



Deploying the Cisco Cloud Network Controller in Google Cloud

- [Creating a Project in Google Cloud for the Infra Tenant, on page 1](#)
- [Generating an SSH Key Pair in Linux or MacOS, on page 4](#)
- [Deploying the Cisco Cloud Network Controller in Google Cloud, on page 5](#)
- [Deleting a Cisco Cloud Network Controller Deployment in Google Cloud, on page 10](#)

Creating a Project in Google Cloud for the Infra Tenant

This procedure describes how to create a project in Google Cloud, enable the appropriate APIs and services on the project, and assign appropriate permissions to the service account.

The tenant that will be created in these procedures will be referred to as the infra tenant.

Step 1 Log into your Google Cloud account.

Step 2 Create or use an existing project that will be used for Cisco Cloud Network Controller.

See [Creating and managing projects](#) in the Google Cloud documentation for those instructions.

If you are using an existing project, verify that there is no previous Cisco Cloud Network Controller deployment on this project. If there is a previous Cisco Cloud Network Controller deployment on this project, delete that existing deployment using the instructions in [Deleting a Cisco Cloud Network Controller Deployment in Google Cloud \(External Connectivity Using Google Cloud Routers\)](#), on page 11.

Step 3 Enable the appropriate APIs and services on your project.

- In the Google Cloud GUI, navigate to the project that you created for Cisco Cloud Network Controller. The **Dashboard** for your project is displayed.
- 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.
- In the **APIs & Services** window, click the + **ENABLE APIS AND SERVICES** tab.
The **API Library** window appears.
- 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 Logging API
- Cloud Pub/Sub API
- Cloud Resource Manager API
- Cloud Runtime Configuration API
- Identity and Access Management (IAM) API
- Service Usage 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:

- IAM Service Account Credentials API
- Cloud OS Login API
- Recommender API

If they are not enabled automatically, enable them manually.

Step 4 Assign the appropriate permissions to the service account.

There are two types of service accounts:

- **Service account for the project:** This service account allows for the deployment of the Cisco Cloud Network Controller.
- **Service account for the user:** This service account communicates with the APIs. Instead of having a user login or password, this service account acts on behalf of the project and will create resources.

For this step, you will be assigning the appropriate permissions to the service account for the project.

- a) In the Google Cloud GUI, navigate back to the **Dashboard** window for your Cisco Cloud Network Controller project.
- 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 for the deployment.

Locate the service account with the entry `Google APIs Service Agent` shown in the **Name** column (also listed with `<project_number>@cloudservices.gserviceaccount.com` in the **Principal** column).

This service account should have been created automatically when you enabled the APIs in the previous step. If this service account was not created automatically, follow these steps to create it manually:

1. Verify that the **PRINCIPALS** tab is selected in the **IAM** window.
2. Click **ADD** at the top part of the window.
3. In the **New Principals** field, enter the name for this service account:
`<project_number>@cloudservices.gserviceaccount.com`
4. Click **SAVE**.

d) Add the necessary role entries for this service account.

You should see the following entry in the **Role** column for this service account:

- Editor

You will also have to add these additional roles for this service account:

- Project IAM Admin
- Role Administrator

To add the additional role entries 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 search for and choose the `Project IAM Admin` role entry.
3. Click + **ADD ANOTHER ROLE** again, then search for and choose the `Role Administrator` role entry.
4. Click **SAVE**.

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

Step 5 Verify that the Google Cloud account has N2 CPUs quota set to at least 16 in the region where the Cisco Cloud Network Controller is deployed, and that the quotas are currently not used.

If this is not the case, raise a case with Google Cloud to increase the quota limit.

Quotas for project "██████████" [EDIT QUOTAS](#)

Near the limit 0 View quotas	Low usage 5,523 View quotas	All quotas 5,754
--	---	---------------------

Filter: Quota: N2 CPUs Enter property name or value

Service	Quota	Dimensions (e.g. location)	Limit	Current usage percentage	7 day peak usage percentage
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: australia-southeast1	500	3.2%	3.2%
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: us-east4	500	0%	3.2%
<input type="checkbox"/> Compute Engine API	N2 CPUs	zone: australia-southeast1-a	Unlimited	16	16
<input type="checkbox"/> Compute Engine API	N2 CPUs	zone: us-east4-c	Unlimited	0	16
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: asia-east1	500	0%	0%
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: asia-east2	500	0%	0%
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: asia-northeast1	200	0%	0%
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: asia-northeast2	200	0%	0%
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: asia-northeast3	200	0%	0%
<input type="checkbox"/> Compute Engine API	N2 CPUs	region: asia-south1	500	0%	0%

Generating an SSH Key Pair in Linux or MacOS

These procedures describe how to generate an SSH public and private key pair in Linux or MacOS.

Step 1 On your Linux virtual machine or Mac, create a public and private key pair using `ssh-keygen`, directing the output to a file.

```
# ssh-keygen -t rsa -f ~/.ssh/cnc-ssh-key -C admin
```

Step 2 Locate the public key file that you saved.

The public key file is saved in this file:

```
~/.ssh/cnc-ssh-key.pub
```

Step 3 Open the public key file and copy the public key information from that file.

The public key information will be in this format:

```
ssh-rsa <public-key-string> admin
```

Verify that you've copied all of the necessary public key information, including the `ssh-rsa` text at the beginning and the `admin` text at the end.

Following is an example of the public key information that you would copy from the file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAgQCA0Aom7Mblv+w7yWE7QOPytvpankAdOsNwd7keptT6nAnr
S2UjHP0c0KCOjABEO7fL0hwQpwKmlRfHi0poQ3FAy7Oof6XcFJx5aCcCayrGDhm96HPbcPoXjhhg0FufR4QyL9cWpbsKn9K1k
OhnIw+KQyaxCQS1DlwMsgREKMDrkdK5MZazqZC8haThaaAO/h+i+OQ9juo6N6QPUogHRZ+E9ztyGU/buU1/0vvnvzTTinvw8aq
mTnPUQxNI6wZ2FpMH8JHiDQ924wIboAEq0tvidnElemG5wsQrwUghD7r1D9uWjI1rsfGAJL8mSIkWBXZFo+AqN1bE69Oa1TIL
```

```
2DfmgYQm3M+qWdzaZPI6i+Ap/dMgGKyy8M4VGFN0o+wbkzi1XdEbMpSEBxyuDtoB5H9T4Kov2yuH/RdqPMSSt+ZgNgBZgc16S  
HXlpSA0GmwyHljYNizo70UMI2JDJDmUc4vCNMgVRxWkNraCWYEZD5iMjnAtIiZvQmZKQwBH0GY3XIc= admin
```

What to do next

Follow the instructions in [Deploying the Cisco Cloud Network Controller in Google Cloud, on page 5](#) to continue the Google Cloud configuration process, which includes pasting the public key information into the Google Cloud deployment template.

Deploying the Cisco Cloud Network Controller in Google Cloud

- Step 1** Log into your Google Cloud account for the Cisco Cloud Network Controller infra tenant.
- Step 2** Navigate to the Google Cloud Marketplace.
- Step 3** In the search bar, search for:
- ```
Cisco Cloud Network Controller
```
- and select the result from that search.
- Step 4** In the **Cisco Cloud Network Controller** window in the Google Cloud Marketplace, click **LAUNCH**. The **New Cisco Cloud Network Controller deployment** window appears.

**i** Product preview. Go through the deployment flow available to Cloud Marketplace customers. Pricing info may not reflected in the preview

Deployment name \*

Zone  
us-east4-c ▼ ?

**Machine type**

**Machine family**


**GENERAL-PURPOSE** COMPUTE-OPTIMIZED MEMORY-OPTIMIZED

Machine types for common workloads, optimized for cost and flexibility

Series  
N2 ▼

Powered by Intel Cascade Lake and Ice Lake CPU platforms

Machine type  
n2-standard-16 (16 vCPU, 64 GB memory) ▼

|                                                                                     | vCPU | Memory |
|-------------------------------------------------------------------------------------|------|--------|
|  | 16   | 64 GB  |

SSH Public key \* ?

**Step 5** In the **New Cisco Cloud Network Controller deployment** window, enter the necessary information in the following fields:

- **Deployment name:** Enter a unique name for this Cisco Cloud Network Controller deployment.
- **Zone:** Select the zone where the Cisco Cloud Network Controller will be deployed.

The Cisco Cloud Network Controller deployment will be supported in all zones that support the following:

- **GENERAL PURPOSE** as the **Machine family**
- **n2-standard-16** as the **Machine type**

For more information, see:

[https://cloud.google.com/compute/docs/general-purpose-machines#n2\\_machines](https://cloud.google.com/compute/docs/general-purpose-machines#n2_machines)

- **Machine type** section:

- **Machine family:** Select the **GENERAL PURPOSE** tab if it is not already selected.
- **Series:** Leave the default **N2** selection as-is.
- **Machine type:** We recommend choosing the **n2-standard-16** option in this field.
- **SSH Public key:** Enter the SSH public key to enable SSH access to the Cisco Cloud Network Controller. You will use this SSH key pair to log into the Cisco Cloud Network Controller.

Paste the public key information that you copied at the end of [Generating an SSH Key Pair in Linux or MacOS, on page 4](#). Note that the **ssh-rsa** string should remain at the beginning of the public key string that you paste into this field. This SSH public key must be in the following format:

```
ssh-rsa <ssh-public-key-string> <user-info>
```

- **Service Account:** Choose an existing service account or create a new service account for the Cisco Cloud Network Controller deployment.
  - **Select an existing Service Account:** If you have an existing service account that you can use for the Cisco Cloud Network Controller deployment, we recommend that you use that existing service account.

Click the **Select an existing Service Account** option.

- If you have an existing service account that you can use for this Cisco Cloud Network Controller deployment, you will see a screen similar to the following:

### Service Account

Choose an existing or create a new service account for the CAPIC node

- Select an existing Service Account
- Create a new Service Account

List of available Service Accounts that have the following roles:


- roles/compute.instanceAdmin.v1
- roles/compute.networkAdmin
- roles/compute.securityAdmin
- roles/compute.orgSecurityPolicyAdmin
- roles/compute.orgFirewallPolicyAdmin
- roles/storage.admin
- roles/pubsub.admin
- roles/logging.configWriter

Select a Service Account

capicserviceaccount (capicserviceaccountid@... ▼

Select the service account in the **Select a Service Account** field in this case.

- If you do not have an existing service account that you can use for this Cisco Cloud Network Controller deployment, you will see a screen similar to the following:

**Service Account** 


Choose an existing or create a new service account for the CAPIC node


Select an existing Service Account

Create a new Service Account

List of available Service Accounts that have the following roles:

- roles/compute.instanceAdmin.v1
- roles/compute.networkAdmin
- roles/compute.securityAdmin
- roles/compute.orgSecurityPolicyAdmin
- roles/compute.orgFirewallPolicyAdmin
- roles/storage.admin
- roles/pubsub.admin
- roles/logging.configWriter

 There are no Service Accounts matching the requirements above

Select a Service Account 

If you see this message, then you must create a new service account for this Cisco Cloud Network Controller deployment. Go to the **Create a new Service Account** option below for those instructions.

- **Create a new Service Account:** If you do not have an existing service account that you can use for the Cisco Cloud Network Controller deployment, click the **Create a new Service Account** option.



## Service Account

Choose an existing or create a new service account for the CAPIC node

- Select an existing Service Account
- Create a new Service Account

### Create a new Service Account



This will create a new Service Account with the following roles:

- roles/compute.instanceAdmin.v1
- roles/compute.networkAdmin
- roles/compute.securityAdmin
- roles/compute.orgSecurityPolicyAdmin
- roles/compute.orgFirewallPolicyAdmin
- roles/storage.admin
- roles/pubsub.admin
- roles/logging.configWriter

Service Account name \*

Service Account ID \*

Service Account description

Enter the following information to create a new service account:

- **Service Account name:** Enter a unique name for this service account. The service account name must be between 1 and 100 characters.
- **Service Account ID:** Enter a unique ID for this service account. The service account ID must be between 6 and 30 characters, and must follow the following pattern:  
[a-z][a-z0-9]+[a-z0-9]
- **Service Account description:** Enter a description for this service account.

- **VPC subnet cidr:** Enter the subnet CIDR to create the subnet and launch the Cisco Cloud Network Controller from this subnet.

This must be a valid CIDR in the form  $x.x.x.x/24$ . The subnet mask must be at least /24.

- **Admin user password:** Enter the password of the Cisco Cloud Network Controller admin user.

The password should follow these rules:

- Contain eight or more characters
  - At least one letter
  - At least one number
  - At least one special character
- **Remote Access:** Enter the external network allowed to access the Cisco Cloud Network Controller. This must be a valid IP CIDR in the form `x.x.x.x/xx`.

**Step 6** Click the box at the bottom of the page to accept the Google Cloud terms, then click **DEPLOY**.

The **Deployment Manager** window appears. A messages saying that the Cisco Cloud Network Controller is being deployed will appear for roughly 5-10 minutes.

- Wait for the message saying that the Cisco Cloud Network Controller has been deployed before proceeding.
- Once you see that message, wait for roughly 10 additional minutes for the system to come to the operational state. You will not be able to log into the Cisco Cloud Network Controller using the password until the system comes to the operational state.

**Note** If you want to delete a Cisco Cloud Network Controller deployment in Google Cloud for any reason, see [Deleting a Cisco Cloud Network Controller Deployment in Google Cloud, on page 10](#) for those procedures.

---

### What to do next

This infra service account that you created with these procedures will be used for each of the user-tenant projects (managed tenants) to establish communication between the infra and user-tenant projects. Next, go to [Configuring Cisco Cloud Network Controller Using the Setup Wizard](#) to set up the cloud infrastructure configuration for your Cisco Cloud Network Controller, where the Cisco Cloud Network Controller deploys the required Google Cloud constructs.

## Deleting a Cisco Cloud Network Controller Deployment in Google Cloud

If you want to delete a Cisco Cloud Network Controller deployment in Google Cloud for any reason, the procedures that you will use to delete that deployment will vary, depending on the release that you are running and the type of deployment that you have:

- If you are running on a release prior to release 25.0(5) and you have external connectivity set up using the Google Cloud routers, then follow the instructions in [Deleting a Cisco Cloud Network Controller Deployment in Google Cloud \(External Connectivity Using Google Cloud Routers\), on page 11](#) if you want to delete that deployment for any reason.
- If you are running on release 25.0(5) or later, and:

- You have external connectivity set up using the Google Cloud routers, then follow the instructions in [Deleting a Cisco Cloud Network Controller Deployment in Google Cloud \(External Connectivity Using Google Cloud Routers\)](#), on page 11 if you want to delete that deployment for any reason.
- You have inter-site connectivity set up using the Cisco Catalyst 8000Vs, then follow the instructions in [Deleting a Cisco Cloud Network Controller Deployment in Google Cloud \(Inter-Site Connectivity Using Cisco Catalyst 8000Vs\)](#), on page 12 if you want to delete that deployment for any reason.

## Deleting a Cisco Cloud Network Controller Deployment in Google Cloud (External Connectivity Using Google Cloud Routers)

These procedures assume that you have already deployed the Cisco Cloud Network Controller in Google Cloud using the procedures provided in [Deploying the Cisco Cloud Network Controller in Google Cloud, on page 5](#), where you configured external connectivity using Google Cloud routers but now you want to delete that Cisco Cloud Network Controller deployment in Google Cloud.

If you want to delete a Cisco Cloud Network Controller deployment for any reason, you will need to delete all the resources that you created earlier before you can delete the deployment. Follow these procedures to delete this type of Cisco Cloud Network Controller deployment:

### Step 1

If you have an external network deployed in Google Cloud for Cisco Cloud Network Controller, delete the configured external network.


Skip to [Step 2, on page 11](#) if you do not have an external network deployed in Google Cloud for Cisco Cloud Network Controller.

- a) In the left navigation bar in the Cisco Cloud Network Controller GUI, navigate to **Application Management** > **External Networks**.
- b) In the **External Networks** window, click the box next to the configured external network, then choose **Actions** > **Delete External Network**.

Click **OK** in the confirmation window to delete the external network.

### Step 2

If you have cloud routers deployed in any region, disable external connectivity first.

- a) In the Cisco Cloud Network Controller GUI, click the Intent icon (  ).
- b) In the **Workflows** area, click **Cisco Cloud Network Controller Setup**.
- c) In the **Region Management** area, click **Edit Configuration**.

The **Region Management** page appears.

- d) In the **Region Management** page, locate the regions that have the checks in the boxes under the **External Connectivity using Google Cloud Routers**.

Having a check in the box in the **External Connectivity using Google Cloud Routers** for a region is an indication that external connectivity is currently enabled for that region.

- e) Click the box in the **External Connectivity using Google Cloud Routers** column to remove the check in the checkbox for each region that you want to disable external network connectivity.

A confirmation window with the following message appears:

**External Connectivity**

Disabling External Connectivity will delete all Hub Networks and IPsec Tunnels, any Route Leaks for External Networks will be disrupted.

- f) Click **Confirm** in the confirmation window to disable external connectivity.
- g) Click **Save and Continue**, then click **Done**.
- h) In the Google Cloud portal, verify that the previously configured VPN connection was successfully deleted by clicking **Hybrid Connectivity > VPN**.

You should not see the previously configured VPN connection for your Cisco Cloud Network Controller in this window.

**Step 3** Delete the firewall rules in Google Cloud.

- a) In the Google Cloud portal, click **VPC network > Firewall**.
- b) Click the box next to **Name** to select all of the firewall rules displayed in this window.
- c) Click **DELETE**.

Click **DELETE** again in the confirmation window to delete these firewall rules.

**Step 4** Delete the deployments in Google Cloud.

- a) In the Google Cloud portal, navigate to the **Cloud Deployment Manager** page.
- b) Click **GO TO CLOUD DEPLOYMENT MANAGER**.

Your Google Cloud deployments are displayed.

- c) Click the box next to the deployment that you want to delete, then click **DELETE**.

In the confirmation window, leave the default setting as-is, where you will delete the deployment and all resources created by the deployment. Click **DELETE ALL** in the confirmation window to delete the deployment.

If the deletion fails, a message is displayed, describing which resource still exists that caused the deletion to fail. Locate and delete that resource in that case, then repeat the steps to delete the deployment.

**Step 5** Verify that the current deployment is deleted completely before attempting to redeploy.

After you have deleted the current deployment, wait for roughly 10 minutes before redeploying the Cisco Cloud Network Controller.

## Deleting a Cisco Cloud Network Controller Deployment in Google Cloud (Inter-Site Connectivity Using Cisco Catalyst 8000Vs)

These procedures assume that you have already deployed the Cisco Cloud Network Controller in Google Cloud using the procedures provided in [Deploying the Cisco Cloud Network Controller in Google Cloud, on page 5](#), where you configured inter-site connectivity using Cisco Catalyst 8000Vs but now you want to delete that Cisco Cloud Network Controller deployment in Google Cloud.

If you want to delete a Cisco Cloud Network Controller deployment for any reason, you will need to delete all the resources that you created earlier before you can delete the deployment. Follow these procedures to delete this type of Cisco Cloud Network Controller deployment:

**Step 1**

Delete the VM instances in Google Cloud.

- a) In the Google Cloud portal, navigate to **Virtual machines > VM instances**.
- b) Click the box next to **Status** to select all of the VM instances displayed in this window (the instance for the Cisco Cloud Network Controller and the instances for the Cisco Catalyst 8000Vs).
- c) Click **DELETE**.

**Note** You might have to click the vertical ellipsis (...) to see the **DELETE** option.

Click **DELETE** again in the confirmation window to delete these VM instances.

**Step 2**

Delete the subnets in Google Cloud.

- a) In the Google Cloud portal, navigate to **VPC network > VPC networks**.


The two VPC networks are shown for the Cisco Cloud Network Controller (the overlay-1 and overlay-1-secondary VPC networks).

- b) Click the overlay-1 VPC network, then click the **SUBNETS** tab.
- c) Click the box next to **Name** to select all of the subnets displayed in this tab, then click the trashcan icon on the same line as each subnet to delete each subnet.
- d) Navigate back to **VPC networks** again, click the overlay-1-secondary VPC network, then click the **SUBNETS** tab in that VPC network.
- e) Click the box next to **Name** to select all of the subnets displayed in this tab, then click the trashcan icon on the same line as each subnet to delete each subnet.
- f) Navigate back to **VPC networks** again and verify that the subnets are no longer showing for each VPC network.

You might have to wait several seconds and click **REFRESH** to see that the subnets have been deleted.

**Step 3**

If you have native cloud routers deployed in any region, disable external connectivity to delete the VPN tunnels, VPN gateways, and native cloud routers.

- a) In the Cisco Cloud Network Controller GUI, click the Intent icon (  ).
- b) In the **Workflows** area, click **Cisco Cloud Network Controller Setup**.
- c) In the **Region Management** area, click **Edit Configuration**.

The **Region Management** page appears.

- d) In the **Region Management** page, locate the regions that have the checks in the boxes under the **External Connectivity using Google Cloud Routers**.

Having a check in the box in the **External Connectivity using Google Cloud Routers** for a region is an indication that external connectivity is currently enabled for that region.

- e) Click the box in the **External Connectivity using Google Cloud Routers** column to remove the check in the checkbox for each region that you want to disable external network connectivity.

A confirmation window with the following message appears:

```
External Connectivity
Disabling External Connectivity will delete all Hub Networks and IPsec Tunnels, any Route
Leaks for External Networks will be disrupted.
```

- f) Click **Confirm** in the confirmation window to disable external connectivity.
- g) Click **Save and Continue**, then click **Done**.

- h) In the Google Cloud portal, verify that the previously configured VPN connection was successfully deleted by clicking **Hybrid Connectivity > VPN**.

You should not see the previously configured VPN connection for your Cisco Cloud Network Controller in this window.

**Step 4** Delete the firewall rules in Google Cloud.

- a) In the Google Cloud portal, navigate to **VPC network > Firewall**.
- b) Click the box next to **Name** to select all of the firewall rules displayed in this window.
- c) Click **DELETE**.

Click **DELETE** again in the confirmation window to delete these firewall rules.

**Step 5** Delete the VPC peerings in Google Cloud.

- a) In the Google Cloud portal, navigate to **VPC network > VPC network peering**.
- b) Click the box next to **Name** to select all of the VPC network peerings displayed in this window.
- c) Click **DELETE**.

Click **DELETE** again in the confirmation window to delete these VPC network peerings.

**Step 6** Delete the VPCs in Google Cloud.

- a) In the Google Cloud portal, navigate to **VPC network > VPC networks**.

The two VPC networks are shown for the Cisco Cloud Network Controller (the overlay-1 and overlay-1-secondary VPC networks).

- b) Click the overlay-1 VPC network.
- c) Click **DELETE VPC NETWORK** to delete this VPC network.

Click **DELETE** again in the confirmation window to delete this VPC network.

- d) Navigate back to **VPC networks** again and click the overlay-1-secondary VPC network.
- e) Click **DELETE VPC NETWORK** to delete this VPC network.

Click **DELETE** again in the confirmation window to delete this VPC network.

**Step 7** If you have an external network deployed in Google Cloud for Cisco Cloud Network Controller, delete the configured external network.

- a) In the left navigation bar in the Cisco Cloud Network Controller GUI, navigate to **Application Management > External Networks**.
- b) In the **External Networks** window, click the box next to the configured external network, then choose **Actions > Delete External Network**.

Click **OK** in the confirmation window to delete the external network.

**Step 8** Delete the deployments in Google Cloud.

- a) In the Google Cloud portal, navigate to the **Cloud Deployment Manager** page.
- b) Click **GO TO CLOUD DEPLOYMENT MANAGER**.

Your Google Cloud deployments are displayed.

- c) Click the box next to the deployment that you want to delete, then click **DELETE**.

In the confirmation window, leave the default setting as-is, where you will delete the deployment and all resources created by the deployment. Click **DELETE ALL** in the confirmation window to delete the deployment.

If the deletion fails, a message is displayed, describing which resource still exists that caused the deletion to fail. Locate and delete that resource in that case, then repeat the steps to delete the deployment.

**Step 9** Verify that the current deployment is deleted completely before attempting to redeploy.

After you have deleted the current deployment, wait for roughly 10 minutes before redeploying the Cisco Cloud Network Controller.

---

