Configuring Cisco Cloud APIC Components

About Configuring the Cisco Cloud APIC

You create the Cisco Cloud APIC components using either the Cisco Cloud APIC GUI or the REST API. This section explains how to create configuration, application management, operations, and administrative components.

Note

- For information about configuring a load balancer and service graph, see Deploying Layer 4 to Layer 7 Services.
- For information about the GUI, such as navigation and a list of configurable components, see About the Cisco Cloud APIC GUI.

Configuring the Cisco Cloud APIC Using the GUI

Creating a Tenant Using the Cisco Cloud APIC GUI

This section explains how to create a tenant using the Cisco Cloud APIC GUI.

Before you begin

- You can create a tenant that is managed by the Cisco Cloud APIC or a tenant that is unmanaged. To establish a managed tenant, you must first obtain the Azure subscription ID from the Azure portal. You enter the subscription ID in the appropriate field of the Cisco Cloud APIC when creating the tenant. Before you can use the managed tenant, you must explicitly grant the Cisco Cloud APIC permission to manage the subscription. The steps for doing so are displayed in the Cisco Cloud APIC GUI during tenant creation. The steps for the infra tenant, however, are displayed in the infra tenant details view:

  1. Click the **Navigation** menu > **Application Management** subtab.

2. Double-click the infra tenant.
3. Click **View Azure Role Assignment Command**. The steps for granting the Cisco Cloud APIC permission to manage the subscription are displayed.

Note For information about obtaining the Azure subscription ID, see the Microsoft Azure documentation.

- Creating an unmanaged tenant requires obtaining a directory (Azure Tenant) ID, an Azure enterprise application ID, and a client secret from the enterprise application. For more information, see the Microsoft Azure documentation.

Note Cloud APIC does not disturb Azure resources created by other applications or users. It only manages the Azure resources created by itself.

- The required steps to explicitly grant the Cisco Cloud APIC permission to manage a given subscription are located in the Cisco Cloud APIC GUI. When creating a tenant, the steps are displayed after entering the client secret. For the infra tenant:
- Cloud APIC enforces ownership checks to prevent deployment of policies in the same tenant-region combination done either intentionally or by mistake. For example, assume that Cloud APIC is deployed in Azure subscription IA1 in region R1. Now you want to deploy a tenant TA1 in region R2. This tenant deployment i.e. account-region combination TA1-R2 is now owned by IA1-R1. If another Cloud APIC attempts to manage the same tenant-region combination later (say Capic2 in Azure subscription IA2 deployed in region R3), this will not be allowed because the current owner for the deployment TA1-R2 is IA1-R1. In other words, only one account in one region can be managed by one Cloud APIC. Example below shows some valid and wrong deployment combinations.

```
Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- Ownership enforcement is done using Azure Resource Groups. When a new tenant in subscription TA1 in region R2 is managed by Cloud APIC, a Resource Group CAPIC_TA1_R2 (e.g. CAPIC_123456789012__eastus2) is created in the subscription. This Resource Group has a resource tag AciOwnerTag with value IA1_R1_TA1_R2, assuming it was managed by Cloud APIC in subscription IA1 and deployed in region R1. If the AciOwnerTag mismatch happens, tenant-region management is aborted.

  Here is a summary of AciOwnerTag mismatch cases:

- Initially Cloud APIC is installed in a subscription, and then taken down and Cloud APIC is installed in a different subscription. All existing tenant-region deployment will fail.
- Another Cloud APIC is managing the same tenant-region.

In ownership mismatch cases, **retry** (to setup tenant-region again) is not currently supported. As a workaround, if you are certain that no other Cloud APIC is managing the same tenant-region combination, logon to the tenant's Azure subscription and manually remove the affected Resource Group (for example: CAPIC_123456789012__eastus2). Next, reload Cloud APIC or delete and add the tenant again.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Tenant**. The **Create Tenant** dialog box appears.

Step 4 Choose the appropriate options and enter the appropriate values in each field as listed in the following *Create Tenant Dialog Box Fields* table then continue.

Table 1: Create Tenant Dialog Box Fields

Properties	Description
Name	Enter the name of the tenant.
Description	Enter a description of the tenant.
Settings	
Add Security Domain	To add a security domain for the tenant: **a.** Click **Add Security Domain**. The **Select Security Domains** dialog appears with a list of security domains in the left pane. **b.** Click to choose a security domain. **c.** Click **Select** to add the security domain to the tenant.
Azure Subscription	
Mode	Choose an account type: • **Create Own**—Choose this option to create a new tenant. • **Select Shared**—Choose this option to inherit the managed or unmanaged settings from an existing tenant.
Azure Subscription ID	Enter the Azure subscription ID.

Properties	Description
Access Type	Choose an access type: • **Unmanaged Identity**—Choose this option if the tenant subscription is not managed by the Cisco Cloud APIC. • **Managed Identity**—Choose this option if the tenant subscription is managed by the Cisco Cloud APIC. For more information, see *Configuring a Tenant Azure Provider*.
Application ID	**Note** This field is only valid for the **Unmanaged Identity** access type. Enter the application ID. **Note** For information about obtaining the application ID, see the Azure documentation or support.
Client Secret	**Note** This field is only valid for the **Unmanaged Identity** access type. Enter the client secret. **Note** • For information about creating a client secret, see the Azure documentation or support. • You must explicitly grant Cloud APIC permission to manage a given subscription. Go to the Azure portal and follow these steps: **a.** Open the Cloud Shell **b.** Choose 'Bash' **c.** Copy and paste the command displayed in the Cisco Cloud APIC GUI.
Active Directory ID	**Note** This field is only valid for the **Unmanaged Identity** access type. Enter the active directory ID. **Note** For information about obtaining the active directory ID, see the Azure documentation or support.

Properties	Description
Add Security Domain	To add a security domain for the account: **a.** Click **Add Security Domain**. The **Select Security Domains** dialog appears with a list of security domains in the left pane. **b.** Click to choose a security domain. **c.** Click **Select** to add the security domain to the tenant.

Step 5 Click **Save** when finished.

Creating an Application Profile Using the Cisco Cloud APIC GUI

This section explains how to create an application profile using the Cisco Cloud APIC GUI.

Before you begin

Create a tenant.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Application Profile**. The **Create Application Profile** dialog box appears.

Step 4 Enter a name in the **Name** field.

Step 5 Choose a tenant:

a) Click **Select Tenant**.

The **Select Tenant** dialog box appears.

b) From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**.

You return to the **Create Application Profile** dialog box.

Step 6 Enter a description in the **Description** field.

Step 7 Click **Save** when finished.

Creating a VRF Using the Cisco Cloud APIC GUI

This section explains how to create a VRF using the Cisco Cloud APIC GUI.

Before you begin

Create a tenant.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create VRF**. The **Create VRF** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create VRF Dialog Box Fields* table then continue.

Table 2: Create VRF Dialog Box Fields

Properties	Description
General	
Name	Enter a name for the VRF in the **Name** field. All VRFs are assigned a *vrfEncoded* value. If the Tenant and VRF name combination has more than 32 characters, then, a VRF name (which also contains the tenant name) is identified in the cloud router using the *vrfEncoded* value. To see the *vrfEncoded* value, navigate to **Application Management** > **VRFs** subtab. Click a VRF on the right hand pane and look for *Encoded VRF Name in Cloud Router*.
Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create VRF** dialog box.
Description	Enter a description of the VRF.

Step 5 When finished, click **Save**.

Creating an EPG Using the Cisco Cloud APIC GUI

This section explains how to create an EPG using the Cisco Cloud APIC GUI. Each service needs at least one consumer EPG and one provider EPG.

Note Beginning with Release 5.0(2), Cisco Cloud APIC creates the overlay-2 VRF in the infra tenant by default during the bring up, along with the overlay-1 VRF.

In addition, beginning with Release 5.0(2), you can create cloud EPGs and cloud external EPGs in the infra tenant, where all the cloud EPGs and cloud external EPGs will be associated with the overlay-2 VRF in the infra tenant. A cloud EPG in the overlay-2 VRF can communicate with other cloud EPGs and cloud external EPGs in the overlay-2 VRF, and can also communicate with cloud EPGS in other user tenant VRFs. We recommend that you do not use existing "cloud-infra" application profiles, and instead create a new application profile in the infra tenant and associate that new application profile to the cloud EPGs and cloud external EPGs in the overlay-2 VRF.

Before you begin

Create an application profile and a VRF.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create EPG**. The **Create EPG** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create EPG Dialog Box Fields* table then continue.

Table 3: Create EPG Dialog Box Fields

Properties	Description
Name	Enter the name of the EPG.
Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column. Beginning with Release 5.0(2), you can select the infra tenant and can create cloud EPGs and cloud external EPGs in the infra tenant, as described earlier in this section. **c.** Click **Select**. You return to the **Create EPG** dialog box.

Properties	Description
Application Profile	To choose an application profile: **a.** Click **Select Application Profile**. The **Select Application Profile** dialog box appears. **b.** From the **Select Application Profile** dialog, click to choose an application profile in the left column. **Note** If you are creating an EPG in the infra tenant, we recommend that you do not choose the `cloud-infra` application profile because that application profile is used by EPGs in the overlay-1 VRF. Select a different application profile or click **Create Application Profile** to create a new one. **c.** Click **Select**. You return to the **Create EPG** dialog box.
Description	Enter a description of the EPG.
Settings	
Type	Choose the EPG type: • **Cloud** - Click to create the EPG in the cloud. • **External** - Click to create an external EPG.
VRF	To choose a VRF: **a.** Click **Select VRF**. The **Select VRF** dialog box appears. **b.** From the **Select VRF** dialog, click to choose a VRF in the left column. If you are creating an EPG in the infra tenant, select the **overlay-2** VRF in this step. A cloud EPG in the overlay-2 VRF can communicate with other cloud EPGs and cloud external EPGs in the overlay-2 VRF, and can also communicate with cloud EPGs in other user tenant VRFs. **c.** Click **Select**. You return to the **Create EPG** dialog box.

Properties	Description
Endpoint Selectors	

Properties	Description
	Note See Configuring Virtual Machines in Azure, on page 20 for instructions on configuring virtual machines in Azure as part of the endpoint selector configuration process. To add an endpoint selector: **a.** Click **Add Endpoint Selector** to open the **Add Endpoint Selector** dialog. **b.** In the **Add Endpoint Selector** dialog, enter a name in the **Name** field. **c.** Click **Selector Expression**. The **Key**, **Operator**, and **Value** fields are enabled. **d.** Click the **Key** drop-down list to choose a key. The options are: • Choose **IP** if you want to use an IP address or subnet for the endpoint selector. • Choose **Region** if you want to use the Azure region for the endpoint selector. • Choose **Custom** if you want to create a custom key for the endpoint selector. **Note** When choosing the **Custom** option, the drop-down list becomes a text box. You need to enter a name for the key in the spaces after **custom:** (for example, **custom: Location**). **e.** Click the **Operator** drop-down list to choose an operator. The options are: • **equals**: Used when you have a single value in the Value field. • **not equals**: Used when you have a single value in the Value field. • **in**: Used when you have multiple comma-separated values in the Value field. • **not in**: Used when you have multiple comma-separated values in the Value field. • **has key**: Used if the expression contains only a key. • **does not have key**: Used if the expression contains only a key. **f.** Enter a value in the **Value** field then click the check mark to validate the entries. The value you enter depends on the choices you made for the **Key** and **Operator** fields. For example, if the **Key** field is set to **IP** and the **Operator** field is set to **equals**, the **Value** field must be an IP address or subnet. However, if the **Operator** field is set to **has key**, the **Value** field is disabled. **g.** When finished, click the check mark to validate the selector expression. **h.** Determine if you want to create additional endpoint selector expressions to the endpoint selector. If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions. For example, assume you created two sets of expressions under a single endpoint selector: • Endpoint selector 1, expression 1: • **Key:** Region • **Operator:** equals

Properties	Description
	• **Value:** westus • Endpoint selector 1, expression 2: • **Key:** IP • **Operator:** equals • **Value:** 192.0.2.1/24 In this case, if *both* of these expressions are true (if the region is westus AND if the IP address belongs to subnet 192.0.2.1/24), then that endpoint is assigned to the Cloud EPG. **i.** Click the check mark after every additional expression that you want to create under this endpoint selector then click **Add** when finished. If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you had created endpoint selector 1 as described in the previous step, and then you created a second endpoint selector as described below: • Endpoint selector 2, expression 1: • **Key:** Region • **Operator:** in • **Value:** eastus, centralus In this case: • If the region is westus AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions) OR • If the region is either eastus or centralus (endpoint selector 2 expression) Then that end point is assigned to the Cloud EPG.

Step 5 Click **Save** when finished.

Creating a Filter Using the Cisco Cloud APIC GUI

This section explains how to create a filter using the Cisco Cloud APIC GUI.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Filter**. The **Create Filter** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Filter Dialog Box Fields* table then continue.

Table 4: Create Filter Dialog Box Fields

Properties	Description
Name	Enter a name for the filter in the **Name** field.
Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Filter** dialog box.
Description	Enter a description of the filter.
Add Filter	To add a filter: **a.** Click **Add Filter Entry**. The **Add Filter Entry** dialog box appears. **b.** Enter a name for the filter entry in the **Name** field. **c.** Click the **Ethernet Type** drop-down list to choose an ethernet type. The options are: • **IP** • **Unspecified** **Note** When **Unspecified** is chosen, any traffic type is alloed, including IP, and the remaining fields are disabled. **d.** Click the **IP Protocol** drop-down menu to choose a protocol. The options are: • **tcp** • **udp** • **Unspecified** **Note** The remaining fields are enabled only when **tcp** or **udp** is chosen. **e.** Enter the appropriate port range information in the **Destination Port** fields. **f.** When finished entering filter entry information, click **Add**. You return to the **Create Filter** dialog box where you can repeat the steps to add another filter entry.

Step 5 When finished, click **Save**.

Creating a Contract Using the Cisco Cloud APIC GUI

This section explains how to create a contract using the Cisco Cloud APIC GUI.

Before you begin

Create filters.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Contract**. The **Create Contract** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Contract Dialog Box Fields* table then continue.

Table 5: Create Contract Dialog Box Fields

Properties	Description
Name	Enter the name of the contract.
Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column. **Note** Beginning in Release 5.0(2), you can create contracts in the infra tenant. You can also export contracts from and import contracts to the infra tenant for shared services use cases. **c.** Click **Select**. You return to the **Create Contract** dialog box.
Description	Enter a description of the contract.
Settings	

Properties	Description
Scope	The scope limits the contract to any endpoint groups within the same application profile, within the same VRF instance, throughout the fabric (globally), or within the same tenant. **Note** Shared services enables communication between EPGs in different tenants and between EPGs in different VRFs. To enable EPGs in one tenant to communicate with EPGs in another tenant, choose **Global** scope. To enable an EPG in one VRF to communicate with another EPG in a different VRF, choose **Global** or **Tenant** scope. For more information about shared services, see Shared Services. Click the drop-down arrow to choose from the following scope options: • **Application Profile** • **VRF** • **Global** • **Tenant**
Add Filter	To choose a filter: **a.** Click **Add Filter**. The filter row appears with a **Select Filter** option. **b.** Click **Select Filter**. The **Select Filter** dialog box appears. **c.** From the **Select Filter** dialog, click to choose a filter in the left column then click **Select**. You return to the **Create Contract** dialog box.

Step 5 Click **Save** when finished.

Creating an Inter-Tenant Contract Using the Cisco Cloud APIC GUI

This section explains how to create an inter-tenant contract using the Cisco Cloud APIC GUI. See Shared Services for more information on situations where you might want to create an inter-tenant contract.

Before you begin

Create filters.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Contract**. The **Create Contract** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Contract Dialog Box Fields* table then continue.

Table 6: Create Contract Dialog Box Fields

Properties	Description
Name	Enter the name of the contract.
Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column. **Note** Beginning in Release 5.0(2), you can create contracts in the infra tenant. You can also export contracts from and import contracts to the infra tenant for shared services use cases. **c.** Click **Select**. You return to the **Create Contract** dialog box.
Description	Enter a description of the contract.
Settings	
Scope	The scope limits the contract to any endpoint groups within the same application profile, within the same VRF instance, throughout the fabric (globally), or within the same tenant. For inter-tenant communication, you will first create a contract with the **Global** scope in one of the tenants (for example, **tenant1**). This tenant's EPG will always be the provider of this contract. This contract will then be exported to the other tenant (for example, **tenant2**). For the other tenant that imports this contract, its EPG will be the consumer of the imported contract. If you want tenant2's EPG to be the provider and tenant1's EPG to be the consumer, then create a contract in **tenant2** and then export it to **tenant1**.
Add Filter	To choose a filter: **a.** Click **Add Filter**. The filter row appears with a **Select Filter** option. **b.** Click **Select Filter**. The **Select Filter** dialog box appears. **c.** From the **Select Filter** dialog, click to choose a filter in the left column then click **Select**. You return to the **Create Contract** dialog box.

Step 5 Click **Save** when finished.

Step 6 Export the contract that you just created to another tenant.

For example, assume the following:

- The contract that you created in the procedure above is named **contract1** in tenant **tenant1**.
- The contract that you want to export is named **exported_contract1** and you are exporting it to tenant **tenant2**.

a) Navigate to the Contracts page (**Application Management** > **Contracts**).

The configured contracts are listed.

b) Select the contract that you just created.

For example, scroll through the list until you see the contract **contract1** and click the box next to it to select it.

c) Go to **Actions** > **Export Contract**.

The **Export Contract** window appears.

d) Click **Select Tenant**.

The **Select Tenant** window appears.

e) Select the tenant that you want to export the contract to, then click **Save**.

For example, **tenant2**. You are returned to the **Export Contract** window.

f) In the **Name** field, enter a name for the exported contract.

For example, **exported_contract1**.

g) In the **Description** field, enter a description for the exported contract, if necessary.

h) Click **Save**.

The list of contracts appears again.

Step 7 Configure the first tenant's EPG as the provider EPG, with the original contract, as the first part of the EPG communication configuration.

a) Click the **Intent** button, then choose **EPG Communication**.

The **EPG Communication** window appears.

b) Click **Let's Get Started**.

c) In the **Contract** area, click **Select Contract**.

The **Select Contract** window appears.

d) Locate and select the contract that you created at the beginning of these procedures.

In this example, you would locate and select **contract1**.

e) Click **Select**.

The **EPG Communication** window appears.

f) In the **Provider EPGs** area, click **Add Provider EPGs**.

The **Select Provider EPGs** window appears.

g) Leave the **Keep selected items** box checked, then select the first tenant's (**tenant1**) EPG.

h) Click **Select**.

The **EPG Communication** window appears.

i) Click **Save**.

Step 8 Configure the second tenant's EPG as the consumer EPG, with the exported contract, as the second part of the EPG communication configuration.

a) Click the **Intent** button, then choose **EPG Communication**.

The **EPG Communication** window appears.

b) Click **Let's Get Started**.

c) In the **Contract** area, click **Select Contract**.

The **Select Contract** window appears.

d) Locate and select the contract that you created at the beginning of these procedures.

In this example, you would locate and select **exported_contract1**.

e) Click **Select**.

The **EPG Communication** window appears.

f) In the **Consumer EPGs** area, click **Add Consumer EPGs**.

The **Select Consumer EPGs** window appears.

g) Leave the **Keep selected items** box checked, then select the second tenant's (**tenant2**) EPG.

h) Click **Select**.

The **EPG Communication** window appears.

i) Click **Save**.

Specifying Consumer and Provider EPGs Using the Cisco Cloud APIC

This section explains how to specify an EPG as a consumer or a provider.

Before you begin

- You have configured a contract.
- You have configured an EPG.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Configuration**.

A list of **Configuration** options appears in the **Intent** menu.

Step 3 From the **Configuration** list in the **Intent** menu, click **EPG Communication**. The **EPG Communication** dialog box appears with the **Consumer EPGs**, **Contract**, and **Provider EPGs** information.

Step 4 To choose a contract:

a) Click **Select Contract**. The **Select Contract** dialog appears.

b) In the pane on the left side of the **Select Contract** dialog, click to choose a contract then click **Select**. The **Select Contract** dialog box closes.

Step 5 To add a consumer EPG:

a) Click **Add Consumer EPGs**. The **Select Consumer EPGs** dialog appears.

Note EPGs within the tenant (where the contract is created) are displayed.

b) In the pane on the left side of the **Select Consumer EPGs** dialog, click to place a check in a check box to choose an EPG.

Step 6 To add a provider EPG:

a) Click **Add Provider EPGs**. The **Select Provider EPGs** dialog appears.

Note EPGs within the tenant (where the contract is created) are displayed.

b) In the pane on the left side of the **Select Provider EPGs** dialog, click to place a check in a check box to choose a provider EPG.

Note If the chosen contract is an Imported Contract, the provider EPG selection is disabled.

c) When finished, click **Select**. The **Select Provider EPGs** dialog box closes, and you return to the **EPG Communication Configuration** window.

d) Click **Save**.

Creating a Cloud Context Profile Using the Cisco Cloud APIC GUI

This section explains how to create a cloud context profile using the Cisco Cloud APIC GUI.

Before you begin

Create a VRF.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Cloud Context Profile**. The **Create Cloud Context Profile** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Cloud Context Profile Dialog Box Fields* table then continue.

Table 7: Create Cloud Context Profile Dialog Box Fields

Properties	Description
Name	Enter the name of the cloud context profile.
Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Cloud Context Profile** dialog box.
Description	Enter a description of the cloud context profile.
Settings	

Properties	Description
Region	To choose a region: **a.** Click **Select Region**. The **Select Region** dialog box appears. **b.** From the **Select Region** dialog, click to choose a region in the left column then click **Select**. You return to the **Create Cloud Context Profile** dialog box.
VRF	To choose a VRF: **a.** Click **Select VRF**. The **Select VRF** dialog box appears. **b.** From the **Select VRF** dialog box, click to choose a VRF in the left column then click **Select**. You return to the **Create Cloud Context Profile** dialog box.
Add CIDR	**Note** The following subnet is reserved and should not be used in this **Add CIDR** field: 192.168.100.0/24 (reserved by the CCR for the bridge domain interface) **Note** You cannot add, delete, or edit a CIDR when VNet peering is enabled. You must disable VNet peering before adding, deleting or editing a CIDR. To disable VNet peering: • For the infra tenant, disable the **Hub Network Peering** option in the cloud context profile • For a user (non-infra) tenant, disable the **VNet Peering** option in the cloud context profile Enable VNet peering again after you have made the changes to the CIDR configuration. **Note** Beginning in Release 5.0(2), you can add additional secondary CIDRs and subnets for infra VPCs (`cloudCtxProfiles` created by the cloud template). You cannot add primary CIDRs or modify the existing CIDRs created by the cloud template. After subnets are created under the user-created CIDRs, the subnets will be implicitly mapped to the overlay-2 VRF. To add a CIDR: **a.** Click **Add CIDR**. The **Add CIDR** dialog box appears. **b.** Enter the address in the **Address** field. **c.** Click **Add Subnet** and enter the subnet address in the **Address** field. **d.** Click to check (enabled) or uncheck (disabled) the **Primary** check box. **e.** When finished, click **Add**.
VNet Gateway Router	Click to check (enable) or uncheck (disable) in the **VNet Gateway Router** check box.

Properties	Description
VNet Peering	Click to check (enable) or uncheck (disable) the Azure VNet peering feature. For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document in the Cisco Cloud APIC documentation page.

Step 5 Click **Save** when finished.

Configuring Virtual Machines in Azure

When you configure endpoint selectors for Cisco Cloud APIC, you will also need to configure the virtual machines that you will need in Azure that will correspond with the endpoint selectors that you configure for Cisco Cloud APIC.

This topic provides the requirements for configuring the virtual machines in Azure. You can use these requirements to configure the virtual machines in Azure either before you configure the endpoint selectors for Cisco Cloud APIC or afterward. For example, you might go to your account in Azure and create a custom tag or label in Azure first, then create an endpoint selector using a custom tag or label in Cisco Cloud APIC afterward. Or you might create an endpoint selector using a custom tag or label in Cisco Cloud APIC first, then go to your account in Azure and create a custom tag or label in Azure afterward.

Before you begin

You must configure a cloud context profile as part of the Azure virtual machine configuration process. When you configure a cloud context profile, the configurations, such as the VRF and region settings, are pushed out to Azure afterward.

Step 1 Review your cloud context profile configuration to get the following information:

- VRF name
- Subnet information
- Subscription Id
- The resource group that corresponds to where the cloud context profile is deployed.

Note In addition to the information above, if you are using tag-based EPGs, you also need to know the tag names. The tag names are not available in the cloud context profile configuration.

To obtain the cloud context profile configuration information:

a) From the **Navigation** menu, choose the **Application Management** tab.

When the **Application Management** tab expands, a list of subtab options appear.

b) Choose the **Cloud Context Profiles** subtab option.

A list of the cloud context profiles that you have created for your Cisco Cloud APIC are displayed.

c) Select the cloud context profile that you will use as part of this Azure virtual machine configuration process.

Various configuration parameters are displayed for this cloud context profile, such as the region, VRF, IP address and subnets. Use the information displayed in this window when you configure the Azure virtual machine.

Step 2 Log in to the Azure portal account for the Cisco Cloud APIC user tenant and begin creating an Azure VM using the information you gathered from the cloud context profile configuration.

Note For information about how to create the VM in the Azure portal, see the Microsoft Azure documentation.

Creating a Backup Configuration Using the Cisco Cloud APIC GUI

This section explains how to create a backup configuration.

Before you begin

Create a remote location and a scheduler, if needed.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

Step 3 From the **Operations** list in the **Intent** menu, click **Create Backup Configuration**. The **Create Backup Configuration** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Backup Configuration Dialog Box Fields* table then continue.

Table 8: Create Backup Configuration Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the backup configuration.
Description	Enter a description of the backup configuration.
Settings	
Backup Destination	Choose a backup destination. • **Local** • **Remote**

Properties	Description
Backup Object	

Properties	Description
	Choose the root hierarchical content to consider for the backup • **Policy Universe** • **Selector Object**—When chosen, this option adds the **Object Type** drop-down list and **Object DN** field. **a.** From the **Object Type** drop-down list, choose from the following options: • **Tenant**—When chosen the **Select Tenant** option appears. • **Application Profile**—When chosen the **Select Application Profile** option appears. • **EPG**—When chosen the **Select EPG** option appears. • **Contract**—When chosen the **Select Contract** option appears. • **Filter**—When chosen the **Select Filter** option appears. • **VRF**—When chosen the **Select VRF**option appears. • **Device**—When chosen the **Select fvcloudLBCtx**option appears. • **Service Graph**—When chosen the **Select Service Graph** option appears. • **Cloud Context Profile**—When chosen the **Select Cloud Context Profile** option appears. **b.** Click the **Select <object_name>**. The **Select <object_name>** dialog appears. **c.** From the **Select <object_name>** dialog, click to choose from the options in the left column then click **Select**. You return to the **Create Backup Configuration** dialog box. **Note** The **Object DN** field is automatically populated with the DN of the object it will use as root of the object tree to backup • **Enter DN**—When chosen, this option displays the **Object DN** field. **a.** From the **Object DN** field, enter the DN of a

Properties	Description
	specific object to use as the root of the object tree to backup.
Scheduler	**a.** Click **Select Scheduler** to open the **Select Scheduler** dialog and choose a scheduler from the left-side column. **b.** Click the **Select** button at the bottom-right corner when finished.
Trigger Backup After Creation	Choose one of the following: • **Yes**—(Default) Trigger a backup after creating the backup configuration. • **No**—Do not trigger a backup after creating the backup configuration.

Step 5 Click **Save** when finished.

Creating a Tech Support Policy Using the Cisco Cloud APIC GUI

This section explains how to create a tech support policy.

Before you begin

When creating a tech support policy for a remote location, you must first create the remote location.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

Step 3 From the **Operations** list in the **Intent** menu, click **Create Tech Support**. The **Create Tech Support** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Tech Support Dialog Box Fields* table then continue.

Table 9: Create Tech Support Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the tech support policy.
Description	Enter a description of the tech support.
Settings	

Properties	Description
Export Destination	Choose an export destination. • **Controller** • **Remote Location**—When chosen the **Select Remote Location** option appears. a. Click **Select Remote Location**. The **Select Remote Location** dialog box appears. b. From the **Select Remote Location** dialog, click to choose a remote location in the left column then click **Select**. You return to the **Create Tech Suport** dialog box.
Include Pre-Upgrade Logs	Click to place a check in the **Enabled** check box if you want to include pre-upgrade logs in the tech support policy.
Trigger After Creation	Click to place a check in the **Enabled** (the default) check box if you want to create the tech support policy after the policy creation. To disable, click the check box to uncheck.

Step 5 Click **Save** when finished.

Creating a Scheduler Using the Cisco Cloud APIC GUI

This section explains how to create a scheduler, which would be in User Laptop Browser local time and will be converted to the Cisco Cloud APIC default UTC time.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

Step 3 From the **Operations** list in the **Intent** menu, click **Create Scheduler**. The **Create Scheduler** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Scheduler Dialog Box Fields* table then continue.

Table 10: Create Scheduler Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the trigger scheduler policy.
Description	Enter a description of the trigger scheduler.
Settings	

Properties	Description
Recurring Windows	Click **Add Recurring Window**. The **Add Recurring Window** dialog appears. **a.** From the **Schedule** drop-down list, choose from the following. • **every-day** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** • **odd-day** • **even-day** **b.** From the **Start Time** field, enter a time. **c.** From the **Maximum Concurrent Tasks** field, enter a number or leave the field empty to specify unlimited. **d.** From the **Maximum Running Time**, click to choose **Unlimited** or **Custom**. **e.** Click **Add** when finished.
Add One Time Window	Click **Add One Time Window**. The **Add One Time Window** dialog appears. **a.** From the **Start Time** field, enter a date and time. **b.** From the **Maximum Concurrent Tasks** field, enter a number or leave the field blank to specify unlimited. **c.** From the **Maximum Running Time**, click to choose **Unlimited** or **Custom**. **d.** Click **Add** when finished.

Step 5 Click **Save** when finished.

Creating a Remote Location Using the Cisco Cloud APIC GUI

This section explains how to create a remote location using the Cisco Cloud APIC.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

Step 3 From the **Operations** list in the **Intent** menu, click **Create Remote Location**. The **Create Remote Location** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Remote Location Dialog Box Fields* table then continue.

Table 11: Create Remote Location Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the remote location policy.
Description	Enter a description of the remote location policy.
Settings	
Hostname/IP Address	Enter the hostname or IP address of the remote location
Protocol	Choose a protocol: • **FTP** • **SFTP** • **SCP**
Path	Enter the path for the remote location.
Port	Enter the port for the remote location.
Username	Enter a username for the remote location.
Authentication Type	When using SFTP or SCP, choose the authentication type: • **Password** • **SSH Key**
SSH Key Content	Enter the SSH key content.
SSH Key Passphrase	SSH key passphrase.
Password	Enter a password for accessing the remote location.
Confirm Password	Reenter the password for accessing the remote location.

Step 5 Click **Save** when finished.

Creating a Login Domain Using the Cisco Cloud APIC GUI

This section explains how to create a login domain using the Cisco Cloud APIC GUI.

Before you begin

Create a provider before creating a non-local domain.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create Login Domain**. The **Create Login Domain** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Table 12: Create Login Domain Dialog Box Fields

Properties	Description
Name	Enter the name of the login domain.
Description	Enter a description of the login domain.
Realm	Choose a realm: • **Local** • **LDAP**—Requires adding providers and choosing an authenication type. • **RADIUS**—Requires adding providers. • **TACACS+**—Requires adding providers. • **SAML**—Requires adding providers.
Providers	To add a provider: **a.** Click **Add Providers**. The **Select Providers** dialog appears with a list of providers in the left pane. **b.** Click to choose a provider. **c.** Click **Select** to add the provider.
Advanced Settings	Displays the **Authentication Type** and **LDAP Group Map Rules** fields.

Properties	Description
Authentication Type	When LDAP is chosen for realm option, choose one of the following authentication types: • **Cisco AV Pairs**—(Default) • **LDAP Group Map Rules**—Requires adding LDAP group map rules.
LDAP Group Map Rules	To add an LDAP group map rule: **a.** Click **Add LDAP Group Map Rule**. The **Add LDAP Group Map Rule** dialog appears with a list of providers in the left pane. **b.** Enter a name for the rule in the **Name** field. **c.** Enter a description for the rule in the **Description** field. **d.** Enter a group DN for the rule in the **Group DN** field. **e.** Add security domains: **1.** Click **Add Security Domain**. The **Add Security Domain** dialog box appears. **2.** Click **Select Security Domain**. The **Select Security Domain** dialog box appears with a list of security domains in the left pane. **3.** Click to choose a security domain. **4.** Click **Select** to add the security domain. You return to the **Add Security Domain** dialog box. **5.** Add a user role: **a.** From the **Add Security Domain** dialog box, click **Select Role**. The **Select Role** dialog box appears with a list of roles in the left pane. **b.** Click to choose a role. **c.** Click **Select** to add the role. You retun to the **Add Security Domain** dialog box. **d.** From the **Add Security Domain** dialog box, click the **Privilege Type** drop-down list and choose **Read Privilege** or **Write Privilege**. **e.** Click the check mark on the right side of the **Privilege Type** drop-down list to confirm. **f.** Click **Add** when finished. You return to the **Add LDAP Group Map Rule** dialog box where you can add another security domain.

Step 5 Click **Save** when finished.

Creating a Security Domain Using the Cisco Cloud APIC GUI

A security domain restricts the tenant to the security domains that you add. If you do not add a security domain, all security domains will have access to this tenant. This section explains how to create a security domain using the GUI.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create Security Domain**. The **Create Security Domain** dialog box appears.

Step 4 In the **Name** field, enter the name of the security domain.

Step 5 In the **Description** field, enter a description of the security domain.

Step 6 Click **Save** when finished.

Creating a Role Using the Cisco Cloud APIC GUI

This section explains how to create a role using the Cisco Cloud APIC GUI.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create Role**. The **Create Role** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Role Dialog Box Fields* table then continue.

Table 13: Create Role Dialog Box Fields

Properties	Description
General	
Name	Enter a name for the role in the **Name** field.
Description	Enter a description of the role.
Settings	

Properties	Description
Privilege	

Properties	Description
	Click to place a check mark in the check boxes of the privileges you want to assign the user. The privileges are: • **aaa**—Used for configuring authentication, authorization, accouting and import/export policies. • **access-connectivity-l1**Used for Layer 1 configuration under infra. Example: selectors and port Layer 1 policy configurations. • **access-connectivity-l2**—Used for Layer 2 configuration under infra. Example: Encap configurations on selectors, and attachable entity. • **access-connectivity-l3**—Used for Layer 3 configuration under infra and static route configurations under a tenant's L3Out. • **access-connectivity-mgmt**—Used for management infra policies. • **access-connectivity-util**—Used for tenant ERSPAN policies. • **access-equipment**—Used for access port configuration. • **access-protocol-l1**—Used for Layer 1 protocol configurations under infra. • **access-protocol-l2**—Used for Layer 2 protocol configurations under infra. • **access-protocol-l3**—Used for Layer 3 protocol configurations under infra. • **access-protocol-mgmt**—Used for fabric-wide policies for NTP, SNMP, DNS, and image management. • **access-protocol-ops**—Used for operations-related access policies such as cluster policy and firmware policies. • **access-protocol-util**—Used for tenant ERSPAN policies. • **access-qos**—Used for changing CoPP and QoS-related policies. • **admin**—Complete access to everything (combine ALL roles) • **fabric-connectivity-l1**—Used for Layer 1 configuration under the fabric. Example: selectors and port Layer 1 policy and VNET protection.

Properties	Description
	• **fabric-connectivity-l2**—Used in firmware and deployment policies for raising warnings for estimating policy deployment impact. • **fabric-connectivity-l3**—Used for Layer 3 configuration under the fabric. Example: Fabric IPv4 and MAC protection groups. • **fabric-connectivity-mgmt**—Used for atomic counter and diagnostic policies on leaf switches and spine switches. • **fabric-connectivity-util**—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches. • **fabric-equipment**—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches. • **fabric-protocol-l1**—Used for Layer 1 protocol configurations under the fabric. • **fabric-protocol-l2**—Used for Layer 2 protocol configurations under the fabric. • **fabric-protocol-l3**—Used for Layer 3 protocol configurations under the fabric. • **fabric-protocol-mgmt**—Used for fabric-wide policies for NTP, SNMP, DNS, and image management. • **fabric-protocol-ops**—Used for ERSPAN and health score policies. • **fabric-protocol-util**—Used for firmware management traceroute and endpoint tracking policies. • **none**—No privilege. • **nw-svc-device**—Used for managing Layer 4 to Layer 7 service devices. • **nw-svc-devshare**—Used for managing shared Layer 4 to Layer 7 service devices. • **nw-svc-params**—Used for managing Layer 4 to Layer 7 service policies. • **nw-svc-policy**—Used for managing Layer 4 to Layer 7 network service orchestration.

Properties	Description
	• **ops**—Used for operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies. • **tenant-connectivity-l1**—Used for Layer 1 connectivity changes, including bridge domains and subnets. • **tenant-connectivity-l2**—Used for Layer 2 connectivity changes, including bridge domains and subnets. • **tenant-connectivity-l3**—Used for Layer 3 connectivity changes, including VRFs. • **tenant-connectivity-mgmt**—Used for tenant in-band and out-of-band management connectivity configurations and for debugging/monitoring policies such as atomic counters and health score. • **tenant-connectivity-util**—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches. • **tenant-epg**—Used for managing tenant configurations such as deleting/creating endpoint groups, VRFs, and bridge domains. • **tenant-ext-connectivity-l2**—Used for managing tenant L2Out configurations. • **tenant-ext-connectivity-l3**—Used for managing tenant L3Out configurations. • **tenant-ext-connectivity-mgmt**—Used as write access for firmware policies. • **tenant-ext-connectivity-util**—Used for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk. • **tenant-ext-protocol-l1**—Used for managing tenant external Layer 1 protocols. Generally only used for write access for firmware policies. • **tenant-ext-protocol-l2**—Used for managing tenant external Layer 2 protocols. Generally only used for write access for firmware policies. • **tenant-ext-protocol-l3**—Used for managing tenant external Layer 3 protocols such as BGP, OSPF, PIM, and IGMP. • **tenant-ext-protocol-mgmt**—Used as write access for firmware policies.

Properties	Description
	• **tenant-ext-protocol-util**—Used for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk. • **tenant-network-profile**—Used for managing tenant configurations, such as deleting and creating network profiles, and deleting and creating endpoint groups. • **tenant-protocol-l1**—Used for managing configurations for Layer 1 protocols under a tenant. • **tenant-protocol-l2**—Used for managing configurations for Layer 2 protocols under a tenant. • **tenant-protocol-l3**—Used for managing configurations for Layer 3 protocols under a tenant. • **tenant-protocol-mgmt**—Only used as write access for firmware policies. • **tenant-protocol-ops**—Used for tenant traceroute policies. • **tenant-protocol-util**—Used for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk. • **tenant-qos**—Only used as Write access for firmware policies. • **tenant-security**—Used for Contract related configurations for a tenant. • **vmm-connectivity**—Used to read all the objects in APIC's VMM inventory required for VM connectivity. • **vmm-ep**—Used to read VM and Hypervisor endpoints in the APIC's VMM inventory. • **vmm-policy**—Used for managing policies for VM networking. • **vmm-protocol-ops**—Not used by VMM policies. • **vmm-security**—Used for Contract related configurations for a tenant.

Step 5 Click **Save** when finished.

Creating an RBAC Rule Using the Cisco Cloud APIC GUI

This section explains how to create an RBAC rule using the GUI.

Before you begin

Create a security domain.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appears in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create RBAC Rule**. The **Create RBAC Rule** dialog box appears.

Step 4 In the **DN** field, enter the DN for the rule.

Step 5 Choose a security domain:

a) Click **Select Security Domain**. The **Select Security Domain** dialog box appears.

b) From the **Select Security Domain** dialog box, click to choose a security domain from the column on the left then click **Select**. You return to the **Create RBAC Rule** dialog box.

Step 6 From the **Allow Writes** field, click **Yes** to allow writes or **No** to not allow writes.

Step 7 Click **Save** when finished.

Creating a Certificate Authority Using the Cisco Cloud APIC GUI

This section explains how to create a certificate authority using the GUI.

Before you begin

- Have the certificate chain.
- If the certificate authority is for a tenant, create the tenant.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appears in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create Certificate Authority**. The **Create Certificate Authority** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Certificate Authority Dialog Box Fields* table then continue.

Table 14: Create Certificate Authority Dialog Box Fields

Properties	Description
Name	Enter the name of the certificate authority.
Description	Enter a description of the certificate authority.

Properties	Description
Used for	Choose from the following options: • **Tenant**—Choose if the certificate authority is for a specific tenant. When chosen, the **Select Tenant** option appears in the GUI. • **System**—Choose if the certificate authority is for the system.
Select Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Certificate Authority** dialog box.
Certificate Chain	Enter the certificate chain in the **Certificate Chain** text box. **Note** Add the certificates for a chain in the following order: **a.** CA **b.** Sub-CA **c.** Subsub-CA **d.** Server

Step 5 Click **Save** when finished.

Creating a Key Ring Using the Cisco Cloud APIC GUI

This section explains how to create a key ring using the Cisco Cloud APIC GUI.

Before you begin

- Create a certificate authority.
- Have a certificate.
- If the key ring is for a specific tenant, create the tenant.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create Key Ring**. The **Create Key Ring** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Key Ring Dialog Box Fields* table then continue.

Table 15: Create Key Ring Dialog Box Fields

Properties	Description
Name	Enter the name of the key ring.
Description	Enter a description of the key ring.
Used for	• **System**—The key ring is for the system. • **Tenant**—The key ring is for a specific tenant. Displays a **Tenant** field for specifying the tenant.
Select Tenant	To choose a tenant: **a.** Click **Select Tenant**. The **Select Tenant** dialog box appears. **b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Key Ring** dialog box.
Settings	
Certificate Authority	To choose a certificate authority: **a.** Click **Select Certificate Authority**. The **Select Certificate Authority** dialog appears. **b.** Click to choose a certificate authority in the column on the left. **c.** Click **Select**. You return to the **Create Key Ring** dialog box.
Private Key	Choose one of the following: • **Generate New Key**—Generates a new key. • **Import Existing Key**—Displays the **Private Key** text box and enables you to use an existing key.
Private Key	Enter an existing key in the **Private Key** text box (for the **Import Existing Key** option).

Properties	Description
Modulus	Click the **Modulus** drop-down list to choose from the following: • **MOD 512** • **MOD 1024** • **MOD 1536** • **MOD 2048**—(Default)
Certificate	Enter the certificate information in the **Certificate** text box.

Step 5 Click **Save** when finished.

Creating a Local User Using the Cisco Cloud APIC GUI

This section explains how to create a local user using the Cisco Cloud APIC GUI.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Create Local User**. The **Create Local User** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Local User Dialog Box Fields* table then continue.

Table 16: Create Local User Dialog Box Fields

Properties	Description
Name	Enter the username of the local user.
Password	Enter the password for the local user.
Confirm Password	Reenter the password for the local user.
Description	Enter a description of the local user.
Settings	
Account Status	To choose the account status: • **Active**—Activates the local user account. • **Inactive**—Deactivates the local user account.
First Name	Enter the first name of the local user.

Properties	Description
Last Name	Enter the last name of the local user.
Email Address	Enter the email address of the local user.
Phone Number	Enter the phone number of the local user.
Security Domains	To add a security domain: **a.** Click **Add Security Domain**. The **Add Security Domain** dialog box appears. **b.** Click **Select Security Domain**. The **Select Security Domain** dialog box appears with a list of security domains in the left pane. **c.** Click to choose a security domain. **d.** Click **Select** to add the security domain. You return to the **Add Security Domain** dialog box. **e.** Add a user role: **1.** From the **Add Security Domain** dialog box, click **Select Role**. The **Select Role** dialog box appears with a list of roles in the left pane. **2.** Click to choose a role. **3.** Click **Select** to add the the role. You retun to the **Add Security Domain** dialog box. **4.** From the **Add Security Domain** dialog box, click the **Privilege Type** drop-down list and choose **Read Privilege** or **Write Privilege**. **5.** Click the check mark on the right side of the **Privilege Type** drop-down list to confirm. **6.** Click **Add** when finished. You return to the **Create Local User** dialog box where you can add another security domain.

Step 5 Click **Advanced Settings** and enter the appropriate values in each field as listed in the following *Create Local User Dialog Box Fields: Advanced Settings* table then continue.

Table 17: Create Local User Dialog Box Fields: Advanced Settings

Property	Description
Account Expires	If you choose **Yes**, the account is set to expire at the time that you choose.
Password Update Required	If you choose **Yes**, the user must change the password upon the next login.

Property	Description
OTP	Put a check in the box to enable the one-time password feature for the user.
User Certificates	To add a user certificate: **a.** Click **Add X509 Certificate**. The **Add X509 Certificate** dialog box appears. **b.** Enter a name in the **Name** field. **c.** Enter the X509 certificate in the **User X509 Certificate** text box. **d.** Click **Add**. The **X509 certificate in the User X509 Certificate** dialog box closes. You return to the **Local User** dialog box.
SSH Keys	To add a an SSH key: **a.** Click **Add SSH Key**. The **Add SSH Key** dialog box appears. **b.** Enter a name in the **Name** field. **c.** Enter the SSH key in the **Key** text box. **d.** Click **Add**. The **Add SSH Key** dialog box closes. You return to the **Local User** dialog box.

Step 6 Click **Save** when finished.

Managing Regions (Configuring a Cloud Template) Using the Cisco Cloud APIC GUI

Regions are configured during the first-time setup. When configured, you specify the regions that are managed by Cisco Cloud APIC and the region's inter-site and inter-region connectivity. This section explains how to manage regions with the cloud template using the Cisco Cloud APIC GUI after the initial installation.

For more information about cloud templates, see About the Cloud Template.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Configuration**.

A list of options appear in the **Intent** menu.

Step 3 From the **Configuration** list in the **Intent** menu, click **cAPIC Setup**. The **Set up - Overview** dialog box appears with options for **DNS and NTP Servers**, **Region Management**, and **Smart Licensing**.

Step 4 For **Region Management**, click **Edit Configuration**. The **Set Up - Region Management** dialog box appears with a list of managed regions.

Step 5 To choose a region that you want to be managed by the Cisco Cloud APIC, click to place a check mark in check box of that region. The **Cloud Routers** and **Inter-Site Connectivity** check boxes are enabled.

Step 6 To deploy cloud routers locally to this region, click to place a check mark in the **Cloud Routers** check box.

Step 7 To enable the cloud routers in the region to connect to on-premises ACI sites, click to place a check mark in the **Inter-Site Connectivity** check box. The **Cloud Routers** check box is automatically checked.

Step 8 To configure the fabric infra connectivity for the cloud site, click **Next**.

Step 9 Add the Fabric Autonomus System number for the Azure Cloud Site.

Step 10 To specify the subnet, click **Add Subnet for Cloud Router** and enter the subnet in the text box.

Note The /24 subnet provided during the cloud apic deployment would be sufficient for up to two cloud sites. If you need to manage more than two cloud sites, you need to add more subnets.

Step 11 To chose the number of routers per region, click the **Number of Routers Per Region** drop-down list and click **2**, **3**, or **4**.

Step 12 Enter a username in the **Username** text box.

Step 13 Enter a password in the **Password** and **Confirm Password** text boxes.

Step 14 To choose the throughput value, click the **Throughput of the routers** drop-down list.

Note Cloud routers should be undeployed from all regions before changing the throughput or login credentials.

Step 15 (Optional) To specify the license token, enter the product instance registration token in the **License Token** text box.

Note If no token is entered, the CSR will be in EVAL mode.

Step 16 To configure inter-site connectivity, click **Next**.

Step 17 To enter a peer public IP address of the IPsec Tunnel peer on-premises in the text box, click **Add Public IP of IPSec Tunnel Peer**.

Step 18 Enter the OSPF area ID in the **OSPF Area Id** text box.

Step 19 To add an external subnet pool, click **Add External Subnet** and enter a subnet pool in the text box.

Step 20 When you have configured all the connectivity options, click **Next** at the bottom of the page.

The **Cloud Resource Naming Rules** page appears, which is described in detail in the Cloud Resources Naming, on page 43 section. If you don't need to make any changes to the naming rules, you can skip this page.

Step 21 Click **Save and Continue** when finished.

Configuring Smart Licensing

This task demonstrates how to set up smart licensing in the Cisco Cloud APIC.

Before you begin

You need the product instance registration token.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Configuration**.

A list of options appear in the **Intent** menu.

Step 3 From the **Configuration** list in the **Intent** menu, click **Set Up cAPIC**. The **Set up - Overview** dialog box appears with options for **DNS Servers**, **Region Management**, and **Smart Licensing**.

Step 4 To register the Cloud APIC to Cisco's unified license management system: From **Smart Licensing**, click **Register**. The **Smart Licensing** dialog appears.

Step 5 Choose a transport setting:

- **Direct to connect to Cisco Smart Software Manager (CSSM)**
- **Transport Gateway/Smart Software Manager Satellite**
- **HTTP/HTTPS Proxy**

Note An IP address is alo required when choosing **HTTP/HTTPS Proxy**.

Step 6 Enter the product instance registration token in the provided text box.

Step 7 Click **Register** when finished.

Cloud Resources Naming

Prior to Cloud APIC Release 5.0(2), the cloud resources created by the Cloud APIC in Azure were assigned names that were derived from the names of the ACI objects:

- Resource groups were created based on the Tenant, VRF, and region. For example, `CAPIC_<tenant>_<vrf>_<region>`.
- VNET names matched the name of the Cloud APIC VRF.
- Subnet names were derived from the CIDR address space. For example, `subnet-10.10.10.0_24` for the `10.10.10.0/24` cloud subnet.
- The cloud application name was derived from the EPG name and the application profile name. For example, `<epg-name>_cloudapp_<app-profile-name>`

This approach is not ideal for deployments with strict cloud resource naming conventions and it does not follow the Azure best practices for naming and tagging of cloud resources.

Starting with Cloud APIC Release 5.0(2), you can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud. You can define custom naming rules for all cloud resources during the first time setup wizard of the Cloud APIC, with the exception of the **Resource group** name used for the Cloud APIC ARM template deployment. The resource group name for the template is defined when you first deploy it and cannot be changed after. In addition to the global policy, you can also explicitly define the names of the cloud resources created from each Cloud APIC object using the REST API.

Note Keep in mind that even with custom naming policy, once a cloud resource is created, you will not be able to modify the name. If you want to change the name of an existing cloud resource, you would need to delete all configured cloud resources and recreate them. Cloud resources to be deleted include overlay-2 CIDR and subnets, Cisco Cloud Services Router 1000Vs deployed by Cloud APIC and therefore IPSec tunnels from the CSRs to every remote site.

Variables Available for Naming Rules

When creating your cloud resources naming policy, you can use the following variables to dynamically define the name of the cloud resource based on the Cloud APIC objects:

- `${tenant}` – the resource will include the name of the Tenant
- `${ctx}` – the resource will include the name of the VRF
- `${ctxprofile}` – the resources will include the cloud context profile, which is a VRF deployed in a given cloud region
- `${app}` – the resource will include the name of the application profile.
- `${epg}` – the resource will include the name of the EPG.
- `${contract}` – the resource will include the name of the contract
- `${region}` – the resource will include the name of the cloud region
- `${priority}` – the resource will include the name of the network security group (NSG) rule priority. This number is allocated automatically to ensure that each NSG rule name is unique

When you define a global naming policy using one or more of the above variables, Cloud APIC validates the string to ensure that all mandatory variables are present and no invalid string is specified.

There is a maximum name length limit in Azure. If the length of the name exceeds the length supported by the cloud provider, it rejects the config and Cloud APIC raises a fault that the resource creation failed. You can then check the fault for details and correct the naming rules. The maximum length limits at the time of Cloud APIC, Release 5.0(2) are listed below, for the latest up-to-date information and any changes to the length limit, consult the Azure documentation.

The following table provides a summary of which cloud resources support each of the naming variables above. Cells denoted with an asterisk (*) indicate variables that are mandatory for that type of cloud resource. Cells denoted with a plus sign (+) indicate that at least one of these variables is mandatory for that type of cloud resource; for example, for VNET resources you can provide `${ctx}`, or `${ctxprofile}`, or both.

Table 18: Supported Variables for Cloud Resources

Azure Resource	${tenant}	${ctx}	${ctxprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
Resource Group Max Length: 90	Yes*	Yes*						Yes*	

Azure Resource	${tenant}	${ctx}	${cbprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
Virtual Network (VNET) Max Length: 64	Yes	Yes+	Yes+					Yes	
Subnet Max Length: 80	Yes	Yes	Yes	Yes*				Yes	
Application Security Group (ASG) Max Length: 80	Yes				Yes*	Yes*		Yes	
Network Security Group (NSG) Max Length: 80	Yes				Yes*	Yes*		Yes	
Network Security Group Rule Max Length: 80	Yes						Yes		Yes* (auto)

Naming Rules Guidelines and Limitations

When configuring custom rules for naming cloud resources, the following restrictions apply:

- You define global naming policy during the Cloud APIC's first time setup using two sets of naming rules:
  - **Hub Resource Naming Rules** define names for the Hub Resource Group, Hub VNET, and Overlay-1 CIDR subnet in the Infra Tenant, as well as the subnet prefixes for subnets that are created automatically by the system in the Infra tenant.
  - **Cloud Resource Naming Rules** define the names of the Network Security Group (NSG), Application Security Group (ASG), and subnets you create in the Infra Tenant, as well as the names of all resources (Resource Groups, Virtual Networks, Subnets, NSG, ASG) in user Tenants.

  After you define the naming rules, you will be required to review and confirm them. Keep in mind that you must confirm the naming rules before any cloud resources are deployed.
- Once a cloud resource is created, its name cannot be changed and the naming policy cannot be updated in the GUI. If you upgrade your Cloud APIC to Release 5.0(2) with some resources already deployed in Azure, you will also not be able to change the global custom naming rules.

  If you want to change the names of the existing cloud resources or the policy, you would need to delete the deployed resources before being able to update the global naming policy in the GUI.

  In these cases you can use the REST API to explicitly assign custom names to any new resources you create.
- When updating cloud resources naming via REST API, we recommend you do not import configuration at the same time.

  We recommend you define any naming rules first. Then any tenant configuration.

We recommend that you do not change the naming policy after the tenant configuration is deployed.

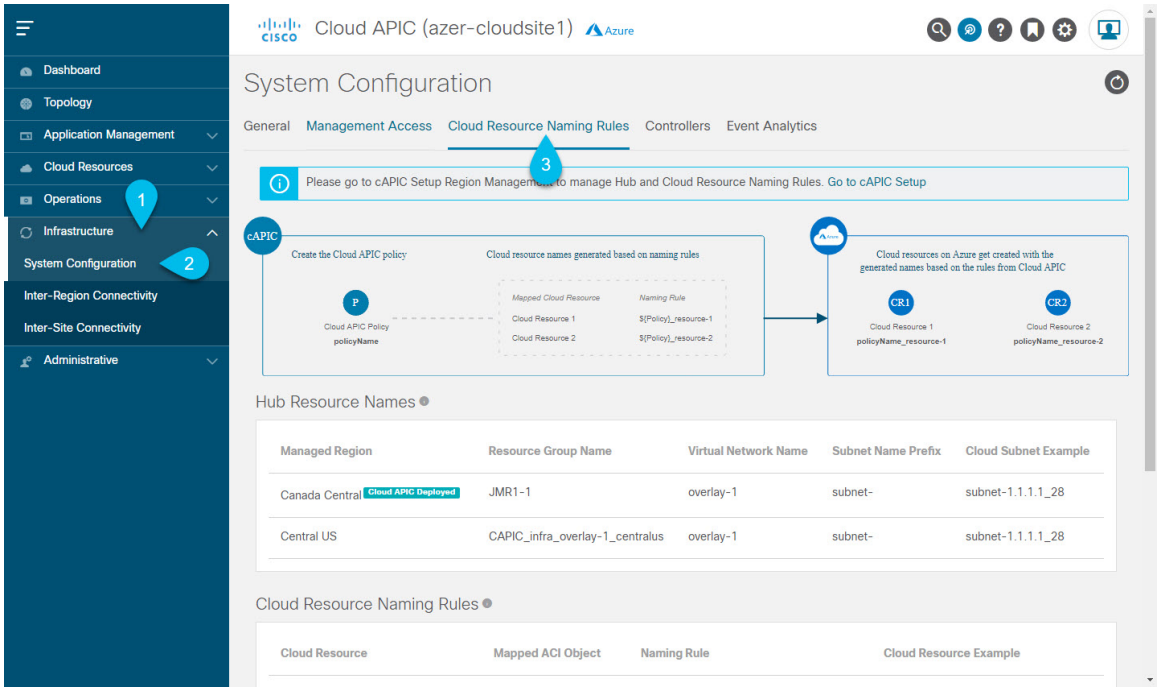
Viewing Cloud Resource Naming Rules

You initially define the cloud resource naming rules in the Region Management part of the first time setup wizard when you deploy your Cloud APIC, which is described in the *Cisco Cloud APIC Installation Guide*. After the initial setup, you can view the rules you configured in the **System Configuration** screen of your Cloud APIC GUI as described in this section.

Note that the information in this screen is presented in read-only view and if you want to change the rules any time after the original deployment, you will need to re-run the first time setup wizard .

Step 1 Log in to your Cloud APIC GUI.

Step 2 Navigate to the **Cloud Resource Naming Rules** screen.



a) In the **Navigation** sidebar, expand the **Infrastructure** category.

b) From the **Infrastructure** category, select **System Configuration**.

c) In the **System Configuration** screen, select the **Cloud Resource Naming Rules** tab.

In the **Cloud Resource Naming Rules** tab, you can see a summary of the currently configured rules for the names of resources that you deploy in the cloud site from your Cloud APIC.

If you did not configure custom naming rules before, the default rules are listed here, which use the Cloud APIC object names for cloud resources.

If you have not accepted the naming rules you have defined during the first time setup, a warning banner will be displayed across the top of the screen.

Note Keep in mind that you must confirm the naming rules before any cloud resources are deployed.

Configuring Cisco Cloud APIC Using the REST API

Creating a Tenant Using the REST API

There are two types of subscriptions: own and shared. Each subscription type has a primary tenant. You choose the own subscription when creating a new managed or unmanaged tenant. You choose the shared subscription when creating a tenant that inherits the managed or unmanaged settings of an existing primary tenant. This section demonstrates how to create a managed and unmanaged tenant with the own type of subscription and how to create a shared subscription.

This section demonstrates how to create a tenant using the REST API using sample POST requests from the body of Postman.

Step 1 Create an own subscription.

a) To create an unmanaged tenant using a client secret:

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{primary-tenant-name}}">
    <cloudAccount id="{{user-tenant-subscription-id}}" vendor="azure" accessType="credentials"
status="">
       <cloudRsCredentials tDn="uni/tn-{{primary-tenant-name }}/credentials-{{ primary-tenant-name
 }}"/>
    </cloudAccount>
    <cloudCredentials name="{{ primary-tenant-name }}" keyId="{{application_key_id}}"
key="{{client_secret_key}}">
        <cloudRsAD tDn="uni/tn-{{ primary-tenant-name }}/ad-{{active_directory_id}}"/>
    </cloudCredentials>
    <cloudAD name="{{active_directory_name}}" id="{{active_directory_id}}" />
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
}}]-vendor-azure" status=""/>
</fvTenant>
```

b) To create a managed tenant:

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{ primary-tenant-name }}">
    <cloudAccount id="{{ user-tenant-subscription-id }}" vendor="azure" accessType="managed"
status="" />
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
}}]-vendor-azure" status=""/>
</fvTenant>
```

Step 2 Create a shared subscription:

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml
```

```
<fvTenant name="{{ primary-tenant-name }}">
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
}}]-vendor-azure" status=""/>
</fvTenant>
```

Creating a Contract Using the REST API

This example demonstrates how to create a contract for the Cisco Cloud APIC using the REST API.

Before you begin

Create filters.

To create a contract:

Example:

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

Creating a Cloud Context Profile Using the REST API

This section demonstrates how to create a cloud context profile.

Before you begin

Create a VRF.

To create a cloud context profile:

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">

    <cloudCtxProfile name="cProfilewestus151">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
      <cloudRsToCtx tnFvCtxName="ctx151"/>
    <cloudCidr addr="15.151.0.0/16" primary="true" status="">
```

```
          <cloudSubnet ip="15.151.1.0/24" name="GatewaySubnet" usage="gateway">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
          <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
    </cloudCidr>

    </cloudCtxProfile>

  </fvTenant>
</polUni>
```

Managing a Cloud Region Using the REST API

This section demonstrates how to manage a cloud region using the REST API.

To create a cloud region:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
       <cloudProvP vendor="azure">
          <cloudRegion adminSt="managed" name="eastus"><cloudZone name="default"/></cloudRegion>
          <cloudRegion adminSt="managed" name="eastus2"><cloudZone name="default"/></cloudRegion>
          <cloudRegion adminSt="managed" name="westus"><cloudZone name="default"/></cloudRegion>
        </cloudProvP>
    </cloudDomP>
</polUni>
```

Creating a Filter Using the REST API

This section demonstrates how to create a filter using the REST API.

To create a filter:

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="t15">
    <vzFilter name="rule1">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>
    <vzFilter name="rule2">
      <vzEntry etherT="ip" dToPort="http" prot="tcp" dFromPort="http" name="http"/>
```

```
    </vzFilter>
    <vzFilter name="rule3">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
    </vzFilter>
    <vzFilter name='all_rule'>
        <vzEntry etherT="ip" prot="unspecified" name="any"/>
  </vzFilter>

    <vzBrCP name="c1">
        <vzSubj name="c1">
            <vzRsSubjFiltAtt tnVzFilterName="rule2"/>
            <vzRsSubjGraphAtt tnVnsAbsGraphName="c13_g1"/>
            <vzRsSubjFiltAtt tnVzFilterName="rule3"/>
            <vzRsSubjFiltAtt tnVzFilterName="all_rule"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

Creating an Application Profile Using the REST API

This section demonstrates how to create an application profile using the REST API.

Before you begin

Create a tenant.

To create an application profile:

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">

    </cloudApp>

  </fvTenant>
</polUni>
```

Creating a Cloud EPG Using the REST API

This example demonstrates how to create a cloud EPG using the REST API.

Before you begin

Create an application profile and a VRF.

To create a cloud EPG:

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">


        <cloudEPg name="epg1">
            <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
            <cloudEPSelector matchExpression="custom:tag1=='value1'" name="selector-1"/>
        </cloudEPg>


    </cloudApp>

  </fvTenant>
</polUni>
```

Creating an External Cloud EPG Using the REST API

This example demonstrates how to create an external cloud EPG using the REST API.

Before you begin

Create an application profile and a VRF.

To create an external cloud EPG:

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="internet" name="extEpg-1">
```

```
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
            <cloudExtEPSelector name="extSelector1" subnet="0.0.0.0/0"/>
        </cloudExtEPg>


    </cloudApp>

  </fvTenant>
</polUni>
```

Creating a Cloud Template Using the REST API

This section demonstrates how to create a cloud template using the REST API. For more information about cloud templates, see About the Cloud Template.

Before you begin

To create a cloud template:

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2" numRoutersPerRegion="2"
status="" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="250M" routerLicenseToken="thisismycsrtoken" />
              </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="westus"/>
        <cloudRegionName provider="azure" region="westus2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="azure" region="westus2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

Defining Global Cloud Resource Naming Rules or Overriding Specific Object's Name

This section provides an example REST API POST you can use to configure a global policy for naming your cloud resources or override a specific cloud resource's name.

Note To ensure that any custom naming conventions can be supported, cloud resource names can be defined on a per-object basis. These explicit name overrides are not available in the Cloud APIC GUI and can be done using REST API only. We recommend using the global cloud resource naming policy to define the names. Explicit name overrides shouldf be used only when naming requirements cannot be met using the global naming policy.

Step 1 To create Hub Resource Naming Rules:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2"
    numRoutersPerRegion="2" status="" vrfName="overlay-1">
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="west's" status="">
          <cloudtemplateRegionNameCustomization ctxProfileName="infra-vnet"
          resourceGroupName="infra-rh" subnetNamePrefix="snet-" />
        </cloudRegionName>
      </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

Step 2 To create Cloud Resource Naming Rules:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
    <cloudNaming
    azResourceGroup="${tenant}-network-${ctx}-${region}-rg"
    azVirtualNetwork="${tenant}-${ctxprofile}-vnet"
    azSubnet="${tenant}-${ctxprofile}-snet-${subnet}"
    azNetworkSecurityGroup="${app}-${epg}-nsg"
    azApplicationSecurityGroup="${app}-${epg}-asg"
    azNetworkSecurityGroupRule="${contract}--${priority}"
    reviewed="yes" />
  </cloudDomP>
</polUni>
```

Step 3 To override an Azure cloud resource name corresponding to a specific Cloud APIC object:

You can use the same variables (for example, `${tenant}`) when specifying the custom name using the API.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<fvTenant name="ExampleCorp" status="">
  <fvRsCloudAccount status="" tDn="uni/tn-infra/act-[<infra-subscription>]-vendor-azure"/>
  <fvCtx name="VRF1"/>
```

```
  <cloudApp name="App1">
    <cloudEPg name="Db" azNetworkSecurityGroup="db-nsg" azApplicationSecurityGroup="db-asg-${region}">

      <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
      <cloudEPSelector matchExpression="custom:EPG=='db'" name="100"/>
    </cloudEPg>
  </cloudApp>
  <cloudCtxProfile name="c02" azResourceGroup="custom-tc-rg1" azVirtualNetwork="vnet1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
    <cloudRsToCtx tnFvCtxName="VRF1"/>
    <cloudCidr addr="10.20.20.0/24" name="cidr1" primary="yes" status="">
      <cloudSubnet ip="10.20.20.0/24" name="subnet1" azSubnet="s1" status="">
        <cloudRsZoneAttach status="" tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
      </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>
</fvTenant>
```