



Server Policies

- [Server Policies, page 1](#)
- [BIOS Policy, page 1](#)
- [IPMI Access Profile, page 41](#)
- [Serial over LAN Policy, page 41](#)
- [Host Firmware Package Policy, page 42](#)
- [iSCSI Adapter Policy, page 43](#)
- [ID Range Access Control Policy, page 44](#)
- [Local Disk Policy, page 44](#)
- [Quality of Service Policy, page 45](#)
- [Scrub Policy, page 46](#)
- [vMedia Policy, page 47](#)

Server Policies

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



Note

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

BIOS Policy

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

To use a BIOS policy:

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

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

Creating or Editing a BIOS Policy

Procedure

- Step 1** In the **Actions** bar, type **Create BIOS Policy** and press Enter.
- Step 2** In the **BIOS Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
- a) Enter a **Name** and optional **Description**.
The policy name is case sensitive.
 - b) (Optional) Complete the other fields as necessary.
For more information, see [Basic BIOS Settings, on page 3](#).
- Step 3** In **Processor**, complete the fields as necessary.
For more information, see [Processor BIOS Settings, on page 7](#).
- Step 4** In **I/O**, complete the fields as necessary.
For more information, see [I/O BIOS Settings, on page 20](#).
- Step 5** In **RAS Memory**, complete the fields as necessary.
For more information, see [RAS Memory BIOS Settings, on page 21](#).
- Step 6** In **USB**, complete the fields as necessary.
For more information, see [USB BIOS Settings, on page 24](#).
- Step 7** In **PCI**, complete the fields as necessary.
For more information, see [PCI BIOS Settings, on page 28](#).
- Step 8** In **Graphics Configuration**, complete the fields as necessary.
For more information, see [Graphics Configuration BIOS Settings, on page 33](#).
- Step 9** In **Boot Options**, complete the fields as necessary.
For more information, see [Boot Options BIOS Settings, on page 34](#).
- Step 10** In **Server Manager**, complete the fields as necessary.
For more information, see [Server Manager BIOS Settings, on page 35](#).
- Step 11** In **Console**, complete the fields as necessary.
For more information, see [Console BIOS Settings, on page 37](#).
- Step 12** Click **Create**.
-

Default BIOS Settings

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

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

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

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

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

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

Basic BIOS Settings

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

Name	Description
Reboot on BIOS Settings Change	<p>When the server is rebooted after you change one or more BIOS settings.</p> <p>Enabled—If you enable this setting, the server is rebooted according to the maintenance policy in the server's service profile. For example, if the maintenance policy requires user acknowledgment, the server is not rebooted and the BIOS changes are not applied until a user acknowledges the pending activity.</p> <p>Disabled—If you do not enable this setting, the BIOS changes are not applied until the next time the server is rebooted, whether as a result of another server configuration change or a manual reboot.</p>

Name	Description
Serial Port A	<p>Whether serial port A is enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The serial port is disabled. • Enabled—The serial port is enabled.
Quiet Boot	<p>What the BIOS displays during Power On Self-Test (POST). This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The BIOS displays all messages and Option ROM information during boot. • Enabled—The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.
Post Error Pause	<p>What happens when the server encounters a critical error during POST. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The BIOS continues to attempt to boot the server. • Enabled—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.
Front Panel Lockout	<p>Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The power and reset buttons on the front panel are active and can be used to affect the server. • Enabled—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.

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

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

Processor BIOS Settings

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

Table 1: Basic Tab

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

Name	Description
Local X2 Application Policy Infrastructure Controller (APIC)	<p>Allows you to set the type of Application Policy Infrastructure Controller (APIC) architecture. This can be one of the following:</p> <ul style="list-style-type: none">• xAPIC—Uses the standard xAPIC architecture.• x2APIC—Uses the enhanced x2APIC architecture to support 32 bit addressability of processors.• Auto—Automatically uses the xAPIC architecture that is detected.• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Frequency Floor Override	<p>Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:</p> <ul style="list-style-type: none">• Disabled—The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance.• Enabled—The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
P-STATE Coordination	<p>Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.</p> <ul style="list-style-type: none"> • HW_ALL—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • SW_ALL—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • SW_ANY—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note Power Technology must be set to Custom or the server ignores the setting for this parameter.</p>
DRAM Clock Throttling	<p>Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Balanced— DRAM clock throttling is reduced, providing a balance between performance and power. • Performance—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • Energy Efficient—DRAM clock throttling is increased to improve energy efficiency. • Auto—The CPU determines the level.

Name	Description
Channel Interleaving	<p>Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following:</p> <ul style="list-style-type: none">• Auto—The CPU determines what interleaving is done.• 1 Way—Some channel interleaving is used.• 2 Way• 3 Way• 4 Way—The maximum amount of channel interleaving is used.• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Rank Interleaving	<p>Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following:</p> <ul style="list-style-type: none">• Auto—The CPU determines what interleaving is done.• 1 Way—Some rank interleaving is used.• 2 Way• 4 Way• 8 Way—The maximum amount of rank interleaving is used.• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Altitude	<p>The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the physical elevation. • 300 M—The server is approximately 300 meters above sea level. • 900 M—The server is approximately 900 meters above sea level. • 1500 M—The server is approximately 1500 meters above sea level. • 3000 M—The server is approximately 3000 meters above sea level. • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Table 2: Prefetchers Tab

Name	Description
Hardware Prefetcher	<p>Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The hardware prefetcher is not used. • Enabled—The processor uses the hardware prefetcher when cache issues are detected. • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note CPU Performance must be set to Custom in order to specify this value. For any value other than Custom, this option is overridden by the setting in the selected CPU performance profile.</p>

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

Table 3: Technology Tab

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

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

Table 4: Power Tab

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

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

Name	Description
Package C State Limit	<p>The amount of power available to the server components when they are idle. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Auto—The CPU determines the available power. • C0 State—The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • C1 State—When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • C2 State—When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • C3 State—When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • C6 State—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • C7 State—When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • C7s State—When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves more power than C7, but it also requires the longest time for the server to return to high performance mode. • No Limit—The server may enter any available C state.

Table 5: Errors and Reporting Tab

Name	Description
Processor C3 Report	<p>Whether the processor sends the C3 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The processor does not send the C3 report. • Enabled—The processor sends the C3 report. • ACPI-C2—The processor sends the C3 report using the advanced configuration and power interface (ACPI) C2 format. • ACPI-C3—The processor sends the C3 report using the ACPI C3 format. <p>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.</p>
Processor C6 Report	<p>Whether the processor sends the C6 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The processor does not send the C6 report. • Enabled—The processor sends the C6 report.
Processor C7 Report	<p>Whether the processor sends the C7 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The processor does not send the C7 report. • Enabled—The processor sends the C7 report. • C7—The processor sends the C7 report. • C7s—The processor sends the C7s report. <p>Note The selections vary depending on the server and operating system.</p>

Name	Description
Max Variable MTRR Setting	<p>Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.• Auto-Max—BIOS uses the default value for the processor.• 8—BIOS uses the number specified for the variable MTRR.
Demand Scrub	<p>Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.• Enabled—Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.• Disabled—Single bit memory errors are not corrected.
Patrol Scrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—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.• Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address.

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

I/O BIOS Settings

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

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

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

RAS Memory BIOS Settings

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

Name	Description
NUMA	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • Disabled—The BIOS does not support NUMA.
LV DDR Mode	<p>Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Power Saving Mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • Performance Mode—The system prioritizes high frequency operations over low voltage operations. • Auto—The CPU determines the priority.
DRAM Refresh Rate	<p>The refresh interval rate for internal memory. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • 1x • 2x • 3x • 4x • Auto

Name	Description
Memory RAS Configuration Mode	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Maximum Performance—System performance is optimized. • Mirroring—System reliability is optimized by using half the system memory as backup. • Lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers. • Sparing—Enables sparing mode.
Sparing Mode	<p>Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population.</p> <p>This option is only available if you choose the sparing option for the Memory RAS Config parameter. It can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • DIMM Sparing—One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • Rank Sparing—A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank.

Name	Description
DDR3 Voltage Selection	<p>The voltage to be used by the dual-voltage RAM. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.• 1500 MV• 1350 MV

USB BIOS Settings

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

Basic Tab

Name	Description
Make Device Non Bootable	<p>Whether the server can boot from a USB device. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.• Disabled—The server can boot from a USB device.• Enabled—The server cannot boot from a USB device.
USB Front Panel Access Lock	<p>USB front panel lock is configured to enable or disable the front panel access to USB ports. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.• Disabled• Enabled

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

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

Device Management Tab

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

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

Name	Description
All USB Devices	<p>Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—All USB devices are disabled. • Enabled—All USB devices are enabled.

PCI BIOS Settings

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

Table 6: Basic Tab

Name	Description
Max Memory Below 4G	<p>Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—Does not maximize memory usage. Choose this option for all operating systems with PAE support. • Enabled—Maximizes memory usage below 4GB for an operating system without PAE support.

Name	Description
Memory Mapped IO Above 4Gb Configuration	<p>Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • Enabled—Maps I/O of 64-bit PCI devices to 4GB or greater address space.
VGA Priority	<p>Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following:</p> <ul style="list-style-type: none"> • Onboard—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • Offboard—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • Onboard VGA Disabled—Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. <p>Note The vKVM does not function when the onboard VGA is disabled.</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note Only onboard VGA devices are supported with Cisco UCS B-Series servers.</p>

Name	Description
PCIe OptionROMs	<p>Whether Option ROM is available on all expansion ports. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The expansion slots are not available. • Enabled—The expansion slots are available. • UEFI-Only—The expansion slots are available for UEFI only. • Legacy Only—The expansion slots are available for legacy only. • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Mezz OptionRom	<p>Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Enabled—All LOM ports are enabled. • Disabled—All LOM ports are disabled.
PCIe 10G LOM 2 Link	<p>Whether Option ROM is available on the 10G LOM port. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Enabled—The expansion slot is available. • Disabled—The expansion slot is not available.
ASPM Support	<p>Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Auto—The CPU determines the power state. • Disabled—ASPM support is disabled in the BIOS. • Force L0—Force all links to L0 standby (L0s) state.

Table 7: PCIe Slot Link Speed Tab

Name	Description
Slot <i>n</i> Link Speed	<p>This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot <i>n</i>. This can be one of the following:</p> <ul style="list-style-type: none">• Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.• gen1 - 2.5 GT/s—2.5GT/s (gigatransfers per second) is the maximum speed allowed.• gen2 - 5 GT/s—5GT/s is the maximum speed allowed.• gen3 - 8 GT/s—8GT/s is the maximum speed allowed.• Auto—The maximum speed is set automatically.• Disabled—The maximum speed is not restricted.

Table 8: PCIe Slot OptionROM Tab

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

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

Name	Description
Slot N1	<p>Whether is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The expansion slot is not available. • Enabled—The expansion slot is available. • UEFI Only—The expansion slot is available for UEFI only. • Legacy Only—The expansion slot is available for legacy only.
Slot N2	<p>Whether is available on the specified port. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Disabled—The expansion slot is not available. • Enabled—The expansion slot is available. • UEFI Only—The expansion slot is available for UEFI only. • Legacy Only—The expansion slot is available for legacy only.

Graphics Configuration BIOS Settings

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

Name	Description
Integrated Graphics	<p>Enables integrated graphics. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Enabled—Integrated graphic is enabled. • Disabled—Integrated graphics is disabled.

Name	Description
Integrated Graphics Aperture Size	<p>Allows you to set the size of mapped memory for the integrated graphics controller. This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • 128 MB • 256 MB • 512 MB • 1024 MB • 2048 MB • 4096 MB
Onboard Graphics	<p>Enables onboard graphics (KVM). This can be one of the following:</p> <ul style="list-style-type: none"> • Platform Default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • Enabled—Onboard graphics is enabled. • Disabled—Onboard graphics is disabled.

Boot Options BIOS Settings

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

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

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

Server Manager BIOS Settings

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

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

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

Console BIOS Settings

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

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

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

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

IPMI Access Profile

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

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

Creating and Editing an IPMI Access Profile

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

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

Procedure

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

What to Do Next

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

Serial over LAN Policy

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

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

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

Creating and Editing a Serial over LAN Policy

Procedure

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

Host Firmware Package Policy

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



Note

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

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

- The global-default host firmware package policy includes all components, but if you create a new custom host firmware package policy, the local disk component is automatically excluded.
- Host firmware package policies created in Cisco UCS Central 1.3 or previous do not support excluding components. These policies are not changed when you upgrade to Cisco UCS Central release 1.4 or above.
- If you create your own custom host firmware package policy with excluded components, including the local disk component that is excluded by default, you cannot include that host firmware package policy in a service profile associated with a server running a Cisco UCS Manager version prior to 2.2.7. If you do, you will see the following error during service profile association:

ucs domain does not have the matching server capabilities for this service-profile
 You can either remove all excluded components in the host firmware package policy, or upgrade your version of Cisco UCS Manager to release 2.2.7 or above.

Creating or Editing a Host Firmware Package Policy

Procedure

- Step 1** In the **Actions** bar, type **Create Host Firmware Package Policy** and press Enter.
- Step 2** In the **Host Firmware Package Policy** dialog box, click **Basic** and choose the **Organization** where you want to create the policy.
- Step 3** Enter a **Name** and optional **Description**.
The policy name is case-sensitive.
- Step 4** Select the **Blade Version** and **Rack Version** of the firmware, as required for your environment.
- Step 5** In the **Components** tab, click **Add** to select any components that want to exclude from the firmware update.
The included and excluded components display.
- Step 6** To exclude all components, click **Excluded Components**.
- Step 7** To remove an excluded component, select it and click **Delete**.
- Step 8** Click **Create**.
- Note** To understand the impact of the policy, click **Evaluate**.
-

iSCSI Adapter Policy

Creating or Editing an iSCSI Adapter Policy

Procedure

- Step 1** In the **Actions** bar, type **Create iSCSI Adapter Policy** and press Enter.
- Step 2** In the **iSCSI Adapter Policy** dialog box, choose the **Organization** in which you want to create the policy.
- Step 3** Enter the **Name** and optional **Description**.
The name is case sensitive.
- Step 4** Enter values for the **Connection Timeout**, **LUN Busy Retry Count**, and **DHCP Timeout**.
- Step 5** Choose whether to enable **TCP Timestamp**, **HBA Mode**, and **Boot To Target**.
- Step 6** Click **Create**.
-

Creating or Editing an iSCSI Authentication Profile

Procedure

- Step 1** In the **Actions** bar, type **Create iSCSI Authentication Profile** and press Enter.
 - Step 2** In the **iSCSI Authentication Profile** dialog box, choose the **Organization** in which you want to create the policy.
 - Step 3** Enter the **Name** and optional **Description**.
The name is case sensitive.
 - Step 4** Enter the **User ID**.
 - Step 5** Type and confirm the password.
 - Step 6** Click **Create**.
-

ID Range Access Control Policy

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

Creating or Editing an ID Range Access Control Policy

Procedure

- Step 1** In the **Actions** bar, type **Create ID Range Access Control Policy** and press Enter.
 - Step 2** In the **ID Range Access Control Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
 - Step 3** Enter the **Name** and optional **Description**.
The name is case sensitive.
 - Step 4** In **Domain Groups**, click **Add** to select the **Permitted Domain Groups** associated with this policy.
 - Step 5** Click **Create**.
-

Local Disk Policy

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

The local disk modes include the following:

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

Creating or Editing a Local Disk Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Local Disk Policy** and press Enter.
- Step 2** In the **Local Disk Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
- Step 3** Enter the **Name** and optional **Description**.
The name is case sensitive.
- Step 4** In **Mode**, select the configuration mode for the local disks.
- Step 5** Choose whether to enable or disable **Configuration Protection**, **FlexFlash**, and **FlexFlash RAID Reporting**.
- Step 6** Click **Create**.
-

Quality of Service Policy

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

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

Creating or Editing a Quality of Service Policy

Procedure

-
- Step 1** In the **Actions** bar, type **Create Quality of Service (QoS) Policy** and press Enter.
- Step 2** In the **Create Quality of Service (QoS) Policy** dialog box, click **Organization** and select the location in which you want to create the policy.
- Step 3** Enter the **Name** and optional **Description**.
The name is case sensitive.
- Step 4** Select an **Egress Priority**.
- Step 5** Choose whether to enable **Host Control Class of Service (CoS)**.
- Step 6** Enter an **Egress Burst Size**, and select the egress average traffic rate.
- Step 7** Click **Create**.
-

Scrub Policy

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



Note

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

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

Disk scrub

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

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

BIOS Settings Scrub

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

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

FlexFlash Scrub

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

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



Note

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

Creating or Editing a Scrub Policy

Procedure

- Step 1** In the **Actions** bar, type **Create Scrub Policy** and press Enter.
- Step 2** In the **Scrub Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
- Step 3** Enter the **Name** and optional **Description**.
The name is case sensitive.
- Step 4** Choose the scrub policies that you want to enable.
- Step 5** Click **Create**.

vMedia Policy

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

**Note**

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

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

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

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

**Note**

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

Creating or Editing a vMedia Policy

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

Procedure

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

- b) Select the **Protocol** and fill in required protocol information.
- c) In **Generate File name from Service Profile Name**, click **Enabled** or **Disabled**.
Enabled will automatically use the Service profile name as ISO name. The ISO file with the same name as the service profile must be available at the required path. If you select **Disabled**, fill in remote ISO file name that the policy must use.

Step 5 Click **Create**.

What to Do Next

Associate the vMedia policy with a service profile.

