Server Boot

Boot Policy

The Cisco UCS Manager enables you to create a boot policy for blade servers and rack servers.

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 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 to associate 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.

Note Changes to a boot policy might be propagated to all servers created with an updating service profile template that includes that boot policy. Re-association of the service profile with the server to rewrite the boot order information in the BIOS is automatically triggered.

You can also specify the following for the boot policy:

- Local LUN name. The name specified is the logical name in the storage profile, not the deployed name. Specify only a primary name. Specifying a secondary name results in a configuration error.
- Specific JBOD disk number for booting from JBOD disks.
- Any LUN for backward compatibility; however, we do not recommend this. Other devices must not have bootable images to ensure a successful boot.

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 except Cisco UCS C125 M5 Server. UEFI boot mode is supported only on M3 and higher servers, and allows you to enable UEFI secure boot mode. Cisco UCS C125 M5 Server supports only UEFI boot mode.

UEFI PXE boot is supported with all Cisco VIC adapters on Cisco UCS rack servers integrated with Cisco UCS Manager Release 2.2(4) and later releases. Beginning with Cisco UCS Manager Release 2.2(1), UEFI PXE boot is supported on all Cisco blade servers.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is not supported with the following combinations:
  - Gen-3 Emulex and QLogic adapters on Cisco UCS blade and rack servers integrated with Cisco UCS Manager.
  - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.
- If you want to use UEFI boot mode with two iSCSI LUNs, you must manually specify a common iSCSI initiator name in the service profile that is applied to both underlying iSCSI eNICs rather than allowing Cisco UCS Manager to select the name from an IQN suffix pool. If you do not supply a common name, Cisco UCS Manager will not be able to detect the second iSCSI LUN.
- 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.

You can create UEFI boot parameters in Cisco UCS Manager. UEFI Boot Parameters, on page 41 provides more information.

UEFI Secure Boot

Cisco UCS Manager supports UEFI secure boot on Cisco UCS B-Series M4 and higher Blade servers, Cisco UCS C-Series M3 and higher Rack servers, and Cisco UCS S-Series M4 Rack servers, and Cisco UCS C125 M5 Servers. Linux secure boot is supported on SLES 15, SLES 13 SP4, Red Hat Linux 7.6 operating systems starting with Release 4.0(4a). 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.
- UEFI boot mode is available only for drives.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.

Note UEFI boot mode is supported on Cisco UCS C-Series and S-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, then re-associate the server before downgrading. Otherwise, server discovery is not successful.
- In Cisco UCS Manager Release 4.0, UEFI secure boot is supported on the following Operating Systems:
  - In Cisco UCS Manager Release 4.0(1), UEFI secure boot is supported only on Windows 2016 and Windows 2012 R2.
  - In Cisco UCS Manager Release 4.0(2), UEFI secure boot is supported only on Windows 2016 and Windows 2019.
  - In Cisco UCS Manager Release 4.0(4), UEFI secure boot is supported on the following:

Table 1: Linux Operating Systems

Linux OS	eNIC/nENIC	fNIC
RHEL 7.5	3.2.210.18.738.12	1.6.0.50
RHEL 7.6	3.2.210.18.738.12	2.0.0.37
CentOS 7.5	3.2.210.18.738.12	1.6.0.50
CentOS 7.6	3.2.210.18.738.12	1.6.0.50
SLES 12.4	3.2.210.18.738.12	2.0.0.32
SLES 15	3.2.210.18.738.12	2.0.0.39-71.0
ESXi	Inbox works	Inbox works

Note

- For ESXi, inbox drivers are signed and work as such. Async drivers are not signed and do not work.
- Oracle OS does not support IPv6.
- XEN OS does not support IPv6.

Table 2: Windows Operating Systems

Windows OS	neNIC	nfNIC
Windows 2016	5.3.25.4	3.2.0.3
Windows 2019	5.3.25.4	3.2.0.3

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 M3M4, M5, and M6 rack servers.

Note CIMC secure boot is enabled by default on the Cisco UCS C220 M4/M5, C240 M4/M5, C480 M5/C480 M5 ML, rack servers, and is automatically enabled on the Cisco UCS C460 M4 rack server after upgrading to CIMC firmware release 2.2(3) or higher.

- After CIMC secure boot is enabled, you cannot disable it.
- 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

Step 1 In the **Navigation** pane, click **Equipment**.

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 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 was enabled, and the operation is in process.
- **Enabled**—CIMC secure boot is enabled on the server.

Enabling CIMC Secure Boot on a Rack Server

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

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 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 supported or is already enabled, this action is greyed.

Step 6 Click **Yes** in the **Enable Secure Boot** confirmation dialog box.

Note After enabled, you cannot disable CIMC secure boot.

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends 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 **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

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

Step 4 Right-click **Boot Policies** and select **Create Boot Policy**.

The **Create Boot Policy** wizard displays.

Step 5 Enter a unique name and description for the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 (Optional) After you make changes to the boot order, check the **Reboot on Boot Order Change** check box to reboot all servers that use this boot policy.

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.

Note Cisco UCS C125 M5 Server supports only UEFI boot mode.

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 35.
- SAN boot—To boot from an operating system image on the SAN, continue with Configuring a SAN Boot for a Boot Policy, on page 7.

  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 33.
- iSCSI boot—To boot from an iSCSI LUN, continue with Creating an iSCSI Boot Policy, on page 18.

What to do next

Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the 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.

Cisco recommends using 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 same operating system image. Therefore, the new server appears as the 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 and 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, Cisco recommends 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 6.

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, Cisco recommends that you first remove all local disks and other SAN LUNs from the boot policy in the server service profile.

This does not apply to the UCS Mini Series.

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**.

You can specify a **Primary** or a **Secondary** SAN boot. If the primary boot fails, the server attempts to boot from the secondary. The **Any** option is for unsupported adapters that connect directly to the SAN storage device and bypasses UCS Manager. Do not use the **Any** option with SAN boot for a supported set of adaptors which are managed by UCSM. For unsupported adaptors, use the instructions from the vendor to configure the adaptor for booting.

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 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 VIC-1340 Virtual Interface Card
- Cisco UCS VIC 1455
- Cisco UCS VIC 1457
- 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 on Cisco UCS rack servers

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 10.

For a high-level procedure for implementing iSCSI boot, see Configuring iSCSI Boot, on page 13.

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.

Note Previously, the host could 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 sees both of the boot paths. So for multipath configurations, a single IQN must be configured on both the boot vNICs. If there are different IQNs configured on the boot vNICs on a host, the host boots 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. Some OSs requires a NIC

driver 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 are 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, include the boot policy in the appropriate service profile.
- The operating system (OS) must be iSCSI Boot Firmware Table (iBFT) compatible.
  - For RHEL 7.x, the kernel parameter "rd.iscsi.ibft=1" is required before the installation. If the parameter is not entered, the iSCSI boot may fail.
  - For SLES 12.x, the following guidelines must be followed:
    - Hit "e" on the install disk before loading the kernel, edit the linuxefi (if using EFI) or kernel (if using legacy), and add the kernel parameter “rd.iscsi.ibft=1 rd.iscsi.firmware=1 rd.neednet=1”. If the parameter is not entered, the iSCSI boot may fail.
    - On an existing system that uses iSCSI, ensure that the /etc/iscsi/iscsid.conf has node.startup=automatic (not manual). Add this parameter to the /etc/default/grub/ and then run grub2-mkconfig -o /boot/grub2/grub.cfg to rebuild grub config.
- 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, re-enable 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 is 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:

  For 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 must be configured in /etc/dhcpd.conf.
  - After the server is 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.

Note 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

You can enable (MPIO) to optimize connectivity with storage arrays.

Note If you change the networking hardware, Windows might 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 the Microsoft Multipath I/O (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 19.

Step 2 Using the primary iSCSI vNIC, install the Windows operating system on the iSCSI target LUN.

Step 3 After Windows installation completes, 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 18.

Configuring iSCSI Boot

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

Procedure

	Command or Action	Purpose
Step 1	(Optional) Configure the iSCSI boot adapter policy.	For more information, see Creating an iSCSI Boot Policy, on page 18
Step 2	(Optional) Configure the authentication profiles for the initiator and target.	For more information, see Creating an iSCSI Authentication Profile, on page 16
Step 3	(Optional) 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.	For more information, see Creating an iSCSI Initiator IP Pool, on page 17
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, Cisco recommends 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 18.
Step 5	If you created a boot policy that can be used in any service profile, 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 19
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.
Step 8	Verify the iSCSI boot operation.	For more information, see *Verifying iSCSI Boot*.
Step 9	Before installing the OS, ensure that the OS is iSCSI Boot Firmware Table (iBFT) compatible.	If the correct parameter is not entered, the iSCSI boot operation may fail.

	Command or Action	Purpose
	• For RHEL 7.x, the kernel parameter "rd.iscsi.ibft=1" is required before installing the OS. • For SLES 12.x, hit "e" on the install disk before loading the kernel, edit the linuxefi (if using EFI) or kernel (if using legacy), and add the kernel parameter “rd.iscsi.ibft=1 rd.iscsi.firmware=1 rd.neednet=1”.	
Step 10	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 11	Boot the server.	

Creating an iSCSI Adapter Policy

Procedure

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

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

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

Step 4 Right-click **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 is saved.

Name	Description
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).
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**.

What to do next

Include the adapter policy in a service profile and template.

Deleting an iSCSI Adapter Policy

Procedure

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

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

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

Step 4 Expand the **Adapter Policies** node.

Step 5 Right-click the adapter policy and choose **Delete.**

Step 6 If a confirmation dialog box displays, 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 **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

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

Step 4 Right-click **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 is saved.
User Id field	The user Id associated with this profile. Enter between 1 and 128 characters, spaces, or special characters.

Name	Description
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 template.

Deleting an iSCSI Authentication Profile

Procedure

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

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

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

Step 4 Expand the **iSCSI Authentication Profiles** node.

Step 5 Right-click the IP pool you want to delete and choose **Delete**.

Step 6 If a confirmation dialog box displays, 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 were assigned as static IP addresses for a server or service profile.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multi tenancy, 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.
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 **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

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

Step 4 Right-click **Boot Policies** and 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 is 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 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 **Servers**.

Step 2 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 is 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, 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 might 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 the *Creating a MAC Pool* section in *Cisco UCS Manager Network Management Guide, Release 3.2*.

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 Setting the Initiator IQN at the Service Profile Level, on page 21.

Deleting an iSCSI vNIC from a Service Profile

Procedure

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

Step 2 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 a confirmation dialog box displays, click **Yes**.

Setting the Initiator IQN at the Service Profile Level

Procedure

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

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the desired node for the organization.

Step 4 Click the service profile with 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 a confirmation dialog box displays, click **Yes**.

Changing the Initiator IQN at the Service Profile Level

Procedure

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

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the desired node for the organization.

Step 4 Click the service profile with 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.

Procedure

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

Step 2 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.
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** 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. 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 22.
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.

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 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 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) **Important** This 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.
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 **Servers**.

Step 2 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 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** 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. 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 22.
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.
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:

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. 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.
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 **SAN**.

Step 2 Expand **SAN** > **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multi tenancy, 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:

Field	Description
Name	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 is saved.
Description	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).

Field	Description
Prefix	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**.

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

What to do next

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

Adding a Block to an IQN Pool

Procedure

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand **SAN** > **Pools**.

Step 3 Expand the node for the organization containing the pool.

If the system does not include multi tenancy, 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 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 were 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 **SAN**.

Step 2 Expand **SAN** > **Pools**.

Step 3 Expand the node for the organization containing the pool.

If the system does not include multi tenancy, 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 were 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 **SAN**.

Step 2 Expand **SAN** > **Pools**.

Step 3 Expand the node for the organization containing the pool.

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

Step 4 Expand the **IQN Pools** node.

Step 5 Right-click the pool that you want to delete and select **Delete**.

Step 6 If a confirmation dialog box displays, 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, Cisco recommends 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 can add a local disk or virtual media boot as a secondary boot device.

This procedure continues directly from Creating a Boot Policy, on page 6.

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 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.

Note For Cisco UCS M3 and higher blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices.

Note When there are more than one boot options provided under same Controller, the boot options is considered as follows instead of the boot order set in Cisco UCS Manager:

- When OS is installed or booted, for UEFI Boot, the installed OS will push its boot option to zero priority (Top Priority) irrespective of the set boot options in Cisco UCS Manager.
- The boot order will be based on the Boot Device enumeration set by BIOS and on how controller exposes the device to host (or as provided in Cisco UCS Manager).

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—Enables boot from local disk or local LUN.
- Local JBOD—Enables boot from a bootable JBOD.
- SD card—Enables boot from SD card.
- Internal USB—Enables boot for internal USB.
- External USB—Enables boot from external USB.
- Embedded Local LUN—Enables boot from the embedded local LUN on all Cisco UCS M4, M5 servers.

- Embedded Local Disk—Enables boot from the embedded local disk on all Cisco UCS M4, M5 servers.

Note For Cisco UCS C125 M5 Servers, if there is no separate PCIe storage controller, then do not use this option. Instead, use **Add Local Disk** option.

Note Second-level devices are only available for Cisco UCS M3 M3 and higher blade and rack servers using enhanced boot order.

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.

Note Second-level devices are only available for Cisco UCS M3 and higher blade and rack servers using enhanced boot order.

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.

NVMe Boot

Beginning with release 3.2(1) Cisco UCS Manager provides the option of adding an NVMe device to the Boot policy for M5 blade and rack servers. BIOS enumerates the NVMe devices present and boots to the first NVMe device having UEFI capable OS installed on it.

Cisco Boot Optimized M.2 RAID Controller

Beginning with 4.0(4a), Cisco UCS Manager supports Cisco boot optimized M.2 RAID controller based off Marvell 88SE92xx PCIe to SATA 6Gb/s controller (UCS-M2-HWRAID). BIOS enumerates the M.2 SATA drives installed on this controller followed by the front panel SATA drives to boot from the first SATA device having UEFI capable OS installed on it

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, Cisco recommends 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 6.

Procedure

Step 1 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 Local JBOD**
  - **Add SD Card**
  - **Add Internal USB**
  - **Add External USB**
  - **Add Embedded Local LUN**
  - **Add Embedded Local Disk**

Important In a setup with the Cisco Boot Optimized M.2 RAID Controller (UCS-M2-HWRAID), in the **Add Embedded Local Disk** dialog box, select **Any** to add the disk. Do not select **Primary** or **Secondary**.

Note For Cisco UCS M3 and higher blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices.

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 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, Cisco recommends 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, Cisco recommends 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 6.

Procedure

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** (For KVM CD/DVD in rack servers)

    In a setup with M5 blade servers, if an ISO is mapped to the KVM console, use only **Add Remote CD/DVD** in **Boot Order**.
- **Add Floppy** or
  - **Add Local Floppy**
  - **Add Remote Floppy**
- **Add Remote Virtual Drive**

Note For Cisco UCS M3 and higher blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices.

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 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 NVMe 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, Cisco recommends 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 6.

Procedure

Step 1 Click the down arrows to expand the **Local Devices** area.

Step 2 Click **Add NVMe** to add the device to the Boot Order table.

Note NVMe boot policy is available only with **Uefi** boot mode, with or without boot security.

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 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.

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 **Servers**.

Step 2 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 multi tenancy, expand the **root** node.

Step 4 Right-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.

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

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-XXXX-XXXXXXXXXXXX	Uses the UUID that you manually assign. Continue with Step 7.
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 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 want to create a pool that all service profiles can access, continue with Step 4. Otherwise, continue with Step 8.

Step 7 (Optional) If you selected the **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** option, do the following:

a) In the **UUID** field, enter the valid UUID that you want to assign to the server that uses this service profile.

Step 8 (Optional) If you want to create a new UUID Suffix pool 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.
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 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 **Servers**.

Step 2 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 a confirmation dialog box displays, 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

- You can configure UEFI boot parameters only if the boot mode is UEFI.
- When you upgrade Cisco UCS Manager to Release 2.2(4) and higher 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.
- You can specify UEFI boot parameters for the following device types:
  - SAN LUN
  - ISCSI LUN
  - Local LUN
- UEFI boot parameters are specific to each operating system. You can specify UEFI boot parameters 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**.

Procedure

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

Step 2 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 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.

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

Field	Description
Boot Loader Name	Specifies the name of the boot loader. This is a mandatory field. Example—grub.efi
Boot Loader Path	Specifies the path where the boot loader is located. This is a mandatory field. The name of the boot loader must not be included in this field. Only the path must be specified. Example—\EFI\RedHat
Boot Loader Description	Describes the boot loader. This is the human readable name that appears in the F6 boot menu.

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 **Servers**.

Step 2 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 with 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:

Field	Description
Boot Loader Name	Specifies the name of the boot loader. This is a mandatory field.

Field	Description
Boot Loader Path	Specifies the path where the boot loader is located. This is a mandatory field.
Boot Loader Description	Describes the boot loader.

Step 7 Click **OK**

Step 8 Click **Save Changes**.