Configuring Cisco UCS Server Pools and Policies

This chapter contains the following sections:

UUID Pools

A UUID pool is a collection of SMBIOS (Systems Management Built In Operating System) UUIDs (Universally Unique Identifiers) that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable. A UUID pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

Creating a UUID Pool

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **UUID Pools**.

Step 8 Click **Add**.

Step 9 On the **Add UUID Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.

Name	Description
Description field	A description for the pool.
Prefix drop-down list	Choose how the prefix is created. This can be one of the following: • **Derived**—The system creates the prefix. • **Other**—You specify the desired prefix. If you select this option, a text field displays where you can enter the desired prefix, in the format XXXXXXXX-XXXX-XXXX.
From field	The first UUID address in the block.
Size field	The number of UUID addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 Click **Submit**.

Adding an Address Block to a UUID Pool

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.
Step 5 Click **Organizations**.
Step 6 Click the organization in which you want to modify the pool and then click **View Details**.
Step 7 Click **UUID Pools**.
Step 8 Click the pool to which you want to add a block of addresses and then click **Add UUID Addresses Block**.
Step 9 On the **Add UUID Pool Block** screen, complete the following fields:

Name	Description
From field	The first UUID address in the block.
Size field	The number of UUID addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy

Step 10 Click **Submit**.

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multitenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

Creating a Server Pool

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **Server Pools**.

Step 8 Click **Add**.

Step 9 On the **Add Server Pool** screen, add a name and description for the pool.

Step 10 (Optional) In the **Servers** field, do the following to add servers to the pool:

a) Click **Select**.

b) On the **Select Items** page, check the check boxes for the servers that you want to add to the pool.

c) Click **Select**.

Step 11 Click **Add**.

Server Pool Qualification Policy

The Server Pool Qualification policy qualifies servers based on the servers available in the system. You can use this policy to qualify servers according to

- Server-related criteria such as model or type, product family, or chassis location
- Domain-related criteria such as domain group or domain name
- Processor-related criteria such as CPU cores, type, and configuration
- Storage configuration and capacity

- Memory type and configuration
- Other criteria such as adapter type, owner, site, or IP address

Based on the criteria added in the Server Pool Qualification policy, the servers qualified can then be used in the create server pool operation.

Creating a Server Pool Qualification Policy

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Server Pool Qualification Policy**.

Step 8 Click **Add**.

Step 9 On the **Create Server Pool Qualification Policy** screen, type a name for the policy, an optional description, and an optional Server Model/PID. Click **Next**.

Step 10 In the **Domain** screen, click the plus (+) sign to optionally add the domain qualifier.
The **Add Entry to Domain Qualifier** screen appears. You can qualify servers based on the following criteria:

- Owner - The owner of the servers.
- Site - The site that the servers belong to.
- IP Address Range - The IP address range of the servers.
- Blade Servers - The chassis IDs and slot IDs of the servers.
- Rack Servers - The rack IDs of the servers.
- Domain Group - The domain groups that the servers belong to.
- Domain Name - The domains that the servers belong to.
- Product Family - The product family of the servers.

Step 11 In the **Add Entry to Domain Qualifier** screen, type a name for the qualifier in the **Name** box. Check the criteria you want to add. Then click the plus (+) sign to add the criteria. After adding the domain qualification option, click **Next**.

Step 12 In the **Hardware - Processors** screen, check the **Processor** box to optionally add processor-related criteria. Then click **Next**.

Step 13 In the **Hardware - Memory** screen, check the **Memory** box to optionally add memory-related criteria. Then click **Next**.

Step 14 In the **Hardware - Storage** screen, check the **Storage** box to optionally add storage-related criteria. Then click **Next**.

Step 15 In the **Hardware - Adapter** screen, check the **Adapter** box to optionally add the adapter type, number of adapters, and Model/PID.

Step 16 After adding all the criteria, click **Submit**.

Editing or Deleting a Server Pool Qualification Policy

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to modify or delete a server qualification policy and then click **View Details**.

Step 7 Click **Server Pool Qualification Policy**.

Step 8 To delete a server pool qualification policy, choose the policy and click **Delete**. A confirmation message appears. Click **Delete** again.

Step 9 To modify an existing server pool qualification policy, choose the policy and click **Edit**.
The **Edit Server Pool Qualification Policy** dialog box appears. It contains the following screens:

- Create Server Pool Policy Qualification Name
- Domain
- Hardware - Processors
- Hardware - Memory
- Hardware - Storage
- Hardware - Adapter

Step 10 After modifying existing qualification options or adding new options, click **Submit**.

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.

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.

Creating a SAN Boot Policy

Tip We recommend that the boot order, in a boot policy, include either a local disk or a SAN LUN, but not both. It helps 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 boots from the local disk rather than the SAN LUN.

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

Before you begin

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.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Organization drop-down list	Is selected by default and not available to change.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If this check box is checked 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.

Name	Description
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If this check box is not checked, the policy 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.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.
Boot Security check box	(*Displays only when* **UEFI** *is selected as the boot mode*.) Enables the secure boot option for the servers that use this boot policy.

Step 10 In the **vHBAs** area, check **Add SAN Boot** and complete the following fields:

Name	Description
Add Primary SAN Boot check box	If checked, primary SAN boot is added to the boot order.
Primary vHBA field	Enter the name of the vHBA that you want to use as the first address defined for the SAN boot location. This field is dispalyed only when the **Add Primary SAN Boot** check box is checked.
Add SAN Boot Target for Primary vHBA check box	If checked, SAN boot is added for primary vHBA. This field is dispalyed only when the **Add Primary SAN Boot** check box is checked.
Add Secondary SAN Boot check box	If checked, secondary SAN boot is added to the boot order.
Secondary vHBA field	Enter the name of the vHBA that you want to use as the second address defined for the SAN boot location. This field is dispalyed only when the **Add Secondary SAN Boot** check box is checked.
Add SAN Boot Target for Secondary vHBA check box	If checked, SAN boot is added for secondary vHBA. This field is dispalyed only when the **Add Secondary SAN Boot** check box is checked.

Name	Description
Primary Boot Target LUN field	The LUN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.
Primary Boot Target WWPN field	The WWPN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.
Secondary Boot Target LUN field	The LUN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.
Secondary Boot Target WWPN field	The WWPN that corresponds to the location of the boot image. This field is dispalyed for Primary vHBA or Secondary vHBA only when the **Add SAN Boot Target for Primary vHBA** or **Add SAN Boot Target for Secondary vHBA** check box is checked.

Step 11 Click **Submit**.

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.

Creating a LAN Boot Policy

The order in which boot devices are invoked within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If checked 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.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy 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. If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.
Boot Security check box	(*Displays only when* **UEFI** *is selected as the boot mode*.) Enables the secure boot option for the servers that use this boot policy.

Step 10 In the **vNICs** area, check **Add LAN Boot** and enter the additional parameters, including the following:

Name	Description
Primary vNIC field	Enter the name of the vNIC that you want to use as the first address defined for the LAN boot location. This option is displayed when you check the **Add LAN Boot** check box.
Add Secondary vNIC check box	Adds secondary vNIC to the boot order.
Secondary vNIC field	Enter the name of the vNIC that you want to use as the second address defined for the LAN boot location. This option is displayed when you check the **Add Secondary vNIC** check box.

Step 11 Click **Submit**.

Local Device Boot

If a server has a local drive, you can configure a boot policy to boot the server from that device or from any of the following local devices:

- Local hard disk drive
- Local JBOD
- Local LUN
- SD Card
- Internal USB
- External USB
- Embedded Local LUN
- Embedded Local Disk

Creating a Local Device Boot Policy

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.

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.
Step 5 Click **Organizations**.
Step 6 Click the organization in which you want to create the policy and then click **View Details**.
Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If checked 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.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy 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.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.
Boot Security check box	(*Displays only when* **UEFI** *is selected as the boot mode*.) Enables the secure boot option for the servers that use this boot policy.

Step 10 In the **Local Devices** area, choose from the following options:

Name	Description
Add Local Disk check box	Adds local disk to the boot policy. If you choose this option, add local LUN, add local JBOD, add SD card, add internal USB, add external USB, add embedded local LUN, and add embedded local disk options are not available. If you select the **Add Local Disk** check box, then you cannot select any of the secondary devices. If you select any of these local devices, then you cannot select the parent option of adding a local disk.

Name	Description
Add Local LUN check box	Adds any local LUN to the boot order. If you choose this option, add local disk option is not available.
Add Primary Local LUN check box	Adds primary local LUN to the boot order. This option is displayed when you check the **Add Local LUN** check box.
Primary Local LUN Name field	Enter the name of the local LUN that you want to use as primary. This option is displayed when you check the **Add Primary Local LUN** check box.
Add Secondary Local LUN check box	Adds secondary local LUN to the boot order. This option is displayed when you check the **Add Local LUN** check box.
Secondary Local LUN Name field	Enter the name of the local LUN that you want to use as secondary. This option is displayed when you check the **Add Secondary Local LUN** check box.
Add Local JBOD check box	Adds local JBOD to the boot order.
Primary JBOD Disk Slot Number field	Enter the slot number of the JBOD disk that you want to use as primary. This option is displayed when you check the **Add Local JBOD** check box.
Add SD Card check box	Adds SD Card to the boot order. If you choose this option, Add Local Disk, and Add Local LUN options are not available.
Add Internal USB check box	Adds Internal USB to the boot order. If you choose this option, Add Local Disk, and Add Local LUN options are not available.
Add External USB check box	Adds External USB to the boot order. If you choose this option, Add Local Disk, and Add Local LUN options are not available.
Add Embedded Local LUN check box	Adds Embedded Local LUN to the boot order.
Add Embedded Local Disk check box	Adds Embedded Local disk to the boot order.

Name	Description
Primary Embedded Local Disk Slot Number field	Enter the slot number of the embedded local disk that you want to use as primary. This option is displayed when you check the **Add Embedded Local Disk** check box.
Secondary Embedded Local Disk Slot Number field	Enter the slot number of the embedded local disk that you want to use as primary. This option is displayed when you check the **Add Embedded Local Disk** check box.
Add CD/DVD ROM Boot check box	Adds CD/DVD ROM to the boot policy. If you choose this option, Add Local CD/DVD, and Add Remote CD/DVD options are not available.
Add Local CD/DVD check box	Adds Local CD/DVD to the boot order.
Add Remote CD/DVD check box	Adds Remote CD/DVD to the boot policy.
Add Floppy Disk check box	Adds floppy disk to the boot policy. If you choose this option, Add Local Floppy Disk, and Add Remote Floppy Disk options are not available.
Add Local Floppy Disk check box	Adds local floppy disk to the boot order.
Add Remote Floppy Disk check box	Adds remote floppy disk to the boot order.
Add Remote Virtual Drive check box	Adds remote virtual drive to the boot policy.

Step 11 Click **Submit**.

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.

Creating a Virtual Media Boot Policy

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.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 In the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If this check box is checked 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.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy uses the vNICs, vHBAs, or iSCSI vNICs (as appropriate for the boot option) if they exist, otherwise vNICs, vHBAs, or iSCSI vNICs with the lowest PCIe bus scan order is used.

Step 10 In the **CIMC Mounted vMedia** area, check one or both of the following options to select the vMedia device to add to the boot policy:

- **Add CIMC Mounted CD/DVD**
- **Add CIMC Mounted HDD**

Step 11 Click **Submit**.

Creating a vMedia Policy and vMounts

vMedia enables dynamic mapping of an external image file to the server's CIMC. If a vMedia file is mapped as a CDD, then the image file presents itself as a CD-ROM image. vMedia can be referenced as a device in a Boot Policy, from which a server attempts to boot.

vMedia policies are bound to Service Profiles (SPs). Any given SP can have only one vMedia policy active at any given time. However, the policy can include one or more vMedia Mount.

Note Changing the vMedia Policy for a service profile does **not** cause service profile reconfiguration, reboot, or service interruption.

Before you begin

Make sure that you have the required minimum version of Cisco UCS Manager, the BIOS, and CIMC. See Cisco UCS Director Compatibility Matrix.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 3 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 4 Click **Organizations**.

Step 5 Choose the organization that you want to update and click **View Details**.

Step 6 Click **vMedia Policy**.

Step 7 Click **Add**.

Step 8 On the **Add vMedia Policy** screen, enter a name and description for the policy.

Step 9 From the **Retry on Mount Failure** drop-down list, choose one of the following to determine whether the vMedia will continue to mount even after a mount failure occurs:

- **Yes**—If you choose this option, the remote server continues to try mounting the vMedia until the operation is successful or until you disable this option.
- **No**—If you choose this option, the remote server does not try to mount the vMedia again if there is a mount failure.

Step 10 Expand **vMedia Mount Points**, and check the vMedia Mount you want to use.

You can create a new vMedia mount point entry using the following steps:

a) Click **Add**.

b) On the **Add Entry to vMedia Mount Points** screen, complete the required fields, including the following:

1. **Device Type**—Choose one of the following options: HDD, or CDD. For each vMedia Policy, you can create a maximum of two vMedia mounts, one for each device type.
2. **Mount Name**—Enter a unique name for the vMedia mount.
3. **Description**—Enter a description of the vMedia mount. You can enter up to 510 characters.
4. **Protocol**—Choose the network access protocol to use when communicating with the mounted remote server. Supported protocols are: HTTPS, HTTP, CIFS, or NFS. After you choose the protocol type, enter the additional parameters for that protocol type.
   - If you chose **HTTPS** protocol, enter the **User Name** and **Password** to log in to the remote server.
   - If you chose **HTTP** protocol, enter the **User Name** and **Password** to log in to the remote server.
   - If you chose **CIFS** protocol, choose an **Authentication protocol** to use when communicating with the mounted remote server. If you do not choose an authentication protocol, it is set to Default.

     (Optional): Enter a **User Name** and **Password** to log in to the remote server.
   - If you chose **NFS** protocol, no additional parameters are required.

5. **Remote Server Host Name/IP Address**—Enter the hostname or IP address of the location where the backup file is going to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.

   Note If you use a hostname, configure the Cisco UCS Domain to use a DNS server. The DNS name can be used when an inband network is configured for that server.

6. **Absolute Remote Path**—Enter the full path to the remote vMedia file.

   Note If the selected protocol is CIFS, then use forward slashes in the path.

7. **Generate File Name from Service Profile Name**—Choose one of the following options:
   - **None**—If you choose this option, enter a **Remote File Name** that the vMedia policy must use.
   - **Service-Profile-Name**—If you choose this option, the service profile name is used as the image name.

c) Click **Submit**.

Step 11 Click **Submit**.

Creating a iSCSI Boot Policy

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

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 a 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 it 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.

For multipath configurations, a single iSCSI Qualified Name (IQN) is configured on both the boot vNICs. If there are different IQNs configured on the boot vNICs on a host, the host will boot with the IQN that is configured on the boot vNIC with the lower PCI order.

Before you begin

- Verify that the storage array is licensed for iSCSI boot and the array side LUN masking must be properly configured.
- Determine two IP addresses, one for each iSCSI initiator. The IP addresses must be on the same subnet as the storage array. The IP addresses are assigned statically or dynamically using the Dynamic Host Configuration Protocol (DHCP).
- Verify that the operating system (OS) is iSCSI Boot Firmware Table (iBFT) compatible.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **Boot Policies**.

Step 8 Click **Add**.

Step 9 On the **Add Boot Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Organization drop-down list	Is selected by default and not available to change.
Reboot on Order Change check box	If checked, reboots all servers that use this boot policy after you change the boot order. If not checked 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.
Enforce vNIC/vHBA Name check box	If checked, a configuration error is displayed if one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table matches the server configuration in the service profile. If not checked, the policy 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.
Boot Mode drop-down list	The boot mode for the servers that use this boot policy. It can be one of the following: • **Legacy** • **UEFI** With this option, you can specify second-level boot devices and you can enable the secure boot option.
Boot Security check box	(*Displays only when* **UEFI** *is selected as the boot mode*.) Enables the secure boot option for the servers that use this boot policy.

Step 10 In the **iSCSI vNICs** area, check **Add iSCSI Boot** and enter the additional parameters, including the following:

Name	Description
Primary iSCSI vNIC field	Enter the name of the iSCSI vNIC that you want to use as the first address defined for the boot location. This option is displayed when you check the **Add iSCSI Boot** check box.
Add Secondary iSCSI vNIC check box	Adds secondary iSCSI vNIC to the boot order.
Secondary iSCSI vNIC field	Enter the name of the iSCSI vNIC that you want to use as the second address defined for the boot location. This option is displayed when you check the **Add Secondary iSCSI vNIC** check box.

Step 11 Click **Submit**.