



Configuring Network-Related Policies

This chapter includes the following sections:

- [Configuring vNIC Templates, page 1](#)
- [Configuring Ethernet Adapter Policies, page 6](#)
- [Configuring Network Control Policies, page 11](#)

Configuring vNIC Templates

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.

Beginning in Cisco UCS, Release 2.0(2), Cisco UCS Manager does not automatically create a VM-FEX port profile 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. Then because the second eth 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

This policy requires that one or more of the following resources already exist in the system:

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

Procedure

- Step 1** In the **Navigation** pane, click the **LAN** tab.
- Step 2** On the **LAN** tab, expand **LAN > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the **root** node.
- Step 4** Right-click the **vNIC Templates** node and choose **Create vNIC Template**.
- Step 5** In the **Create vNIC Template** dialog box:
- a) In the **General** area, complete the following fields:

Name	Description
Name field	<p>The name of the vNIC template.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</p>
Description field	<p>A user-defined description of the template.</p> <p>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), or = (equal sign).</p>

Name	Description
Fabric ID field	<p>The fabric interconnect associated with the component.</p> <p>If you want vNICs created from this template to be able to access the second fabric interconnect if the default one is unavailable, check the Enable Failover check box.</p> <p>Note Do not enable vNIC fabric failover under the following circumstances:</p> <ul style="list-style-type: none"> • 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, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server. • 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 configuration 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.
Target list box	<p>A list of the possible targets for vNICs created from this template. The target you choose determines whether or not Cisco UCS Manager automatically creates a VM-FEX port profile with the appropriate settings for the vNIC template. This can be one of the following:</p> <ul style="list-style-type: none"> • 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.
Template Type field	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • 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.

- b) In the **VLANs** area, use the table to select the VLAN to assign to vNICs created from this template. The table contains the following columns:

Name	Description
Select column	Check the check box in this column for each VLAN that you want to use.
Name column	The name of the VLAN.
Native VLAN column	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.

- c) In the **Policies** area, complete the following fields:

Name	Description
MTU field	The maximum transmission unit, or packet size, that vNICs created from this vNIC template should 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 may be dropped during data transmission.
MAC Pool drop-down list	The MAC address pool that vNICs created from this vNIC template should use.
QoS Policy drop-down list	The quality of service policy that vNICs created from this vNIC template should use.
Network Control Policy drop-down list	The network control policy that vNICs created from this vNIC template should use.
Pin Group drop-down list	The LAN pin group that vNICs created from this vNIC template should use.
Stats Threshold Policy drop-down list	The statistics collection policy that vNICs created from this vNIC template should use.

Step 6 Click **OK**.

What to Do Next

Include the vNIC template in a service profile.

Deleting a vNIC Template

Procedure

-
- Step 1** In the **Navigation** pane, click the **LAN** tab.
 - Step 2** On the **LAN** tab, expand **LAN > Policies > Organization_Name**.
 - Step 3** Expand the **vNIC Templates** node.
 - Step 4** Right-click the policy you want to delete and choose **Delete**.
 - Step 5** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Binding a vNIC to a vNIC Template

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



Important If the vNIC is reconfigured when you bind it to a template, Cisco UCS Manager reboots the server associated with the 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 with the vNIC you want to bind. If the system does not include multi-tenancy, expand the **root** node.
 - Step 4** Expand **Service_Profile_Name > vNICs**.
 - Step 5** Click the vNIC you want to bind to a template.
 - Step 6** In the **Work** pane, click the **General** tab.
 - Step 7** In the **Actions** area, click **Bind to a Template**.
 - Step 8** In the **Bind to a vNIC Template** dialog box, do the following:
 - a) From the **vNIC Template** drop-down list, choose the template to which you want to bind the vNIC.

b) Click **OK**.

Step 9 In the warning dialog box, click **Yes** to acknowledge that Cisco UCS Manager may need to reboot the server if the binding causes the vNIC to be reconfigured.

Unbinding a vNIC from a vNIC 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 with the vNIC you want to unbind. If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand *Service_Profile_Name* > vNICs.

Step 5 Click the vNIC you want to unbind from a template.

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

Step 7 In the **Actions** area, click **Unbind from a Template**.

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

Configuring Ethernet Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in a cluster configuration with two fabric interconnects

**Note**

For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

**Important**

We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

$$\text{Completion Queues} = \text{Transmit Queues} + \text{Receive Queues}$$
$$\text{Interrupt Count} = (\text{Completion Queues} + 2) \text{ rounded up to nearest power of } 2$$

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

$$\text{Completion Queues} = 1 + 8 = 9$$
$$\text{Interrupt Count} = (9 + 2) \text{ rounded up to the nearest power of } 2 = 16$$

Creating an Ethernet Adapter Policy

**Tip**

If the fields in an area are not displayed, click the **Expand** icon to the right of the heading.

Procedure

- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the **root** node.
- Step 4** Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.
- Step 5** Enter a name and description for the policy in the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend that you include 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), or = (equal sign).

- Step 6** (Optional) In the **Resources** area, adjust the following values:

Name	Description
Transmit Queues field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Receive Queues field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.
Completion Queues field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.

Name	Description
Interrupts field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.

Step 7 (Optional) In the **Options** area, adjust the following values:

Name	Description
Transmit Checksum Offload field	This can be one of the following: <ul style="list-style-type: none"> • Disabled—The CPU calculates all packet checksums. • Enabled—The CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. <p>Note This option affects only packets sent from the interface.</p>
Receive Checksum Offload field	This can be one of the following: <ul style="list-style-type: none"> • Disabled—The CPU validates all packet checksums. • Enabled—The CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. <p>Note This option affects only packets received by the interface.</p>
TCP Segmentation Offload field	This can be one of the following: <ul style="list-style-type: none"> • Disabled—The CPU segments large TCP packets. • Enabled—The CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. <p>Note This option is also known as Large Send Offload (LSO) and affects only packets sent from the interface.</p>
TCP Large Receive Offload field	This can be one of the following: <ul style="list-style-type: none"> • Disabled—The CPU processes all large packets. • Enabled—The hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. <p>Note This option affects only packets received by the interface.</p>

Name	Description
Receive Side Scaling field	RSS distributes network receive processing across multiple CPUs in multiprocessor systems. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Network receive processing is always handled by a single processor even if additional processors are available. • Enabled—Network receive processing is shared across processors whenever possible.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600.
Interrupt Mode field	The preferred driver interrupt mode. This can be one of the following: <ul style="list-style-type: none"> • MSI X—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • MSI—MSI only. • INTx—PCI INTx interrupts.
Interrupt Coalescing Type field	This can be one of the following: <ul style="list-style-type: none"> • Min—The system waits for the time specified in the Interrupt Timer field before sending another interrupt event. • Idle—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the Interrupt Timer field.
Interrupt Timer field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter a value between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.

Step 8 Click **OK**.

Step 9 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting an Ethernet Adapter Policy

Procedure

- Step 1** In the **Navigation** pane, click the **LAN** tab.
- Step 2** On the **LAN** tab, expand **LAN > Policies > Organization_Name**.
- Step 3** Expand the **Adapter Policies** node.
- Step 4** Right-click the Ethernet adapter policy that you want to delete and choose **Delete**.
- Step 5** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Configuring Network Control Policies

Network Control Policy

This policy configures the network control settings for the Cisco UCS domain, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the VIF behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Manager takes on the remote Ethernet interface, vEthernet interface, or vFibreChannel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs.

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Manager to bring the vEthernet or vFibreChannel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default behavior directs Cisco UCS Manager to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibreChannel interfaces that are bound to the remote Ethernet interface are brought down as well.

**Note**

Cisco UCS Manager, release 1.4(2) and earlier did not enforce the **Action on Uplink Fail** property for those types of non-VM-FEX capable converged network adapters mentioned above. If the **Action on Uplink Fail** property was set to link-down, Cisco UCS Manager would ignore this setting and instead issue a warning. In the current version of Cisco UCS Manager this setting is enforced. Therefore, if your implementation includes one of those converged network adapters and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning.

Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

In Cisco UCS Manager, releases 1.4 and earlier, MAC addresses were installed on all of the VLANs belonging to an interface. Starting in release 2.0, MAC addresses are installed only on the native VLAN by default. In most implementations this maximizes the VLAN port count.

**Note**

If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating a Network Control Policy

MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns. This is either the source MAC address used in the FCoE Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

- Step 1** In the **Navigation** pane, click the **LAN** tab.
- Step 2** On the **LAN** tab, expand **LAN > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the **root** node.
- Step 4** Right-click the **Network Control Policies** node and select **Create Network Control Policy**.
- Step 5** In the **Create Network Control Policy** dialog box, complete the following fields:

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

Name	Description
CDP field	<p>This option determines whether Cisco Discovery Protocol (CDP) is enabled on servers associated with a service profile that includes this policy. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled • Enabled
MAC Register Mode field	<p>Whether adapter-registered MAC addresses are added only to the native VLAN associated with the interface or added to all VLANs associated with the interface. This can be one of the following:</p> <ul style="list-style-type: none"> • Only Native Vlan—MAC addresses are only added to the native VLAN. This option is the default, and it maximizes the port+VLAN count. • All Host Vlans—MAC addresses are added to all VLANs with which they are associated. Select this option if your VLANs are configured to use trunking but are <i>not</i> running in Promiscuous mode.
Action on Uplink Fail field	<p>This option determines how the VIF behaves if no uplink port is available when the fabric interconnect is in end-host mode. This can be one of the following:</p> <ul style="list-style-type: none"> • Link Down— Changes the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and enables fabric failover for vNICs. • Warning— Maintains server-to-server connectivity even when no uplink port is available, and disables fabric failover when uplink connectivity is lost on the fabric interconnect. <p>The default is Link Down.</p> <p>Note Cisco UCS Manager, release 1.4(2) and earlier did not enforce the Action on Uplink Fail property for those types of non-VM-FEX capable converged network adapters mentioned above. If the Action on Uplink Fail property was set to link-down, Cisco UCS Manager would ignore this setting and instead issue a warning. In the current version of Cisco UCS Manager this setting is enforced. Therefore, if your implementation includes one of those converged network adapters and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the Action on Uplink Fail property with a value of warning.</p> <p>Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.</p>

- Step 6** In the **MAC Security** area, do the following to determine whether the server can use different MAC addresses when sending packets to the fabric interconnect:
- Click the **Expand** icon to expand the area and display the radio buttons.
 - Click one of the following radio buttons to determine whether forged MAC addresses are allowed or denied when packets are sent from the server to the fabric interconnect:
 - Allow**— All server packets are accepted by the fabric interconnect, regardless of the MAC address associated with the packets.
 - Deny**— After the first packet has been sent to the fabric interconnect, all other packets must use the same MAC address or they will be silently rejected by the fabric interconnect. In effect, this option enables port security for the associated vNIC.

If you plan to install VMware ESX on the associated server, you must configure the **MAC Security** to **allow** for the network control policy applied to the default vNIC. If you do not configure **MAC Security** for **allow**, the ESX installation may fail because the MAC security permits only one MAC address while the installation process requires more than one MAC address.

- Step 7** Click **OK**.
-

Deleting a Network Control Policy

Procedure

- Step 1** In the **Navigation** pane, click the **LAN** tab.
 - Step 2** On the **LAN** tab, expand **LAN > Policies > Organization_Name**.
 - Step 3** Expand the **Network Control Policies** node.
 - Step 4** Right-click the policy you want to delete and select **Delete**.
 - Step 5** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-