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 Cisco ACI 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 the Cisco Cloud Services Router 1000Vs 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, Release 4.0(1).
- Cisco ACI Multi-Site: Available at Cisco ACI Multi-Site documentation, such as Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 2.0(1).
- Cisco Cloud Services Router 1000V: Available at Cisco CSR 1000v 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 CSR OSPF area	
On-premises APIC IP address	
Cisco Cloud APIC IP address	

Understanding Limitations for Number of Sites, Regions and CSRs

Throughout this document, you will be asked to decide on various configurations for sites, regions and CSRs. 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)**: ACI 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)**: ACI Multi-Site multi-cloud deployments support a combination of any two cloud sites (AWS, Azure, or both) for a total of two sites.
- **Cloud First: Single-Cloud Configuration**: ACI Multi-Site multi-cloud deployments support a single cloud site (AWS or Azure)

Regions

Within each site, you can have a maximum of four regions per site. Cloud APIC can manage multiple regions as a single site.

CSRs

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

- You must have at least one region with CSRs deployed to have inter-VNET (Azure), inter-VPC (AWS), or inter-VRF communications.
- You do not have to have CSRs in every region.

- For regions with CSRs deployed to enable connectivity:
  - CSRs can be deployed on all four managed regions.
  - A maximum of four CSRs per managed region is supported, for a total of 16 CSRs per cloud site.

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

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 CSRs.

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 CSRs to have inter-VPC communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

The CSR 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 CSRs deployed to have inter-VPC or inter-VNET communications. However, if you choose multiple regions in this page, you do not have to have CSRs in every region that you choose. See Understanding Limitations for Number of Sites, Regions and CSRs, 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.

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 **TGW Connect** field, click the checkbox if you want to enable the AWS Transit Gateway Connect feature.

For more information on the AWS Transit Gateway Connect feature, see the *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect* document.

e) 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.

f) To add a subnet pool for the CSRs, click **Add Subnet Pool for Cloud Router** 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 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.

g) Enter a value in the **BGP Autonomous System Number for CSRs** 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.

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

- To have a public IP address assigned to the CSR interfaces, leave the check in the **Enabled** check box. By default, the **Enabled** check box is checked.
- To have public IP disabled to the CSR 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 CSR are displayed with the other details of the router in the Cloud Resources area. If a public IP is not assigned to a CSR, only the private IP is displayed.

i) Under the **Cloud Router Template** area, in the **Number of Routers Per Region** field, choose the number of Cisco Cloud Services Routers that will be used in each region.

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

j) In the **Username**, enter the username for the Cisco Cloud Services Router.

Configuring Cisco Cloud APIC Using the Setup Wizard

k) In the **Password** field, enter the password for the Cisco Cloud Services Router.

l) In the **Throughput of the routers** field, choose the throughput of the Cisco Cloud Services Router.

Changing the value in this field changes the size of the CSR 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 CSR, 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 CSR 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.

m) 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.

n) In the **License Token** field, enter the license token for the Cisco Cloud Services Router.

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 CSRs in 15.h, on page 6, the only supported option is **AWS Direct Connect or Azure Express Route to Cisco Smart Software Manager (CSSM)** when registering smart licensing for CSRs 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.

Step 16 Click the appropriate button, depending on whether you are configuring inter-site connectivity or not.

- If you are not configuring inter-site connectivity (if you did not select **Inter-Site Connectivity** when you were selecting regions to manage in the **Region Management** page), click **Save and Continue**. The **Let's Configure the Basics** page appears again. Skip to Step 19, on page 8.
- If you are configuring inter-site connectivity (if you selected **Inter-Site Connectivity** when you were selecting regions to manage in the **Region Management** page), click **Next** at the bottom of the page. The **Inter-Site Connectivity** page appears.

Step 17 Enter the following information in the **Inter-Site Connectivity** page:

- **IPSec Tunnels to Inter-Site Routers**: This field is necessary only for on-premises connectivity to cloud sites. There is no need to enter information in this field if you don't have an on-premises site.

  In this area, click the + button next to the **Add Public IP of IPsec Tunnel Peer** field.

Configuring Cisco Cloud APIC Using the Setup Wizard

- Enter the peer IP address for the IPsec tunnel termination to the on-premises device.
- Click the check mark to add this peer IP address.

- **OSPF Area for Inter-Site Connectivity**: Enter the underlay OSPF area ID that will be used with on-premises ISN peering (for example, `0.0.0.1`)
- Under the **External Subnets for Inter-Site Connectivity** heading, click the + button next to the **+Add External Subnet** field.
  - Enter the subnet tunnel endpoint pool (the cloud TEP) that will be used in AWS. It must be a valid IPv4 subnet with a mask between /16 and /22 (for example, `30.29.0.0/16`). This subnet will be used to address the IPsec tunnel interfaces and loopbacks of the Cloud Routers used for on-premises connectivity, and cannot overlap with other on-premises TEP pools.
  - Click the check mark after you have entered in the appropriate subnet pools.

Step 18 When you have entered all the necessary information on this page, click **Save and Continue** at the bottom of the page.

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

Step 19 In the **Smart Licensing** row, click **Register**.

The **Smart Licensing** page appears.

Step 20 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 21 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 22 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 (if you selected the **Inter-Site Connectivity** option in the **Region Management** page), go to Managing Cisco Cloud APIC Through Cisco ACI 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 (if you selected only the **Cloud Routers** option in the **Region Management** page), you will not need to use the Cisco ACI Multi-Site 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 Cisco ACI Multi-Site.