Configuring Service Profiles

This chapter includes the following sections:

Service Profiles that Override Server Identity

This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies set up in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server and then associate it with another server. This re-association can be done either manually or through an automated server pool policy. The burned-in settings, such as UUID and MAC address, on the new server are overwritten with the configuration in the service profile. As a result, the change in server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Unless the service profile contains power management policies, a server pool qualification policy, or another policy that requires a specific hardware configuration, the profile can be used for any type of server in the Cisco UCS instance.

You can associate these service profiles with either a rack-mount server or a blade server. The ability to migrate the service profile depends upon whether you choose to restrict migration of the service profile.

Note If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association may fail.

Service Profiles that Inherit Server Identity

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved or migrated to another server.

You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two NICs
- For a converged network adapter or a virtual interface card, the WWN addresses for the two HBAs
- BIOS versions
- Server UUID

Important The server identity and configuration information inherited through this service profile may not be the values burned into the server hardware at manufacture if those values were changed before this profile is associated with the server.

Service Profile Templates

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.

Tip If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

Initial template

Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles created from this template, you must change each profile individually.

Updating template

Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Guidelines and Recommendations for Service Profiles

In addition to any guidelines or recommendations that are specific to policies and pools included in service profiles and service profile templates, such as the local disk configuration policy, you need to be aware of the following guidelines and recommendations that impact the ability to associate a service profile with a server:

Limit to the Number of vNICs that Can Be Configured on a Rack-Mount Server

You can configure up to 56 vNICs per supported adapter, such as the Cisco UCS P81E Virtual Interface Card (N2XX-ACPCI01), on any rack-mount server that is integrated with Cisco UCS Manager.

No Power Capping Support for Rack-Mount Servers

Power capping is not supported for rack servers. If you include a power control policy in a service profile that is associated with a rack-mount server, the policy is not implemented.

Creating Service Profiles

Creating a Service Profile with the Expert Wizard

Procedure

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

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

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the organization and select **Create Service Profile (expert)**.

Step 5 In the **Create Service Profile (expert)** wizard, complete the following:

- Page 1: Identifying the Service Profile , on page 4
- Page 2: Configuring the Storage Options, on page 5
- Page 3: Configuring the Networking Options, on page 10

Page 1: Identifying the Service Profile

This procedure directly follows the steps in Creating a Service Profile with the Expert Wizard, on page 3. It describes how to set the identity of a service profile on the **Identify Service Profile** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 In the **Name** field, enter a unique name that you can use to identify the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

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

Step 2 From the **UUID Assignment** drop-down list, do one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool. Continue with Step 5.
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server. Continue with Step 5.
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	Uses the UUID that you manually assign. Continue with Step 3.

Option	Description
Pools *Pool_Name*	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool. If you do not want use any of the existing pools, but instead want to create a pool that all serivce profiles can access, continue with Step 4. Otherwise, continue with Step 5.

Step 3 (Optional) If you selected the **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** option, do the following:

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

b) To verify that the selected UUID is available, click the **here** link.

Step 4 (Optional) If you want to create a new UUID Suffix pool to use to use in this service profile, click **Create UUID Suffix Pool** and complete the fields in the **Create UUID Suffix Pool** wizard.
For more information, see Creating a UUID Suffix Pool.

Step 5 (Optional) In the text box, enter a description of this service profile.
The user-defined description for this service profile.

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

Step 6 Click **Next**.

What to Do Next

Complete the steps in Page 2: Configuring the Storage Options, on page 5.

Page 2: Configuring the Storage Options

This procedure directly follows Page 1: Identifying the Service Profile , on page 4. It describes how to configure the storage options for a service profile on the **Storage** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Local Storage** drop-down list, choose one of the following:

Option	Description
Select Local Storage Policy to use	Assigns the default local disk storage policy to this service profile. Continue with Step 4.
Create a Specific Storage Policy	Enables you to create a local disk policy that can only be accessed by this service profile. Continue with Step 2.
Storage Policies *Policy_Name*	Select an existing local disk policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to the service profile. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you chose **Create a Specific Storage Policy** and want to create a new policy that can only be used by this service profile, do the following:

a) From the **Mode** drop-down list, choose one of 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 Stripes**—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.
- **RAID 6 Stripes 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 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.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

Note 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 after you apply the **No RAID** mode.

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.

b) If you want to ensure that the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile, check the **Protect Configuration** check box. 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.

c) Continue with Step 4.

Step 3 (Optional) To create a local disk configuration policy that will be available to all service profiles, do the following:

a) Click the **Create Local Disk Configuration Policy** link.

b) In the **Create Local Disk Configuration** dialog box, complete the fields.
For more information, see Creating a Local Disk Configuration Policy.

c) Click **OK**.

d) From the **Local Storage** drop-down list, choose the policy you created.

Step 4 In the **How would you like to configure SAN storage?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vHBAs for this service profile. Continue with Step 7.
Expert	Allows you to create an unlimited number of vHBAs for this service profile. Continue with Step 8.
No vHBAs	Does not include any vHBAs for connections to a Fibre Channel SAN in the service profile. Continue with Step 9.
Hardware Inherited	Uses the vHBAs assigned to the Fibre Channel adapter profile associated with the server. Continue with Step 9.

Step 5 (Optional) If you chose the simple SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.

- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) In the **vHBA 0 (Fabric A)** area, complete the following fields:

- In the **Name** field, enter a unique name for the vHBA.
- From the **Select VSAN** drop-down list, choose the name of the VSAN with which this vHBA should be associated.

If the VSAN you need is not in the drop-down list, click the **Create VSAN** link. For more information, see Creating a Named VSAN.

c) Repeat Step 7b in the **vHBA 1 (Fabric B)** area to create a VSAN for that vHBA.

d) Continue with Step 9.

Step 6 (Optional) If you chose the expert SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.
- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) Click **Add** on the icon bar of the table to open the **Create vHBA** dialog box.

c) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	The name of this vHBA. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use SAN Connectivity Template check box	Check this check box if you want to use a template to create the vHBA. Cisco UCS Manager GUI displays the **vHBA Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more SAN connectivity templates exist in the system.
Create vHBA Template link	Click this link if you want to create a vHBA template.

Name	Description
WWPN Assignment drop-down list	If you want to: • Use the default WWPN pool, leave this field set to **Select (pool default used by default)**. • Use the WWPN assigned to the server by the manufacturer, select **Hardware Default**. • A specific WWPN, select **20:00:00:25:B5:00:00:00**, **20:XX:XX:XX:XX:XX:XX:XX**, or **5X:XX:XX:XX:XX:XX:XX:XX** and enter the WWPN in the **WWPN** field. To verify that this WWPN is available, click the corresponding link. • A WWPN from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available WWN addresses in the pool and the second is the total number of WWPN addresses in the pool. To create a new WWPN pool, click **WWPN Pool**.

d) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.
Persistent Binding field	This can be: • **disabled** • **enabled**
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
Operational Parameters Section	

Name	Description
Stats Threshold Policy drop-down list box	The threshold policy with which this vHBA is associated.

e) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

f) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 3: Configuring the Networking Options, on page 10.

Page 3: Configuring the Networking Options

This procedure directly follows Page 2: Configuring the Storage Options, on page 5. It describes how to configure the networking options, including LAN connectivity, on the **Networking** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 (Optional) If you plan to assign this service profile to a server with an adapter that supports dynamic vNICs, choose one of the following options from the **Dynamic vNIC Connection** drop-down list:

Option	Description
Select a Policy to use	Enables you to create a service profile without a dynamic vNIC connection policy for a server with an adapter that does not support dynamic vNICs. This option does not include a dynamic vNIC connection policy in the service profile. Continue with Step 4.

Option	Description
Create a Specific Dynamic vNIC Connection Policy	Enables you to create a dynamic vNIC connection policy that can only be accessed by this service profile. Continue with Step 2.
Dynamic vNIC Connection Policies *Policy_Name*	Select an existing dynamic vNIC connection policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to the service profile. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you clicked **Create a Specific Dynamic vNIC Connection Policy**, do the following to create a new dynamic vNIC connection policy that can only be used by this service profile:

a) Complete the following fields:

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.

b) Continue with Step 4.

Step 3 (Optional) To create a dynamic vNIC connection policy that will be available to all service profiles, do the following:

a) Click **Create Dynamic vNIC Connection Policy**.
b) In the **Create Dynamic vNIC Connect Policy** dialog box, complete the fields.
For more information, see Creating a Dynamic vNIC Connection Policy.
c) Click **OK**.
d) From the **Dynamic vNIC Connection** drop-down list, choose the policy you created.
e) Continue with Step 4.

Step 4 In the **How would you like to configure LAN connectivity?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vNICs, in dual fabric mode, for this service profile. Continue with Step 5.
Expert	Allows you to create an unlimited number of vNICs for this service profile. Continue with Step 6.

Option	Description
No vNICs	Does not include any vNICs for connections to a LAN in the service profile. Any server associated with this service profile cannot be able to communicate with a LAN unless you modify the service profile to add vNICs. Continue with Step 7.
Hardware Inherited	Uses the vNICs assigned to the Ethernet adapter profile associated with the server. Continue with Step 7.

Step 5 (Optional) If you chose the simple LAN connectivity option, do the following:

a) In the **vNIC 0 (Fabric A)** area, complete the following fields:

- In the **Name** field, enter a unique name for the vNIC.
- From the **Select Native VLAN** drop-down list, choose the name of the VLAN with which this vNIC should communicate.

If the VLAN you need is not in the drop-down list, click the **Create VLAN** link. For more information, see Creating a Named VLAN.

b) Repeat Step 2a in the **vNIC 1 (Fabric B)** area to create a VLAN for that vNIC.

c) Continue with Step 4.

Step 6 If you chose the expert LAN connectivity option, do the following:

a) Click **Add** on the icon bar of the table to open the **Create vNICs** dialog box.

b) Complete the following fields to specify the identity information for the vNIC:

Name	Description
Name field	Enter a name for this vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use LAN Connectivity Template check box	Check this check box if you want to use a template to create the vNIC. Cisco UCS Manager GUI displays the **vNIC Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more LAN connectivity templates exist in the system.
Create vNIC Template link	Click this link if you want to create a vNIC template.

Name	Description
MAC Address Assignment drop-down list	If you want to: • Use the default MAC address pool, leave this field set to **Select (pool default used by default)**. • Use the MAC address assigned to the server by the manufacturer, select **Hardware Default**. • A specific MAC address, select **02:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link. • A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

c) In the **Fabric Interconnect** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not enable fabric failover for the vNIC under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • if you plan to associate this vNIC with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.

Name	Description
VLANs table	This table lists the VLANs that can be associated with this vNIC. The columns are: • **Select**—Check the check box in this column for each VLAN you want to use. • **Name**—The name of the VLAN. • **Native VLAN**—To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216.
Pin Group drop-down list	Choose the LAN pin group you want associated with this vNIC.
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Operational Parameters Section	
Stats Threshold Policy drop-down list	The statistics collection policy with which this vNIC is associated.

d) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list	The Ethernet adapter policy with which this vNIC is associated.
Create Ethernet Adapter Policy link	Click this link if you want to create an Ethernet adapter policy.
QoS drop-down list	The quality of service policy with which this vNIC is associated.
Create QoS Policy link	Click this link if you want to create a quality of service policy.
Network Control Policy drop-down list	The network control policy with which this vNIC is associated.
Create Network Control Policy Policy link	Click this link if you want to create a network control policy.

e) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 4: Setting the vNIC/vHBA Placement, on page 15.

Page 4: Setting the vNIC/vHBA Placement

This procedure directly follows Page 3: Configuring the Networking Options, on page 10. It describes how to set the vNIC and vHBA placement options on the **vNIC/vHBA Placement** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Select Placement** drop-down list, choose one of the following:

Option	Description
Let System Perform Placement	Specifies that Cisco UCS Manager determines the vNIC/vHBA placement for the server associated with the service profile. The placement is determined by the order set in the PCI Order table. Continue with Step 2.
Specify Manually	Enables you to do the following: • Explicitly assign the vNICs and vHBAs associated with this service profile to a virtual network interface connection (vCon). • Configure the types of vNICs and vHBAs that can be assigned to a vCon, either manually or through a vNIC/vHBA placement policy. Continue with Step 3.
vNIC/vHBA Placement Profiles ***Placement Profile Name***	Assigns an existing vNIC/vHBA placement policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, click **Create Placement Policy** and continue with Step 4. Otherwise, continue with Step 5.

Step 2 (Optional) If you chose **Let System Perform Placement**, do the following:

a) Use one or more of the following buttons to adjust the order of the vNICs and vHBAs:

Name	Description
Move Up button	Moves the selected vNIC or VHBA to a higher priority in the list.

Name	Description
Move Down button	Moves the selected vNIC or vHBA to a lower priority in the list.
Delete button	Deletes the selected vNIC or vHBA.
Reorder button	Returns all vNICs and vHBAs to their original order.
Modify button	Enables you to modify the currently-selected vNIC or vHBA. **Note** You can change any options for the vNIC or vHBA except its name.

b) Continue with Step 5.

Step 3 (Optional) If you chose **Specify Manually**, do the following:

a) On the appropriate tab in the **vNIC/vHBA** table, click a vNIC or vHBA.

b) In the **Virtual Host Interface** table, click a vCON row and if necessary, choose one of the following values from the **Selection Preference** column:

- **all**—All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic.
- **assigned-only**—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.
- **exclude-dynamic**—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.
- **exclude-unassigned**—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.

c) Click **Assign**.
If you need to undo an assignment, click **Remove**.

d) Repeat Steps a through c until you have assigned all vNICs and vHBAs.

e) When you have specified all vNIC and vHBA placements, continue with Step 5.

Step 4 If you clicked **Create Placement Policy**, do the following in the **Create Placement Policy** dialog box:

a) In the **Name** field, enter a unique name for the placement policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Selection Preference** column for each **Virtual Slot**, choose one of the following from the drop-down list:

- **all**—All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic.

- **assigned-only**—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.
- **exclude-dynamic**—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.
- **exclude-unassigned**—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.

c) Click **OK**.
d) After the dialog box closes, choose the policy you created from the **Select Placement** drop-down list.

Step 5 Click **Next**.

What to Do Next

Complete Page 5: Setting the Server Boot Order, on page 17.

Page 5: Setting the Server Boot Order

This procedure directly follows Page 4: Setting the vNIC/vHBA Placement, on page 15. It describes how to set the server boot order options on the **Server Boot Order** page of the **Create Service Profile (expert)** wizard.

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.

Procedure

Step 1 From the **Boot Policy** drop-down list, choose one of the following:

Option	Description
Select Boot Policy to use	Assigns the default boot policy to this service profile. Continue with Step 9.
Create a Specific Boot Policy	Enables you to create a local boot policy that can only be accessed by this service profile. Continue with Step 3.

Option	Description
Boot Policies *Policy_Name*	Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click **Create Boot Policy** and continue with Step 2. Otherwise, choose a policy from the list and continue with Step 9.

Step 2 If you clicked **Create Boot Policy** to create a boot policy that all service profiles and templates can use, do the following:

a) In the **Create Boot Policy** dialog box, enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Continue with Step 3.

Step 3 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 4 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 5 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.

b) Click one of the following links to add the device to the **Boot Order** table:

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

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 6 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.

b) Click the **Add LAN Boot** link.

c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.

d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 7 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.

b) Click the **Add SAN Boot** link.

c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 8 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Boot Policy** drop-down list.

Step 9 Click **Next**.

What to Do Next

Complete Page 6: Adding the Maintenance Policy, on page 20.

Page 6: Adding the Maintenance Policy

This procedure directly follows Page 5: Setting the Server Boot Order, on page 17. It describes how to add a maintenance policy to the service profile on the **Maintenance Policy** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Maintenance Policy** drop-down list, choose one of the following:

Option	Description
Select a Maintenance Policy to Use (default policy shown)	Assigns the default maintenance policy to this service profile. Continue with Step 4.
Maintenance Policies ***Policy_Name***	Assigns an existing maintenance policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click **Create Maintenance Policy** and continue with Step 2. Otherwise, choose a policy from the list and continue with Step 4.

Step 2 If you clicked **Create Maintenance Policy** to create a maintenance policy that all service profiles and templates can use, do the following:

a) In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Name	Description
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, the server needs to be rebooted to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be: • **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. • **timer-automatic**—Cisco UCS defers all service profile associations and changes until the maintenance window defined by the schedule shown in the **Schedule** field.
Schedule drop-down list	If the **Reboot Policy** is set to **timer-automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.

b) Click **OK** and continue with Step 3.

Step 3 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Maintenance Policy** drop-down list.

Step 4 Click **Next**.

What to Do Next

Complete Page 7: Specifying the Server Assignment, on page 21.

Page 7: Specifying the Server Assignment

This procedure directly follows Page 6: Adding the Maintenance Policy, on page 20. It describes how to specify the way a server is assigned and which firmware packages are associated with the service profile on the **Server Assignment** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Server Assignment** drop-down list, choose one of the following:

Option	Description
Assign Later	Allows you to assign a server after you have created and configured the service profile. Continue with Step 6.
Pre-provision a slot	Specifies the chassis and slot that contains the server which will be assigned to the service profile. If the server is not in the slot or is otherwise unavailable, the service profile will be associated with the server when it becomes available. Continue with Step 2.
Select existing Server	Displays a table of available, unassociated servers that you can use to select the server which will be assigned to the service profile. Continue with Step 3.
Select from a Pool ***Pool_Name***	Select a server pool from the list at the bottom of the drop-down list. Cisco UCS Manager assigns a server from this pool to the service profile. Continue with Step 4.

Step 2 If you chose **Pre-provision a slot**, do the following:

a) In the **Chassis Id** field, enter the number of the chassis where the selected server is located.
b) In the **Slot Id** field, enter the number of the slot where the selected server is located.
c) Continue with Step 4.

Step 3 If you chose **Select existing Server**, do the following:

a) In the **Select** column of the table of available servers, click the radio button for the server that meets the needs of this service profile.
b) Continue with Step 4.

Step 4 In the **Power State** field, click one of the following radio buttons to set the power state that will be applied to the server when it is associated with this service profile:

- **Down** if you want the server to be powered down before the profile is associated with the server.
- **Up** if you want the server to be powered up before the profile is associated with the server

By default, the server is powered up.

Step 5 If you want to restrict the migration of the service profile after it has been associated with a server, check the **Restrict Migration.** check box.
If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association may fail.

Step 6 (Optional) In the **Firmware Management** area, do the following to use policies to update the firmware on the server associated with the service profile:

a) Click the down arrows on the **Firmware Management** bar to expand the area.
b) Complete the following fields:

Name	Description
Host Firmware drop-down list	To associate a host firmware package with this service profile, choose its name from the drop-down list.
Create Host Firmware Package link	Click this link if you want to create a host firmware package.
Management Firmware drop-down list	To associate a management firmware package with this service profile, choose its name from the drop-down list.
Create Management Firmware Package link	Click this link if you want to create a management firmware package.

Step 7 Click **Next**.

What to Do Next

Complete Page 8: Adding Operational Policies, on page 23.

Page 8: Adding Operational Policies

This procedure directly follows Page 7: Specifying the Server Assignment, on page 21. It describes how to add operational policies to the service profile on the **Operational Policies** page of the **Create Service Profile (expert)** wizard. These policies are optional.

Procedure

Step 1 To override the default BIOS settings and configure them through the service profile, click the down arrows to expand the **BIOS Configuration** bar and do one of the following:

- To add an existing policy, select the desired BIOS policy from the **BIOS Policy** drop-down list .
- To create a BIOS policy that is available to all service profiles, click **Create BIOS Policy**, complete the fields in the dialog box, and then select that policy from the **BIOS Policy** drop-down list .

For more information about how to create a BIOS policy, see Creating a BIOS Policy.

Step 2 To provide external access to the CIMC on the server, click the down arrows to expand the **External IPMI Management Configuration** bar and add an IPMI profile and a serial over LAN policy.
If you do not want to provide external access, continue with Step 4.

Step 3 To add an IPMI profile to the service profile, do one of the following:

- To add an existing policy, select the desired IPMI profile from the **IPMI Access Profile** drop-down list.

- If the **IPMI Access Profile** drop-down list does not include an IPMI profile with the desired user access, click the **Create Access IPMI Profile** link to create an IPMI profile that is available to all service profiles and then select that profile from the **IPMI Access Profile** drop-down list.

For more information about how to create an IPMI profile, see Creating an IPMI Access Profile.

Step 4 To add a Serial over LAN policy to the service profile, do one of the following:

- To add an existing policy, select the desired Serial over LAN policy from the **SoL Configuration Profile** drop-down list.
- To create a Serial over LAN policy that is only available to service profile created from this template, select **Create a Specific SoL Policy** from the **SoL Configuration Profile** drop-down list and complete the **Admin State** field and the **Speed** drop-down list.
- To create a Serial over LAN policy that is available to all service profile templates, click the **Create Serial over LAN Policy** link, complete the fields in the dialog box, and then select that policy from the **SoL Configuration Profile** drop-down list.

For more information about how to create a serial over LAN policy, see Creating a Serial over LAN Policy.

Step 5 To configure the management IP required for external access to the CIMC on the server, click the down arrows to expand the **Management IP Address** bar and do the following:

a) Click one of the following radio buttons:

- **none**—No management IP address is assigned to the service profile. The management IP address is set based on the CIMC management IP address settings on the server.
- **static**—A static management IP address is assigned to the service profile, based on the information entered in this area.
- **pooled**—A management IP address is assigned to the service profile from the management IP address pool.

b) If you selected **static**, complete the following fields:

Field	Description
IP Address	The static IPv4 address to be assigned to the service profile
Subnet Mask	The subnet mask for the IP address.
Default Gateway	The default gateway that the IP address should use.

Step 6 To monitor thresholds and collect statistics for the associated server, click the down arrows to expand the **Monitoring Configuration (Thresholds)** bar and do one of the following:

- To add an existing policy, select the desired threshold policy from the **Threshold Policy** drop-down list.
- To create a threshold policy that is available to all service profiles, click the **Create Threshold Policy** link, complete the fields in the dialog box, and then select that policy from the **Threshold Policy** drop-down list.

For more information about how to create a threshold policy, see Creating a Server and Server Component Threshold Policy.

Step 7 To associate a power control policy with the service profile, click the down arrows to expand the **Power Control Policy Configuration** bar and do one of the following:

- To add an existing policy, select the desired power control policy from the **Power Control Policy** drop-down list.
- To create a power control policy that is available to all service profiles, click the **Create Power Control Policy** link , complete the fields in the dialog box, and then select that policy from the **Power Control Policy** drop-down list.

For more information about how to create a power control policy, see Creating a Power Control Policy.

Step 8 To associate a scrub policy with the service profile, click the down arrows to expand the **Scrub Policy** bar and do one of the following:

- To add an existing policy, select the desired scrub policy from the **Scrub Policy** drop-down list .
- To create a scrub policy that is available to all service profiles, click the **Create Scrub Policy** link , complete the fields in the dialog box, and then select that policy from the **Scrub Policy** drop-down list .

For more information about how to create a scrub policy, see Creating a Scrub Policy.

Step 9 Click **Finish**.

Creating a Service Profile that Inherits Server Identity

Procedure

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

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

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the organization and select **Create Service Profile**.

Step 5 In the **Naming** area of the **Create Service Profile** dialog box, complete the following fields:

a) In the **Name** field, enter a unique name that you can use to identify the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Description** field, enter a description of this service profile.

Step 6 In the **vNICs** area of the **Create Service Profile** dialog box, complete the following fields:

Name	Description
Primary vNIC Section	

Name	Description
Primary vNIC check box	Check this check box if you want to create a vNIC for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vNIC.
Fabric field	The fabric interconnect that this vNIC is associated with.
Network drop-down list	The LAN that this vNIC is associated with.
Secondary vNIC Section	
Secondary vNIC check box	Check this check box if you want to create a second vNIC for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vNIC.
Fabric field	The fabric interconnect that this vNIC is associated with.
Network drop-down list	The LAN that this vNIC is associated with.

Step 7 In the **vHBAs** area of the **Create Service Profile** dialog box, complete the following fields:

Name	Description
Primary vHBA Section	
Primary vHBA check box	Check this check box if you want to create a vHBA for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vHBA.
Fabric field	The fabric interconnect that this vHBA is associated with. Do not associate the primary vHBA with the same fabric as the secondary vHBA.
Secondary vHBA Section	
Secondary vHBA check box	Check this check box if you want to create a second vHBA for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Name field	The name of the vHBA.

Name	Description
Fabric field	The fabric interconnect that this vHBA is associated with. Do not associate the secondary vHBA with the same fabric as the primary vHBA.

Step 8 In the **Boot Order** area of the **Create Service Profile** dialog box, complete the following fields:

Name	Description
Primary Boot Device Section	
Primary Boot Device check box	Check this check box if you want to set a boot device for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.
Type field	This can be: • **local-disk**—The server boots from its local disk. **Note** If you select this option, you cannot select **local-disk** or **san** as your secondary boot type. • **san**—The server boots from an image stored in a SAN. If you select this option, Cisco UCS Manager GUI displays the **SAN** area. • **lan**—The server boots from the LAN. If you select this option, Cisco UCS Manager GUI displays the **Network** area that lets you specify which vNIC the server should use for the PXE boot. • **CD-ROM**—The server boots from a virtual CD-ROM. • **Floppy**—The server boots from a virtual floppy.
SAN area	If **Type** is set to **san**, this area contains the following field: • **vHBA**—The vHBA used to access the SAN boot image • **LUN**—The LUN that corresponds to the location of the boot image • **WWN**—The WWN that corresponds to the location of the boot image
Network (PXE) area	If **Type** is set to **lan**, this area contains the **vNIC** drop-down list from which you can choose the vNIC from which the server should boot.
Secondary Boot Device Section	
Secondary Boot Device check box	Check this check box if you want to set a second boot device for this service profile. If you check this box, Cisco UCS Manager GUI displays the rest of the fields in this section.

Name	Description
Type field	This can be: • **local-disk**—The server boots from its local disk. • **san**—The server boots from an image stored in a SAN. If you select this option, Cisco UCS Manager GUI displays the **SAN** area. • **lan**—The server boots from the LAN. If you select this option, Cisco UCS Manager GUI displays the **Network** area that lets you specify which vNIC the server should use for the PXE boot. • **CD-ROM**—The server boots from a virtual CD-ROM. • **Floppy**—The server boots from a virtual floppy.
SAN area	If **Type** is set to **san**, this area contains the following field: • **vHBA**—The vHBA used to access the SAN boot image • **LUN**—The LUN that corresponds to the location of the boot image • **WWN**—The WWN that corresponds to the location of the boot image
Network (PXE) area	If **Type** is set to **lan**, this area contains the **vNIC** drop-down list from which you can choose the vNIC from which the server should boot.

Step 9 (Optional) In the **Select** column of the **Server Association (optional)** area, click the radio button for a server to associate this service profile with that server.

Step 10 Click **OK**.

Creating a Hardware Based Service Profile for a Blade Server

You cannot move a hardware based service profile to another server.

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.

Step 3 Choose the server for which you want to create a hardware based service profile.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Create Service Profile**.

Step 6 In the **Create Service Profile for Server** dialog box, do the following:

a) Click the **Hardware Based Service Profile** radio button.
b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
c) If you want Cisco UCS Manager to create vNICs for the service profile, check the **Create Default vNICs** check box.
d) If you want Cisco UCS Manager to create vHBAs for the service profile, check the **Create Default vHBAs** check box.
e) Click **OK**.

Cisco UCS Manager inherits and automatically applies the identity and configuration information in the server, creates the service profile, and associates it with the server.

Creating a Hardware Based Service Profile for a Rack-Mount Server

You cannot move a hardware based service profile to another server.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment** > **Rack Mounts** > **Servers**.
Step 3 Choose the server for which you want to create a hardware based service profile.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Create Service Profile**.
Step 6 In the **Create Service Profile for Server** dialog box, do the following:
a) Click the **Hardware Based Service Profile** radio button.
b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
c) If you want Cisco UCS Manager to create vNICs for the service profile, check the **Create Default vNICs** check box.
d) If you want Cisco UCS Manager to create vHBAs for the service profile, check the **Create Default vHBAs** check box.
e) Click **OK**.

Cisco UCS Manager inherits and automatically applies the identity and configuration information in the server, creates the service profile, and associates it with the server.

Working with Service Profile Templates

Creating a Service Profile Template

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization where you want to create the service profile template.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the organization and select **Create Service Profile Template**.

Step 5 In the **Create Service Profile Template** wizard, complete the following:

- Page 1: Identifying the Service Profile Template, on page 30
- Page 2: Specifying the Storage Options, on page 31
- Page 3: Specifying the Networking Options, on page 36
- Page 4: Setting the vNIC/vHBA Placement, on page 41
- Page 5: Setting the Server Boot Order, on page 43
- Page 6: Adding the Maintenance Policy, on page 46
- Page 7: Specifying the Server Assignment Options, on page 47
- Page 8: Adding Operational Policies, on page 49

Page 1: Identifying the Service Profile Template

This procedure directly follows the steps in Creating a Service Profile Template, on page 30. It describes how to set the identity of a service profile template on the **Identify Service Profile Template** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 In the **Name** field, enter a unique name that you can use to identify this service profile template.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

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

Step 2 In the **Type** field, click one of the following radio buttons:

- **Initial Template**—Any service profiles created from this template are not updated if the template changes
- **Updating Template**—Any service profiles created from this template are updated if the template changes

Step 3 From the **UUID Assignment** drop-down list, choose one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool.
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.
Pools ***Pool_Name***	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.

Step 4 (Optional) In the text box, enter a description of this service profile template.
A user-defined description of the service profile template.

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

Step 5 Click **Next**.

What to Do Next

Complete the steps in Page 2: Specifying the Storage Options, on page 31.

Page 2: Specifying the Storage Options

This procedure directly follows Page 1: Identifying the Service Profile Template, on page 30. It describes how to configure the storage options for a service profile template on the **Storage** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 From the **Local Storage** drop-down list, choose one of the following:

Option	Description
Select Local Storage Policy to use	Assigns the default local disk storage policy to every service profile created from this template. Continue with Step 4.
Create a Specific Storage Policy	Enables you to create a local disk policy that can only be accessed by a service profile created from this template. Continue with Step 2.
Storage Policies *Policy_Name*	Select an existing local disk policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to every service profile created from this template. If you do not want use any of the existing policies but instead want to create a new policy that all service profiles and templates can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you chose **Create a Specific Storage Policy** and want to create a new policy that can only be used by service profiles created from this service profile template, do the following:

a) From the **Mode** drop-down list, choose one of 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 Stripes**—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.
- **RAID 6 Stripes 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 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.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

Note 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 after you apply the **No RAID** mode.

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.

b) If you want to ensure that the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile, check the **Protect Configuration** check box. 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.

c) Continue with Step 4.

Step 3 (Optional) To create a local disk configuration policy that will be available to all service profiles and templates, do the following:

a) Click the **Create Local Disk Configuration Policy** link.

b) In the **Create Local Disk Configuration** dialog box, complete the fields.
For more information, see Creating a Local Disk Configuration Policy.

c) Click **OK**.

d) From the **Local Storage** drop-down list, choose the policy you created.

Step 4 In the **How would you like to configure SAN storage?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vHBAs for every service profile created from this template. Continue with Step 5.
Expert	Allows you to create an unlimited number of vHBAs for every service profile created from this template. Continue with Step 6.
No vHBAs	Does not include any vHBAs for connections to a Fibre Channel SAN in a service profile created from this template. Continue with Step 7.

Step 5 (Optional) If you chose the simple SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.

- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) In the **vHBA 0 (Fabric A)** area, complete the following fields:

- In the **Name** field, enter a unique name for the vHBA.
- From the **Select VSAN** drop-down list, choose the name of the VSAN with which this vHBA should be associated.

If the VSAN you need is not in the drop-down list, click the **Create VSAN** link. For more information, see Creating a Named VSAN.

c) Repeat Step 7b in the **vHBA 1 (Fabric B)** area to create a VSAN for that vHBA.

d) Continue with Step 9.

Step 6 (Optional) If you chose the expert SAN storage option, do the following:

a) From the **WWNN Assignment** drop-down list, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

  You can specify a WWNN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.
- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

b) Click **Add** on the icon bar of the table to open the **Create vHBA** dialog box.

c) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	The name of this vHBA. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use SAN Connectivity Template check box	Check this check box if you want to use a template to create the vHBA. Cisco UCS Manager GUI displays the **vHBA Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more SAN connectivity templates exist in the system.

Name	Description
Create vHBA Template link	Click this link if you want to create a vHBA template.
WWPN Assignment drop-down list	If you want to: • Use the default WWPN pool, leave this field set to **Select (pool default used by default)**. • Use the WWPN assigned to the server by the manufacturer, select **Hardware Default**. • A specific WWPN, select **20:00:00:25:B5:00:00:00**, **20:XX:XX:XX:XX:XX:XX:XX**, or **5X:XX:XX:XX:XX:XX:XX:XX** and enter the WWPN in the **WWPN** field. To verify that this WWPN is available, click the corresponding link. • A WWPN from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available WWN addresses in the pool and the second is the total number of WWPN addresses in the pool. To create a new WWPN pool, click **WWPN Pool**.

d) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.
Persistent Binding field	This can be: • **disabled** • **enabled**
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
Operational Parameters Section	

Name	Description
Stats Threshold Policy drop-down list box	The threshold policy with which this vHBA is associated.

e) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

f) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 3: Specifying the Networking Options, on page 36.

Page 3: Specifying the Networking Options

This procedure directly follows Page 2: Specifying the Storage Options, on page 31. It describes how to configure the networking options, including LAN connectivity, on the **Networking** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 (Optional) If you plan to assign service profiles created from this template to a server with an adapter that supports dynamic vNICs, choose one of the following options from the **Dynamic vNIC Connection** drop-down list:

Option	Description
Select a Policy to use	Enables you to create a service profile template without a dynamic vNIC connection policy for a server with an adapter that does not support dynamic vNICs. This option does not include a dynamic vNIC connection policy in the template. Continue with Step 4.

Option	Description
Create a Specific Dynamic vNIC Connection Policy	Enables you to create a dynamic vNIC connection policy that can only be accessed by this service profile template. Continue with Step 2.
Dynamic vNIC Connection Policies *Policy_Name*	Select an existing dynamic vNIC connection policy from the list at the bottom of the drop-down list. Cisco UCS Manager assigns this policy to the service profile template. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles and templates can access, continue with Step 3. Otherwise, continue with Step 4.

Step 2 (Optional) If you clicked **Create a Specific Dynamic vNIC Connection Policy**, do the following to create a new dynamic vNIC connection policy that can only be used by service profiles created from this template:

a) Complete the following fields:

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.

b) Continue with Step 4.

Step 3 (Optional) To create a dynamic vNIC connection policy that will be available to all service profiles and templates, do the following:

a) Click **Create Dynamic vNIC Connection Policy**.
b) In the **Create Dynamic vNIC Connect Policy** dialog box, complete the fields.
For more information, see Creating a Dynamic vNIC Connection Policy.
c) Click **OK**.
d) From the **Dynamic vNIC Connection** drop-down list, choose the policy you created.
e) Continue with Step 4.

Step 4 In the **How would you like to configure LAN connectivity?** field, click one of the following options:

Option	Description
Simple	Allows you to create a maximum of two vNICs, in dual fabric mode, for every service profile created from this template. Continue with Step 5.
Expert	Allows you to create an unlimited number of vNICs for every service profile created from this template. Continue with Step 6.

Option	Description
No vNICs	Does not include any vNICs for connections to a LAN in a service profile created from this template. Any server associated with these service profiles cannot communicate with a LAN unless you modify the individual service profile later. Continue with Step 7.

Step 5 (Optional) If you chose the simple LAN connectivity option, do the following:

a) In the **vNIC 0 (Fabric A)** area:

- In the **Name** field, enter a unique name for the vNIC.
- From the **Select Native VLAN** drop-down list, choose the name of the VLAN with which this vNIC should communicate.

If the VLAN you need is not in the drop-down list, click the **Create VLAN** link. For more information, see Creating a Named VLAN.

b) Repeat Step 2a in the **vNIC 1 (Fabric B)** area to create a VLAN for that vNIC.

c) Continue with Step 4.

Step 6 If you chose the expert LAN connectivity option, do the following:

a) Click **Add** on the icon bar of the table to open the **Create vNICs** dialog box.

b) Complete the following fields to specify the identity information for the vNIC:

Name	Description
Name field	Enter a name for this vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use LAN Connectivity Template check box	Check this check box if you want to use a template to create the vNIC. Cisco UCS Manager GUI displays the **vNIC Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more LAN connectivity templates exist in the system.
Create vNIC Template link	Click this link if you want to create a vNIC template.

Name	Description
MAC Address Assignment drop-down list	If you want to: • Use the default MAC address pool, leave this field set to **Select (pool default used by default)**. • Use the MAC address assigned to the server by the manufacturer, select **Hardware Default**. • A specific MAC address, select **02:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link. • A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

c) In the **Fabric Interconnect** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not enable fabric failover for the vNIC under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • if you plan to associate this vNIC with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.

Name	Description
VLANs table	This table lists the VLANs that can be associated with this vNIC. The columns are: • **Select**—Check the check box in this column for each VLAN you want to use. • **Name**—The name of the VLAN. • **Native VLAN**—To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216.
Pin Group drop-down list	Choose the LAN pin group you want associated with this vNIC.
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Operational Parameters Section	
Stats Threshold Policy drop-down list	The statistics collection policy with which this vNIC is associated.

d) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list	The Ethernet adapter policy with which this vNIC is associated.
Create Ethernet Adapter Policy link	Click this link if you want to create an Ethernet adapter policy.
QoS drop-down list	The quality of service policy with which this vNIC is associated.
Create QoS Policy link	Click this link if you want to create a quality of service policy.
Network Control Policy drop-down list	The network control policy with which this vNIC is associated.
Create Network Control Policy Policy link	Click this link if you want to create a network control policy.

e) Click **OK**.

Step 7 Click **Next**.

What to Do Next

Complete Page 4: Setting the vNIC/vHBA Placement, on page 41.

Page 4: Setting the vNIC/vHBA Placement

This procedure directly follows Page 3: Specifying the Networking Options, on page 36. It describes how to set the vNIC and vHBA placement options on the **vNIC/vHBA Placement** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 From the **Select Placement** drop-down list, choose one of the following:

Option	Description
Let System Perform Placement	Specifies that Cisco UCS Manager determines the vNIC/vHBA placement for all servers associated with a service profile created from this template. The placement is determined by the order set in the PCI Order table. Continue with Step 2.
Specify Manually	Enables you to do the following: • Explicitly assign the vNICs and vHBAs associated with this service profile template to a virtual network interface connection (vCon). • Configure the types of vNICs and vHBAs that can be assigned to a vCon, either manually or through a vNIC/vHBA placement policy. Continue with Step 3.
vNIC/vHBA Placement Profiles ***Placement Profile Name***	Assigns an existing vNIC/vHBA placement policy to a service profile created from this template. If you choose this option, Cisco UCS Manager displays the details of the policy. If a vNIC/vHBA placement policy has not been configured in Cisco UCS Manager, this option may not display in the drop-down list. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles and templates can access, click **Create Placement Policy** and continue with Step 4. Otherwise, continue with Step 5.

Step 2 (Optional) If you chose **Let System Perform Placement**, do the following:

a) Use one or more of the following buttons to adjust the order of the vNICs and vHBAs:

Name	Description
Move Up button	Moves the selected vNIC or VHBA to a higher priority in the list.
Move Down button	Moves the selected vNIC or vHBA to a lower priority in the list.
Delete button	Deletes the selected vNIC or vHBA.
Reorder button	Returns all vNICs and vHBAs to their original order.
Modify button	Enables you to modify the currently-selected vNIC or vHBA. **Note** You can change any options for the vNIC or vHBA except its name.

b) Continue with Step 5.

Step 3 (Optional) If you chose **Specify Manually**, do the following:

a) On the appropriate tab in the **vNIC/vHBA** table, click a vNIC or vHBA.

b) In the **Virtual Host Interface** table, click a vCon row and if necessary, choose one of the following values from the **Selection Preference** column:

- **all**—All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic.
- **assigned-only**—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.
- **exclude-dynamic**—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.
- **exclude-unassigned**—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.

c) Click **Assign**.
If you need to undo an assignment, click **Remove**.

d) Repeat Steps a through c until you have assigned all vNICs and vHBAs.

e) When you have specified all vNIC and vHBA placements, continue with Step 5.

Step 4 If you clicked **Create Placement Policy**, do the following in the **Create Placement Policy** dialog box:

a) In the **Name** field, enter a unique name for the placement policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) In the **Selection Preference** column for each **Virtual Slot**, choose one of the following from the drop-down list:

- **all**—All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic.
- **assigned-only**—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.
- **exclude-dynamic**—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.
- **exclude-unassigned**—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.

c) Click **OK**.
d) After the dialog box closes, choose the policy you created from the **Select Placement** drop-down list.

Step 5 Click **Next**.

What to Do Next

Complete Page 5: Setting the Server Boot Order, on page 43

Page 5: Setting the Server Boot Order

This procedure directly follows Page 4: Setting the vNIC/vHBA Placement, on page 41. It describes how to set the server boot order options on the **Server Boot Order** page of the **Create Service Profile Template** wizard.

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.

Procedure

Step 1 From the **Boot Policy** drop-down list, choose one of the following:

Option	Description
Select Boot Policy to use	Assigns the default boot policy to every service profile created from this template. Continue with Step 9.

Option	Description
Create a Specific Boot Policy	Enables you to create a local boot policy that can only be accessed by a service profile created from this template. Continue with Step 3.
Boot Policies *Policy_Name*	Assigns an existing boot policy to every service profile created from this template. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles and templates can access, continue with Step 2. Otherwise, choose a policy from the list and continue with Step 9.

Step 2 If you clicked **Create Boot Policy** to create a boot policy that all service profiles and templates can use, do the following:

a) In the **Create Boot Policy** dialog box, enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

b) Continue with Step 3.

Step 3 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 4 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 5 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.

b) Click one of the following links to add the device to the **Boot Order** table:

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

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 6 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.

b) Click the **Add LAN Boot** link.

c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.

d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 7 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.

b) Click the **Add SAN Boot** link.
c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 8 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Boot Policy** drop-down list.

Step 9 Click **Next**.

What to Do Next

Complete Page 6: Adding the Maintenance Policy, on page 46.

Page 6: Adding the Maintenance Policy

This procedure directly follows Page 5: Setting the Server Boot Order, on page 43. It describes how to add a maintenance policy to the service profile on the **Maintenance Policy** page of the **Create Service Profile (expert)** wizard.

Procedure

Step 1 From the **Maintenance Policy** drop-down list, choose one of the following:

Option	Description
Select a Maintenance Policy to Use (default policy shown)	Assigns the default maintenance policy to this service profile. Continue with Step 4.
Maintenance Policies ***Policy_Name***	Assigns an existing maintenance policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies but instead want to create a policy that all service profiles can access, click **Create Maintenance Policy** and continue with Step 2. Otherwise, choose a policy from the list and continue with Step 4.

Step 2 If you clicked **Create Maintenance Policy** to create a maintenance policy that all service profiles and templates can use, do the following:

a) In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (backslash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark).

Name	Description
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, the server needs to be rebooted to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be: • **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. • **timer-automatic**—Cisco UCS defers all service profile associations and changes until the maintenance window defined by the schedule shown in the **Schedule** field.
Schedule drop-down list	If the **Reboot Policy** is set to **timer-automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.

b) Click **OK** and continue with Step 3.

Step 3 If you created a new boot policy accessible to all service profiles and template, select that policy from the **Maintenance Policy** drop-down list.

Step 4 Click **Next**.

What to Do Next

Complete Page 7: Specifying the Server Assignment, on page 21.

Page 7: Specifying the Server Assignment Options

This procedure directly follows Page 6: Adding the Maintenance Policy, on page 46. It describes how to specify the way a server is assigned to a service profile created from this template on the **Server Assignment** page of the **Create Service Profile Template** wizard.

Procedure

Step 1 From the **Server Assignment** drop-down list, choose one of the following:

Option	Description
Assign Later	Allows you to assign a server after you have created and configured the service profile template. Continue with Step 2.
Select from a Pool ***Pool_Name***	Select a server pool from the list at the bottom of the drop-down list. Cisco UCS Manager assigns a server from this pool to a service profile created from this template. Continue with Step 2.

Step 2 In the **Power State** field, click one of the following radio buttons to set the power state that will be applied to the server when it is associated with a service profile created from this template:

- **Down** if you want the server to be powered down before the profile is associated with the server
- **Up** if you want the server to be powered up before the profile is associated with the server

By default, the server is powered up.

Step 3 If you want to restrict the migration of the service profile after it has been associated with a server, check the **Restrict Migration.** check box.
If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association may fail.

Step 4 (Optional) In the **Firmware Management** area, do the following to use policies to update the firmware on the server associated with a service profile created from this template:

a) Click the down arrows on the **Firmware Management** bar.
b) Complete the following fields:

Name	Description
Host Firmware drop-down list	To associate a host firmware package with this service profile, choose its name from the drop-down list.
Create Host Firmware Package link	Click this link if you want to create a host firmware package.
Management Firmware drop-down list	To associate a management firmware package with this service profile, choose its name from the drop-down list.
Create Management Firmware Package link	Click this link if you want to create a management firmware package.

Step 5 Click **Next**.

What to Do Next

Complete Page 8: Adding Operational Policies, on page 49.

Page 8: Adding Operational Policies

This procedure directly follows Page 7: Specifying the Server Assignment Options, on page 47. It describes how to add operational policies to the service profile template on the **Operational Policies** page of the **Create Service Profile Template** wizard. These policies are optional.

Procedure

Step 1 To override the default BIOS settings and configure them through the service profile, click the down arrows to expand the **BIOS Configuration** bar and do one of the following:

- To add an existing policy, select the desired BIOS policy from the **BIOS Policy** drop-down list .
- To create a BIOS policy that is available to all service profiles, click **Create BIOS Policy**, complete the fields in the dialog box, and then select the desired BIOS policy from the **BIOS Policy** drop-down list .

For more information about how to create a BIOS policy, see Creating a BIOS Policy.

Step 2 To provide external access to the CIMC on the server, click the down arrows to expand the **External IPMI Management Configuration** bar and add an IPMI profile and a serial over LAN policy.
If you do not want to provide external access, continue with Step 4.

Step 3 To add an IPMI profile to service profiles created from this template, do one of the following:

- To add an existing policy, select the desired IPMI profile from the **IPMI Access Profile** drop-down list.
- If the **IPMI Access Profile** drop-down list does not include an IPMI profile with the desired user access, click the **Create Access IPMI Profile** link to create an IPMI profile that is available to all service profiles and then select that profile from the **IPMI Access Profile** drop-down list.

For more information about how to create an IPMI profile, see Creating an IPMI Access Profile.

Step 4 To add a Serial over LAN policy to service profiles created from this template, do one of the following:

- To add an existing policy, select the desired Serial over LAN policy from the **SoL Configuration Profile** drop-down list.
- To create a Serial over LAN policy that is only available to service profile created from this template, select **Create a Specific SoL Policy** from the **SoL Configuration Profile** drop-down list and complete the **Admin State** field and the **Speed** drop-down list.
- To create a Serial over LAN policy that is available to all service profile templates, click the **Create Serial over LAN Policy** link and complete the fields in the dialog box and then select that policy from the **SoL Configuration Profile** drop-down list.

For more information about how to create a serial over LAN policy, see Creating a Serial over LAN Policy.

Step 5 To configure the management IP required for external access to the CIMC on the server, click the down arrows to expand the **Management IP Address** bar and click one of the following radio buttons:

- **none**—No management IP address is assigned to the service profile. The management IP address is set based on the CIMC management IP address settings on the server.
- **pooled**—A management IP address is assigned to the service profile from the management IP address pool.

Step 6 To monitor thresholds and collect statistics for the associated server, click the down arrows to expand the **Monitoring Configuration** bar and do one of the following:

- To add an existing policy, select the desired threshold policy from the **Threshold Policy** drop-down list.
- To create a threshold policy that is available to all service profiles, click the **Create Threshold Policy** link, complete the fields in the dialog box, and then select that policy from the **Threshold Policy** drop-down list.

For more information about how to create a threshold policy, see Creating a Server and Server Component Threshold Policy.

Step 7 To associate a power control policy with the service profile template, click the down arrows to expand the **Power Control Policy Configuration** bar and do one of the following:

- To add an existing policy, select the desired power control policy from the **Power Control Policy** drop-down list.
- To create a power control policy that is available to all service profiles and templatesw, click the **Create Power Control Policy** link , complete the fields in the dialog box, and then select that policy from the **Power Control Policy** drop-down list.

For more information about how to create a power control policy, see Creating a Power Control Policy.

Step 8 To associate a scrub policy with the service profile template, click the down arrows to expand the **Scrub Policy** bar and do one of the following:

- To add an existing policy, select the desired scrub policy from the **Scrub Policy** drop-down list .
- To create a scrub policy that is available to all service profiles and templates, click the **Create Scrub Policy** link , complete the fields in the dialog box, and then select that policy from the **Scrub Policy** drop-down list .

For more information about how to create a scrub policy, see Creating a Scrub Policy.

Step 9 Click **Finish**.

Creating One or More Service Profiles from a Service Profile Template

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template that you want to use as the basis for your service profiles.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile template from which you want to create the profiles and select **Create Service Profiles From Template**.

Step 5 In the **Create Service Profiles From Template** dialog box, complete the following fields:

Name	Description
Naming Prefix field	The prefix to use for the template name. When the system creates the service profile, it appends a unique numeric identifier to this prefix. For example, if you specify the prefix MyProfile and request two profiles, the first service profile would be called MyProfile1 and the second would be MyProfile2. If you return at a later date and create three more profiles with the same prefix, they would be named MyProfile3, MyProfile4, and MyProfile5.
Number field	The number of service profiles to create.

Step 6 Click **OK**.

Creating a Template Based Service Profile for a Blade Server

Before You Begin

A qualified service profile template with the desired values must exist in Cisco UCS Manager.

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.

Step 3 Choose the server for which you want to create a template based service profile.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Create Service Profile**.

Step 6 In the **Create Service Profile for Server** dialog box, do the following:

a) Click the **Template Based Service Profile** radio button.
b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
c) From the **Service Profile Template** drop-down list, select the template from which you want to create the service profile associated with this server.
d) Click **OK**.

Creating a Template Based Service Profile for a Rack-Mount Server

Before You Begin

A qualified service profile template with the desired values must exist in Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment** > **Rack Mounts** > **Servers**.
Step 3 Choose the server for which you want to create a template based service profile.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Create Service Profile**.
Step 6 In the **Create Service Profile for Server** dialog box, do the following:
a) Click the **Template Based Service Profile** radio button.
b) In the **Name** field, enter a unique name for the service profile.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
c) From the **Service Profile Template** drop-down list, select the template from which you want to create the service profile associated with this server.
d) Click **OK**.

Creating a Service Profile Template from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.
Step 3 Expand the node for the organization that contains the service profile that you want to use as the basis for your template.

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

Step 4 Right-click the service profile from which you want to create the template and select **Create a Service Profile Template**.

Step 5 In the **Create Template From Service Profile** dialog box, complete the following fields:

Name	Description
Service Profile Template Name field	The name of the service profile template. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Org drop-down list	Select the organization that you want this template to be associated with.
Type field	This can be: • **Initial Template**—Any service profiles created from this template are not updated if the template changes • **Updating Template**—Any service profiles created from this template are updated if the template changes

Step 6 Click **OK**.

Managing Service Profiles

Cloning a Service Profile

Procedure

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

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

Step 3 Expand the node for the organization where you want to create the service profile.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile you want to clone and select **Create a Clone**.

Step 5 In the **Create Clone From Service Profile** dialog box:

a) Enter the name you want to use for the new profile in the **Clone Name** field.
This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

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

b) Click **OK**.

Step 6 Navigate to the service profile you just created and make sure that all options are correct.

Associating a Service Profile with a Server or Server Pool

Follow this procedure if you did not associate the service profile with a blade server or server pool when you created it, or to change the blade server or server pool with which a service profile is associated.

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile that you want to associate with a new server or server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile you want to associate with a server and select **Change Service Profile Association**.

Step 5 In the **Associate Service Profile** dialog box, select one of the following options:

Option	Description
Server Pool	Select a server pool from the drop-down list. Cisco UCS Manager assigns a server from this pool to the service profile. Continue with Step 7.
Server	Navigate to the desired available server in the navigation tree and select the server which will be assigned to the service profile. Continue with Step 7.
Custom Server	Specifies the chassis and slot that contains the server that will be assigned to the service profile. If the server is not in the slot or is otherwise unavailable, the service profile will be associated with the server when it becomes available. Continue with Step 6.

Step 6 If you chose **Custom Server**, do the following:

a) In the **Chassis Id** field, enter the number of the chassis where the selected server is located.

b) In the **Server Id** field, enter the number of the slot where the selected server is located.

Step 7 If you want to restrict the migration of the service profile after it has been associated with a server, check the **Restrict Migration.** check box.
If you choose not to restrict migration, Cisco UCS Manager does not perform any compatibility checks on the new server before migrating the existing service profile. If the hardware of both servers are not similar, the association may fail.

Step 8 Click **OK**.

Disassociating a Service Profile from a Server or Server Pool

When you disassociate a service profile, Cisco UCS Manager attempts to shutdown the operating system on the server. If the operating system does not shutdown within a reasonable length of time, Cisco UCS Manager forces the server to shutdown.

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile that you want to disassociate from a server or server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile you want to disassociate from a server and select **Disassociate Service Profile**.

Step 5 In the **Disassociate Service Profile** dialog box, click **Yes** to confirm that you want to disassociate the service profile.

Step 6 (Optional) Monitor the status and FSM for the server to confirm that the disassociation completed.

Associating a Service Profile Template with a Server Pool

Follow this procedure if you did not associate the service profile template with a server pool when you created it, or to change the server pool with which a service profile created from this template is associated.

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile that you want to associate with a server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile template you want to associate with a server pool and select **Associate with Server Pool**.
The **Associate with Server Pool** dialog box opens.

Step 5 From the **Server Pool** section of the **Pool Assignment** drop-down list, select a server pool.
If you select **Assign Later**, the service profile template is not associated with a server pool.

Step 6 Select one of the following radio buttons to determine the power state applied to a server which is associated with a service profile created from this template:

- **Down**
- **Up**

Step 7 From the **Select Qualification** drop-down list, select the server pool policy qualifications you want to apply to a server that is associated with a service profile created from this template.

Step 8 Click **OK**.

Disassociating a Service Profile Template from its Server Pool

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile that you want to disassociate from its server pool.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the service profile template you want to disassociate from its server pool and select **Disassociate Template**.

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

Changing the UUID in a Service Profile

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to change the UUID.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile that requires the UUID for the associated server to be changed.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Change UUID**.

Step 7 From the **UUID Assignment** drop-down list, do one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool. Continue with Step 9.

Option	Description
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server. Continue with Step 9.
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	Uses the UUID that you manually assign. Continue with Step 8.
Pools *Pool_Name*	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool. Continue with Step 9.

Step 8 (Optional) If you selected the **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** option, do the following:

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

b) To verify that the selected UUID is available, click the **here** link.

Step 9 Click **OK**.

Changing the UUID in a Service Profile Template

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template for which you want to change the UUID.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Choose the service profile template whose UUID assignment you want to change.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Change UUID**.

Step 7 From the **UUID Assignment** drop-down list, choose one of the following:

Option	Description
Select (pool default used by default)	Assigns a UUID from the default UUID Suffix pool.
Hardware Default	Uses the UUID assigned to the server by the manufacturer. If you choose this option, the UUID remains unassigned until the service profile is associated with a server. At that point, the UUID is set to the UUID value assigned to the server by the manufacturer. If the service profile is later moved to a different server, the UUID is changed to match the new server.
Pools ***Pool_Name***	Assigns a UUID from the UUID Suffix pool that you select from the list at the bottom of the drop-down list. Each pool name is followed by two numbers in parentheses that show the number of UUIDs still available in the pool and the total number of UUIDs in the pool.

Step 8 Click **OK**.

Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template

If you change the UUID suffix pool assigned to an updating service profile template, Cisco UCS Manager does not change the UUID assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a UUID from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the UUID. You can only reset the UUID assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a UUID assigned from a UUID suffix pool.
- The UUID suffix pool name is specified in the service profile. For example, the pool name is not empty.
- The UUID value is not 0, and is therefore not derived from the server hardware.

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to reset the UUID.

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

Step 4 Choose the service profile that requires the UUID for the associated server to be reset to a different UUID suffix pool.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Reset UUID**.
If this action is not visible, then the UUID configuration in the service profile does not meet the requirements for resetting a UUID.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 Click **OK**

Modifying the Boot Order in a Service Profile

Procedure

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

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

Step 3 Expand the node for the organization that includes the service profile for which you want to change the boot order.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile for which you want to change the boot order.

Step 5 In the **Work** pane, click the **Boot Order** tab.

Step 6 Click **Modify Boot Policy** to change the existing boot policy.

Step 7 In the **Modify Boot Policy** dialog box, choose one of the following from the **Boot Policy** drop-down list:

Option	Description
Select Boot Policy to use	Assigns the default boot policy to this service profile. Continue with Step 14.
Create a Specific Boot Policy	Enables you to create a local boot policy that can only be accessed by this service profile. Continue with Step 8.
Boot Policies *Policy_Name*	Assigns an existing boot policy to the service profile. If you choose this option, Cisco UCS Manager displays the details of the policy. If you do not want use any of the existing policies, but instead want to create a policy that all service profiles can access, click **Create Boot Policy** and continue with Step 2. Otherwise, continue with Step 14.

Step 8 If you chose to create a boot policy, in the **Create Boot Policy** dialog box, enter a unique name and description for the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 9 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.
In the Cisco UCS Manager GUI, if the **Reboot on Boot Order Change** check box is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, deleting or adding the device does not directly affect the boot order and the server does not reboot.

Step 10 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 11 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order, do the following:

a) Click the down arrows to expand the **Local Devices** area.
b) Click one of the following links to add the device to the **Boot Order** table:

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

c) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 12 To add a LAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vNICs** area.
b) Click the **Add LAN Boot** link.
c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.
d) Add another device to the **Boot Order** table, or click **OK** to finish.

Step 13 To add a SAN boot to the boot order, do the following:

a) Click the down arrows to expand the **vHBAs** area.
b) Click the **Add SAN Boot** link.
c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.

e) Add another boot device to the **Boot Order** table, or click **OK** to finish.

Step 14 Click **OK**.

Creating a vNIC for a Service Profile

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to create a vNIC.

Step 4 Expand the service profile for which you want to create a vNIC.

Step 5 Right-click the **vNICs** node and choose **Create vNICs**.

Step 6 In the **Create vNICs** dialog box, do the following:

a) Complete the following fields to specify the identity information for the vNIC:

Name	Description
Name field	Enter a name for this vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Use LAN Connectivity Template check box	Check this check box if you want to use a template to create the vNIC. Cisco UCS Manager GUI displays the **vNIC Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more LAN connectivity templates exist in the system.
Create vNIC Template link	Click this link if you want to create a vNIC template.
MAC Address Assignment drop-down list	If you want to: • Use the default MAC address pool, leave this field set to **Select (pool default used by default)**. • Use the MAC address assigned to the server by the manufacturer, select **Hardware Default**. • A specific MAC address, select **02:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link. • A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

b) Complete the following fields to specify the fabric connection information:

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not enable fabric failover for the vNIC under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • if you plan to associate this vNIC with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
VLANs table	This table lists the VLANs that can be associated with this vNIC. The columns are: • **Select**—Check the check box in this column for each VLAN you want to use. • **Name**—The name of the VLAN. • **Native VLAN**—To designate one of the VLANs as the native VLAN, click the radio button in this column.
Create VLAN link	Click this link if you want to create a VLAN.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216.
Pin Group drop-down list	Choose the LAN pin group you want associated with this vNIC.
Create LAN Pin Group link	Click this link if you want to create a LAN pin group.
Operational Parameters Section	
Stats Threshold Policy drop-down list	The statistics collection policy with which this vNIC is associated.

c) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list	The Ethernet adapter policy with which this vNIC is associated.
Create Ethernet Adapter Policy link	Click this link if you want to create an Ethernet adapter policy.
QoS drop-down list	The quality of service policy with which this vNIC is associated.
Create QoS Policy link	Click this link if you want to create a quality of service policy.
Network Control Policy drop-down list	The network control policy with which this vNIC is associated.
Create Network Control Policy Policy link	Click this link if you want to create a network control policy.

d) Click **OK**.

Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template

If you change the MAC pool assigned to an updating service profile template, Cisco UCS Manager does not change the MAC address assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a MAC address from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the MAC address. You can only reset the MAC address assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a MAC address assigned from a MAC pool.
- The MAC pool name is specified in the service profile. For example, the pool name is not empty.
- The MAC address value is not 0, and is therefore not derived from the server hardware.

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to reset the MAC address.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand *Service_Profile_Name* > **vNICs**.
Step 5 Click the vNIC for which you want to reset the MAC address.
Step 6 In the **Work** pane, click the **General** tab.
Step 7 In the **Actions** area, click **Reset MAC Address**.
Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **OK**.

Deleting a vNIC from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.
Step 3 Expand the node for the organization that contains the service profile from which you want to delete a vNIC.
Step 4 Expand the service profile from which you want to delete a vNIC.
Step 5 Expand the **vNICs** node.
Step 6 Right-click the vNIC you want to delete and choose **Delete**.
Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Creating a vHBA for a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.
Step 3 Expand the node for the organization that contains the service profile for which you want to create a vHBA.
Step 4 Expand the service profile for which you want to create a vHBA.
Step 5 Right-click the **vHBAs** node and choose **Create vHBAs**.
Step 6 In the **Create vHBAs** dialog box, do the following:
a) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	The name of this vHBA. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Name	Description
Use SAN Connectivity Template check box	Check this check box if you want to use a template to create the vHBA. Cisco UCS Manager GUI displays the **vHBA Template** drop-down list from which you can select the appropriate template, and the **Adapter Performance Profile** area from which you can select an adapter profile. **Note** You can only select this option if one or more SAN connectivity templates exist in the system.
Create vHBA Template link	Click this link if you want to create a vHBA template.
WWPN Assignment drop-down list	If you want to: • Use the default WWPN pool, leave this field set to **Select (pool default used by default)**. • Use the WWPN assigned to the server by the manufacturer, select **Hardware Default**. • A specific WWPN, select **20:00:00:25:B5:00:00:00**, **20:XX:XX:XX:XX:XX:XX:XX**, or **5X:XX:XX:XX:XX:XX:XX:XX** and enter the WWPN in the **WWPN** field. To verify that this WWPN is available, click the corresponding link. • A WWPN from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available WWN addresses in the pool and the second is the total number of WWPN addresses in the pool. To create a new WWPN pool, click **WWPN Pool**.

b) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.

Name	Description
Persistent Binding field	This can be: • **disabled** • **enabled**
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
Operational Parameters Section	
Stats Threshold Policy drop-down list box	The threshold policy with which this vHBA is associated.

c) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

d) Click **OK**.

Changing the WWPN for a vHBA

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to change the WWPN.

Step 4 Expand ***Service_Profile_Name*** > **vHBAs**.

Step 5 Click the vHBA for which you want to change the WWPN.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Change World Wide Name**.

Step 8 In the **Change World Wide Port Name** dialog box, do the following:

a) From the **WWPN Assignment** drop-down list , do one of the following:

- Use the default WWPN pool, choose **Select (pool default used by default)**.
- Use a WWPN derived from the manufacturers specifications, choose **Hardware Default**.
- A specific WWPN, choose **20:00:00:25:B5:00:00:00** and enter the WWNN in the **WWPN** field.
- A WWPN from a pool, select the pool name from the list. Each pool name is followed by number of available/total WWPNs in the pool.

b) Click **OK**.

Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template

If you change the WWPN pool assigned to an updating service profile template, Cisco UCS Manager does not change the WWPN assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a WWPN from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the WWPN. You can only reset the WWPN assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a WWPN assigned from a WWPN pool.
- The WWPN pool name is specified in the service profile. For example, the pool name is not empty.
- The WWPN value is not 0, and is therefore not derived from the server hardware.

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to reset the WWPN. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** > **vHBAs**.

Step 5 Click the vHBA for which you want to reset the WWPN.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Reset WWPN**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **OK**.

Clearing Persistent Binding for a vHBA

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile for which you want to modify the vHBA.

Step 4 Expand ***Service_Profile_Name*** > **vHBAs**.

Step 5 Click the vHBA for which you want to clear the persistent binding.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Clear Persistent Binding**.

Step 8 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a vHBA from a Service Profile

Procedure

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

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

Step 3 Expand the node for the organization that contains the service profile from which you want to delete a vHBA.

Step 4 Expand the service profile from which you want to delete a vHBA.

Step 5 Expand the **vHBAs** node.

Step 6 Right-click the vHBA you want to delete and choose **Delete**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Binding a Service Profile to a Service Profile Template

You can bind a service profile to a service profile template. When you bind the service profile to a template, Cisco UCS Manager configures the service profile with the values defined in the service profile template. If the existing service profile configuration does not match the template, Cisco UCS Manager reconfigures the service profile. You can only change the configuration of a bound service profile through the associated template.

Procedure

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

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

Step 3 Expand the node for the organization that includes the service profile you want to bind.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile you want to bind.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Bind to a Template**.

Step 7 In the **Bind to a Service Profile Template** dialog box, do the following:

a) From the **Service Profile Template** drop-down list, choose the template to which you want to bind the service profile.

b) Click **OK**.

Unbinding a Service Profile from a Service Profile Template

Procedure

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

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

Step 3 Expand the node for the organization that includes the service profile you want to unbind.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile you want to unbind.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Unbind from the Template**.

Step 7 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Service Profile

Procedure

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

Step 2 In the **Servers** tab, expand **Servers** > **Service Profiles** > *Organization_Name* .

Step 3 Right-click the service profile you want to delete and select **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 5 Click **OK**.