Completing the Initial Configuration

Configuring an External Network

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 Configuring Cisco Cloud APIC Using the Setup Wizard.

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

Table 1: 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**. **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**.

Creating a Tenant

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

Understanding Google Cloud Deployments with Cisco Cloud APIC

Google Cloud organizes resources in a way that resembles a file system, where:

- The *Organization* at the top level can have multiple *Folders*.
- Every *Folder* can contain other *Folders*, or can contain *Projects*, where every *Project* has a unique ID.
- Cloud *resources* (such as VMs, VPCs, and subnets) are contained within a *Project*.

While the Organization and Folder levels are useful areas to understand from the Google Cloud perspective, the Project level is the most relevant from the Cisco Cloud APIC perspective.

Each Cisco Cloud APIC tenant is mapped one-to-one to a Google Cloud Project, which means that:

- A Cisco Cloud APIC tenant cannot span multiple Google Cloud Projects
- There cannot be more than one Cisco Cloud APIC tenant in a Google Cloud Project

With Cisco Cloud APIC, Google Cloud provides access to Projects using **Service Accounts**. These accounts are meant for applications that need to access Google Cloud services. They can be used to run and deploy Cisco Cloud APIC and to push policies for other tenants. Service accounts used in applications running within Google Cloud do not need credentials, whereas applications that are run external to Google Cloud need a pre-generated private key. Service Accounts reside in one Google Cloud Project, but they can also be given access to manage policies for other Projects (for Cisco Cloud APIC, other tenants).

The following sections provide more information on different ways that Cisco Cloud APIC tenants can be configured with Google Cloud:

- User Tenants With Managed Credentials, on page 4
- User Tenants With Unmanaged Credentials, on page 5

User Tenants With Managed Credentials

This type of user tenant has the following characteristics:

- This tenant account is managed by the Cisco Cloud APIC.
- You will first choose **Managed Identity** in the Cisco Cloud APIC GUI as part of the tenant configuration process for this type of user tenant.
- After you have configured the necessary parameters in the Cisco Cloud APIC, you must then set the necessary roles for this tenant in Google Cloud. Add the service account created by the Cloud APIC as an IAM user with the following rules:
  - Cloud Functions Service Agent
  - Compute Instance Admin (v1)
  - Compute Network Admin
  - Compute Security Admin
  - Logging Admin
  - Pub/Sub Admin
  - Storage Admin

For instructions on creating this sort of tenant, see Creating a Managed Tenant Using the Cisco Cloud APIC GUI, on page 7.

User Tenants With Unmanaged Credentials

This type of user tenant has the following characteristics:

- This tenant account is not managed by the Cisco Cloud APIC.
- Before configuring the necessary parameters in the Cisco Cloud APIC for this type of tenant, you must first download the JSON file that contains the necessary private key information from Google Cloud for the service account associated with this tenant.
- You will then choose **Unmanaged Identity** in the Cisco Cloud APIC GUI as part of the tenant configuration process for this type of user tenant. As part of the configuration process for this type of tenant in Cisco Cloud APIC, you will provide the following information from the downloaded JSON file:
  - Key ID
  - RSA Private Key
  - Client ID
  - Email

For instructions on creating this sort of tenant, see Creating an Unmanaged Tenant Using the Cisco Cloud APIC GUI, on page 11.

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 5 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	
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, on page 4.
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 9 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.

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 10 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 5 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 3: 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.

Properties	Description
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, on page 4.
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 10.
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 10.
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 10.
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.