Configuring Cisco Cloud APIC Using the Setup Wizard

Configuring and Deploying Inter-Site Connectivity

Before you can begin to configure and deploy your Cloud APIC, you must first configure and deploy your Multi-Site and your on-premises Cisco ACI, if you are connecting an on-premises site to cloud sites. The actual configuration for each varies, depending on your requirements and setup. If you are connecting an on-premises site to cloud sites, you will also need to configure and deploy an on-premises IPsec termination device to connect to theCloud Services Router deployed by Cloud APIC in AWS. See Components of Extending Cisco ACI Fabric to the Public Cloud for more information.

Following are documents that will aid you in the process of configuring and deploying these components:

- Cisco ACI documentation: Available at Cisco Application Policy Infrastructure Controller (APIC) documentation, such as Operating Cisco Application Centric Infrastructure and Cisco APIC Basic Configuration Guide.
- Nexus Dashboard documentation: Available at Nexus Dashboard documentation, such as Multi-Site Orchestrator Installation and Upgrade Guide.
- Cisco Cloud Services Router 1000v: Available at Cisco CSR 1000v documentation.
- Cisco Catalyst 8000v Edge Software: Available at Cisco Catalyst 8000v Edge software documentation.

Gathering On-Premises Configuration Information

Note You do not have to gather any information in this section if you are only configuring cloud site-to-cloud site connectivity for your Cisco Cloud APIC.

Use the following list to gather and record the necessary on-premises configuration information that you will need throughout these procedures to set up your Cisco Cloud APIC:

Necessary On-Premises Information	Your Entry
On-premises IPsec device public IP address	
IPsec termination device to CCR OSPF area	
On-premises APIC IP address	
Cisco Cloud APIC IP address	

Understanding Limitations for Number of Sites, Regions and CCRs

Throughout this document, you will be asked to decide on various configurations for sites, regions and CCRs. Following is a list of limitations for each that you should keep in mind as you're making configuration decisions for each.

Sites

The total number of sites that you can have with Cloud APIC depends on the type of configuration that you are setting up:

- **On-premises ACI site-to-cloud site configuration (AWS or Azure)**: Multi-Site multi-cloud deployments support any combination of one or two cloud sites (AWS or Azure) and one or two on-premises sites for a maximum total of four sites. The connectivity options are:
  - Hybrid-Cloud: On-premises-to-single cloud site connectivity
  - Hybrid Multi-Cloud: On-premises-to-multiple cloud sites connectivity
- **Multi-Cloud: Cloud site-to-cloud site connectivity (AWS or Azure)**: Multi-Site multi-cloud deployments support a combination of:
  - Two cloud sites in EVPN deployment mode (AWS and Azure only)
  - Beginning with release 25.0(2), three clouds in BGP IPv4 deployment mode (AWS, Azure, and GCP)

  GCP to GCP is not yet supported, either with BGP IPv4 or BGP EVPN.

- **Cloud First: Single-Cloud Configuration**: Multi-Site multi-cloud deployments support a single cloud site (AWS, Azure, or GCP)

Regions

In Cisco Cloud APIC Release 25.0(1), the supported region limits are:

- Four regions can be managed in AWS and Azure clouds. All four regions can be used for workload deployments and external connectivity.
- All regions can be managed in the GCP cloud. Four regions can be used for workload deployments and external connectivity.

In Cisco Cloud APIC Release 25.0(2) and later, the supported region limits are:

- Sixteen regions can be managed in AWS and Azure clouds. Of the 16, only 4 regions can be external connectivity. All 16 regions can be used for workload deployment.
- All regions can be managed in the GCP cloud. Sixteen regions can be used for workload deployments, but only 4 regions can be used for external connectivity.

CCRs

You can have a certain number of CCRs within some regions, with the following limitations:

- You must have at least one region with CCRs deployed to have inter-VNET (Azure), inter-VPC (AWS), or inter-VRF communications.
- You do not have to have CCRs in every region.
- For regions with CCRs deployed to enable connectivity:
  - CCRs can be deployed on all four managed regions.
  - A maximum of four CCRs per managed region is supported, for a total of 16 CCRs per cloud site.

Note The number of CCRs per managed region differs between AWS and Azure, with four CCRs per region supported for AWS (for a total of 16 CCRs per cloud site) and eight CCRs per region supported for Azure for release 5.1(2) and later (for a total of 32 CCRs per cloud site).

- CCR deployment in GCP by Cloud APIC is not yet supported.

Locating the Cloud APIC IP Address

These procedures describe how to locate the IP address for the Cloud APIC through the AWS site.

Step 1 Go to the AWS account for the Cloud APIC infra tenant.

Step 2 Click the **Services** link at the top of the screen, then click the **EC2** link.

The **EC2 Dashboard** screen appears.

Step 3 In the EC2 Dashboard screen, you should see text displaying the number of running instances in the **Resources** area (for example, **1 Running Instances**). Click this running instances link.

The **Instances** screen appears.

Step 4 Choose the Cloud APIC instance named `Capic-1` and copy the IP address that is shown in the **IPv4 Public IP** column.

This is the Cloud APIC IP address that you will use to log into the Cloud APIC.

Note You can also get the Cloud APIC IP address by going back to the **CloudFormation** page, clicking on the box next to the Cisco Cloud APIC and then clicking on the **Outputs** tab. The Cisco Cloud APIC IP address is shown in the **Value** column.

Configuring Cisco Cloud APIC Using the Setup Wizard

Follow the procedures in this topic to set up the cloud infrastructure configuration for your Cloud APIC. Cloud APIC will automatically deploy the required AWS constructs and the necessary CCRs.

Before you begin

Following are the prerequisites for this task:

- You have met the requirements that are outlined in Requirements for Extending the Cisco ACI Fabric to the Public Cloud before proceeding with the tasks in this section.
- You have successfully completed the procedures that are provided in Configuring the Cloud Formation Template Information for the Cisco Cloud APIC.

Step 1 In the AWS site, get the Cloud APIC IP address.

See Locating the Cloud APIC IP Address, on page 3 for those instructions.

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 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 Cloud APIC:

- **Username:** Enter **admin** for this field.
- **Password:** Enter the password that you provided on the Specify Details page from 12 in the Deploying the Cloud APIC in AWS procedures.
- **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 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 Servers**
- **Region Management**
- **Smart Licensing**

Step 6 In the **DNS 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 5 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 Determine if you want to use AWS Transit Gateway.

Use Transit Gateway to avoid using VPN tunnels for connectivity within a region and across the regions where TGW peering is supported. For more information, see the *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect* document.

In the **Use Transit Gateway** area, click the checkbox next to **Enable** if you want to use AWS Transit Gateway.

Step 11 In the **Regions to Manage** area, verify that the Cloud APIC home region is selected.

The region that you selected in 2 in Deploying the Cloud APIC in AWS is the home region and should be selected already in this page. This is the region where the Cloud APIC is deployed (the region that will be managed by Cloud APIC), and will be indicated with the text `cAPIC deployed` in the Region column.

Step 12 Select additional regions if you want the Cloud APIC to manage additional regions, and to possibly deploy CCRs to have inter-VPC communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

The CCR can manage four regions, including the home region where Cloud APIC is deployed.

A Cloud APIC can manage multiple cloud regions as a single site. In a typical Cisco ACI configuration, a site represents anything that can be managed by an APIC cluster. If a Cloud APIC cluster manages two regions, those two regions are considered a single site by Cisco ACI.

Step 13 To deploy cloud routers locally to this region, click to place a check mark in the **Cloud Routers** check box for that region.

You must have at least one region with CCRs deployed to have inter-VPC or inter-VNET communications. However, if you choose multiple regions in this page, you do not have to have CCRs in every region that you choose. See Understanding Limitations for Number of Sites, Regions and CCRs, on page 2 for more information.

Step 14 When you have selected all the appropriate regions, click **Next** at the bottom of the page.

The **General Connectivity** page appears.

Step 15 Enter the following information on the **General Connectivity** page.

- If you enabled the AWS Transit Gateway Connect feature in Step 10, on page 5, then the Hub Network fields will be available in this window. Go to 15.a, on page 6.
- If you did not enable the AWS Transit Gateway Connect feature in Step 10, on page 5, skip to 15.e, on page 6.

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) In the **BGP Autonomous System Number** field, enter a zero for AWS to choose a number, or enter a value between 64512 and 65534, inclusive, for each hub network, and then click the check mark next to the field.

To configure your own BGP autonomous number, enter a value between 64512 and 65534 for each hub network.

We recommend that you use different numbers for different instances of AWS Transit Gateway.

d) In the **CIDRs** area, click **Add CIDR**.

This will be the AWS Transit Gateway Connect CIDR block, which will be used as the connect peer IP address (the GRE outer peer IP address) on the Transit Gateway side.

1. In the **Region** field, select the appropriate region.
2. In the **CIDR Block Range** field, enter the CIDR block that will be used as the connect peer IP address on the Transit Gateway side.
3. Click the checkmark to accept these values for this CIDR block.
4. For every managed region that will be using the AWS Transit Gateway Connect feature, repeat these steps to add CIDR blocks to be used for each of those managed regions.

e) To add a subnet pool for the CCRs, click **Add Subnet Pool for Cloud Routers** and enter the subnet in the text box.

The first subnet pool for the first two regions is automatically populated. If you selected more than two regions, you will need to add a subnet for the cloud router to the list for the additional two regions. Addresses from this

Configuring Cisco Cloud APIC Using the Setup Wizard

subnet pool will be used for inter-region connectivity for any additional regions that are added that need to be managed by the Cloud APIC after the first two regions. This must be a valid IPv4 subnet with mask /24.

Note The /24 subnet provided during the Cloud APIC deployment would be sufficient for up to two cloud sites. If you need to manage more than two cloud sites, you need to add more subnets.

f) In the **IPSec Tunnel Subnet Pool** area, click **Add IPSec Tunnel Subnet Pools**.

The **Add IPSec Tunnel Subnet Pools** window appears.

g) Enter the subnet pool to be used for IPSec tunnels, if necessary.

This subnet pool is used to create an IPSec tunnel between your cloud router and the router on the branch office or external network. This subnet will be used to address the IPSec tunnel interfaces and loopbacks of the cloud routers used for external connectivity.

You can add more subnets to be used for IPSec tunnels in this area, or delete entries in this area if subnets are not used by any tunnels.

Click the check mark after you have entered in the appropriate subnet pools.

h) In the **CCRs** area, enter a value in the **BGP Autonomous System Number for CCRs** field.

The BGP ASN can be in the range of 1 - 65534.

Note Do not use **64512** as the autonomous system number in this field.

i) In the **Assign Public IP to CCR Interface** field, determine if you want to have a public or a private IP address assigned to the CCR interfaces.

- To have a public IP address assigned to the CCR interfaces, leave the check in the **Enabled** check box. By default, the **Enabled** check box is checked.
- To have public IP disabled to the CCR interfaces, uncheck the **Enabled** check box. A private IP address is used for connectivity in this case.

Note Disabling or enabling a public IP address is a disruptive operation and can result in traffic loss.

Beginning with release 5.2(1), both the public and private IP addresses assigned to a CCR are displayed with the other details of the router in the Cloud Resources area. If a public IP is not assigned to a CCR, only the private IP is displayed.

j) In the **Number of Routers Per Region** field, choose the number of CCRs that will be used in each region.

See Understanding Limitations for Number of Sites, Regions and CCRs, on page 2 for more information on any limitations on the number of CCRs per region.

k) In the **Username**, enter the username for the CCR.

l) In the **Password** field, enter the password for the CCR.

m) In the **Pricing Type** field, select one of the two types of licensing models:

Note There are two PAYG options for consuming licenses in the AWS marketplace: **Catalyst 8000V Cisco DNA Essentials** and **Catalyst 8000V Cisco DNA Advantage** . Cisco Cloud APIC will make use of **Catalyst 8000V Cisco DNA Advantage**.

1. **BYOL**
2. **PAYG**

Configuring Cisco Cloud APIC Using the Setup Wizard

For the **BYOL Pricing Type**, the steps are as follows:

1. In the **Throughput of the routers** field, choose the throughput of the CCR.

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

   Note If you wish to change this value at some point in the future, you must delete the CCR, 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.

   In addition, the licensing of the CCR is based on this setting. You will need the equivalent or higher license in your Smart account for it to be compliant. See Requirements for the AWS Public Cloud for more information.

   Note Cloud routers should be undeployed from all regions before changing the router throughput or login credentials.

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

   Beginning with Release 5.0(2l), the **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied all cloud router interfaces, including VPN tunnels towards the cloud and external tunnels towards the on-premises site 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.

3. In the **License Token** field, enter the license token for the CCR.

   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.

   Note If the public IP addresses are disabled to the CCRs in 15.i, on page 7, the only supported option is **AWS Direct Connect or Azure Express Route to Cisco Smart Software Manager (CSSM)** when registering smart licensing for CCRs with private IP addresses (available by navigating to **Administrative** > **Smart Licensing**). You must provide reachability to the CSSM through AWS Direct Connect or Azure Express Route in this case. When the public IP addresses are disabled, public internet cannot be used because private IP addresses are being used. The connectivity should therefore use Private Connection, which is AWS Direct Connect or Azure Express Route.

For the **PAYG Pricing Type**, the steps are as follows:

1. In the **VM Type** field, select one of the AWS EC2 Instances as per your requirement.

   Cisco Cloud APIC supports a range of AWS EC2 instances for cloud networking needs powered by Cisco's Catalyst 8000V virtual router. The table below shows the cloud instance type supported by Cisco Cloud APIC on AWS.

AWS EC2 Instance	CCR Throughput	vCPUs	Memory
c5.xlarge	up to 5 Gigabit throughput	4	8 GiB
c5.2xlarge	up to 10 Gigabit throughput	8	16 GiB

Configuring Cisco Cloud APIC Using the Setup Wizard

AWS EC2 Instance	CCR Throughput	vCPUs	Memory
c5.4xlarge	up to 10 Gigabit throughput	16	32 GiB
c5.9xlarge	up to 10 Gigabit throughput	36	72 GiB
c5n.xlarge	up to 25 Gigabit throughput	4	10.5 GiB
c5n.2xlarge	up to 25Gigabit throughput	8	21 GiB
c5n.4xlarge	up to 25 Gigabit throughput	16	42 GiB
c5n.9xlarge	up to 50 Gigabit throughput	36	96 GiB

Changing the value in this field changes the other factors of the CCR as listed in the table above. Choosing a higher value for the VM size results in higher throughput.

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

   Beginning with Release 5.0(2l), the **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied all cloud router interfaces, including VPN tunnels towards the cloud and external tunnels towards the on-premises site 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.

Note User need not provide the License token on selecting PAYG.

Note All the features supported in BYOL will be supported by PAYG.

Step 16 Click **Save and Continue**.

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

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

The **Smart Licensing** page appears.

Step 18 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 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 19 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 20 Verify the information on the **Summary** page, then click **Close**.

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

If this is the first time that you are deploying your 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

Determine if you are managing additional sites along with the Cisco Cloud APIC site or not:

- If you are managing additional sites (an on-premises site or cloud sites) along with the Cisco Cloud APIC site, go to Managing Cisco Cloud APIC Through Multi-Site.
- If you are setting up a Cloud First configuration, where you are not managing any other sites along with the Cisco Cloud APIC site, you will not need to use the Cisco Cisco Nexus Dashboard Orchestrator for additional configurations. However, you will have additional configurations that you must perform in the Cisco Cloud APIC GUI in this case. Use the Global Create option in the Cisco Cloud APIC GUI to configure the following components:
  - Tenant
  - Application Profile
  - EPG

  See Navigating the Cisco Cloud APIC GUI and Configuring Cisco Cloud APIC Components for more information.

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 regions that you selected are shown as **managed** in the Admin State column.
- Under **Infrastructure**, click on **Inter-Region Connectivity** and verify the information in this screen is correct.
- Under **Infrastructure**, click on **On Premises Connectivity** and verify the information in this screen is correct.
- Click on Dashboard and use the information in the On Premises Connectivity Status and the Inter-Region Connectivity Status boxes to verify that the setup wizard and tunnel configurations were done properly.

What to do next

Complete the multi-site configuration using the procedures provided in Managing Cisco Cloud APIC Through Multi-Site.