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 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

The following sections describe how to create a managed tenant or unmanaged tenant.

Setting Up the Google Cloud Project for a User Tenant

Perform the procedures in this section to set up the Google Cloud project for a user tenant, where that user tenant is either a managed or an unmanaged tenant.

Step 1 Create a Google Cloud project for the user tenant, if necessary.

Each user tenant is mapped one-to-one to a Google Cloud project. If you do not have a Google Cloud project created yet for your user tenant, follow these procedures to create a Google Cloud project.

a) Log into your Google account.
b) Navigate to **IAM & Admin** > **Manage resources**.

c) Using the **Select organization** drop-down list at the top of the page, choose the organization where you want to create a project.

d) Click **+ CREATE PROJECT**.

e) In the **New Project** window that appears, enter a project name and select a billing account as applicable.

   A project name can contain only letters, numbers, single quotes, hyphens, spaces, or exclamation points, and must be between 4 and 30 characters.

f) Enter the parent organization or folder in the **Location** field.

   That resource will be the hierarchical parent of the new project.

g) Click **CREATE**.

Step 2 In Google Cloud, enable the appropriate service APIs in the service account associated with this user tenant.

a) In the Google Cloud GUI, log into the Google Cloud project that is associated with this user tenant.
   The **Dashboard** for the project is displayed.

b) In the search bar at the top of the **Dashboard**, search for **APIs & Services**, then click the result from that search to access the **APIs & Services** window.

c) In the **APIs & Services** window, click the **+ ENABLE APIS AND SERVICES** tab.

   The **API Library** window appears.

d) In the **Search for APIs & Services** field, search for and enable the necessary services.

   For each of the services in the list below:

   1. Search for the API or service in the **Search for APIs & Services** field.
   2. Click on the search result to display the page for that API or service.
   3. Click the **ENABLE** button in that API or service page.

   Following are the APIs and services that you must search for and enable:

   - Compute Engine API
   - Cloud Deployment Manager V2 API
   - Cloud Pub/Sub API
   - Cloud Resource Manager API
   - Service Usage API
   - Cloud Logging API

   Each API or service takes several minutes to enable. You will have to navigate back to the **APIs & Services** window after you enable each API or service.

   Note that the following additional APIs and services should be enabled automatically when you enable all of the APIs and services listed above:

   - Identity and Access Management (IAM) API
   - IAM Service Account Credentials API
   - Cloud OS Login API
   - Cloud DNS API

- Recommender API

If they are not enabled automatically, enable them manually.

Step 3 Set the necessary permissions for this user tenant in Google Cloud.

a) In the Google Cloud GUI, log into the Google Cloud project that is associated with this user tenant.
The **Dashboard** for the project is displayed.

b) In the left nav bar, click on **IAM & Admin**, then choose **IAM**.

The **IAM** window appears with several service accounts displayed.

c) Locate the appropriate service account.

d) Set the permissions for this service account.

1. Click the pencil icon on the row for this service account.

   The **Edit Permissions** window is displayed.

2. Click **+ ADD ANOTHER ROLE**, then choose **Editor** as the role.

   You are returned to the **IAM** window with the service accounts displayed.

3. Click **+ ADD ANOTHER ROLE** again, then add the remaining necessary roles for this service account.

   Following is the full list of roles that you must assign to this service account, including the Cloud Functions Service Agent that you added in the first step of this process:

   - Editor
   - Role Admin
   - Project IAM Admin

4. After you have added all the necessary roles, click **SAVE**.

   You are returned to the **IAM** window with the service accounts displayed and the necessary roles assigned to this service account.

Creating a Managed Tenant

The following sections provide the information that you'll need to create a managed tenant, where you will:

- Create a managed tenant in Cisco Cloud APIC
- Set the necessary permissions for the managed tenant in Google Cloud

Creating a Managed Tenant Using the Cisco Cloud APIC GUI

This section explains how to create a tenant that will be managed by Cisco Cloud APIC using the GUI.

Step 1 Set up the Google Cloud project for the user tenant.

See Setting Up the Google Cloud Project for a User Tenant, on page 1 for those procedures.

Step 2 In the Cisco Cloud APIC GUI, navigate to **Application Management** > **Tenants**.

A table of already-configured tenants is displayed.

Step 3 Click **Actions** and choose **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. Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.
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.
Google Cloud Project	
Google Cloud Project ID	Enter the Google Cloud Project ID that will be associated with this Cisco Cloud APIC tenant.
Access Type	For a tenant that will be managed by the Cisco Cloud APIC, choose **Managed Identity** as the access type. For more information, see Understanding Google Cloud Deployments with Cisco Cloud APIC.
Add Security Domain for Google Cloud Project	**Note** Adding a security domain for Google Cloud is optional when creating a tenant. To add a security domain for the account: **a.** Click **Add Security Domain for Google Cloud Project**. 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.

What to do next

Complete the necessary configurations in Google Cloud for the managed tenant. Go to Setting the Necessary Permissions in Google Cloud for a Managed Tenant, on page 5 for those procedures.

Setting the Necessary Permissions in Google Cloud for a Managed Tenant

If you are creating a managed tenant, you must now set the necessary permissions in Google Cloud.

Note You do not have to follow the steps in this procedure if you are creating an unmanaged tenant.

Step 1 In the Google Cloud GUI, log into the Google Cloud project that is associated with this managed tenant.

The **Dashboard** for the project is displayed.

Step 2 In the left nav bar, click on **IAM & Admin**, then choose **IAM**.

The **IAM** window appears with several service accounts displayed.

Step 3 Locate the service account that was created in the project that is associated with the infra account.

Step 4 Copy the service account name.

Step 5 Add this service account name as an IAM user in the user tenant project.

Step 6 Set the permissions for this service account.

a) Click the pencil icon on the row for this service account.

The **Edit Permissions** window is displayed.

b) Click **+ ADD ANOTHER ROLE**, then choose **Cloud Functions Service Agent** as the role.

You are returned to the **IAM** window with the service accounts displayed.

c) Click **+ ADD ANOTHER ROLE** again, then add the remaining necessary roles for this service account.

Following is the full list of roles that you must assign to this service account, including the Cloud Functions Service Agent that you added in the first step of this process:

- Cloud Functions Service Agent
- Compute Instance Admin (v1)
- Compute Network Admin
- Compute Security Admin
- Logging Admin
- Pub/Sub Admin
- Storage Admin

d) After you have added all the necessary roles, click **SAVE**.

You are returned to the **IAM** window with the service accounts displayed and the necessary roles assigned to this service account.

Creating an Unmanaged Tenant

The following sections provide the information that you'll need to create an unmanaged tenant, where you will:

- Generate and download the necessary private key information from Google Cloud for an unmanaged tenant
- Create an unmanaged tenant in Cisco Cloud APIC

Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant

If you are creating an unmanaged tenant, you must first generate and download the necessary private key information from Google Cloud.

Note You do not have to follow the steps in this procedure if you are creating a managed tenant.

Step 1 In Google Cloud, select the Google Cloud project that will be associated with this unmanaged tenant, if you have not selected it already .

Step 2 In the left nav bar, click on **IAM & Admin**, then choose **Service Accounts**.

The service accounts for this Google Cloud project are displayed.

Step 3 Select an existing service account or click **+ CREATE SERVICE ACCOUNT** to create a new one.

Information on this service account is displayed, with the **Details** tab selected by default.

Step 4 Click the **KEYS** tab.

Step 5 Click **ADD KEY** > **Create New Key**.

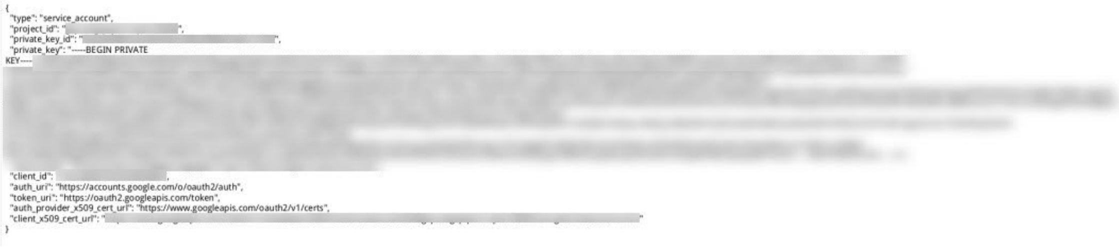
A window appears, providing an option to create a private key for this service account.

Step 6 Leave the **JSON** key type selected, then click **Create**.

A window appears, saying that the private key has been saved to your computer.

Step 7 Locate the JSON file that was downloaded to your computer and move it to a secure location on your computer.

This JSON file will contain the key information that you need to fill in the fields for the unmanaged tenant.



```
{
  "type": "service_account",
  "project_id": "[redacted]",
  "private_key_id": "[redacted]",
  "private_key": "-----BEGIN PRIVATE
KEY----[redacted]
  "client_id": [redacted],
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "[redacted]"
}
```

Creating an Unmanaged Tenant Using the Cisco Cloud APIC GUI

This section explains how to create a tenant that will not be managed by Cisco Cloud APIC using the GUI.

Before you begin

Complete the procedures provided in Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 6 before proceeding with the procedures in this section.

Step 1 Set up the Google Cloud project for the user tenant.

See Setting Up the Google Cloud Project for a User Tenant, on page 1 for those procedures.

Step 2 In the Cisco Cloud APIC GUI, navigate to **Application Management** > **Tenants**.

A table of already-configured tenants is displayed.

Step 3 Click **Actions** and choose **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 2: Create Tenant Dialog Box Fields

Properties	Description
Name	Enter the name of the tenant. Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.
Description	Enter a description of the tenant.
Settings	

Properties	Description
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.
Google Cloud Project	
Google Cloud Project ID	Enter the Google Cloud Project ID that will be associated with this Cisco Cloud APIC tenant.
Access Type	For a tenant that will not be managed by the Cisco Cloud APIC, choose **Unmanaged Identity** as the access type. For more information, see Understanding Google Cloud Deployments with Cisco Cloud APIC.
Key ID	Enter the information from the `private_key_id` field in the JSON file that you downloaded in Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 6.
RSA Private Key	Enter the information from the `private_key` field in the JSON file that you downloaded in Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 6.
Client ID	Enter the information from the `client_id` field in the JSON file that you downloaded in Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 6.
Email	Enter the email address associated with your Google Cloud project.
Add Security Domain for Google Cloud Project	**Note** Adding a security domain for Google Cloud is optional when creating a tenant. To add a security domain for the account: **a.** Click **Add Security Domain for Google Cloud Project**. 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.

Note the following restrictions:

- Match the regular expression:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

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.

Note To configure a external VRF, you will select infra in the **Tenant** field below. The VRF will be identified as a external VRF if it is:

- Configured under the infra tenant
- Associated with an external network (see Creating an External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI, on page 11)
- Not associated with a cloud context profile

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 3: Create VRF Dialog Box Fields

Properties	Description
General	
Name	Enter a name for the VRF in the **Name** field. Note the following restrictions: • Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen. • We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name. 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*.

Properties	Description
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 External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI

This procedure describes how to create an external network. You can have a single external network that can connect to multiple routers on the on-premises site, or you can have multiple external networks with multiple VRFs that you can use to connect to CCRs.

Before you begin

You must have a hub network created before you can create an external network.

Step 1 In the left navigation bar, navigate to **Application Management** > **External Networks**.
The configured external networks are displayed. Note that because Cisco Cloud APIC supports only one hub network, you will see only one hub network displayed in the **Hub Network** column.

Step 2 Click **Actions**, then choose **Create External Network**.
The **Create External Network** window appears.

Note If there is no hub network configured yet, you will see a warning at the top of the page, saying that you must create a hub network before you can create an external network. Click the blue `Cloud APIC Setup` link in the message to create a hub network, then return here. For more information on creating a hub network, see the "Configuring Cisco Cloud APIC Using the Setup Wizard" chapter in the Cisco Cloud APIC for Google Cloud Installation Guide, Release 25.0(x) or later.

Step 3 Enter the appropriate values in each field as listed in the following *Create External Network Dialog Box Fields* table then continue.

Table 4: Create External Network Dialog Box Fields

Properties	Description
General	
Name	Enter the name for the external network.

Properties	Description
VRF	This external VRF will be used for external connectivity with the on-premises CCR. You can create multiple external VRFs for this purpose. This VRF will be identified as an external VRF if the VRF has all three of the following characteristics: • Configured under the `infra` tenant • Associated with an external network • Not associated with a cloud context profile Any VRF that is associated with an external network becomes an external VRF. At that point, that external VRF is not allowed to be created under any tenant other than the infra tenant, and that external VRF is not allowed to be associated with a cloud context profile or subnet. To choose an external 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. You can also create a VRF using the **+ Create VRF** option. **c.** Click **Select**. You return to the **Create External Network** dialog box.
Hub Network	The hub network is displayed automatically after you configured it in the First Time Setup. **Note** If there is no hub network configured yet, you must create a hub network before you can create an external network. For more information on creating a hub network, see the "Configuring Cisco Cloud APIC Using the Setup Wizard" chapter in the Cisco Cloud APIC for Google Cloud Installation Guide, Release 25.0(x) or later.
VPN Router	This field is not editable. The default VPN router is automatically selected.
Settings	
Regions	To choose a region: **a.** Click **Add Regions**. The **Select Regions** dialog box appears. • The regions that you selected as part of the First Time Setup are displayed here. • You can select multiple regions to bring up the cloud router in multiple regions. **b.** From the **Select Regions** dialog, click to choose a region in the left column then click **Select**. You return to the **Create External Network** dialog box.

Properties	Description
VPN Networks	The VPN networks entries are used for internal connectivity. All configured VPN networks will be applied to all the selected regions. To add a VPN network: **a.** Click **Add VPN Network**. The **Add VPN Network** dialog box appears. **b.** In the **Name** field, enter a name for the VPN network. **c.** Click **+ Add IPSec Peer**. Two tunnels are created for each IPSec peer entry. **d.** Enter values for the following fields for the IPSec peer that you want to add: • **Public IP of IPSec Tunnel Peer** • **Pre-Shared Key** • **IKE Version**: Select **ikev1** or **ikev2** for IPSec tunnel connectivity • **BGP Peer ASN** • **Subnet Pool Name**: Click **Select Subnet Pool Name**. The **Select Subnet Pool Name** dialog box appears. Select one of the available subnet pools that are listed, then click **Select**. **Note** Additional IPsec tunnel subnet pools can be added in the **External Networks** page, or through the Cloud APIC First Time Set Up, if necessary. For more information on adding additional subnet pools through the Cloud APIC First Time Set Up, see the chapter "Configuring Cisco Cloud Network Controller Using the Setup Wizard" in the *Cisco Cloud APIC for GCP Installation Guide*, Release 25.0(1)- 25.0(4). The subnet pool size should be large enough to accommodate the number of IPsec tunnels that will get created. **e.** Click the checkmark to add this IPSec tunnel. Click **+ Add IPSec Tunnel** if you want to add another IPSec tunnel. **f.** Click **Add** in the **Add VPN Network** dialog box. You return to the **Create External Network** dialog box.

Step 4 When you have finished creating the external network, click **Save**.
After you click **Save** in the **Create External Network** window, cloud routers are then configured in Google Cloud.

To verify that cloud routers were configured in Google Cloud, in your Google Cloud account, navigate to **Hybrid Connectivity** > **Cloud Routers**. You should see the cloud routers created for the different regions (note that you might have to click Refresh to bring up the newly-configured cloud routers).

To see the IPSec sessions, navigate to **Hybrid Connectivity** > **VPN** > **Cloud VPN Tunnels**.

Configuring Inter-VRF Route Leaking Using the Cisco Cloud APIC GUI

Using inter-VRF route leaking, you can configure an independent routing policy to specify which routes to leak between a pair of VRFs when you are setting up routing between these types of sites:

- Two cloud sites
- A cloud site and a non-ACI on-premises site

Note See Configuring Routing and Security Policies Separately for more information.

Step 1 In the left navigation bar, navigate to **Application Management** > **VRFs**.
The configured VRFs are displayed.

Step 2 Click the **Leak Routes** tab.
Any already-configured leak routes are displayed.

Step 3 Click **Actions**, then choose **Create Leak Route**.
The **Create Leak Route** window appears.

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

Table 5: Create Leak Routes Dialog Box Fields

Properties	Description
Source VRF	To choose a source VRF: **a.** Click **Select a Source VRF**. The **Select a VRF** dialog box appears. **b.** From the **Select a VRF** dialog, click to choose a VRF in the left column to use for the source VRF. Note that the source VRF can be an internal or an external (transport) VRF. **c.** Click **Select** to select this source VRF. You return to the **Create Leak Route** dialog box.
Destination VRF	To choose a destination VRF: **a.** Click **Select a Destination VRF**. The **Select a VRF** dialog box appears. **b.** From the **Select a VRF** dialog, click to choose a VRF in the left column to use for the destination VRF. **c.** Click **Select** to select this destination VRF. You return to the **Create Leak Route** dialog box.

Properties	Description
Type	Choose the type of leaked route that you want to configure: • **Leak All**: Select to configure all routes to leak between the VRFs. The entry `0.0.0.0/0` is entered automatically in the subnet IP area by default in this case. • **Subnet IP**: Select to configure a specific subnet IP address as the route to leak between VRFs. The **Subnet IP** box appears. In the **Subnet IP** box, enter a subnet IP address as the route to leak between VRFs. To configure multiple subnet IP addresses as the route to leak between VRFs, enter additional entries for the different subnets.

Step 5 When finished, click **Save**.
The **Success** window appears.

Step 6 Determine if you want to configure additional inter-VRF route leaking.

- If you want to add another route to leak between a pair of VRFs, click the **Add Another Route** option in the **Success** window.

  You are returned to the **Add Leak Route** window. Repeat Step 4, on page 14 through Step 5, on page 15 to configure another route to leak between a pair of VRFs.

- If you want to add a reverse route, where:

  - The destination VRF from the previous configuration now becomes the source VRF, and
  - The source VRF from the previous configuration now becomes the destination VRF

  Then click the **Add Reverse Route** option in the **Success** window.

  You are returned to the **Add Leak Route** window. Repeat Step 4, on page 14 through Step 5, on page 15 to configure another route, but this time:

  - In the **Source VRF** field, select the VRF that you had selected as a destination VRF in the previous configuration.
  - In the **Destination VRF** field, select the VRF that you had selected as a source VRF in the previous configuration.

Step 7 When you have finished configuring leak routes, click **Done**.

The **Leak Routes** tab in the main **VRFs** page is displayed again, with the newly configured leak route displayed.

Step 8 To get more information on a source or destination VRF, or to make changes to a configured leak route, double-click the VRF in the **Leak Routes** tab in the main **VRFs** page.
The **Overview** page for that VRF is displayed.

Step 9 Click the **Application Management** tab at the top of the VRF page, then click the **Leak Routes** tab in the left nav bar.
The leak routes associated with this particular VRF are displayed.

Step 10 Configure additional leak routes associated with this VRF, if necessary.

- To add a leak route from this VRF, click **Actions**, then choose **Add Leak Route from <VRF_name>**.

The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in Step 4, on page 14. Note that the entry in the **Source VRF** is pre-selected and cannot be changed in this situation.

- To add a leak route to this VRF, click **Actions**, then choose **Add Leak Route to <VRF_name>**.

  The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in Step 4, on page 14. Note that the entry in the **Destination VRF** is pre-selected and cannot be changed in this situation.

Enabling Connectivity Between Google Cloud and External Devices

Follow these procedures to manually enable connectivity between a Google Cloud Router and an external device.

Downloading the External Device Configuration Files

Step 1 In the Cisco Cloud APIC GUI, click on **Dashboard**.
The **Dashboard** view for the Cisco Cloud APIC appears.

Step 2 In the **Connectivity** area, under **External Connectivity Status**, click on the number above the **Cloud Routers** entry.
The **External Connectivity** window appears.

Step 3 Click **Actions** > **Download External Device Configuration Files**.
The **Download External Device Configuration Files** pop-up appears.

Step 4 Select the external device configuration files to download and click **Download**.
This action downloads a zip file that contains configuration information that you will use to enable connectivity between the Google Cloud Router and the external devices.

Enabling Connectivity Between Google Cloud and the External Devices

Before you begin

Download the external device configuration files using the procedures in Downloading the External Device Configuration Files, on page 16.

Step 1 Gather the necessary information that you will need to enable connectivity between the Google Cloud Router and the external devices.

Step 2 Log into the external device.

Step 3 Enter the configuration information to connect an external networking device with the cloud ACI fabric.

If you downloaded the external device configuration files using the instructions in Downloading the External Device Configuration Files, on page 16, locate the configuration information for the first tunnel and enter that configuration information.

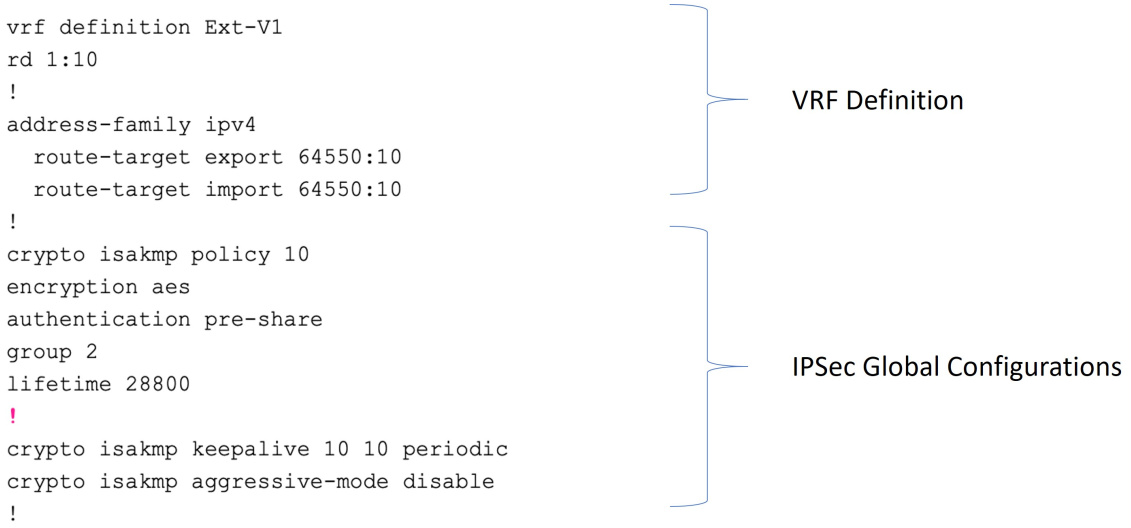
Following is an example of what the external device configuration file might look like for the first tunnel, where **PRESHARED-KEY** is taken from the vpn-connectivity configuration page:

```
! The following file contains configuration recommendation to connect an external networking device
 with the cloud ACI Fabric
! The configurations here are provided for an IOS-XE based device. The user is expected to understand
 the configs and make any necessary amends before using them
! on the external device. Cisco does not assume any responsibility for the correctness of the config.

! Tunnel to 54.215.245.58 5.500 for
hcextnwTunnIf.acct-[infra]/region-[us-west1]/hubCtx-[1]-id-[0]/ext-[extnwfoo_us-west1]/vpn-[vpnnwfoo]/rtr-default-peer-54.215.245.58/src-1-dest-[54.215.245.58]
! USER-DEFINED: please define rd: RD
! USER-DEFINED: please provide preshared-key: PRESHARED-KEY
! USER-DEFINED: please define router-id: ROUTER-ID
! USER-DEFINED: please define gig-number: GIG-NUMBER
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! ikev: ikev2
! vrf-name: extv1
! user name: root
! tunnel counter: 5
! IPV4 address: 35.220.50.132
! tunnel interface destination: 54.215.245.58
! tunne id: 500
! BGP peer address: 169.254.10.6
! BGP peer neighbor address: 169.254.10.5
! BGP peer ASN: 64513
! hcloudHubCtx ASN: 64512

vrf definition extv1
    rd RD:1
    address-family ipv4
    exit-address-family
exit

interface Loopback0
    vrf forwarding extv1
    ip address 41.41.41.41 255.255.255.255
exit


crypto ikev2 proposal ikev2-1
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-1
    proposal ikev2-1
exit

crypto ikev2 keyring keyring-root-5
    peer peer-ikev2-keyring
        address 35.220.50.132
        pre-shared-key PRESHARED-KEY
    exit
exit

crypto ikev2 profile ikev-profile-root-5
    match address local interface GIG-NUMBER
    match identity remote address 35.220.50.132 255.255.255.255
    identity local address 54.215.245.58
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-root-5
    lifetime 3600
    dpd 10 5 periodic
```

```
exit

crypto ipsec transform-set ikev-transport-root-5 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev-profile-root-5
    set transform-set ikev-transport-root-5
    set pfs group14
    set ikev2-profile ikev-profile-root-5
exit

interface Tunnel500
    vrf forwarding extv1
    ip address 169.254.10.6 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GIG-NUMBER
    tunnel mode ipsec ipv4
    tunnel destination 35.220.50.132
    tunnel protection ipsec profile ikev-profile-root-5
exit

ip route 35.220.50.132 255.255.255.255 GIG-NUMBER GIG-GATEWAY

router bgp 64513
    bgp router-id ROUTER-ID
    bgp log-neighbor-changes

    address-family ipv4 vrf extv1
        network 41.41.41.41 mask 255.255.255.255
        neighbor 169.254.10.5 remote-as 64512
        neighbor 169.254.10.5 ebgp-multihop 255
        neighbor 169.254.10.5 activate
    exit-address-family
exit
```

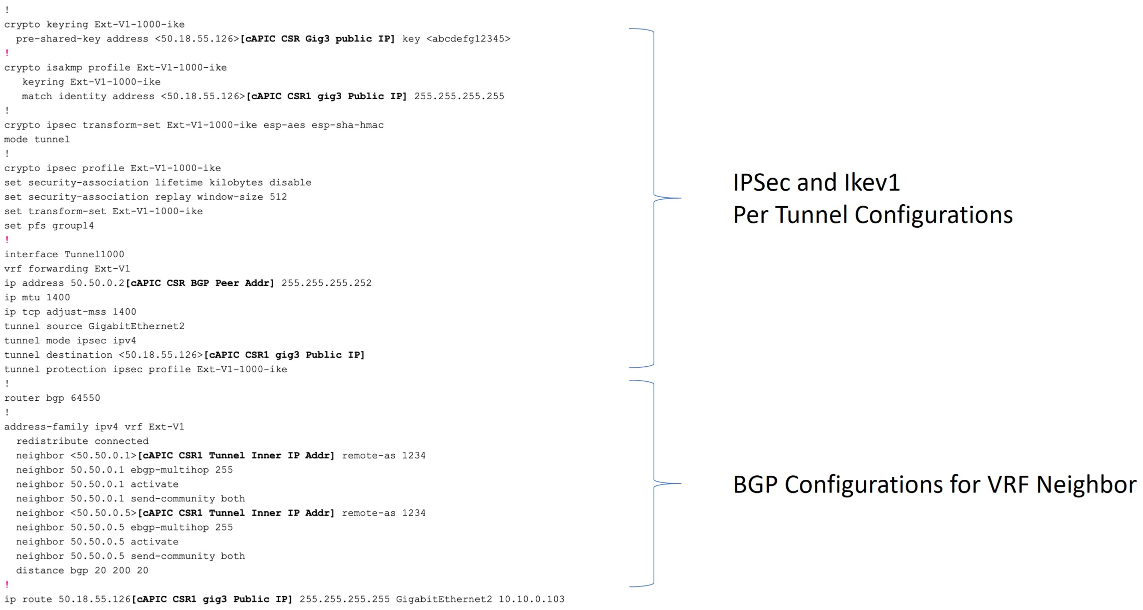
The following figures provide more information on what each set of fields is used for in the external device configuration file:

- The fields shown in the following figure are used to configure these areas:
    - VRF definition
    - IPSec global configurations



```
vrf definition Ext-V1
rd 1:10
!
address-family ipv4
  route-target export 64550:10
  route-target import 64550:10
!
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
lifetime 28800
!
crypto isakmp keepalive 10 10 periodic
crypto isakmp aggressive-mode disable
!
```

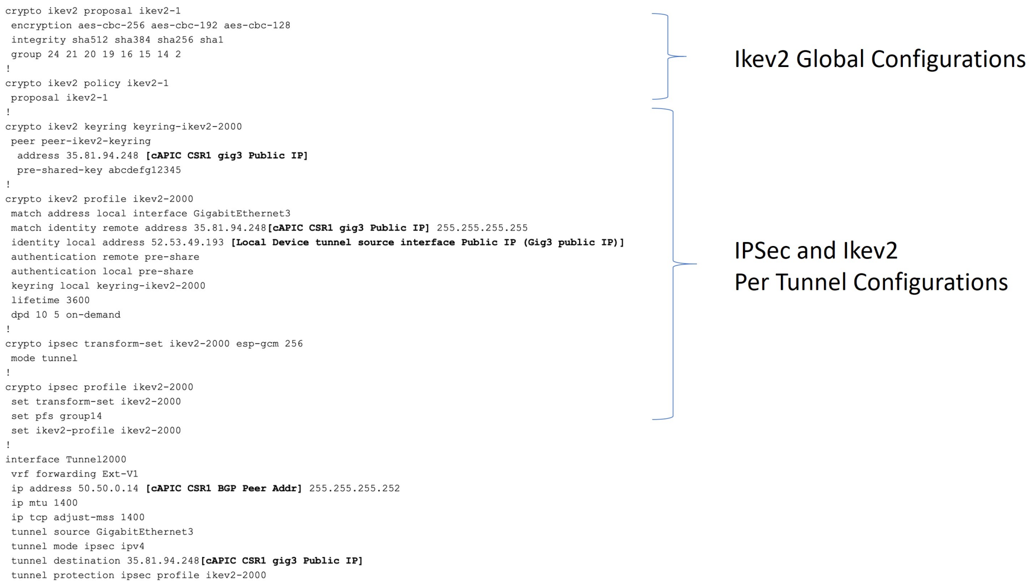
- The fields shown in the following figure are used to configure these areas:
    - IPSec and ikev1 per tunnel configurations
    - BGP configurations for the VRF neighbor



```
!
crypto keyring Ext-V1-1000-ike
  pre-shared-key address <50.18.55.126>[cAPIC CSR Gig3 public IP] key <abcdefg12345>
!
crypto isakmp profile Ext-V1-1000-ike
   keyring Ext-V1-1000-ike
   match identity address <50.18.55.126>[cAPIC CSR1 gig3 Public IP] 255.255.255.255
!
crypto ipsec transform-set Ext-V1-1000-ike esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile Ext-V1-1000-ike
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set Ext-V1-1000-ike
set pfs group14
!
interface Tunnel1000
vrf forwarding Ext-V1
ip address 50.50.0.2[cAPIC CSR BGP Peer Addr] 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1400
tunnel source GigabitEthernet2
tunnel mode ipsec ipv4
tunnel destination <50.18.55.126>[cAPIC CSR1 gig3 Public IP]
tunnel protection ipsec profile Ext-V1-1000-ike
!
router bgp 64550
!
address-family ipv4 vrf Ext-V1
  redistribute connected
  neighbor <50.50.0.1>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.1 ebgp-multihop 255
  neighbor 50.50.0.1 activate
  neighbor 50.50.0.1 send-community both
  neighbor <50.50.0.5>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.5 ebgp-multihop 255
  neighbor 50.50.0.5 activate
  neighbor 50.50.0.5 send-community both
  distance bgp 20 200 20
!
ip route 50.18.55.126[cAPIC CSR1 gig3 Public IP] 255.255.255.255 GigabitEthernet2 10.10.0.103
```

IPSec and Ikev1
Per Tunnel Configurations
BGP Configurations for VRF Neighbor

- The fields shown in the following figure are used to configure these areas:
    - Ikev2 global configurations
    - IPSec and ikev2 per tunnel configurations



```
crypto ikev2 proposal ikev2-1
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1
 group 24 21 20 19 16 15 14 2
!
crypto ikev2 policy ikev2-1
 proposal ikev2-1
!
crypto ikev2 keyring keyring-ikev2-2000
 peer peer-ikev2-keyring
  address 35.81.94.248 [cAPIC CSR1 gig3 Public IP]
  pre-shared-key abcdefg12345
!
crypto ikev2 profile ikev2-2000
 match address local interface GigabitEthernet3
 match identity remote address 35.81.94.248[cAPIC CSR1 gig3 Public IP] 255.255.255.255
 identity local address 52.53.49.193 [Local Device tunnel source interface Public IP (Gig3 public IP)]
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-ikev2-2000
 lifetime 3600
 dpd 10 5 on-demand
!
crypto ipsec transform-set ikev2-2000 esp-gcm 256
 mode tunnel
!
crypto ipsec profile ikev2-2000
 set transform-set ikev2-2000
 set pfs group14
 set ikev2-profile ikev2-2000
!
interface Tunnel2000
 vrf forwarding Ext-V1
 ip address 50.50.0.14 [cAPIC CSR1 BGP Peer Addr] 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel destination 35.81.94.248[cAPIC CSR1 gig3 Public IP]
 tunnel protection ipsec profile ikev2-2000
```

Creating an EPG Using the Cisco Cloud APIC GUI

Use the procedures in this section to create an application EPG or an external EPG. The available configuration options vary, depending on which type of EPG you are creating.

Creating an Application EPG Using the Cisco Cloud APIC GUI

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

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 6: Create EPG Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the EPG. Note the following restrictions: • Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen. • We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.
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. **c.** Click **Select**. You return to the **Create EPG** dialog box.
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	Because this will be an application EPG, choose **Application** as the EPG type.
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. **c.** Click **Select**. You return to the **Create EPG** dialog box.

Properties	Description
Endpoint Selectors	

Properties	Description
	Note See Configuring Virtual Machines in Google Cloud, on page 36 for instructions on configuring virtual machines in Google Cloud 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 Google Cloud 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 for an expression that does not contain 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 • **Value:** us-west1

Properties	Description
	• 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 us-west1 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:** us-east1, us-central1 In this case: • If the region is us-west1 AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions) OR • If the region is either us-east1 or us-central1 (endpoint selector 2 expression) Then that end point is assigned to the Cloud EPG.

Step 5 Click **Save** when finished.

Creating an External EPG Using the Cisco Cloud APIC GUI

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

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 7: Create EPG Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the EPG. Note the following restrictions: • Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen. • We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.
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. **c.** Click **Select**. You return to the **Create EPG** dialog box.
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	Because this will be an external EPG, choose **External** as the EPG type.

Properties	Description
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. **c.** Click **Select**. You return to the **Create EPG** dialog box.
Route Reachability	The type of route reachability for the external EPG will be automatically selected (either **Internet** or **External-Site**).
Endpoint Selectors	**Note** See Configuring Virtual Machines in Google Cloud, on page 36 for instructions on configuring virtual machines in Google Cloud as part of the endpoint selector configuration process. To add an endpoint selector: **a.** Click **Add Endpoint Selector** to add an endpoint selector. **b.** Enter a name in the **Name** field. **c.** Enter a subnet in the **Subnet**. **d.** When finished, click the check mark to validate the endpoint selector. **e.** Determine if you want to create additional endpoint selectors. If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you created two endpoint selectors: • Endpoint selector 1: • **Name:** EP_Sel_1 • **Subnet:** 192.1.1.1/24 • Endpoint selector 2: • **Name:** EP_Sel_2 • **Subnet:** 192.2.2.2/24 In this case: • If the IP address belongs to the 192.1.1.1/24 subnet (endpoint selector 1) OR • If the IP address belongs to the 192.2.2.2/24 subnet (endpoint selector 2) 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 8: 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.

Properties	Description
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 allowed, including IP, and the remaining fields are disabled. **d.** Click the **IP Protocol** drop-down menu to choose a protocol. The options are: • **ICMP** • **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 9: Create Contract Dialog Box Fields

Properties	Description
Name	Enter the name of the contract. Note the following restrictions: • Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen. • We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.
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. **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. 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.

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 10: Create Contract Dialog Box Fields

Properties	Description
Name	Enter the name of the contract. This is the name of the contract in Google Cloud. Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.
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. **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 11: Create Cloud Context Profile Dialog Box Fields

Properties	Description
Name	Enter the name of the cloud context profile. Match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.
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.

Properties	Description
Settings	
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.

Properties	Description
Add CIDR	**Note** See Understanding VPCs and Subnets Under Google Cloud and Cloud Context Profiles Under Cloud APIC for more information on primary and secondary CIDRs and subnet group labels. To add a CIDR: **a.** Click **Add CIDR**. The **Add CIDR** dialog box appears. **b.** Enter the address in the **CIDR Block Range** field. **c.** Click to check (enabled) or uncheck (disabled) the **Primary** check box. • You must have at least one primary CIDR added for each cloud context profile. • If you are adding additional secondary CIDRs and subnets for VPCs, leave the **Primary** box unchecked. **d.** Click **Add Subnet** and enter the following information: • In the **Address** field, enter the subnet address. • In the **Name** field, enter the name for this subnet. • In the **Subnet Group Label** field, choose one of the following: • **Select Existing**: Click **Select Subnet Group Label**, then choose an existing subnet group label to associate with this subnet. • **Create New**: Enter a unique name for the subnet group label to associate with this subnet. **e.** In the **VRF** field, make a selection, if necessary. • If you checked the box next to the **Primary** field, this CIDR is automatically associated with the primary VRF. • If you did not check the box next to the **Primary** field, you can associate this CIDR with a secondary VRF. Click the **X** next to the VRF, then click on **Select VRF** to select the secondary VRF to associate with this CIDR. **f.** When finished, click **Add**.

Step 5 Click **Save** when finished.

Configuring Virtual Machines in Google Cloud

When you configure endpoint selectors for Cisco Cloud APIC, you will also need to configure the virtual machines that you will need in Google Cloud 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 Google Cloud. You can use these requirements to configure the virtual machines in Google Cloud either before you configure the endpoint selectors for Cisco Cloud APIC or afterward.

For example, assume that you are using **Custom** as the type of endpoint selector, as described in Endpoints and Endpoint Selectors.

- You might go to your account in Google Cloud and create a custom tag or label in Google Cloud 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 Google Cloud and create a custom tag or label in Google Cloud afterward.

Before you begin

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

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

- VRF name
- Subnet information
- Google Cloud Project 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 Google Cloud 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 Google Cloud virtual machine.

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

Note For information about how to create the VM in the Google Cloud portal, see the Google Cloud 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 12: 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	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. • **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 specific object to use as the root of the object tree to backup.

Properties	Description
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 13: 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.

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 14: 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** • **Even Days** • **Odd Days** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** **b.** From the **Start Time** field, enter a time. **c.** In the **Maximum Concurrent Tasks** field, choose one of the following: • **Unlimited**: There is no maximum number of concurrent tasks that can be enforced on the scheduler window. • **Custom**: In the second **Maximum Concurrent Tasks** field, enter the maximum number of tasks that can be processed concurrently. The maximum value allowed in this field is 65535. **d.** In the **Maximum Running Time** field, choose one of the following: • **Unlimited**: There is no time limit enforced on the scheduler window. • **Custom**: In the second **Maximum Running Time** field, enter the maximum duration of the window. The acceptable format for this field is `dd:hh:mm:ss`. **e.** Click **Add** when finished.

Properties	Description
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 15: 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**

Properties	Description
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 16: Create Login Domain Dialog Box Fields

Properties	Description
Name	Enter the name of the login domain.
Description	Enter a description of the login domain.

Properties	Description
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.
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.

Properties	Description
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 **Security** > **Security Domains** > **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 In the **Type** field, choose the type of security domain:

- **Unrestricted**: Users who are assigned to this domain are able to see policies, profiles, or users configured in other security domains.
- **Restricted**: Users who are assigned to this domain will not be able to see policies, profiles, or users configured in other security domains.

Step 7 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 17: 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**—Used for Layer 1-3 configuration under infra, static route configurations under a tenant's L3Out, management infra policies, and tenant ERSPAN policies. • **access-equipment**—Used for access port configuration. • **access-protocol**—Used for Layer 1-3 protocol configurations under infra, fabric-wide policies for NTP, SNMP, DNS, and image management, and operations-related access policies such as cluster policy and firmware policies. • **access-qos**—Used for changing CoPP and QoS-related policies. • **admin**—Complete access to everything (combine ALL roles) • **config-manager** • **custom-port-privilege** • **custom-privilege-1 through custom-privilege-22** • **fabric-connectivity**—Used for Layer 1-3 configuration under the fabric, firmware and deployment policies for raising warnings for estimating policy deployment impact, and 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**—Used for Layer 1-3 protocol configurations under the fabric, fabric-wide policies for NTP, SNMP, DNS, and image management, ERSPAN and health score policies, and firmware management traceroute and endpoint tracking policies. • **none**—No privilege. • **nw-svc-params**—Used for managing Layer 4 to Layer 7 service policies. • **nw-svc-policy**—Used for managing Layer 4 to Layer 7 service devices and network service orchestration. • **ops**—Used for operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies. • **site-admin** • **site-policy** • **tenant-connectivity**—Used for Layer 1-3 connectivity changes, including bridge domains, subnets, and VRFs; for atomic counter, diagnostic, and image management policies on leaf switches and spine switches; tenant in-band and out-of-band management

Properties	Description
	connectivity configurations; and debugging/monitoring policies such as atomic counters and health score. • **tenant-epg**—Used for managing tenant configurations such as deleting/creating endpoint groups, VRFs, and bridge domains. • **tenant-ext-connectivity**—Used for write access firmware policies; managing tenant L2Out and L3Out configurations; and debugging/monitoring/observer policies. • **tenant-ext-protocol**—Used for managing tenant external Layer 1-3 protocols, including BGP, OSPF, PIM, and IGMP, and for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk. Generally only used for write access for firmware policies. • **tenant-network-profile**—Used for managing tenant configurations, such as deleting and creating network profiles, and deleting and creating endpoint groups. • **tenant-protocol**—Used for managing configurations for Layer 1-3 protocols under a tenant, for tenant traceroute policies, and as write access for firmware policies. • **tenant-qos**—Only used as Write access for firmware policies. • **tenant-security**—Used for Contract related configurations for a tenant. • **vmm-policy**—Used for managing policies for VM networking.

Step 5 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 18: Create Certificate Authority Dialog Box Fields

Properties	Description
Name	Enter the name of the certificate authority.
Description	Enter a description of the certificate authority.
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 19: 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 20: Create Local User Dialog Box Fields

Properties	Description
Username	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. • **Blocked**—Blocks the local user account. • **Inactive**—Deactivates the local user account.

Properties	Description
First Name	Enter the first name of the local user.
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 21: 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.

Property	Description
Password Update Required	If you choose **Yes**, the user must change the password upon the next login.
OTP	Put a check in the box to enable the one-time password feature for the user.
User Certificate Attribute	The attribute for the user certificate.
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

With Google Cloud, the VPC resource is a global resource, which means that it spans all Google Cloud regions. By default, all regions are managed by Google Cloud and inter-region connectivity is present. Cisco Cloud APIC manages all 25 Google Cloud regions.

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

Step 2 In the **Workflows** area, click **Cloud APIC Setup**.
The **Set up - Overview** dialog box appears with options for **DNS and NTP Servers**, **Region Management**, and **Smart Licensing**.

Step 3 For **Region Management**, click **Edit Configuration**.
The **Region Management** window appears.

Step 4 Determine if you want to configure external connectivity.

Click the box next to **Enable** to enable external connectivity.

Step 5 Verify that all of the regions in the page are selected.

This page shows all of the regions that are supported by Google Cloud. All of the regions are managed by Cisco Cloud APIC.

Step 6 Click **Next** at the bottom of the page.

If you enabled external connectivity, the **General Connectivity** page appears.

Step 7 Enter the necessary information in the **Hub Network** area.

Hub network management is used to deploy cloud routers on specific managed regions. Configure the fabric infra connectivity for the cloud site and define the configuration template used for the cloud routers in the cloud site in this area.

Note the following restrictions:

- You can create only one hub network in Google Cloud.
- Under the hub network, only one cloud router is created in Google Cloud.

a) In the **Hub Network** area, click **Add Hub Network**.

The **Add Hub Network** window appears.

b) In the **Name** field, enter a name for the hub network.

c) Enter a value in the **BGP Autonomous System Number** field.

The BGP Autonomous System Number (ASN) is used for BGP peering inside the cloud site and for MP-BGP IPv4 peering to other sites.

The ASN must be a private ASN. Enter a value between 64512 and 65534 or between 4200000000 and 4294967294, inclusive, for each hub network, then click the check mark next to the field.

d) In the **Region** field, select the appropriate regions.

You can add up to four regions to deploy hub network in this area. The hub network will create one cloud router in each region selected.

e) In the **VPN Router** field, enter a name for the VPN router.

The infra VPC uses the cloud router and VPN Gateway to create IPSec tunnels and BGP sessions to on-premises sites or other cloud sites. The spoke VPCs peer with the infra VPC to share the VPN connections to external sites.

Step 8 Enter the necessary information in the **IPSec Tunnel Subnet Pools** area.

a) In the **IPSec Tunnel Subnet Pools** area, click **Add IPSec Tunnel Subnet Pools**.

The **Add IPSec Tunnel Subnet Pools** window appears.

b) Enter the subnet pool to be used for IPSec tunnels, if necessary.

By default, a subnet pool of `169.254.0.0/16` is populated to create the IPsec tunnels. You can delete the existing subnet pool and add additional subnet pools, if necessary.

The subnets used for the **IPSec Tunnel Subnet Pools** entry must be common /30 CIDRs from the `169.254.0.0/16` block. For example, `169.254.7.0/24` and `169.254.8.0/24` would be acceptable entries for the subnet pools in this field.

Click the check mark after you have entered in the appropriate subnet pools.

Step 9 When you have entered all the necessary information on this page, click **Save and Continue** at the bottom of the page.

You are given the option to create external networks and complete external connectivity configurations, if necessary. Go to Creating an External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI, on page 11 for those procedures.

Configuring Cisco Cloud APIC Using the REST API

Creating a Tenant Using the REST API

Before you begin

Review the information provided in Understanding Google Cloud Deployments with Cisco Cloud APIC before proceeding with the procedures in this section.

Step 1 Enter the following POST to share the same credentials across multiple tenants, where you are duplicating the `cloudCredentials` object in each tenant and specifying the same Google Cloud Service Account.

Note the following:

- Tenant `T1` defines the `cloudCredentials` object that carries the private key for the Service Account.
- Both tenant `T1` and `T2` then refer to this `cloudCredentials` object through the `cloudRsCredentials` relation.
- The Service Account defined by tenant `T1` must be a member of Google Cloud Projects `project1` and `project2` in this scenario.
- The highlighted areas in the POST for tenant T2 show the credentials that are shared with the first user tenant

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

<fvTenant name="T1">
    <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-T1/credentials-creds1" />
    </cloudAccount>
    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T1/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-T2/credentials-creds1" />
    </cloudAccount>
```

```
   <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

Step 2 To create a user tenant where the Cisco Cloud APIC runs outside of Google Cloud (the infra tenant with credentials):

Note that the new properties added specifically for Google Cloud are highlighted below.

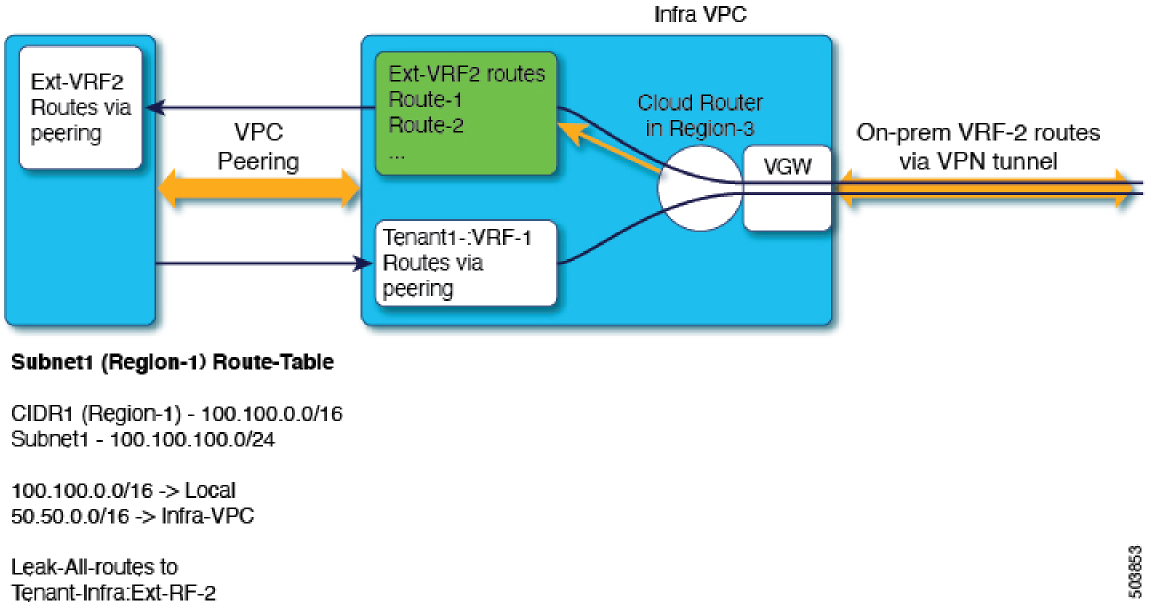
```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
    </cloudAccount>
    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
    </cloudAccount>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

Step 3 To create a managed user tenant where the user shares the infra service account across multiple Google Cloud projects:

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

<fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

Configuring Inter-VRF Route Leaking Using the REST API

This example demonstrates how to configure leak routes for the Cisco Cloud APIC using the REST API. This example shows how to configure inter-VRF route leaking, between an external VRF and a cloud VRF, as shown in the following figure.


Infra VPC
Ext-VRF2 Routes via peering
VPC Peering
Ext-VRF2 routes
Route-1
Route-2
...
Cloud Router in Region-3
VGW
On-prem VRF-2 routes via VPN tunnel
Tenant1-:VRF-1 Routes via peering
Subnet1 (Region-1) Route-Table
CIDR1 (Region-1) - 100.100.0.0/16
Subnet1 - 100.100.100.0/24
100.100.0.0/16 -> Local
50.50.0.0/16 -> Infra-VPC
Leak-All-routes to
Tenant-Infra:Ext-RF-2
503853

To configure inter-VRF route leaking for this example:

Example:

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="VRF1">
            <leakRoutes>
                <leakInternalPrefix ip="0.0.0.0/0" status="">
                    <leakTo tenantName="infra" ctxName="Ext-VRF2" scope="public" status=""/>
                </leakInternalPrefix>
            </leakRoutes>
        </fvCtx>
        <cloudCtxProfile name="v1-us-west1" type="regular" vpcGroup="one" status="">
            <cloudRsToCtx tnFvCtxName="VRF1"/>
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
            <cloudCidr addr="100.100.0.0/16" primary="yes">
                <cloudSubnet ip="100.100.100.0/20" scope="public,shared" subnetGroup="one">
                    <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
    <fvTenant name="infra" status="">
        <fvCtx name="Ext-VRF2">
            <leakRoutes>
                <leakExternalPrefix ip="0.0.0.0/0" status="">
                    <leakTo tenantName="t1" ctxName="VRF1" scope="public" status=""/>
                </leakInternalPrefix>
            </leakRoutes>
        </fvCtx>
    </fvTenant>
</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 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:

```
<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>
```

Note the following restrictions for the name of the contract (the `vzBrCP` entry):

- Match the regular expression:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

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.

Step 1 To create a basic cloud context profile:

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
  <cloudCtxProfile name="cProfilewest1151">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
   <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-gcp/region-us-west1/zone-default"/>
    </cloudSubnet>
    <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
      <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
    </cloudSubnet>
     <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
       <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
    </cloudSubnet>
  </cloudCidr>
  </cloudCtxProfile>
 </fvTenant>
</polUni>
```

Step 2 To create a cloud context profile where you are adding a secondary VRF, CIDR, and subnet for a VNet:

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tenant1" status="">
        <fvCtx name="VRF1" />
        <fvCtx name="VRF2” />
        <cloudCtxProfile name="vpc1" status="">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-central1" status=""/>
            <cloudRsToCtx tnFvCtxName="VRF1" />
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
            <cloudCidr name="cidr1" addr="192.0.2.0/16" primary="yes" status="">
                <cloudSubnet ip="192.0.3.0/24" usage="gateway" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-gcp/region-us-central1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr name="cidr1" addr="193.0.2.0/16" primary="no" status="">
                <cloudSubnet ip="193.0.3.0/24" usage="" status="">
                    <cloudRsSubnetToCtx tnFvCtxName="VRF2"/>
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-gcp/region-us-central1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </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-[<gcp-id>]-vendor-gcp" />


        <fvCtx name="ctx151"/>

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

    </cloudApp>

  </fvTenant>
</polUni>
```

For the application profile name, note the following restrictions:

- Match the regular expression:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

Creating an EPG Using the REST API

Use the procedures in this section to create an application EPG or an external EPG using the REST API.

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:

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


        <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>
```

Note the following restrictions:

- Match the regular expression:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

Creating an External Cloud EPG Using the REST API

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

For the name of the external EPG, note the following restrictions:

- Match the regular expression:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to Naming Length Restrictions Imposed By Google Cloud Firewall Rules to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

Before you begin

Create an application profile and a VRF.

Step 1 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-[<gcp-id>]-vendor-gcp" />
        <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>
```

Step 2 To create an external cloud EPG with type **site-external**, or an infra L3Out EPG:

Example:

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

```
<polUni>
    <fvTenant name="infra">
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="ctx152"/>
            <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

Creating Cloud Routers, External Networks, and External VRFs Using the REST API

This section demonstrates how to create cloud routers, external networks, and external VRFs using the REST API.

Following is an example POST that shows how to bring up the cloud router in four regions and add an external network with an external VRF in each region.

```
<polUni>
    <fvTenant name="infra" status="">
        <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
         <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
          <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

           <cloudtemplateInfraNetwork name="default" vrfName="overlay-1" hostRouterMode="manual"
status="">
            <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24" poolname="pool1" />
             <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24" poolname="pool2" />
              <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24" poolname="pool3" />

            <cloudtemplateHubNetwork name="default" status="" >
                <cloudtemplateHubNetworkName name="foo1" asn="64514" status="">
                    <cloudRegionName provider="gcp" region="us-west4" status="" />
                    <cloudRegionName provider="gcp" region="us-west2" status="" />
                    <cloudRegionName provider="gcp" region="us-east1" status="" />
                      <cloudRegionName provider="gcp" region="us-west1" status=""/>
                </cloudtemplateHubNetworkName>
            </cloudtemplateHubNetwork>

            <cloudtemplateIntNetwork name="default">
                <cloudRegionName provider="gcp" region="us-west1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-west2">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-east1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                  </cloudRegionName>
                    <cloudRegionName provider="gcp" region="us-west4">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
            </cloudtemplateIntNetwork>
            <cloudtemplateExtNetwork name="default">
         </cloudtemplateExtNetwork>
               <cloudtemplateExtNetwork name="extnwfoo1" vrfName="extv1" hubNetworkName="foo1"
vpnRouterName="default" status="">
                    <cloudRegionName provider="gcp" region="us-west1" status=""/>
                       <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">
                 <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd" poolname="pool1"
 status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
            <cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
vpnRouterName="default" status="">
             <cloudRegionName provider="gcp" region="us-west2" status=""/>
                <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
                       <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
poolname="pool2" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
             <cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3" hubNetworkName="foo1"
vpnRouterName="default" status="">
                <cloudRegionName provider="gcp" region="us-east1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
                       <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
poolname="pool3" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
                  </cloudtemplateExtNetwork>
        </cloudtemplateInfraNetwork>
    </fvTenant>
</polUni>
```