



# Configuring Policies

---

This chapter includes the following sections:

- [Configuring Dynamic vNIC Connection Policies, page 1](#)
- [Creating a Custom Ethernet Adapter Policy for SR-IOV, page 5](#)

## Configuring Dynamic vNIC Connection Policies

### Dynamic vNIC Connection Policy



**Note**

In an SR-IOV topology, such as a Hyper-V or KVM cluster, a Virtual Function (VF) takes the place of the dynamic vNIC. The VF is essentially a restricted version of the dynamic vNIC, in which all system communication and configuration of the VF is performed through the associated physical function (PF).

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

#### **Ethernet Adapter Policy**

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

For Hyper-V, use the predefined Ethernet adapter policy named Windows.

## Server Migration



**Note** If you migrate a server that is configured with dynamic vNICs, the dynamic interface used by the vNICs fails and notifies you of that failure.

When the server comes back up, assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

## Creating a Dynamic vNIC Connection Policy

You can create a dynamic vNIC connection 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 **Dynamic vNIC Connection Policies** node and choose **Create Dynamic vNIC Connection Policy**.
- Step 5** In the **Create Dynamic vNIC Connection Policy** dialog box, complete the following fields:

Name	Description
Name field	<p>The name of the policy.</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 is saved.</p> <p><b>Note</b> Do not specify "default" as the value for the dynamic vNIC connection policy name. Cisco UCS Manager automatically resolves any empty policy references to "default". Any service profiles or service profile templates with only static vNICs defined will automatically reference the policy "default" when it is present. If you specify "default" for the dynamic vNIC connection policy name, then unexpected dynamic vNICs might be created on those service profiles or service profile templates.</p>
Description field	<p>A description of the policy. Cisco recommends including information about where and when to use the policy.</p> <p>Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), &gt; (greater than), &lt; (less than), or ' (single quote).</p>

Name	Description
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects. Enter an integer between 0 and 256. The default is 54. <b>Note</b> Components of your system might limit this number to fewer than 256 vNICs.
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.
Protection field	Dynamic vNICs are always protected in Cisco UCS, but this field allows you to select a preferred fabric, if any. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>Protected Pref A</b>—Cisco UCS attempts to use fabric A but fails over to fabric B if necessary</li> <li>• <b>Protected Pref B</b>—Cisco UCS attempts to use fabric B but fails over to fabric A if necessary</li> <li>• <b>Protected</b>—Cisco UCS uses whichever fabric is available</li> </ul>

**Step 6** Click **OK**.

**Step 7** If a confirmation dialog box appears, click **Yes**.

## Changing a Dynamic vNIC Connection Policy

You can change a dynamic vNIC connection 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 that contains the policy that you want to change.  
If the system does not include multitenancy, expand the **root** node.

**Step 4** Expand the **Dynamic vNIC Connection Policies** node and click the policy that you want to change.

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

**Step 6** Change one or more of the following fields:

Name	Description
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy.

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.

You cannot change the other properties of the policy, such as the **Name** field.

- Step 7** Click **Save Changes**.
  - Step 8** If a confirmation dialog box displays, click **Yes**.
- 

## Deleting a Dynamic vNIC Connection Policy

You can delete a dynamic vNIC connection 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 **Dynamic vNIC Connection Policies** node.
  - Step 4** Right-click the policy that you want to delete and choose **Delete**.
  - Step 5** If a confirmation dialog box displays, click **Yes**.
- 

## Viewing Dynamic vNIC Properties in a VM

You can view dynamic vNIC properties in a VM.

### Before You Begin

The VM must be operational.

### Procedure

---

- Step 1** In the **Navigation** pane, click the **VM** tab.
  - Step 2** On the VM tab, expand **All**.
  - Step 3** Expand **Virtual Machines**.
  - Step 4** Expand the virtual machine that contains the dynamic vNIC.
  - Step 5** Choose the dynamic vNIC.
  - Step 6** In the **Work** pane, click the **General** tab.  
In the **Properties** area, the vNIC properties appear.
- 

## Creating a Custom Ethernet Adapter Policy for SR-IOV

The predefined **SRIOV** Ethernet adapter policy supports up to 32 CPU threads. If the server has more than 32 CPU threads, you must follow this procedure to create and specify a custom adapter policy that supports a number of interrupts equal to the number of CPU threads.

For more information about creating an adapter policy, see "Configuring Ethernet Adapter Policies" in the *Cisco UCS Manager GUI Configuration Guide*.



---

**Tip** If the fields in an area do not display, click the **Expand** icon to the right of the heading.

---

### Before You Begin

Determine the number of CPU threads used by your server. You can find this information by navigating to **Equipment > Chassis > Servers** and viewing the **Threads** heading for your server in the **Servers** table.

### Procedure

---

- Step 1** If you opened the **Create Ethernet Adapter Policy** directly from another menu, skip to Step 6.
- Step 2** In the **Navigation** pane, click the **Servers** tab.
- Step 3** On the **Servers** tab, expand **Servers > Policies**.
- Step 4** 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 5** Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.
- Step 6** 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) and _ (underscore), and you cannot change this name after the object has been saved.
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

**Step 7** In the **Resources** area, configure the following values as shown:

Name	Setting
Transmit Queues	1
Ring Size	256
Receive Queues	4
Ring Size	512
Completion Queues	5
Interrupts	Enter the number of CPU threads used by the server.

**Step 8** In the **Options** area, configure the following values as shown:

Name	Setting
All offload settings	Enabled
RSS	Enabled
Fallback Timeout	5 seconds
Interrupt Mode	MSIX
Interrupt Coalescing Type	Min
Interrupt Timer	125 microseconds

**Step 9** Click **OK**.

**Step 10** If a confirmation dialog box displays, click **Yes**.