Configuring Server-Related Policies

This chapter includes the following sections:

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 options such as the following:

Main Server Settings	• Quiet boot

	• Resume on AC power loss • Front panel lockout
Processor Settings	• Intel TurboBoost Technology • Enhanced Intel SpeedStep • Intel Hyperthreading Technology • Intel Virtualization Technology • Processor C3 report • Processor C6 report
Intel-Directed I/O	• Intel VT for directed I/O • Interrupt remap • Coherency support • ATS Support • Pass Through DMA
RAS Memory	• Memory RAS configuration • NUMA Optimized • Mirroring mode • LV DDR mode

Depending upon the needs of the data center, you can combine both of these options in a 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 until the server is rebooted.

If you change a BIOS policy, you must reboot any servers associated with service profiles that include the policy for the changes to take effect.

If you change the default BIOS settings, those changes are applied to servers upon association with service profiles that do not include a BIOS policy or when the server is rebooted. Changes to the default BIOS settings do not affect servers that are already associated with service profiles.

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:

- Create the BIOS policy in Cisco UCS Manager
- Assign the BIOS policy to one or more service profiles
- 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

Default BIOS settings are applicable to all servers of a specific type that do not have a BIOS policy included in their service profiles. These settings are available only in the root organization and are global. Only one set of BIOS settings can exist for each server platform supported by Cisco UCS.

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

If you change a BIOS policy, you must reboot any servers associated with service profiles that include the policy for the changes to take effect.

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 In the **Main** page of the **Create BIOS Policy** wizard, fill in the following fields:

Name	Description
Name field	The name of the policy.

Name	Description
	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.
Quiet Boot field	Determines what the BIOS displays during Power On Self-Test (POST). This can be: • **disabled**—The BIOS displays the logo screen. • **enabled**—The BIOS does not display any messages during boot. • **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 field	Determines how the server behaves when power is restored after an unexpected power loss. This can be: • **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 field	Whether the power and reset buttons on the front panel are ignored by the server. This can be: • **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.

Step 6 Click **Next**.

Step 7 In the **Processor** page of the **Create BIOS Policy** wizard, fill in the following fields:

Name	Description
Turbo Boost Tech field	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: • **disabled**—The processor never increases its frequency automatically.

Name	Description
	• **enabled**—The processor utilizes Turbo Boost Technology if required. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Enhanced Intel Speedstep Tech field	Whether the processor uses Enhanced Intel SpeedStep Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. This can be: • **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. Contact your operating system vendor to make sure the operating system supports this feature. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Hyper Threading Tech field	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be: • **disabled**—The processor does not permit hyperthreading. • **enabled**—The processor allows for the parallel execution of multiple threads. Contact your operating system vendor to make sure the operating system supports this feature. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Virtualization Technology field	Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be: • **disabled**—The processor does not permit virtualization. • **enabled**—The processor allows multiple operating systems in independent partitions. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Processor C3 Report field	Determines whether the processor sends the C3 report to the operating system. This can be:

Name	Description
	• **disabled**—The processor does not send the C3 report. • **acpi-c2**—The processor sends the C3 report using the ACPI C2 format. • **acpi-c2**—The processor sends the C3 report using the ACPI C3 format. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. On the B400 server, the BIOS Setup menu uses **enabled** and **disabled** for these options. If you specify **acpi-c2** or **acpi-c2**, the server sets the BIOS value for that option to **enabled**.
Processor C6 Report field	Determines whether the processor sends the C6 report to the operating system. This can be: • **disabled**—The processor does not send the C6 report. • **enabled**—The processor sends the C6 report. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Step 8 Click **Next**.

Step 9 In the **Intel Directed IO** page of the **Create BIOS Policy** wizard, fill in the following fields:

Name	Description
VT for Directed IO field	Whether the processor uses Intel Virtualization Technology for Directed I/O. This can be: • **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 field	Whether the processor supports Intel VT-d Interrupt Remapping. This can be: • **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 field	Whether the processor supports Intel VT-d Coherency. This can be:

Name	Description
	• **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 field	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be: • **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.
Pass Through DMA Support field	Whether the processor supports Intel VT-d Pass-through DMA. This can be: • **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.

Step 10 Click **Next**.

Step 11 In the **RAS Memory** page of the **Create BIOS Policy** wizard, fill in the following fields:

Name	Description
Memory RAS Config drop-down list	The memory reliability, availability and serviceability (RAS) configuration. This can be: • **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 B400 servers. • **maximum performance**—System performance is optimized. • **mirroring**—System reliability is optimized by using half the system memory as backup. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
NUMA field	Whether the BIOS supports NUMA. This can be:

Name	Description
	• **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 field	Memory mirroring is used to enhance system reliability by keeping two identical data images in memory. This can be: • **intersocket**—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • **intrasocket**—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. **Note** To use mirroring mode, you must set the **Memory RAS Config** option to **mirroring**.
LV DDR Mode field	Whether the system prioritizes low voltage or high frequency memory operations. This can be: • **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.

Step 12 Click **Next**.

Step 13 In the **Server Management** page of the **Create BIOS Policy** wizard, fill in the following fields:

Name	Description
Console Redirection field	Whether a serial port can be used for server management tasks. This can be: • **disabled**—Serial ports cannot be used for management tasks. • **serial-port-a**—Serial port A is configured for management tasks. • **serial-port-b**—Serial port B is configured for management tasks.

Name	Description
	- **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
BAUD Rate drop-down list	If a serial port can be used for management tasks, use this field to set the serial port transmission speed so that it matches the rate of the remote terminal application. This can be: • **115200** • **19200** • **38400** • **57600** • **9600** • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This field is not displayed if console redirection is disabled.

Step 14 Click **Finish**.

Modifying the BIOS Defaults

If you change the default BIOS settings, those changes are applied to servers upon association with service profiles that do not include a BIOS policy or when the server is rebooted. Changes to the default BIOS settings do not affect servers that are already associated with service profiles.

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 BIOS model number whose defaults you want to set.

Step 5 In the **Main** tab, fill in the following fields:

Name	Description
Quiet Boot field	Determines what the BIOS displays during Power On Self-Test (POST). This can be: • **disabled**—The BIOS displays the logo screen.

Name	Description
	- **enabled**—The BIOS does not display any messages during boot. - **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 field	Determines how the server behaves when power is restored after an unexpected power loss. This can be: - **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 field	Whether the power and reset buttons on the front panel are ignored by the server. This can be: - **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.

Step 6 Click the **Advanced** tab.

Step 7 In the **Processor** subtab, fill in the following fields:

Name	Description
Turbo Boost Tech field	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: - **disabled**—The processor never increases its frequency automatically. - **enabled**—The processor utilizes Turbo Boost Technology if required. - **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Enhanced Intel Speedstep Tech field	Whether the processor uses Enhanced Intel SpeedStep Technology allows the system to dynamically adjust processor voltage and core

Name	Description
	frequency, which can result in decreased average power consumption and decreased average heat production. This can be: • **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. Contact your operating system vendor to make sure the operating system supports this feature. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Hyper Threading Tech field	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be: • **disabled**—The processor does not permit hyperthreading. • **enabled**—The processor allows for the parallel execution of multiple threads. Contact your operating system vendor to make sure the operating system supports this feature. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Virtualization Technology field	Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be: • **disabled**—The processor does not permit virtualization. • **enabled**—The processor allows multiple operating systems in independent partitions. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Processor C3 Report field	Determines whether the processor sends the C3 report to the operating system. This can be: • **disabled**—The processor does not send the C3 report. • **acpi-c2**—The processor sends the C3 report using the ACPI C2 format. • **acpi-c2**—The processor sends the C3 report using the ACPI C3 format.

Name	Description
	• **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. On the B400 server, the BIOS Setup menu uses **enabled** and **disabled** for these options. If you specify **acpi-c2** or **acpi-c2**, the server sets the BIOS value for that option to **enabled**.
Processor C6 Report field	Determines whether the processor sends the C6 report to the operating system. This can be: • **disabled**—The processor does not send the C6 report. • **enabled**—The processor sends the C6 report. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Step 8 In the **Intel Directed IO** subtab, fill in the following fields:

Name	Description
VT for Directed IO field	Whether the processor uses Intel Virtualization Technology for Directed I/O. This can be: • **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 field	Whether the processor supports Intel VT-d Interrupt Remapping. This can be: • **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 field	Whether the processor supports Intel VT-d Coherency. This can be: • **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.

Name	Description
ATS Support field	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be: • **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.
Pass Through DMA Support field	Whether the processor supports Intel VT-d Pass-through DMA. This can be: • **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.

Step 9 In the **RAS Memory** subtab, fill in the following fields:

Name	Description
Memory RAS Config drop-down list	The memory reliability, availability and serviceability (RAS) configuration. This can be: • **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 B400 servers. • **maximum performance**—System performance is optimized. • **mirroring**—System reliability is optimized by using half the system memory as backup. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
NUMA field	Whether the BIOS supports NUMA. This can be: • **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.

Name	Description
Mirroring Mode field	Memory mirroring is used to enhance system reliability by keeping two identical data images in memory. This can be: • **intersocket**—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • **intrasocket**—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. **Note** To use mirroring mode, you must set the **Memory RAS Config** option to **mirroring**.
LV DDR Mode field	Whether the system prioritizes low voltage or high frequency memory operations. This can be: • **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.

Step 10 Go the **Server Management** tab and fill in the following fields:

Name	Description
Console Redirection field	Whether a serial port can be used for server management tasks. This can be: • **disabled**—Serial ports cannot be used for management tasks. • **serial-port-a**—Serial port A is configured for management tasks. • **serial-port-b**—Serial port B is configured for management tasks. • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
BAUD Rate drop-down list	If a serial port can be used for management tasks, use this field to set the serial port transmission speed so that it matches the rate of the remote terminal application. This can be: • **115200** • **19200** • **38400**

Name	Description
	• **57600** • **9600** • **platform-default**—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This field is not displayed if console redirection is disabled.

Step 11 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** sub-tab.

Step 6 In the **BIOS Settings** area, click the **Expand** icon to the right of the heading to display the tabs and fields with the BIOS settings for that server platform.

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, 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 may 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 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, then 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: • **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.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries.

Name	Description
	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.

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.
Role field	This can be: • **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:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **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.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **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.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **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 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.

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 and Considerations for a Local Disk Configuration Policy

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 RAID configuration or in a single blade server.

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.

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 select **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.
Mode drop-down list	This can be one of the following local disk policy modes: • **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes. • **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. • **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered. • **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. • **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates. • **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 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.

Name	Description
	- **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. **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. 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.
Protect Configuration check box	If checked, the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile. This property is checked by default. 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. **Note** If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

Step 6 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.
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 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.
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	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.

Name	Description
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Serial over LAN State field	This can be: • **disable**—Serial over LAN access is blocked. • **enable**—Serial over LAN access is permitted.
Speed drop-down list	This can be: • **115200** • **19200** • **38400** • **57600** • **9600**

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 **Admin** 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	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.
Qualification drop-down list	The server pool policy qualification associated with this autoconfiguration 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.

Name	Description
	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 **Admin** 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 **Admin** 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 **Admin** 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 **Admin** 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.
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 **Admin** 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.
Target Pool drop-down list	If you want to associate this policy with a server pool, select that pool from the drop-down list.
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
- 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	The adapter type. This can be: • **fcoe**—Fibre Channel over Ethernet • **non-virtualized-eth-if**

Name	Description
	• **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** Once you save the adapter qualification, this type cannot be changed.
Model field	A regular expression that the adapter model name must match.
Maximum Capacity field	The maximum capacity for the selected type.

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 CPU capacity required, in megabytes.
Max Cap field	The maximum CPU 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.
Max Number of Cores field	The maximum number of CPU cores allowed.

Name	Description
Min Number of Threads field	The minimum number of CPU threads required.
Max Number of Threads field	The maximum number of CPU threads allowed.
CPU Speed field	The minimum CPU speed required.
CPU Stepping field	The minimum CPU version required.

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
Number of Blocks field	The minimum number of blocks required.
Block Size field	The minimum block size required, in bytes.
Min Cap field	The minimum storage capacity required, in megabytes.
Max Cap field	The maximum storage capacity allowed, in megabytes.
Per Disk Cap field	The minimum storage capacity per disk required, in gigabytes.
Units field	The number of 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 Verify the qualifications in the table and correct if necessary.

Step 14 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 assign vNICs or vHBAs to the physical adapters on a server. Each vNIC/vHBA placement policy contains two 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 to a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters. For servers with only one adapter, both vCons are assigned to the adapter; for servers with two adapters, one vCon is assigned to each adapter.

You can assign vNICs or vHBAs to either of the two vCons, and they are then assigned to the physical adapters based on the vCon assignment during server association. Additionally, vCons use the following selection preference criteria to assign vHBAs and vNICs:

All	The vCon is used for vNICs or vHBAs assigned to it, vNICs or vHBAs not assigned to either vCon, and dynamic vNICs or vHBAs.
Assigned-Only	The vCon is reserved for only vNICs or vHBAs assigned to it.
Exclude-Dynamic	The vCon is not used for dynamic vNICs or vHBAs.
Exclude-Unassigned	The vCon is not used for vNICs or vHBAs not assigned to the vCon. The vCon is used for dynamic vNICs and vHBAs.

For servers with two adapters, if you do not include a vNIC/vHBA placement policy in a service profile, or you do not configure vCons for a service profile, Cisco UCS equally distributes the vNICs and vHBAs between the two adapters.

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**
- **assigned-only**
- **exclude-dynamic**
- **exclude-unassigned**

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**.