Cisco Cloud APIC for Google Cloud Installation Guide, Release 25.0(1)-25.0(4)

First Published: 2021-09-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

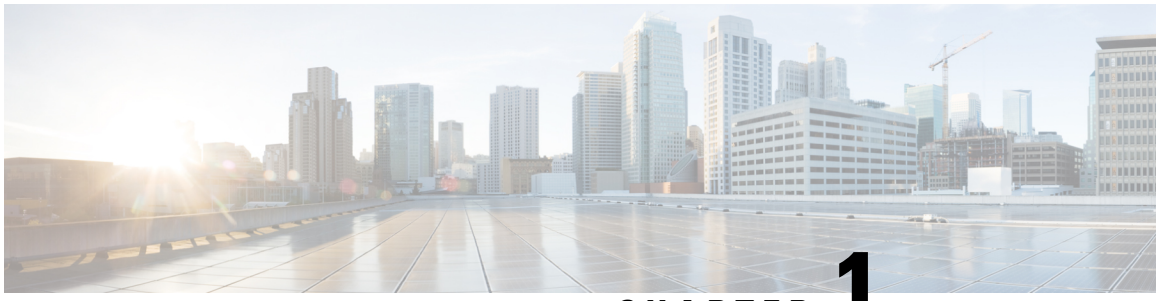
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

CONTENTS



CHAPTER 1

New and Changed Information

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in Cisco Cloud APIC for Release 25.0(4)

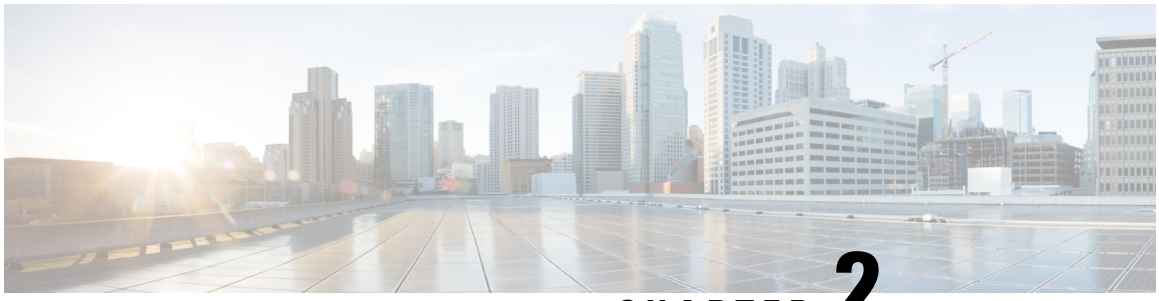
Feature or Change	Description	Where Documented
No changes were made in this document for the 25.0(4) release.		

Table 2: New Features and Changed Behavior in Cisco Cloud APIC for Release 25.0(3)

Feature or Change	Description	Where Documented
Move from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V	Cisco Cloud APIC moves from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V beginning with release 25.0(3).	
Terms used for Cisco Cloud Services Router 1000v and Cisco Catalyst 8000V	The following terms are used for the two types of routers described above: • **CSR**: Short for Cloud Services Router. Refers to the Cisco Cloud Services Router 1000v, used in releases prior to release 25.0(3). • **CCR**: Short for Cisco Cloud Router. Refers to the Cisco Catalyst 8000V, used in release 25.0(3) and later. In addition, throughout this document, **CCR** is used as a generic term for either of the routers described above, depending on your release.	

Table 3: New Features and Changed Behavior in Cisco APIC for Cisco APIC Release 25.0(1)

Feature or Change	Description	Where Documented
Change in release numbering for Cisco Cloud APIC	Beginning with release 25.0(1), the release numbering has changed for Cisco Cloud APIC. The sequential order of releases for Cisco Cloud APIC is as follows: • 4.1(x) (support for AWS only) • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(x) (this release)	
Support for Google Cloud with Cisco Cloud APIC	Beginning with release 25.0(1), support is now available for Google Cloud with Cisco Cloud APIC.	



CHAPTER 2

Overview

Policy Terminology

A key feature of Cisco Cloud APIC is translation of Cisco Application Centric Infrastructure (ACI) policy to the native constructs of the public cloud.

The following table lists Cisco ACI policy terms and the equivalent terms in Google Cloud.

Cisco ACI	Google Cloud
Tenant	Project
Virtual Routing and Forwarding (VRF)	VPC (virtual private cloud)
BD subnet	Subnet
Contract, filter	Firewall rules
EP-to-EPG mapping	Routing and firewall rules
Endpoint	Network adapter on VM instances

Cisco Cloud APIC Licensing

This section lists the licensing requirements to use Cisco Cloud Application Policy Infrastructure Controller (Cisco Cloud APIC).

Cisco Cloud APIC

Cisco licenses Cisco Cloud APIC by each virtual machine (VM) instance that it manages. The Cisco Cloud APIC binary images are available on the Google Cloud portal and support the Bring Your Own License (BYOL) model.

The Essential Cloud tier includes licenses for a single policy domain or a single instance of Cisco Cloud APIC on a public cloud. If you deploy multiple instances of Cisco Cloud APIC, buy an Advantage Cloud license for each VM instance that Cisco Cloud APIC manages.

For licensing details, see the *Cisco Application Centric Infrastructure Ordering Guide*.

In addition to obtaining one or more Cisco Cloud APIC licenses, you must register your Cisco Cloud APIC with Cisco Smart Software Licensing.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Complete the following steps to register Cisco Cloud APIC:

1. Ensure that this product has access to the internet or a Smart Software Manager satellite that is installed on your network.
2. Log in to Smart Account:
   a. Smart Software Manager: https://software.cisco.com/
   b. Smart Software Manager Satellite: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
3. Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
4. Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

Cisco Cloud APIC-Related Documentation

You can find information about Cisco Cloud APIC and Google Cloud from different resources.

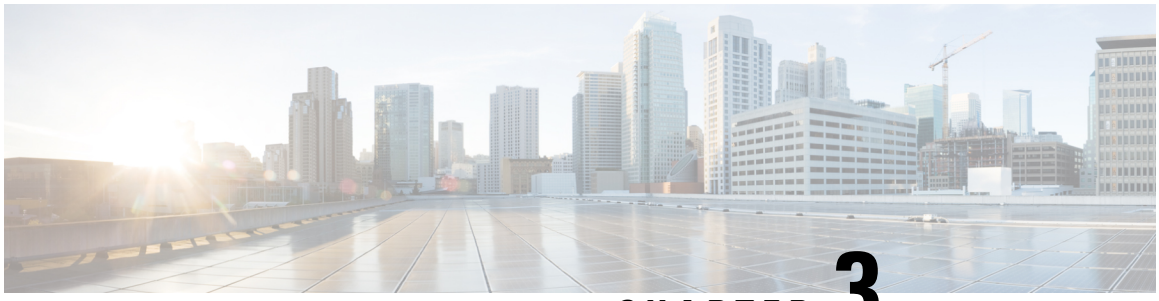
Cisco Cloud APIC Documentation

You can find documentation for Cisco Cloud APIC Cisco.com:

Cisco Cloud APIC documentation library

Google Cloud Documentation

You can find documentation, including user guides, FAQs, case studies, and white papers, on the Google Cloud website.



CHAPTER 3

Preparing for Installing Cisco Cloud APIC

Resources Used for Cisco Cloud APIC Deployment in Google Cloud

This section lists the requirements for Cisco Cloud APIC deployment in Google Cloud.

Cisco Cloud APIC Resources

When you deploy Cisco Cloud APIC in Google Cloud, the Cisco Cloud APIC will use the following instance profile and will create the necessary resources:

- One compute instance:
  - Instance type: n2-standard-16
  - CPU: 16 vCPU
  - Memory: 64 GB
  - Disks: OS disk [300GB] , Data Disk – 100GB [empty]
- Data Disk:
  - Empty data disk
  - Size: 100GB
  - Type: Standard SSD
- VPC network: With autoCreateSubnetworks set to False
- Subnet: Cisco Cloud APIC management NIC is attached to this subnet.
- Google Cloud projects: A minimum of two Google Cloud projects:
  - One for ACI infra

- One per tenant

Cisco Cloud APIC Communication Ports

When configuring your Cisco Cloud APIC environment, keep in mind that the following ports are required for network communications:

- For the Cisco Cloud APIC, use the same Cisco Cloud APIC management IP address that you will use to log into the Cisco Cloud APIC at the beginning of Configuring Cisco Cloud APIC Using the Setup Wizard, on page 19.
- For the Google Cloud firewall rules:
  - WEB-Server: Ingress allow 80, 443
  - SSH-Allow: Ingress allow 22
- For license registration (towards `tools.cisco.com`): Port 443 (outbound) is required
- For DNS: UDP Port 53 outbound
- For NTP: UDP Port 123 outbound
- If remote authentication is used (LDAP, Radius, TACACS+, SAML), open the proper ports
- If a certificate authority is used, open the proper ports

Cisco Cloud APIC Installation Workflow

This section provides a high-level description of the tasks that are required to install and deploy Cisco Cloud APIC. You perform installation tasks through Google Cloud management portal and the Cloud APIC First Time Setup Wizard.

1. Fulfill all prerequisites to prepare for support of Google Cloud with Cisco Cloud APIC.

   See Preparing for Installing Cisco Cloud APIC, on page 5.

2. Deploy Cisco Cloud APIC in Google Cloud.

   See Deploying the Cloud APIC in Google Cloud, on page 7.

3. Configure Cisco Cloud APIC using the First Time Setup Wizard.

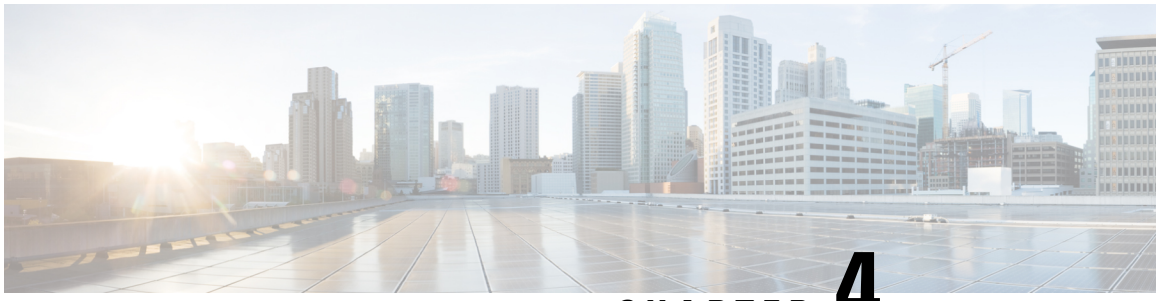
   See Configuring Cisco Cloud APIC Using the Setup Wizard, on page 19.

4. Make the necessary configurations through Cisco Cloud APIC.

   See Navigating the Cisco Cloud APIC GUI, on page 37 and Configuring Cisco Cloud APIC Components, on page 37.

5. Delete the deployment, if necessary.

   See Deleting a Cisco Cloud APIC Deployment in Google Cloud, on page 16.



CHAPTER 4

Deploying the Cloud APIC in Google Cloud

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 APIC.

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 APIC deployment on this project. If there is a previous Cisco Cloud APIC deployment on this project, delete that existing deployment using the instructions in Deleting a Cisco Cloud APIC Deployment in Google Cloud, on page 16.

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

a) In the Google Cloud GUI, navigate to the project that you created for Cisco Cloud APIC.
The **Dashboard** for your 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 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 APIC.
- **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 APIC 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.

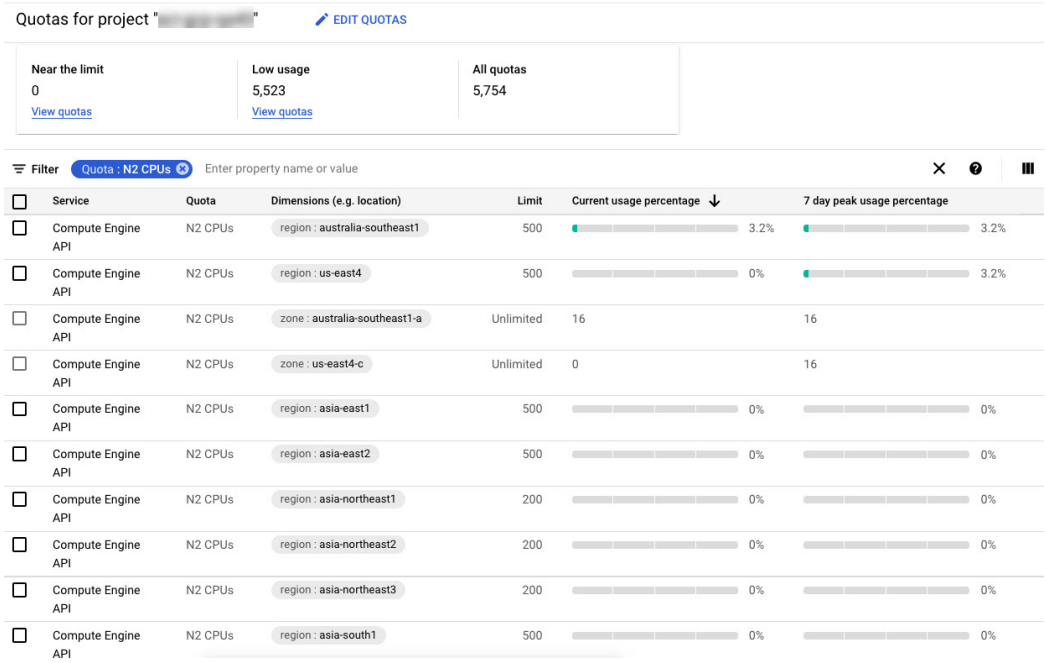
   The **Edit Permissions** window is displayed.

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 APIC 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.



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/capic-ssh-key -C admin
```

Step 2 Locate the public key file that you saved.

The public key file is saved in this file:

```
~/.ssh/capic-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 AAAAB3NzaC1yc2EAAAADAQABABABgQC+0Aom7Mblv+w7yWE7QOPytvpankAdOsNWd7keptT6nAnr
S2UjHP0c0KC0jABEo7fL0hwQpwKmLRfHi0poQ3FAy7Oof6XcFJx5aCcCayrGDhm96HPbcPoXjhhg0Fufr4QyL9cWpbsKn9K1k
OhnIw+KQyaxCQS1D1wMsgREKMDrkdk5MZazqZC8haThaaAO/h+i+OQ9juo6N6QPUogHRZ+E9ztyGU/buU1/0vnvzTTinvw8aq
mTnPUQxNI6wZ2FpMH8JHiDQ924wIboAEq0tvidnElemG5wsQrwUghD7r1D9uWjI1rsfGAJL8mSIkWbXZFo+AqNlbE69Oa1TIL
```

```
2DfmgYQm3M+qWdzaZPI6i+Ap/dMgGKyy8M4VGFN0o+wbkzi1XdEbMpSEBxyuDtoB5H9T4Kov2yuH/RdqPMSSt+ZgNgBZgcl6S
HXlpSA0GmwyHljYNizo70UMI2JDJDmUc4vCNMgVRxWkNraCWYEZD5iMjnAtIiZvQGmZKQwBH0GY3XIc= admin
```

What to do next

Follow the instructions in Deploying the Cloud APIC in Google Cloud, on page 11 to continue the Google Cloud configuration process, which includes pasting the public key information into the Google Cloud deployment template.

Deploying the Cloud APIC in Google Cloud

Step 1 Log into your Google Cloud account for the Cisco Cloud APIC infra tenant.

Step 2 Navigate to the Google Cloud Marketplace.

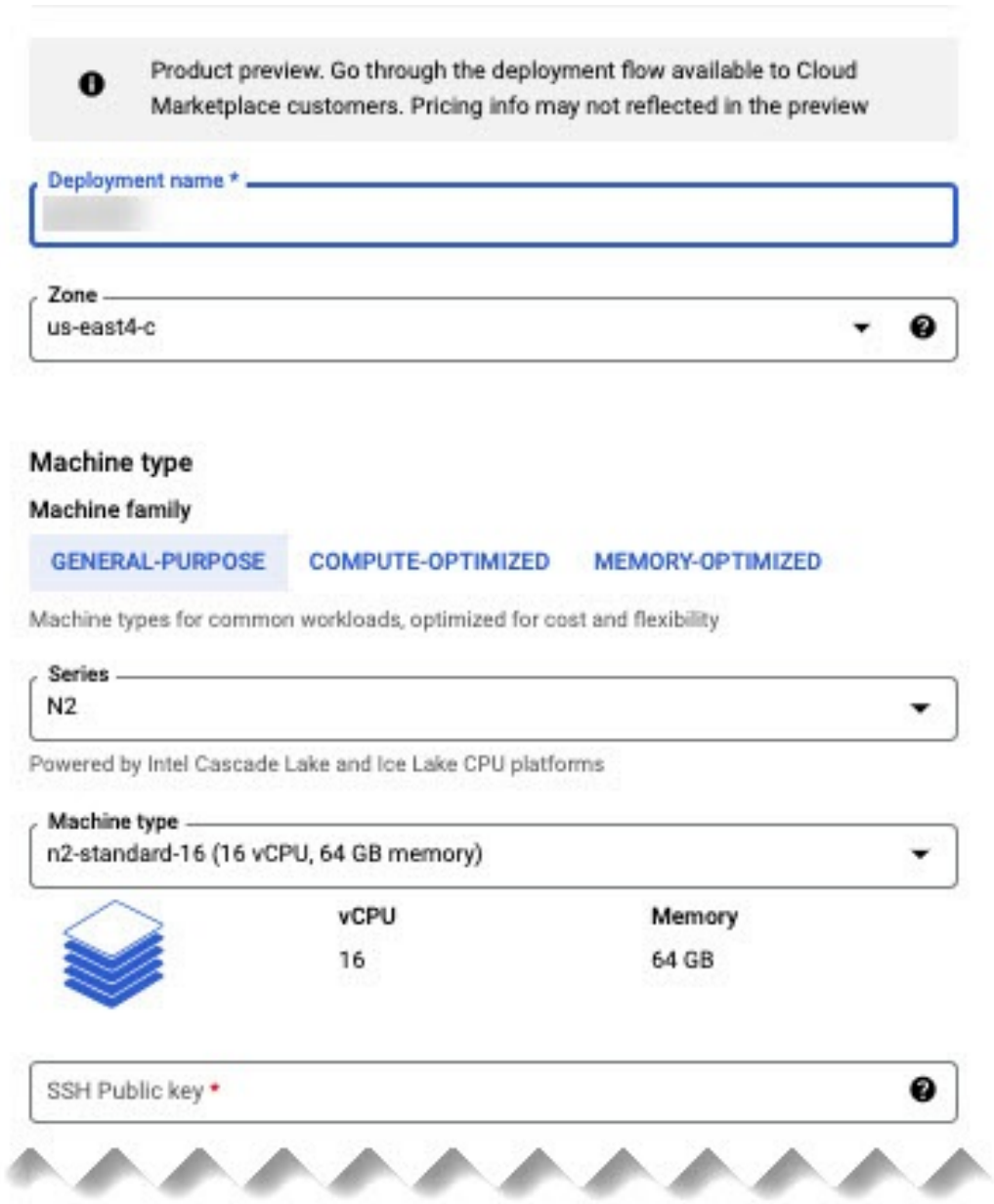
Step 3 In the search bar, search for:

```
Cisco Cloud APIC
```

and select the result from that search.

Step 4 In the **Cisco Cloud APIC** window in the Google Cloud Marketplace, click **LAUNCH**.

The **New Cisco Cloud APIC deployment** window appears.



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

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

  The Cisco Cloud APIC 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

- **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 APIC. You will use this SSH key pair to log into the Cloud APIC.

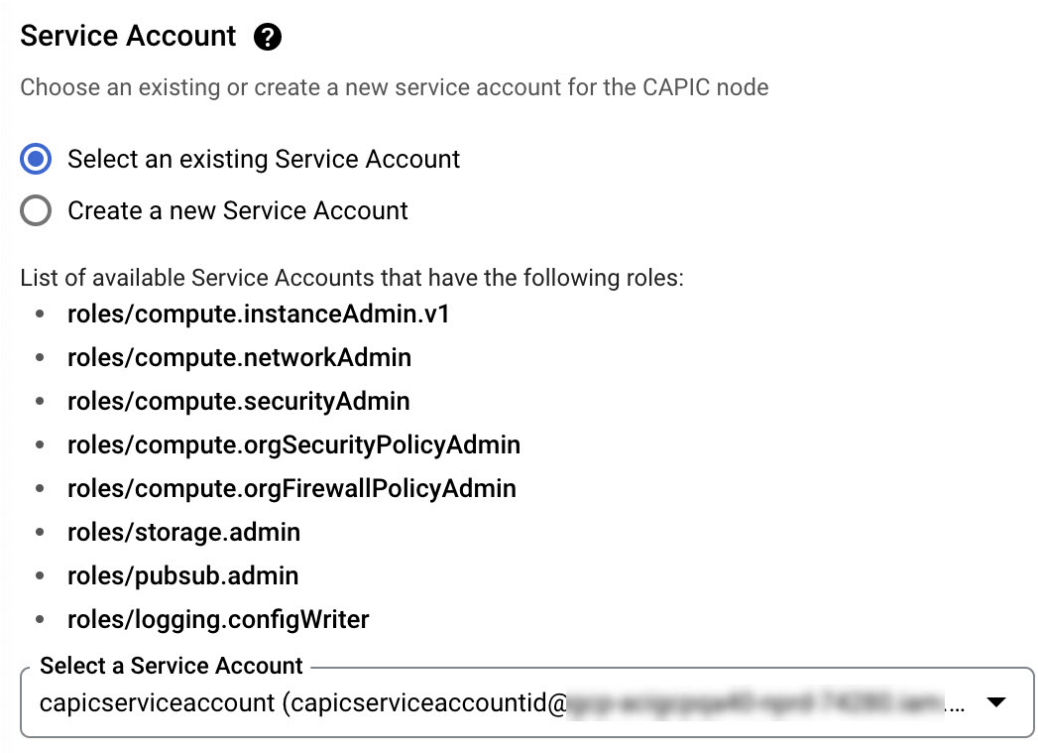
    Paste the public key information that you copied at the end of Generating an SSH Key Pair in Linux or MacOS, on page 10. Note that the **ssh-rsa** string should remain at the beginning of the public key string that you paste into this field. This SSH public key must be in the following format:

    ```
    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 APIC deployment.
    - **Select an existing Service Account**: If you have an existing service account that you can use for the Cisco Cloud APIC deployment, we recommend that you use that existing service account.

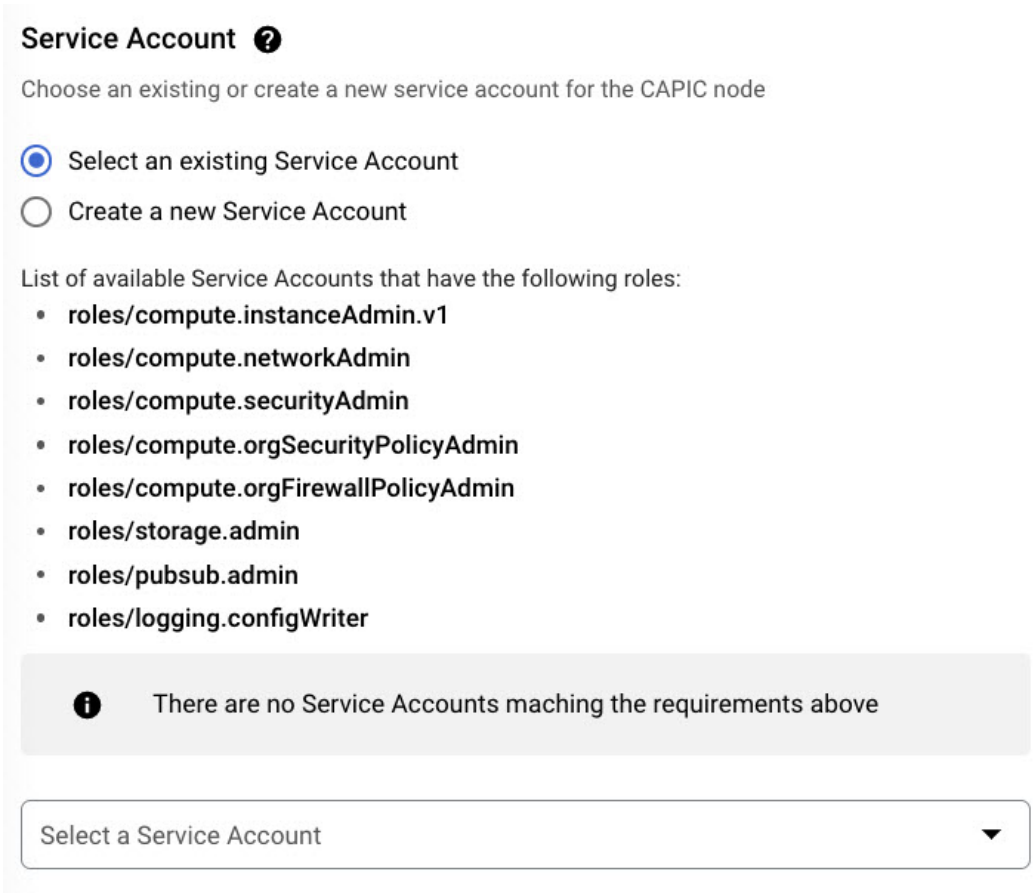
      Click the **Select an existing Service Account** option.

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



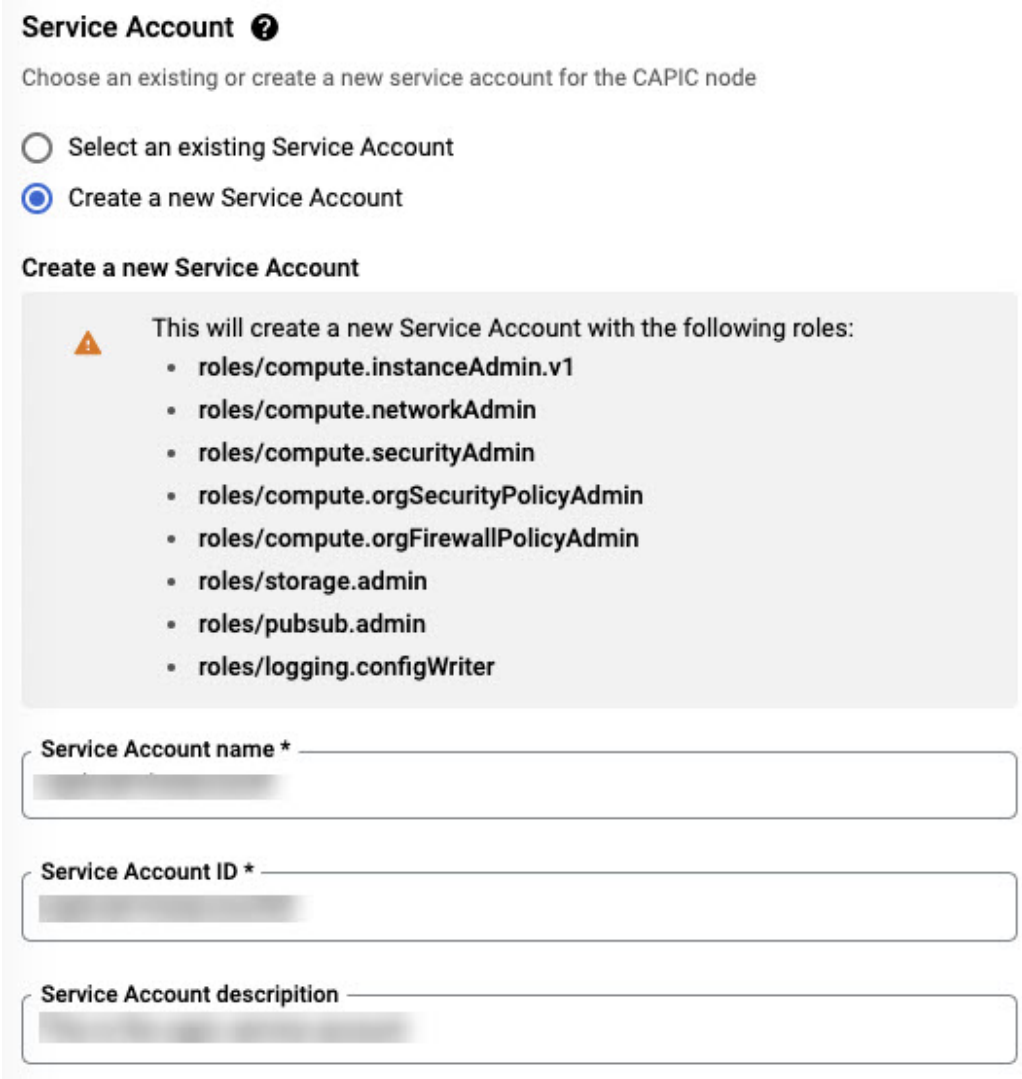
      Select the service account in the **Select a Service Account** field in this case.

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



  If you see this message, then you must create a new service account for this Cisco Cloud APIC 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 APIC deployment, click the **Create a new Service Account** option.



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 APIC 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 APIC 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 APIC.

  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 APIC is being deployed will appear for roughly 5-10 minutes.

- Wait for the message saying that the Cisco Cloud APIC 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 APIC using the password until the system comes to the operational state.

Note If you want to delete a Cisco Cloud APIC deployment in Google Cloud for any reason, see Deleting a Cisco Cloud APIC Deployment in Google Cloud, on page 16 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 APIC Using the Setup Wizard, on page 19 to set up the cloud infrastructure configuration for your Cisco Cloud APIC, where the Cisco Cloud APIC deploys the required Google Cloud constructs.

Deleting a Cisco Cloud APIC Deployment in Google Cloud

These procedures assume that you have already deployed the Cisco Cloud APIC in Google Cloud using the procedures provided in Deploying the Cloud APIC in Google Cloud, on page 11, but now you want to delete that Cisco Cloud APIC deployment in Google Cloud.

If you want to delete a Cisco Cloud APIC 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 a Cisco Cloud APIC deployment:

Step 1 If you have an external network deployed in Google Cloud for Cisco Cloud APIC, delete the configured external network.

Skip to Step 2, on page 17 if you do not have an external network deployed in Google Cloud for Cisco Cloud APIC.

a) In the left navigation bar in the Cisco Cloud APIC 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 APIC GUI, click the Intent icon ( ).
b) In the **Workflows** area, click **Cloud APIC Setup**.
c) In the **Region Management** area, click **Edit Configuration**.

The **Region Management** page appears.

d) In the **Region Management** page, locate the **External Connectivity** area.

In the **External Connectivity** area, the box next to **Enable** should be checked at this point, indicating that external connectivity is currently enabled.

e) Click the box next to **Enable** to remove the check in the checkbox.

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 APIC 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.

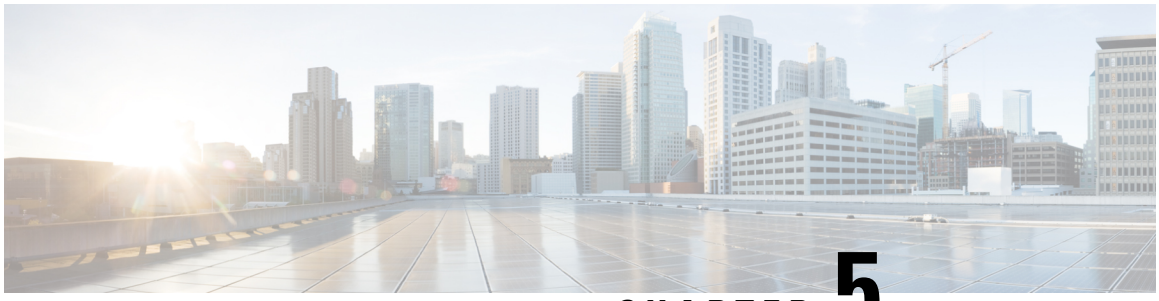
c) Click the box next to the deployment that you want to delete, then click **DELETE**.

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 APIC.



CHAPTER 5

Configuring Cisco Cloud APIC Using the Setup Wizard

Configuring Cisco Cloud APIC Using the Setup Wizard

Follow the procedures in this topic to set up the cloud infrastructure configuration for your Cisco Cloud APIC. Cisco Cloud APIC will automatically deploy the required Google Cloud constructs.

Before you begin

Following are the prerequisites for this task:

- You have a minimum of two Google Cloud projects, one for ACI infra and one per tenant.
- You have successfully completed the procedures that are provided in Deploying the Cloud APIC in Google Cloud, on page 7.

Step 1 Locate the IP address for your Cisco Cloud APIC.

The management IP address is shown at the end of the output from the Deployment Manager in Deploying the Cloud APIC in Google Cloud, on page 11.

You can also locate the IP address for your Cisco Cloud APIC by navigating to **Compute Engine** > **VM instances**. The IP address shown in the **External IP** column is the IP address for your Cisco Cloud APIC.

Step 2 Open a browser window and, using the secure version of HTTP (`https://`), paste the IP address into the URL field, then press Return to access this Cisco Cloud APIC.

For example, `https://192.168.0.0`.

If you see a message asking you to **Ignore Risk and Accept Certificate**, accept the certificate to continue.

Step 3 Enter the following information in the login page for the Cisco Cloud APIC:

- **Username:** Enter **admin** for this field.
- **Password:** Enter the password that you provided to log into the Cisco Cloud APIC.

- **Domain:** If you see the **Domain** field, leave the default Domain entry as-is.

Step 4 Click **Login** at the bottom of the page.

Note If you see an error message when you try to log in, such as `REST Endpoint user authentication datastore is not initialized - Check Fabric Membership Status of this fabric node`, wait for several minutes, then try again after a few minutes. You might also have to refresh the page in order to log in.

The Welcome to Cisco Cloud APIC setup wizard page appears.

Step 5 Click **Begin Set Up**.

The **Let's Configure the Basics** page appears, with these areas to be configured:

- **DNS and NTP Servers**
- **Region Management**
- **Smart Licensing**

Step 6 In the **DNS and NTP Servers** row, click **Edit Configuration**.

The **DNS and NTP** page appears.

Step 7 In the **DNS and NTP** page, add the DNS, if necessary, and NTP servers.

- A DNS server is already configured by default. Add a DNS server if you want to use a specific DNS server.
- An NTP server is not configured by default, however, so we recommend that you configure an NTP server. Skip to 7.d, on page 20 if you want to configure an NTP server and you do not want to configure a DNS server.

a) If you want to use a specific DNS server, under the **DNS Servers** area, click **+Add DNS Provider**.
b) Enter the IP address for the DNS servers and, if necessary, check the box next to Preferred DNS Provider.
c) Click the check mark next to the DNS server, and repeat for any additional DNS servers that you want to add.
d) Under the **NTP Servers** area, click **+Add Providers**.
e) Enter the IP address for the NTP servers and, if necessary, check the box next to Preferred NTP Provider.
f) Click the check mark next to the NTP server, and repeat for any additional NTP servers that you want to add.

Step 8 When you have finished adding the DNS and NTP servers, click **Save and Continue**.

The **Let's Configure the Basics** page appears again.

Step 9 In the **Region Management** row, click **Begin**.

The **Region Management** page appears.

Step 10 Verify that all of the regions in the page are selected.

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 (all of the regions are selected and can't be unselected) and inter-region connectivity is present.

Step 11 Determine if you want to configure external network connectivity.

- click the box next to **Enable** to enable external network connectivity.

Step 12 Click **Next** at the bottom of the page.

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

Step 13 Enter the necessary information in the **Hub Network** area, if necessary.

Hub network management is used to deploy cloud routers on specific managed regions.

Note the following restrictions:

- You can create only one hub network in Google Cloud.
- Under the hub network, only one cloud router per region can be 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.

d) Click **+ Add Region** to add regions.

You can add up to four regions.

e) Click **Done** when you are finished entering information in the **Add Hub Network** window.

You are returned to the **General Connectivity** page.

f) The default entry is displayed in the **VPN Router** field.

g) 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.

Step 14 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 default 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 15 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 Configuring an External Network, on page 25 for those procedures.

Configuring Cisco Cloud APIC Using the Setup Wizard

- If you do not want to create external networks, click **Go to Dashboard**.

  You are returned to the main **Dashboard** window.

Step 16 Click the **Intent** icon.
The **Intent** menu appears.

Step 17 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 18 In the **Smart Licensing** row, click **Register**.

The **Smart Licensing** page appears.

Step 19 Enter the necessary information in the **Smart Licensing** page.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To register your Cisco Cloud APIC with Cisco Smart Software Licensing, do the following

- Ensure that this product has access to the internet or a Smart Software Manager satellite installed on your network.
- Log in to Smart Account:
  - Smart Software Manager: https://software.cisco.com/
  - Smart Software Manager Satellite: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
- Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Step 20 Click **Register** at the bottom of the page if you entered the necessary licensing information on this page, or click **Continue in Evaluation Mode** if you want to continue in evaluation mode instead.

The **Summary** page appears.

Step 21 Verify the information on the **Summary** page, then click **Finish**.

At this point, you are finished with the internal network connectivity configuration for your Cisco Cloud APIC.

If this is the first time that you are deploying your Cisco Cloud APIC, this process might take quite a bit of time, possibly 30 minutes or so before the process is successfully completed.

What to do next

Complete the procedures in any of the following sections or documents, if necessary:

- Verifying the Cisco Cloud APIC Setup Wizard Configurations, on page 23
- Completing the Initial Configuration, on page 25
  - Configuring an External Network, on page 25
  - Creating a Tenant, on page 27

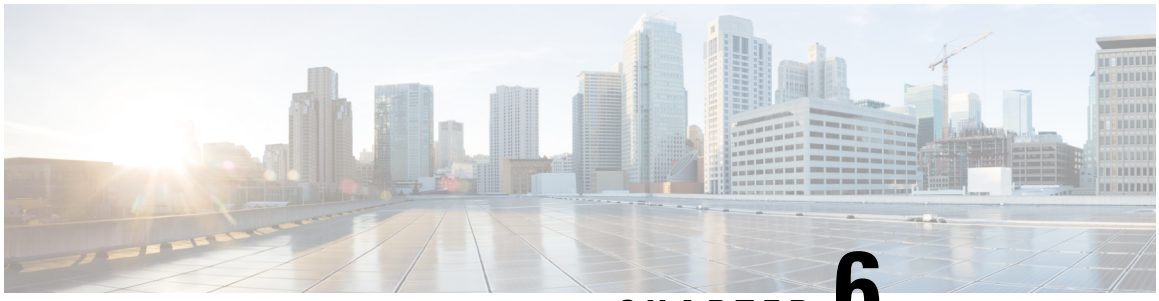
- If you are managing additional sites (an on-premises site or cloud sites) along with the Cisco Cloud APIC site, refer to the Managing Google Cloud Sites Using Nexus Dashboard Orchestrator document.
- Understanding the Cisco Cloud APIC GUI, on page 37
- Logging Into Cloud APIC Through SSH, on page 39

Verifying the Cisco Cloud APIC Setup Wizard Configurations

Use the procedures in this topic to verify that the configuration information that you entered in the Cloud APIC Setup Wizard are applied correctly.

In Cisco Cloud APIC, verify the following settings:

- Under **Cloud Resources**, click on **Regions** and verify that the all of the regions are shown as **managed** in the Admin State column.
- Under **Infrastructure**, click on **External Connectivity** and verify the information in this screen is correct.
- Click on **Dashboard** and use the external connectivity status to verify that the setup wizard and tunnel configurations were done properly.



CHAPTER 6

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, on page 19.

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**. **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 28
- User Tenants With Unmanaged Credentials, on page 29

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 31.

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 35.

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 29 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 5: 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 28.
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 33 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 34 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 29 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.

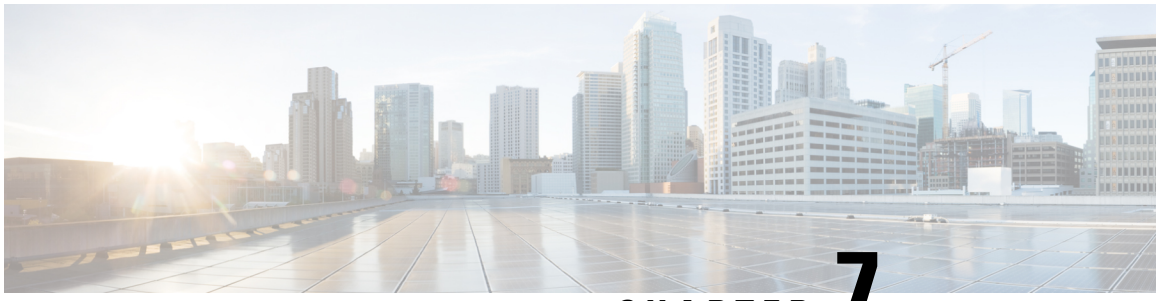
Step 4 Choose the appropriate options and enter the appropriate values in each field as listed in the following *Create Tenant Dialog Box Fields* table then continue.

Table 6: 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 28.
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 34.
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 34.
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 34.
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.



CHAPTER 7

Understanding the Cisco Cloud APIC GUI

Navigating the Cisco Cloud APIC GUI

After you install Cisco Cloud APIC, you can use it for extending Cisco Application Centric Infrastructure (ACI) policy to the Google Cloud. You do so through the Cisco Cloud APIC GUI.

In the Cisco Cloud APIC GUI, you can create a tenant, configure application profiles, endpoint groups (EPGs), contracts, filters, and VRFs. You can also view Cisco Cloud APIC topology, configurations, and resources.

You perform configuration steps with the. **Intent** feature. For instructions on using the **Intent** feature, see the section Configuring Cisco Cloud APIC Components, on page 37. Also see the section "Understanding the Cisco Cloud APIC GUI Icons" in the *Cisco Cloud APIC User Guide*.

The steps for performing basic tasks in Cisco Cloud APIC differ from the steps in regular Cisco APIC. However, the functions of the tenant, application profile, and other elements of Cisco APIC are the same. For more information, see the *Cisco Application Centric Infrastructure Fundamentals Guide* on Cisco.com.

You view configurations and other information with the left navigation pane. You can choose **Dashboard** (the default view), **Topology**, **Application Management**, **Cloud Resources**, **Operations**, **Infrastructure**, and **Administrative**.

For information abut the icons, see the section "Understanding the Cisco Cloud APIC GUI Icons" in the *Cisco Cisco Cloud APIC User Guide* on Cisco.com.

Creating a Tenant Using the Cisco Cloud APIC GUI

The following sections describe how to create a tenant using the Cisco Cloud APIC GUI.

Configuring Cisco Cloud APIC Components

This section provides an overview of performing key tasks in Cisco Cloud APIC, including creating a tenant, application profile, and endpoint group (EPG).

Before you begin

You must have installed Cisco Cloud APIC. See the previous installation sections in this guide.

Step 1 Log into Cisco Cloud APIC.

Step 2 At the upper right of the **Dashboard** pane, click the icon with an arrow pointing to a bull's-eye.

This icon might be referred to as the **Intent** icon or feature.

Step 3 In the **What do you want to do?** window, type a term in the search window to bring up a list of options.

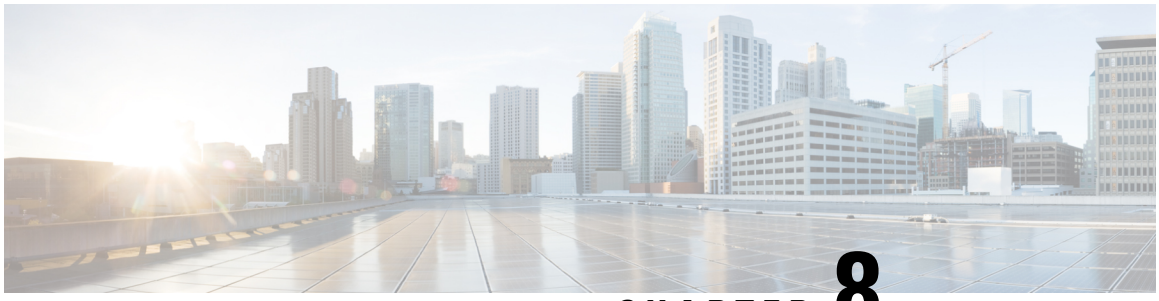
For example, if you want to configure a tenant, type the word tenant in the search window. The search returns a list of tasks that are related to creating and configuring tenants.

Step 4 Click a task and perform the configuration steps in the windows that open.

What to do next

You can view the configuration in the left navigation pane. Expand the pane by clicking the hamburger icon at the upper left of the **Dashboard** pane. Expand the appropriate heading to view the configurations.

For example, if you've configured a tenant, expand **Application Management** and click **Tenants**. Information about tenants appears in the central work pane.



CHAPTER 8

Logging Into Cloud APIC Through SSH

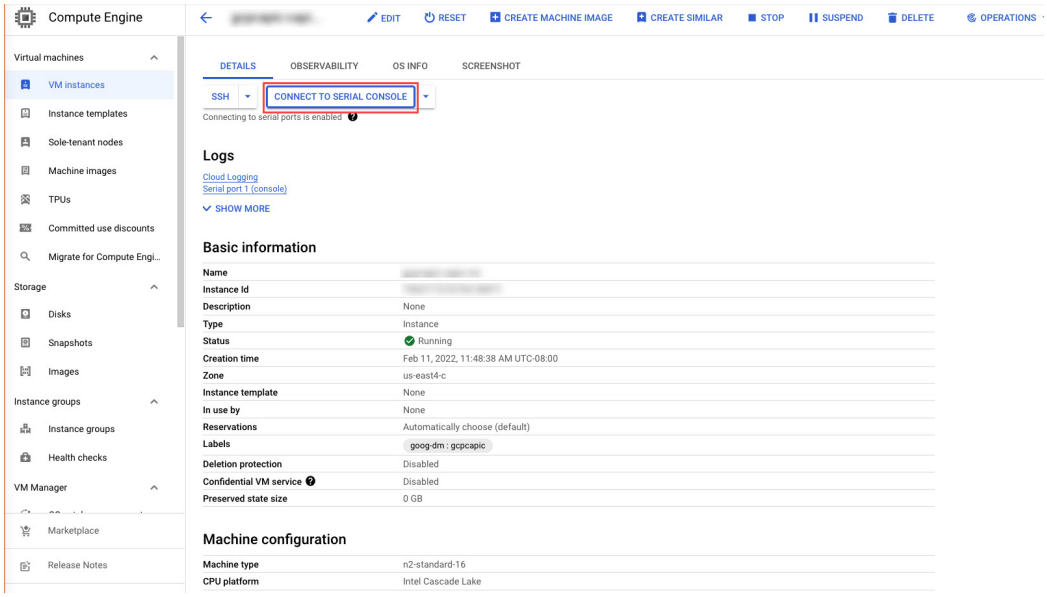
Normally, you will log into your Cisco Cloud APIC through a browser, as described in Configuring Cisco Cloud APIC Using the Setup Wizard, on page 19. If you need to log into your Cisco Cloud APIC through SSH for any reason, however, the following sections describe how to log into the Cisco Cloud APIC using the SSH keys that you generated in the previous sections or using SSH password authentication.

Connecting To Serial Console Through Google Cloud

You can connect to the serial console through Google Cloud by navigating here:

Virtual Machines > **VM instances**

In the **VM instances** page, click on the **Instances** tab and then click the instance for the Cisco Cloud APIC, then click on **CONNECT TO SERIAL CONSOLE**.



Note Connecting to serial console is the only operation that is allowed in this Google Cloud page. For example, attempting to SSH into Cisco Cloud APIC through this page in Google Cloud is not permitted. You can SSH into Cisco Cloud APIC through the other methods described in Logging Into Cloud APIC Through SSH, on page 39.

Log Into Cloud APIC Using SSH Keys

Step 1 Log into your Google Cloud account for the Cisco Cloud APIC infra tenant.

Step 2 Locate the IP address for your Cisco Cloud APIC.

The management IP address shown at the end of the output from the Deployment Manager in Deploying the Cloud APIC in Google Cloud, on page 11.

You can also locate the IP address for your Cisco Cloud APIC by navigating to **Compute Engine** > **VM instances**. The IP address shown in the **External IP** column is the IP address for your Cisco Cloud APIC.

Step 3 For Linux systems, enter the following to log into your Cloud APIC using the SSH keys.

```
# ssh -i ~/.ssh/capic-ssh-key admin@public-IP-address
```

For example:

```
# ssh -i ~/.ssh/capic-ssh-key admin@192.0.2.1
```

See Generating an SSH Key Pair in Linux or MacOS, on page 10 for more information on the location and format of the public key file.

Log Into Cloud APIC Using SSH Password Authentication

Unlike SSH using a public key, SSH Password Authentication is disabled by default. Use these procedures to enable SSH Password Authentication so that you can SSH into your Cloud APIC with a username and password.

Step 1 Open a browser window and, using the secure version of HTTP (`https://`), paste the IP address into the URL field, then press Return to access this Cloud APIC.

For example, `https://192.0.2.1`.

Step 2 Enter the following information in the login page for the Cloud APIC:

- **Username**: Enter admin for this field.
- **Password**: Enter the password that you provided to log into the Cloud APIC.
- **Domain**: If you see the Domain field, leave the default Domain entry as-is.

Step 3 Click **Login** at the bottom of the page.

Step 4 Navigate to **Infrastructure** > **System Configuration**, then click the **Management Access** tab in the **System Configuration** page.

Step 5 Click the pencil icon in the upper right corner of the screen to edit the SSH settings.

The Settings page appears for SSH.

Step 6 In the Password Authentication State field, select Enabled.

Step 7 Click **Save**.

You can now SSH into your Cloud APIC without having to access the public and private key files:

```
# ssh admin@192.0.2.1
```