Configuring Network Connections

This chapter contains the following sections:

Global VLANs

You can define global VLANs in the domain group root, or a domain group below the root. Global VLANs can only be common or global. You cannot assign them to a specific fabric interconnect.

Resolution of global VLANs takes place prior to the deployment of global service profiles. If a global service profile references a global VLAN, and that VLAN does not exist, deployment of the global service profile fails due to insufficient resources. All global VLANs created in a Cisco UCS Central account must be resolved before deploying the global service profile.

All global VLANs configured in a Cisco UCS Central account are common to the domains in which they are created. However, organization permissions must first be assigned before the Cisco UCS domains that are part of the organizations can consume the resources. By default, no organization permissions are assigned when you create a global VLAN. Once organization permissions have been granted to a VLAN, it becomes visible to those organizations. It is also available to be referenced in service profiles that are part of those organizations.

A global VLAN is visible to a Cisco UCS Manager account only if you deploy a global service profile that references the VLANs. Once a VLAN that is deployed with a global service profile becomes available in a Cisco UCS Manager account, you can include it in a local service profile and policy. You cannot turn a global VLAN into a local VLAN.

A global VLAN is not deleted when you delete a global service profile that references it. Delete the global VLAN from the Cisco UCS Central account.

Creating a Global VLAN

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

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

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

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

Step 5 Click **Common VLANs**.

Step 6 Click **Add**.

Step 7 On the **Add VLAN** screen, do the following:

a) In the **VLAN Name** field, enter a unique name for the VLAN.
The VLAN name is case-sensitive.

b) In the **VLAN ID** field, enter a unique identifier to be assigned to the network.
A VLAN ID can:

- Be between 1 and 3967
- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups
- The VLAN IDs you specify must also be supported on the switch that you are using.

c) From the **Fabric ID** drop-down list, choose the the Fabric ID.

d) In the **Domain Group** field, check the check box for the domain group in which you want to create the global VLAN.

e) Click **Submit**.

Publishing a Global VLAN

Global VLANs can be published to the associated domains, and those VLANs are then available at domain level. For a VLAN associated to a domain group (x), it can be published to any of the domains linked with the same domain group (x).

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.
Step 5 Click **Common VLANs**.
Step 6 From the list of VLANs, select the VLAN to be published.
Step 7 From the **More Actions** drop-down list, choose **Publish to USC Domain**.
Step 8 On the **Publish VLAN to USC Domain** screen, click the **Select** button.
Step 9 From the Select list, click the check box of the desired domain and click the **Select** button.
Step 10 In the **Publish VLAN to USC Domain**, click the **Submit** button.

Modifying Organization Permissions for a Global VLAN

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.
Step 5 Click the **Common VLANs**.
Step 6 Click the row for the global VLAN for which you want to modify organization permissions.
Step 7 From the **More Actions** drop-down list, choose **Modify Org Permissions**.
Step 8 On the **Organization List** screen, check the check boxes for the organizations in which you want to include the global VLAN.
Step 9 Click **Submit**.

IP Pools

IP pools are a collection of IP addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

- For external management of Cisco UCS Manager servers.
- For iSCSI boot initiators.
- For both external management and iSCSI boot initiators in Cisco UCS Manager

Creating an IP Pool

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

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

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

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

Step 5 Click **Organizations**.

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

Step 7 Click **IP Pools**.

Step 8 Click **Add**.

Step 9 On the **IP Pool** screen, enter a name and description for the IP pool.

Step 10 Expand the **IPv4 Block** field, enter the following:

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

Name	Description
Scope	Whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following: **public** -The IP addresses in the block can be assigned to only one registered Cisco UCS domain. **private** -The IP addresses in the block can be assigned to multiple registered Cisco UCS domains.
ID Range Qualification Policy	Optional

Step 11 Expand the **IPv6 Block** field, enter the following:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the block.
Subnet Mask field	The subnet mask associated with the IP addresses in the block.
Default Gateway field	The default gateway associated with the IP addresses in the block.
Primary DNS field	The primary DNS server that this block of IP addresses is to access.
Secondary DNS	The secondary DNS server that this block of IP addresses is to access.
Scope	Whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following: **public** -The IP addresses in the block can be assigned to only one registered Cisco UCS domain. **private** -The IP addresses in the block can be assigned to multiple registered Cisco UCS domains.
ID Range Qualification Policy	Optional

Step 12 Click **Submit**.

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their Layer 2 environment and are available to be assigned to vNICs on a server. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multitenancy, you can use the organizational hierarchy to ensure that MAC pools can be used only by specific applications or business services. Cisco UCS uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Creating a MAC Pool

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

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 Click **Submit**.

Adding an Address Block to a MAC Pool

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

Name	Description
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.
IP Range Qualification Policy drop-down list	Choose the IP Range Qualification Policy.

Step 10 Click **Submit**.

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

A VM-FEX port profile is not automatically created with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM.

You need to include this policy in a service profile for it to take effect.

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Because the second Ethernet interface is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Creating a vNIC Template

Before You Begin

One or more of the following resources must exist:

- Global VLAN
- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy

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

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

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

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

Step 5 Click **Organization**.

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

Step 7 Click **vNIC Templates**.

Step 8 Click **Add**.

Step 9 On the **Add vNIC Template** screen, enter a unique name and description for the policy.

Step 10 From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with vNICs created from this template.

Step 11 Check the **Enable Failover** check box if you want vNICs created from this template to be able to access the other fabric interconnect if the chosen one is unavailable.

Note Do not enable vNIC fabric failover 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 one or more vNICs created from this template 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, a configuration fault is generated when you associate the service profile with the server.

Step 12 Check one or both of the following **Target** check boxes to determine whether or not a VM-FEX port profile is automatically created with the appropriate settings for the vNIC template:

- **Adapter—**The vNICs apply to all adapters. No VM-FEX port profile is created if you choose this option.
- **VM—**The vNICs apply to all virtual machines. A VM-FEX port profile is created if you choose this option.

Step 13 From the **Template Type** drop-down list, choose one of the following:

- **Initial Template—**vNICs created from this template are not updated if the template changes.
- **Updating Template—**vNICs created from this template are updated if the template changes.

Step 14 Expand the **VLANs**, do the following to select the VLAN to be assigned to vNICs created from this template:

a) Click +. This displays the **Add Entry to VLANs**dialog box.
b) In the **Add Entry to VLANs** dialog box, complete the following fields and click **Submit**:

- **Name** drop-down list**—**Choose the VLAN that you want to associate with the vNIC template.
- **Set as Native VLAN** check box**—**Check the check box if you want this VLAN to be the native VLAN for the port.

Step 15 To associate policies with vNICs created from this template, complete the following fields:

Name	Description
MTU field	The MTU, or packet size, that vNICs created from this vNIC template must use. Enter an integer between 1500 and 9216. **Note** If the vNIC template has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets might be dropped during data transmission.
MAC Pool drop-down list	Choose the MAC address pool that vNICs created from this vNIC template should use.
QoS Policy drop-down list	Choose the quality of service policy that vNICs created from this vNIC template should use.
Network Control Policy drop-down list	Choose the network control policy that vNICs created from this vNIC template should use.
Pin Group drop-down list	Choose the LAN pin group that vNICs created from this vNIC template should use.
Stats Threshold Policy drop-down list	Choose the statistics collection policy that vNICs created from this vNIC template should use.

Step 16 Click **Submit**.

What to Do Next

Include the vNIC template in a vNIC policy.

Creating a vNIC Policy

Before You Begin

Make sure that at least one of the following exists in the Cisco UCS Central account and organization to which this policy applies:

- vNIC template
- Ethernet adapter policy

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Central**.

Step 2 Click **vNIC**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central vNIC Policy** screen, do the following:

a) In the **vNIC Name** field, enter a unique name for the policy.
b) From the **Account Name** drop-down list, choose a Cisco UCS Central account to which this policy applies.
c) From the **Organization** drop-down list, choose the organization to which this policy applies.
The **Use LAN Connectivity** checkbox, is selected by default.
d) From the **vNIC Template** drop-down list, choose a vNIC template.
e) From the **Adapter Policy** drop-down list, choose an adapter policy.
f) Click **Submit.**

What to Do Next

Include the vNIC policy in a network policy.

LAN Connectivity Policy

LAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Creating a LAN Connectivity Policy

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

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

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

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

Step 5 Click **Organization**.

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

Step 7 Click **LAN Connectivity Policies**.

Step 8 Click **Add**.

Step 9 On the **LAN Connectivity Policy** screen, enter a name and description for the policy.

Step 10 Expand **vNICs**, click **Add** and do the following:

a) Enter a name for the vNIC.

b) To use a vNIC template to create the vNIC, check the **Use vNIC Template** check box. Select the appropriate template and adapter policy from the drop-down lists that are displayed.

c) To create a new vNIC without a template, do not check the **Use vNIC Template** check box and complete the fields that are displayed.
For more information about these fields, see Creating a vNIC Template, on page 8.

d) Click **Submit**.

Repeat this step if you want to add more vNICs to the LAN Connectivity policy.

Step 11 After you have created all vNICs required for the policy, click **Submit**.

Network Policy

The network policy is a Cisco UCS Director policy that configures the connections between a server and the LAN, including the virtual network interface cards (vNICs) used by the server. Depending upon the configuration you choose, this policy can be used to configure two or more vNICs for the server. You can choose to create the vNICs in this policy or use a LAN connectivity policy to determine the vNIC configuration.

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

Creating a Network Policy

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Central**.

Step 2 Click **Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central Network Policy** screen, enter a name and description for the policy.

Step 5 Complete the following fields to specify the Cisco UCS Central connections for the policy:

- **UCS Central Account Name** drop-down list—Choose the Cisco UCS Central account to which you want to add this policy.
- **UCS Central Organization Name** drop-down list—Choose the Cisco UCS Central organization to which you want to add this policy.

Step 6 If this policy is to be assigned to service profiles for servers that support dynamic vNICs, choose a dynamic vNIC connection policy from the **Dynamic vNIC Connection Policy** drop-down list.

Step 7 From the **LAN Connectivity Type** drop-down list, choose one of the following connectivity types:

Option	Description
Expert	Allows you to create up to 10 vNICs that the server can use to access the LAN. Continue with Step 8.
Simple	Allows you to create a maximum of two vNICs that the server can use to access the LAN. Continue with Step 9.
No vNICs	Does not allow you to create any vNICs. If you choose this option, any server associated with a service profile that includes this policy is not connected to the LAN. Continue with Step 11.
Hardware Inherited	Uses the vNICs assigned to the Ethernet adapter profile associated with the server. Continue with Step 11.
Use LAN Connectivity Policy	Uses a LAN connectivity policy to determine the LAN connectivity for the server. Continue with Step 10.

Step 8 If you chose the expert LAN option, do the following:

a) In the **Add vNIC** field, specify the number of vNICs that you want to add to the network policy. Up to 10 vNICs can be created.
b) From the **Template For vNIC1 ... vNIC10** drop-down list, choose a vNIC policy.
c) Continue with Step 11.

Step 9 If you chose the simple LAN option, do the following:

a) In the **vNIC0 (Fabric A)** area, complete the following fields:

- In the **vNIC0 Name** field, enter a unique name for the vNIC.
- From the **Select VLAN** drop-down list, choose the name of the VLAN with which this vNIC should be associated.

b) In the **vNIC1 (Fabric B)** area, complete the following fields:

- In the **vNIC1 Name** field, enter a unique name for the vNIC.
- From the **Select VLAN** drop-down list, choose the name of the VLAN with which this vNIC should be associated.

c) Continue with Step 11.

Step 10 If you chose the LAN connectivity policy option, choose the policy that you want to associate with the server from the **LAN Connectivity Policy** drop-down list.

Step 11 Click **Submit**.

What to Do Next

Include the network policy in a service profile.