

Configuring Server Boot

This chapter includes the following sections:

- Boot Policy, page 1
- UEFI Boot Mode, page 2
- UEFI Secure Boot, page 3
- CIMC Secure Boot, page 3
- Creating a Boot Policy, page 5
- SAN Boot, page 6
- iSCSI Boot, page 7
- LAN Boot, page 31
- Local Devices Boot, page 32
- Deleting a Boot Policy, page 39
- UEFI Boot Parameters, page 39

Boot Policy

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu, and determines the following:

- Selection 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 can either create a named boot policy that can be associated with one or more service profiles, or create a boot policy for a specific service profile. A boot policy must be included 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, Cisco UCS Manager applies the default boot policy.



Changes to a boot policy might 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 automatically triggered.

UEFI Boot Mode

Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. Cisco UCS Manager uses UEFI to replace the BIOS firmware interfaces. This allows the BIOS to run in UEFI mode while still providing legacy support.

You can choose either legacy or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported only on M3 and M4 servers, and allows you to enable UEFI secure boot mode.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is only supported on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers.
- UEFI boot mode is not supported with the following combinations:
 - Gen-3 Emulex & QLogic adapters on Cisco UCS blade & rack servers integrated with Cisco UCS Manager.
 - PXE boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.
 - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.
- You cannot mix UEFI and legacy boot mode on the same server.
- The server will boot correctly in UEFI mode only if the boot devices configured in the boot policy have UEFI-aware operating systems installed. If a compatible OS is not present, the boot device is not displayed on the **Actual Boot Order** tab in the **Boot Order Details** area.
- In some corner cases, the UEFI boot may not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation could occur in the following situations:
 - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is manually powered on using the **Equipment** tab or the front panel.
 - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.
 - If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

UEFI Secure Boot

Cisco UCS Manager supports UEFI secure boot on Cisco UCS B-Series M3 and M4 Blade servers and Cisco UCS C-Series M3 and M4 Rack servers. When UEFI secure boot is enabled, all executables, such as boot loaders and adapter drivers, are authenticated by the BIOS before they can be loaded. To be authenticated, the images must be signed by either the Cisco Certificate Authority (CA) or a Microsoft CA.

The following limitations apply to UEFI secure boot:

- UEFI boot mode must be enabled in the boot policy.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.



• UEFI boot mode is supported on Cisco UCS C-Series rack servers beginning with Release 2.2(3a).

- User-generated encryption keys are not supported.
- UEFI secure boot can only be controlled by Cisco UCS Manager.
- If you want to downgrade to an earlier version of Cisco UCS Manager, and you have a server in secure boot mode, you must disassociate and reassociate the server before downgrading. Otherwise, the server will not be discovered successfully.

CIMC Secure Boot

With CIMC secure boot, only Cisco signed firmware images can be installed and run on the servers. When the CIMC is updated, the image is certified before the firmware is flashed. If certification fails, the firmware is not flashed. This prevents unauthorized access to the CIMC firmware.

Guidelines and Limitations for CIMC Secure Boot

• CIMC secure boot is supported on Cisco UCS M3 rack servers.



Note CIMC secure boot is enabled by default on the Cisco UCS C220 M4 and C240 M4 rack servers, and is automatically enabled on the Cisco UCS C460 M4 rack server after upgrading to CIMC firmware release 2.2(3).

- After CIMC secure boot is enabled, it cannot be disabled.
- After CIMC secure boot is enabled on a server, you cannot downgrade to a CIMC firmware image prior to 2.1(3).

Determining the CIMC Secure Boot Status

Procedure

| Ste | o 1 | In t | he N | Vaviga | tion | pane, | click | the: | Eq | ui | pment | tał |). |
|-----|-----|------|------|--------|------|-------|-------|------|----|----|-------|-----|----|
|-----|-----|------|------|--------|------|-------|-------|------|----|----|-------|-----|----|

- **Step 2** Expand **Equipment** > **Rack-Mounts** > **Server** Name.
- **Step 3** In the Work area, click the **Inventory** tab.
- **Step 4** Click the CIMC subtab.
- **Step 5** In the **CIMC** area, note the **Secure Boot Operational State** field. This can be one of the following:
 - Unsupported—CIMC secure boot is not supported on the server.
 - Disabled—CIMC secure boot is supported, but is disabled on the server.
 - Enabling—CIMC secure boot has been enabled, and the operation is in process.
 - Enabled—CIMC secure boot is enabled on the server.

Enabling CIMC Secure Boot on a Rack Server

| Step 1 | 1 In the Navigation pane, click the Equipment tab. | | | |
|--------|---|--|--|--|
| Step 2 | Expand Equipment > Rack-Mounts > Servers > Server Name. | | | |
| Step 3 | In the Work area, click the Inventory tab. | | | |
| Step 4 | Click the CIMC subtab. | | | |
| Step 5 | 5 In the Actions area, click Enable Secure Boot. CIMC secure boot is only supported on Cisco UCS M3 rack servers. If CIMC secure boot is not supporte or has already been enabled, this action is greyed out. | | | |
| Step 6 | Click Yes in the Enable Secure Boot confirmation dialog box. Note Once enabled, CIMC secure boot cannot be disabled. | | | |

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.

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 multitenancy, expand the **root** node.
- Step 4Right-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 other than - (hyphen), _ (underscore), : (colon), and . (period), 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.
 For boot policies applied to a server with a non-Cisco VIC adapter, even if the Reboot on Boot Order Change check box is not checked, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.
- Step 7 (Optional) If desired, check the Enforce vNIC/vHBA/iSCSI Name check box.
 - If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the **Boot Order** table match the server configuration in the service profile.
 - If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.
- **Step 8** In the Boot Mode field, choose the Legacy or UEFI radio button.
- **Step 9** If you selected UEFI, check the **Boot Security** checkbox if you want to enable UEFI boot security.
- Step 10 Configure one or more of the following boot options for the boot policy and set their boot order:
 - Local Devices boot—To boot from local devices, such as local disks on the server, virtual media, or remote virtual disks, continue with Configuring a Local Disk Boot for a Boot Policy, on page 33.
 - SAN boot—To boot from an operating system image on the SAN, continue with Configuring a SAN Boot for a Boot Policy, on page 6.

You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

• LAN boot—To boot from a centralized provisioning server, continue with Configuring a LAN Boot for a Boot Policy, on page 32.

• iSCSI boot—To boot from an iSCSI LUN, continue with Creating an iSCSI Boot Policy, on page 16.

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.

SAN Boot

You can configure a boot policy to boot one or more servers from an operating system image on the SAN. The boot policy can include 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.

To use a SAN boot, ensure that the following is configured:

- The Cisco UCS domain must be able to communicate with the SAN storage device that hosts the operating system image.
- A boot target LUN (Logical Unit Number) on the device where the operating system image is located.



Note

SAN boot is not supported on Gen-3 Emulex adapters on Cisco UCS blade & rack servers.

Configuring a SAN Boot for 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

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.

This procedure continues directly from Creating a Boot Policy, on page 5.

Before You Begin

Note

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

This does not apply for Cisco UCS M3 and M4 servers.

Procedure

- **Step 1** Click the down arrows to expand the **vHBAs** area.
- Step 2 Click the Add SAN Boot link.
- Step 3 In the Add San Boot dialog box, specify the vHBA and type, then click OK.
- Step 4 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, specify the boot target LUN, boot target WWPN, and type, then click OK:
- **Step 5** Do one of the following:
 - Add another boot device to the Boot Order table.
 - 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.

iSCSI Boot

iSCSI boot enables a server to boot its operating system from an iSCSI target machine located remotely over a network.

iSCSI boot is supported on the following Cisco UCS hardware:

- Cisco UCS blade servers that have the Cisco UCS M51KR-B Broadcom BCM57711 network adapter and use the default MAC address provided by Broadcom.
- Cisco UCS M81KR Virtual Interface Card
- Cisco UCS VIC-1240 Virtual Interface Card
- Cisco UCS VIC-1280 Virtual Interface Card
- Cisco UCS rack servers that have the Cisco UCS M61KR-B Broadcom BCM57712 network adapter.
- Cisco UCS P81E Virtual Interface Card
- Cisco UCS VIC 1225 Virtual Interface Card

There are prerequisites that must be met before you configure iSCSI boot. For a list of these prerequisites, see iSCSI Boot Guidelines and Prerequisites, on page 8.

For a high-level procedure for implementing iSCSI boot, see Configuring iSCSI Boot, on page 11.

iSCSI Boot Process

Cisco UCS Manager uses the iSCSI vNIC and iSCSI boot information created for the service profile in the association process to program the adapter, located on the server. After the adapter is programmed, the server reboots with the latest service profile values. After the power on self-test (POST), the adapter attempts to initialize using these service profile values. If the adapter can use the values and log in to its specified target, the adapter initializes and posts an iSCSI Boot Firmware Table (iBFT) to the host memory and a valid bootable LUN to the system BIOS. The iBFT that is posted to the host memory contains the initiator and target configuration that is programmed on the primary iSCSI VNIC.



Previously, the host would see only one of the boot paths configured, depending on which path completed the LUN discovery first, and would boot from that path. Now, when there are two iSCSI boot vNICs configured, the host will see both of the boot paths. So for multipath configurations, a single IQN needs to be configured on both the boot vNICs If there are different IQNs configured on the boot vNICs on a host, the host will boot with the IQN that is configured on the boot vNIC with the lower PCI order.

The next step, which is the installation of the operating system (OS), requires an OS that is iBFT capable. During installation of the OS, the OS installer scans the host memory for the iBFT table and uses the information in the iBFT to discover the boot device and create an iSCSI path to the target LUN. In some OS's a NIC driver is required to complete this path. If this step is successful, the OS installer finds the iSCSI target LUN on which to install the OS.

Note

The iBFT works at the OS installation software level and might not work with HBA mode (also known as TCP offload). Whether iBFT works with HBA mode depends on the OS capabilities during installation. Also, for a server that includes a Cisco UCS M51KR-B Broadcom BCM57711 adapter, the iBFT normally works at a maximum transmission unit (MTU) size of 1500, regardless of the MTU jumbo configuration. If the OS supports HBA mode, you might need to set HBA mode, dual-fabric support, and jumbo MTU size after the iSCSI installation process.

iSCSI Boot Guidelines and Prerequisites

These guidelines and prerequisites must be met before configuring iSCSI boot:

- After the iSCSI boot policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create iSCSI boot policies.
- To set up iSCSI boot from a Windows 2008 server where the second vNIC (failover vNIC) must boot from an iSCSI LUN, consult Microsoft Knowledge Base Article 976042. Microsoft has a known issue where Windows might fail to boot from an iSCSI drive or cause a bugcheck error if the networking hardware is changed. To work around this issue, follow the resolution recommended by Microsoft.

- The storage array must be licensed for iSCSI boot and the array side LUN masking must be properly configured.
- Two IP addresses must be determined, one for each iSCSI initiator. If possible, the IP addresses should be on the same subnet as the storage array. The IP addresses are assigned statically or dynamically using the Dynamic Host Configuration Protocol (DHCP).
- You cannot configure boot parameters in the Global boot policy. Instead, after configuring boot parameters, you need to include the boot policy in the appropriate service profile.
- The operating system (OS) must be iSCSI Boot Firmware Table (iBFT) compatible.
- For Cisco UCS M51KR-B Broadcom BCM57711 network adapters:
 - Servers that use iSCSI boot must contain the Cisco UCS M51KR-B Broadcom BCM57711 network adapter. For information on installing or replacing an adapter card, see the *Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*. The service note is accessible from the *Cisco UCS B-Series Servers Documentation Roadmap* at http://www.cisco.com/go/ unifiedcomputing/b-series-doc.
 - Set the MAC addresses on the iSCSI device.
 - If you are using the DHCP Vendor ID (Option 43), configure the MAC address of an iSCSI device in /etc/dhcpd.conf.
 - HBA mode (also known as TCP offload) and the boot to target setting are supported. However, only Windows OS supports HBA mode during installation.
 - Before installing the OS, disable the boot to target setting in the iSCSI adapter policy, then after installing the OS, reenable the boot to target setting.



Each time you change an adapter policy setting, the adapter reboots to apply the new setting.

- When installing the OS on the iSCSI target, the iSCSI target must be ordered *before* the device where the OS image resides. For example, if you are installing the OS on the iSCSI target from a CD, the boot order should be the iSCSI target and then the CD.
- After the server has been iSCSI booted, do not modify the Initiator Name, Target name, LUN, iSCSI device IP, or Netmask/gateway using the Broadcom tool.
- Do not interrupt the POST (power on self-test) process or the Cisco UCS M51KR-B Broadcom BCM57711 network adapter will fail to initialize.
- For Cisco UCS M81KR Virtual Interface Card and Cisco UCS VIC-1240 Virtual Interface Card:
 - ° Do not set MAC addresses on the iSCSI device.
 - HBA mode and the boot to target setting are not supported.
 - When installing the OS on the iSCSI target, the iSCSI target must be ordered *after* the device where the OS image resides. For example, if you are installing the OS on the iSCSI target from a CD, the boot order should be the CD and then the iSCSI target.
 - If you are using the DHCP Vendor ID (Option 43), the MAC address of the overlay vNIC needs to be configured in /etc/dhcpd.conf.

- After the server has been iSCSI booted, do not modify the IP details of the overlay vNIC.
- The VMware ESX/ESXi operating system does not support storing a core dump file to an iSCSI boot target LUN. Dump files must be written to a local disk.

Initiator IQN Configuration

Cisco UCS uses the following rules to determine the initiator IQN for an adapter iSCSI vNIC at the time a service profile is associated with a physical server:

- An initiator IQN at the service profile level *and* at the iSCSI vNIC level cannot be used together in a service profile.
- If an initiator IQN is specified at the service profile level, all of the adaptor iSCSI vNICs are configured to use the same initiator IQN, except in the case of DHCP Option 43, where the initiator IQN is set to empty on the adapter iSCSI vNIC.
- When an initiator IQN is set at the iSCSI vNIC level, the initiator IQN at the service profile level is removed, if one is present.
- If there are two iSCSI vNIC in a service profile and only one of them has the initiator IQN set, the second
 one is configured with the default IQN pool. You can change this configuration later. The only exception
 is if DHCP Option 43 is configured. In this case, the initiator IQN on the second iSCSI vNIC is removed
 during service profile association.



If you change an iSCSI vNIC to use the DHCP Option 43 by setting the vendor ID, it does not remove the initiator IQN configured at the service profile level. The initiator IQN at the service profile level can still be used by another iSCSI vNIC which does not use the DHCP Option 43.

Enabling MPIO on Windows



If you change the networking hardware, Windows may fail to boot from an iSCSI drive. For more information, see Microsoft support Article ID: 976042.

Before You Begin

The server on which you enable MPIO must have a Cisco VIC driver.

If there are multiple paths configured to the boot LUN, only one path should be enabled when the LUN is installed.

Procedure

Step 1 In the service profile associated with the server, configure the primary iSCSI vNIC.

For more information, see Creating an iSCSI vNIC for a Service Profile, on page 17.

- Step 2 Using the primary iSCSI vNIC, install the Windows operating system on the iSCSI target LUN.
- **Step 3** After Windows installation is completed, enable MPIO on the host.
- **Step 4** In the service profile associated with the server, add the secondary iSCSI vNIC to the boot policy. For more information, see Creating an iSCSI Boot Policy, on page 16.

Configuring iSCSI Boot

When you configure an adapter or blade in Cisco UCS to iSCSI boot from a LUN target, you need to complete all of the following steps.

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | Configure the iSCSI boot adapter policy. | (Optional) For more information, see Creating an iSCSI Adapter Policy, on page 12 |
| Step 2 | Configure the authentication profiles to be used by the initiator and target. | (Optional) For more information, see Creating an iSCSI Authentication Profile, on page 14 |
| Step 3 | If you plan to configure the iSCSI initiator to use an IP address from a pool of IP addresses, add a block of IP addresses to the iSCSI initiator pool. | (Optional) For more information, see Creating an iSCSI Initiator IP Pool, on page 15 |
| Step 4 | Create a boot policy that can be used in any service profile. Alternatively, you can create a local boot policy only for the specific service policy. However, we recommend that you create a boot policy that can be shared with multiple service profiles. | For more information about creating a boot policy that can be used in any service profile, see Creating an iSCSI Boot Policy, on page 16. |
| Step 5 | If you created a boot policy that can be used in any service profile, you need to assign it to the service profile. Otherwise, proceed to the next step. | You can assign the boot policy to the service profile while configuring the iSCSI boot and vNIC parameters in the service profile in step 7. |
| Step 6 | Create an iSCSI vNIC in a service profile. | For more information, see Creating an iSCSI vNIC for a Service Profile, on page 17 |
| Step 7 | Configure the iSCSI boot parameters, including the iSCSI qualifier name (IQN), initiator, target interfaces, and iSCSI vNIC parameters in a service profile in expert mode or service profile template. | For more information, see Creating a Service Profile with the Expert Wizard or Creating a Service Profile Template, respectively. |

| | Command or Action | Purpose |
|---------|----------------------------------|--|
| Step 8 | Verify the iSCSI boot operation. | For more information, see Verifying iSCSI Boot |
| Step 9 | Install the OS on the server. | For more information, see one of the following guides: |
| | | • Cisco UCS B-Series Blade Servers VMware Installation Guide |
| | | • Cisco UCS B-Series Blade Servers Linux Installation Guide |
| | | • Cisco UCS B-Series Blade Servers Windows Installation Guide |
| Step 10 | Boot the server. | |

Creating an iSCSI Adapter Policy

Procedure

| Step 1 | In the Naviga | tion pane, | click the Serv | ers 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 multitenancy, expand the **root** node.

Step 4 Right-click Adapter Policies and choose Create iSCSI Adapter Policy.

Step 5 In the Create iSCSI Adapter 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 other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved. |
| Connection Timeout field | The number of seconds to wait until Cisco UCS assumes that the initial login has failed and the iSCSI adapter is unavailable. |
| | Enter an integer between 0 and 255. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds). |

| Name | Description | | | |
|--------------------------------|---|--|--|--|
| LUN Busy Retry Count field | The number of times to retry the connection in case of a failure during iSCSI LUN discovery. | | | |
| | Enter an integer between 0 and 60. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds). | | | |
| DHCP Timeout field | The number of seconds to wait before the initiator assumes that the DHCP server is unavailable. | | | |
| | Enter an integer between 60 and 300 (default: 60 seconds). | | | |
| Enable TCP Timestamp check box | Check this box if you want to use a TCP Timestamp. With this setting, transmitted packets are given a time stamp of when the packet was sent so that the packet's round-trip time can be calculated, when needed. | | | |
| | Note This option only applies to servers with the Cisco UCS NIC M51KR-B adapter. | | | |
| HBA Mode check box | Check this box to enable HBA mode (also known as TCP offload). | | | |
| | Important This option should only be enabled for servers with the Cisco UCS NIC M51KR-B adapter running the Windows operating system. | | | |
| Boot to Target check box | Check this box to boot from the iSCSI target. | | | |
| | Note This option only applies to servers with the Cisco UCS NIC M51KR-B adapter. It should be disabled until you have installed an operating system on the server. | | | |
| Owner field | This can be one of the following: | | | |
| | • Local—This policy is available only to service profiles and service profile templates in this Cisco UCS domain. | | | |
| | • Pending Global —Control of this policy is being transferred to Cisco UCS Central. Once the transfer is complete, this policy will be available to all Cisco UCS domains registered with Cisco UCS Central. | | | |
| | • Global—This policy is managed by Cisco UCS Central. Any changes to this policy must be made through Cisco UCS Central. | | | |

Step 6 Click OK.

ſ

What to Do Next

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

Deleting an iSCSI Adapter 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 multitenancy, expand the root node. |
| Step 4 | Expand the Adapter Policies node. |
| Step 5 | Right-click the adapter policy and choose Delete. |
| Step 6 | If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes. |

Creating an iSCSI Authentication Profile

For iSCSI boot, you need to create both an initiator and a target iSCSI authentication profile.

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 multitenancy, expand the **root** node.
- Step 4 Right-click iSCSI Authentication Profiles and choose Create iSCSI Authentication Profile.
- **Step 5** In the Create Authentication Profile dialog box, complete the following fields:

| Name | Description |
|------------------------|---|
| Name field | The name of the authentication profile. |
| | This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved. |
| User Id field | The user Id associated with this profile. |
| | Enter between 1 and 128 characters, spaces, or special characters. |
| Password field | The password associated with this profile. |
| | Enter between 12 and 16 characters, including special characters. |
| Confirm Password field | The password again for confirmation purposes. |

Step 6 Click OK.

What to Do Next

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

Deleting an iSCSI Authentication Profile

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 multitenancy, expand the root node. |
| Step 4 | Expand the iSCSI Authentication Profiles node. |
| Step 5 | Right-click the IP pool you want to delete and choose Delete. |
| Step 6 | If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes. |

Creating an iSCSI Initiator IP Pool

You can create a group of IP addresses to be used for iSCSI boot. Cisco UCS Manager reserves the block of IPv4 addresses you specify.

The IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

- **Step 1** In the Navigation pane, click the LAN tab.
- **Step 2** In the LAN tab, expand LAN > Pools.
- **Step 3** Expand the node for the organization where you want to create the pool. If the system does not include multitenancy, expand the **root** node.
- **Step 4** Expand the **IP Pools** node.
- Step 5 Right-click IP Pool iscsi-initiator-pool and choose Create Block of IPv4 Addresses.
- **Step 6** In the **Create a Block of IPv4 Addresses** dialog box, complete the following fields:

| Name | Description |
|-------------|--|
| Name column | The range of IPv4 addresses assigned to the block. |

| Name | Description |
|------------------------|---|
| From column | The first IPv4 address in the block. |
| To column | The last IPv4 address in the block. |
| Subnet column | The subnet mask associated with the IPv4 addresses in the block. |
| Default Gateway column | The default gateway associated with the IPv4 addresses in the block. |
| Primary DNS column | The primary DNS server that this block of IPv4 addresses should access. |
| Secondary DNS column | The secondary DNS server that this block of IPv4 addresses should access. |

Step 7 Click OK.

What to Do Next

Configure one or more service profiles or service profile templates to obtain the iSCSI initiator IP address from the iSCSI initiator IP pool.

Creating an iSCSI Boot Policy

You can add up to two iSCSI vNICs per boot policy. One vNIC acts as the primary iSCSI boot source, and the other acts as the secondary iSCSI boot source.

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 multitenancy, expand the root node. |
| Step 4 | Right-click Boot Policies and choose 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 other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved. |
| Step 6 | (Optional) To reboot a server that uses 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. |

- **Note** This applies only to servers using the standard boot order.
- Step 7 (Optional) If desired, check the Enforce vNIC/vHBA/iSCSI Name check box.
 - If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the **Boot Order** table match the server configuration in the service profile.
 - If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

Step 8 To add a iSCSI boot to the boot policy, do the following:

- a) Click the down arrows to expand the iSCSI vNICs area.
- b) Click the Add iSCSI Boot link.
- c) In the Add iSCSI Boot dialog box, enter a name for the iSCSI vNIC, and click OK.
- d) Repeat steps b and c to create another iSCSI vNIC.

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.

Creating an iSCSI vNIC for a Service Profile

| 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 that contains the service profile for which you want to create an iSCSI vNIC. | | | |
| Step 4 | Expand the service profile for which you want to create a iSCSI vNIC. | | | |
| Step 5 | Right-click the iSCSI vNICs node and choose Create vNICs. | | | |
| Step 6 | In the Create iSCSI vNIC dialog box, complete the following fields: | | | |
| | Name | Description | | |
| | Name field | The name of the iSCSI vNIC. | | |
| | | This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved. | | |
| | Overlay vNIC drop-down list | The LAN vNIC associated with this iSCSI vNIC, if any. | | |

| Name | Description | | |
|--|--|--|--|
| iSCSI Adapter Policy drop-down list | The iSCSI adapter policy associated with this iSCSI vNIC, if any. | | |
| Create iSCSI Adapter Policy link | Click this link to create a new iSCSI adapter policy that will be available to all iSCSI vNICs. | | |
| MAC Address field | The MAC address associated with this iSCSI vNIC, if any. If the MAC address is not set, the Cisco UCS Manager GUI displays Derived . | | |
| MAC Pool field | The MAC pool associated with this iSCSI vNIC, if any. | | |
| VLAN drop-down list | The virtual LAN associated with this iSCSI vNIC. The default VLAN is default . | | |
| | Note For the Cisco UCS M81KR Virtual Interface Card and the Cisco UCS VIC-1240 Virtual Interface Card, the VLAN that you specify must be the same as the native VLAN on the overlay vNIC. | | |
| | For the Cisco UCS M51KR-B Broadcom BCM57711 Adapter, the VLAN that you specify can be any VLAN assigned to the overlay vNIC. | | |

- **Step 7** In the **MAC Address Assignment** drop-down list in the **iSCSI MAC Address** area, choose one of the following:
 - Leave the MAC address unassigned, select **Select (None used by default)**. Select this option if the server that will be associated with this service profile contains a Cisco UCS M81KR Virtual Interface Card adapter or a Cisco UCS VIC-1240 Virtual Interface Card.
 - Important If the server that will be associated with this service profile contains a Cisco UCS NIC M51KR-B adapter, you must specify a MAC address.
 - A specific MAC address, select **00:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link.
 - A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

If this Cisco UCS domain is registered with Cisco UCS Central, there may be two pool categories. **Domain Pools** are defined locally in the Cisco UCS domain and **Global Pools** are defined in Cisco UCS Central.

- Step 8 (Optional) If you want to create a MAC pool that will be available to all service profiles, click Create MAC Pool and complete the fields in the Create MAC Pool wizard. For more information, see Creating a MAC Pool.
- Step 9 Click OK.
- Step 10 (Optional) If you want to set or change the initiator name, from the iSCSI vNICs tab, click Reset Initiator Name or Change Initiator Name and complete the fields in the Change Initiator Name dialog box or click

. For more information, see either Setting the Initiator IQN at the Service Profile Level, on page 19 or Setting the Initiator IQN at the Service Profile Level, on page 19.

Deleting an iSCSI vNIC from a Service Profile

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 that contains the service profile from which you want to delete an iSCSI vNIC. | |
| Step 4 | Expand the service profile from which you want to delete an iSCSI vNIC. | |
| Step 5 | Expand the iSCSI vNICs node. | |
| Step 6 | Right-click the iSCSI vNIC you want to delete and choose Delete. | |
| Step 7 | If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes. | |

Setting the Initiator IQN at the Service Profile Level

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 desired node for the organization. |
| Step 4 | Click the service profile that has the iSCSI vNIC that you want to change. |
| Step 5 | In the Work pane, click the iSCSI vNICs tab. |
| Step 6 | Click Reset Initiator Name. |
| Step 7 | If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes. |

Changing the Initiator IQN at the Service Profile Level

Procedure

| Step I In the Navigation pane, click the Servers tat | Step 1 | In the Navigation | pane, click the | Servers tab. |
|--|--------|-------------------|-----------------|--------------|
|--|--------|-------------------|-----------------|--------------|

- **Step 2** On the Servers tab, expand Servers > Service Profiles.
- **Step 3** Expand the desired node for the organization.
- Step 4 Click the service profile that has the iSCSI vNIC that you want to change.
- **Step 5** In the Work pane, click the iSCSI vNICs tab.
- **Step 6** In the Actions area, click Change Initiator Name.
- Step 7 In the Change Initiator Name dialog box, change the values in the following fields

| Name | Description |
|--|--|
| Initiator Name Assignment drop-down list | Choose the IQN initiator name that you want to use from the drop-down list. |
| Initiator Name field | If you selected a manual initiator name assignment, enter the initiator name. |
| Create IQN Suffix Pool link | Click to create a new IQN suffix pool. |

Step 8 Click OK.

Setting iSCSI Boot Parameters

You can set iSCSI boot parameters, including the boot order, boot policy, iSCSI authentication profile, initiator interface, and target interface for an iSCSI vNIC.

I

- **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 that contains the service profile for which you want to create iSCSI boot parameters. If the system does not include multi-tenancy, expand the root node.
- Step 4 Click the service profile for which you want to create iSCSI boot parameters.
- **Step 5** Click the **Boot Order** tab.
- Step 6 In the Specific Boot Policy area, click the down arrows to expand the iSCSI vNICs area.
- **Step 7** In the **iSCSI vNICs** area, double-click the iSCSI vNICs from which you want to boot the server to add them to the **Boot Order** table.
- Step 8In the iSCSI vNICs area, click the Set Boot Parameters link.If there are two iSCSI vNICs, choose the one for which you want to set boot parameters.

Step 9 In the **Set iSCSI Boot Parameters** dialog box, complete the following fields:

| Name | Description |
|--|---|
| Name field | The name of the iSCSI vNIC for which you are setting the boot parameters. |
| Authentication Profile drop-down list | The name of the associated iSCSI authentication profile. |
| Create Authentication Profile link | Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs. |

Step 10 In the **Initiator Name** area, complete the following fields:

| Name | Description | |
|---|---|--|
| Initiator Name Assignment drop-down list | Select how the iSCSI boot initiator name is assigned. Choose on the following methods: | |
| | • Manual —You will enter a name in the Initiator Name field. The initiator name can contain up to 223 characters. | |
| | • Pools- assigne | -Choose an IQN suffix pool from which the name will be ed. |
| | Note If y mo | ou need to, you can change or reset the initiator name. For re information, see Changing the Initiator IQN at the Service |
| | Note Set dia not con vN | the Level, on page 20 ting the Initiator Name from the Set iSCSI Boot Parameters log box sets the initiator IQN at the iSCSI vNIC level and at the service profile level. If more than one path is figured, you must set the initiator IQN from the iSCSI ICs tab or when creating a service profile. |

| Name | Description |
|-----------------------------|--|
| Create IQN Suffix Pool link | Click this link to create a new IQN suffix pool that will be available to all iSCSI vNICs. |
| Initiator Name field | A regular expression that defines the name of the iSCSI initiator. |
| | You can enter any alphanumeric string as well as the following special characters: |
| | • . (period) |
| | • : (colon) |
| | • - (dash) |
| | |

Step 11 From the Initiator IP Address Policy drop-down list, choose of the following:

| Option | Description |
|-------------------------------|--|
| Select (DHCP used by default) | The system selects an interface automatically using DHCP. Proceed to Step 13. |
| Static | A static IPv4 address is assigned to the iSCSI boot vNIC based on the information entered in this area. Proceed to Step 12. |
| Pool | An IPv4 address is assigned to the iSCSI boot vNIC from the management IP address pool. Proceed to Step 13. |

Step 12 If you chose Static from the Initiator IP Address Policy drop-down list, complete the following fields:

| Name | Description |
|-----------------------|--|
| IPv4 Address field | The IPv4 address assigned to the iSCSI boot vNIC. |
| | If you want to specify this address, you must select Static in the Initiator IP Address Policy drop-down list. |
| Subnet Mask field | The subnet mask associated with the IPv4 address. |
| Default Gateway field | The default gateway associated with the IPv4 address. |
| Primary DNS field | The primary DNS server address. |
| Secondary DNS field | The secondary DNS server address. |

Step 13 For the iSCSI target interface, choose one of the following radio buttons:

ſ

| Option | Description |
|-------------------------------|---|
| iSCSI Static Target Interface | The system creates a static target interface that you need to configure. Proceed to Step 14. |
| iSCSI Auto Target Interface | The system creates an auto target interface. You need to specify whether the auto target uses an initiator or a DCHP vendor ID. Proceed to Step 16. |

Step 14 If you chose iSCSI Static Target Interface, in the Static Target Interface table, click Add.

Step 15 In the Create iSCSI Static Target dialog box, complete the following fields:

| Name | Description | |
|---|--|--|
| iSCSI Target Name field | A regular expression that defines the iSCSI Qualified Name (IQN) or Extended Unique Identifier (EUI) name of the iSCSI target. | |
| | You can enter any alphanumeric characters as well as the following special characters: | |
| | • . (period) | |
| | • : (colon) | |
| | • - (dash) | |
| | ImportantThis name must be properly formatted using standard IQN or EUI guidelines.The following examples show properly formatted iSCSI target names: | |
| | • iqn.2001-04.com.example | |
| | • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 | |
| | iqn.2001-04.com.example:storage.tape1.sys1.xyz | |
| | • iqn.2001-04.com.example:storage.disk2.sys1.xyz | |
| | • eui.02004567A425678D | |
| Priority field | The system-assigned priority for the iSCSI target. | |
| Port field | The port associated with the iSCSI target. | |
| | Enter an integer between 1 and 65535. The default is 3260. | |
| Authentication Profile drop-down list | The name of the associated iSCSI authentication profile. | |
| Create iSCSI Authentication Profile link | Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs. | |
| IPv4 Address field | The IPv4 address assigned to the iSCSI target. | |

| Name | Description |
|--------------|---|
| LUN Id field | The LUN identifier in the iSCSI target. |

Step 16 If you chose **iSCSI Auto Target Interface**, enter either the initiator name or the DHCP vendor ID in the **DHCP Vendor Id** field. The initiator must have already been configured. The vendor ID can be up to 32 alphanumeric characters.

Step 17 Click OK.

Modifying iSCSI Boot Parameters

You can modify iSCSI boot parameters, including the boot order, boot policy, iSCSI authentication profile, initiator interface, and target interface for an iSCSI vNIC.

Procedure

| Step 1 In the Navigation | pane, | click the | e Servers | tab. |
|--------------------------|-------|-----------|-----------|------|
|--------------------------|-------|-----------|-----------|------|

Step 2 On the Servers tab, expand Servers > Service Profiles.

- **Step 3** Expand the node for the organization that contains the service profile for which you want to modify iSCSI boot parameters. If the system does not include multi-tenancy, expand the root node.
- Step 4 Click the service profile for which you want to modify iSCSI boot parameters.
- **Step 5** Click the **Boot Order** tab.
- **Step 6** In the **Specific Boot Policy** area, click the down arrows to expand the **iSCSI vNICs** area.
- **Step 7** To add or delete an iSCSI vNIC from the boot order or to change the boot order, do one of the following:
 - To add an iSCSI vNIC, in the **iSCSI vNICs** area, double-click an iSCSI vNICs to add it to the **Boot Order** table.
 - To delete an iSCSI vNIC from the boot order, in the **Boot Order** table, select the iSCSI vNIC and click **Delete**.

• To change the iSCSI vNIC boot order, in the **Boot Order** table, select the iSCSI vNIC and click either **Move Up** or **Move Down**.

Step 8 To change the boot parameters, in the **iSCSI vNICs** area, click the **Set Boot Parameters** link. If there are two iSCSI vNICs, choose the one for which you want to change boot parameters.

Step 9 In the **Set iSCSI Boot Parameters** dialog box, change the values in any of the following fields:

| Name | Description |
|------------|---|
| Name field | The name of the iSCSI vNIC for which you are setting the boot parameters. |

I

| Name | Description |
|--|---|
| Authentication Profile drop-down list | The name of the associated iSCSI authentication profile. |
| Create Authentication Profile link | Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs. |

Step 10 In the **Initiator Name** area, complete the following fields:

| Name | Description |
|---|---|
| Initiator Name Assignment drop-down list | Select how the iSCSI boot initiator name is assigned. Choose one of the following methods: |
| | • Manual —You will enter a name in the Initiator Name field. The initiator name can contain up to 223 characters. |
| | • Pools —Choose an IQN suffix pool from which the name will be assigned. |
| | Note If you need to, you can change or reset the initiator name. For more information, see Changing the Initiator IQN at the Service Profile Level, on page 20 Setting the Initiator Name from the Set iSCSI Boot Parameters dialog box sets the initiator IQN at the iSCSI vNIC level and not at the service profile level. If more than one path is configured, you must set the initiator IQN from the iSCSI vNICs tab or when creating a service profile. |
| Create IQN Suffix Pool link | Click this link to create a new IQN suffix pool that will be available to all iSCSI vNICs. |
| Initiator Name field | A regular expression that defines the name of the iSCSI initiator. |
| | You can enter any alphanumeric string as well as the following special characters: • . (period) • : (colon) • - (dash) |
| | |

Step 11 From the **Initiator IP Address Policy** drop-down list, change the selection to one of the following:

| Option | Description |
|-------------------------------|--|
| Select (DHCP used by default) | The system selects an interface automatically using DHCP. Proceed to Step 13. |

| Option | Description |
|--------|--|
| Static | A static IPv4 address is assigned to the iSCSI boot vNIC based on the information entered in this area. Proceed to Step 12. |
| Pool | An IPv4 address is assigned to the iSCSI boot vNIC from the management IP address pool. Proceed to Step 13. |

Step 12 If you chose **Static** from the **Initiator IP Address Policy** drop-down list, complete or change the following fields:

| Name | Description |
|-----------------------|--|
| IPv4 Address field | The IPv4 address assigned to the iSCSI boot vNIC. |
| | If you want to specify this address, you must select Static in the Initiator IP Address Policy drop-down list. |
| Subnet Mask field | The subnet mask associated with the IPv4 address. |
| Default Gateway field | The default gateway associated with the IPv4 address. |
| Primary DNS field | The primary DNS server address. |
| Secondary DNS field | The secondary DNS server address. |

Step 13 For the iSCSI target interface, choose one of the following radio buttons:

| Option | Description |
|-------------------------------|---|
| iSCSI Static Target Interface | The system creates a static target interface that you need to configure. Proceed to Step 14. |
| iSCSI Auto Target Interface | The system creates an auto target interface. You need to specify whether the auto target uses an initiator or a DCHP vendor ID. Proceed to Step 15. |

Step 14 If you chose iSCSI Static Target Interface, do one of the following in the Static Target Interface table:

• To add an iSCSI static target interface, click **Add** or to modify an iSCSI target interface, select the iSCSI target interface that you want to change and click **Modify**. Then and complete or change the following fields in the **Create iSCSI Static Target** dialog box:

I

| Name | Description |
|---|--|
| iSCSI Target Name field | A regular expression that defines the iSCSI Qualified Name (IQN) or Extended Unique Identifier (EUI) name of the iSCSI target. |
| | You can enter any alphanumeric characters as well as the following special characters: |
| | • . (period) |
| | • : (colon) |
| | • - (dash) |
| | Important This name must be properly formatted using standard IQN or EUI guidelines. |
| | names: |
| | • iqn.2001-04.com.example |
| | • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 |
| | • iqn.2001-04.com.example:storage.tape1.sys1.xyz |
| | • iqn.2001-04.com.example:storage.disk2.sys1.xyz |
| | • eui.02004567A425678D |
| Priority field | The system-assigned priority for the iSCSI target. |
| Port field | The port associated with the iSCSI target. |
| | Enter an integer between 1 and 65535. The default is 3260. |
| Authentication Profile drop-down list | The name of the associated iSCSI authentication profile. |
| Create iSCSI Authentication Profile link | Click this link to create a new iSCSI authentication profile that will be available to all iSCSI vNICs. |
| IPv4 Address field | The IPv4 address assigned to the iSCSI target. |
| LUN Id field | The LUN identifier in the iSCSI target. |

• To delete an iSCSI target interface, select the iSCSI target interface that you want to delete and click **Delete**.

Note If you have two iSCSI static targets and you delete the first priority target, the second priority target becomes the first priority target, although Cisco UCS Manager still shows it as the second priority target.

- Step 15 If you chose iSCSI Auto Target Interface, change the entry to either the initiator name or the DHCP vendor ID in the DHCP Vendor Id field. The initiator must have already been configured. The vendor ID can be up to 32 alphanumeric characters.
- Step 16 Click OK.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain.

IQN pool members are of the form *prefix:suffix:number*, where you can specify the prefix, suffix, and a block (range) of numbers.

An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but sharing the same prefix.

Creating an IQN Pool

Note

In most cases, the maximum IQN size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

- **Step 1** In the Navigation pane, click the SAN tab.
- **Step 2** On the **SAN** tab, expand **SAN** > **Pools**.
- **Step 3** Expand the node for the organization where you want to create the pool. If the system does not include multitenancy, expand the **root** node.
- Step 4 Right-click IQN Pools and select Create IQN Suffix Pool.
- **Step 5** In the **Define Name and Description** page of the **Create IQN Suffix Pool** wizard, fill in the following fields:

| Name | Description |
|--------------------------|---|
| Name field | The name of the iSCSI Qualified Name (IQN) pool. |
| | This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved. |
| Description field | The user-defined description of the pool. |
| | Enter up to 256 characters. You can use any characters or spaces except `(accent mark), \(backslash), ^(carat), "(double quote), = (equal sign), > (greater than), < (less than), or '(single quote). |

| Name | Description |
|------------------------|---|
| Prefix field | The prefix for any IQN blocks created for this pool. |
| | Enter from 1 to 150 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use iqn1.alpha.com. |
| Assignment Order field | This can be one of the following: |
| | • Default —Cisco UCS Manager selects a random identity from the pool. |
| | • Sequential—Cisco UCS Manager selects the lowest available identity from the pool. |

- Step 6 Click Next.
- Step 7 In the Add IQN Blocks page of the Create IQN Suffix Pool wizard, click Add.
- **Step 8** In the Create a Block of IQN Suffixes dialog box, fill in the following fields:

| Name | Description |
|--------------|---|
| Suffix field | The suffix for this bock of iSCSI Qualified Names (IQNs). |
| | Enter from 1 to 64 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use alphadc-1. |
| From field | The first suffix number in the block. |
| Size field | The number of suffixes in the block. |

Step 9 Click OK.

I

Step 10 Click **Finish** to complete the wizard.

What to Do Next

Include the IQN suffix pool in a service profile and/or template.

Adding a Block to an IQN Pool

Procedure

| | Name | Description |
|--------|---|---|
| Step 6 | In the Create a Block of IQN Suffi | xes dialog box, fill in the following fields: |
| Step 5 | Right-click the desired IQN pool an | d select Create a Block of IQN Suffixes. |
| Step 4 | Expand the IQN Pools node. | |
| Step 3 | Expand the node for the organizatio If the system does not include multi | n containing the pool. tenancy, expand the root node. |
| Step 2 | On the SAN tab, expand $SAN > Poolement Poo$ | bls. |
| Step 1 | In the Navigation pane, click the S A | N tab. |

| iname | Description |
|--------------|---|
| Suffix field | The suffix for this bock of iSCSI Qualified Names (IQNs). |
| | Enter from 1 to 64 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use alphadc-1. |
| From field | The first suffix number in the block. |
| Size field | The number of suffixes in the block. |

Step 7 Click OK.

Deleting a Block from an IQN Pool

If you delete an address block from a pool, Cisco UCS Manager does not reallocate any addresses in that block that have been assigned to vNICs or vHBAs. All assigned addresses from a deleted block remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

- Step 1 In the Navigation pane, click the SAN tab.
- **Step 2** On the **SAN** tab, expand **SAN** > **Pools**.
- **Step 3** Expand the node for the organization containing the pool.

If the system does not include multitenancy, expand the **root** node.

- Step 4 Expand the IQN Pools node.
- **Step 5** Choose the IQN pool for which you want to delete a block of IQN suffixes.
- **Step 6** In the Work pane, click the IQN Blocks tab.
- **Step 7** Right-click the block to be deleted and select **Delete**.
- Step 8 Click Yes to confirm the deletion.
- Step 9 Click Save Changes.

Deleting an IQN Pool

If you delete a pool, Cisco UCS Manager does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

| Step 1 | In the Navigation pane, click the SAN tab. |
|--------|--|
| Step 2 | On the SAN tab, expand SAN > Pools. |
| Step 3 | Expand the node for the organization containing the pool. If the system does not include multitenancy, expand the root node. |
| Step 4 | Expand the IQN Pools node. |
| Step 5 | Right-click the pool you want to delete and select Delete. |
| Step 6 | If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes. |

LAN Boot

You can configure a boot policy to boot one or more servers from a centralized provisioning server on the LAN. A LAN (or PXE) boot is frequently used to install operating systems on a server from that LAN server.

You can add more than one type of boot device to a LAN boot policy. For example, you could add a local disk or virtual media boot as a secondary boot device.

Configuring a LAN Boot for 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.

You can add more than one type of boot device to a boot policy. For example, you could add a local disk or virtual media boot as a secondary boot device.

This procedure continues directly from Creating a Boot Policy, on page 5.

Procedure

- **Step 1** Click the down arrows to expand the vNICs area.
- Step 2 Click the Add LAN Boot link.
- Step 3 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.
- **Step 4** Do one of the following:
 - Add another boot device to the Boot Order table.
 - 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.

Local Devices Boot

Cisco UCS Manager allows you to boot from different local devices.



For Cisco UCS M3 and M4 blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can only select a top-level device.

Local Disk Boot

If a server has a local drive, you can configure a boot policy to boot the server from the top-level local disk device or from any of the following second-level devices:

- Local LUN
- SD card

- Internal USB
- External USB



Second-level devices are only available for Cisco UCS M3 and M4 blade and rack servers using enhanced boot order. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can choose only the top-level Add Local Disk.

Virtual Media Boot

You can configure a boot policy to boot one or more servers from a virtual media device that is accessible from the server. A virtual media device mimics the insertion of a physical CD/DVD disk (read-only) or floppy disk (read-write) into a server. This type of server boot is typically used to manually install operating systems on a server.



Second-level devices are only available for Cisco UCS M3 and M4 blade and rack servers using enhanced boot order. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can choose only the top-level Add CD/DVD or Add Floppy.

Remote Virtual Drive Boot

You can configure a boot policy to boot one or more servers from a remote virtual drive that is accessible from the server.

Configuring a Local Disk Boot for 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.

You can add more than one type of boot device to a boot policy. For example, you could add an SD card boot as a secondary boot device.

This procedure continues directly from Creating a Boot Policy, on page 5.

- **Step 1** Click the down arrows to expand the **Local Devices** area.
- **Step 2** Click any of the following links to add the device to the **Boot Order** table:
 - Add Local Disk or
 - Add Local LUN
 - Add SD Card
 - ° Add Internal USB

Add External USB

- **Note** For Cisco UCS M3 and M4 blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can only select a top-level device.
- **Step 3** Do one of the following:
 - Add another boot device to the **Boot Order** table.
 - 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.

Configuring a Virtual Media Boot for 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.

You can add more than one type of boot device to a boot policy. For example, you could add a local disk boot as a second boot device.

Note

Virtual Media requires the USB to be enabled. If you modify the BIOS settings that affect the USB functionality, you also affect the Virtual Media. Therefore, we recommend that you leave the following USB BIOS defaults for best performance:

- Make Device Non Bootable-set to disabled
- USB Idle Power Optimizing Setting-set to high-performance

This procedure continues directly from Creating a Boot Policy, on page 5.

- **Step 1** Click the down arrows to expand the Local Devices area.
- **Step 2** Click any of the following links to add the device to the **Boot Order** table:
 - Add CD/DVD or
 - Add Local CD/DVD
 - Add Remote CD/DVD

· Add Floppy or

Add Local Floppy

- Add Remote Floppy
- Add Remote Virtual Drive
- **Note** For Cisco UCS M3 and M4 blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS M1 and M2 blade and rack servers using standard boot order, you can only select a top-level device.

Step 3 Do one of the following:

- Add another boot device to the **Boot Order** table.
- 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.

Creating a vMedia Boot Policy

I

| Step | 1 | In | the | Navigatio | on pane, | click the | Servers tab. | |
|------|---|----|-----|-----------|----------|-----------|--------------|--|
| • | - | ~ | | ~ | | 1.0 | | |

- **Step 2** On the Servers tab, expand Servers > Policies.
- **Step 3** Right-click **Boot Policies** and select **Create Boot Policy**.
- Step 4 In the Create Boot Policy dialog box, complete the following fields:

| Name | Description |
|-------------------|---|
| Name field | The name of the policy. |
| Description field | A description of the policy. We recommend that you include information about where and when the policy should be used. |
| | Enter up to 256 characters. You can use any characters or spaces except `(accent mark), \(backslash), ^(carat), "(double quote), = (equal sign), > (greater than), < (less than), or '(single quote). |

| Name | Description | |
|---|---|--|
| Reboot on Boot Order Change check box | If checked, the system reboots the server if you make changes to the boot order. If this option is selected, following action occurs: | |
| | • If any CDD/HDD device is present in vMedia policy and same device is present in boot policy, any change in vmedia policy for that particular device will cause server reboot. The purpose of this reboot is to boot from the latest mounted image. | |
| | • If any CDD/HDD device is present in vMedia policy and same device is not present in boot policy, any change in vmedia policy for that particular device will not cause a server reboot. | |
| | Note If this option is not selected, any modification in vMedia policy will not cause host reboot. If you add or change boot devices for a non-virtualized adapter, the system always reboots the server. | |
| Boot Mode field | The type of boot mode that is enabled. This can be one of the following: | |
| | • Legacy—Select if the system is not UEFI-enabled. | |
| | • Uefi—Select if the system is UEFI-enabled. | |
| | Note UEFI boot mode requires that the adapter firmware is UEFI-enabled, the boot device has a UEFI-aware operating system, and the service profile be associated with a Cisco UCS M3 blade or rack server. | |

- Step 5 Expand the CIMC Mounted vMedia to add a virtual Remote vMedia Device to the boot order.
- Step 6Click the Add Remote vMedia HDD or Add Remote vMedia CD/DVD link.Depending on the vMedia device you select, the Add Remote vMedia dialog box displays.
- Step 7 Add the CIMC Mounted CD/DVD or CIMC Mounted HDD from the drop-down list.

Step 8 Click OK.

The vMedia Boot Policy is added to the Boot Order pane.

What to Do Next

Associate the vMedia and Boot Policies with a Service Profile.

Adding a Boot Policy to a vMedia Service Profile

This procedure describes how to set the boot policy options for vMedia on the Server Boot Order page of the Create Service Profile (expert) wizard.

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 where you want to create the service profile. If the system does not include multitenancy, expand the **root** node.
- Step 4Right-click the organization and select Create Service Profile (expert).The Unified Computing System Manager pane displays.
- Step 5 In the Name field, enter a unique name that you can use to identify the service profile. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.

This name must be unique within the organization or sub-organization in which you are creating the service profile.

| Option | Description |
|--|---|
| Select (pool default used by default) | Assigns a UUID from the default UUID Suffix pool. |
| | Continue with Step 8. |
| Hardware Default | Uses the UUID assigned to the server by the manufacturer. |
| | If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server. Continue with Step 8. |
| XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXXXX | Uses the UUID that you manually assign. |
| | Continue with Step 7. |

Step 6 From the **UUID** Assignment drop-down list, do one of the following:

| Option | Description |
|-----------------|---|
| Pools Pool_Name | Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. |
| | Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool. |
| | If you do not want use any of the existing pools, but instead want to create a pool that all service profiles can access, continue with Step 4. Otherwise, continue with Step 8. |

- - a) In the UUID field, enter the valid UUID that you want to assign to the server which uses this service profile.
 - b) To verify that the selected UUID is available, click the here link.
- Step 8 (Optional) If you want to create a new UUID Suffix pool to use to use in this service profile, click Create UUID Suffix Pool and complete the fields in the Create UUID Suffix Pool wizard. For more information, see Creating a UUID Suffix Pool.
- **Step 9** (Optional) In the text box, enter a description of this service profile. The user-defined description for this service profile.

Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), $^$ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

- Step 10 Click Next.
- **Step 11** Navigate to Create Service Profile (expert) and click Server Boot Order. The Boot Policy pane displays.
- Step 12 From the Boot Policy drop-down list, choose one of the following:

| Option | Description |
|-------------------------------|--|
| Select Boot Policy to use | Assigns the default boot policy to this service profile. Continue with Step 13. |
| Create a Specific Boot Policy | Enables you to create a local boot policy that can only be accessed by this service profile. |

| Option | Description |
|---------------------------|---|
| Boot Policies Policy_Name | Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. |
| | If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click Create Boot Policy . Otherwise, choose a policy from the list and continue with Step 13. |

Step 13 If you created a new boot policy accessible to all service profiles and template, choose that policy from the Boot Policy drop down list.

Step 14 Click Next.

What to Do Next

Associate your Service Profile with a Cisco UCS 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 > <i>Organization_Name</i> . | |
| Step 3 | Expand the Boot Policies node. | |
| Step 4 | Right-click the policy you want to delete and choose Delete. | |
| Step 5 | If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes. | |

UEFI Boot Parameters

UEFI boot mode for servers is dependent on information that is stored on the platform hardware. The boot entry, which contains information about the UEFI OS boot loader, is stored in the BIOS flash of the server. In Cisco UCS Manager releases earlier than Release 2.2(4), when a service profile is migrated from one server to another server, the boot loader information is not available on the destination server. Hence, the BIOS cannot load the boot loader information for the server to boot in UEFI boot mode.

Cisco UCSM Release 2.2(4) introduces UEFI boot parameters to provide the BIOS with information about the location of the UEFI OS boot loader on the destination server from where the BIOS loads it. Now, the server can use the boot loader information and boot in UEFI boot mode.

Guidelines and Limitations for UEFI Boot Parameters

• UEFI boot parameters can be configured only if the boot mode is UEFI.

- When you upgrade Cisco UCS Manager to Release 2.2(4), UEFI boot failure during service profile migration is not handled automatically. You must explicitly create the UEFI boot parameters in the target device to successfully boot to the UEFI-capable OS.
- UEFI boot parameters are supported on all M3 and higher servers that support second-level boot order.
- UEFI boot parameters can be specified for the following device types:
 - \circ SAN LUN
 - ISCSI LUN
 - Local LUN
- UEFI boot parameters are specific to each Operating System. They can be specified for the following Operating Systems:
 - ° VMware ESX
 - SuSE Linux
 - ° Microsoft Windows
 - Red Hat Enterprise Linux 7

Setting UEFI Boot Parameters

Before You Begin

Ensure that the **Boot Mode** of the boot policy is **Uefi**.

| Step 1 | In the Navigation pane, click the Servers tab. | | | |
|------------------|---|---|--|--|
| Step 2 | On the Servers tab, expand Servers > Policies. | | | |
| Step 3 | Expand Boot Policies and select the boot policy for which you want to configure UEFI boot parameters. | | | |
| Step 4 | In the Work pane, click the General tab. | | | |
| Step 5 Step 6 | tep 5 To set UEFI boot parameters for a LUN, select the LUN in the Boot Order area and click Set Uefi Boot Parameters. Important You can configure UEFI boot parameters only for local LUNs, SAN LUNs, and iSCSI LUNs. tep 6 In the Set Uefi Boot Parameters dialog box, enter the following information: | | | |
| - | Name | Description | | |
| | Boot Loader Name field | Specifies the name of the boot loader. This is a mandatory field. | | |
| | Boot Loader Path field | Specifies the path where the boot loader is located. This is a mandatory field. | | |

| Name | Description |
|-------------------------------|----------------------------|
| Boot Loader Description field | Describes the boot loader. |

Step 7 Click OK

Step 8 Click Save Changes.

Modifying UEFI Boot Parameters

Before You Begin

Ensure that the Boot Mode of the boot policy is Uefi.

Procedure

| Step 1 In the Navigation pane, click the Servers ta | аb. |
|---|-----|
|---|-----|

- **Step 2** On the Servers tab, expand Servers > Policies.
- Step 3 Expand Boot Policies and select the boot policy for which you want to modify UEFI boot parameters.
- **Step 4** In the Work pane, click the General tab.
- Step 5 To modify UEFI boot parameters for a LUN that already has UEFI boot parameters, select the LUN in the Boot Order area and click Modify Uefi Boot Parameters.
 Important You can configure UEFI boot parameters only for local LUNs, SAN LUNs, and iSCSI LUNs.

Step 6 In the Modify Uefi Boot Parameters dialog box, enter the following information:

| Name | Description |
|-------------------------------|---|
| Boot Loader Name field | Specifies the name of the boot loader. This is a mandatory field. |
| Boot Loader Path field | Specifies the path where the boot loader is located. This is a mandatory field. |
| Boot Loader Description field | Describes the boot loader. |

Step 7 Click OK

Step 8 Click Save Changes.

٦