



Configuring Server Boot

This chapter includes the following sections:

- [Boot Policy, page 1](#)
- [Creating a Boot Policy, page 2](#)
- [SAN Boot, page 3](#)
- [iSCSI Boot, page 5](#)
- [LAN Boot, page 27](#)
- [Local Disk Boot, page 28](#)
- [Virtual Media Boot, page 28](#)
- [Deleting a Boot Policy, page 30](#)

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.

Creating a Boot Policy

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

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 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.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.
- Step 7** (Optional) 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, vHBAs, or iSCSI vNICs (as appropriate for the boot option) from the server configuration in the service profile. It does not report whether the vNICs, vHBAs, or iSCSI vNICs specified in the boot policy match the server configuration in the service profile.
- Step 8** Configure one or more of the following boot options for the boot policy and set their boot order:
- **SAN Boot**—To boot from an operating system image on the SAN, continue with [Configuring a SAN Boot for a Boot Policy](#), on page 3.
You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.
 - **iSCSI Boot**—To boot from an iSCSI LUN, continue with [Creating an iSCSI Boot Policy](#), on page 13.
 - **LAN Boot**—To boot from a centralized provisioning server, continue with [Configuring a LAN Boot for a Boot Policy](#), on page 27.
 - **Local Disk boot**—To boot from the local disk on the server, continue with [Configuring a Local Disk Boot for a Boot Policy](#), on page 28.

- **Virtual Media Boot** —To boot from virtual media that mimics the insertion of a physical CD or floppy drive into a server, continue with [Configuring a Virtual Media Boot for a Boot Policy](#), on page 29.

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 on the device where the operating system image is located.

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, except for iSCSI boot, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.



Tip

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

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

This procedure continues directly from [Creating a Boot Policy](#), on page 2.

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.

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, complete the following fields, and click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • Primary—The first address defined for the associated boot device class. A boot policy can only have one primary LAN, SAN, or iSCSI boot location. • Secondary—The second address defined for the associated boot device class. Each boot policy can have only one secondary LAN or SAN boot location. <p>The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.</p>

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, complete the following fields, then click **OK**:

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

Name	Description
Type field	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • Primary—The first address defined for the associated boot device class. A boot policy can only have one primary LAN, SAN, or iSCSI boot location. • Secondary—The second address defined for the associated boot device class. Each boot policy can have only one secondary LAN or SAN boot location. <p>The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.</p>

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 server blades 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 M82-8P 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 6.

For a high-level procedure for implementing iSCSI boot, see [Configuring iSCSI Boot](#), on page 8.

iSCSI Boot Process

The Cisco UCS Manager iSCSI vNIC and iSCSI boot information created for the service profile is used in the association process to program the mezzanine adapter, located on the blade server. After the adapter is programmed, the blade 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.

**Note**

The iBFT only uses the first iSCSI vNIC and only Target 1 for the initiator-to-target initialization. This scenario is true even if a second target (Target 2) exists for the first iSCSI vNIC.

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 (also known as TCP offload), 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:

- 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:

- Blades 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), the MAC address of an iSCSI device needs to be configured 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.



Note 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 M82-8P 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.

Enabling MPIO on Windows



Note 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.

Procedure

-
- Step 1** In the service profile associated with the server, configure the primary and secondary iSCSI vNICs. For more information, see [Creating an iSCSI vNIC for a Service Profile, on page 14](#).
 - Step 2** Using the primary iSCSI vNIC, install the Windows operating system on the iSCSI target LUN.
 - Step 3** After Windows installation is completed, use the Microsoft software iSCSI initiator to connect to the secondary iSCSI vNIC.
 - Step 4** Enable MPIO on the host
 - Step 5** 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 13](#).
-

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.

Procedure

	Command or Action	Purpose
Step 1	Configure the iSCSI boot adapter policy.	(Optional) For more information, see Creating an iSCSI Adapter Policy, on page 9
Step 2	Configure the authentication profiles to be used by the initiator and target.	(Optional) For more information, see Creating an Authentication Profile, on page 11
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 12

	Command or Action	Purpose
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 13.
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 14
Step 7	Configure the iSCSI boot parameters, including the initiator and 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.
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: <ul style="list-style-type: none"> • <i>Cisco UCS B-Series Blade Servers VMware Installation Guide</i> • <i>Cisco UCS B-Series Blade Servers Linux Installation Guide</i> • <i>Cisco UCS B-Series Blade Servers Windows Installation Guide</i>
Step 10	Boot the server.	

Creating 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** 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	<p>The name of the policy.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</p>
Connection Timeout field	<p>The number of seconds to wait until Cisco UCS assumes that the initial login has failed and the iSCSI adapter is unavailable.</p> <p>Enter an integer between 0 and 255. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds).</p>
LUN Busy Retry Count field	<p>The number of times to retry the connection in case of a failure during iSCSI LUN discovery.</p> <p>Enter an integer between 0 and 60. If you enter 0, Cisco UCS uses the value set in the adapter firmware (default: 15 seconds).</p>
DHCP Timeout field	<p>The number of seconds to wait before the initiator assumes that the DHCP server is unavailable.</p> <p>Enter an integer between 60 and 300 (default: 60 seconds).</p>
Enable TCP Timestamp check box	<p>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.</p> <p>Note This option only applies to servers with the Cisco UCS NIC M51KR-B adapter.</p>
HBA Mode check box	<p>Check this box to enable HBA mode.</p> <p>Important This option should only be enabled for servers with the Cisco UCS NIC M51KR-B adapter running the Windows operating system.</p>
Boot to Target check box	<p>Check this box to boot from the iSCSI target.</p> <p>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.</p>

Step 6 Click **OK**.

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 Authentication Profile

For iSCSI boot, you need to create both an initiator and a target 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 **Authentication Profiles** and choose **Create 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 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 **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 IP 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.

Procedure

- 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** Right-click **IP Pool (iscsi-initiator-pool)** and choose **Create Block of IP Addresses**.
- Step 5** In the **Create a Block of IP Addresses** dialog box, complete the following fields:

Name	Description
From field	The first IP address in the block.

Name	Description
Size field	The number of IP addresses in the pool.
Subnet Mask field	The subnet mask associated with the IP addresses in the block. All IP addresses in the management IP pool must be in the same subnet as the IP address of the fabric interconnect.
Default Gateway field	The default gateway associated with the IP addresses in the block.

Step 6 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.

Deleting an iSCSI Initiator IP Pool

Procedure

- Step 1** In the **Navigation** pane, click the **LAN** tab.
- Step 2** In the **LAN** tab, expand **LAN > Pools > *Organization_Name***.
- Step 3** Expand the **IP Pools (iscsi-initiator-pools)** node.
- Step 4** Right-click the IP pool you want to delete and choose **Delete**.
- Step 5** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

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 all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.
- Step 7** (Optional) 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, vHBAs, or iSCSI vNICs (as appropriate for the boot option) from the server configuration in the service profile. It does not report whether the vNICs, vHBAs, or iSCSI vNICs specified in the boot policy match the server configuration in 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

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 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.
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, 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 M82-8P 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 M82-8P 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.

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](#).

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 iSCSI Boot Parameters

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

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 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 8** 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 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.

Name	Description
Authentication Profile drop-down list	The name of the associated authentication profile.
Create Authentication Profile link	Click this link to create a new authentication profile policy 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: <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • . (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.

Option	Description
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:

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 DHCP 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	<p>A regular expression that defines the iSCSI Qualified Name (IQN) or Extended Unique Identifier (EUI) name of the iSCSI target.</p> <p>You can enter any alphanumeric characters as well as the following special characters:</p> <ul style="list-style-type: none"> • . (period) • : (colon) • - (dash) <p>Important This name must be properly formatted using standard IQN or EUI guidelines.</p> <p>The following examples show properly formatted iSCSI target names:</p> <ul style="list-style-type: none"> • 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	<p>The port associated with the iSCSI target.</p> <p>Enter an integer between 1 and 65535. The default is 3260.</p>
Authentication Profile drop-down list	The name of the associated authentication profile.
Create Authentication Profile link	Click this link to create a new authentication profile policy 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.

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, authentication profile, initiator interface, and target interface for an iSCSI vNIC.

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 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.
Authentication Profile drop-down list	The name of the associated authentication profile.
Create Authentication Profile link	Click this link to create a new authentication profile policy 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: <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • . (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.
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.

Name	Description
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 DHCP 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:

Name	Description
iSCSI Target Name field	<p>A regular expression that defines the iSCSI Qualified Name (IQN) or Extended Unique Identifier (EUI) name of the iSCSI target.</p> <p>You can enter any alphanumeric characters as well as the following special characters:</p> <ul style="list-style-type: none"> . (period) : (colon) - (dash) <p>Important This name must be properly formatted using standard IQN or EUI guidelines.</p> <p>The following examples show properly formatted iSCSI target names:</p> <ul style="list-style-type: none"> 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

Name	Description
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 authentication profile.
Create Authentication Profile link	Click this link to create a new authentication profile policy 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.

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 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 ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark), or = (equal sign).
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.

- 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 block 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 alphad-1.

Name	Description
From field	The first suffix number in the block.
Size field	The number of suffixes in the pool.

Step 9 Click **OK**.

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

What to Do Next

- (Optional) Add additional blocks of IQN suffixes to the IQN pool.
- Include the IQN suffix pool in a service profile and/or template.

Adding a Block to an IQN 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 desired IQN pool and select **Create a Block of IQN Suffixes**.

Step 6 In the **Create a Block of IQN Suffixes** dialog box, fill in the following fields:

Name	Description
Suffix field	The suffix for this block 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 pool.

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.

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** 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, except for iSCSI boot, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

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 2](#).

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 Disk Boot

If a server has a local drive, you can configure a boot policy to boot the server 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.

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, except for iSCSI boot, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

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

This procedure continues directly from [Creating a Boot Policy, on page 2](#).

Procedure

- Step 1** Click the down arrows to expand the **Local Devices** area.
- Step 2** Click **Add Local Disk** to add the device to the **Boot Order** table.
- 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.

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-ROM 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.

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, except for iSCSI boot, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

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 secondary 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 2.

Procedure

- Step 1** Click the down arrows to expand the **Local Devices** area.
- Step 2** Click one of the following links to add the device to the **Boot Order** table:
 - **Add CD-ROM**
 - **Add Floppy**
- 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.

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