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.

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.

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 2 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 for those procedures.

• 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:

• Completing the Initial Configuration

• Configuring an External Network

• Creating a Tenant

- 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

- Logging Into Cloud APIC Through SSH

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.