



About Cisco Cloud APIC

- [Overview, on page 1](#)
- [Guidelines and Limitations, on page 2](#)
- [About the Cisco Cloud APIC GUI, on page 4](#)

Overview

Cisco Application Policy Infrastructure Controller (APIC) Release 4.1(1) introduces Cisco Cloud APIC, which is a software deployment of Cisco APIC that you deploy on a cloud-based virtual machine (VM). Release 4.1(1) supports Amazon Web Services. Beginning in Release 4.2(x), support is added for Azure.

When deployed, the Cisco Cloud APIC:

- Provides an interface that is similar to the existing Cisco APIC to interact with the Azure public cloud
- Automates the deployment and configuration of cloud constructs
- Configures the cloud router control plane
- Configures the data path between the on-premises Cisco ACI fabric and the cloud site
- Translates Cisco ACI policies to cloud native construct
- Discovers endpoints
- Provides a consistent policy, security, and analytics for workloads deployed either on or across on-premises data centers and the public cloud



Note

- Cisco Multi-Site pushes the MP-BGP EVPN configuration to the on-premises spine switches
 - On-premises VPN routers require a manual configuration for IPsec
-

- Provides an automated connection between on-premises data centers and the public cloud with easy provisioning and monitoring

- Policies are pushed by Cisco Multi-Site Orchestrator to the on-premises and cloud sites, and Cisco Cloud APIC translates the policies to the cloud native constructs to keep the policies consistent with the on-premises site

For more information about extending Cisco ACI to the public cloud, see the *Cisco Cloud APIC Installation Guide*.

When the Cisco Cloud APIC is up and running, you can begin adding and configuring Cisco Cloud APIC components. This document describes the Cisco Cloud APIC policy model and explains how to manage (add, configure, view, and delete) the Cisco Cloud APIC components using the GUI and the REST API.

Guidelines and Limitations

This section contains the guidelines and limitations for Cisco Cloud APIC.

- You cannot stretch more than one VRF between on-prem and the cloud while using inter-VRF route leaking in the cloud CSRs (cloud routers). For example, in a situation where VRF1 with EPG1 is stretched and VRF2 with EPG2 is also stretched, EPG1 cannot have a contract with EPG2. However, you can have multiple VRFs in the cloud, sharing one or more contracts with one on-premises VRF.
- Set the BD subnet for on-premises sites as advertised externally to advertise to the CSR1kv on the cloud.
- Before configuring an object for a tenant, first check for any stale cloud resource objects. A stale configuration might be present if it was not cleaned properly from the previous Cisco Cloud APIC virtual machines that managed the account. Cisco Cloud APIC can display stale cloud objects, but it cannot remove them. You must log in to the cloud account and remove them manually.



Note It takes some time for Cisco Cloud APIC to detect the stale cloud resources after adding the tenant subscription ID.

Azure allows multiple tenants to share an Azure account owned by one tenant. When the account is shared by multiple tenants, only the owner tenant is able to view the stale objects in the other tenants.

To check for stale cloud resources:

1. From the Cisco Cloud APIC GUI, click the **Navigation menu > Application Management > Tenants**. The **Tenants** summary table appears in the work pane with a list of tenants as rows in a summary table.
2. Double click the tenant you are creating objects for. The Overview, Cloud Resources, Application Management, Statistics, and Event Analytics tabs appear.
3. Click the **Cloud Resources > Actions > View Stale Cloud Objects**. The **Stale Cloud Objects** dialog box appears.

- Cisco Cloud APIC tries to manage the Azure resources that it created. It does not attempt to manage resources created by other applications, other than listing existing resources as inventory. At the same time, it is also expected that Azure IAM users in the Azure infra tenant subscription, and the other tenant subscriptions, do not disturb the resources that Cisco Cloud APIC creates. For this purpose, all resources Cisco Cloud APIC creates on Azure has at least one of these two tags:

- AciDnTag
- AciOwnerTag

Cisco Cloud APIC must prevent Azure IAM users who have access to create, delete, or update VM, or any other resources, from accessing or modifying the resources that Cisco Cloud APIC created and manages. Such restrictions should apply on both the infra tenant and other user tenant subscriptions. Azure subscription administrators should utilize the above two tags to prevent their unintentional access and modifications. For example, you can have an access policy like the following to prevent access to resources managed by Cloud APIC:

```
{
  "properties": {
    "level": "CanNotDelete",
    "notes": "Optional text notes."
  }
}
```

- When configuring shared L3Out:
 - An on-premises L3Out and cloud EPGs cannot be in tenant common.
 - If an on-premises L3Out and a cloud EPG are in different tenants, define a contract in tenant common. The contract cannot be in the on-premises site or the cloud tenant.
 - Specify the CIDR for the cloud EPG in the on-premises L3Out external EPGs (l3extInstP).
 - When an on-premises L3Out has a contract with a cloud EPG in a different VRF, the VRF in which the cloud EPG resides cannot be stretched to the on-premises site and cannot have a contract with any other VRF in the on-premises site.
 - When configuring an external subnet in an on-premises external EPG:
 - Specify the external subnet as a non-zero subnet.
 - The external subnet cannot overlap with another external subnet.
 - Mark the external subnet with a shared route-control flag to have a contract with a cloud EPG.
 - The external subnet that is marked in the on-premises external EPG should have been learned through the routing protocol in the L3Out or created as a static route.
- For the total supported scale, see the following Scale Supported table:



Note With the scale that is specified in the Scale Supported table, you can have only 4 total managed regions.

Table 1: Scale Supported

Component	Number Supported
Tenants	20
Application Profiles	500

Component	Number Supported
EPGs	500
Cloud Endpoints	1000
VRFs	20
Cloud Context Profiles	40
Contracts	1000
Service Graphs	200
Service Devices	100

About the Cisco Cloud APIC GUI

The Cisco Cloud APIC GUI is categorized into groups of related windows. Each window enables you to access and manage a particular component. You move between the windows using the **Navigation** menu that is located on the left side of the GUI. When you hover your mouse over any part of the menu, the following list of tab names appear: **Dashboard**, **Application Management**, **Cloud Resources**, **Operations**, **Infrastructure**, and **Administrative**.

Each tab contains a different list of subtabs, and each subtab provides access to a different component-specific window. For example, to view the EPG-specific window, hover your mouse over the **Navigation** menu and click **Application Management > EPGs**. From there, you can use the **Navigation** menu to view the details of another component. For example, you can navigate to the **Active Sessions** window from **EPGs** by clicking **Operations > Active Sessions**.

The **Intent** menu bar icon enables you to create a component from anywhere in the GUI. For example, to create a tenant while viewing the **Routers** window, click the **Intent** icon. A dialog appears with a search box and a drop-down list. When you click the drop-down list and choose **Application Management**, a list of options, including the **Tenant** option, appears. When you click the **Tenant** option, the **Create Tenant** dialog appears displaying a group of fields that are required for creating the tenant.


For more information about the GUI icons, see [Understanding the Cisco Cloud APIC GUI Icons](#), on page 4

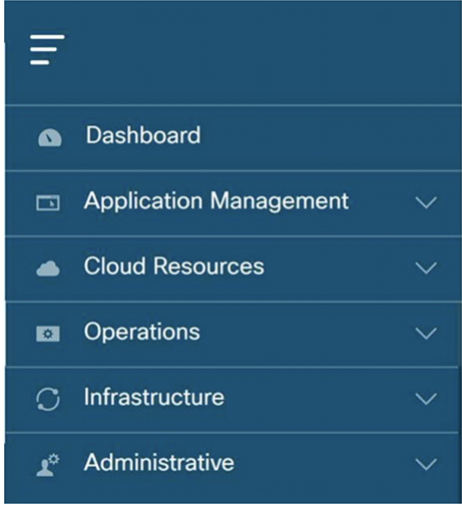

For more information about configuring Cisco Cloud APIC components, see [Configuring Cisco Cloud APIC Components](#)

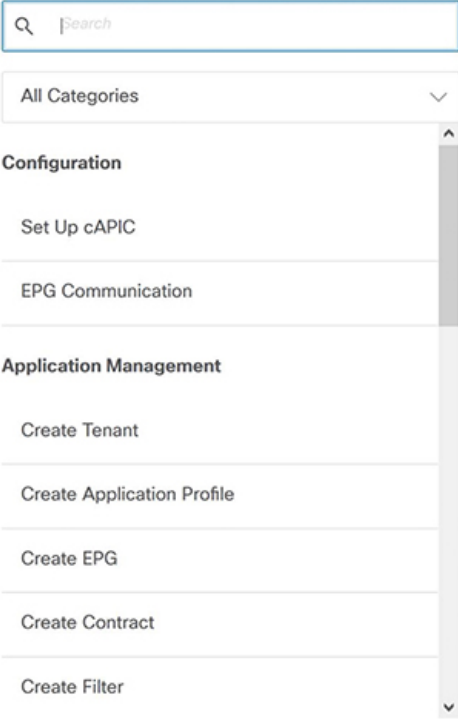
Understanding the Cisco Cloud APIC GUI Icons

This section provides a brief overview of the commonly used icons in the Cisco Cloud APIC GUI.





Table 2: Cisco Cloud APIC GUI Icons

Icon	Description
<p>Figure 1: Navigation Pane (Collapsed)</p> 	<p>The left side of the GUI contains the Navigation pane, which collapses and expands. To expand the pane, hover your mouse icon over it or click the menu icon at the top. When you click the menu icon, the Navigation pane locks in the open position. To collapse it, click the menu icon again. When you expand the Navigation pane by hovering the mouse icon over the menu icon, you collapse the Navigation pane by moving the mouse icon away from it.</p> <p>When expanded, the Navigation pane displays a list of tabs. When clicked, each tab displays a set of subtabs that enable you to navigate between the Cisco Cloud APIC component windows.</p>

Icon	Description
<p>Figure 2: Navigation Pane (Expanded)</p> 	<p>The Cisco Cloud APIC component windows are organized in the Navigation pane as follows:</p> <ul style="list-style-type: none"> • Dashboard Tab—Displays summary information about the Cisco Cloud APIC components. • Application Management Tab—Displays information about tenants, application profiles, EPGs, contracts, filters, VRFs, service graphs, devices, and cloud context profiles. • Cloud Resources Tab—Displays information about regions, VNETs, routers, security groups (application security groups/network security groups), endpoints, instances, and cloud services (and target groups). • Operations Tab—Displays information about event analytics, active sessions, backup & restore policies, tech support policies, firmware management, schedulers, and remote locations. • Infrastructure Tab—Displays information about the system configuration, inter-region connectivity, and on-premises connectivity. • Administrative Tab—Displays information about authentication, event analytics, security, local and remote users, and smart licensing. <p>Note For more information about the contents of these tabs, see Viewing System Details</p>
<p>Figure 3: Intent Menu-Bar Icon</p> 	<p>The Intent icon appears in the menu bar between the search and the help icons.</p> <p>When clicked, the Intent dialog appears (see below). The Intent dialog enables you to create a component from any window in the Cisco Cloud APIC GUI. When you create or view a component, a dialog box opens and hides the Intent icon. Close the dialog box to access the Intent icon again.</p> <p>For more information about creating a component, see Configuring Cisco Cloud APIC Components.</p>

Icon	Description
Figure 4: Intent Dialog Box	
	

Icon	Description
	<p>The Intent dialog box contains a search box and a drop-down list. The drop-down list enables you to apply a filter for displaying specific options. The search box enables you to enter text for searching through the filtered list.</p> <ul style="list-style-type: none"> • All Categories • Configuration—Displays the following options: <ul style="list-style-type: none"> • Set Up cAPIC • EPG Communication • Application Management—Displays the following options: <ul style="list-style-type: none"> • Create Tenant • Create Application Profile • Create EPG • Create Contract • Create Filter • Create VRF • Create Device • Create Service Graph • Create Cloud Context Profile • Operations—Displays the following options: <ul style="list-style-type: none"> • Create Backup Configuration • Create Tech Support • Create Scheduler • Create Remote Location • Administrative—Displays the following options: <ul style="list-style-type: none"> • Create Login Domain • Create Security Domain • Create Role • Create RBAC Rule • Create Certificate Authority • Create Key Ring

Icon	Description
	<ul style="list-style-type: none"> • Create Local User
<p>Figure 5: Help Menu-Bar Icon</p> 	<p>The help menu-bar icon opens the Cisco Cloud APIC Quick Start Guide .</p>
<p>Figure 6: System Tools Menu-Bar Icon</p> 	<p>The system tools menu-bar icon provides the following options:</p> <ul style="list-style-type: none"> • About—Display the Cisco Cloud APIC version. • ObjectStore Browser—Open the Managed Object Browser, or Visore, which is a utility that is built into Cisco Cloud APIC that provides a graphical view of the managed objects (MOs) using a browser.
<p>Figure 7: Search Menu-Bar Icon</p> 	<p>The search menu-bar icon displays the search field, which enables you to search for any object by name or any other distinctive fields.</p>
<p>Figure 8: User Profile Menu-Bar Icon</p> 	<p>The user profile menu-bar icon provides the following options:</p> <ul style="list-style-type: none"> • Change Password—Enables you to change the password. • Change SSH Key—Enables you to change the SSH key. • Change User Certificate—Enables you to change the user certificate. • Logout—Enables you to log out of the GUI.

