Configuring Cisco UCS Server Pools and Policies

This chapter contains the following sections:

- Global Equipment Policies, page 1
- UUID Pools, page 4
- Server Pools, page 5
- Management IP Pool, page 7
- Boot Policy, page 8
- Local Disk Configuration Policy, page 45
- Maintenance Policy, page 50
- Server Pool Policy Qualification Overview, page 52
- Server Pool Policy Overview, page 56
- vNIC/vHBA Placement Policies, page 57
- Placement Policy, page 62

Global Equipment Policies

Chassis/FEX Discovery Policy

The chassis/FEX discovery policy determines how the system reacts when you add a new chassis or FEX. Cisco UCS uses the settings in the chassis/FEX discovery policy to determine:

- the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect
- whether to group links from the IOM to the fabric interconnect in a fabric port channel

For more information about chassis links, including an overview of how the chassis/FEX discovery policy works in a multichassis Cisco UCS domain, see the Cisco UCS Manager configuration guides.

Configuring the Chassis/FEX Discovery Policy

You can configure a chassis policy to specify how the system reacts when a new chassis is added.

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Equipment Global Policies** tab.

Step 4 Check the **Chassis/FEX Discovery Policy** check box.

Step 5 From the **Action** drop-down list, choose the minimum threshold for the number of links between the chassis or Fabric Extender (FEX) and the fabric interconnect:

- **1-link**
- **2-link**
- **4-link**
- **8-link**

Step 6 From the **Link Grouping Preference** drop-down list, choose whether the links from the IOMs or FEXes to the fabric interconnects are grouped in a port channel.

Note The link grouping preference takes effect only if both sides of the links between an IOM or FEX and the fabric interconnect support fabric port channels. If one side of the links does not support fabric port channels, this preference is ignored and the links are not grouped in a port channel.

Step 7 Click **Save**.

Rack Server Discovery Policy

The rack server discovery policy determines how the system reacts when you add a new rack-mount server. Cisco UCS uses the settings in the rack server discovery policy to determine whether any data on the hard disks are scrubbed and whether server discovery occurs immediately or must wait for explicit user acknowledgment.

Cisco UCS cannot discover any rack-mount server that has not been correctly cabled and connected to the fabric interconnects. For information about how to integrate a supported Cisco UCS rack-mount server, see the appropriate rack-mount server integration guide.

Configuring the Rack Server Discovery Policy

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Equipment Global Policies** tab.

Step 4 Check the **Rack Server Discovery Policy** check box.

Step 5 From the **Action** drop-list, choose what happens when you add a new rack server:

- **Immediate—**The new server is discovered automatically.
- **User-acknowledged—**Nothing happens until you acknowledge the new server.

Step 6 From the **Scrub Policy** drop-down list, choose the scrub policy to run on a newly discovered server if that server meets the criteria in the server pool policy qualification.

Step 7 Click **Save**.

Rack Management Connection Policy

The rack management connection policy determines whether a newly added rack-mount server is automatically managed by Cisco UCS or whether it must wait for explicit user acknowledgment. We recommend that you configure this policy for auto-acknowledgment.

Configuring the Rack Management Connection Policy

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Equipment Global Policies** tab.

Step 4 Check the **Rack Management Connection Policy** check box.

Step 5 From the **Action** drop-down list, choose one of the following:

- **auto-acknowledged—**Acknowledgment happens automatically.
- **user-acknowledged—**Nothing happens until you acknowledge the server.

Step 6 Click **Save**.

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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click the **UUID Pools** tab.

Step 6 Click **Add**.

Step 7 In the **Add UUID Pool** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the pool.
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.

Step 8 Click **Submit**.

Adding an Address Block to a UUID Pool

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to modify the pool and then click **View Details**.

Step 5 Click the **UUID Pools** tab.

Step 6 Click on the pool to which you want to add a block of addresses and then click **Add UUID Addresses Block**.

Step 7 In the **Add UUID Pool Block** dialog box, 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.

Step 8 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

Cisco UCS Director displays only the managed servers in a server pool, but the size of the pool includes all servers. For example, if a server pool contains two servers and only one server is managed by Cisco UCS

Director, all server pool reports and actions on that pool display only one (managed) server. However, the pool size is displayed as two.

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.
Step 3 In the right pane, click the **Organizations** tab.
Step 4 Click the organization in which you want to create the pool and then click **View Details**.
Step 5 Click the **Server Pools** tab.
Step 6 Click **Add**.
Step 7 In the **Add Server Pool** dialog box, add a name and description for the pool
Step 8 (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 9 Click **Add**.

Assigning a Server Pool to a Cisco UCS Director Group

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.
Step 3 In the right pane, click the **Organizations** tab.
Step 4 Click the organization that contains the pool you want to assign and then click **View Details**.
Step 5 Click the **Server Pools** tab.
Step 6 Click the row in the table for the pool that you want to assign to a Cisco UCS Director group.
Step 7 Click **Assign Group**.
Step 8 In the **Select Group** dialog box, do the following:
a) From the **Group** drop-down list, choose the Cisco UCS Director group to which you want to assign this server pool.
b) In the **Label** field, enter a label to identify this server pool.
c) Click **Submit**.

Unassigning a Server Pool from a Cisco UCS Director Group

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.
Step 3 In the right pane, click the **Organizations** tab.
Step 4 Click the organization that contains the pool you want to unassign and then click **View Details**.
Step 5 Click the **Server Pools** tab.
Step 6 Click the row in the table for the pool that you want to unassign from a Cisco UCS Director group.
Step 7 Click **Unassign Group**.
Step 8 Click **Unassign Group**.
Step 9 In the **Unassign Group** dialog box, click **Unassign**.

Management IP Pool

A management IP pool is a collection of external IP addresses. Each block of IP addresses in the management IP pool is reserved for external access that terminates in the CIMC (Cisco Integrated Management Controller) on a server.

All IP addresses in the management IP pool must be in the same subnet as the IP address of the fabric interconnect.

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

Adding an IP Address Block to the Management IP Pool

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

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.
Step 3 In the right pane, click the **Management IP Pool** tab.
Step 4 Click **Add**.
Step 5 In the **Create Block of IP Addresses** dialog box, complete the following fields:

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

Step 6 Click **Submit**.

Boot Policy

Important Cisco UCS Manager Release 3.1(2) and later releases do not support Cisco UCS M-Series Servers.

The Cisco UCS Manager enables you to create a boot policy for blade servers, rack servers, and modular 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. For modular servers, you can specify both a primary and secondary name. For other servers, specify only a primary name. Specifying a secondary name results in a configuration error.
- Specific JBOD disk number for booting from JBOD disks. This is not supported for the Modular servers.
- 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. UEFI boot mode is supported only on M3 and M4 servers, and allows you to enable UEFI secure boot mode.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is only supported on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers.
- UEFI boot mode is not supported with the following combinations:
  - Gen-3 Emulex and QLogic adapters on Cisco UCS blade and rack servers integrated with Cisco UCS Manager.
  - PXE boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.
  - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS Manager.
- 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.

UEFI Secure Boot

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

The following limitations apply to UEFI secure boot:

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

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

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

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, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server might boot from the local disk rather than the SAN LUN.

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

Before You Begin

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

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Boot Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Add Boot Policy** dialog box, 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.

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 8 In the **Add Boot Device** area, check the **Add SAN Boot** check box.

Step 9 In the **Primary vHBA** field, enter the name of the vHBA that you want to use as the first address defined for the SAN boot location.

Step 10 In the **Secondary vHBA** field, enter the name of the vHBA that you want to use as the second address defined for the SAN boot location.

Step 11 (Optional) If either or both of the primary and secondary vHBAs points to a bootable SAN image, check the appropriate **Add SAN Boot Target** check box or both check boxes and complete the following fields:

Name	Description
Primary Boot Target LUN field	The primary LUN ID number that corresponds to the location of the boot image.
Primary Boot Target WWPN field	The primary WWPN value that corresponds to the location of the boot image.
Secondary Boot Target LUN field	The secondary LUN ID number that corresponds to the location of the boot image.
Secondary Boot Target WWPN field	The secondary WWPN value that corresponds to the location of the boot image.

Step 12 In the **Add Boot Device** area, check the **Add iSCSI Boot** check box.

Step 13 In the **Add Primary iSCSI Vnic** field, enter the name of the iSCSI VNIC that you want to use as the first address defined for the SAN boot location.

Step 14 In the **Add Secondary iSCSI Vnic** field, enter the name of the iSCSI VNIC that you want to use as the second address defined for the SAN boot location.

Step 15 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

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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Boot Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Add Boot Policy** dialog box, 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.

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 8 In the **Add Boot Device** area, check the **Add LAN Boot** check box.

Step 9 In the **Primary vNIC** field, enter the name of the vNIC that you want to use as the first address defined for the LAN boot location.

Step 10 In the **Secondary vNIC** field, enter the name of the vNIC that you want to use as the second address defined for the LAN boot location.

Step 11 In the **Add Boot Device** area, check the **Add iSCSI Boot** check box.

Step 12 In the **Add Primary iSCSI Vnic** field, enter the name of the iSCSI VNIC that you want to use as the first address defined for the LAN boot location.

Step 13 In the **Add Secondary iSCSI Vnic** field, enter the name of the iSCSI VNIC that you want to use as the second address defined for the LAN boot location.

Step 14 Click **Submit**.

Local Disk 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

- SD card
- Internal USB
- External USB

Creating a Local Disk 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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Boot Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Add Boot Policy** dialog box, 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 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.

Name	Description
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	Enables the secure boot option for the servers that use this boot policy. This option is visible only when UEFI is selected as the boot mode.

Step 8 In the **Add Local Device** area, check the **Add Local Disk** check box.
There are more secondary options such as adding local LUN, SD card, internal and external USB devices as local boot devices. If you select the **Add Local Disk** check box, then you cannot select any of these secondary devices. If you select any of these local devices, then you cannot select the parent option of adding a local disk.

Step 9 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 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Boot Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Add Boot Policy** dialog box, 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 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.

Name	Description
Boot Security check box	Enables the secure boot option for the servers that use this boot policy. This option is visible only when UEFI is selected as the boot mode.

Step 8 In the **Add Boot Device** area, check one or both of the following check boxes:

- **Add CD ROM**
- **Add Floppy Disk**

There are more secondary options such as adding local or remote CD/DVD, or adding local or remote floppy disks. If you select the **Add CD ROM** or **Add Floppy Disk** check box, then you cannot select any of these secondary devices. If you select any of these secondary devices, then you cannot select the parent option of adding a CD ROM or floppy disk.

Step 9 Click **Submit**.

iSCSI Boot

iSCSI boot enables a server with a virtual interface card (VIC adapter) to boot its operating system from an iSCSI target machine located remotely over a network. Cisco UCS Director supports iSCSI boot with the following storage:

- EMC VNX
- NetApp ONTAP
- NetApp Data Fabric Manager (DFM)
- NetApp C-Mode

When you configure iSCSI boot in Cisco UCS Director, you first configure iSCSI boot for Cisco UCS and then configure the iSCSI boot workflow for Cisco UCS Director.

For more information about iSCSI boot within Cisco UCS, including guidelines for implementing it, see the Cisco UCS Manager configuration guides.

Prerequisites for iSCSI Boot

The following prerequisites must be met before you configure iSCSI boot:

- The Cisco UCS domain, including all firmware, must be at Cisco UCS, Release 2.0(1m) or later.
- The Cisco UCS servers must have a supported VIC adapter, such as the following:
  - Cisco UCS M81KR Virtual Interface Card

- Cisco UCS VIC-1240 Virtual Interface Card
- Cisco UCS VIC-1280 Virtual Interface Card

- The storage array must be licensed for iSCSI boot.
- The array side LUN masking and network interface must be properly configured with access to the VLAN that the iSCSI traffic uses.
- The appropriate aggregates and volumes must be created in the storage array.
- The uplink ports from the fabric interconnects must also have access to the iSCSI traffic VLAN.
- The server operating system (OS) must be iSCSI Boot Firmware Table (iBFT) compatible.

Configuring iSCSI Boot

Note This procedure provides a high-level overview of the steps required to configure iSCSI boot. Ensure that you complete all of the following steps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Create the required VLANs to carry iSCSI traffic.	See Creating a VLAN.
Step 2	Create one or more MAC pools for the servers within the appropriate organizations.	See Creating a MAC Pool.
Step 3	Create one or more vNIC templates within the appropriate organizations.	See Creating a vNIC Template.
Step 4	Create a vNIC for fabric A and fabric B.	See Creating a vNIC.
Step 5	Create a network policy that includes those vNICs.	See Creating a Network Policy.
Step 6	Create a storage policy.	See Creating a Storage Policy.
Step 7	Create one or more IQN pools within the appropriate organizations.	See Creating an IQN Pool, on page 20.
Step 8	Create one or more IP address blocks for the iSCSI IP Pool.	See Adding a Block of Addresses to the iSCSI IP Pool, on page 22.
Step 9	Create an initiator and target iSCSI authentication profile.	See Creating an iSCSI Authentication Profile, on page 22.
Step 10	Create one or more iSCSI adapter policies.	See Creating an iSCSI Adapter Policy, on page 23.
Step 11	Create an iSCSI boot workflow and add the required tasks to that workflow.	The following example shows the workflow to create an iSCSI boot workflow for NetApp ONTAP storage: **1** Example: Creating an iSCSI Boot Workflow, on page 24

	Command or Action	Purpose
		2 Adding a Task: Create Service Profile, on page 26 **3** Adding a Task: Add vNIC to Service Profile, on page 28 **4** Adding a Task: Add iSCSI vNIC to Service Profile, on page 29 **5** Adding a Task: Create Service Profile iSCSI Boot Policy, on page 30 **6** Adding a Task: Associate Service Profile, on page 32 **7** Adding a Task: Create Flexible Volume, on page 33 **8** Adding a Task: Create LUN, on page 35 **9** Adding a Task: Create Initiator Group, on page 36 **10** Adding a Task: Add an Initiator to Initiator Group, on page 38 **11** Adding a Task: Map LUN to Initiator Group, on page 39 **12** Adding a Task: Set Up PXE Boot, on page 40 **13** Adding a Task: Power On UCS Server, on page 41 **14** Adding a Task: Monitor PXE Boot, on page 42 **15** Adding a Task: Power Off UCS Server, on page 43 **16** Adding a Task: Modify Service Profile Boot Policy to Boot from iSCSI, on page 44 **17** Add a second Power On UCS Server task.

Creating an IQN Pool

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.

Note Usually, the maximum IQN size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, limit the IQN size to 128 characters.

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click the **IQN Pools** tab.

Step 6 Click **Add**.

Step 7 In the **Define Name and Description** screen of the **Create IQN Pool** wizard, complete the following fields:

Name	Description
Name field	A unique name for the iSCSI Qualified Name (IQN) pool.
Description field	A user-defined description of the pool.
Prefix field	The prefix for any IQN blocks created for this pool.

Step 8 In the **Add IQN Blocks** screen of the **Create IQN Pool** wizard, do the following:

a) Click **Add**.

b) In the **Add Entry to IQN Pool Blocks** dialog box, complete the following fields:

Name	Description
Suffix field	The suffix for this block of IQNs.
From field	The first suffix number in the block.
Size field	The number of suffixes in the block.

c) Click **Submit**.

Repeat this step until you have added all desired IQN pool blocks.

Step 9 Click **Submit**.

Adding a Block of Addresses to the iSCSI IP Pool

The iSCSI IP pool is a group of IP addresses that is reserved for iSCSI boot. This IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **iSCSI IP Pool** tab.

Step 4 Click **Add**.

Step 5 In the **Create Block of IP Addresses** dialog box, complete the following fields:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the pool.
Subnet Mask field	The subnet mask associated with the IP addresses in the block.
Default Gateway field	The default gateway associated with the IP addresses in the block.
Primary DNS field	The primary DNS server that this block of IP addresses must access.
Secondary DNS field	The secondary DNS server that this block of IP addresses must access.

Step 6 Click **Submit**.

Creating an iSCSI Authentication Profile

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **iSCSI Auth Profiles** tab.

Step 6 Click **Add**.

Step 7 In the **iSCSI Authentication Profile** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the iSCSI authentication profile.

Name	Description
User ID field	The user ID associated with this profile.
Password field	The password associated with this profile.
Confirm Password field	The password again for confirmation purposes.

Step 8 Click **Submit**.

Creating an iSCSI Adapter Policy

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.
Step 3 In the right pane, click the **Organizations** tab.
Step 4 Click the organization in which you want to create the policy and then click **View Details**.
Step 5 Click the **iSCSI Adapter Policy** tab.
Step 6 Click **Add**.
Step 7 In the **iSCSI Adapter Policy** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Connection Timeout field	The number of seconds to wait until Cisco UCS assumes that the initial sign-in 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 if there is 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).

Name	Description
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). **Note** This option must 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 must be disabled until you have installed an operating system on the server.

Step 8 Click **Submit**.

Example: Creating an iSCSI Boot Workflow

This example shows how to create an iSCSI boot workflow for NetApp ONTAP. The steps for configuring the Cisco UCS components are the same for all types of storage.

Step 1 On the menu bar, choose **Policies** > **Orchestration**.

Step 2 Click the **Workflows** tab.

Step 3 Click **Add Workflow**.

Step 4 In the **Add Workflow Details** screen of the **Add Workflow** wizard, complete the following fields and then click **Next**.

Name	Description
Name field	A unique name for the workflow. We recommend that this name describe the purpose of the workflow.
Description field	A description for the workflow.
Workflow Context drop-down list	Choose the context in which the workflow is used. This can be one of the following: • **Any—**Allows the workflow to be used in any context. • **Selected VM—**Allows the workflow to be executed only when a VM is selected.

Name	Description
Save as Compound Task check box	If checked, the workflow is defined as a compound task.
Place in New Folder check box	The folder where you want to save the workflow. If you check this check box, enter a folder name in the **Folder Name** field.
Select Folder drop-down list	Choose the folder in which you want to save the workflow. This drop-down list is only visible if you do not check the **Place in New Folder** check box.

Step 5 In the **Add User Inputs** screen of the **Add Workflow** wizard, do the following:

a) Click **Add**.

b) In the **Add User Inputs** dialog box, complete the following fields and then click **Submit**:
If you configure the workflow with the required user inputs, you can configure workflow tasks to prompt for certain values when the workflow is run.

Name	Description
Input Label field	The label assigned to the input.
Input Description field	A description for the input.
Input Type field	The type of input category.
Admin Input field	Input from the administrator based on the input type. The inputs are not required to be provided by the end user who executes the workflow. You can also prevent an end user from providing certain types.
Admin Input List field	The current administrator's list of inputs. The input order can be rearranged.
Admin Input Filter field	The administrator's input filter value used to define custom inputs based on a filter (static or dynamic). For example, you can filter on aggregate, volumes, and POD

Repeat this step if you want to add more user inputs.

Step 6 Click **Submit**.
If you created the workflow in a new folder, you might need to click **Refresh** to see that folder in the folder list.

What to Do Next

Add tasks to the empty workflow.

Adding a Task: Create Service Profile

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Create UCS Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Create UCS Service Profile)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Create UCS Service Profile)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the service profile when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile Name**
- **Description**
- **Organization**
- **Storage Policy**
- **Network Policy**
- **PXE Boot Policy**
- **Server Boot Policy**
- **IP Address**
- **Subnet Mask**
- **Default Gateway**
- **Server Power State**

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Create UCS Service Profile)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Service Profile Name—**Required. Enter a unique name for the service profile.
- **Description—**Optional. Enter a description for the service profile.
- **Organization—**Required. Choose the organization in which you want to run the workflow and create the service profile. This option also chooses the Cisco UCS Manager account for the workflow.
- **UUID Assignment—**Required. Include this policy to specify the UUID for the server.
- **Storage Policy—**Required. Specify the storage policy that you created for iSCSI boot.
- **Network Policy—**Required. Specify the network policy
- **Placement Policy—**Optional. Include this policy if you want to specify the vNIC, vHBA, and vCon placement for the server.
- **PXE Boot Policy—**Optional. Include this policy if you want to have the server to perform a PXE boot. The secondary boot in this policy must be from a local disk or a SAN boot. If you do not include this policy, the server uses the server boot policy to determine the boot order.
- **Server Boot Policy—**Required. Include this policy to determine the server boot order.
- **BIOS Policy—**Optional. Include this policy if you want to change any of the default settings for the BIOS on the server.
- **IPMI Access Profile—**Optional. Include this policy if you want to be able to access the server through IPMI.
- **SOL Configuration Profile—**Optional. Include this policy if you want to be able to access the server through Serial over LAN.
- **Threshold Policy—**Optional. Include this policy to specify the thresholds for the server.
- **Scrub Policy—**Optional. Include this policy if you want to specify what happens to the local data and BIOS settings on a server during discovery and disassociation.
- **Host Firmware Policy—**Optional. Include this policy if you want to use a host firmware package to upgrade the server firmware.
- **Maintenance Policy—**Optional. Include this policy if you want to specify what happens when change that requires a server reboot is made to this service profile.
- **Power Control Policy—**Optional. Include this policy if the service profile is associated with a blade server and you want to specify the initial power allocation for the server.
- **Server Power State—**Required. Sets the power state that is applied to the server when it is associated with this service profile.

b) Click **Submit**.

Adding a Task: Add vNIC to Service Profile

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

This task adds a third vNIC to the service profile that serves as an overlay vNIC for the iSCSI vNIC.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Add vNIC to Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Add vNIC to Service Profile)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Add vNIC to Service Profile)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the vNIC when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Chooses an existing service profile to which you want to add the vNIC.
- **vNIC Name—**Adds an existing vNIC to the service profile.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Add vNIC to Service Profile)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:
Use this option if you want to create a new vNIC to add to the service profile.

- **Service Profile Name—**Required. Choose an existing service profile that is configured for iSCSI boot.
- **vNIC Name—**Required.
- **MAC Pool—**Required.
- **Fabric ID—**Required.
- **Enable Failover—**Required. Check this check box.

- **VLANs—**Required. Choose a VLAN you created to carry iSCSI traffic.
- **Set as Native VLAN—**Optional.
- **MTU—**Required. Enter a value between 1500 and 9000.
- **Pin Group—**Optional.
- **Adapter Policy—**Optional.
- **QoS Policy—**Optional.
- **Network Control Policy—**Optional.
- **Stats Threshold Policy—**Optional.

b) Click **Submit**.

Adding a Task: Add iSCSI vNIC to Service Profile

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Add iSCSI vNIC to Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Add iSCSI vNIC to Service Profile)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Add iSCSI vNIC to Service Profile)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the vNIC when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Prompts for the service profile to which you want to add the vNIC.
- **iSCI vNIC Name—**Adds an existing iSCSI vNIC to the service profile.
- **Overlay vNIC Name—**Uses an existing overlay vNIC.
- **VLANs—**Uses existing VLANs.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Add vNIC to Service Profile)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Service Profile Name—**Required. Choose an existing service profile that is configured for iSCSI boot.
- **iSCSI vNIC Name—**Required.
- **Overlay vNIC—**Required. Choose the third vNIC that you added to the service profile.
- **iSCSI Adapter Policy—**Optional.
- **MAC Pool—**DO NOT select a MAC Pool.
- **VLANs—**Required. Choose a VLAN you created to carry iSCSI traffic.

b) Click **Submit**.

Adding a Task: Create Service Profile iSCSI Boot Policy

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Create Service Profile iSCSI Boot Policy** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Create Service Profile iSCSI Boot Policy)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details
d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Create Service Profile iSCSI Boot Policy)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the policy when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Uses an existing service profile to create the iSCSI boot policy.
- **Primary vNIC—**Adds an existing vNIC as the primary vNIC for a LAN boot.
- **Secondary vNIC—**Adds an existing vNIC as the secondary vNIC for a LAN boot.
- **Primary iSCSI vNIC—**Adds an existing iSCSI vNIC as the primary iSCSI vNIC.
- **Select Filer—**Allows you to choose an existing Filer or vFiler where the LUN was created.
- **iSCSI Target Name—**Allows you to specify the target node name for the filer.
- **IPv4 Address—**Allows you to specify the iSCSI-enabled VLAN IP address on the filer.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Create Service Profile iSCSI Boot Policy)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

Name	Description
Service Profile button	Choose an existing service profile that is configured for iSCSI boot.
Add LAN Boot check box	Check this check box to add a LAN boot to the policy.
Primary vNIC field	The primary vNIC that you want to use for the LAN boot. This field is only visible if you check the **Add LAN Boot** check box.
Secondary vNIC field	The secondary vNIC that you want to use for the LAN boot. This field is only visible if you check the **Add LAN Boot** check box.
Set Boot Parameters check box	Check this check box to configure the iSCSI boot parameters. The following fields are only visible if you check this check box.
Set iSCSI Boot Parameters area	
Authentication Profile button	Choose an iSCSI authentication profile.
Initiator Name Assignment button	Choose the IQN pool from which initiators are assigned for the iSCSI vNIC.
Initiator IP Address Policy drop-down list	Choose how the IP address is assigned to the iSCSI vNIC. By default, the IP address is assigned from the iSCSI IP pool.

Name	Description
Create iSCSI Static Target area	
Select Filer button	Choose the filer, such as a NetApp filer or vFiler, where the LUN associated with the target is created.
iSCSI Target Name drop-down list	Choose the target node for the filer.
Port field	The port ID for the connection to the storage array.
Authentication Profile button	Choose the associated iSCSI authentication profile.
IPv4 Address drop-down list	Choose the iSCSI-enabled VLAN IP address on the filer.
LUN ID field	The LUN identifier in the iSCSI target.

b) Click **Submit**.

Adding a Task: Associate Service Profile

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Associate UCS Service Profile** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Associate UCS Service Profile)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Associate UCS Service Profile)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Service Profile—**Chooses the service profile that you want to associate with a server.
- **Server—**Chooses the server to which you want to associate the service profile.
- **Server Pool—**Chooses the server pool that contains the type of server to which you want to associate the service profile.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Associate UCS Service Profile)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Service Profile—**Required. Choose an existing service profile that is configured for iSCSI boot.
- **Server Selection Scope—**Required. Choose how you want to select the server.
- **Server—**Required if you chose a scope of **Include Servers**. Choose the server to which you want to associate the service profile.
- **Server Pool—**Required if you chose a scope of **Include Server Pools**. Choose the server pool that contains the type of server to which you want to associate the service profile.

b) Click **Submit**.

Adding a Task: Create Flexible Volume

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Note We recommend that you create a volume of at least 12 GB for an ESXi installation.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Create Flexible Volume** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Create Flexible Volume)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Create Flexible Volume)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Aggregate Name—**Chooses the aggregate where you want to create the volume.
- **Volume Name—**Assigns a name to the volume.
- **Volume Size—**Specifies the size of the volume as an integer.
- **Volume Size Units—**Specifies the unit of size, such as MB, GB, or TB.
- **Space Guarantee—**Specifies the type of space guarantee.
- **Snapshot Size—**Specifies the percentage of the volume snapshot.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Create Flexible Volume)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Aggregate Name—**Choose the aggregate where you want to create the volume.
- **Volume Name—**Enter a unique name for the volume.
- **Volume Size—**Enter the size of the volume as an integer. You must

- **Volume Size Units—**Choose the unit of size.
- **Space Guarantee—**Choose the type of space guarantee.
- **Snapshot Size—**Enter the percentage of the volume snapshot.
- **Security Style NTFS—**Do not check this check box.
- **NFS Export—**Do not check this check box.

b) Click **Submit**.

Adding a Task: Create LUN

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Note We recommend that you create a LUN of at least 10 GB for an ESXi installation.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Create LUN** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Create LUN)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Create LUN)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Volume Name—**Specifies the volume where you want to create the LUN.

- **LUN Name—**Specifies the name of the LUN you want to create.
- **OS Type—**Specifies the type of OS for the LUN.
- **LUN Size—**Specifies the size of the LUN as an integer.
- **LUN Size Units—**Specifies the unit of size, such as MB, GB, or TB.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Create LUN)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Volume Name—**Select the volume where you want to create the LUN.
- **LUN Name—**Enter the name of the LUN you want to create.
- **OS Type—**Choose the type of OS for the LUN.
- **LUN Size—**Enter the size of the LUN as an integer.
- **LUN Size Units—**Choose the unit of size, such as MB, GB, or TB.
- **Reserve Space—**Check this check box if you want to reserve the space for the LUN.

b) Click **Submit**.

Adding a Task: Create Initiator Group

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Create Initiator Group** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Create Initiator Group)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details
d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Create Initiator Group)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Filer Identity Name—**Specifies the filer where you want to create the initiator group
- **Initiator Group Name—**Specifies the name of the initiator group you want to create.
- **Group Type—**Specifies iSCSI for the type of initiator group.
- **OS Type—**Specifies the type of OS for the initiators in the group.
- **Port Set—**Specifies the port set.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Create Initiator Group)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Filer Identity Name—**Choose the filer where you want to create the initiator group
- **Initiator Group Name—**Enter the name of the initiator group you want to create.
- **Group Type—**Choose iSCSI for the type of initiator group.
- **OS Type—**Choose the type of OS for the initiators in the group.
- **Port Set—**Enter the port set.

b) Click **Submit**.

Adding a Task: Add an Initiator to Initiator Group

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Add an Initiator to Initiator Group** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Add an Initiator to Initiator Group)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Add an Initiator to Initiator Group)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Initiator Group Name—**Specifies the name of the initiator group to which you want to add an initiator.
- **Initiator Name—**Specifies the initiator you want to add to the group.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Add an Initiator to Initiator Group)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Initiator Group Name—**Choose the initiator group to which you want to add an initiator.
- **Initiator Name—**Enter the initiator you want to add to the group. To add more than one initiator, separate the names with commas.
- **Force—**Check this check box if you want to forcibly add the initiator to the group.

b) Click **Submit**.

Adding a Task: Map LUN to Initiator Group

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Storage Tasks** > **NetApp Tasks** > **NetApp ONTAP Tasks**.

Step 4 Click the **Create Initiator Group** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Map LUN to Initiator Group)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Map LUN to Initiator Group)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input:

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Filer Identity Name—**Specifies the filer for the initiator group.
- **Initiator Group Name—**Specifies the initiator group you want to map.
- **LUN ID—**Specifies the LUN that you want to map to the initiator group.
- **LUN Path—**Specifies the file path to the LUN.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Map LUN to Initiator Group)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **Filer Identity Name—**Choose the filer for the initiator group.
- **Initiator Group Name—**Choose the initiator group you want to map.

- **LUN ID—**Check this box to specify the LUN that you created earlier in the workflow.
- **LUN Path—**Choose the file path to the LUN.

b) Click **Submit**.

Adding a Task: Set Up PXE Boot

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Network Services Tasks**.

Step 4 Click the **Setup PXE Boot** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Setup PXE Boot)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Setup PXE Boot)** wizard, do the following:

a) If you want to be prompted to enter some of the configuration attributes for the volume when the workflow is run, check one or more of the following check boxes and choose a user input.

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

- **Server MAC Address—**Specifies the MAC address for the server you want to PXE boot. If you want to set up multiple servers, separate the entries with commas.
- **Server IP Address—**Specifies the IP address for the server. If you want to set up multiple servers, place a hyphen (-) between the first and last IP addresses, or separate the entries with commas.
- **Server Net Mask—**Specifies the net mask used to PXE boot.
- **Server Host Name—**Specifies the host name for the server.
- **Server Gateway—**Specifies the gateway used to PXE boot.
- **Root Password—**Specifies the root password for the server.

- **Timezone—**Specifies the time zone for the server.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Setup PXE Boot)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **OS Type—**Choose the OS for the server.
- **Server MAC Address—**Enter the MAC address for the server you want to PXE boot. If you want to set up multiple servers, separate the entries with commas.
- **Server IP Address—**Enter the IP address for the server. If you want to set up multiple servers, place a hyphen (-) between the first and last IP addresses, or separate the entries with commas.
- **Server Net Mask—**Enter the net mask used to PXE boot.
- **Server Host Name—**Enter the host name for the server.
- **Server Gateway—**Enter the gateway used to PXE boot.
- **Server Name Server—**Enter the name server used to PXE boot.
- **Management VLAN—**Enter the VLAN used to PXE boot.
- **Root Password—**Enter the root password for the server.
- **Timezone—**Choose the time zone for the server.

b) Click **Submit**.

Adding a Task: Power On UCS Server

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Power On UCS Server** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Power On UCS Server)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.

- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details
d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Power On UCS Server)** wizard, do the following:

a) If you want to be prompted to specify the server that you want to power on when the workflow is run, check the **Server** check box and choose a user input.
b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Power On UCS Server)** wizard, do the following:

a) If you did not choose to prompt for user input, choose the server that you want to power on from the **Server** drop-down list.
b) Click **Submit**.

Adding a Task: Monitor PXE Boot

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Network Services Tasks**.

Step 4 Click the **Monitor PXE Boot** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Monitor PXE Boot)** wizard, do the following:

a) Enter a task name and comment to identify the task.
b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details
d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Monitor PXE Boot)** wizard, do the following:

a) If you want to be prompted to enter the PXE request ID when the workflow is run, check the **PXE Request ID** check box and choose a user input.

Note To map user inputs, you must have added the user inputs with the appropriate permissions to the workflow.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Monitor PXE Boot)** wizard, do the following:

a) For those configuration attributes for which you did not choose to prompt for user input, complete the following fields:

- **PXE Request ID—**Enter the PXE request ID.
- **Max Wait Time—**Choose the maximum number of hours you want to wait for the PXE boot to complete.

b) Click **Submit**.

Adding a Task: Power Off UCS Server

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Power Off UCS Server** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Power Off UCS Server)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Power Off UCS Server)** wizard, do the following:

a) If you want to be prompted to specify the server that you want to power off when the workflow is run, check the **Server** check box and choose a user input.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Power Off UCS Server)** wizard, do the following:

a) If you did not choose to prompt for user input, choose the server that you want to power off from the **Server** drop-down list.

b) Click **Submit**.

Adding a Task: Modify Service Profile Boot Policy to Boot from iSCSI

This procedure assumes that you have created a workflow, as described in Example: Creating an iSCSI Boot Workflow, on page 24, and that you are already on the **Workflow** tab within Orchestration.

Step 1 In the left pane, expand the folder where the workflow is located and click the row for the iSCSI workflow to which you want to add the task.

Step 2 On the icon bar, click the purple drop-down list icon and choose **Workflow Designer**.

Step 3 In the **Available Tasks** pane of the Workflow Designer, expand **Physical Compute Tasks** > **Cisco UCS Tasks**.

Step 4 Click the **Modify Service Profile Boot Policy to Boot from iSCSI** task, and then drag and drop the selected task onto the workflow designer window.

Step 5 In the **Task Information** screen of the **Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)** wizard, do the following:

a) Enter a task name and comment to identify the task.

b) If you want Cisco UCS Director to automatically retry the workflow if it encounters an error, do the following:

- Check the **Retry Execution** check box.
- From the **Retry Count** drop-down list, choose the number of retry attempts.
- In the **Retry Frequency** field, enter a comma-separated list of values that represents the number of seconds between retries.

c) Review the task details

d) Click **Next**.

Step 6 In the **User Mapping Inputs** screen of the **Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)** wizard, do the following:

a) If you want to be prompted to specify the service profile that you want to modify when the workflow is run, check the **Service Profile** check box and choose a user input.

b) Click **Next**.

Step 7 In the **Task Inputs** screen of the **Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)** wizard, do the following:

a) If you did not choose to prompt for user input, click the **Service Profile** button to choose the service profile that you want to modify.

b) Click **Submit**.

Changing the Boot Order in a Boot Policy

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to modify a policy and then click **View Details**.

Step 5 Click the **Boot Policies** tab.

Step 6 Choose the boot policy that you want to clone and click **Manage Boot Devices Order**.

Step 7 Use the following buttons to change the order of the boot devices:

- **Move Up**
- **Move Down**
- **Delete**

Step 8 When you are done, click **Back**.

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **No Local Storage—**For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Striped—**Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored—**Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration—**For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID—**For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

  If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.

- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

You must include this policy in a service profile and that service profile must be associated with a server for the policy to take effect.

Note For a Cisco UCS C-Series server integrated with Cisco UCS Manager, with an embedded on-board RAID controller, the local disk mode should always be **Any Configuration**, and the RAID must be configured directly on the controller.

Guidelines for all Local Disk Configuration Policies

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single server or RAID configuration.

Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or re-assign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes those with Any Configuration or JBOD configuration.

JBOD Mode Support

The B200 M3 server supports JBOD mode for local disks.

Note Only B200 M1, B200 M2, B200 M3, B250 M1, B250 M2 and B22 M3 blade servers support the JBOD mode for local disks.

Guidelines for Local Disk Configuration Policies Configured for RAID

Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server. You can do this either by configuring the local disk configuration policy in the service profile using one of the defined RAID modes for that server, or you can use the **Any Configuration** mode with the LSI Utilities toolset to create the RAID volumes.

If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

Server May Not Boot After RAID1 Cluster Migration if Any Configuration Mode Specified in Service Profile

After RAID1 clusters are migrated, you need to associate a service profile with the server. If the local disk configuration policy in the service profile is configured with **Any Configuration** mode rather than **RAID1**, the RAID LUN remains in "inactive" state during and after association. As a result, the server cannot boot.

To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the **Any Configuration** mode.

Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with a MegaRAID storage controllers. JBOD mode and operations are not intended for nor are they fully functional on these servers.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

Maximum of One RAID Volume and One RAID Controller in Blade Servers

A blade server can have a maximum of one RAID volume irrespective of how many drives are present in the server. All the local hard drives must be connected to only one RAID controller. For example, a B200 M3 server has an LSI controller and an Intel Patsburg controller, but only the LSI controller can be used as a RAID controller.

In addition, do not use third party tools to create multiple RAID LUNs on blade servers. does not support that configuration.

Number of Disks Selected in Mirrored RAID Should Not Exceed Two

If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

License Required for Certain RAID Configuration Options on Some Servers

Some Cisco UCS servers require a license for certain RAID configuration options. When associates a service profile containing this local disk policy with a server, verifies that the selected RAID option is properly licensed. If there are issues, displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

B420 M3 Server Does Not Support All Configuration Modes

The B420 M3 server does not support the following configuration modes in a local disk configuration policy:

- No RAID
- RAID 6 Striped Dual Parity

In addition, the B420 M3 does not support JBOD modes or operations.

Single-Disk RAID 0 Configurations Not Supported on Some Blade Servers

A single-disk RAID 0 configuration is not supported in the following blade servers:

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

Creating a Local Disk Configuration Policy

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Local Disk Configuration Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Local Disk Configuration Policy** dialog box, do the following:

a) In the **Name** field, enter a unique name for the policy.

b) In the **Description** field, enter a description of the policy.
We recommend that you include information about where and when the policy should be used.

c) From the **Mode** drop-down list, choose one of the following local disk policy modes:

- **No Local Storage—**For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Striped—**Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored—**Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration—**For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID—**For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

  If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

  To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.
- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

Note Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Manager associates a service profile containing this local disk policy with a server, Cisco UCS Manager verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Manager displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

d) If you want the server to retain the configuration in this local disk configuration policy even if the server is disassociated from the service profile, check the **Protect Configuration** check box.

Caution Protect Configuration becomes non-functional if one or more disks in the server are defective or faulty.

This property is checked by default.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Note If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.

e) From the **Flex Flash State** drop-down list, choose whether you want to enable or disable the SD card module.

Note This parameter only applies to a server with an SD card module.

f) Click **Submit**.

What to Do Next

Include the policy in a service profile or service profile template.

Maintenance Policy

A maintenance policy determines what kind of request Cisco UCS Director sends to when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how the service profile changes are deployed. This deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with administrator privileges
- Automatically at the time specified in a schedule

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid schedule. The schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

For more information about maintenance policies and deferred deployment of service profile changes, including guidelines for implementing them, see the Cisco UCS Manager configuration guides.

Creating a Maintenance Policy

Before You Begin

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Maintenance Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description of the policy. We recommend that you include information about where and when the policy should be used.
Reboot Policy drop-down list	Choose when the reboot occurs for servers associated with a service profile that includes this maintenance policy. This can be one of the following: • **Timer Automatic—**All service profile associations and changes are deferred until the maintenance window defined by the schedule shown in the **Schedule** field. • **Immediate—**The server is rebooted automatically as soon as the service profile association is complete or service profile changes are saved by the user. • **User Ack—**The user must reboot the server manually after the service profile association is complete or changes are made.
Schedule drop-down list	Choose the schedule that sets the time period when you want maintenance operations, such as service profile associations and changes, to occur. During the scheduled time period, the servers associated with service profiles that include this maintenance policy are rebooted and all service profile changes are completed. This field is only available if the **Reboot Policy** is set to **Timer Automatic**.The schedule specifies when maintenance operations can be applied to the server.

Step 8 Click **Submit**.

What to Do Next

Include the policy in a service profile or service profile template.

Server Pool Policy Qualification Overview

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you might need to configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating Server Pool Policy Qualifications

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **Server Pool Policy Qualifications** tab.

Step 6 Click **Add**.

Step 7 In the **Create Server Pool Policy Qualifications** wizard, enter a name and description for the policy and click **Next**.

Step 8 On the **Adapter Qualifications** page, do the following to add adapter qualifications to the policy or click **Next** if you do not want to add them:

a) Check the **Add Adapter Qualifications** check box.

b) From the **Type** drop-down list, choose the type of adapter that you want to include in the policy.
After you save the adapter qualification, this type cannot be changed.

c) In the **Model(RegEx)** field, enter a regular expression that the adapter PID must match.

d) In the **Maximum Capacity** field, enter the maximum capacity for the selected type.

e) Click **Next**.

Step 9 On the **Chassis/Server Qualifications** page, do the following to add chassis qualifications and server qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Chassis/Server Qualifications** check box.

b) From the **First Chassis ID** field, enter the first chassis ID from which server pools associated with this policy can draw.
After you save the adapter qualification, this type cannot be changed.

c) In the **Number of Chassis** field, enter the total number of chassis to include in the pool, starting with the chassis identified in the **First Chassis ID** field.

d) In the **Server Qualification Ranges** field, enter the range of server locations that you want to use.
If you want to enter more than one range, separate the ranges by commas. For example, enter 1:5,2:6.

e) Click **Next**.

Example:
For example, if you want to use chassis 5, 6, 7, and 8, enter 5 in the **First Chassis ID** field and 4 in the **Number of Chassis** field. If you want to use only chassis 3, enter 3 in the **First Chassis ID** field and 1 in the **Number of Chassis** field.

Step 10 On the **Memory Qualifications** page, do the following to add memory qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Memory Qualifications** check box.

b) Complete the following fields:

Name	Description
Clock field	The minimum clock speed required, in megahertz.

Name	Description
Min Cap field	The minimum memory capacity required, in megabytes.
Max Cap field	The maximum memory capacity allowed, in megabytes.
Width field	The minimum width of the data bus.
Latency field	The maximum latency allowed, in nanoseconds.
Units field	The unit of measure to associate with the value in the Width field.

c) Click **Next**.

Step 11 On the **CPU/Cores Qualifications** page, do the following to add CPU qualifications and cores qualifications to the policy,or click **Next** if you do not want to add them:

a) Check the **Add CPU/Cores Qualifications** check box.

b) Complete the following fields:

Name	Description
Processor Architecture drop-down list	Choose the CPU architecture to which this policy applies.
Min Number of Cores field	The minimum number of CPU cores required. This integer can be between 1 and 65535.
Max Number of Cores field	The maximum number of CPU cores allowed. This integer can be between 1 and 65535.
Min Number of Threads field	The minimum number of CPU threads required. This integer can be between 1 and 65535 in the associated text field.
Max Number of Threads field	The maximum number of CPU threads allowed. This integer can be between 1 and 65535.
CPU Speed field	The minimum CPU speed required.
Model(RegEx) field	A regular expression that the processor PID must match.
CPU Stepping field	The minimum CPU version required.

c) Click **Next**.

Step 12 On the **Storage Qualifications** page, do the following to add storage qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Storage Qualifications** check box.

b) Complete the following fields:

Name	Description
Diskless drop-down list	Choose whether the available storage must be diskless. Your choice can be one of the following: • **Unspecified—**Either storage type is acceptable. • **Yes—**The storage must be diskless. • **No—**The storage cannot be diskless. If you choose **Yes**, no additional fields are displayed.
Min Cap field	The minimum storage capacity across all disks in the server, in megabytes.
Max Cap field	The maximum storage capacity allowed, in megabytes.
Number of Blocks field	The minimum number of blocks required.
Per Disk Cap field	The minimum storage capacity per disk required, in gigabytes.
Block Size field	The minimum block size required, in bytes.
Units field	The number of units.

c) Click **Next**.

Step 13 On the **Power Group Qualifications** page, do the following to add power group qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Power Group Qualifications** check box.
b) From the **Power Group** drop-down list, choose the power group that you want to include in the policy.
c) Click **Next**.

Step 14 On the **Rack Qualifications** page, do the following to add rack-mount server qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Rack Qualifications** check box.
b) From the **First Slot ID** field, enter the first rack-mount server ID from which server pools associated with this policy can draw.
After you save the adapter qualification, this type cannot be changed.
c) In the **Number of Slots** field, enter the total number of rack-mount server slots to include in the pool, starting with the server slot identified in the **First Slot ID** field.
d) Click **Next**.

Step 15 On the **Server Model Qualifications** page, do the following to add rack-mount server qualifications to the policy, or click **Next** if you do not want to add them:

a) Check the **Add Server Model Qualifications** check box.

b) In the **Model(RegEx)** field, enter a regular expression that the server model PID must match.
c) Click **Next**.

Step 16 Click **Submit**.

Server Pool Policy Overview

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Creating a Server Pool Policy

Before You Begin

This policy requires that at least one of the following resources exists in the system:

- A minimum of one server pool.
- Server pool policy qualifications, if you choose to have servers automatically added to pools.

Step 1 On the menu bar, choose **Physical** > **Compute**.
Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.
Step 3 In the right pane, click the **Organizations** tab.
Step 4 Click the organization in which you want to create the policy and then click **View Details**.
Step 5 Click the **Server Pool Policies** tab.
Step 6 Click **Add**.
Step 7 In the **Create Server Pool Policy** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Target Pool drop-down list	Choose a server pool to associate with the policy.
Qualification drop-down list	Choose a server pool qualification policy to associate with the policy.

Step 8 Click **Submit**.

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine the following:

- How the virtual network interface connections (vCons) are mapped to the physical adapters on a server.
- What types of vNICs or vHBAs can be assigned to each vCon.

Each vNIC/vHBA placement policy contains four vCons that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters and the vNICs and vHBAs are assigned to those vCons.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the type of server and the selected virtual slot mapping scheme, which can be **Round Robin** or **Linear Ordered**. For details about the available mapping schemes, see vCon to Adapter Placement, on page 58.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the **Selection Preference** for each vCon. This can be one of the following:

- —All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- —vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- —Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- —Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.
- —Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

Note An SRIOV usNIC that is explicitly assigned to a vCon set to will remain assigned to that vCon.

If you do not include a vNIC/vHBA placement policy in the service profile, Cisco UCS defaults to the **Round Robin** vCon mapping scheme and the **All** vNIC/vHBA selection preference, distributing the vNICs and vHBAs between the adapters based on the capabilities and relative capacities of each adapter.

vCon to Adapter Placement

Cisco UCS maps every vCon in a service profile to a physical adapter on the server. How that mapping occurs and how the vCons are assigned to a specific adapter in a server depends on the following:

- The type of server. N20-B6620-2 and N20-B6625-2 blade servers with two adapter cards use a different mapping scheme than other supported rack or blade servers.
- The number of adapters in the server.
- The setting of the virtual slot mapping scheme in the vNIC/vHBA placement policy, if applicable.

You must consider this placement when you configure the vNIC/vHBA selection preference to assign vNICs and vHBAs to vCons.

Note vCon to adapter placement is not dependent upon the PCIE slot number of the adapter. The adapter numbers used for the purpose of vCon placement are not the PCIE slot numbers of the adapters, but the ID assigned to them during server discovery.

vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers

In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme:

- —Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default.
- —Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.

vCon to Adapter Placement for All Other Supported Servers

For all other servers supported by Cisco UCS in addition to the N20-B6620-2 and N20-B6625-2 blade servers, the vCon assignment depends on the number of adapters in the server and the virtual slot mapping scheme.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the selected virtual slot mapping scheme: Round Robin or Linear Ordered.

Table 1: vCon to Adapter Placement Using the Round - Robin Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
2	Adapter1	Adapter2	Adapter1	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter2
4	Adapter1	Adapter2	Adapter3	Adapter4

Round Robin is the default mapping scheme.

Table 2: vCon to Adapter Placement Using the Linear Ordered Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter1	Adapter2	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter3
4	Adapter1	Adapter2	Adapter3	Adapter4

Note If you are using a vCon policy with two adapters in the Cisco UCS B440 M2 Blade Server, be aware of the following mapping.

- vCon 2 to adapter 1 maps first
- vCon 1 to adapter 2 maps second ZXA Q

vNIC/vHBA to vCon Assignment

Cisco UCS provides two options for assigning vNICs and vHBAs to vCons through the vNIC/vHBA placement policy: explicit assignment and implicit assignment.

Explicit Assignment of vNICs and vHBAs

With explicit assignment, you specify the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned. Use this assignment option when you must determine how the vNICs and vHBAs are distributed between the adapters on a server.

To configure a vCon and the associated vNICs and vHBAs for explicit assignment, do the following:

- Set the vCon configuration to any of the available options. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server. If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon.

- Assign the vNICs and vHBAs to a vCon. You can make this assignment through the virtual host interface placement properties of the vNIC or vHBA or in the service profile associated with the server.

If you attempt to assign a vNIC or vHBA to a vCon that is not configured for that type of vNIC or vHBA, a message displays that advises you of the configuration error.

During service profile association, Cisco UCS validates the configured placement of the vNICs and vHBAs against the number and capabilities of the physical adapters in the server before assigning the vNICs and vHBAs according to the configuration in the policy. Load distribution is based on the explicit assignments to the vCons and adapters configured in this policy.

If the adapters do not support the assignment of one or more vNICs or vHBAs, Cisco UCS raises a fault against the service profile.

Implicit Assignment of vNICs and vHBAs

With implicit assignment, Cisco UCS determines the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned according to the capability of the adapters and their relative capacity. Use this assignment option if the adapter to which a vNIC or vHBA is assigned is not important to your system configuration.

To configure a vCon for implicit assignment, do the following:

- Set the vCon configuration to **All**, **Exclude Dynamic**, or **Exclude Unassigned**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server.
- Do not set the vCon configuration to **Assigned Only**. Implicit assignment cannot be performed with this setting.
- Do not assign any vNICs or vHBAs to a vCon.

During service profile association, Cisco UCS verifies the number and capabilities of the physical adapters in the server and assigns the vNICs and vHBAs accordingly. Load distribution is based on the capabilities of the adapters, and placement of the vNICs and vHBAs is performed according to the actual order determined by the system. For example, if one adapter can accommodate more vNICs than another, that adapter is assigned more vNICs.

If the adapters cannot support the number of vNICs and vHBAs configured for that server, Cisco UCS raises a fault against the service profile.

Implicit Assignment of vNICs in a Dual Adapter Environment

When you use implicit vNIC assignment for a dual slot server with an adapter card in each slot, Cisco UCS typically assigns the vNICs/vHBAs as follows:

- If the server has the same adapter in both slots, Cisco UCS assigns half the vNICs and half the vHBAs to each adapter.
- If the server has one non-VIC adapter and one VIC adapter, Cisco UCS assigns two vNICs and two vHBAs to the non-VIC adapter and the remaining vNICs and vHBAs to the VIC adapter.
- If the server has two different VIC adapters, Cisco UCS assigns the vNICs and vHBAs proportionally, based on the relative capabilities of the two adapters.

The following examples show how Cisco UCS would typically assign the vNICs and vHBAs with different combinations of supported adapter cards:

- If you want to configure four vNICs and the server contains two Cisco UCS M51KR-B Broadcom BCM57711 adapters (with two vNICs each), Cisco UCS assigns two vNICs to each adapter.
- If you want to configure 50 vNICs and the server contains a Cisco UCS CNA M72KR-E adapter (2 vNICs) and a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs), Cisco UCS assigns two vNICs to the Cisco UCS CNA M72KR-E adapter and 48 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter.
- If you want to configure 150 vNICs and the server contains a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs) and a Cisco UCS VIC-1240 Virtual Interface Card adapter (256 vNICs), Cisco UCS assigns 50 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter and 100 vNICs to the Cisco UCS VIC-1240 Virtual Interface Card adapter.

Note Exceptions to this implicit assignment occur if you configure the vNICs for fabric failover and if you configure dynamic vNICs for the server.

For a configuration that includes vNIC fabric failover where one adapter does not support vNIC failover, Cisco UCS implicitly assigns all vNICs that have fabric failover enabled to the adapter that supports them. If the configuration includes only vNICs that are configured for fabric failover, no vNICs are implicitly assigned to the adapter that does not support them. If some vNICs are configured for fabric failover and some are not, Cisco UCS assigns all failover vNICs to the adapter that supports them and a minimum of one nonfailover vNIC to the adapter that does not support them, according to the ratio above.

For a configuration that includes dynamic vNICs, the same implicit assignment would occur. Cisco UCS assigns all dynamic vNICs to the adapter that supports them. However, with a combination of dynamic vNICs and static vNICs, at least one static vNIC is assigned to the adapter that does not support dynamic vNICs.

Creating a vNIC/vHBA Placement Policy

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **Organizations** tab.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click the **vNIC/vHBA Placement Policies** tab.

Step 6 Click **Add**.

Step 7 In the **Add Network Control Policy** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the policy.

Name	Description
Virtual Slot drop-down list	Choose the virtual network interface for each virtual slot. This can be one of the following: • —All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default. • —vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA. • —Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it. • —Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it. • —Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic. **Note** An SRIOV usNIC that is explicitly assigned to a vCon set to will remain assigned to that vCon.

Step 8 Click **Submit**.

Placement Policy

The placement policy is a Cisco UCS Director policy that allows you to select and map vCons to vNICs and vHBAs. Depending upon the configuration you choose, you can allow the system to do the placement, choose the placement yourself, or use a vNIC/vHBA placement policy to determine the placement.

This policy assigns vNICs or vHBAs to the physical adapters on a server. Each placement policy contains virtual network interface connections (vCons) that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated to a server, the vCons in the placement policy are assigned to the physical adapters. For servers with only one adapter, both vCons are assigned to the adapter; for servers with two adapters, one vCon is assigned to each adapter.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating a Placement Policy

Before You Begin

Before you create a placement policy, review the guidelines for vNIC/vHBA placement policies in the Cisco UCS Manager configuration guides to ensure that you understand the impact of the choices that you make.

Step 1 On the menu bar, choose**Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click the **Placement Policy** tab.

Step 3 Click **Add**.

Step 4 In the **Placement Policy Details** screen of the **Add Placement Policy** wizard, complete the following fields:

a) In the **Policy Name** field, enter a name for the placement policy.
b) In the **Policy Description** field, enter a description for the policy.
c) From the **UCS Account Name** drop-down list, choose the Cisco UCS Manager account to which you want to add this policy.
d) From the **UCS Organization Name** drop-down list, choose the Cisco UCS organization to which you want to add this policy.
e) From the **Storage Policy** drop-down list, choose the storage policy that you want to apply to this policy.
f) From the **Network Policy** drop-down list, choose the network policy that you want to apply to this policy.
g) From the **Select Placement Type** drop-down list, choose one of the following options:

- **Let System Perform Placement—**Cisco UCS Director determines the optimal placement for the vNICs and vHBAs. If you choose this option, continue with Step 6.
- **Manual Placement—**You choose the virtual network interface preferences for each of the vCons. If you choose this option, continue with Step 5.
- **Select Placement Policy—**The vNIC/vHBA placement policy that you choose determines the placement of the vNICs and vHBAs. If you choose this option, choose a policy from the **Select vNIC/vHBA Placement Policy** drop-down list and continue with Step 6.

Step 5 If you chose the manual placement option, do the following:

a) In the **Virtual Network Interface Selection Preference** area, choose one of the following options from the drop-down list for each of the vCons.

- **—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- **—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- **—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- **—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.

- —Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

  Note An SRIOV usNIC that is explicitly assigned to a vCon set to will remain assigned to that vCon.

b) Click **Next**.
c) From the **Select Virtual Interface (vNIC/vHBA)** drop-down list, choose a vNIC or vHBA.
d) Click **Add**.
e) From the **Assign to Virtual Network Interface** drop-down list, choose the vCon where you want to place the vNIC or vHBA.
f) Repeat steps 5c to 5e until you have placed all the vNICs and vHBAs.
g) Click **Next** and continue with Step 6.

Step 6 On the **Virtual Interface Order** screen of the **Add Placement Policy** wizard, do the following:

a) In the **Virtual Network Interface** table, review the order of the vHBAs and vNICs.
b) If necessary, check the check box for a vNIC or vHBA and one or more of the following to set the interface order:

- Click the **Move UP** or **Move DOWN** buttons to move the vNIC or vHBA up or down in order.
- Choose a number from the **Virtual Interface Order** drop-down list to set the desired order.

Step 7 After you have completed the placement configuration, click **Submit**.