



# Configuring Cisco Cloud APIC Using the Setup Wizard

---

- [Configuring and Deploying Your On-Premises Cisco ACI and Cisco ACI Multi-Site](#) , on page 1
- [Gathering On-Premises Configuration Information](#), on page 1
- [Understanding Limitations for Number of Sites, Regions and CSRs](#), on page 2
- [Locating the Cloud APIC IP Address](#), on page 3
- [Configuring Cisco Cloud APIC Using the Setup Wizard](#), on page 3
- [Verifying the Cisco Cloud APIC Setup Wizard Configurations](#), on page 8

## Configuring and Deploying Your On-Premises Cisco ACI and Cisco ACI Multi-Site

Before you can begin to configure and deploy your Cloud APIC, you must first configure and deploy your on-premises Cisco ACI and Cisco ACI Multi-Site. The actual configuration for both varies, depending on your requirements and setup. 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

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	
ACI Multi-Site Orchestrator 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, the number of CSRs that you can deploy in each region varies:

- For cloud site-to-cloud site configurations (Multi-Cloud):
  - CSRs can be deployed on a maximum of two managed regions.
  - A maximum of two CSRs per managed region is supported, for a total of four CSRs per cloud site.
- For on-premises-to-cloud site (Hybrid-Cloud or Hybrid Multi-Cloud) or for single-cloud (Cloud First) configurations :
  - CSRs can be deployed on all four managed regions.
  - The number of CSRs supported per managed region varies, depending on the release:
    - For releases prior to 5.1(2), a maximum of four CSRs per managed region is supported, for a total of 16 CSRs per cloud site.
    - For Release 5.1(2) and later, a maximum of eight CSRs per managed region is supported, for a total of 32 CSRs per cloud site. For more information on increasing the number of CSRs, see the Cloud APIC for AWS User Guide.

## 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** 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 11** 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.

The following options are available on the row for any region that you select:

- **Cloud Routers:** Select this option if you want to deploy CSRs in this 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.
- **Inter-Site Connectivity:** This option is shown as On Premises Connectivity in releases prior to 4.2(1).

Select this option if you want this region to connect to other sites (for example, if you want this region to connect to an on-premises site, or to connect cloud site-to-cloud site, through Cisco ACI Multi-Site). Infra VPCs or VNETs are deployed on all regions selected for inter-site connectivity. Note that when you select inter-site connectivity for a region, the cloud routers option is also selected automatically for this region because you must have two cloud routers deployed for inter-site connectivity hubs.

**Step 12** When you have selected all the appropriate regions, click Next at the bottom of the page.

The General Connectivity page appears.

**Step 13** Enter the following information on the General Connectivity page.

- a) In the Fabric Autonomous System Number field, enter the BGP autonomous system number (ASN) that is unique to this site.

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

- b) In the Subnet for Cloud Router field, enter the subnet for the cloud router.

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.

- c) 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.

- d) In the Username, enter the username for the Cisco Cloud Services Router.  
 e) In the Password field, enter the password for the Cisco Cloud Services Router.  
 f) 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.

- g) 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.

**Step 14** 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 17, on page 7](#).
- 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 15** 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.

- 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 16** 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 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 (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](#).