(policy-mgr) /domain-group/ip-pool*# create ipv6-block 2001:0000::808:808
2001:0000::808:880 2001:0000::808:801 64
UCSC(policy-mgr) /domain-group/ip-pool/ipv6-block* # commit buffer
UCSC(policy-mgr) /domain-group/ip-pool/ipv6-block # show detail
Block of IPv6 Addresses:
From To Prefix Block Qualifier
----------------------- ----------------------- ------ ---------------
2001:0000::808:808 2001:0000::808:880 64
```

Assigning KVM Outband to a UCS Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	
Step 2	UCSC(resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC(resource-mgr) /fabric# **scope domain** *ID*	Enters the specific domain .
Step 4	UCSC(resource-mgr) /fabric/domain # **scope domain-profile default**	Sets the default domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile # **set outband-management-pool** *name*	Assigns the Outband Management pool to the domain.
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to assign a 'pool-abc' to domain 1009 as a KVM Outband and show detail:

```
--------------------------------------
UCSC# connect resouce-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr) /fabric # scope domain 1009
UCSC(resource-mgr) /fabric # scope domain-profile default
UCSC(resource-mgr) /fabric/domain/domain-profile # set outband-management-pool pool-abc
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
UCSC(resource-mgr) /fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: HwCDP-UserAck
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc <<<<
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
```