



Configuring Server-Related Policies

This chapter includes the following sections:

- [Configuring BIOS Settings, page 1](#)
- [Configuring Boot Policies, page 22](#)
- [Configuring IPMI Access Profiles, page 27](#)
- [Configuring Local Disk Configuration Policies, page 28](#)
- [Configuring Scrub Policies, page 34](#)
- [Configuring Serial over LAN Policies, page 36](#)
- [Configuring Server Autoconfiguration Policies, page 38](#)
- [Configuring Server Discovery Policies, page 40](#)
- [Configuring Server Inheritance Policies, page 41](#)
- [Configuring Server Pool Policies, page 43](#)
- [Configuring Server Pool Policy Qualifications, page 44](#)
- [Configuring vNIC/vHBA Placement Policies, page 51](#)

Configuring BIOS Settings

Server BIOS Settings

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

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

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS instance, or you can use only one of

them. You can also use Cisco UCS Manager to view the actual BIOS settings on a server and determine whether they are meeting current needs.

**Note**

Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the 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 and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers

Main BIOS Settings

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

Name	Description
Reboot on BIOS Settings Change	<p>When the server is rebooted after you change one or more BIOS settings.</p> <p>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>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>
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"> • disabled—The BIOS displays all messages and Option ROM information during boot. • enabled—The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Post Error Pause	<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"> • disabled—The BIOS continues to attempt to boot the server. • enabled—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Resume Ac On Power Loss	<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"> • stay-off—The server remains off until manually powered on. • last-state—The server is powered on and the system attempts to restore its last state. • reset—The server is powered on and automatically reset. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Front Panel Lockout	<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"> • disabled—The power and reset buttons on the front panel are active and can be used to affect the server. • enabled—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
ACPI10 Support	<p>Whether the BIOS publishes the ACPI 1.0 version of FADT in the Root System Description table. This version may be required for compatibility with OS versions that only support ACPI 1.0. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—ACPI 1.0 version is not published. • enabled—ACPI 1.0 version is published. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Processor BIOS Settings

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

Name	Description
Turbo Boost	<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"> • disabled—The processor does not increase its frequency automatically. • enabled—The processor utilizes Turbo Boost Technology if required. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
<p>Enhanced Intel Speedstep</p>	<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"> • disabled—The processor never dynamically adjusts its voltage or frequency. • enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
<p>Hyper Threading</p>	<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"> • disabled—The processor does not permit hyperthreading. • enabled—The processor allows for the parallel execution of multiple threads. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Name	Description
Core Multi Processing	<p>Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • all—Enables multi processing on all logical processor cores. • 1 through 10—Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Execute Disabled Bit	<p>Classifies memory areas on the server to specify where where 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"> • disabled—The processor does not classify memory areas. • enabled—The processor classifies memory areas. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>We recommend that you contact your operating system vendor to make sure the 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"> • disabled—The processor does not permit virtualization. • enabled—The processor allows multiple operating systems in independent partitions. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>

Name	Description
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"> • disabled—Data from I/O devices is not placed directly into the processor cache. • enabled—Data from I/O devices is placed directly into the processor cache. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Processor C State	<p>Significantly reduces the power of the processor during idle periods. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled • enabled • platform-default <p>We recommend that you contact your operating system vendor to make sure the 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"> • disabled • enabled • platform-default
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"> • disabled—The processor does not send the C3 report. • acpi-c2—The processor sends the C3 report using the ACPI C2 format. • acpi-c3—The processor sends the C3 report using the ACPI C3 format. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>On the 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>

Name	Description
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"> • disabled—The processor does not send the C6 report. • enabled—The processor sends the C6 report. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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"> • enterprise—All prefetchers and data reuse are disabled. • high-throughput—All prefetchers are enabled, and data reuse is disabled. • hpc—All prefetchers and data reuse are enabled. This setting is also known as high performance computing. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Max Variable MTRR Setting	<p>Allows you to select the number of MTRR variables. This can be one of the following:</p> <ul style="list-style-type: none"> • auto-max—The BIOS uses the default value for the processor. • 8—The BIOS uses the number specified for the variable MTRR. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Intel Directed I/O BIOS Settings

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

Name	Description
VT for Directed IO	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not use virtualization technology. • enabled—The processor uses virtualization technology. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Interrupt Remap	<p>Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support remapping. • enabled—The processor uses VT-d Interrupt Remapping as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Coherency Support	<p>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support coherency. • enabled—The processor uses VT-d Coherency as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
ATS Support	<p>Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support ATS. • enabled—The processor uses VT-d ATS as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Pass Through DMA Support	<p>Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support pass-through DMA. • enabled—The processor uses VT-d Pass-through DMA as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

RAS Memory BIOS Settings

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

Name	Description
Memory RAS Config	<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"> • 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—System reliability is enhanced with a degree of memory redundancy while making more memory available to the operating system than mirroring. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
NUMA	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The BIOS does not support NUMA • enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Mirroring Mode	<p>Memory mirroring enhances system reliability by keeping two identical data images in memory.</p> <p>This option is only available if you choose the mirroring option for Memory RAS Config. It can be one of the following:</p> <ul style="list-style-type: none"> • inter-socket—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • intra-socket—One IMC is mirrored with another IMC in the same socket. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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 sparing option for Memory RAS Config. It can be one of the following:</p> <ul style="list-style-type: none"> • dim-sparing—One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • rank-sparing—A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
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"> • power-saving-mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • performance-mode—The system prioritizes high frequency operations over low voltage operations. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Serial Port BIOS Settings

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

Name	Description
Serial Port A	<p>Whether serial port A is enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The serial port is disabled. • enabled—The serial port is enabled. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

USB BIOS Settings

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

Name	Description
Make Device Non Bootable	<p>Whether the server can boot from a USB device. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The server cannot boot from a USB device. • enabled—The server can boot from a USB device. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

PCI Configuration BIOS Settings

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

Name	Description
Max Memory Below 4G	<p>Whether the BIOS maximizes memory usage below 4GB for an operating without PAE support, depending on the system configuration. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—Does not maximize memory usage. Choose this option for all operating systems with PAE support. • enabled—Maximizes memory usage below 4GB for an operating system without PAE support. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory Mapped IO Above 4Gb Config	<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"> • disabled—Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • enabled—Maps I/O of 64-bit PCI devices to 4GB or greater address space. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Boot Options BIOS Settings

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

Name	Description
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: <ul style="list-style-type: none"> • disabled—Waits for user input before retrying NON-EFI based boot options. • enabled—Continually retries NON-EFI based boot options without waiting for user input. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID	Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following: <ul style="list-style-type: none"> • disabled—The Intel SAS Entry RAID Module is disabled. • enabled—The Intel SAS Entry RAID Module is enabled. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID Module	How the Intel SAS Entry RAID Module is configured. This can be one of the following: <ul style="list-style-type: none"> • it-ir-raid—Configures the RAID module to use Intel IT/IR RAID. • intel-esrtii—Configures the RAID module to use Intel Embedded Server RAID Technology II. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Server Management BIOS Settings

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

General Settings

Name	Description
Assert Nmi on Serr	<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"> • disabled—The BIOS does not generate an NMI or log an error when a SERR occurs. • enabled—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable Assert Nmi on Perr. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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"> • disabled—The BIOS does not generate an NMI or log an error when a PERR occurs. • enabled—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable Assert Nmi on Serr to use this setting. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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"> • disabled—The watchdog timer is not used to track how long the server takes to boot. • enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the predefined length of time, the CIMC resets the system and logs an error. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <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"> • power-off—The server is powered off if the watchdog timer expires during OS boot. • reset—The server is reset if the watchdog timer expires during OS boot. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <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"> • 5-minutes—The watchdog timer expires 5 minutes after the OS begins to boot. • 10-minutes—The watchdog timer expires 10 minutes after the OS begins to boot. • 15-minutes—The watchdog timer expires 15 minutes after the OS begins to boot. • 20-minutes—The watchdog timer expires 20 minutes after the OS begins to boot. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>This option is only available if you enable the OS Boot Watchdog Timer.</p>

Console Redirection Settings

Name	Description
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"> • disabled—No console redirection occurs during POST. • serial-port-a—Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • serial-port-b—Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.</p>
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"> • none—No flow control is used. • rts-cts—RTS/CTS is used for flow control. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note This setting must match the setting on the remote terminal application.</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"> • 9600—A 9600 BAUD rate is used. • 19200—A 19200 BAUD rate is used. • 38400—A 38400 BAUD rate is used. • 57600—A 57600 BAUD rate is used. • 115200—A 115200 BAUD rate is used. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <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"> • pc-ansi—The PC-ANSI terminal font is used. • vt100—A supported vt100 video terminal and its character set are used. • vt100-plus—A supported vt100-plus video terminal and its character set are used. • vt-utf8—A video terminal with the UTF-8 character set is used. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note This setting must match the setting on the remote terminal application.</p>
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"> • disabled—The serial port enabled for console redirection is hidden from the legacy operating system. • enabled—The serial port enabled for console redirection is visible to the legacy operating system. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

BIOS Policy

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

To use a BIOS policy, do the following:

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

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

Default BIOS Settings

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

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

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

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

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

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

Creating a BIOS Policy



Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the 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 and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **BIOS Policies** and select **Create BIOS Policy**.
- Step 5** On the **Main** page of the **Create BIOS Policy** wizard, enter a name for the BIOS policy in the **Name** field. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
- Step 6** In the **Create BIOS Policy** wizard, do the following to configure the BIOS settings:
- If you want to change a BIOS setting, click the desired radio button or make the appropriate choice from the drop-down list.
For descriptions and information about the options for each BIOS setting, see the following topics:
 - **Main** page: [Main BIOS Settings](#), on page 2
 - **Processor** page: [Processor BIOS Settings](#), on page 4
 - **Intel Directed IO** page: [Intel Directed I/O BIOS Settings](#), on page 8
 - **RAS Memory** page: [RAS Memory BIOS Settings](#), on page 10
 - **Serial Port** page: [Serial Port BIOS Settings](#), on page 12
 - **USB** page: [USB BIOS Settings](#), on page 12
 - **PCI Configuration** page: [PCI Configuration BIOS Settings](#), on page 13
 - **Boot Options** page: [Boot Options BIOS Settings](#), on page 14
 - **Server Management** page: [Server Management BIOS Settings](#), on page 14
 - Click **Next** after each page to move to the
- Step 7** After you have configured all of the BIOS settings for the policy, click **Finish**.
-

Modifying the BIOS Defaults

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

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

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
 - Step 2** On the **Servers** tab, expand **Servers > Policies**.
 - Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.
 - Step 4** Expand **BIOS Defaults** and select the server model number for which you want to modify the default BIOS settings.
 - Step 5** In the **Work** pane, click the appropriate tab and then click the desired radio button or make a choice from the drop-down list to modify the default BIOS settings:
For descriptions and information about the options for each BIOS setting, see the following topics. Not all BIOS settings are available for each type of server.
 - **Main** tab: [Main BIOS Settings, on page 2](#)
 - **Advanced** tab:
 - **Processor** subtab: [Processor BIOS Settings, on page 4](#)
 - **Intel Directed IO** subtab: [Intel Directed I/O BIOS Settings, on page 8](#)
 - **RAS Memory** subtab: [RAS Memory BIOS Settings, on page 10](#)
 - **Serial Port** subtab: [Serial Port BIOS Settings, on page 12](#)
 - **USB** subtab: [USB BIOS Settings, on page 12](#)
 - **PCI Configuration** subtab: [PCI Configuration BIOS Settings, on page 13](#)
 - **Boot Options** tab: [Boot Options BIOS Settings, on page 14](#)
 - **Server Management** tab: [Server Management BIOS Settings, on page 14](#)
 - Step 6** Click **Save Changes**.
-

Viewing the Actual BIOS Settings for a Server

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

Procedure

-
- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Choose the server for which you want to view the actual BIOS settings.
- Step 4** On the **Work** pane, click the **Inventory** tab.
- Step 5** Click the **Motherboard** subtab.
- Step 6** In the **BIOS Settings** area, click the **Expand** icon to the right of the heading to open that area. Each tab in the **BIOS Settings** area displays the settings for that server platform. Some of the tabs contain subtabs with additional information.
-

Configuring Boot Policies

Boot Policy

The boot policy determines the following:

- Configuration of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the server uses the default settings in the BIOS to determine the boot order.



Important

Changes to a boot policy may be propagated to all servers created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is auto-triggered.

Guidelines

When you create a boot policy, you can add one or more of the following to the boot policy and specify their boot order:

Boot type	Description
SAN boot	Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary. We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network.
LAN boot	Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.
Local disk boot	If the server has a local drive, boots from that drive. Note Cisco UCS Manager does not differentiate between the types of local drives. If an operating system has been installed on more than one local drive or on an internal USB drive (eUSB), you cannot specify which of these local drives the server should use as the boot drive.
Virtual media boot	Mimics the insertion of a physical CD-ROM disk (read-only) or floppy disk (read-write) into a server. It is typically used to manually install operating systems on a server.

**Note**

The default boot order is as follows:

- 1 Local disk boot
 - 2 LAN boot
 - 3 Virtual media read-only boot
 - 4 Virtual media read-write boot
-

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, except for iSCSI boot, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

**Tip**

We recommend that the boot order in a boot policy include either a local disk or a SAN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server might boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

Before You Begin

If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, you must first remove all local disks from servers associated with a service profile that includes the boot policy.

Procedure

-
- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **Boot Policies** and select **Create Boot Policy**.
The **Create Boot Policy** wizard displays.
- Step 5** Enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
- Step 6** (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.
- Step 7** (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.
- Step 8** To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:
- a) Click the down arrows to expand the **Local Devices** area.
 - b) Click one of the following links to add the device to the **Boot Order** table:
 - **Add Local Disk**
 - **Add CD-ROM**
 - **Add Floppy**

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 9 To add a LAN boot to the boot order, do the following:

- a) Click the down arrows to expand the **vNICs** area.
- b) Click the **Add LAN Boot** link.
- c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.
- d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 10 To add a SAN boot to the boot order, do the following:

- a) Click the down arrows to expand the **vHBAs** area.
- b) Click the **Add SAN Boot** link.
- c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: <ul style="list-style-type: none"> • primary—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • secondary—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.

Name	Description
Type field	<p>This can be:</p> <ul style="list-style-type: none"> • primary—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • secondary—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. <p>The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.</p>

- e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

What to Do Next

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

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the **Boot Order Details** area on the **General** tab for the server.

Deleting a Boot Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies > *Organization_Name***.
- Step 3** Expand the **Boot Policies** node.
- Step 4** Right-click the policy you want to delete and select **Delete**.
- Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring IPMI Access Profiles

IPMI Access Profile

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

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

Creating an IPMI Access Profile

Before You Begin

An IPMI profile requires that one or more of the following resources already exist in the system:

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

Procedure

-
- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **IPMI Profiles** and select **Create IPMI Profiles**.
- Step 5** In the **Create IPMI Profile** dialog box:
- a) Enter a unique name and description for the profile.
 - b) Click **OK**.
- Step 6** In the **IPMI Profile Users** area of the navigator, click **+**.
- Step 7** In the **User Properties** dialog box:
- a) Complete the following fields:

Name	Description
Name field	The username to associate with this IPMI profile.
Password field	The password associated with this username.
Confirm Password field	The password a second time for confirmation purposes.

Name	Description
Role field	The user role. This can be: <ul style="list-style-type: none"> • admin • Read Only

b) Click **OK**.

Step 8 Repeat Steps 6 and 7 to add another user.

Step 9 Click **OK** to return to the IPMI profiles in the **Work** pane.

What to Do Next

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

Deleting an IPMI Access Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 In the **Servers** tab, expand **Servers > Policies > Organization_Name**

Step 3 Expand the **IPMI Profiles** node.

Step 4 Right-click the profile you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Local Disk Configuration Policies

Local Disk Configuration Policy

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

The local disk modes include the following:

- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.

- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

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

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.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

Unassociated Servers

After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.



Note

If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers

Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Guidelines for Local Disk Configuration Policies Configured for RAID

No Mixed HDDs and SSDs

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

Do Not Use the Any Configuration Mode on Servers with MegaRAID Storage Controllers

If a blade server or rack-mount server in a Cisco UCS instance includes a MegaRAID storage controller, do not configure the local disk configuration policy in the service profile for that server with the **Any Configuration** mode. If you use this mode for servers with a MegaRAID storage controller, the installer for the operating system cannot detect any local storage on the server.

If you want to install an operating system on local storage on a server with a MegaRAID storage controller, you must configure the local disk configuration policy with a mode that creates a RAID LUN (RAID volume) on the server.

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.

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.

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."

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.

Creating a Local Disk Configuration Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **Local Disk Config Policies** and choose **Create Local Disk Configuration Policy**.
- Step 5** In the **Create Local Disk Configuration Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Name	Description
Mode drop-down list	<p>This can be one of the following local disk policy modes:</p> <ul style="list-style-type: none"> • No Local Storage—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk. • RAID 0 Stripes—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails. • RAID 1 Mirrored—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives. • Any Configuration—For a server configuration that carries forward the local disk configuration without any changes. • No RAID—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered. • RAID 6 Stripes Dual Parity—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored. • RAID 5 Striped Parity—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates. • RAID10 Mirrored and Striped— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates. <p>Note If you choose No RAID and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences after you apply the No RAID mode.</p> <p>To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the No RAID configuration mode.</p>

Name	Description
Protect Configuration check box	<p>If checked, the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile.</p> <p>This property is checked by default.</p> <p>When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.</p> <p>Note If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.</p>

Step 6 Click **OK**.

Changing a Local Disk Configuration Policy

This procedure describes how to change a local disk configuration policy from an associated service profile. You can also change a local disk configuration policy from the **Policies** node of the **Servers** tab.

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Service Profiles**.
- Step 3** Expand the organization that includes the service service profile with the local disk configuration policy you want to change.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Click the service profile that contains the local disk configuration policy you want to change.
- Step 5** In the **Work** pane, click the **Policies** tab.
- Step 6** In the **Actions** area, click **Change Local Disk Configuration Policy**.
- Step 7** In the **Change Local Disk Configuration Policy** dialog box, choose one of the following options from the **Select the Local Disk Configuration Policy** drop-down list.

Option	Description
Use a Disk Policy	Select an existing local disk configuration policy from the list below this option. Cisco UCS Manager assigns this policy to the service profile.
Create a Local Disk Policy	Enables you to create a local disk configuration policy that can only be accessed by the selected service profile.

Option	Description
No Disk Policy	Does not use a local disk configuration policy for the selected service profile.

Step 8 Click **OK**.

Step 9 (Optional) Expand the **Local Disk Configuration Policy** area to confirm that the change has been made.

Deleting a Local Disk Configuration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers > Policies > Organization_Name**.

Step 3 Expand the **Local Disk Config Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Scrub Policies

Scrub Policy

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process and when the server is disassociated from a service profile. 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

Creating a Scrub Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **Scrub Policies** and select **Create Scrub Policy**.
- Step 5** In the **Create Scrub Policy** wizard, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Disk Scrub field	If this field is set to yes , when a service profile containing this scrub policy is disassociated from a server, all data on the server local drives is completely erased. If this field is set to no , the data on the local drives is preserved, including all local storage configuration.
BIOS Settings Scrub field	If the field is set to yes , when a service profile containing this scrub policy is disassociated from a server, the BIOS settings for that server are erased and reset to the defaults for that server type and vendor. If this field is set to no , the BIOS settings are preserved.

Step 6 Click **OK**.

Deleting a Scrub Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
 - Step 2** On the **Servers** tab, expand **Servers > Policies > Organization_Name**.
 - Step 3** Expand the **Scrub Policies** node.
 - Step 4** Right-click the policy you want to delete and select **Delete**.
 - Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Configuring Serial over LAN Policies

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

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

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

Creating a Serial over LAN Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **Serial over LAN Policies** and select **Create Serial over LAN Policy**.
- Step 5** In the **Create Serial over LAN Policy** wizard, complete the following fields:

Name	Description
Name field	<p>The name of the policy.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.</p>
Description field	<p>A description of the policy. We recommend including information about where and when the policy should be used.</p> <p>Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).</p>
Serial over LAN State field	<p>This can be:</p> <ul style="list-style-type: none"> • disable—Serial over LAN access is blocked. • enable—Serial over LAN access is permitted.
Speed drop-down list	<p>This can be:</p> <ul style="list-style-type: none"> • 9600 • 19200 • 38400 • 57600 • 115200

Step 6 Click **OK**.

Deleting a Serial over LAN Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
 - Step 2** On the **Servers** tab, expand **Servers > Policies > *Organization_Name***.
 - Step 3** Expand the **Serial over LAN Policies** node.
 - Step 4** Right-click the policy you want to delete and select **Delete**.
 - Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Configuring Server Autoconfiguration Policies

Server Autoconfiguration Policy

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

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

Creating an Autoconfiguration Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- Server pool policy qualifications
- Service profile template
- Organizations, if a system implements multi-tenancy

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Autoconfig Policies** subtab.
- Step 5** On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.
- Step 6** In the **Create Autoconfiguration Policy** dialog box, complete the following fields:

Name	Description
Name field	<p>The name of the policy.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.</p>

Name	Description
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Qualification drop-down list	The server pool policy qualification associated with this auto-configuration policy. If a new server is discovered that matches the criteria specified in the server pool policy qualification, Cisco UCS automatically creates a service profile based on the service profile template selected in the Service Profile Template Name drop-down list and associates the newly created service profile with the server.
Org drop-down list	The organization associated with this autoconfiguration policy. If Cisco UCS automatically creates a service profile to associate with a server, it places the service profile under the organization selected in this field.
Service Profile Template Name drop-down list	The service profile template associated with this policy.

Step 7 Click **OK**.

Deleting an Autoconfiguration Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Autoconfig Policies** subtab.
- Step 5** Right-click the autoconfiguration policy that you want to delete and choose **Delete**.
- Step 6** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Discovery Policies

Server Discovery Policy

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

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

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

Creating a Server Discovery Policy

Before You Begin

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

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Policies** tab.
 - Step 4** Click the **Server Discovery Policies** subtab.
 - Step 5** Click the + icon on the table icon bar to open the **Create Server Discovery Policy** dialog box.
 - Step 6** In the **Description** field, enter a description for the discovery policy.
 - Step 7** In the **Action** field, select one of the following options:
 - **immediate**—The system attempts to discover new servers automatically
 - **user-acknowledged**—The system waits until the user tells it to search for new servers
 - Step 8** (Optional) To associate this policy with a server pool, select server pool policy qualifications from the **Qualification** drop-down list.
 - Step 9** (Optional) To include a scrub policy, select a policy from the **Scrub Policy** drop-down list.
 - Step 10** Click **OK**.
-

What to Do Next

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

Deleting a Server Discovery Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Policies** tab.
 - Step 4** Click the **Server Discovery Policies** subtab.
 - Step 5** Right-click the server discover policy that you want to delete and choose **Delete**.
 - Step 6** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Configuring Server Inheritance Policies

Server Inheritance Policy

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

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

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

Creating a Server Inheritance Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Server Inheritance Policies** subtab.
- Step 5** On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create Server Inheritance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.
Org drop-down list	If you want to associate an organization with this policy, or if you want to change the current association, choose the desired organization from the drop-down list.

Step 7 Click **OK**.

Deleting a Server Inheritance Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Server Inheritance Policies** subtab.
- Step 5** Right-click the server inheritance policy that you want to delete and choose **Delete**.
- Step 6** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring Server Pool Policies

Server Pool Policy

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

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

Creating a Server Pool Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- A minimum of one server pool
- Server pool policy qualifications, if you choose to have servers automatically added to pools

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **Server Pool Policies** and select **Create Server Pool Policy**.
- Step 5** In the **Create Server Pool Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).
Target Pool drop-down list	If you want to associate this policy with a server pool, select that pool from the drop-down list.

Name	Description
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.

Step 6 Click **OK**.

Deleting a Server Pool Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies > Organization_Name**.
- Step 3** Expand the **Server Pool Policies** node.
- Step 4** Right-click the policy you want to delete and select **Delete**.
- Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Configuring Server Pool Policy Qualifications

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration

- Storage configuration and capacity
- Server model

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

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

Creating Server Pool Policy Qualifications

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click the **Server Pool Policy Qualifications** node and select **Create Server Pool Policy Qualification**.
- Step 5** In the **Create Server Pool Policy Qualification** dialog box, enter a unique name and description for the policy.
- Step 6** (Optional) To use this policy to qualify servers according to their adapter configuration, do the following:
 - a) Click **Create Adapter Qualifications**.
 - b) In the **Create Adapter Qualifications** dialog box, complete the following fields:

Name	Description
Type drop-down list	<p>The adapter type. This can be:</p> <ul style="list-style-type: none"> • fcoe—Fibre Channel over Ethernet • non-virtualized-eth-if • non-virtualized-fc-if • path-encap-consolidated • path-encap-virtual • protected-eth-if • protected-fc-if • protected-fcoe • virtualized-eth-if • virtualized-fc-if • virtualized-scsi-if <p>Once you save the adapter qualification, this type cannot be changed.</p>
Model field	A regular expression that the adapter model name must match.
Maximum Capacity field	<p>The maximum capacity for the selected type.</p> <p>To specify a capacity, choose select and enter the desired maximum capacity.</p>

c) Click **OK**.

Step 7 (Optional) To use this policy to qualify servers according to the chassis in which they physically reside, do the following:

- a) Click **Create Chassis/Server Qualifications**.
- b) In the **Chassis Qualifications** area of the **Create Chassis and Server Qualifications** dialog box, complete the following fields to specify the range of chassis you want to use:
 - **First Chassis ID** field—The first chassis ID from which server pools associated with this policy can draw.
 - **Number of Chassis** field—The total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.

Example:

For example, if you want to use chassis 5, 6, 7, and 8, enter 5 in the **First Chassis ID** field and 4 in the **Number of Chassis** field. If you want to use only chassis 3, enter 3 in the **First Chassis ID** field and 1 in the **Number of Chassis** field.

Tip If you want to use chassis 5, 6, and 9, create a chassis/server qualification for the range 5-6 and another qualification for chassis 9. You can add as many chassis/server qualifications as needed.

c) Click **Finish**.

Step 8 (Optional) To use this policy to qualify servers according to both the chassis and slot in which they physically reside, do the following:

a) Click **Create Chassis/Server Qualifications**.

b) In the **Chassis Qualifications** area of the **Create Chassis and Server Qualifications** dialog box, complete the following fields to specify the range of chassis you want to use:

- **First Chassis ID** field—The first chassis ID from which server pools associated with this policy can draw.
- **Number of Chassis** field—The total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.

c) In the **Server Qualifications** table, click **Add**.

d) In the **Create Server Qualifications** dialog box, complete the following fields to specify the range of server locations you want to use:

- **First Slot ID** field—The first slot ID from which server pools associated with this policy can draw.
- **Number of Slots** field—The total number of slots from which server pools associated with this policy can draw.

e) Click **Finish Stage**.

f) To add another range of slots, click **Add** and repeat steps d and e.

g) When you have finished specifying the slot ranges, click **Finish**.

Step 9 (Optional) To use this policy to qualify servers according to their memory configuration, do the following:

a) Click **Create Memory Qualifications**.

b) In the **Create Memory Qualifications** dialog box, complete the following fields:

Name	Description
Clock field	The minimum clock speed required, in megahertz.
Latency field	The maximum latency allowed, in nanoseconds.
Min Cap field	The minimum memory capacity required, in megabytes.
Max Cap field	The maximum memory capacity allowed, in megabytes.
Width field	The minimum width of the data bus.
Units field	The unit of measure to associate with the value in the Width field.

c) Click **OK**.

Step 10 (Optional) To use this policy to qualify servers according to their CPU/Cores configuration, do the following:

a) Click **Create CPU/Cores Qualifications**.

b) In the **Create CPU/Cores Qualifications** dialog box, complete the following fields:

Name	Description
Processor Architecture drop-down list	The CPU architecture to which this policy applies.
Model field	A regular expression that the processor model name must match.
Min Number of Cores field	The minimum number of CPU cores required. To specify a capacity, choose select and enter the minimum number of cores.
Max Number of Cores field	The maximum number of CPU cores allowed. To specify a capacity, choose select and enter the maximum number of cores.
Min Number of Threads field	The minimum number of CPU threads required. To specify a capacity, choose select and enter the minimum number of threads.
Max Number of Threads field	The maximum number of CPU threads allowed. To specify a capacity, choose select and enter the maximum number of threads.
CPU Speed field	The minimum CPU speed required. To specify a capacity, choose select and enter the minimum CPU speed.
CPU Stepping field	The minimum CPU version required. To specify a capacity, choose select and enter the maximum CPU speed.

c) Click **OK**.

Step 11 (Optional) To use this policy to qualify servers according to their storage configuration and capacity, do the following:

a) Click **Create Storage Qualifications**.

b) In the **Create Storage Qualifications** dialog box, complete the following fields:

Name	Description
Diskless field	Whether the available storage must be diskless. This can be: <ul style="list-style-type: none"> • unspecified—Either storage type is acceptable. • yes—The storage must be diskless. • no—The storage cannot be diskless.

Name	Description
Number of Blocks field	The minimum number of blocks required. To specify a capacity, choose select and enter the number of blocks.
Block Size field	The minimum block size required, in bytes. To specify a capacity, choose select and enter the block size.
Min Cap field	The minimum storage capacity across all disks in the server, in megabytes. To specify a capacity, choose select and enter the minimum storage capacity.
Max Cap field	The maximum storage capacity allowed, in megabytes. To specify a capacity, choose select and enter the maximum storage capacity.
Per Disk Cap field	The minimum storage capacity per disk required, in gigabytes. To specify a capacity, choose select and enter the minimum capacity on each disk.
Units field	The number of units. To specify a capacity, choose select and enter the desired units.

c) Click **OK**.

Step 12 (Optional) To use this policy to qualify servers according to the model of the server, do the following:

- a) Click **Create Server Model Qualifications**.
- b) In the **Create Server Model Qualifications** dialog box, enter a regular expression that the server model must match in the **Model** field.
- c) Click **OK**.

Step 13 (Optional) To use this policy to qualify servers according to power group, do the following:

- a) Click **Create Power Group Qualifications**.
- b) In the **Create Power Group Qualifications** dialog box, choose a power group from the **Power Group** drop-down list.
- c) Click **OK**.

Step 14 (Optional) To use this policy to qualify the rack-mount servers that can be added to the associated server pool, do the following:

- a) Click **Create Rack Qualifications**.
- b) In the **Create Rack Qualifications** dialog box, complete the following fields:

Name	Description
First Slot ID field	The first rack-mount server slot ID from which server pools associated with this policy can draw.

Name	Description
Number of Slots field	The total number of rack-mount server slots from which server pools associated with this policy can draw.

Step 15 Verify the qualifications in the table and correct if necessary.

Step 16 Click **OK**.

Deleting Server Pool Policy Qualifications

Procedure

-
- Step 1** In the **Navigation** pane, click the **Servers** tab.
 - Step 2** On the **Servers** tab, expand **Servers > Policies > Organization_Name**.
 - Step 3** Expand the **Server Pool Policy Qualifications** node.
 - Step 4** Right-click the policy qualifications you want to delete and select **Delete**.
 - Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Deleting Qualifications from Server Pool Policy Qualifications

Use this procedure to modify Server Pool Policy Qualifications by deleting one or more sets of qualifications.

Procedure

-
- Step 1** In the **Navigation** pane, click the **Servers** tab.
 - Step 2** On the **Servers** tab, expand **Servers > Policies > Organization_Name**.
 - Step 3** Expand the **Server Pool Policy Qualifications** node.
 - Step 4** Choose the policy you want to modify.
 - Step 5** In the **Work** pane, choose the **Qualifications** tab.
 - Step 6** To delete a set of qualifications:
 - a) In the table, choose the row that represents the set of qualifications.
 - b) Right-click the row and select **Delete**.
 - Step 7** Click **Save Changes**.
-

Configuring vNIC/vHBA Placement Policies

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine what types of vNICs or vHBAs can be assigned to the physical adapters on a server. Each vNIC/vHBA placement policy contains four virtual network interface connections (vCons) that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters.

If you do not include a vNIC/vHBA placement policy in the service profile or you use the default configuration for a server with two adapters, Cisco UCS Manager defaults to the **All** configuration and equally distributes the vNICs and vHBAs between the adapters.

You can use this policy to assign vNICs or vHBAs to either of the two vCons. Cisco UCS Manager uses the vCon assignment to determine how to assign the vNICs and vHBAs to the physical adapter during service profile association.

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

vCon to Adapter Placement

Cisco UCS Manager maps every vCon in a service profile to a physical adapter on the server. How that mapping occurs and how the vCons are assigned to a specific adapter in a server with two adapters depends upon the type of server. You must consider this placement when you configure the vNIC/vHBA placement policy to assign vNICs and vHBAs to vCons.

**Note**

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

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

In these blade servers, the adapters are numbered left to right, but vCons are numbered right to left. If the server has a single adapter, all vCons are assigned to that adapter. However, if the server has two adapters, the vCons are assigned to the adapters in reverse order, as follows:

- Adapter1 is assigned vCon2 and vCon4
- Adapter2 is assigned vCon1 and vCon3

vCon to Adapter Placement for All Other Supported Servers

For all other servers supported by Cisco UCS, the vCon assignment depends upon the number of adapters in the server, as follows:

Table 1: vCon to Adapter Placement by Number of Adapters in Server

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

vNIC/vHBA to vCon Assignment

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

Explicit Assignment of vNICs and vHBAs

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

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

- Set the vCon configuration to **Assigned Only**, **Exclude Dynamic**, or **Exclude Unassigned**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server. If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon.
- Assign the vNICs and vHBAs to a vCon. You can make this assignment through the Virtual Host Interface Placement properties of the vNIC or vHBA or in the service profile associated with the server.

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

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

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

**Note**

vCon to adapter assignment occurs in a round-robin order. This order means that vNICs are placed on the adapters in the following order: vnic-1, vnic-3, vnic-2, vnic-4. As a result, under the following circumstances, the PCIE order of vNICs can be different than the explicit assignment configured in Cisco UCS Manager:

- In a server with two adapters, vNICs are explicitly assigned to all four vCons.
- A service profile that includes explicit assignment is migrated from a server with a higher number of adapters to one with a lower number of adapters.

Implicit Assignment of vNICs and vHBAs

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

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

- Set the vCon configuration to **All**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server.
- Do not assign any vNICs or vHBAs to a vCon.

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

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

Creating a vNIC/vHBA Placement Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Right-click **vNIC/vHBA Placement Policies** and choose **Create Placement Policy**.
- Step 5** In the **Create Placement Policy** dialog box, do the following:
 - a) In the **Name** field, enter a unique name for the placement policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

- b) In the **Selection Preference** column for each **Virtual Slot**, choose one of the following from the drop-down list:
- **all**—All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic.
 - **assigned-only**—vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
 - **exclude-dynamic**—Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
 - **exclude-unassigned**—Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.
- c) Click **OK**.
-

Deleting a vNIC/vHBA Placement Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies > *Organization_Name***.
- Step 3** Expand the **vNIC/vHBA Placement Policies** node.
- Step 4** Right-click the policy you want to delete and choose **Delete**.
- Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Explicitly Assigning a vNIC to a vCon

Before You Begin

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

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

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

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Service Profiles**.
- Step 3** Expand the node for the organization which contains the service profile whose vNICs you want to explicitly assign to a vCon.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Expand *Service_Profile_Name* > vNICs.
- Step 5** Click on the vNIC that you want to explicitly assign to a vCon.
- Step 6** In the **Work** pane, click the **General** tab.
- Step 7** In the **Virtual Host Interface Placement** section, complete the following fields:

Table 2:

Name	Description
Desired Placement drop-down list	The user-specified virtual network interface connection (vCon) placement for the vNIC. This can be: <ul style="list-style-type: none"> • any—Allows Cisco UCS Manager to determine the vCon to which the vNIC is assigned. • 1—Explicitly assigns the vNIC to vCon1. • 2—Explicitly assigns the vNIC to vCon2. • 3—Explicitly assigns the vNIC to vCon3. • 4—Explicitly assigns the vNIC to vCon4.
Actual Assignment field	The actual vCon assignment of the vNIC on the server.

If you attempt to assign a vNIC to a vCon that is not configured for that type of vNIC, Cisco UCS Manager displays a message box to advise you of the configuration error. You must either assign the vNIC to another vCon or change the vCon configuration in the service profile.

- Step 8** In the **Order** section, complete the following fields:

Table 3:

Name	Description
Desired Order field	The user-specified PCI order for the vNIC. Enter an integer between 0 and 128. You cannot create more than 128 vNICs for a server.
Actual Order field	The actual PCI order of the vNIC on the server.

Step 9 Click **Save Changes**.

Explicitly Assigning a vHBA to a vCon

Before You Begin

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

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

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

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Service Profiles**.
- Step 3** Expand the node for the organization which contains the service profile whose vHBAs you want to explicitly assign to a vCon.
If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Expand **Service_Profile_Name > vHBAs**.
- Step 5** Click on the vHBA that you want to explicitly assign to a vCon.
- Step 6** In the **Work** pane, click the **General** tab.
- Step 7** In the **Virtual Host Interface Placement** section, complete the following fields:

Name	Description
Desired Placement field	The user-specified virtual network interface connection (vCon) placement for the vHBA. This can be: <ul style="list-style-type: none"> • any—Allows Cisco UCS Manager to determine the vCon to which the vHBA is assigned. • 1—Explicitly assigns the vHBA to vCon1. • 2—Explicitly assigns the vHBA to vCon2. • 3—Explicitly assigns the vHBA to vCon3. • 4—Explicitly assigns the vHBA to vCon4.
Actual Assignment field	The actual vCon assignment of the vHBA on the server.

If you attempt to assign a vHBA to a vCon that is not configured for that type of vHBA, Cisco UCS Manager displays a message box to advise you of the configuration error. You must either assign the vHBA to another vCon or change the vCon configuration in the service profile.

Step 8 In the **Order** section, complete the following fields:

Name	Description
Desired Order field	The user-specified PCI order for the vHBA. Enter an integer between 0 and 128. You cannot create more than 128 vHBAs for a server.
Actual Order field	The actual PCI order of the vHBA on the server.

Step 9 Click **Save Changes**.
