Configuring Cisco Cloud Network Controller Using the Setup Wizard

Configuring Cisco Cloud Network Controller Using the Setup Wizard

Follow the procedures in this topic to set up the cloud infrastructure configuration for your Cisco Cloud Network Controller. Cisco Cloud Network Controller 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 Cisco Cloud Network Controller in Google Cloud.

Step 1 Locate the IP address for your Cisco Cloud Network Controller.

The management IP address is shown at the end of the output from the Deployment Manager in Deploying the Cisco Cloud Network Controller in Google Cloud.

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

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 Network Controller.

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 Network Controller:

Configuring Cisco Cloud Network Controller Using the Setup Wizard

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

Configuring Cisco Cloud Network Controller Using the Setup Wizard

Step 11 Determine if you want to configure inter-site connectivity and/or external network connectivity.

- For releases prior to release 25.0(5), click the box next to **Enable** to enable external network connectivity.
- For release 25.0(5) and later, determine if you want to configure inter-site connectivity and/or external network connectivity:
  - **Catalyst 8000Vs**: Click the box in this column for a region if you want to use the Cisco Catalyst 8000V router for inter-site connectivity for inter-site use cases.This is functionality introduced in release 25.0(5) that allows you to configure a BGP-EVPN connection for inter-site connectivity between a Google Cloud site and other cloud sites or an ACI on-premises site using Cisco Catalyst 8000V routers. See "Inter-Site Connectivity Using BGP-EVPN" in the *Cisco Cloud Network Controller for Google Cloud User Guide* for more information.
  - **External Connectivity using Google Cloud Routers**: Click the box in this column for any region where you want to use the Google Cloud router for external network connectivity. This allows you to configure an IPv4 connection between a Google Cloud site and non-Google Cloud sites or an external device, where a VPN connection is created between a Google Cloud router and an external device. See "External Network Connectivity" in the *Cisco Cloud Network Controller for Google Cloud User Guide* for more information.

Step 12 Click the appropriate button to advance to the next page.

- If you did not configure inter-site connectivity or external network connectivity in the **Region Management** page (if you didn't select any options in the **Region Management** page), then click **Save and Continue**. You are returned to the **Let's Configure the Basics** page. Go to Step 20, on page 6.
- If you enabled inter-site connectivity and/or external network connectivity, click **Next** at the bottom of the page. The **General Connectivity** page appears.

Step 13 If you configured inter-site connectivity (if you selected the **Catalyst 8000Vs** option for one or more regions in the **Region Management** page), enter the necessary information in the **Subnet Pools for Cloud Routers** area.

The first subnet pool is automatically populated (shown as `System Internal`). Addresses from this subnet pool will be used for inter-region connectivity for any additional regions that are added that need to be managed by the Cisco Cloud Network Controller. Subnet pools added in this field must be a valid IPv4 subnet with mask /24.

If you selected additional regions to have Catalyst 8000Vs deployed in the **Region Management** page, add *one* additional subnet pool for every region where you will have 2-4 Catalyst 8000Vs deployed (if you enter **2**, **3**, or **4** in the **Number of Routers Per Region** field in 16.c, on page 5)

Step 14 If you configured external network connectivity (if you selected the **External Connectivity using Google Cloud Routers** option for one or more regions in the **Region Management** page), 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.
- You can add up to four regions to deploy the hub network. The hub network will create one cloud router in each region selected in the previous **Region Management** page.

In the previous **Region Management** page:

- If you enabled inter-site connectivity (if you clicked the boxes in the **Catalyst 8000Vs** column for certain regions) and you did *not* enable external network connectivity (you did not click any boxes in the **External Connectivity using Google Cloud Routers** column for any regions), then the **Hub Network** area has the following entries by default and cannot be edited:
  - **Name**: default
  - **BGP Autonomous System Number**: 65534
  - **VPN Router**: default
- If you did enable external network connectivity (you did click one or more boxes in the **External Connectivity using Google Cloud Routers** column for any regions), then you can edit the default entry in the **BGP Autonomous System Number** field, if necessary.

a) In the **Hub Network** area, click the pencil icon to edit the information in the**Hub Network** field.

The **Edit Hub Network** window appears. Note that the default entries in the **Name** and **VPN Router** fields cannot be edited.

b) Change the value in the **BGP Autonomous System Number** field, if necessary.

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.

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

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

Step 15 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 16 Enter the necessary information in the **Catalyst 8000Vs** area.

a) In the **BGP Autonomous System Number for C8kVs** field, enter a unique BGP autonomous system number (ASN).

The BGP autonomous system number can be in the range of 1 - 65535.

b) In the **Assign Public IP to C8kV Interface** field, determine if you want to assign public IP addresses to the Catalyst 8000V interfaces.

Configuring Cisco Cloud Network Controller Using the Setup Wizard

Private IP addresses are assigned to the Catalyst 8000V interfaces by default. The **Assign Public IP to C8kV Interface** option determines whether public IP addresses will also be assigned to the Catalyst 8000V interfaces or not.

The Catalyst 8000V interface IP addresses are used for the following purposes:

- Allows you to manage the Catalyst 8000V or allows you to SSH to the Catalyst 8000V directly
- Allows you to cross-program the interfaces across sites for multi-cloud and hybrid cloud connectivity through the Cisco Nexus Dashboard Orchestrator
- For the Catalyst 8000Vs for both control plane and data plane traffic

By default, the **Enabled** check box is checked. This means that public IP addresses can be assigned to the Catalyst 8000Vs.

- If you want *public* IP addresses assigned to the Catalyst 8000Vs in addition to the private IP addresses, leave the check in the box next to **Enabled**.
- If you want only *private* IP addresses assigned to the Catalyst 8000Vs, remove the check in the box next to **Enabled** to disable this option.

Note that changing the Catalyst 8000V connectivity from private to public, or vice versa, may cause disruption in your network. In addition, if the public IP address is removed from the Catalyst 8000V, then the Google Cloud site will connect to the on-premises ACI site using the private IP address via the Google Cloud interconnect. You will have to configure private intersite connectivity for the Google Cloud site from Nexus Dashboard Orchestrator and configure Google Cloud interconnect from the Google Cloud portal.

Note Both the public and private IP addresses assigned to a Catalyst 8000V are displayed with the other details of the router in the **Cloud Resources** area. If public IP addresses are not assigned to a Catalyst 8000V, only the private IP addresses are displayed.

c) In the **Number of Routers Per Region** field, choose the number of Catalyst 8000Vs that will be used in each region.

d) In the **Username**, enter the username for the Catalyst 8000V.

e) In the **Password** field, enter the password for the Catalyst 8000V.

Enter the password again in the **Confirm Password** field.

f) In the **Throughput of the routers** field, choose the throughput of the Catalyst 8000V.

Changing the value in this field changes the size of the Catalyst 8000V instance that is deployed. Choosing a higher value for the throughput results in a larger VM being deployed.

Note the following:

- The licensing of the Catalyst 8000V is based on this setting. You will need the equivalent or higher license in your Smart account for it to be compliant. See Resources Used for Cisco Cloud Network Controller Deployment in Google Cloud for more information.
- Cloud routers should be undeployed from all regions before changing the router throughput or login credentials.

  If you wish to change this value at some point in the future, you must delete the Catalyst 8000V, then repeat the processes in this chapter again and select the new value that you would like in the same **Throughput of the routers** field.

g) Enter the necessary information in the **TCP MSS** field, if applicable.

The **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied to all cloud router interfaces, including data Gigabit Ethernet interfaces, IPSec tunnel interfaces of cloud routers, and VPN tunnel interfaces toward cloud, on-premises, or other cloud sites. For VPN tunnels towards the cloud, if the cloud provider's MSS value is less than the value that you enter in this field, then the lower value is used; otherwise, the value that you enter in this field is used.

The MSS value affects only TCP traffic, and has no impact on other types of traffic, such as ping traffic.

h) In the **License Token** field, enter the license token for the Catalyst 8000V.

This is the Product Instance Registration token from your Cisco Smart Software Licensing account. To get this license token, go to http://software.cisco.com, then navigate to **Smart Software Licensing** > **Inventory** > **Virtual Account** to find the Product Instance Registration token. See Cisco Cloud Network Controller Licensing for more information.

Note If you assigned private IP addresses to the Catalyst 8000Vs in 16.b, on page 4, the only supported option is **Direct connect to Cisco Smart Software Manager (CSSM)** when registering smart licensing for Catalyst 8000Vs with private IP addresses. You must provide reachability to the CSSM through express route in this case.

Step 17 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 18 Click the **Intent** icon.
The **Intent** menu appears.

Step 19 In the **Workflows** area, click **Cisco Cloud Network Controller Setup**.
The **Set up - Overview** dialog box appears with options for **DNS and NTP Servers**, **Advanced Settings**, **Region Management**, and **Smart Licensing**.

Step 20 In the **Advanced Settings** area, click **Edit Configuration**.

Step 21 In the **Contract Based Routing** field, click the box next to **yes** to enable contract-based routing, then click **Save and Continue**.

Note You can also enable contract-based routing through Nexus Dashboard Orchestrator by navigating to the Google Cloud site, then clicking the **Contract Based Routing** option under the **Inter-Site Connectivity** area.

Step 22 In the **Smart Licensing** row, click **Register**.

The **Smart Licensing** page appears.

Step 23 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 Network Controller 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/

Configuring Cisco Cloud Network Controller Using the Setup Wizard

- 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 24 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 25 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 Network Controller.

If this is the first time that you are deploying your Cisco Cloud Network Controller, 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 Network Controller Setup Wizard Configurations, on page 8
- Completing the Initial Configuration
  - Configuring an External Network
  - Creating a Tenant
  - If you configured a BGP-EVPN connection for inter-site connectivity using Cisco Catalyst 8000V routers, follow the procedures in Configuring VPC Peering for Inter-Site Connectivity Using BGP-EVPN to allow the user VPCs in the Google Cloud site to communicate with VPCs in other cloud sites or an ACI on-premises site.
- If you are managing additional sites (an on-premises site or cloud sites) along with the Cisco Cloud Network Controller site, refer to the Managing Google Cloud Sites Using Nexus Dashboard Orchestrator document.
- Understanding the Cisco Cloud Network Controller GUI
- Logging Into Cisco Cloud Network Controller Through SSH

Verifying the Cisco Cloud Network Controller Setup Wizard Configurations

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

Step 1 In Cisco Cloud Network Controller, 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.

Step 2 If you set up a BGP-EVPN connection for inter-site connectivity using the Catalyst 8000Vs, verify that the number of VM instances on the Google Cloud side match the number of Catalyst 8000Vs that you set up in the Cisco Cloud Network Controller.

a) Log into the Google Cloud project associated with the infra tenant.
b) Navigate to **Compute Engine** > **VM instances** in Google Cloud.
c) Verify that the number of VM instances shown in the **Instances** tab match the total number of Catalyst 8000Vs that you have for the BGP-EVPN connection for inter-site connectivity.

   For example, when you were setting up the cloud infrastructure configuration for your Cisco Cloud Network Controller in Configuring Cisco Cloud Network Controller Using the Setup Wizard, on page 1, if you chose two regions and two Catalyst 8000Vs for each region, you should see four VM instances in the **Instances** tab.

Step 3 If you set up a BGP-EVPN connection for inter-site connectivity using the Catalyst 8000Vs, verify that you have the VPC networks set up for the overlay-1 VPC and overlay-1 secondary VPC in Google Cloud.

See "Inter-Site Connectivity Using BGP-EVPN" in the *Cisco Cloud Network Controller for Google Cloud User Guide* for more information.

a) Navigate to **VPC network** > **VPC networks** in Google Cloud.
b) Verify that you see the VPC networks that were set up for the overlay-1 VPC and overlay-1 secondary VPC in the **VPC networks** screen.