



## **Cisco Cloud APIC for Google Cloud User Guide, Release 25.0(1)-25.0(4)**

**First Published:** 2021-09-20

**Last Modified:** 2022-08-08

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





## Trademarks

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at:

<http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)





## CONTENTS

---

<b>PREFACE</b>	<b>Trademarks</b> iii
----------------	-----------------------

---

<b>CHAPTER 1</b>	<b>New and Changed Information</b> 1
	New and Changed Information 1

---

<b>CHAPTER 2</b>	<b>About Cisco Cloud APIC</b> 3
	Overview 3
	Guidelines and Limitations 4
	About the Cisco Cloud APIC GUI 4
	Understanding the Cisco Cloud APIC GUI Icons 4

---

<b>CHAPTER 3</b>	<b>About Cisco Cloud APIC and Google Cloud</b> 9
	Summary of Changes in Release 25.0(1) 9
	Locating Important Google Cloud Project Information 9
	Understanding Google Cloud Deployments with Cisco Cloud APIC 10
	External Network Connectivity Using Cloud Native Routers 12
	Configuring Routing and Security Policies Separately 16
	Configuring Routing Policies 16
	Configuring Security Policies 17
	Understanding VPCs and Subnets Under Google Cloud and Cloud Context Profiles Under Cloud APIC 20
	Guidelines and Limitations For Configuring Cisco Cloud APIC with Google Cloud 24

---

<b>CHAPTER 4</b>	<b>Cisco Cloud APIC Policy Model</b> 27
	About the ACI Policy Model 27
	Policy Model Key Characteristics 27

Logical Constructs	28
The Cisco ACI Policy Management Information Model	29
Tenants	30
Cloud Context Profile	31
VRFs	31
Cloud Application Profiles	32
Cloud Endpoint Groups	33
Contracts	34
Filters and Subjects Govern Cloud EPG Communications	35
About the Cloud Template	36
Managed Object Relations and Policy Resolution	38
Default Policies	39

---

**CHAPTER 5**

<b>Configuring Cisco Cloud APIC Components</b>	<b>41</b>
About Configuring the Cisco Cloud APIC	41
Configuring the Cisco Cloud APIC Using the GUI	41
Creating a Tenant	41
Setting Up the Google Cloud Project for a User Tenant	41
Creating a Managed Tenant	43
Creating an Unmanaged Tenant	46
Creating an Application Profile Using the Cisco Cloud APIC GUI	49
Creating a VRF Using the Cisco Cloud APIC GUI	49
Creating an External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI	51
Configuring Inter-VRF Route Leaking Using the Cisco Cloud APIC GUI	54
Enabling Connectivity Between Google Cloud and External Devices	56
Downloading the External Device Configuration Files	56
Enabling Connectivity Between Google Cloud and the External Devices	56
Creating an EPG Using the Cisco Cloud APIC GUI	60
Creating an Application EPG Using the Cisco Cloud APIC GUI	60
Creating an External EPG Using the Cisco Cloud APIC GUI	64
Creating a Filter Using the Cisco Cloud APIC GUI	67
Creating a Contract Using the Cisco Cloud APIC GUI	68
Creating an Inter-Tenant Contract Using the Cisco Cloud APIC GUI	70
Specifying Consumer and Provider EPGs Using the Cisco Cloud APIC	73

Creating a Cloud Context Profile Using the Cisco Cloud APIC GUI	74
Configuring Virtual Machines in Google Cloud	76
Creating a Backup Configuration Using the Cisco Cloud APIC GUI	78
Creating a Tech Support Policy Using the Cisco Cloud APIC GUI	80
Creating a Scheduler Using the Cisco Cloud APIC GUI	81
Creating a Remote Location Using the Cisco Cloud APIC GUI	83
Creating a Login Domain Using the Cisco Cloud APIC GUI	84
Creating a Security Domain Using the Cisco Cloud APIC GUI	87
Creating a Role Using the Cisco Cloud APIC GUI	87
Creating a Certificate Authority Using the Cisco Cloud APIC GUI	90
Creating a Key Ring Using the Cisco Cloud APIC GUI	91
Creating a Local User Using the Cisco Cloud APIC GUI	93
Managing Regions (Configuring a Cloud Template) Using the Cisco Cloud APIC GUI	95
Configuring Cisco Cloud APIC Using the REST API	97
Creating a Tenant Using the REST API	97
Configuring Inter-VRF Route Leaking Using the REST API	98
Creating a Filter Using the REST API	100
Creating a Contract Using the REST API	100
Creating a Cloud Context Profile Using the REST API	101
Creating an Application Profile Using the REST API	102
Creating an EPG Using the REST API	103
Creating a Cloud EPG Using the REST API	103
Creating an External Cloud EPG Using the REST API	104
Creating Cloud Routers, External Networks, and External VRFs Using the REST API	105

---

**CHAPTER 6**
**Viewing System Details 107**

Monitoring VM Host Metrics	107
Monitoring VM Host Metrics Using the GUI	107
Monitoring VM Host Metrics Using the REST API	109
Viewing Application Management Details	110
Viewing Cloud Resource Details	111
Viewing Operations Details	112
Viewing Infrastructure Details	114
Viewing Administrative Details	114

Viewing Health Details Using the Cisco Cloud APIC GUI 116

---

**CHAPTER 7****Cisco Cloud APIC Statistics 119**

About Google Cloud Statistics 119

Guidelines and Limitations For Configuring Google Cloud Statistics 120

Enabling Flow Log Statistics 120

Viewing Flow Log Statistics 121

Enabling VPC Flow Log Statistics Using the REST API 123

---

**CHAPTER 8****Cisco Cloud APIC Security 125**

Access, Authentication, and Accounting 125

Configuration 125

Configuring TACACS+, RADIUS, LDAP and SAML Access 126

Overview 126

Configuring Cloud APIC for TACACS+ Access 126

Configuring Cloud APIC for RADIUS Access 127

Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the Cloud APIC 128

Configuring LDAP Access 129

Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair 129

Configuring Cloud APIC for LDAP Access 129

Configuring Cloud APIC for SAML Access 131

About SAML 131

Configuring Cloud APIC for SAML Access 132

Setting Up a SAML Application in Okta 133

Setting Up a Relying Party Trust in AD FS 134

Configuring HTTPS Access 134

About HTTPS Access 134

Guidelines for Configuring Custom Certificates 134

Configuring a Custom Certificate for Cisco Cloud APIC HTTPS Access Using the GUI 135





# CHAPTER 1

## New and Changed Information

This chapter contains the following sections:

- [New and Changed Information, on page 1](#)

## New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

*Table 1: New Features and Changed Behavior in Cisco Cloud APIC for Release 25.0(4)*

Feature or Change	Description	Where Documented
Support for flow log statistics	Beginning in Cisco Cloud APIC Release 25.0(4), you can view statistics that are derived by processing Google Cloud flow logs. Available statistics include ingress and egress bytes and packets for VPCs, regions, and endpoints.	<a href="#">Cisco Cloud APIC Statistics, on page 119</a>

*Table 2: New Features and Changed Behavior in Cisco Cloud APIC for Release 25.0(3)*

Feature or Change	Description	Where Documented
Move from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V	Cisco Cloud APIC moves from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V beginning with release 25.0(3).	

Feature or Change	Description	Where Documented
Terms used for Cisco Cloud Services Router 1000v and Cisco Catalyst 8000V	<p>The following terms are used for the two types of routers described above:</p> <ul style="list-style-type: none"> <li>• <b>CSR</b>: Short for Cloud Services Router. Refers to the Cisco Cloud Services Router 1000v, used in releases prior to release 25.0(3).</li> <li>• <b>CCR</b>: Short for Cisco Cloud Router. Refers to the Cisco Catalyst 8000V, used in release 25.0(3) and later.</li> </ul> <p>In addition, throughout this document, <b>CCR</b> is used as a generic term for either of the routers described above, depending on your release.</p>	

**Table 3: New Features and Changed Behavior in Cisco APIC for Cisco APIC Release 25.0(1)**

Feature or Change	Description	Where Documented
Change in release numbering for Cisco Cloud APIC	<p>Beginning with release 25.0(1), the release numbering has changed for Cisco Cloud APIC. The sequential order of releases for Cisco Cloud APIC is as follows:</p> <ul style="list-style-type: none"> <li>• 4.1(x) (support for AWS only)</li> <li>• 4.2(x)</li> <li>• 5.0(x)</li> <li>• 5.1(x)</li> <li>• 5.2(x)</li> <li>• 25.0(x) (this release)</li> </ul>	
Support for Google Cloud with Cisco Cloud APIC	Beginning with release 25.0(1), support is now available for Google Cloud with Cisco Cloud APIC.	
Support for Prometheus Node Exporter on Cisco Cloud APIC	The Prometheus Node Exporter is supported on Cisco Cloud APIC beginning with release 25.0(1).	<a href="#">Monitoring VM Host Metrics, on page 107</a>



## CHAPTER 2

# About Cisco Cloud APIC

---

- [Overview, on page 3](#)
- [Guidelines and Limitations, on page 4](#)
- [About the Cisco Cloud APIC GUI, on page 4](#)

## Overview

Cisco Application Centric Infrastructure (ACI) customers who own a private cloud sometimes may run part of their workload on a public cloud. However, migrating the workload to the public cloud requires working with a different interface and learning different ways to set up connectivity and define security policies. Meeting these challenges can result in increased operational cost and loss of consistency.

Beginning in Cisco Application Policy Infrastructure Controller (APIC) Release 4.1(1), Cisco ACI can use Cisco Cloud APIC to extend a Cisco ACI fabric to certain public clouds.

Cisco Cloud APIC is supported on the following cloud computing platforms:

- Release 4.1(1): Support for Amazon Web Services (AWS)
- Release 4.2(1): Support for Microsoft Azure
- Release 25.0(1): Support for Google Cloud

### What Cisco Cloud APIC Is

Cisco Cloud APIC is a software component of Cisco APIC that can be deployed on a cloud-based virtual machine (VM). Cisco Cloud APIC provides the following features:

- Provides an interface that is similar to the existing Cisco APIC to interact with the Google Cloud public cloud.
- Automates the deployment and configuration of cloud connectivity.
- Configures the cloud router control plane.
- Translates Cisco ACI policies to cloud native policies.
- Discovers endpoints.

## Guidelines and Limitations

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

- 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.

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, Topology, Cloud Resources, Application Management, and Event Analytics tabs appear.
3. Click the **Cloud Resources > Actions > View Stale Cloud Objects**. The **Stale Cloud Objects** dialog box appears.

## 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 **EPGs** 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.

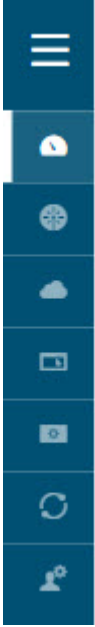
For more information about the GUI icons, see [Understanding the Cisco Cloud APIC GUI Icons, on page 4](#)

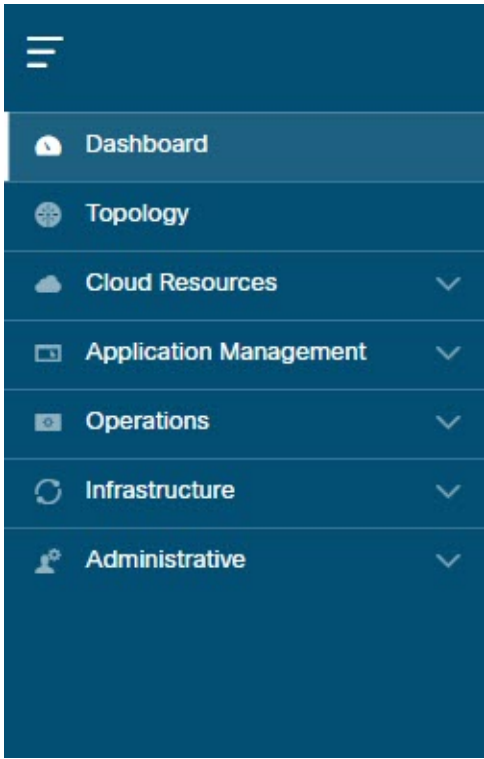


For more information about configuring Cisco Cloud APIC components, see [Configuring Cisco Cloud APIC Components, on page 41](#)







## 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 4: Cisco Cloud APIC GUI Icons

Icon	Description
<p data-bbox="139 342 467 369"><i>Figure 1: Navigation Pane (Collapsed)</i></p> 	<p data-bbox="807 342 1523 562">The left side of the GUI contains the <b>Navigation</b> 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 <b>Navigation</b> pane locks in the open position. To collapse it, click the menu icon again. When you expand the <b>Navigation</b> pane by hovering the mouse icon over the menu icon, you collapse the <b>Navigation</b> pane by moving the mouse icon away from it.</p> <p data-bbox="807 583 1523 674">When expanded, the <b>Navigation</b> 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 data-bbox="100 289 428 315"><b>Figure 2: Navigation Pane (Expanded)</b></p> 	<p data-bbox="771 289 1484 352">The Cisco Cloud APIC component windows are organized in the <b>Navigation</b> pane as follows:</p> <ul data-bbox="808 373 1484 1031" style="list-style-type: none"> <li>• <b>Dashboard</b> Tab—Displays summary information about the Cisco Cloud APIC components.</li> <li>• <b>Topology</b> Tab—Displays topology information about the Cisco Cloud APIC.</li> <li>• <b>Cloud Resources</b> Tab—Displays information about regions, VPCs, routers, endpoints, and instances.</li> <li>• <b>Application Management</b> Tab—Displays information about tenants, application profiles, EPGs, contracts, filters, VRFs, cloud context profiles, and external networks.</li> <li>• <b>Operations</b> Tab—Displays information about event analytics, active sessions, backup &amp; restore policies, tech support policies, firmware management, schedulers, and remote locations.</li> <li>• <b>Infrastructure</b> Tab—Displays information about the system configuration and external connectivity.</li> <li>• <b>Administrative</b> Tab—Displays information about authentication, security, local and remote users, and smart licensing.</li> </ul> <p data-bbox="771 1062 1484 1125"><b>Note</b> For more information about the contents of these tabs, see <a href="#">Viewing System Details, on page 107</a></p>
<p data-bbox="100 1165 380 1190"><b>Figure 3: Search Menu-Bar Icon</b></p> 	<p data-bbox="771 1165 1484 1260">The <b>search</b> menu-bar icon displays the search field, which enables you to search for any object by name or any other distinctive fields.</p>
<p data-bbox="100 1369 367 1394"><b>Figure 4: Intent Menu-Bar Icon</b></p> 	<p data-bbox="771 1369 1484 1432">The <b>Intent</b> icon appears in the menu bar between the <b>search</b> and the <b>feedback</b> icons.</p> <p data-bbox="771 1453 1484 1610">When clicked, the <b>Intent</b> dialog appears (see below). The <b>Intent</b> 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 <b>Intent</b> icon. Close the dialog box to access the <b>Intent</b> icon again.</p> <p data-bbox="771 1631 1484 1694">For more information about creating a component, see <a href="#">Configuring Cisco Cloud APIC Components, on page 41</a>.</p>

Icon	Description
<p><b>Figure 5: Intent Dialog Box</b></p> 	<p>The <b>Intent</b> (What do you want to do?) 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>
<p><b>Figure 6: Feedback Icon</b></p> 	<p>The <b>feedback</b> icon appears in the menu bar between the <b>Intent</b> and the <b>bookmark</b> icons.</p> <p>When clicked, the <b>feedback</b> panel appears.</p>
<p><b>Figure 7: Bookmark Icon</b></p> 	<p>The <b>bookmark</b> icon appears in the menu bar between the <b>feedback</b> and the <b>system tools</b> icons.</p> <p>When clicked, the current page is bookmarked on your system.</p>
<p><b>Figure 8: System Tools Menu-Bar Icon</b></p> 	<p>The <b>system tools</b> menu-bar icon provides the following options:</p> <ul style="list-style-type: none"> <li>• <b>Open Object Store Browser</b>—Opens 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.</li> <li>• <b>Model Documentation</b>—Open the <b>Cloud APIC Object Model Documentation</b> window.</li> </ul>
<p><b>Figure 9: Help Menu-Bar Icon</b></p> 	<p>The <b>help</b> menu-bar icon shows the <b>About Cloud APIC</b> menu option, which provides the version information for the Cloud APIC. The <b>help</b> menu-bar icon also shows the <b>Help Center</b> and <b>Welcome Screen</b> menu options.</p>
<p><b>Figure 10: User Profile Menu-Bar Icon</b></p> 	<p>The <b>user profile</b> menu-bar icon provides the following options:</p> <p>"User Preferences" which is setting for time format Local/UTC.</p> <ul style="list-style-type: none"> <li>• <b>User Preferences</b>—Allows you to set the time format (Local or UTC) and enable or disable the Welcome Screen at login.</li> <li>• <b>Change Password</b>—Enables you to change the password.</li> <li>• <b>Change SSH Key</b>—Enables you to change the SSH key.</li> <li>• <b>Change User Certificate</b>—Enables you to change the user certificate.</li> <li>• <b>Logout</b>—Enables you to log out of the GUI.</li> </ul>







## CHAPTER 3

# About Cisco Cloud APIC and Google Cloud

---

Beginning with release 25.0(1), support is now available for Google Cloud with Cisco Cloud APIC. The following topics in this chapter provide information on how Cisco Cloud APIC deployments work with Google Cloud.

- [Summary of Changes in Release 25.0\(1\), on page 9](#)
- [Locating Important Google Cloud Project Information, on page 9](#)
- [Understanding Google Cloud Deployments with Cisco Cloud APIC, on page 10](#)
- [External Network Connectivity Using Cloud Native Routers, on page 12](#)
- [Configuring Routing and Security Policies Separately, on page 16](#)
- [Understanding VPCs and Subnets Under Google Cloud and Cloud Context Profiles Under Cloud APIC, on page 20](#)
- [Guidelines and Limitations For Configuring Cisco Cloud APIC with Google Cloud, on page 24](#)

## Summary of Changes in Release 25.0(1)

Following is a summary of changes that are part of release 25.0(1):

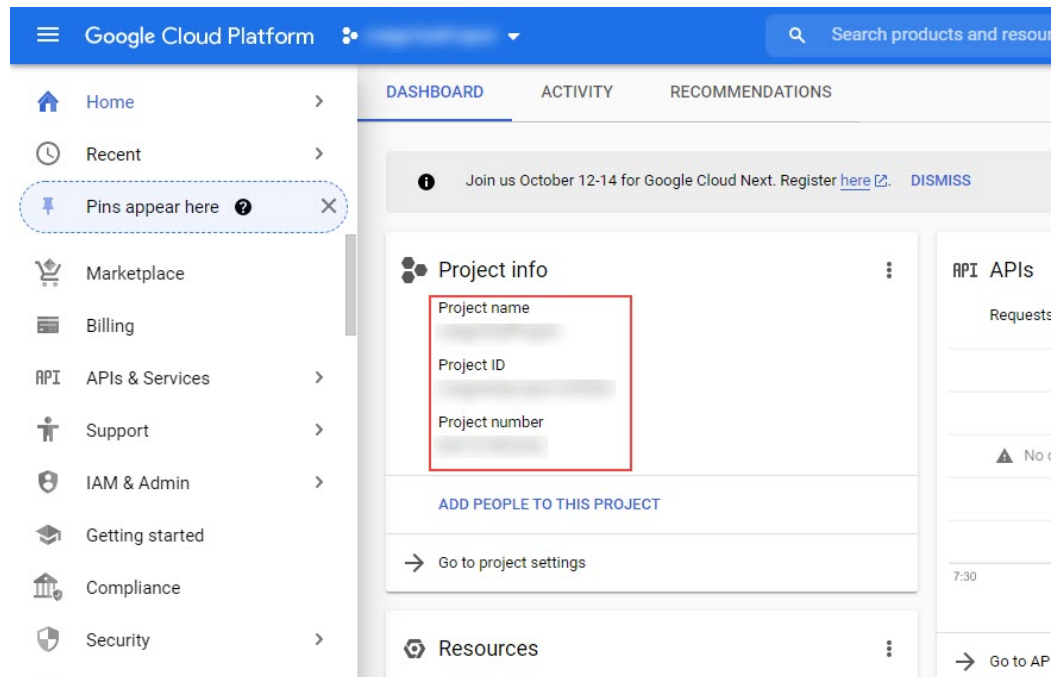
- Support for Google Cloud with Cisco Cloud APIC.
- Support is available for external connectivity from Google Cloud to other external sites. See [External Network Connectivity Using Cloud Native Routers, on page 12](#) for more information.
- Support for configuring routing and security policies separately. See [Configuring Routing and Security Policies Separately, on page 16](#) for more information.
  - Cisco Cloud APIC supports using route maps to configure routing policies independent of security policies between a pair of VRFs, where both VRFs are internal VRFs or one VRF is an internal and the other VRF is an external VRF. See [Configuring Routing Policies, on page 16](#) for more information.
  - Support for configuring security policies using firewall rules. See [Configuring Security Policies, on page 17](#) for more information.

## Locating Important Google Cloud Project Information

After you create a Google Cloud project, that project will be assigned three unique identifiers:

- Project name
- Project ID
- Project number

You will need these three identifiers for your Google Cloud project at various points in the Cisco Cloud APIC configuration process. To locate the **Project Info** pane with these Google Cloud project identifiers, log into your Google Cloud account and select your particular Google Cloud project in the **Select a project** window. The **Dashboard** for this project is displayed, which provides the Project Info pane with these three unique identifiers for your Google Cloud project.



## Understanding Google Cloud Deployments with Cisco Cloud APIC

Google Cloud organizes resources in a way that resembles a file system, where:

- The *Organization* at the top level can have multiple *Folders*.
- Every *Folder* can contain other *Folders*, or can contain *Projects*, where every *Project* has a unique ID.
- Cloud *resources* (such as VMs, VPCs, and subnets) are contained within a *Project*.

While the Organization and Folder levels are useful areas to understand from the Google Cloud perspective, the Project level is the most relevant from the Cisco Cloud APIC perspective.

Each Cisco Cloud APIC tenant is mapped one-to-one to a Google Cloud Project, which means that:

- A Cisco Cloud APIC tenant cannot span multiple Google Cloud Projects

- There cannot be more than one Cisco Cloud APIC tenant in a Google Cloud Project

With Cisco Cloud APIC, Google Cloud provides access to Projects using **Service Accounts**. These accounts are meant for applications that need to access Google Cloud services. They can be used to run and deploy Cisco Cloud APIC and to push policies for other tenants. Service accounts used in applications running within Google Cloud do not need credentials, whereas applications that are run external to Google Cloud need a pre-generated private key. Service Accounts reside in one Google Cloud Project, but they can also be given access to manage policies for other Projects (for Cisco Cloud APIC, other tenants).

The following sections provide more information on different ways that Cisco Cloud APIC tenants can be configured with Google Cloud:

- [User Tenants With Managed Credentials, on page 11](#)
- [User Tenants With Unmanaged Credentials, on page 11](#)

### User Tenants With Managed Credentials

This type of user tenant has the following characteristics:

- This tenant account is managed by the Cisco Cloud APIC.
- You will first choose **Managed Identity** in the Cisco Cloud APIC GUI as part of the tenant configuration process for this type of user tenant.
- After you have configured the necessary parameters in the Cisco Cloud APIC, you must then set the necessary roles for this tenant in Google Cloud. Add the service account created by the Cloud APIC as an IAM user with the following rules:
  - Cloud Functions Service Agent
  - Compute Instance Admin (v1)
  - Compute Network Admin
  - Compute Security Admin
  - Logging Admin
  - Pub/Sub Admin
  - Storage Admin

For instructions on creating this sort of tenant, see [Creating a Managed Tenant Using the Cisco Cloud APIC GUI, on page 43](#).

### User Tenants With Unmanaged Credentials

This type of user tenant has the following characteristics:

- This tenant account is not managed by the Cisco Cloud APIC.
- Before configuring the necessary parameters in the Cisco Cloud APIC for this type of tenant, you must first download the JSON file that contains the necessary private key information from Google Cloud for the service account associated with this tenant.

- You will then choose **Unmanaged Identity** in the Cisco Cloud APIC GUI as part of the tenant configuration process for this type of user tenant. As part of the configuration process for this type of tenant in Cisco Cloud APIC, you will provide the following information from the downloaded JSON file:
  - Key ID
  - RSA Private Key
  - Client ID
  - Email

For instructions on creating this sort of tenant, see [Creating an Unmanaged Tenant Using the Cisco Cloud APIC GUI, on page 47](#).

## External Network Connectivity Using Cloud Native Routers

Support is available for external connectivity between a Google Cloud site and non-Google Cloud sites or an external device. You can have this IPv4 connection by creating a VPN connection between a Google Cloud router and an external device.

The following sections provide more information on the components that allow for the new external network connectivity provided in release 25.0(1):

- [External VRF, on page 12](#)
- [Cloud Native Routers, on page 12](#)
- [VPN Communication, on page 13](#)
- [Hub Network Configuration, on page 13](#)

### External VRF

An **external VRF** is a unique VRF that does not have any presence in the cloud. This VRF is not referred to in any cloud context profile used by Cisco Cloud APIC.

An external VRF represents an external network that is connected to other cloud sites or to on-premises sites. Multiple cloud VRFs can leak routes to an external VRF or can get the routes from an external VRF. When an external network is created on an external VRF, inter-VRF routing is set up so that routes received and advertised on the external network are received or advertised on the external VRF.

### Cloud Native Routers

When configuring Cisco Cloud APIC with Google Cloud, the infra VPC uses Google Cloud native routers (Cloud Router and Cloud VPN gateway) to create IPsec tunnels and BGP sessions to on-premises sites, other cloud sites, or any remote device. Only IPv4 connectivity is supported for this type of connectivity using cloud native routers, where IPv4 sessions are created on an external VRF.

Google Cloud supports VPN connections both with static routes and with BGP. To create a VPN connection with BGP, Cisco Cloud APIC needs both a Cloud Router and a VPN gateway. A VPC can have multiple Cloud Routers and VPN gateways. However, Google Cloud has a restriction that both the Cloud Routers and

the VPN gateways must be in the same region and in the same VPC. In addition, Cisco Cloud APIC has a restriction where only one cloud router and one cloud VPN gateway is supported per region.

### VPN Communication

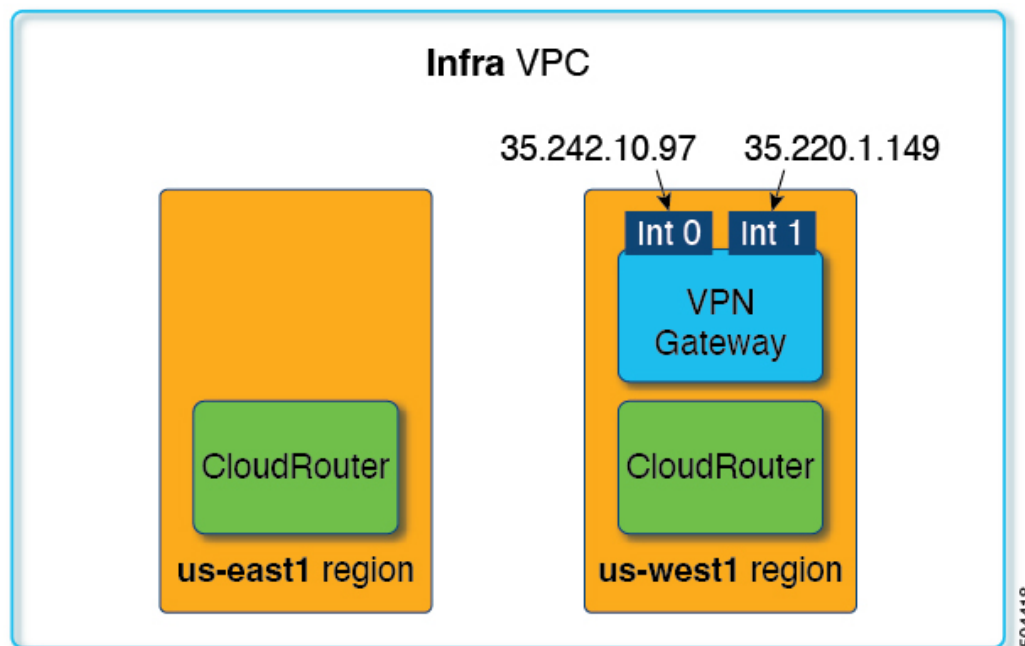
When configuring Cisco Cloud APIC with Google Cloud, the infra VPC is used to host the Cisco Cloud APIC and to host the VPN connections to external devices and sites. However, the infra VPC is not used as a transit to implement spoke-to-spoke communication. Instead, when configuring Cisco Cloud APIC with Google Cloud, spoke-to-spoke communication is done through spoke-to-spoke VPC peering.

The infra VPC uses the Google Cloud Router and Google Cloud VPN Gateway to create IPsec tunnels and BGP sessions to on-premises sites or to other cloud sites. Spoke VPCs peer with the infra VPC to share the VPN connections to external sites, where:

- Routes received on the VPN connections are leaked to the spoke VPCs
- Spoke VPC routes are advertised on the VPN connections

Using inter-VRF routing, the route is leaked between the external VRF of the VPN connections and the cloud local spoke VRFs.

A VPN gateway has two interfaces, and Google Cloud allocates public IP addresses to each of the interfaces. While the Google Cloud VPN gateway could have one or two interfaces, Cisco Cloud APIC only supports VPN gateways with two interfaces because two interfaces are required to achieve high availability.



### Hub Network Configuration

Starting with release 25.0(1), rather than creating the hub network in a region based on the spoke attachments, the `cloudRegionName` MOs under a `cloudtemplateHubNetworkName` represents the regions where the hub network will be deployed, where `cloudtemplateHubNetworkName` represents a Google Cloud Router. For release 25.0(1), Cisco Cloud APIC has a restriction of only one `cloudtemplateHubNetworkName`.

The hub network provides a way for establishing connectivity to an external site. Creating a hub network is a pre-requisite to creating an external network. Starting with release 25.0(1), you can create a hub network by specifying a name for the hub and the regions where the hub network should be deployed. For example, you may choose to deploy the hub network in us-central1 and us-east1. Cisco Cloud APIC will provision the Google Cloud Routers in these regions. Remember that only one hub network can be created, which means that Cisco Cloud APIC will only deploy one Cloud Router per region.

The following POST shows an example of network connectivity beginning with release 25.0(1) using this model. The `cloudtemplateHubNetwork` is used to create the hub network. In this example, the hub network is deployed in four regions. External networks are created from each of the four regions using the `cloudtemplateExtNetwork` MOs.

```
<polUni>
  <fvTenant name="infra" status="">
    <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
    <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
    <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1"
hostRouterMode="manual" status="">
      <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24" poolname="pool1"
/>
      <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24" poolname="pool2"
/>
      <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24"
poolname="pool3" />

    <cloudtemplateHubNetwork name="default" status="" >
      <cloudtemplateHubNetworkName name="fool" asn="64514" status="">
        <cloudRegionName provider="gcp" region="us-west4" status="" />
        <cloudRegionName provider="gcp" region="us-west2" status="" />
        <cloudRegionName provider="gcp" region="us-east1" status="" />
        <cloudRegionName provider="gcp" region="us-west1" status="" />
      </cloudtemplateHubNetworkName>
    </cloudtemplateHubNetwork>

    <cloudtemplateIntNetwork name="default">
      <cloudRegionName provider="gcp" region="us-west1">
        <cloudtemplateVpnRouter name="default" status=""/>
      </cloudRegionName>
      <cloudRegionName provider="gcp" region="us-west2">
        <cloudtemplateVpnRouter name="default" status=""/>
      </cloudRegionName>
      <cloudRegionName provider="gcp" region="us-east1">
        <cloudtemplateVpnRouter name="default" status=""/>
      </cloudRegionName>
      <cloudRegionName provider="gcp" region="us-west4">
        <cloudtemplateVpnRouter name="default" status=""/>
      </cloudRegionName>
    </cloudtemplateIntNetwork>

    <cloudtemplateExtNetwork name="default">
      </cloudtemplateExtNetwork>
      <cloudtemplateExtNetwork name="extnwfool" vrfName="extv1" hubNetworkName="fool"
vpnRouterName="default" status="">
        <cloudRegionName provider="gcp" region="us-west1" status=""/>
        <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">

          <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd"
poolname="pool1" status="">
            <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
          </cloudtemplateIpSecTunnel>
        </cloudtemplateVpnNetwork>
      </cloudtemplateExtNetwork>
    </cloudtemplateExtNetwork>
  </fvTenant>
</polUni>
```

```

        </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
</cloudtemplateExtNetwork>
<cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
vpnRouterName="default" status="">
    <cloudRegionName provider="gcp" region="us-west2" status=""/>
    <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
        <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
poolname="pool2" status="">
            <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
        </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
</cloudtemplateExtNetwork>
<cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3" hubNetworkName="foo1"
vpnRouterName="default" status="">
    <cloudRegionName provider="gcp" region="us-east1" status=""/>
    <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
        <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
poolname="pool3" status="">
            <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
        </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
</cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
</fvTenant>
</polUni>

```

In this example POST:

- **cloudtemplateExtNetwork:** You can have multiple `cloudtemplateExtNetwork` entries, each with a unique name, that represent an external network on an external VRF.

Within the `cloudtemplateExtNetwork` area are the following fields:

- **vrfName:** This property represents the VRF used for the external network (for example, a transport VRF). Multiple remote sites can use the same transport VRF, which means that all of these remote sites are treated as one VRF on the cloud and all of the remote sites receive the same routes from the cloud.
- **hubNetworkName:** This property represents the name of the hub network used by this external network. This name refers to one of the hub networks created in the `cloudtemplateHubNetworkName` area.
- **vpnRouterName:** This property represents the name of the VPN router used by this external network. This name refers to the VPN router created by `cloudtemplateVpnRouter`.

In addition, an external network can be deployed in multiple regions, and a router used on the external network should be deployed in those regions (in other words, `hubNetworkName` and `vpnRouterName` should exist in those regions).

- **cloudtemplateVpnNetwork:** This MO represents a remote site.

Within the `cloudtemplateVpnNetwork` area is the `remoteSiteId` field. This property represents the remote site ID.

- **cloudtemplateVpnRouter:** This MO translates to a Google Cloud VPN gateway. For release 25.0(1), only one `cloudtemplateVpnRouter` is allowed, with the name `default`.
- **cloudtemplateIpSecTunnel:** This MO represents a remote peer.

- `cloudtemplateBgpIpv4`: This MO represents a remote site IPv4 BGP peer.

If the `peeraddr` entry under `cloudtemplateBgpIpv4` has the default address (0.0.0.0/0), then the remote BGP peer is assumed to be the inner address of the tunnel on the remote device.

Note that the model above supports the following:

- Both `ikev1` and `ikev2` to an external device.
- Multiple `cloudtemplateIpSecTunnelSubnetPool` subnet pools. The allowed IP ranges in the `cloudtemplateIpSecTunnelSubnetPool` subnet pools is dependent on the cloud provider and use case. For example, 169.254.0.0/16 or a lesser subnet of it is supported for Google Cloud VPN connections.

## Configuring Routing and Security Policies Separately

To allow communication between two endpoints in different VRFs, you need to establish routing and security policies separately:

- **Routing policies:** Policies used to define routes to establish traffic flow
- **Security policies:** Rules used for security purposes, such as zoning rules, security-group rules, ACLs, and so on

For Google Cloud, routing must be configured independent of security. In other words, for Google Cloud, "contracts" are used only for security. To configure routing, you must configure route-maps.

## Configuring Routing Policies

Using inter-VRF routing, you can configure an independent routing policy to specify which routes to leak between a pair of VRFs. To establish routing, you must configure route maps between a pair of VRFs.

For situations where you can use route maps to set which routes to leak between a pair of VRFs, the following types of VRFs are used for inter-VRF routing:

- **External VRF** is a VRF that is associated with one or more external networks.
- **Internal VRF** is a VRF that has one or more cloud context profiles or cloud subnets associated with it.

When configuring inter-VRF routing with these types of VRFs:

- Between a pair of internal VRFs, you must always leak all routes.
- From an internal VRF to an external VRF, you can leak specific routes or all routes.
- From an external VRF to an internal VRF, you must leak all routes.

### Guidelines and Restrictions

The following guidelines apply when using inter-VRF routing to leak routes between a pair of VRFs using route maps:

- Routes are always leaked bi-directionally between two VRFs. For every route leak entry from one tenant/VRF under another tenant/VRF, there must be a corresponding route leak entry going in the opposite direction.



For example, assume there are two tenants ( $t_1$  and  $t_2$ ) and two corresponding VRFs ( $v_1$  and  $v_2$ ). For every route leak entry  $t_1:v_1$  under the VRF  $t_2:v_2$ , there must be a corresponding route leak entry  $t_2:v_2$  under the VRF  $t_1:v_1$ .

- Once you associate an external VRF with an external network, if you want to change the external VRF, you need to delete the external network and then recreate the external network with the new external VRF.
- You cannot configure "smaller" prefixes to be leaked while a "larger" prefix is already being leaked. For example, configuring the 10.10.10.0/24 prefix will be rejected if you already have the 10.10.0.0/16 prefix configured to be leaked. Similarly, if you configure the 0.0.0.0/0 (leak all) prefix, no other prefix will be allowed to be configured.

## Configuring Security Policies

While an EPG in Cisco Cloud APIC corresponds to security groups in AWS and Azure, there is no equivalent corresponding component in Google Cloud for an EPG. The closest equivalent in Google Cloud is a combination of firewall rules and network tags.

The firewall resource in Google Cloud is global to the project (tenant). Firewall rules are associated with a single VPC and their scope applies to the entire VPC globally. The scope of the firewall rule is further defined by the Target parameter. In other words, the set of instances that a rule is applied to can be selected by one or more of the following Target types:

- **Network tags:** Network tags are key strings that drive the VM's firewall and routing configuration on Google Cloud. Instances (for example, VMs) can be tagged with unique strings. Firewall rules are applied to all instances with equal tags. Multiple tag values act as a logical 'or' operator, where the firewall rule is applied as long as at least one tag matches.
- **All instances in the network:** The firewall rule applies to all instances in the VPC.

Firewall rules also identify the source and destination of the traffic. Depending on whether the rule is for ingress traffic (going to a VM) or egress traffic (leaving a VM), the source and destination fields accept different values. The following list provides more information on those values:

- **Ingress rules:**
  - **Source:** Can be identified using:
    - Network tags
    - IP addresses
    - A combination of IP addresses and network tags with a logical 'or' operator
  - **Destination:** The Target parameter identifies the destination instances
- **Egress rules:**
  - **Source:** The Target parameter identifies the source instances
  - **Destination:** Can be identified using only IP addresses (not network tags)

## How Cisco Cloud APIC Implements Firewall Rules With Google Cloud

The following list describes how Cisco Cloud APIC implements firewall rules with Google Cloud :

- **Global resources:** VPCs and firewalls in Google Cloud are global resources, so Cisco Cloud APIC does not have to program firewall rules for endpoints that span multiple regions. The same firewall rules apply for any region where the endpoint resides.
- **Firewall egress rules and network tags:** Firewall egress rules do not support network tags as a destination field, so you must list individual IP addresses for endpoints.
- **Source tags in firewall ingress rules and alias IP ranges:** Firewall ingress rules do not include the alias IP ranges of VMs matching the network tags used in the source field.
- **Priority fields in firewall rules:** Google Cloud evaluates firewall rules following their priority values.

Given that Google Cloud firewall rules follow a priority list, Cisco Cloud APIC configures a pair of low-priority deny-all ingress and egress rules when the VPC is created. Afterwards, Cisco Cloud APIC configures rules that open traffic according to the EPG's contracts with higher priority. Therefore, if there is no explicit rule that allows certain traffic as a result of an EPG contract, the low-priority rule matches and the default behavior is deny-all.

## Endpoints and Endpoint Selectors

On the Cisco Cloud APIC, a cloud EPG is a collection of endpoints that share the same security policy. Cloud EPGs can have endpoints in one or more subnets and are tied to a VRF.

The Cisco Cloud APIC has a feature called endpoint selector, which is used to assign an endpoint to a Cloud EPG. The endpoint selector is essentially a set of rules run against the cloud instances assigned to the Google Cloud VPC managed by Cisco ACI. Any endpoint selector rules that match endpoint instances will assign that endpoint to the Cloud EPG. The endpoint selector is similar to the attribute-based microsegmentation available in Cisco ACI.

Following are the types of endpoint selectors available for the two types of cloud EPGs:

- **Application EPGs:**
  - **IP:** Used to select by the IP address or subnet.
  - **Region:** Used to select by the region of the endpoint.
  - **Custom:** Used to select by a custom tag or label. For example, if you added a Location tag in Google Cloud, you might create the custom tag Location in this field to match the Location tag that you added in Google Cloud earlier.
- **External EPGs:**
  - **Subnet:** The subnet selector is a type of endpoint selector where the match expression uses the IP address of a subnet, so an entire subnet is assigned as being part of the EPG. Essentially, when you use the subnet selector as the endpoint selector, all of the endpoints within that subnet belongs to the associated EPG.

When using Cisco Cloud APIC endpoint selectors with Google Cloud, a network tag is applied that associates the EPG to the matching VM in Google Cloud. Once the network tag is configured in the VM, Google Cloud applies the firewall rules for the VM's traffic.

VMs on Google Cloud also support labels. Labels are key-value pairs that are meant to be an organizational tool. The custom endpoint selector in Cisco Cloud APIC recognizes the labels assigned to the VMs in Google Cloud.

Cisco Cloud APIC reserves a unique network tag string for each EPG. In Google Cloud, this value is used as the target field in the firewall rules created for the EPG. When a new VM matches an endpoint selector of the EPG, Cisco Cloud APIC appends this value to the existing VM's network tags. In addition, the EPG's network tag is used in the source field of the Google Cloud firewall rules.

For example, consider the sample configuration below:

```
<cloudEPg name="epg1" >
  <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
  <fvRsProv tnVzBrCPName="httpSSHFamily"/>
  <cloudEPSelector name="web-selector" matchExpression="custom:server=='web'"/>
  <cloudEPSelector name="web-selector" matchExpression="custom:server==backend"/>
</cloudEPg>
<cloudEPg name="epg2" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
  <fvRsCons tnVzBrCPName="httpSSHFamily"/>
  <cloudEPSelector name="database-selector" matchExpression="custom:server=='database'"/>
</cloudEPg>
```

Assuming there are three endpoints in the VPC with the following configuration, Cisco Cloud APIC configures the following network tags, where the Cisco Cloud APIC-configured network tags are in the following format:

capic-*<app-profile-name>*-*<epg-name>*

Endpoint	Application Profile	EPG	Primary IP	Labels	Cloud APIC-Configured Network Tags
EP1	First application profile (app01)	First EPG (epg01)	10.0.0.1	server:web	capic-app01-epg01
EP2	Second application profile (app02)	Second EPG (epg02)	20.0.0.1	server:backend	capic-app02-epg02
EP3	Second application profile (app02)	Third EPG (epg03)	30.0.0.1	server:database	capic-app02-epg03

Cisco Cloud APIC needs admin permission over the VMs in order to set their network tags. This permission is granted by the *Compute Instance Admin* role.

There might be cases where Cisco Cloud APIC does not have this permission and cannot manage the VM's tags. In those scenarios, you can configure the network tags in your VMs first and then provide the proper endpoint selector configuration to Cisco Cloud APIC later on.

To see firewall rules:

- **In Google Cloud:** In your Google Cloud account, navigate to **VPC Network > Firewall**.
  - If the VM is part of an EPG, you can find the endpoints by expanding a firewall rule and then viewing the multiple entries shown in the **Filters** column, which are the endpoints.
  - Use the entry in the **Type** column to determine if a particular firewall rule is an ingress or an egress firewall rule.

- If the firewall rule is an ingress type, then traffic is being sent to these endpoints.
  - If the firewall rule is an egress type, then these entries show where it can receive the traffic.
- **In Cisco Cloud APIC:** Firewall rules are associated with VPCs, so navigate to **Cloud Resources > VPCs**, then double-click on a VPC to get the detail screen. Then click on the **Cloud Resources** tab; there you will see the ingress and egress rules.

## Understanding VPCs and Subnets Under Google Cloud and Cloud Context Profiles Under Cloud APIC

In Google Cloud, a VPC is a global resource, whereas a subnet is regional and spans every availability zone in the region, but a subnet cannot overlap with other subnets in the same VPC or in peered VPCs.

Each subnet must have exactly one primary CIDR block (IP range) and can have up to 30 secondary CIDR blocks. There can be up to 300 primary and secondary CIDRs in a VPC. The NIC for each VM gets its primary internal IP address from the primary CIDR block, whereas secondary IP ranges can only be used for **alias IP ranges**, which is a Google Cloud organizational tool to assign address pools to containers or applications running inside the VM.

The following provides more information on the associations between Cisco Cloud APIC objects and Google Cloud objects:

- **One-to-one mapping of Google Cloud VPC to Cisco Cloud APIC VRF:** A Google Cloud VPC is deployed for each Cisco Cloud APIC VRF (`fvCtx` object). Cloud context profiles (`cloudCtxProfile` object) define the set of regional subnets to deploy. Every cloud context profile in the same VRF maps to the same VPC.
- **Google Cloud subnets and their secondary IP ranges:** Cisco Cloud APIC deploys a subnet with primary and secondary IP ranges using Cisco Cloud APIC CIDR and subnet objects. The Cisco Cloud APIC subnet object is used to represent an IP range and the Cisco Cloud APIC CIDR's primary property tells whether it is primary or secondary. Secondary Cisco Cloud APIC subnet objects are associated with the corresponding primary one, because only the latter deploys the actual subnet in Google Cloud.

### Understanding VPC Groups

The cloud context profile is used within Cisco Cloud APIC as a mapping tool for a VPC, where one cloud context profile is associated with one VPC. The cloud context profile also contains information on the region association, where the cloud context profile is used to determine which region a VPC gets deployed to.

In Google Cloud, when you want to create a VPC, you might have to create multiple cloud context profiles through Cisco Cloud APIC if you want to deploy subnets in multiple regions. However, VPCs are global in nature with Google Cloud, where a VPC spans all the regions.

Therefore, a property called **VPC group** (`vpcGroup`) is available within the cloud context profile that allows Cisco Cloud APIC to group multiple cloud context profiles together to form one VPC. Multiple cloud context profiles that are associated with each other using the VPC group feature form the VPC construct within Google Cloud, where the VPC group name is shown in Google Cloud.

Since only one Google Cloud VPC is allowed within one Cisco Cloud APIC VRF for release 25.0(1), you must use the same name for the VPC group property for each cloud context profile listed in a VRF. Profiles having the same VPC group name reside in the same VPC.

The scope of this matching mechanism is at the tenant level. The same values can be reused across tenants, but they implicitly define different groups, since they are also part of different Google Cloud Projects.

Cisco Cloud APIC deploys a VPC for each distinct `fvCtx`, `cloudRsToCtx` and `vpcGroup` tuple, as long as there is at least one `cloudSubnet` defined. The cloud context profile becomes a container of regional resources, such as subnets, associated to a VRF, and it no longer maps to a VPC.

The example below defines two context profiles (c1 and c2) inside the same VRF (v1) with one VPC group (`vpc-1`). This configuration deploys one VPC, where the subnets defined in profiles c1 and c2 are deployed in that VPC because they are part of the same VPC group.

```
<fvTenant name="t1">
  <fvCtx name="v1"/>
  <cloudCtxProfile name="c1" vpcGroup="vpc-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
    <cloudRsToCtx tnFvCtxName="v1"/>
    <cloudCidr addr="10.0.0.0/16" primary="yes" >
      <cloudSubnet ip="10.0.1.0/24">
        <cloudRsZoneAttach
          tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  <cloudCtxProfile name="c2" vpcGroup="vpc-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-east1" />
    <cloudRsToCtx tnFvCtxName="v1"/>
    <cloudCidr addr="20.0.0.0/16" primary="yes" >
      <cloudSubnet ip="20.0.1.0/24">
        <cloudRsZoneAttach
          tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
</fvTenant>
```

### Understanding Primary and Secondary Subnets and Subnet Groups

Cisco Cloud APIC deploys every subnet (`cloudSubnet`) in the VPC (which is identified by the tuple `fvCtx`, `cloudRsToCtx`, and `vpcGroup`) in the region that is pointed to by the `cloudRsCtxProfileToRegion` relation.

In Google Cloud, there is no concept of a primary CIDR for the VPC, but the **primary** flag in the CIDR (`cloudCidr`) field in the cloud context profile is available for Cisco Cloud APIC to support secondary IP ranges. Every subnet configured under a primary CIDR will be deployed as an actual Google Cloud subnet with the specified primary IP range (named *primary subnets*). For release 25.0(1) for Google Cloud, having multiple CIDRs set as primary under a given cloud context profile (`cloudCtxProfile`) is supported. Therefore, you can have more than one primary CIDR under a given cloud context profile with multiple primary subnets.

The following POST shows an example where one VPC and three subnets are deployed in Google Cloud.

```
<polUni>
  <fvTenant name="t1">
    <fvCtx name="v1"/>
    <cloudCtxProfile name="c1" vpcGroup="vpc-1">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
      <cloudRsToCtx tnFvCtxName="v1"/>
```

```

        <cloudCidr addr="10.0.0.0/16" primary="yes" >
          <cloudSubnet ip="10.0.1.0/24">
            <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
          </cloudSubnet>
          <cloudSubnet ip="10.0.2.0/24">
            <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west/zone-default"/>
          </cloudSubnet>
        </cloudCidr>
        <cloudCidr addr="20.0.0.0/16" primary="yes" >
          <cloudSubnet ip="20.0.1.0/24">
            <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west/zone-default"/>
          </cloudSubnet>
        </cloudCidr>
      </cloudCtxProfile>
</polUni>

```

In the example above, one VPC is configured for the VRF `v1` with three primary subnets (10.0.1.0/24, 10.0.2.0/24, and 20.0.1.0/24) deployed in the us-west region.

A secondary CIDR contains the secondary IP ranges (called *secondary subnets*) that are configured in the existing primary subnets. When designating a CIDR as either primary or secondary, it's helpful to consider these differences between the two:

- The primary CIDR is normally the VM.
- The secondary CIDR is more of a container used for the application.

You can group together primary and secondary subnets into a **subnet group**. This grouping mechanism assigns secondary subnets (for example, IP ranges) to a primary subnet, which is mapped to an actual Google Cloud subnet. The scope of the subnet group is at the cloud context profile level. While you can have multiple cloud context profiles within the same tenant, subnets are part of a subnet group only within the same cloud context profile.

You will use the **subnet group label** to assign a unique label to a specific subnet group. If you have multiple subnets that have the same subnet group label, then those subnets all belong to the same subnet group as long as they are all within the same cloud context profile. Note that while the subnet group label is used within Cisco Cloud APIC to group primary and secondary subnets, it is not used in Google Cloud.

Note the following guidelines for the primary and secondary CIDRs:

- **Primary CIDR:**
  - Any subnet group can have at maximum of only one subnet from the primary CIDR.
  - You can have multiple subnets in the primary CIDR, but all of the subnets must be in a separate subnet group.
- **Secondary CIDR:** You can have multiple subnets from the secondary CIDR in the same subnet group.

The following POST shows an example where two VPCs with two subnets each in different regions and having secondary CIDRs are deployed in Google Cloud.

```

<polUni>
  <fvTenant name="t1">
    <fvCtx name="v1"/>
    <fvCtx name="v2"/>
    <cloudCtxProfile name="c1" vpcGroup="vpc-1">

```

```

    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
    <cloudRsToCtx tnFvCtxName="v1"/>
    <cloudCidr addr="10.0.0.0/16" primary="yes" >
      <cloudSubnet ip="10.0.1.0/24" subnetGroup="subnet-1">
        <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
      <cloudSubnet ip="10.0.2.0/24" subnetGroup="subnet-2">
        <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    <cloudCidr addr="40.0.0.0/16" primary="no">
      <cloudSubnet ip="40.0.1.0/24" subnetGroup="subnet-1">
        <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  <cloudCtxProfile name="c2" vpcGroup="vpc-2">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-east1" />
    <cloudRsToCtx tnFvCtxName="v2"/>
    <cloudCidr addr="20.0.0.0/16" primary="yes">
      <cloudSubnet ip="20.0.1.0/24" subnetGroup="subnet-1">
        <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    <cloudCidr addr="30.0.0.0/16" primary="no">
      <cloudSubnet ip="30.0.1.0/24" subnetGroup="subnet-1">
        <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>

```

Note that the subnet group `subnet-1` in the cloud context profile `c2` is not the same subnet group in the cloud context profile `c1`, because the scope of the subnet group is at the cloud context profile level.

The intent of the example above is summarized as follows:

- Tenant `t1` defines VRF `v1` and `v2`.
- Cloud context profile `c1` defines the subnets in region `us-west1` for VRF `v1` and VPC group `vpc-1`. This deploys VPC `vpc-1`.
- Cloud context profile `c2` defines the subnets in region `us-east1` for VRF `v2` and VPC group `vpc-2`. This deploys VPC `vpc-2`.
- The following subnets are deployed in VPC `vpc-1` in region `us-west1`:
  - `Subnet-1` subnet group:
    - Primary IP range: `10.0.1.0/24`
    - Secondary IP ranges: `40.0.1.0/24`
  - `Subnet-2` subnet group:
    - Primary IP range: `10.0.2.0/24`

- The following subnets are deployed in VPC `vpc-2` in region `us-east1`:
  - Subnet-1:
    - Primary IP range: `20.0.1.0/24`
    - Secondary IP ranges: `30.0.1.0/24`

## Guidelines and Limitations For Configuring Cisco Cloud APIC with Google Cloud

Following are the guidelines and limitations when configuring Cisco Cloud APIC with Google Cloud:

- Google Cloud does not support routing based on contracts.
- External connectivity between two Google Cloud sites is not supported in release 25.0(1).
- The external VRF can be configured only in the infra tenant in Cisco Cloud APIC.
- The tenant `common` in Cisco Cloud APIC cannot be associated with any Google Cloud project.
- In Google Cloud, the infra VPC and spoke VPCs are connected through VPC peering.
- For release 25.0(1), in order to configure connectivity between the on-premises data center and the public cloud, you must manually configure the remote device by downloading the external device configuration files and manually enabling connectivity between Google Cloud and the external devices.

The external device configuration files that you download are not final configurations. Instead, the external device configuration files are provided more as a guidance. You must manually modify the information in the configuration files to configure the Google Cloud Router with IPsec, which is used to create connectivity between the on-premises data center and the public cloud, where:

- The Google Cloud Router and tunnels are deployed in the infra (hub) VPC.
- For release 25.0(1), one cloud router per region is supported. Cloud routers can be deployed in a maximum of four regions.
- Spoke VPCs peer with the infra VPC to share the VPN connections to external sites, such as the on-premises data center.

### Naming Length Restrictions Imposed By Google Cloud Firewall Rules

Google Cloud firewall rules are named resources, and Cisco Cloud APIC derives a name from the internal policy and uses that to deploy the Google Cloud firewall rules. Cisco Cloud APIC uses the following naming scheme for the internal policy:

```
{VPC-name}-{in/eg}-{target App-name}-{target EPG-name}-{contract-name}
```

The maximum length for a Google Cloud firewall rule name is 62 characters. This imposes a restriction on the names that you can use when configuring the following Cisco Cloud APIC components whose names are used in the Google Cloud firewall rule name:

- VPC group



- Application profile
- Application EPG or external EPG
- Contract

Knowing that the maximum number of characters is 62 for a Google Cloud firewall rule name, and taking into account the fixed areas in the string that makes up the Google Cloud firewall rule name:

- Hyphens (4 characters total)
- `in` (ingress) or `eg` (egress) value (2 characters)

That means that the total number of characters available for the combined names of all of the individual Cisco Cloud APIC components cannot exceed 56:

$$62 - 4 (\text{number of hypens}) - 2 (\text{in or eg characters}) = 56 \text{ characters}$$

So, the sum of the lengths of the names of the VPC group, application profile, application EPG or external EPG, and contract must be smaller than 56 characters. On average, this allows for roughly 14 characters for the name of each component.





## CHAPTER 4

# Cisco Cloud APIC Policy Model

---

- [About the ACI Policy Model, on page 27](#)
- [Policy Model Key Characteristics, on page 27](#)
- [Logical Constructs, on page 28](#)
- [The Cisco ACI Policy Management Information Model, on page 29](#)
- [Tenants, on page 30](#)
- [Cloud Context Profile, on page 31](#)
- [VRFs, on page 31](#)
- [Cloud Application Profiles, on page 32](#)
- [Cloud Endpoint Groups, on page 33](#)
- [Contracts, on page 34](#)
- [About the Cloud Template, on page 36](#)
- [Managed Object Relations and Policy Resolution, on page 38](#)
- [Default Policies, on page 39](#)

## About the ACI Policy Model

The ACI policy model enables the specification of application requirements policies. The Cisco Cloud APIC automatically renders policies in the cloud infrastructure. When you or a process initiates an administrative change to an object in the cloud infrastructure, the Cisco Cloud APIC first applies that change to the policy model. This policy model change then triggers a change to the actual managed item. This approach is called a model-driven framework.

## Policy Model Key Characteristics

Key characteristics of the policy model include the following:

- As a model-driven architecture, the software maintains a complete representation of the administrative and operational state of the system (the model). The model applies uniformly to cloud infrastructure, services, system behaviors, and virtual devices attached to the network.
- The logical and concrete domains are separated; the logical configurations are rendered into concrete configurations by applying the policies in relation to the available resources. No configuration is carried out against concrete entities. Concrete entities are configured implicitly as a side effect of the changes to the Cisco Cloud policy model.

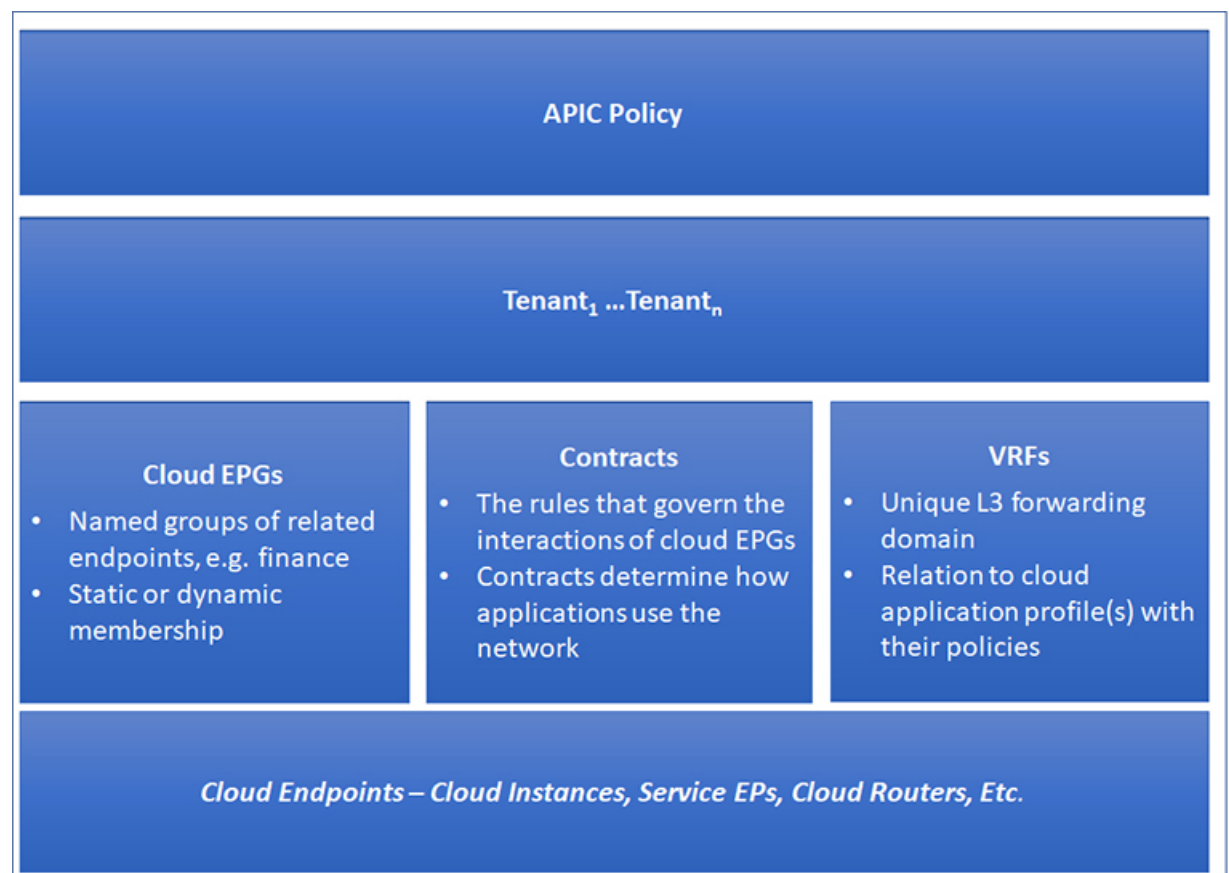
- The system prohibits communications with newly connected endpoints until the policy model is updated to include the new endpoint.
- Network administrators do not configure logical system resources directly. Instead, they define logical (hardware-independent) configurations and the Cisco Cloud APIC policies that control different aspects of the system behavior.

Managed object manipulation in the model relieves engineers from the task of administering isolated, individual component configurations. These characteristics enable automation and flexible workload provisioning that can locate any workload anywhere in the infrastructure. Network-attached services can be easily deployed, and the Cisco Cloud APIC provides an automation framework to manage the lifecycle of those network-attached services.

## Logical Constructs

The policy model manages the entire cloud infrastructure, including the infrastructure, authentication, security, services, applications, cloud infrastructure, and diagnostics. Logical constructs in the policy model define how the cloud infrastructure meets the needs of any of the functions of the cloud infrastructure. The following figure provides an overview of the ACI policy model logical constructs.

**Figure 11: ACI Policy Model Logical Constructs Overview**



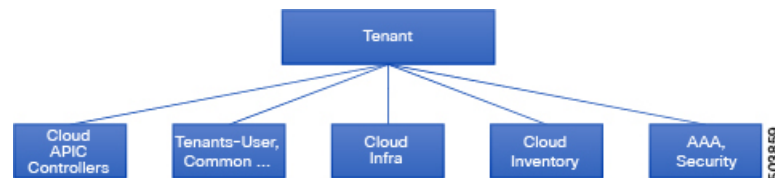
cloud infrastructure-wide or tenant administrators create predefined policies that contain application or shared resource requirements. These policies automate the provisioning of applications, network-attached services, security policies, and tenant subnets, which puts administrators in the position of approaching the resource pool in terms of applications rather than infrastructure building blocks. The application needs to drive the networking behavior, not the other way around.

## The Cisco ACI Policy Management Information Model

The cloud infrastructure comprises the logical components as recorded in the Management Information Model (MIM), which can be represented in a hierarchical management information tree (MIT). The Cisco Cloud APIC runs processes that store and manage the information model. Similar to the OSI Common Management Information Protocol (CMIP) and other X.500 variants, the Cisco Cloud APIC enables the control of managed resources by presenting their manageable characteristics as object properties that can be inherited according to the location of the object within the hierarchical structure of the MIT.

Each node in the tree represents a managed object (MO) or group of objects. MOs are abstractions of cloud infrastructure resources. An MO can represent a concrete object, such as a cloud router, adapter, or a logical object, such as an application profile, cloud endpoint group, or fault. The following figure provides an overview of the MIT.

**Figure 12: Cisco ACI Policy Management Information Model Overview**



The hierarchical structure starts with the policy universe at the top (Root) and contains parent and child nodes. Each node in the tree is an MO and each object in the cloud infrastructure has a unique distinguished name (DN) that describes the object and locates its place in the tree.

The following managed objects contain the policies that govern the operation of the system:

- A tenant is a container for policies that enable an administrator to exercise role-based access control. The system provides the following four kinds of tenants:
  - The administrator defines user tenants according to the needs of users. They contain policies that govern the operation of resources such as applications, databases, web servers, network-attached storage, virtual machines, and so on.
  - Although the system provides the common tenant, it can be configured by the cloud infrastructure administrator. It contains policies that govern the operation of resources accessible to all tenants, such as firewalls, load balancers, intrusion detection appliances, and so on.
  - The infrastructure tenant is provided by the system but can be configured by the cloud infrastructure administrator. It contains policies that govern the operation of infrastructure resources. It also enables a cloud infrastructure provider to selectively deploy resources to one or more user tenants. Infrastructure tenant policies are configurable by the cloud infrastructure administrator.
- The cloud infra policies enable you to manage on-premises and inter-region connectivity when setting up the Cisco Cloud APIC. For more information, see the *Cisco Cloud APIC Installation Guide*.

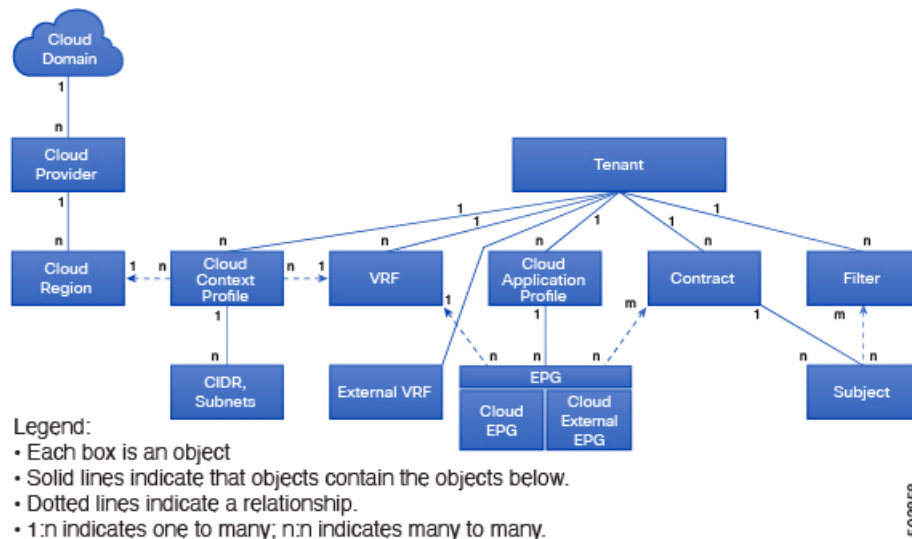
- Cloud inventory is a service that enables you to view different aspects of the system using the GUI. For example, you can view the regions that are deployed from the aspect of an application or the applications that are deployed from the aspect of a region. You can use this information for cloud resource planning and troubleshooting.
- Access, authentication, and accounting (AAA) policies govern user privileges, roles, and security domains of the Cisco Cloud APIC cloud infrastructure. For more information, see [Cisco Cloud APIC Security, on page 125](#)

The hierarchical policy model fits well with the REST API interface. When invoked, the API reads from or writes to objects in the MIT. URLs map directly into distinguished names that identify objects in the MIT. Any data in the MIT can be described as a self-contained structured tree text document encoded in XML or JSON.

## Tenants

A tenant ( $fvTenant$ ) is a logical container for application policies that enable an administrator to exercise domain-based access control. A tenant represents a unit of isolation from a policy perspective, but it does not represent a private network. Tenants can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies. The following figure provides an overview of the tenant portion of the management information tree (MIT).

**Figure 13: Tenants**



Tenants can be isolated from one another or can share resources. The primary elements that the tenant contains are filters, contracts, Virtual Routing and Forwarding (VRF) instances, cloud context profiles, Google Cloud provider configurations, and cloud application profiles that contain cloud endpoint groups (cloud EPGs). Entities in the tenant inherit its policies. VRFs are also known as contexts; each VRF can be associated with multiple cloud context profiles. A cloud context profile, in conjunction with a VRF, tenant and region, represents a resource group in Google Cloud. A VPC is created inside the resource group based on the VRF name.

Tenants are logical containers for application policies. The cloud infrastructure can contain multiple tenants. The ACI cloud infrastructure supports IPv4 and dual-stack configurations for tenant networking.

## Cloud Context Profile

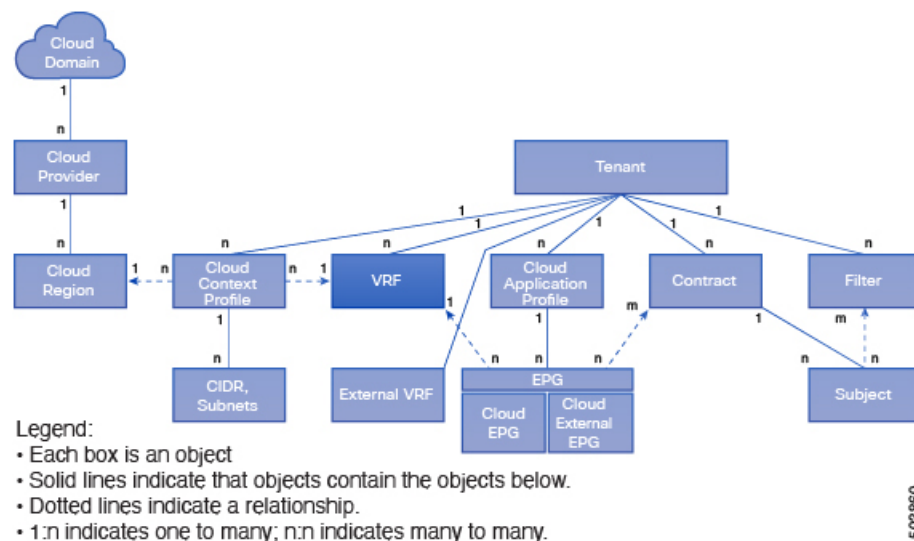
The cloud context profile contains information on the following Cisco Cloud APIC components:

- CIDRs
- VRFs
- EPGs
- Regions
- VPCs
- Endpoints

## VRFs

A Virtual Routing and Forwarding (VRF) object (`fVContext`) or context is a tenant network (called a VRF in the Cisco Cloud APIC GUI). A tenant can have multiple VRFs. A VRF is a unique Layer 3 forwarding and application policy domain. The following figure shows the location of VRFs in the management information tree (MIT) and their relation to other objects in the tenant.

**Figure 14: VRFs**



A VRF defines a Layer 3 address domain. One or more cloud context profiles are associated with a VRF. You can only associate one cloud context profile with a VRF in a given region. All the endpoints within the Layer 3 domain must have unique IP addresses because it is possible to forward packets directly between these devices if the policy allows it. A tenant can contain multiple VRFs. After an administrator creates a logical device, the administrator can create a VRF for the logical device, which provides a selection criteria policy

for a device cluster. A logical device can be selected based on a contract name, a graph name, or the function node name inside the graph.

### External VRF

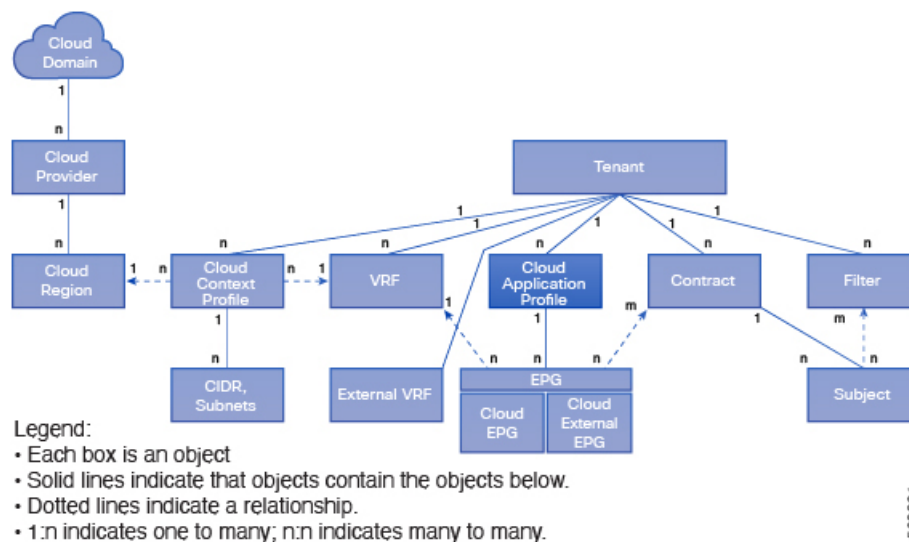
Beginning with release 25.0(1), an **external VRF** is introduced as a new type of VRF available for Cisco Cloud APIC. An external VRF is a unique VRF that does not have any presence in the cloud. This VRF is not referred to in any cloud context profile used by Cisco Cloud APIC.

An external VRF represents an external network that is connected to other cloud sites or to on-premises sites. Multiple cloud VRFs can leak routes to an external VRF or can get the routes from an external VRF. When an external network is created on an external VRF, inter-VRF routing is set up so that routes received and advertised on the external network are received or advertised on the external VRF.

## Cloud Application Profiles

A cloud application profile (`cloudAp`) defines the policies, services and relationships between cloud EPGs. The following figure shows the location of cloud application profiles in the management information tree (MIT) and their relation to other objects in the tenant.

**Figure 15: Cloud Application Profiles**



Cloud application profiles contain one or more cloud EPGs. Modern applications contain multiple components. For example, an e-commerce application could require a web server, a database server, data located in a storage service, and access to outside resources that enable financial transactions. The cloud application profile contains as many (or as few) cloud EPGs as necessary that are logically related to providing the capabilities of an application.

Cloud EPGs can be organized according to one of the following:

- The application they provide, such as a DNS server or SAP application (see *Tenant Policy Example* in *Cisco APIC REST API Configuration Guide*).
- The function they provide (such as infrastructure)

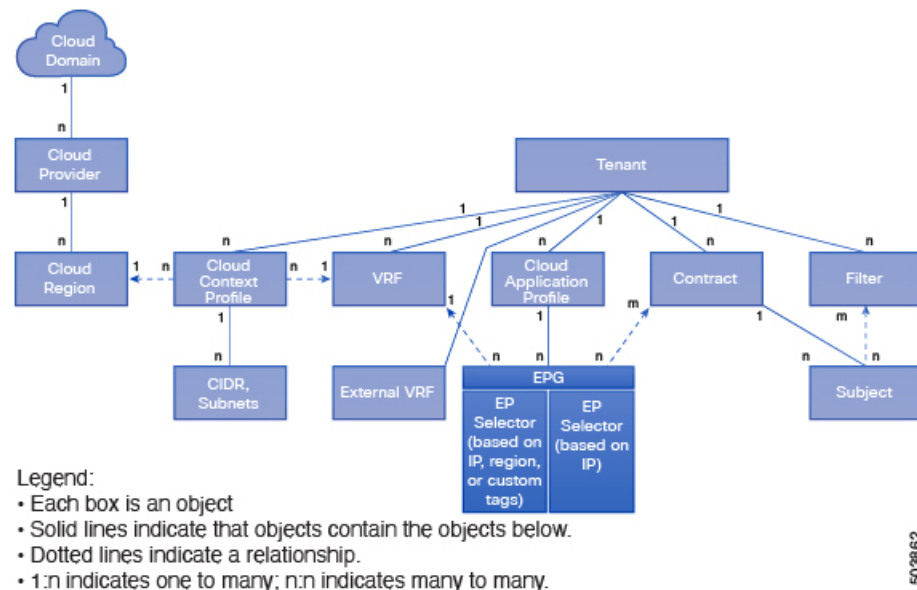


- Where they are in the structure of the data center (such as DMZ)
- Whatever organizing principle that a cloud infrastructure or tenant administrator chooses to use

## Cloud Endpoint Groups

The cloud endpoint group (cloud EPG) is the most important object in the policy model. The following figure shows where application cloud EPGs are located in the management information tree (MIT) and their relation to other objects in the tenant.

**Figure 16: Cloud Endpoint Groups**



A cloud EPG is a managed object that is a named logical entity that contains a collection of endpoints. Endpoints are devices that are connected to the network. They have an address (identity), a location, attributes (such as version or patch level), and are virtual. Knowing the address of an endpoint also enables access to all its other identity details. Cloud EPGs are fully decoupled from the physical and logical topology. Endpoint examples include servers, virtual machines, storage services, or clients on the Internet. Endpoint membership in a cloud EPG can be dynamic or static.

The ACI cloud infrastructure can contain the following types of cloud EPGs:

- Cloud endpoint group (`cloudEPg`)
- Cloud external endpoint group (`cloudExtEPg`)

Cloud EPGs contain endpoints that have common policy requirements such as security services. Rather than configure and manage endpoints individually, they are placed in a cloud EPG and are managed as a group.

Policies apply to cloud EPGs, never to individual endpoints.

Regardless of how a cloud EPG is configured, cloud EPG policies are applied to the endpoints they contain.

WAN router connectivity to the cloud infrastructure is an example of a configuration that uses a static cloud EPG. To configure WAN router connectivity to the cloud infrastructure, an administrator configures a `cloudExtEPg` cloud EPG that includes any endpoints within an associated WAN subnet. The cloud infrastructure learns of the cloud EPG endpoints through a discovery process as the endpoints progress through their connectivity life cycle. Upon learning of the endpoint, the cloud infrastructure applies the `cloudExtEPg` cloud EPG policies accordingly. For example, when a WAN connected client initiates a TCP session with a server within an application (`cloudEPg`) cloud EPG, the `cloudExtEPg` cloud EPG applies its policies to that client endpoint before the communication with the (`cloudEPg`) cloud EPG web server begins. When the client server TCP session ends, and communication between the client and server terminates, the WAN endpoint no longer exists in the cloud infrastructure.

The Cisco Cloud APIC uses endpoint selectors to assign endpoints to Cloud EPGs. The endpoint selector is essentially a set of rules that are run against the cloud instances that are assigned to the Google Cloud VPC managed by Cisco ACI. Any endpoint selector rules that match endpoint instances assign that endpoint to the Cloud EPG. The endpoint selector is similar to the attribute-based microsegmentation available in Cisco ACI.

## Contracts

In addition to cloud EPGs, contracts (`vzBrCP`) are key objects in the policy model. Cloud EPGs can only communicate with other cloud EPGs according to contract rules. The following figure shows the location of contracts in the management information tree (MIT) and their relation to other objects in the tenant.

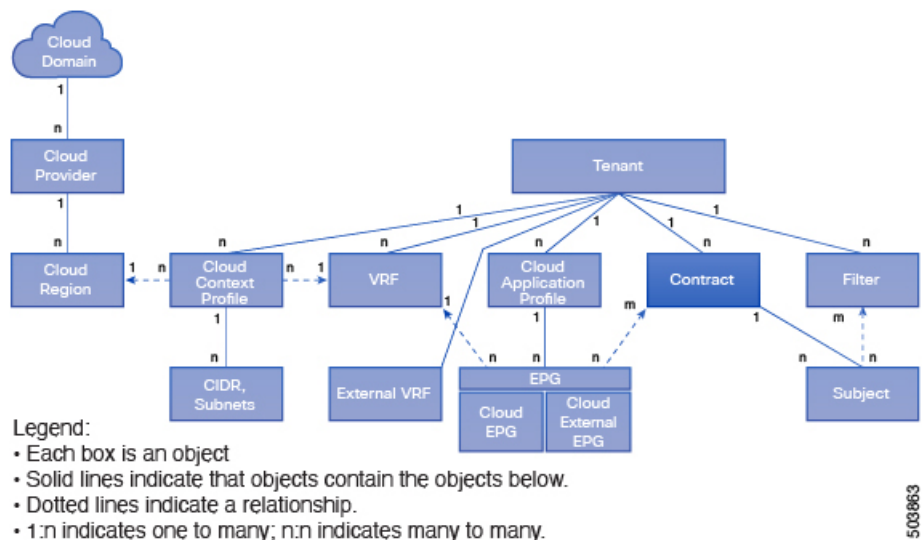


Figure 17: Contracts

An administrator uses a contract to select one or more types of traffic that can pass between cloud EPGs, including the protocols and ports allowed. If there is no contract, inter-EPG communication is disabled by default. There is no contract required for intra-EPG communication; intra-EPG communication is always implicitly allowed.

Contracts govern the following types of cloud EPG communications:

- Between cloud EPGs (`cloudEPg`), both intra-tenant and inter-tenant



**Note** In the case of a shared service mode, a contract is required for inter-tenant communication. A contract is used to specify static routes across VRFs, although the tenant VRF does not enforce a policy.

- Between cloud EPGs and cloud external EPGs (`cloudExtEPg`)

Contracts govern the communication between cloud EPGs that are labeled providers, consumers, or both. The relationship between a cloud EPG and a contract can be either a provider or consumer. When a cloud EPG provides a contract, communication with the cloud endpoints in that cloud EPG can be initiated from cloud endpoints in other cloud EPGs as long as the communication complies with the provided contract. When a cloud EPG consumes a contract, the cloud endpoints in the consuming cloud EPG may initiate communication with any cloud endpoint in a cloud EPG that is providing that contract.

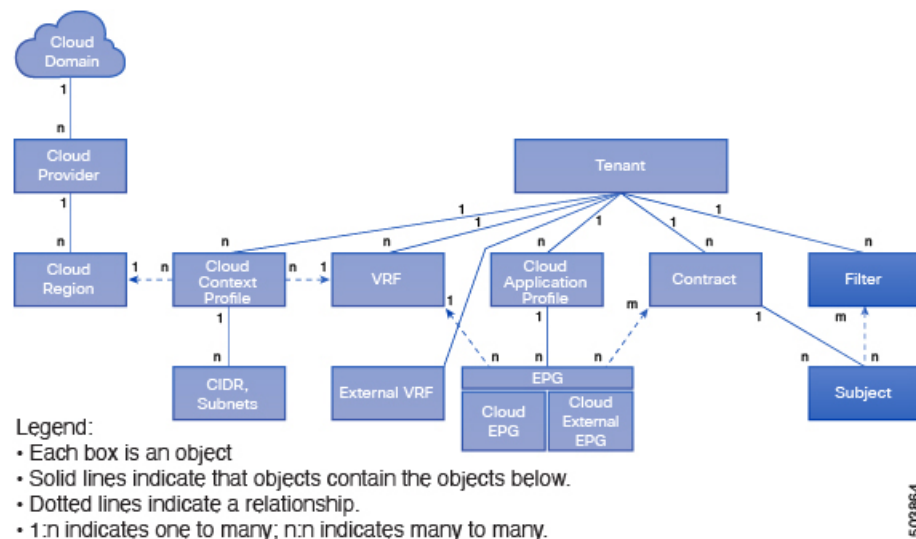


**Note** A cloud EPG can both provide and consume the same contract. A cloud EPG can also provide and consume multiple contracts simultaneously.

## Filters and Subjects Govern Cloud EPG Communications

Subject and filter managed-objects enable mixing and matching among cloud EPGs and contracts so as to satisfy various applications or service delivery requirements. The following figure shows the location of application subjects and filters in the management information tree (MIT) and their relation to other objects in the tenant.

**Figure 18: Subjects and Filters**



Contracts can contain multiple communication rules and multiple cloud EPGs can both consume and provide multiple contracts. A policy designer can compactly represent complex communication policies and re-use these policies across multiple instances of an application.



**Note** Subjects are hidden in Cisco Cloud APIC and not configurable. For rules installed in Google Cloud, source port provided in the filter entry is not taken into account.

Subjects and filters define cloud EPG communications according to the following options:

- Filters are Layer 3 to Layer 4 fields, TCP/IP header fields such as Layer 3 protocol type, Layer 4 ports, and so forth. According to its related contract, a cloud EPG provider dictates the protocols and ports in both the in and out directions. Contract subjects contain associations to the filters (and their directions) that are applied between cloud EPGs that produce and consume the contract.
- Subjects are contained in contracts. A subject within a contract uses filters to specify the type of traffic that can be communicated and how it occurs. For example, for HTTPS messages, the subject specifies the direction and the filters that specify the IP address type (for example, IPv4), the HTTP protocol, and the ports allowed. Subjects determine if filters are unidirectional or bidirectional. A unidirectional filter is used in one direction. Unidirectional filters define in or out communications but not the same for both. Bidirectional filters are the same for both; they define both in and out communications.
- ACI contracts rendered in Google Cloud constructs are always stateful, allowing return traffic.

## About the Cloud Template

The cloud template provides a template that configures and manages the Cisco Cloud APIC infra network. The template requires only the most essential elements for the configuration. From these elements, the cloud template generates a detailed configuration necessary for setting up the Cisco Cloud APIC infra network. However, it is not a one-time configuration generation—it is possible to add, modify, or remove elements of the template input. The cloud template updates the resulting configuration accordingly.

One of the central things in the Google Cloud network configuration is the Virtual Private Cloud (VPC). Google Cloud supports many regions worldwide and one VPC is specific to one region.

The cloud template accepts one or more region names and generates the entire configuration for the infra VPCs in those regions. They are the infra VPCs. The Cisco Cloud APIC-managed object (MO) corresponding to the Google Cloud VPC is `cloudCtxProfile`. For every region specified in the cloud template, it generates the `cloudCtxProfile` configuration. A `cloudCtxProfile` is the topmost MO for all the configuration corresponding to a region. Underneath, it has many of other MOs organized as a tree to capture a specific configuration. The `cloudCtxProfile` MO for the infra VPC is generated by the cloud template. It carries `ctxProfileOwner == SYSTEM`, which means that this MO is generated by the system. For the non-infra network, it is possible to configure `cloudCtxProfile` directly; in this case, `cloudCtxProfile` carries `ctxProfileOwner == USER`.

A primary property of a Google Cloud VPC is the CIDR. In Cisco Cloud APIC, you can choose and deploy CIDRs in the user VPCs. The CIDRs for the infra VPC are provided by users to the cloud template during the initial setup of the cloud site, and are deployed to the Google Cloud by the cloud template.

A property called `createdBy` is also available for the CIDR. The default value for this `createdBy` property is `USER`.

- For all user-created CIDRs, the value for the `createdBy` property is set to `USER`.
- For cloud template-created CIDRs, the value for the `createdBy` property is set to `SYSTEM`.

Multiple CIDR and subnet blocks can be configured on the infra VPC. You can create CIDRs and associate subnets in the infra VPC. The cloud template subnets will be mapped to the overlay-1 VRF. All subnets in the respective VRFs will have separate route tables in the cloud for VRF segregation.

For more information, see [Creating an Application EPG Using the Cisco Cloud APIC GUI, on page 60](#).

The cloud template generates and manages a huge number of MOs in the `cloudCtxProfile` subtree including, but not limited to, the following:

- Subnets
- Cloud routers
- IP address allocation for the cloud router interfaces
- IP address allocation and configuration for tunnels
- IP address allocation and configuration for loopbacks

Without the cloud template, you would be responsible for configuring and managing these.

The *Cisco Cloud Template MO* table contains a brief summary of the inputs (MOs) to the cloud template.

**Table 5: Cloud Template MOs**

MO	Purpose
<code>cloudtemplateInfraNetwork</code>	The root of the cloud template configuration. Attributes include:  <code>numRoutersPerRegion</code> —The number of cloud routers for each <code>cloudRegionName</code> specified under <code>cloudtemplateIntNetwork</code> .
<code>cloudtemplateIntNetwork</code>	Contains a list of regions, which specify where you deploy the cloud routers. Each region is captured through a <code>cloudRegionName</code> child MO
<code>cloudtemplateExtNetwork</code>	Contains infra network configuration input that is external of the cloud.  Contains a list of regions where cloud routers are configured for external networking.  Each region is captured through a <code>cloudRegionName</code> child MO
<code>cloudtemplateIpSecTunnel</code>	Captures the IP address of the IPSec peer in the ACI on-premises site.

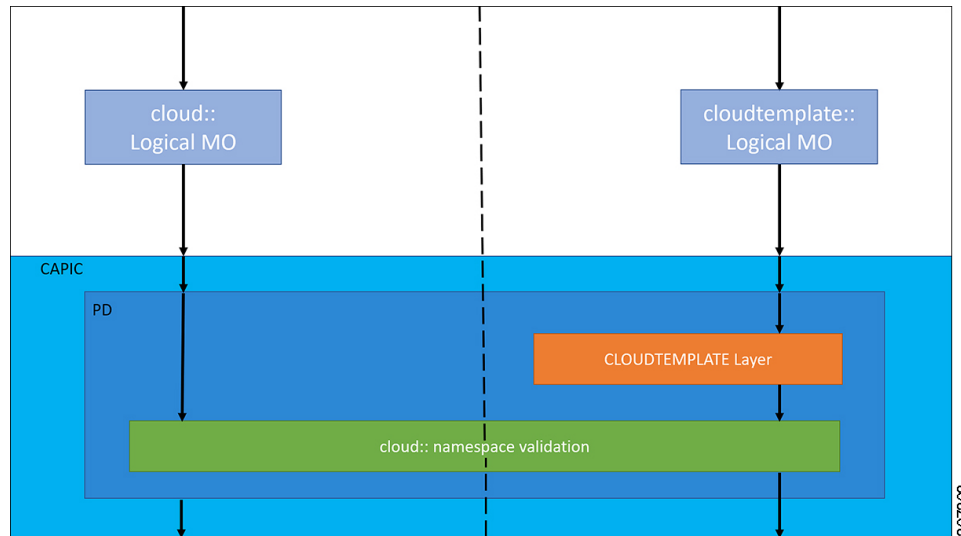
In Cisco Cloud APIC, the layering of MOs is slightly different from a regular Cisco APIC due to the cloud template. In a regular Cisco APIC, you post logical MOs that go through two layers of translation:

1. Logical MO to resolved MO
2. Resolved MO to concrete MO

In Cisco Cloud APIC, there is an additional layer of translation for the infra network. This additional layer is where the cloud template translates logical MOs in the `cloudtemplate` namespace to logical MOs in the cloud

namespace. For configurations outside of the infra network, you post logical MOs in the cloud namespace. In this case, the MOs go through the usual two-layer translation as in the regular Cisco APIC.

**Figure 19: Cloud and Cloud Template MO Conversion**



**Note** For information about configuring the cloud template, see [Configuring Cisco Cloud APIC Components, on page 41](#)

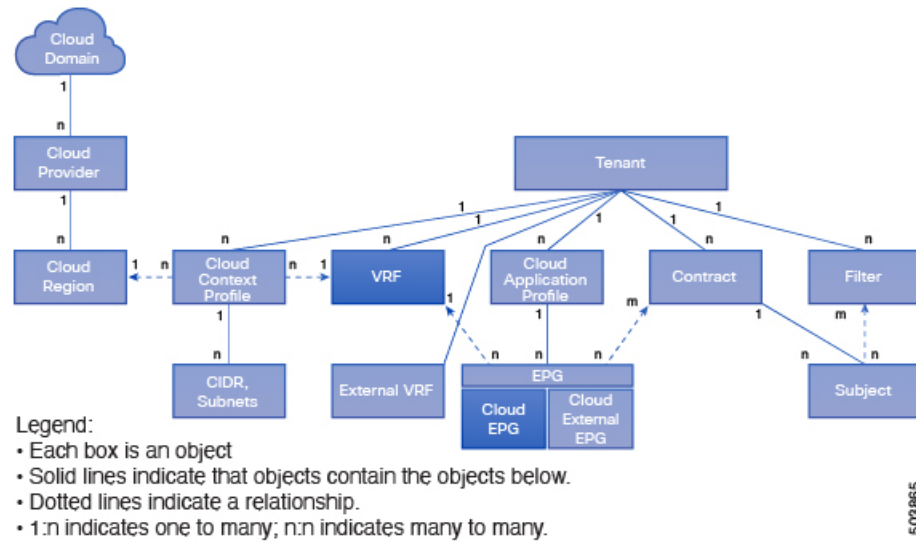
## Managed Object Relations and Policy Resolution

Relationship-managed objects express the relation between managed object instances that do not share containment (parent-child) relations. MO relations are established between the source MO and a target MO in one of the following two ways:

- An explicit relation, such as with `cloudRsCloudEPgCtx`, defines a relationship that is based on the target MO distinguished name (DN).
- A named relation defines a relationship that is based on the target MO name.

The dotted lines in the following figure show several common MO relations.

Figure 20: MO Relations



For example, the dotted line between the cloud EPG and the VRF defines the relation between those two MOs. In this figure, the cloud EPG (`cloudEPg`) contains a relationship MO (`cloudRsCloudEPgCtx`) that is named with the name of the target VRF MO (`fVCtx`). For example, if production is the VRF name (`fVCtx.name=production`), then the relation name is production (`cloudRsCloudEPgCtx.tnFvCtxName=production`).

In the case of policy resolution based on named relations, if a target MO with a matching name is not found in the current tenant, the ACI cloud infrastructure tries to resolve in the common tenant. For example, if the user tenant cloud EPG contained a relationship MO targeted to a VRF that did not exist in the tenant, the system tries to resolve the relationship in the common tenant. If a named relation cannot be resolved in either the current tenant or the common tenant, the ACI cloud infrastructure attempts to resolve to a default policy. If a default policy exists in the current tenant, it is used. If it does not exist, the ACI cloud infrastructure looks for a default policy in the common tenant. Cloud context profile, VRF, and contract (security policy) named relations do not resolve to a default.

## Default Policies



**Warning** Default policies can be modified or deleted. Deleting a default policy can result in a policy resolution process to complete abnormally.

The ACI cloud infrastructure includes default policies for many of its core functions. Examples of default policies include the following:

- Google Cloud provider (for the infra tenant)
- Monitoring



---

**Note** To avoid confusion when implementing configurations that use default policies, document changes made to default policies. Be sure that there are no current or future configurations that rely on a default policy before deleting a default policy. For example, deleting a default firmware update policy could result in a problematic future firmware update.

---

A default policy serves multiple purposes:

- Allows a cloud infrastructure administrator to override the default values in the model.
- If an administrator does not provide an explicit policy, the Cisco Cloud APIC applies the default policy. An administrator can create a default policy and the Cisco Cloud APIC uses that unless the administrator provides any explicit policy.

The policy model specifies that an object is using another policy by having a relation-managed object (MO) under that object and that relation MO refers to the target policy by name. If this relation does not explicitly refer to a policy by name, then the system tries to resolve a policy that is called default. Cloud context profiles and VRFs are exceptions to this rule.





## CHAPTER 5

# Configuring Cisco Cloud APIC Components

---

- [About Configuring the Cisco Cloud APIC, on page 41](#)
- [Configuring the Cisco Cloud APIC Using the GUI, on page 41](#)
- [Configuring Cisco Cloud APIC Using the REST API, on page 97](#)

## About Configuring the Cisco Cloud APIC

You create the Cisco Cloud APIC components using either the Cisco Cloud APIC GUI or the REST API. This section explains how to create configuration, application management, operations, and administrative components.



---

**Note** For information about the GUI, such as navigation and a list of configurable components, see [About the Cisco Cloud APIC GUI, on page 4](#).

---

## Configuring the Cisco Cloud APIC Using the GUI

### Creating a Tenant

The following sections describe how to create a managed tenant or unmanaged tenant.

### Setting Up the Google Cloud Project for a User Tenant

Perform the procedures in this section to set up the Google Cloud project for a user tenant, where that user tenant is either a managed or an unmanaged tenant.

---

**Step 1** Create a Google Cloud project for the user tenant, if necessary.

Each user tenant is mapped one-to-one to a Google Cloud project. If you do not have a Google Cloud project created yet for your user tenant, follow these procedures to create a Google Cloud project.

- a) Log into your Google account.
- b) Navigate to **IAM & Admin > Manage resources**.

- c) Using the **Select organization** drop-down list at the top of the page, choose the organization where you want to create a project.
- d) Click + **CREATE PROJECT**.
- e) In the **New Project** window that appears, enter a project name and select a billing account as applicable.  
A project name can contain only letters, numbers, single quotes, hyphens, spaces, or exclamation points, and must be between 4 and 30 characters.
- f) Enter the parent organization or folder in the **Location** field.  
That resource will be the hierarchical parent of the new project.
- g) Click **CREATE**.

**Step 2**

In Google Cloud, enable the appropriate service APIs in the service account associated with this user tenant.

- a) In the Google Cloud GUI, log into the Google Cloud project that is associated with this user tenant.  
The **Dashboard** for the project is displayed.
- b) In the search bar at the top of the **Dashboard**, search for **APIs & Services**, then click the result from that search to access the **APIs & Services** window.
- c) In the **APIs & Services** window, click the + **ENABLE APIS AND SERVICES** tab.  
The **API Library** window appears.
- d) In the **Search for APIs & Services** field, search for and enable the necessary services.

For each of the services in the list below:

1. Search for the API or service in the **Search for APIs & Services** field.
2. Click on the search result to display the page for that API or service.
3. Click the **ENABLE** button in that API or service page.

Following are the APIs and services that you must search for and enable:

- Compute Engine API
- Cloud Deployment Manager V2 API
- Cloud Pub/Sub API
- Cloud Resource Manager API
- Service Usage API
- Cloud Logging API

Each API or service takes several minutes to enable. You will have to navigate back to the **APIs & Services** window after you enable each API or service.

Note that the following additional APIs and services should be enabled automatically when you enable all of the APIs and services listed above:

- Identity and Access Management (IAM) API
- IAM Service Account Credentials API
- Cloud OS Login API
- Cloud DNS API

- Recommender API

If they are not enabled automatically, enable them manually.

### Step 3

Set the necessary permissions for this user tenant in Google Cloud.

- a) In the Google Cloud GUI, log into the Google Cloud project that is associated with this user tenant. The **Dashboard** for the project is displayed.
- b) In the left nav bar, click on **IAM & Admin**, then choose **IAM**.

The **IAM** window appears with several service accounts displayed.

- c) Locate the appropriate service account.
- d) Set the permissions for this service account.
  1. Click the pencil icon on the row for this service account.

The **Edit Permissions** window is displayed.

2. Click + **ADD ANOTHER ROLE**, then choose **Editor** as the role.

You are returned to the **IAM** window with the service accounts displayed.

3. Click + **ADD ANOTHER ROLE** again, then add the remaining necessary roles for this service account.

Following is the full list of roles that you must assign to this service account, including the Cloud Functions Service Agent that you added in the first step of this process:

- Editor
- Role Admin
- Project IAM Admin

4. After you have added all the necessary roles, click **SAVE**.

You are returned to the **IAM** window with the service accounts displayed and the necessary roles assigned to this service account.

---

## Creating a Managed Tenant

The following sections provide the information that you'll need to create a managed tenant, where you will:

- Create a managed tenant in Cisco Cloud APIC
- Set the necessary permissions for the managed tenant in Google Cloud

### Creating a Managed Tenant Using the Cisco Cloud APIC GUI

This section explains how to create a tenant that will be managed by Cisco Cloud APIC using the GUI.

---

#### Step 1

Set up the Google Cloud project for the user tenant.

See [Setting Up the Google Cloud Project for a User Tenant, on page 41](#) for those procedures.

**Step 2** In the Cisco Cloud APIC GUI, navigate to **Application Management > Tenants**.

A table of already-configured tenants is displayed.

**Step 3** Click **Actions** and choose **Create Tenant**.

The **Create Tenant** dialog box appears.

**Step 4** Choose the appropriate options and enter the appropriate values in each field as listed in the following *Create Tenant Dialog Box Fields* table then continue.

**Table 6: Create Tenant Dialog Box Fields**

Properties	Description
<b>Name</b>	Enter the name of the tenant. Match the regular expression:  [a-z]([-a-z0-9]*[a-z0-9])?  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.
<b>Description</b>	Enter a description of the tenant.
<b>Settings</b>	
<b>Add Security Domain</b>	To add a security domain for the tenant:  a. Click <b>Add Security Domain</b> . The <b>Select Security Domains</b> dialog appears with a list of security domains in the left pane.  b. Click to choose a security domain.  c. Click <b>Select</b> to add the security domain to the tenant.
<b>Google Cloud Project</b>	
<b>Google Cloud Project ID</b>	Enter the Google Cloud Project ID that will be associated with this Cisco Cloud APIC tenant.
<b>Access Type</b>	For a tenant that will be managed by the Cisco Cloud APIC, choose <b>Managed Identity</b> as the access type.  For more information, see <a href="#">Understanding Google Cloud Deployments with Cisco Cloud APIC, on page 10</a> .
<b>Add Security Domain for Google Cloud Project</b>	<b>Note</b> Adding a security domain for Google Cloud is optional when creating a tenant.  To add a security domain for the account:  a. Click <b>Add Security Domain for Google Cloud Project</b> . The <b>Select Security Domains</b> dialog appears with a list of security domains in the left pane.  b. Click to choose a security domain.  c. Click <b>Select</b> to add the security domain to the tenant.

**Step 5** Click **Save** when finished.

---

#### What to do next

Complete the necessary configurations in Google Cloud for the managed tenant. Go to [Setting the Necessary Permissions in Google Cloud for a Managed Tenant, on page 45](#) for those procedures.

### Setting the Necessary Permissions in Google Cloud for a Managed Tenant

If you are creating a managed tenant, you must now set the necessary permissions in Google Cloud.



**Note** You do not have to follow the steps in this procedure if you are creating an unmanaged tenant.

---

**Step 1** In the Google Cloud GUI, log into the Google Cloud project that is associated with this managed tenant. The **Dashboard** for the project is displayed.

**Step 2** In the left nav bar, click on **IAM & Admin**, then choose **IAM**. The **IAM** window appears with several service accounts displayed.

**Step 3** Locate the service account that was created in the project that is associated with the infra account.

**Step 4** Copy the service account name.

**Step 5** Add this service account name as an IAM user in the user tenant project.

**Step 6** Set the permissions for this service account.

a) Click the pencil icon on the row for this service account.

The **Edit Permissions** window is displayed.

b) Click + **ADD ANOTHER ROLE**, then choose **Cloud Functions Service Agent** as the role.

You are returned to the **IAM** window with the service accounts displayed.

c) Click + **ADD ANOTHER ROLE** again, then add the remaining necessary roles for this service account.

Following is the full list of roles that you must assign to this service account, including the Cloud Functions Service Agent that you added in the first step of this process:

- Cloud Functions Service Agent
- Compute Instance Admin (v1)
- Compute Network Admin
- Compute Security Admin
- Logging Admin
- Pub/Sub Admin
- Storage Admin

d) After you have added all the necessary roles, click **SAVE**.

You are returned to the **IAM** window with the service accounts displayed and the necessary roles assigned to this service account.

---

## Creating an Unmanaged Tenant

The following sections provide the information that you'll need to create an unmanaged tenant, where you will:

- Generate and download the necessary private key information from Google Cloud for an unmanaged tenant
- Create an unmanaged tenant in Cisco Cloud APIC

### Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant

If you are creating an unmanaged tenant, you must first generate and download the necessary private key information from Google Cloud.



---

**Note** You do not have to follow the steps in this procedure if you are creating a managed tenant.

---

- 
- Step 1** In Google Cloud, select the Google Cloud project that will be associated with this unmanaged tenant, if you have not selected it already .
- Step 2** In the left nav bar, click on **IAM & Admin**, then choose **Service Accounts**.  
The service accounts for this Google Cloud project are displayed.
- Step 3** Select an existing service account or click + **CREATE SERVICE ACCOUNT** to create a new one.  
Information on this service account is displayed, with the **Details** tab selected by default.
- Step 4** Click the **KEYS** tab.
- Step 5** Click **ADD KEY > Create New Key**.  
A window appears, providing an option to create a private key for this service account.
- Step 6** Leave the **JSON** key type selected, then click **Create**.  
A window appears, saying that the private key has been saved to your computer.
- Step 7** Locate the JSON file that was downloaded to your computer and move it to a secure location on your computer.  
This JSON file will contain the key information that you need to fill in the fields for the unmanaged tenant.



Properties	Description
<b>Add Security Domain</b>	To add a security domain for the tenant: <ol style="list-style-type: none"> <li>Click <b>Add Security Domain</b>. The <b>Select Security Domains</b> dialog appears with a list of security domains in the left pane.</li> <li>Click to choose a security domain.</li> <li>Click <b>Select</b> to add the security domain to the tenant.</li> </ol>
<b>Google Cloud Project</b>	
<b>Google Cloud Project ID</b>	Enter the Google Cloud Project ID that will be associated with this Cisco Cloud APIC tenant.
<b>Access Type</b>	For a tenant that will not be managed by the Cisco Cloud APIC, choose <b>Unmanaged Identity</b> as the access type. For more information, see <a href="#">Understanding Google Cloud Deployments with Cisco Cloud APIC, on page 10</a> .
<b>Key ID</b>	Enter the information from the <code>private_key_id</code> field in the JSON file that you downloaded in <a href="#">Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 46</a> .
<b>RSA Private Key</b>	Enter the information from the <code>private_key</code> field in the JSON file that you downloaded in <a href="#">Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 46</a> .
<b>Client ID</b>	Enter the information from the <code>client_id</code> field in the JSON file that you downloaded in <a href="#">Generating and Downloading Private Key Information from Google Cloud for an Unmanaged Tenant, on page 46</a> .
<b>Email</b>	Enter the email address associated with your Google Cloud project.
<b>Add Security Domain for Google Cloud Project</b>	<p><b>Note</b> Adding a security domain for Google Cloud is optional when creating a tenant.</p> <p>To add a security domain for the account:</p> <ol style="list-style-type: none"> <li>Click <b>Add Security Domain for Google Cloud Project</b>. The <b>Select Security Domains</b> dialog appears with a list of security domains in the left pane.</li> <li>Click to choose a security domain.</li> <li>Click <b>Select</b> to add the security domain to the tenant.</li> </ol>



**Step 5** Click **Save** when finished.

---

## Creating an Application Profile Using the Cisco Cloud APIC GUI

This section explains how to create an application profile using the Cisco Cloud APIC GUI.

### Before you begin

Create a tenant.

---

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

**Step 3** From the **Application Management** list in the **Intent** menu, click **Create Application Profile**. The **Create Application Profile** dialog box appears.

**Step 4** Enter a name in the **Name** field.

Note the following restrictions:

- Match the regular expression:

```
[a-z]([-a-z0-9]*[a-z0-9])?
```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to [Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24](#) to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

**Step 5** Choose a tenant:

- a) Click **Select Tenant**.

The **Select Tenant** dialog box appears.

- b) From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**.

You return to the **Create Application Profile** dialog box.

**Step 6** Enter a description in the **Description** field.

**Step 7** Click **Save** when finished.

---

## Creating a VRF Using the Cisco Cloud APIC GUI

This section explains how to create a VRF using the Cisco Cloud APIC GUI.



**Note** To configure a external VRF, you will select `infra` in the **Tenant** field below. The VRF will be identified as a external VRF if it is:

- Configured under the `infra` tenant
- Associated with an external network (see [Creating an External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI, on page 51](#))
- Not associated with a cloud context profile

### Before you begin

Create a tenant.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

**Step 3** From the **Application Management** list in the **Intent** menu, click **Create VRF**. The **Create VRF** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create VRF Dialog Box Fields* table then continue.

**Table 8: Create VRF Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	<p>Enter a name for the VRF in the <b>Name</b> field.</p> <p>Note the following restrictions:</p> <ul style="list-style-type: none"> <li>• Match the regular expression:  <code>[a-z]([-a-z0-9]*[a-z0-9])?</code></li> </ul> <p>This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.</p> <ul style="list-style-type: none"> <li>• We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to <a href="#">Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24</a> to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.</li> </ul> <p>All VRFs are assigned a <code>vrfEncoded</code> value. If the Tenant and VRF name combination has more than 32 characters, then a VRF name (which also contains the tenant name) is identified in the cloud router using the <code>vrfEncoded</code> value. To see the <code>vrfEncoded</code> value, navigate to <b>Application Management &gt; VRFs</b> subtab. Click a VRF on the right hand pane and look for <i>Encoded VRF Name in Cloud Router</i>.</p>

Properties	Description
<b>Tenant</b>	To choose a tenant: <ol style="list-style-type: none"> <li>a. Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>b. From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column then click <b>Select</b>. You return to the <b>Create VRF</b> dialog box.</li> </ol>
<b>Description</b>	Enter a description of the VRF.

**Step 5** When finished, click **Save**.

## Creating an External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI

This procedure describes how to create an external network. You can have a single external network that can connect to multiple routers on the on-premises site, or you can have multiple external networks with multiple VRFs that you can use to connect to CCRs.

### Before you begin

You must have a hub network created before you can create an external network.

- Step 1** In the left navigation bar, navigate to **Application Management > External Networks**. The configured external networks are displayed. Note that because Cisco Cloud APIC supports only one hub network, you will see only one hub network displayed in the **Hub Network** column.
- Step 2** Click **Actions**, then choose **Create External Network**. The **Create External Network** window appears.
- Note** If there is no hub network configured yet, you will see a warning at the top of the page, saying that you must create a hub network before you can create an external network. Click the blue **cloud APIC Setup** link in the message to create a hub network, then return here. For more information on creating a hub network, see the "Configuring Cisco Cloud APIC Using the Setup Wizard" chapter in the [Cisco Cloud APIC for Google Cloud Installation Guide](#), Release 25.0(x) or later.
- Step 3** Enter the appropriate values in each field as listed in the following *Create External Network Dialog Box Fields* table then continue.

**Table 9: Create External Network Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name for the external network.

Properties	Description
<b>VRF</b>	<p>This external VRF will be used for external connectivity with the on-premises CCR. You can create multiple external VRFs for this purpose.</p> <p>This VRF will be identified as an external VRF if the VRF has all three of the following characteristics:</p> <ul style="list-style-type: none"> <li>• Configured under the <code>infra</code> tenant</li> <li>• Associated with an external network</li> <li>• Not associated with a cloud context profile</li> </ul> <p>Any VRF that is associated with an external network becomes an external VRF. At that point, that external VRF is not allowed to be created under any tenant other than the <code>infra</code> tenant, and that external VRF is not allowed to be associated with a cloud context profile or subnet.</p> <p>To choose an external VRF:</p> <ol style="list-style-type: none"> <li>Click <b>Select VRF</b>. The <b>Select VRF</b> dialog box appears.</li> <li>From the <b>Select VRF</b> dialog, click to choose a VRF in the left column. You can also create a VRF using the + <b>Create VRF</b> option.</li> <li>Click <b>Select</b>. You return to the <b>Create External Network</b> dialog box.</li> </ol>
<b>Hub Network</b>	<p>The hub network is displayed automatically after you configured it in the First Time Setup.</p> <p><b>Note</b> If there is no hub network configured yet, you must create a hub network before you can create an external network. For more information on creating a hub network, see the "Configuring Cisco Cloud APIC Using the Setup Wizard" chapter in the <a href="#">Cisco Cloud APIC for Google Cloud Installation Guide</a>, Release 25.0(x) or later.</p>
<b>VPN Router</b>	This field is not editable. The default VPN router is automatically selected.
<b>Settings</b>	
<b>Regions</b>	<p>To choose a region:</p> <ol style="list-style-type: none"> <li>Click <b>Add Regions</b>. The <b>Select Regions</b> dialog box appears. <ul style="list-style-type: none"> <li>• The regions that you selected as part of the First Time Setup are displayed here.</li> <li>• You can select multiple regions to bring up the cloud router in multiple regions.</li> </ul> </li> <li>From the <b>Select Regions</b> dialog, click to choose a region in the left column then click <b>Select</b>. You return to the <b>Create External Network</b> dialog box.</li> </ol>

Properties	Description
<p><b>VPN Networks</b></p>	<p>The VPN networks entries are used for internal connectivity. All configured VPN networks will be applied to all the selected regions.</p> <p>To add a VPN network:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add VPN Network</b>. The <b>Add VPN Network</b> dialog box appears.</li> <li>b. In the <b>Name</b> field, enter a name for the VPN network.</li> <li>c. Click <b>+ Add IPSec Peer</b>. Two tunnels are created for each IPSec peer entry.</li> <li>d. Enter values for the following fields for the IPSec peer that you want to add: <ul style="list-style-type: none"> <li>• <b>Public IP of IPSec Tunnel Peer</b></li> <li>• <b>Pre-Shared Key</b></li> <li>• <b>IKE Version:</b> Select <b>ikev1</b> or <b>ikev2</b> for IPSec tunnel connectivity</li> <li>• <b>BGP Peer ASN</b></li> <li>• <b>Subnet Pool Name:</b> Click <b>Select Subnet Pool Name</b>. The <b>Select Subnet Pool Name</b> dialog box appears. Select one of the available subnet pools that are listed, then click <b>Select</b>.</li> </ul> <p><b>Note</b> Additional IPsec tunnel subnet pools can be added in the <b>External Networks</b> page, or through the Cloud APIC First Time Set Up, if necessary. For more information on adding additional subnet pools through the Cloud APIC First Time Set Up, see the chapter "Configuring Cisco Cloud Network Controller Using the Setup Wizard" in the <i>Cisco Cloud APIC for GCP Installation Guide</i>, Release 25.0(1)- 25.0(4). The subnet pool size should be large enough to accommodate the number of IPsec tunnels that will get created.</p> </li> <li>e. Click the checkmark to add this IPSec tunnel. Click <b>+ Add IPSec Tunnel</b> if you want to add another IPSec tunnel.</li> <li>f. Click <b>Add</b> in the <b>Add VPN Network</b> dialog box. You return to the <b>Create External Network</b> dialog box.</li> </ol>

- Step 4** When you have finished creating the external network, click **Save**.  
After you click **Save** in the **Create External Network** window, cloud routers are then configured in Google Cloud.
- To verify that cloud routers were configured in Google Cloud, in your Google Cloud account, navigate to **Hybrid Connectivity > Cloud Routers**. You should see the cloud routers created for the different regions (note that you might have to click Refresh to bring up the newly-configured cloud routers).
- To see the IPSec sessions, navigate to **Hybrid Connectivity > VPN > Cloud VPN Tunnels**.

## Configuring Inter-VRF Route Leaking Using the Cisco Cloud APIC GUI

Using inter-VRF route leaking, you can configure an independent routing policy to specify which routes to leak between a pair of VRFs when you are setting up routing between these types of sites:

- Two cloud sites
- A cloud site and a non-ACI on-premises site



**Note** See [Configuring Routing and Security Policies Separately, on page 16](#) for more information.

- Step 1** In the left navigation bar, navigate to **Application Management > VRFs**.  
The configured VRFs are displayed.
- Step 2** Click the **Leak Routes** tab.  
Any already-configured leak routes are displayed.
- Step 3** Click **Actions**, then choose **Create Leak Route**.  
The **Create Leak Route** window appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Leak Routes Dialog Box Fields* table then continue.

**Table 10: Create Leak Routes Dialog Box Fields**

Properties	Description
Source VRF	<p>To choose a source VRF:</p> <ol style="list-style-type: none"> <li>Click <b>Select a Source VRF</b>. The <b>Select a VRF</b> dialog box appears.</li> <li>From the <b>Select a VRF</b> dialog, click to choose a VRF in the left column to use for the source VRF. Note that the source VRF can be an internal or an external (transport) VRF.</li> <li>Click <b>Select</b> to select this source VRF. You return to the <b>Create Leak Route</b> dialog box.</li> </ol>
Destination VRF	<p>To choose a destination VRF:</p> <ol style="list-style-type: none"> <li>Click <b>Select a Destination VRF</b>. The <b>Select a VRF</b> dialog box appears.</li> <li>From the <b>Select a VRF</b> dialog, click to choose a VRF in the left column to use for the destination VRF.</li> <li>Click <b>Select</b> to select this destination VRF. You return to the <b>Create Leak Route</b> dialog box.</li> </ol>

Properties	Description
Type	<p>Choose the type of leaked route that you want to configure:</p> <ul style="list-style-type: none"> <li>• <b>Leak All:</b> Select to configure all routes to leak between the VRFs. The entry 0.0.0.0/0 is entered automatically in the subnet IP area by default in this case.</li> <li>• <b>Subnet IP:</b> Select to configure a specific subnet IP address as the route to leak between VRFs. The <b>Subnet IP</b> box appears. In the <b>Subnet IP</b> box, enter a subnet IP address as the route to leak between VRFs. To configure multiple subnet IP addresses as the route to leak between VRFs, enter additional entries for the different subnets.</li> </ul>

**Step 5** When finished, click **Save**.  
The **Success** window appears.

**Step 6** Determine if you want to configure additional inter-VRF route leaking.

- If you want to add another route to leak between a pair of VRFs, click the **Add Another Route** option in the **Success** window.

You are returned to the **Add Leak Route** window. Repeat [Step 4, on page 54](#) through [Step 5, on page 55](#) to configure another route to leak between a pair of VRFs.

- If you want to add a reverse route, where:
  - The destination VRF from the previous configuration now becomes the source VRF, and
  - The source VRF from the previous configuration now becomes the destination VRF

Then click the **Add Reverse Route** option in the **Success** window.

You are returned to the **Add Leak Route** window. Repeat [Step 4, on page 54](#) through [Step 5, on page 55](#) to configure another route, but this time:

- In the **Source VRF** field, select the VRF that you had selected as a destination VRF in the previous configuration.
- In the **Destination VRF** field, select the VRF that you had selected as a source VRF in the previous configuration.

**Step 7** When you have finished configuring leak routes, click **Done**.

The **Leak Routes** tab in the main **VRFs** page is displayed again, with the newly configured leak route displayed.

**Step 8** To get more information on a source or destination VRF, or to make changes to a configured leak route, double-click the VRF in the **Leak Routes** tab in the main **VRFs** page.  
The **Overview** page for that VRF is displayed.

**Step 9** Click the **Application Management** tab at the top of the VRF page, then click the **Leak Routes** tab in the left nav bar.  
The leak routes associated with this particular VRF are displayed.

**Step 10** Configure additional leak routes associated with this VRF, if necessary.

- To add a leak route from this VRF, click **Actions**, then choose **Add Leak Route from <VRF\_name>**.

The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in [Step 4, on page 54](#). Note that the entry in the **Source VRF** is pre-selected and cannot be changed in this situation.

- To add a leak route to this VRF, click **Actions**, then choose **Add Leak Route to <VRF\_name>**.

The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in [Step 4, on page 54](#). Note that the entry in the **Destination VRF** is pre-selected and cannot be changed in this situation.

## Enabling Connectivity Between Google Cloud and External Devices

Follow these procedures to manually enable connectivity between a Google Cloud Router and an external device.

### Downloading the External Device Configuration Files

- 
- Step 1** In the Cisco Cloud APIC GUI, click on **Dashboard**.  
The **Dashboard** view for the Cisco Cloud APIC appears.
- Step 2** In the **Connectivity** area, under **External Connectivity Status**, click on the number above the **Cloud Routers** entry.  
The **External Connectivity** window appears.
- Step 3** Click **Actions > Download External Device Configuration Files**.  
The **Download External Device Configuration Files** pop-up appears.
- Step 4** Select the external device configuration files to download and click **Download**.  
This action downloads a zip file that contains configuration information that you will use to enable connectivity between the Google Cloud Router and the external devices.
- 

## Enabling Connectivity Between Google Cloud and the External Devices

### Before you begin

Download the external device configuration files using the procedures in [Downloading the External Device Configuration Files, on page 56](#).

- 
- Step 1** Gather the necessary information that you will need to enable connectivity between the Google Cloud Router and the external devices.
- Step 2** Log into the external device.
- Step 3** Enter the configuration information to connect an external networking device with the cloud ACI fabric.

If you downloaded the external device configuration files using the instructions in [Downloading the External Device Configuration Files, on page 56](#), locate the configuration information for the first tunnel and enter that configuration information.

Following is an example of what the external device configuration file might look like for the first tunnel, where **PRESHARED-KEY** is taken from the vpn-connectivity configuration page:



```

! The following file contains configuration recommendation to connect an external networking device
! with the cloud ACI Fabric
! The configurations here are provided for an IOS-XE based device. The user is expected to understand
! the configs and make any necessary amends before using them
! on the external device. Cisco does not assume any responsibility for the correctness of the config.

! Tunnel to 54.215.245.58 5.500 for
hextwTunIf.act-[infra]/region-[us-west1]/hcloudHubCtx-[1]-id-[0]/ext-[extwTunIf_us-west1]/vpr-[vprwTunIf]/itr-default-peer-54.215.245.58/src-1-dest-[54.215.245.58]
! USER-DEFINED: please define rd: RD
! USER-DEFINED: please provide preshared-key: PRESHARED-KEY
! USER-DEFINED: please define router-id: ROUTER-ID
! USER-DEFINED: please define gig-number: GIG-NUMBER
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! ikev: ikev2
! vrf-name: extv1
! user name: root
! tunnel counter: 5
! IPV4 address: 35.220.50.132
! tunnel interface destination: 54.215.245.58
! tunne id: 500
! BGP peer address: 169.254.10.6
! BGP peer neighbor address: 169.254.10.5
! BGP peer ASN: 64513
! hcloudHubCtx ASN: 64512

vrf definition extv1
  rd RD:1
  address-family ipv4
  exit-address-family
exit

interface Loopback0
  vrf forwarding extv1
  ip address 41.41.41.41 255.255.255.255
exit

crypto ikev2 proposal ikev2-1
  encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
  integrity sha512 sha384 sha256 sha1
  group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-1
  proposal ikev2-1
exit

crypto ikev2 keyring keyring-root-5
  peer peer-ikev2-keyring
  address 35.220.50.132
  pre-shared-key PRESHARED-KEY
  exit
exit

crypto ikev2 profile ikev-profile-root-5
  match address local interface GIG-NUMBER
  match identity remote address 35.220.50.132 255.255.255.255
  identity local address 54.215.245.58
  authentication remote pre-share
  authentication local pre-share
  keyring local keyring-root-5
  lifetime 3600
  dpd 10 5 periodic

```

```

exit

crypto ipsec transform-set ikev-transport-root-5 esp-gcm 256
  mode tunnel
exit

crypto ipsec profile ikev-profile-root-5
  set transform-set ikev-transport-root-5
  set pfs group14
  set ikev2-profile ikev-profile-root-5
exit

interface Tunnel500
  vrf forwarding extv1
  ip address 169.254.10.6 255.255.255.252
  ip mtu 1400
  ip tcp adjust-mss 1400
  tunnel source GIG-NUMBER
  tunnel mode ipsec ipv4
  tunnel destination 35.220.50.132
  tunnel protection ipsec profile ikev-profile-root-5
exit

ip route 35.220.50.132 255.255.255.255 GIG-NUMBER GIG-GATEWAY

router bgp 64513
  bgp router-id ROUTER-ID
  bgp log-neighbor-changes

  address-family ipv4 vrf extv1
    network 41.41.41.41 mask 255.255.255.255
    neighbor 169.254.10.5 remote-as 64512
    neighbor 169.254.10.5 ebgp-multihop 255
    neighbor 169.254.10.5 activate
  exit-address-family
exit

```

The following figures provide more information on what each set of fields is used for in the external device configuration file:

- The fields shown in the following figure are used to configure these areas:
  - VRF definition
  - IPSec global configurations

```
vrf definition Ext-V1
rd 1:10
!
address-family ipv4
  route-target export 64550:10
  route-target import 64550:10
!
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
lifetime 28800
!
crypto isakmp keepalive 10 10 periodic
crypto isakmp aggressive-mode disable
!
```

VRF Definition

IPSec Global Configurations

- The fields shown in the following figure are used to configure these areas:
  - IPSec and ikev1 per tunnel configurations
  - BGP configurations for the VRF neighbor

```
!
crypto keyring Ext-V1-1000-ike
pre-shared-key address <50.18.55.126>[cAPIC CSR GIG3 Public IP] key <abodefg12345>
!
crypto isakmp profile Ext-V1-1000-ike
  keyring Ext-V1-1000-ike
  match identity address <50.18.55.126>[cAPIC CSR1 gig3 Public IP] 255.255.255.255
!
crypto ipsec transform-set Ext-V1-1000-ike esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile Ext-V1-1000-ike
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set Ext-V1-1000-ike
set pfs group14
!
interface Tunnel1000
vrf forwarding Ext-V1
ip address 50.50.0.2[cAPIC CSR BGP Peer Addr] 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1400
tunnel source GigabitEthernet2
tunnel mode ipsec ipv4
tunnel destination <50.18.55.126>[cAPIC CSR1 gig3 Public IP]
tunnel protection ipsec profile Ext-V1-1000-ike
!
router bgp 64550
!
address-family ipv4 vrf Ext-V1
redistribute connected
neighbor <50.50.0.1>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
neighbor 50.50.0.1 ebgp-multihop 255
neighbor 50.50.0.1 activate
neighbor 50.50.0.1 send-community both
neighbor <50.50.0.5>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
neighbor 50.50.0.5 ebgp-multihop 255
neighbor 50.50.0.5 activate
neighbor 50.50.0.5 send-community both
distance bgp 20 200 20
!
ip route 50.18.55.126[cAPIC CSR1 gig3 Public IP] 255.255.255.255 GigabitEthernet2 10.10.0.103
```

IPSec and Ikev1  
Per Tunnel Configurations

BGP Configurations for VRF Neighbor

- The fields shown in the following figure are used to configure these areas:
  - Ikev2 global configurations
  - IPSec and ikev2 per tunnel configurations

```

crypto ikev2 proposal ikev2-1
  encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
  integrity sha512 sha384 sha256 sha1
  group 24 21 20 19 16 15 14 2
  !
crypto ikev2 policy ikev2-1
  proposal ikev2-1
  !
crypto ikev2 keyring keyring-ikev2-2000
peer peer-ikev2-keyring
  address 35.81.94.248 [cAPIC CSR1 gig3 Public IP]
  pre-shared-key abcdefgl2345
  !
crypto ikev2 profile ikev2-2000
  match address local interface GigabitEthernet3
  match identity remote address 35.81.94.248[cAPIC CSR1 gig3 Public IP] 255.255.255.255
  identity local address 52.53.49.193 [Local Device tunnel source interface Public IP (Gig3 public IP)]
  authentication remote pre-share
  authentication local pre-share
  keyring local keyring-ikev2-2000
  lifetime 3600
  dpd 10 5 on-demand
  !
crypto ipsec transform-set ikev2-2000 esp-gcm 256
  mode tunnel
  !
crypto ipsec profile ikev2-2000
  set transform-set ikev2-2000
  set pfs group14
  set ikev2-profile ikev2-2000
  !
interface Tunnel2000
  vrf forwarding Ext-V1
  ip address 50.50.0.14 [cAPIC CSR1 BGP Peer Addr] 255.255.255.252
  ip mtu 1400
  ip tcp adjust-mss 1400
  tunnel source GigabitEthernet3
  tunnel mode ipsec ipv4
  tunnel destination 35.81.94.248[cAPIC CSR1 gig3 Public IP]
  tunnel protection ipsec profile ikev2-2000

```

Ikev2 Global Configurations

IPSec and Ikev2  
Per Tunnel Configurations

## Creating an EPG Using the Cisco Cloud APIC GUI

Use the procedures in this section to create an application EPG or an external EPG. The available configuration options vary, depending on which type of EPG you are creating.

### Creating an Application EPG Using the Cisco Cloud APIC GUI

This section explains how to create an application EPG using the Cisco Cloud APIC GUI. Each service needs at least one consumer EPG and one provider EPG.

#### Before you begin

Create an application profile and a VRF.

- 
- Step 1** Click the **Intent** icon.  
The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Create EPG**.  
The **Create EPG** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create EPG Dialog Box Fields* table then continue.

Table 11: Create EPG Dialog Box Fields

Properties	Description
<b>General</b>	
<b>Name</b>	<p>Enter the name of the EPG.</p> <p>Note the following restrictions:</p> <ul style="list-style-type: none"> <li>Match the regular expression:  <code>[a-z]([-a-z0-9]*[a-z0-9])?</code></li> </ul> <p>This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.</p> <ul style="list-style-type: none"> <li>We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to <a href="#">Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24</a> to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.</li> </ul>
<b>Tenant</b>	<p>To choose a tenant:</p> <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column.</li> <li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ol>
<b>Application Profile</b>	<p>To choose an application profile:</p> <ol style="list-style-type: none"> <li>Click <b>Select Application Profile</b>. The <b>Select Application Profile</b> dialog box appears.</li> <li>From the <b>Select Application Profile</b> dialog, click to choose an application profile in the left column. <ul style="list-style-type: none"> <li><b>Note</b> If you are creating an EPG in the infra tenant, we recommend that you do not choose the <code>cloud-infra</code> application profile because that application profile is used by EPGs in the overlay-1 VRF. Select a different application profile or click <b>Create Application Profile</b> to create a new one.</li> </ul> </li> <li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ol>
<b>Description</b>	Enter a description of the EPG.
<b>Settings</b>	
<b>Type</b>	Because this will be an application EPG, choose <b>Application</b> as the EPG type.
<b>VRF</b>	<p>To choose a VRF:</p> <ol style="list-style-type: none"> <li>Click <b>Select VRF</b>. The <b>Select VRF</b> dialog box appears.</li> <li>From the <b>Select VRF</b> dialog, click to choose a VRF in the left column.</li> <li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ol>

Properties	Description
Endpoint Selectors	

Properties	Description
	<p><b>Note</b> See <a href="#">Configuring Virtual Machines in Google Cloud, on page 76</a> for instructions on configuring virtual machines in Google Cloud as part of the endpoint selector configuration process.</p> <p>To add an endpoint selector:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add Endpoint Selector</b> to open the <b>Add Endpoint Selector</b> dialog.</li> <li>b. In the <b>Add Endpoint Selector</b> dialog, enter a name in the <b>Name</b> field.</li> <li>c. Click <b>Selector Expression</b>. The <b>Key</b>, <b>Operator</b>, and <b>Value</b> fields are enabled.</li> <li>d. Click the <b>Key</b> drop-down list to choose a key. The options are: <ul style="list-style-type: none"> <li>• Choose <b>IP</b> if you want to use an IP address or subnet for the endpoint selector.</li> <li>• Choose <b>Region</b> if you want to use the Google Cloud region for the endpoint selector.</li> <li>• Choose <b>Custom</b> if you want to create a custom key for the endpoint selector.</li> </ul> <p><b>Note</b> When choosing the <b>Custom</b> option, the drop-down list becomes a text box. You need to enter a name for the key in the spaces after <b>custom:</b> (for example, <b>custom: Location</b>).</p> </li> <li>e. Click the <b>Operator</b> drop-down list to choose an operator. The options are: <ul style="list-style-type: none"> <li>• <b>equals</b>: Used when you have a single value in the Value field.</li> <li>• <b>not equals</b>: Used when you have a single value in the Value field.</li> <li>• <b>in</b>: Used when you have multiple comma-separated values in the Value field.</li> <li>• <b>not in</b>: Used when you have multiple comma-separated values in the Value field.</li> <li>• <b>has key</b>: Used if the expression contains only a key.</li> <li>• <b>does not have key</b>: Used for an expression that does not contain a key.</li> </ul> </li> <li>f. Enter a value in the <b>Value</b> field then click the check mark to validate the entries. The value you enter depends on the choices you made for the <b>Key</b> and <b>Operator</b> fields. For example, if the <b>Key</b> field is set to <b>IP</b> and the <b>Operator</b> field is set to <b>equals</b>, the <b>Value</b> field must be an IP address or subnet. However, if the <b>Operator</b> field is set to <b>has key</b>, the <b>Value</b> field is disabled.</li> <li>g. When finished, click the check mark to validate the selector expression.</li> <li>h. Determine if you want to create additional endpoint selector expressions to the endpoint selector. If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions.</li> </ol> <p>For example, assume you created two sets of expressions under a single endpoint selector:</p> <ul style="list-style-type: none"> <li>• Endpoint selector 1, expression 1: <ul style="list-style-type: none"> <li>• <b>Key</b>: Region</li> <li>• <b>Operator</b>: equals</li> <li>• <b>Value</b>: us-west1</li> </ul> </li> </ul>

Properties	Description
	<ul style="list-style-type: none"> <li>• Endpoint selector 1, expression 2:               <ul style="list-style-type: none"> <li>• <b>Key:</b> IP</li> <li>• <b>Operator:</b> equals</li> <li>• <b>Value:</b> 192.0.2.1/24</li> </ul> </li> </ul> <p>In this case, if <i>both</i> of these expressions are true (if the region is us-west1 AND if the IP address belongs to subnet 192.0.2.1/24), then that endpoint is assigned to the Cloud EPG.</p> <p>i. Click the check mark after every additional expression that you want to create under this endpoint selector then click <b>Add</b> when finished.</p> <p>If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you had created endpoint selector 1 as described in the previous step, and then you created a second endpoint selector as described below:</p> <ul style="list-style-type: none"> <li>• Endpoint selector 2, expression 1:               <ul style="list-style-type: none"> <li>• <b>Key:</b> Region</li> <li>• <b>Operator:</b> in</li> <li>• <b>Value:</b> us-east1, us-central1</li> </ul> </li> </ul> <p>In this case:</p> <ul style="list-style-type: none"> <li>• If the region is us-west1 AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions)</li> </ul> <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> <li>• If the region is either us-east1 or us-central1 (endpoint selector 2 expression)</li> </ul> <p>Then that end point is assigned to the Cloud EPG.</p>

**Step 5** Click **Save** when finished.

## Creating an External EPG Using the Cisco Cloud APIC GUI

This section explains how to create an external EPG using the Cisco Cloud APIC GUI. Each service needs at least one consumer EPG and one provider EPG.

### Before you begin

Create an application profile and a VRF.

**Step 1** Click the **Intent** icon.

The **Intent** menu appears.



**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

**Step 3** From the **Application Management** list in the **Intent** menu, click **Create EPG**.

The **Create EPG** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create EPG Dialog Box Fields* table then continue.

**Table 12: Create EPG Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	<p>Enter the name of the EPG.</p> <p>Note the following restrictions:</p> <ul style="list-style-type: none"> <li>Match the regular expression:  <code>[a-z]([-a-z0-9]*[a-z0-9])?</code></li> </ul> <p>This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.</p> <ul style="list-style-type: none"> <li>We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to <a href="#">Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24</a> to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.</li> </ul>
<b>Tenant</b>	<p>To choose a tenant:</p> <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column.</li> <li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ol>
<b>Application Profile</b>	<p>To choose an application profile:</p> <ol style="list-style-type: none"> <li>Click <b>Select Application Profile</b>. The <b>Select Application Profile</b> dialog box appears.</li> <li>From the <b>Select Application Profile</b> dialog, click to choose an application profile in the left column.</li> </ol> <p><b>Note</b> If you are creating an EPG in the infra tenant, we recommend that you do not choose the <code>cloud-infra</code> application profile because that application profile is used by EPGs in the overlay-1 VRF. Select a different application profile or click <b>Create Application Profile</b> to create a new one.</p> <ol style="list-style-type: none"> <li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ol>
<b>Description</b>	Enter a description of the EPG.
<b>Settings</b>	
<b>Type</b>	Because this will be an external EPG, choose <b>External</b> as the EPG type.

Properties	Description
<b>VRF</b>	<p>To choose a VRF:</p> <ol style="list-style-type: none"> <li>a. Click <b>Select VRF</b>. The <b>Select VRF</b> dialog box appears.</li> <li>b. From the <b>Select VRF</b> dialog, click to choose a VRF in the left column.</li> <li>c. Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ol>
<b>Route Reachability</b>	<p>The type of route reachability for the external EPG will be automatically selected (either <b>Internet</b> or <b>External-Site</b>).</p>
<b>Endpoint Selectors</b>	<p><b>Note</b> See <a href="#">Configuring Virtual Machines in Google Cloud, on page 76</a> for instructions on configuring virtual machines in Google Cloud as part of the endpoint selector configuration process.</p> <p>To add an endpoint selector:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add Endpoint Selector</b> to add an endpoint selector.</li> <li>b. Enter a name in the <b>Name</b> field.</li> <li>c. Enter a subnet in the <b>Subnet</b>.</li> <li>d. When finished, click the check mark to validate the endpoint selector.</li> <li>e. Determine if you want to create additional endpoint selectors.</li> </ol> <p>If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you created two endpoint selectors:</p> <ul style="list-style-type: none"> <li>• Endpoint selector 1: <ul style="list-style-type: none"> <li>• <b>Name:</b> EP_Sel_1</li> <li>• <b>Subnet:</b> 192.1.1.1/24</li> </ul> </li> <li>• Endpoint selector 2: <ul style="list-style-type: none"> <li>• <b>Name:</b> EP_Sel_2</li> <li>• <b>Subnet:</b> 192.2.2.2/24</li> </ul> </li> </ul> <p>In this case:</p> <ul style="list-style-type: none"> <li>• If the IP address belongs to the 192.1.1.1/24 subnet (endpoint selector 1)</li> </ul> <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> <li>• If the IP address belongs to the 192.2.2.2/24 subnet (endpoint selector 2)</li> </ul> <p>Then that end point is assigned to the Cloud EPG.</p>

**Step 5** Click **Save** when finished.

## Creating a Filter Using the Cisco Cloud APIC GUI

This section explains how to create a filter using the Cisco Cloud APIC GUI.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

**Step 3** From the **Application Management** list in the **Intent** menu, click **Create Filter**. The **Create Filter** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Filter Dialog Box Fields* table then continue.

**Table 13: Create Filter Dialog Box Fields**

Properties	Description
Name	Enter a name for the filter in the <b>Name</b> field.
Tenant	To choose a tenant: <b>a.</b> Click <b>Select Tenant</b> . The <b>Select Tenant</b> dialog box appears. <b>b.</b> From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column then click <b>Select</b> . You return to the <b>Create Filter</b> dialog box.
Description	Enter a description of the filter.

Properties	Description
<b>Add Filter</b>	<p>To add a filter:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add Filter Entry</b>. The <b>Add Filter Entry</b> dialog box appears.</li> <li>b. Enter a name for the filter entry in the <b>Name</b> field.</li> <li>c. Click the <b>Ethernet Type</b> drop-down list to choose an ethernet type. The options are: <ul style="list-style-type: none"> <li>• <b>IP</b></li> <li>• <b>Unspecified</b></li> </ul> <p><b>Note</b> When <b>Unspecified</b> is chosen, any traffic type is allowed, including IP, and the remaining fields are disabled.</p> </li> <li>d. Click the <b>IP Protocol</b> drop-down menu to choose a protocol. The options are: <ul style="list-style-type: none"> <li>• <b>ICMP</b></li> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> <li>• <b>Unspecified</b></li> </ul> <p><b>Note</b> The remaining fields are enabled only when <b>TCP</b> or <b>UDP</b> is chosen.</p> </li> <li>e. Enter the appropriate port range information in the <b>Destination Port</b> fields.</li> <li>f. When finished entering filter entry information, click <b>Add</b>. You return to the <b>Create Filter</b> dialog box where you can repeat the steps to add another filter entry.</li> </ol>

**Step 5** When finished, click **Save**.

## Creating a Contract Using the Cisco Cloud APIC GUI

This section explains how to create a contract using the Cisco Cloud APIC GUI.

### Before you begin

Create filters.

- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Create Contract**. The **Create Contract** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Contract Dialog Box Fields* table then continue.

**Table 14: Create Contract Dialog Box Fields**

Properties	Description
<b>Name</b>	<p>Enter the name of the contract.</p> <p>Note the following restrictions:</p> <ul style="list-style-type: none"> <li>Match the regular expression:  <math>[a-z]([-a-z0-9]*[a-z0-9])?</math></li> </ul> <p>This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.</p> <ul style="list-style-type: none"> <li>We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to <a href="#">Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24</a> to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.</li> </ul>
<b>Tenant</b>	<p>To choose a tenant:</p> <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column.</li> <li>Click <b>Select</b>. You return to the <b>Create Contract</b> dialog box.</li> </ol>
<b>Description</b>	Enter a description of the contract.
<b>Settings</b>	

Properties	Description
Scope	<p>The scope limits the contract to any endpoint groups within the same application profile, within the same VRF instance, throughout the fabric (globally), or within the same tenant.</p> <p><b>Note</b> Shared services enables communication between EPGs in different tenants and between EPGs in different VRFs.</p> <p>To enable EPGs in one tenant to communicate with EPGs in another tenant, choose <b>Global</b> scope.</p> <p>To enable an EPG in one VRF to communicate with another EPG in a different VRF, choose <b>Global</b> or <b>Tenant</b> scope.</p> <p>Click the drop-down arrow to choose from the following scope options:</p> <ul style="list-style-type: none"> <li>• <b>Application Profile</b></li> <li>• <b>VRF</b></li> <li>• <b>Global</b></li> <li>• <b>Tenant</b></li> </ul>
Add Filter	<p>To choose a filter:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add Filter</b>. The filter row appears with a <b>Select Filter</b> option.</li> <li>b. Click <b>Select Filter</b>. The <b>Select Filter</b> dialog box appears.</li> <li>c. From the <b>Select Filter</b> dialog, click to choose a filter in the left column then click <b>Select</b>. You return to the <b>Create Contract</b> dialog box.</li> </ol>

**Step 5** Click **Save** when finished.

## Creating an Inter-Tenant Contract Using the Cisco Cloud APIC GUI

This section explains how to create an inter-tenant contract using the Cisco Cloud APIC GUI.

### Before you begin

Create filters.

- 
- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Create Contract**. The **Create Contract** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Contract Dialog Box Fields* table then continue.

Table 15: Create Contract Dialog Box Fields

Properties	Description
<b>Name</b>	<p>Enter the name of the contract.</p> <p>This is the name of the contract in Google Cloud. Match the regular expression:</p> <pre>[a-z]([-a-z0-9]*[a-z0-9])?</pre> <p>This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.</p>
<b>Tenant</b>	<p>To choose a tenant:</p> <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column.</li> <li>Click <b>Select</b>. You return to the <b>Create Contract</b> dialog box.</li> </ol>
<b>Description</b>	Enter a description of the contract.
<b>Settings</b>	
<b>Scope</b>	<p>The scope limits the contract to any endpoint groups within the same application profile, within the same VRF instance, throughout the fabric (globally), or within the same tenant.</p> <p>For inter-tenant communication, you will first create a contract with the <b>Global</b> scope in one of the tenants (for example, <b>tenant1</b>). This tenant's EPG will always be the provider of this contract.</p> <p>This contract will then be exported to the other tenant (for example, <b>tenant2</b>). For the other tenant that imports this contract, its EPG will be the consumer of the imported contract. If you want tenant2's EPG to be the provider and tenant1's EPG to be the consumer, then create a contract in <b>tenant2</b> and then export it to <b>tenant1</b>.</p>
<b>Add Filter</b>	<p>To choose a filter:</p> <ol style="list-style-type: none"> <li>Click <b>Add Filter</b>. The filter row appears with a <b>Select Filter</b> option.</li> <li>Click <b>Select Filter</b>. The <b>Select Filter</b> dialog box appears.</li> <li>From the <b>Select Filter</b> dialog, click to choose a filter in the left column then click <b>Select</b>. You return to the <b>Create Contract</b> dialog box.</li> </ol>

**Step 5** Click **Save** when finished.

**Step 6** Export the contract that you just created to another tenant.

For example, assume the following:

- The contract that you created in the procedure above is named **contract1** in tenant **tenant1**.
- The contract that you want to export is named **exported\_contract1** and you are exporting it to tenant **tenant2**.

a) Navigate to the Contracts page (**Application Management > Contracts**).

The configured contracts are listed.

- b) Select the contract that you just created.  
For example, scroll through the list until you see the contract **contract1** and click the box next to it to select it.
- c) Go to **Actions > Export Contract**.  
The **Export Contract** window appears.
- d) Click **Select Tenant**.  
The **Select Tenant** window appears.
- e) Select the tenant that you want to export the contract to, then click **Save**.  
For example, **tenant2**. You are returned to the **Export Contract** window.
- f) In the **Name** field, enter a name for the exported contract.  
For example, **exported\_contract1**.
- g) In the **Description** field, enter a description for the exported contract, if necessary.
- h) Click **Save**.  
The list of contracts appears again.

**Step 7** Configure the first tenant's EPG as the provider EPG, with the original contract, as the first part of the EPG communication configuration.

- a) Click the **Intent** button, then choose **EPG Communication**.  
The **EPG Communication** window appears.
- b) Click **Let's Get Started**.
- c) In the **Contract** area, click **Select Contract**.  
The **Select Contract** window appears.
- d) Locate and select the contract that you created at the beginning of these procedures.  
In this example, you would locate and select **contract1**.
- e) Click **Select**.  
The **EPG Communication** window appears.
- f) In the **Provider EPGs** area, click **Add Provider EPGs**.  
The **Select Provider EPGs** window appears.
- g) Leave the **Keep selected items** box checked, then select the first tenant's (**tenant1**) EPG.
- h) Click **Select**.  
The **EPG Communication** window appears.
- i) Click **Save**.

**Step 8** Configure the second tenant's EPG as the consumer EPG, with the exported contract, as the second part of the EPG communication configuration.

- a) Click the **Intent** button, then choose **EPG Communication**.  
The **EPG Communication** window appears.
- b) Click **Let's Get Started**.



- c) In the **Contract** area, click **Select Contract**.  
The **Select Contract** window appears.
  - d) Locate and select the contract that you created at the beginning of these procedures.  
In this example, you would locate and select **exported\_contract1**.
  - e) Click **Select**.  
The **EPG Communication** window appears.
  - f) In the **Consumer EPGs** area, click **Add Consumer EPGs**.  
The **Select Consumer EPGs** window appears.
  - g) Leave the **Keep selected items** box checked, then select the second tenant's (**tenant2**) EPG.
  - h) Click **Select**.  
The **EPG Communication** window appears.
  - i) Click **Save**.
- 

## Specifying Consumer and Provider EPGs Using the Cisco Cloud APIC

This section explains how to specify an EPG as a consumer or a provider.

### Before you begin

- You have configured a contract.
  - You have configured an EPG.
- 

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Configuration**.

A list of **Configuration** options appears in the **Intent** menu.

**Step 3** From the **Configuration** list in the **Intent** menu, click **EPG Communication**. The **EPG Communication** dialog box appears with the **Consumer EPGs**, **Contract**, and **Provider EPGs** information.

**Step 4** To choose a contract:

- a) Click **Select Contract**. The **Select Contract** dialog appears.
- b) In the pane on the left side of the **Select Contract** dialog, click to choose a contract then click **Select**. The **Select Contract** dialog box closes.

**Step 5** To add a consumer EPG:

- a) Click **Add Consumer EPGs**. The **Select Consumer EPGs** dialog appears.

**Note** EPGs within the tenant (where the contract is created) are displayed.

- b) In the pane on the left side of the **Select Consumer EPGs** dialog, click to place a check in a check box to choose an EPG.

- Step 6** To add a provider EPG:
- Click **Add Provider EPGs**. The **Select Provider EPGs** dialog appears.
 

**Note** EPGs within the tenant (where the contract is created) are displayed.
  - In the pane on the left side of the **Select Provider EPGs** dialog, click to place a check in a check box to choose a provider EPG.
 

**Note** If the chosen contract is an Imported Contract, the provider EPG selection is disabled.
  - When finished, click **Select**. The **Select Provider EPGs** dialog box closes, and you return to the **EPG Communication Configuration** window.
  - Click **Save**.

## Creating a Cloud Context Profile Using the Cisco Cloud APIC GUI

This section explains how to create a cloud context profile using the Cisco Cloud APIC GUI.

### Before you begin

Create a VRF.

- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Create Cloud Context Profile**. The **Create Cloud Context Profile** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Cloud Context Profile Dialog Box Fields* table then continue.

**Table 16: Create Cloud Context Profile Dialog Box Fields**

Properties	Description
<b>Name</b>	Enter the name of the cloud context profile. Match the regular expression:  [a-z]([-a-z0-9]*[a-z0-9])?  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.
<b>Tenant</b>	To choose a tenant: <b>a.</b> Click <b>Select Tenant</b> . The <b>Select Tenant</b> dialog box appears. <b>b.</b> From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column then click <b>Select</b> . You return to the <b>Create Cloud Context Profile</b> dialog box.
<b>Description</b>	Enter a description of the cloud context profile.

Properties	Description
<b>Settings</b>	
<b>Region</b>	To choose a region: <ol style="list-style-type: none"><li data-bbox="521 394 1208 426">a. Click <b>Select Region</b>. The <b>Select Region</b> dialog box appears.</li><li data-bbox="521 447 1520 510">b. From the <b>Select Region</b> dialog, click to choose a region in the left column then click <b>Select</b>. You return to the <b>Create Cloud Context Profile</b> dialog box.</li></ol>
<b>VRF</b>	To choose a VRF: <ol style="list-style-type: none"><li data-bbox="521 600 1159 632">a. Click <b>Select VRF</b>. The <b>Select VRF</b> dialog box appears.</li><li data-bbox="521 653 1520 716">b. From the <b>Select VRF</b> dialog box, click to choose a VRF in the left column then click <b>Select</b>. You return to the <b>Create Cloud Context Profile</b> dialog box.</li></ol>

Properties	Description
Add CIDR	<p><b>Note</b> See <a href="#">Understanding VPCs and Subnets Under Google Cloud and Cloud Context Profiles Under Cloud APIC, on page 20</a> for more information on primary and secondary CIDRs and subnet group labels.</p> <p>To add a CIDR:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add CIDR</b>. The <b>Add CIDR</b> dialog box appears.</li> <li>b. Enter the address in the <b>CIDR Block Range</b> field.</li> <li>c. Click to check (enabled) or uncheck (disabled) the <b>Primary</b> check box. <ul style="list-style-type: none"> <li>• You must have at least one primary CIDR added for each cloud context profile.</li> <li>• If you are adding additional secondary CIDRs and subnets for VPCs, leave the <b>Primary</b> box unchecked.</li> </ul> </li> <li>d. Click <b>Add Subnet</b> and enter the following information: <ul style="list-style-type: none"> <li>• In the <b>Address</b> field, enter the subnet address.</li> <li>• In the <b>Name</b> field, enter the name for this subnet.</li> <li>• In the <b>Subnet Group Label</b> field, choose one of the following: <ul style="list-style-type: none"> <li>• <b>Select Existing</b>: Click <b>Select Subnet Group Label</b>, then choose an existing subnet group label to associate with this subnet.</li> <li>• <b>Create New</b>: Enter a unique name for the subnet group label to associate with this subnet.</li> </ul> </li> </ul> </li> <li>e. In the <b>VRF</b> field, make a selection, if necessary. <ul style="list-style-type: none"> <li>• If you checked the box next to the <b>Primary</b> field, this CIDR is automatically associated with the primary VRF.</li> <li>• If you did not check the box next to the <b>Primary</b> field, you can associate this CIDR with a secondary VRF. Click the <b>X</b> next to the VRF, then click on <b>Select VRF</b> to select the secondary VRF to associate with this CIDR.</li> </ul> </li> <li>f. When finished, click <b>Add</b>.</li> </ol>

**Step 5** Click **Save** when finished.

## Configuring Virtual Machines in Google Cloud

When you configure endpoint selectors for Cisco Cloud APIC, you will also need to configure the virtual machines that you will need in Google Cloud that will correspond with the endpoint selectors that you configure for Cisco Cloud APIC.

This topic provides the requirements for configuring the virtual machines in Google Cloud. You can use these requirements to configure the virtual machines in Google Cloud either before you configure the endpoint selectors for Cisco Cloud APIC or afterward.

For example, assume that you are using **Custom** as the type of endpoint selector, as described in [Endpoints and Endpoint Selectors, on page 18](#).

- You might go to your account in Google Cloud and create a custom tag or label in Google Cloud first, then create an endpoint selector using a custom tag or label in Cisco Cloud APIC afterward.
- Or you might create an endpoint selector using a custom tag or label in Cisco Cloud APIC first, then go to your account in Google Cloud and create a custom tag or label in Google Cloud afterward.

### Before you begin

You must configure a cloud context profile as part of the Google Cloud virtual machine configuration process. When you configure a cloud context profile, the configurations, such as the VRF and region settings, are pushed out to Google Cloud afterward.

---

**Step 1** Review your cloud context profile configuration to get the following information:

- VRF name
- Subnet information
- Google Cloud Project ID
- The resource group that corresponds to where the cloud context profile is deployed.

**Note** In addition to the information above, if you are using tag-based EPGs, you also need to know the tag names. The tag names are not available in the cloud context profile configuration.

To obtain the cloud context profile configuration information:

a) From the **Navigation** menu, choose the **Application Management** tab.

When the **Application Management** tab expands, a list of subtab options appear.

b) Choose the **Cloud Context Profiles** subtab option.

A list of the cloud context profiles that you have created for your Cisco Cloud APIC are displayed.

c) Select the cloud context profile that you will use as part of this Google Cloud virtual machine configuration process.

Various configuration parameters are displayed for this cloud context profile, such as the region, VRF, IP address and subnets. Use the information displayed in this window when you configure the Google Cloud virtual machine.

**Step 2** Log in to the Google Cloud portal account for the Cisco Cloud APIC user tenant and begin creating an Google Cloud VM using the information you gathered from the cloud context profile configuration.

**Note** For information about how to create the VM in the Google Cloud portal, see the Google Cloud documentation.

---

## Creating a Backup Configuration Using the Cisco Cloud APIC GUI

This section explains how to create a backup configuration.

### Before you begin

Create a remote location and a scheduler, if needed.

- 
- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Operations**.  
A list of **Operations** options appear in the **Intent** menu.
- Step 3** From the **Operations** list in the **Intent** menu, click **Create Backup Configuration**. The **Create Backup Configuration** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Backup Configuration Dialog Box Fields* table then continue.

**Table 17: Create Backup Configuration Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the backup configuration.
<b>Description</b>	Enter a description of the backup configuration.
<b>Settings</b>	
<b>Backup Destination</b>	Choose a backup destination. <ul style="list-style-type: none"> <li>• <b>Local</b></li> <li>• <b>Remote</b></li> </ul>

Properties	Description
<b>Backup Object</b>	<p>Choose the root hierarchical content to consider for the backup</p> <ul style="list-style-type: none"> <li>• <b>Policy Universe</b></li> <li>• <b>Selector Object</b>—When chosen, this option adds the <b>Object Type</b> drop-down list and <b>Object DN</b> field. <ul style="list-style-type: none"> <li>a. From the <b>Object Type</b> drop-down list, choose from the following options: <ul style="list-style-type: none"> <li>• <b>Tenant</b>—When chosen the <b>Select Tenant</b> option appears.</li> <li>• <b>Application Profile</b>—When chosen the <b>Select Application Profile</b> option appears.</li> <li>• <b>EPG</b>—When chosen the <b>Select EPG</b> option appears.</li> <li>• <b>Contract</b>—When chosen the <b>Select Contract</b> option appears.</li> <li>• <b>Filter</b>—When chosen the <b>Select Filter</b> option appears.</li> <li>• <b>VRF</b>—When chosen the <b>Select VRF</b> option appears.</li> <li>• <b>Cloud Context Profile</b>—When chosen the <b>Select Cloud Context Profile</b> option appears.</li> </ul> </li> <li>b. Click the <b>Select &lt;object_name&gt;</b>. The <b>Select &lt;object_name&gt;</b> dialog appears.</li> <li>c. From the <b>Select &lt;object_name&gt;</b> dialog, click to choose from the options in the left column then click <b>Select</b>. You return to the <b>Create Backup Configuration</b> dialog box. <p><b>Note</b> The <b>Object DN</b> field is automatically populated with the DN of the object it will use as root of the object tree to backup</p> </li> </ul> </li> <li>• <b>Enter DN</b>—When chosen, this option displays the <b>Object DN</b> field. <ul style="list-style-type: none"> <li>a. From the <b>Object DN</b> field, enter the DN of a specific object to use as the root of the object tree to backup.</li> </ul> </li> </ul>

Properties	Description
<b>Scheduler</b>	<ol style="list-style-type: none"> <li>a. Click <b>Select Scheduler</b> to open the <b>Select Scheduler</b> dialog and choose a scheduler from the left-side column.</li> <li>b. Click the <b>Select</b> button at the bottom-right corner when finished.</li> </ol>
<b>Trigger Backup After Creation</b>	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Yes</b>—(Default) Trigger a backup after creating the backup configuration.</li> <li>• <b>No</b>—Do not trigger a backup after creating the backup configuration.</li> </ul>

**Step 5** Click **Save** when finished.

## Creating a Tech Support Policy Using the Cisco Cloud APIC GUI

This section explains how to create a tech support policy.

### Before you begin

When creating a tech support policy for a remote location, you must first create the remote location.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

**Step 3** From the **Operations** list in the **Intent** menu, click **Create Tech Support**. The **Create Tech Support** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Tech Support Dialog Box Fields* table then continue.

**Table 18: Create Tech Support Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the tech support policy.
<b>Description</b>	Enter a description of the tech support.
<b>Settings</b>	



Properties	Description
<b>Export Destination</b>	Choose an export destination. <ul style="list-style-type: none"> <li>• <b>Controller</b></li> <li>• <b>Remote Location</b>—When chosen the <b>Select Remote Location</b> option appears.               <ol style="list-style-type: none"> <li>a. Click <b>Select Remote Location</b>. The <b>Select Remote Location</b> dialog box appears.</li> <li>b. From the <b>Select Remote Location</b> dialog, click to choose a remote location in the left column then click <b>Select</b>. You return to the <b>Create Tech Support</b> dialog box.</li> </ol> </li> </ul>
<b>Include Pre-Upgrade Logs</b>	Click to place a check in the <b>Enabled</b> check box if you want to include pre-upgrade logs in the tech support policy.

**Step 5** Click **Save** when finished.

## Creating a Scheduler Using the Cisco Cloud APIC GUI

This section explains how to create a scheduler, which would be in User Laptop Browser local time and will be converted to the Cisco Cloud APIC default UTC time.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

**Step 3** From the **Operations** list in the **Intent** menu, click **Create Scheduler**. The **Create Scheduler** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Scheduler Dialog Box Fields* table then continue.

**Table 19: Create Scheduler Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the trigger scheduler policy.
<b>Description</b>	Enter a description of the trigger scheduler.
<b>Settings</b>	

Properties	Description
<p><b>Recurring Windows</b></p>	<p>Click <b>Add Recurring Window</b>. The <b>Add Recurring Window</b> dialog appears.</p> <ol style="list-style-type: none"> <li>a. From the <b>Schedule</b> drop-down list, choose from the following. <ul style="list-style-type: none"> <li>• <b>Every Day</b></li> <li>• <b>Even Days</b></li> <li>• <b>Odd Days</b></li> <li>• <b>Monday</b></li> <li>• <b>Tuesday</b></li> <li>• <b>Wednesday</b></li> <li>• <b>Thursday</b></li> <li>• <b>Friday</b></li> <li>• <b>Saturday</b></li> <li>• <b>Sunday</b></li> </ul> </li> <li>b. From the <b>Start Time</b> field, enter a time.</li> <li>c. In the <b>Maximum Concurrent Tasks</b> field, choose one of the following: <ul style="list-style-type: none"> <li>• <b>Unlimited</b>: There is no maximum number of concurrent tasks that can be enforced on the scheduler window.</li> <li>• <b>Custom</b>: In the second <b>Maximum Concurrent Tasks</b> field, enter the maximum number of tasks that can be processed concurrently. The maximum value allowed in this field is 65535.</li> </ul> </li> <li>d. In the <b>Maximum Running Time</b> field, choose one of the following: <ul style="list-style-type: none"> <li>• <b>Unlimited</b>: There is no time limit enforced on the scheduler window.</li> <li>• <b>Custom</b>: In the second <b>Maximum Running Time</b> field, enter the maximum duration of the window. The acceptable format for this field is <code>dd:hh:mm:ss</code>.</li> </ul> </li> <li>e. Click <b>Add</b> when finished.</li> </ol>

Properties	Description
Add One Time Window	<p>Click <b>Add One Time Window</b>. The <b>Add One Time Window</b> dialog appears.</p> <ol style="list-style-type: none"> <li>From the <b>Start Time</b> field, enter a date and time.</li> <li>From the <b>Maximum Concurrent Tasks</b> field, enter a number or leave the field blank to specify unlimited.</li> <li>From the <b>Maximum Running Time</b>, click to choose <b>Unlimited</b> or <b>Custom</b>.</li> <li>Click <b>Add</b> when finished.</li> </ol>

**Step 5** Click **Save** when finished.

## Creating a Remote Location Using the Cisco Cloud APIC GUI

This section explains how to create a remote location using the Cisco Cloud APIC.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Operations**.

A list of **Operations** options appear in the **Intent** menu.

**Step 3** From the **Operations** list in the **Intent** menu, click **Create Remote Location**. The **Create Remote Location** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Remote Location Dialog Box Fields* table then continue.

*Table 20: Create Remote Location Dialog Box Fields*

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the remote location policy.
<b>Description</b>	Enter a description of the remote location policy.
<b>Settings</b>	
<b>Hostname/IP Address</b>	Enter the hostname or IP address of the remote location
<b>Protocol</b>	Choose a protocol: <ul style="list-style-type: none"> <li>• <b>FTP</b></li> <li>• <b>SFTP</b></li> <li>• <b>SCP</b></li> </ul>

Properties	Description
Path	Enter the path for the remote location.
Port	Enter the port for the remote location.
Username	Enter a username for the remote location.
Authentication Type	When using SFTP or SCP, choose the authentication type: <ul style="list-style-type: none"> <li>• Password</li> <li>• SSH Key</li> </ul>
SSH Key Content	Enter the SSH key content.
SSH Key Passphrase	SSH key passphrase.
Password	Enter a password for accessing the remote location.
Confirm Password	Reenter the password for accessing the remote location.

**Step 5** Click **Save** when finished.

## Creating a Login Domain Using the Cisco Cloud APIC GUI

This section explains how to create a login domain using the Cisco Cloud APIC GUI.

### Before you begin

Create a provider before creating a non-local domain.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

**Step 3** From the **Administrative** list in the **Intent** menu, click **Create Login Domain**. The **Create Login Domain** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

**Table 21: Create Login Domain Dialog Box Fields**

Properties	Description
Name	Enter the name of the login domain.
Description	Enter a description of the login domain.

Properties	Description
<b>Realm</b>	Choose a realm: <ul style="list-style-type: none"> <li>• <b>Local</b></li> <li>• <b>LDAP</b>—Requires adding providers and choosing an authentication type.</li> <li>• <b>RADIUS</b>—Requires adding providers.</li> <li>• <b>TACACS+</b>—Requires adding providers.</li> <li>• <b>SAML</b>—Requires adding providers.</li> </ul>
<b>Providers</b>	To add a provider: <ol style="list-style-type: none"> <li>a. Click <b>Add Providers</b>. The <b>Select Providers</b> dialog appears with a list of providers in the left pane.</li> <li>b. Click to choose a provider.</li> <li>c. Click <b>Select</b> to add the provider.</li> </ol>
<b>Advanced Settings</b>	Displays the <b>Authentication Type</b> and <b>LDAP Group Map Rules</b> fields.
<b>Authentication Type</b>	When LDAP is chosen for realm option, choose one of the following authentication types: <ul style="list-style-type: none"> <li>• <b>Cisco AV Pairs</b>—(Default)</li> <li>• <b>LDAP Group Map Rules</b>—Requires adding LDAP group map rules.</li> </ul>

Properties	Description
<b>LDAP Group Map Rules</b>	<p>To add an LDAP group map rule:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add LDAP Group Map Rule</b>. The <b>Add LDAP Group Map Rule</b> dialog appears with a list of providers in the left pane.</li> <li>b. Enter a name for the rule in the <b>Name</b> field.</li> <li>c. Enter a description for the rule in the <b>Description</b> field.</li> <li>d. Enter a group DN for the rule in the <b>Group DN</b> field.</li> <li>e. Add security domains: <ol style="list-style-type: none"> <li>1. Click <b>Add Security Domain</b>. The <b>Add Security Domain</b> dialog box appears.</li> <li>2. Click <b>Select Security Domain</b>. The <b>Select Security Domain</b> dialog box appears with a list of security domains in the left pane.</li> <li>3. Click to choose a security domain.</li> <li>4. Click <b>Select</b> to add the security domain. You return to the <b>Add Security Domain</b> dialog box.</li> </ol> </li> <li>5. Add a user role: <ol style="list-style-type: none"> <li>a. From the <b>Add Security Domain</b> dialog box, click <b>Select Role</b>. The <b>Select Role</b> dialog box appears with a list of roles in the left pane.</li> <li>b. Click to choose a role.</li> <li>c. Click <b>Select</b> to add the role. You return to the <b>Add Security Domain</b> dialog box.</li> <li>d. From the <b>Add Security Domain</b> dialog box, click the <b>Privilege Type</b> drop-down list and choose <b>Read Privilege</b> or <b>Write Privilege</b>.</li> <li>e. Click the check mark on the right side of the <b>Privilege Type</b> drop-down list to confirm.</li> <li>f. Click <b>Add</b> when finished. You return to the <b>Add LDAP Group Map Rule</b> dialog box where you can add another security domain.</li> </ol> </li> </ol>

**Step 5** Click **Save** when finished.

## Creating a Security Domain Using the Cisco Cloud APIC GUI

A security domain restricts the tenant to the security domains that you add. If you do not add a security domain, all security domains will have access to this tenant. This section explains how to create a security domain using the GUI.

- 
- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.  
A list of **Administrative** options appear in the **Intent** menu.
- Step 3** From the **Administrative** list in the **Intent** menu, click **Security > Security Domains > Create Security Domain**. The **Create Security Domain** dialog box appears.
- Step 4** In the **Name** field, enter the name of the security domain.
- Step 5** In the **Description** field, enter a description of the security domain.
- Step 6** In the **Type** field, choose the type of security domain:
- **Unrestricted:** Users who are assigned to this domain are able to see policies, profiles, or users configured in other security domains.
  - **Restricted:** Users who are assigned to this domain will not be able to see policies, profiles, or users configured in other security domains.
- Step 7** Click **Save** when finished.
- 

## Creating a Role Using the Cisco Cloud APIC GUI

This section explains how to create a role using the Cisco Cloud APIC GUI.

- 
- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.  
A list of **Administrative** options appear in the **Intent** menu.
- Step 3** From the **Administrative** list in the **Intent** menu, click **Create Role**. The **Create Role** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Role Dialog Box Fields* table then continue.

**Table 22: Create Role Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter a name for the role in the <b>Name</b> field.
<b>Description</b>	Enter a description of the role.
<b>Settings</b>	

Properties	Description
Privilege	



Properties	Description
	<p>Click to place a check mark in the check boxes of the privileges you want to assign the user. The privileges are:</p> <ul style="list-style-type: none"> <li>• <b>aaa</b>—Used for configuring authentication, authorization, accounting and import/export policies.</li> <li>• <b>access-connectivity</b>—Used for Layer 1-3 configuration under infra, static route configurations under a tenant's L3Out, management infra policies, and tenant ERSPAN policies.</li> <li>• <b>access-equipment</b>—Used for access port configuration.</li> <li>• <b>access-protocol</b>—Used for Layer 1-3 protocol configurations under infra, fabric-wide policies for NTP, SNMP, DNS, and image management, and operations-related access policies such as cluster policy and firmware policies.</li> <li>• <b>access-qos</b>—Used for changing CoPP and QoS-related policies.</li> <li>• <b>admin</b>—Complete access to everything (combine ALL roles)</li> <li>• <b>config-manager</b></li> <li>• <b>custom-port-privilege</b></li> <li>• <b>custom-privilege-1 through custom-privilege-22</b></li> <li>• <b>fabric-connectivity</b>—Used for Layer 1-3 configuration under the fabric, firmware and deployment policies for raising warnings for estimating policy deployment impact, and atomic counter, diagnostic, and image management policies on leaf switches and spine switches.</li> <li>• <b>fabric-equipment</b>—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches.</li> <li>• <b>fabric-protocol</b>—Used for Layer 1-3 protocol configurations under the fabric, fabric-wide policies for NTP, SNMP, DNS, and image management, ERSPAN and health score policies, and firmware management traceroute and endpoint tracking policies.</li> <li>• <b>none</b>—No privilege.</li> <li>• <b>nw-svc-params</b>—Used for managing Layer 4 to Layer 7 service policies.</li> <li>• <b>nw-svc-policy</b>—Used for managing Layer 4 to Layer 7 service devices and network service orchestration.</li> <li>• <b>ops</b>—Used for operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies.</li> <li>• <b>site-admin</b></li> <li>• <b>site-policy</b></li> <li>• <b>tenant-connectivity</b>—Used for Layer 1-3 connectivity changes, including bridge domains, subnets, and VRFs; for atomic counter, diagnostic, and image management policies on leaf switches and spine switches; tenant in-band and out-of-band management</li> </ul>

Properties	Description
	<p>connectivity configurations; and debugging/monitoring policies such as atomic counters and health score.</p> <ul style="list-style-type: none"> <li>• <b>tenant-epg</b>—Used for managing tenant configurations such as deleting/creating endpoint groups, VRFs, and bridge domains.</li> <li>• <b>tenant-ext-connectivity</b>—Used for write access firmware policies; managing tenant L2Out and L3Out configurations; and debugging/monitoring/observer policies.</li> <li>• <b>tenant-ext-protocol</b>—Used for managing tenant external Layer 1-3 protocols, including BGP, OSPF, PIM, and IGMP, and for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk. Generally only used for write access for firmware policies.</li> <li>• <b>tenant-network-profile</b>—Used for managing tenant configurations, such as deleting and creating network profiles, and deleting and creating endpoint groups.</li> <li>• <b>tenant-protocol</b>—Used for managing configurations for Layer 1-3 protocols under a tenant, for tenant traceroute policies, and as write access for firmware policies.</li> <li>• <b>tenant-qos</b>—Only used as Write access for firmware policies.</li> <li>• <b>tenant-security</b>—Used for Contract related configurations for a tenant.</li> <li>• <b>vmm-policy</b>—Used for managing policies for VM networking.</li> </ul>

**Step 5** Click **Save** when finished.

## Creating a Certificate Authority Using the Cisco Cloud APIC GUI

This section explains how to create a certificate authority using the GUI.

### Before you begin

- Have the certificate chain.
- If the certificate authority is for a tenant, create the tenant.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appears in the **Intent** menu.

**Step 3** From the **Administrative** list in the **Intent** menu, click **Create Certificate Authority**. The **Create Certificate Authority** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Certificate Authority Dialog Box Fields* table then continue.

Table 23: Create Certificate Authority Dialog Box Fields

Properties	Description
<b>Name</b>	Enter the name of the certificate authority.
<b>Description</b>	Enter a description of the certificate authority.
<b>Used for</b>	Choose from the following options: <ul style="list-style-type: none"> <li>• <b>Tenant</b>—Choose if the certificate authority is for a specific tenant. When chosen, the <b>Select Tenant</b> option appears in the GUI.</li> <li>• <b>System</b>—Choose if the certificate authority is for the system.</li> </ul>
<b>Select Tenant</b>	To choose a tenant: <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column then click <b>Select</b>. You return to the <b>Create Certificate Authority</b> dialog box.</li> </ol>
<b>Certificate Chain</b>	Enter the certificate chain in the <b>Certificate Chain</b> text box. <p><b>Note</b> Add the certificates for a chain in the following order:</p> <ol style="list-style-type: none"> <li>CA</li> <li>Sub-CA</li> <li>Subsub-CA</li> <li>Server</li> </ol>

**Step 5** Click **Save** when finished.

## Creating a Key Ring Using the Cisco Cloud APIC GUI

This section explains how to create a key ring using the Cisco Cloud APIC GUI.

### Before you begin

- Create a certificate authority.
- Have a certificate.
- If the key ring is for a specific tenant, create the tenant.

- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.  
A list of **Administrative** options appear in the **Intent** menu.
- Step 3** From the **Administrative** list in the **Intent** menu, click **Create Key Ring**. The **Create Key Ring** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Key Ring Dialog Box Fields* table then continue.

Table 24: Create Key Ring Dialog Box Fields

Properties	Description
<b>Name</b>	Enter the name of the key ring.
<b>Description</b>	Enter a description of the key ring.
<b>Used for</b>	<ul style="list-style-type: none"> <li>• <b>System</b>—The key ring is for the system.</li> <li>• <b>Tenant</b>—The key ring is for a specific tenant. Displays a <b>Tenant</b> field for specifying the tenant.</li> </ul>
<b>Select Tenant</b>	<p>To choose a tenant:</p> <ol style="list-style-type: none"> <li>a. Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li> <li>b. From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column then click <b>Select</b>. You return to the <b>Create Key Ring</b> dialog box.</li> </ol>
<b>Settings</b>	
<b>Certificate Authority</b>	<p>To choose a certificate authority:</p> <ol style="list-style-type: none"> <li>a. Click <b>Select Certificate Authority</b>. The <b>Select Certificate Authority</b> dialog appears.</li> <li>b. Click to choose a certificate authority in the column on the left.</li> <li>c. Click <b>Select</b>. You return to the <b>Create Key Ring</b> dialog box.</li> </ol>
<b>Private Key</b>	<p>Choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Generate New Key</b>—Generates a new key.</li> <li>• <b>Import Existing Key</b>—Displays the <b>Private Key</b> text box and enables you to use an existing key.</li> </ul>
<b>Private Key</b>	Enter an existing key in the <b>Private Key</b> text box (for the <b>Import Existing Key</b> option).

Properties	Description
<b>Modulus</b>	Click the <b>Modulus</b> drop-down list to choose from the following: <ul style="list-style-type: none"> <li>• <b>MOD 512</b></li> <li>• <b>MOD 1024</b></li> <li>• <b>MOD 1536</b></li> <li>• <b>MOD 2048</b>—(Default)</li> </ul>
<b>Certificate</b>	Enter the certificate information in the <b>Certificate</b> text box.

**Step 5** Click **Save** when finished.

## Creating a Local User Using the Cisco Cloud APIC GUI

This section explains how to create a local user using the Cisco Cloud APIC GUI.

**Step 1** Click the **Intent** icon. The **Intent** menu appears.

**Step 2** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

**Step 3** From the **Administrative** list in the **Intent** menu, click **Create Local User**. The **Create Local User** dialog box appears.

**Step 4** Enter the appropriate values in each field as listed in the following *Create Local User Dialog Box Fields* table then continue.

**Table 25: Create Local User Dialog Box Fields**

Properties	Description
<b>Username</b>	Enter the username of the local user.
<b>Password</b>	Enter the password for the local user.
<b>Confirm Password</b>	Reenter the password for the local user.
<b>Description</b>	Enter a description of the local user.
<b>Settings</b>	
<b>Account Status</b>	To choose the account status: <ul style="list-style-type: none"> <li>• <b>Active</b>—Activates the local user account.</li> <li>• <b>Blocked</b>—Blocks the local user account.</li> <li>• <b>Inactive</b>—Deactivates the local user account.</li> </ul>

Properties	Description
<b>First Name</b>	Enter the first name of the local user.
<b>Last Name</b>	Enter the last name of the local user.
<b>Email Address</b>	Enter the email address of the local user.
<b>Phone Number</b>	Enter the phone number of the local user.
<b>Security Domains</b>	<p>To add a security domain:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add Security Domain</b>. The <b>Add Security Domain</b> dialog box appears.</li> <li>b. Click <b>Select Security Domain</b>. The <b>Select Security Domain</b> dialog box appears with a list of security domains in the left pane.</li> <li>c. Click to choose a security domain.</li> <li>d. Click <b>Select</b> to add the security domain. You return to the <b>Add Security Domain</b> dialog box.</li> <li>e. Add a user role: <ol style="list-style-type: none"> <li>1. From the <b>Add Security Domain</b> dialog box, click <b>Select Role</b>. The <b>Select Role</b> dialog box appears with a list of roles in the left pane.</li> <li>2. Click to choose a role.</li> <li>3. Click <b>Select</b> to add the the role. You return to the <b>Add Security Domain</b> dialog box.</li> <li>4. From the <b>Add Security Domain</b> dialog box, click the <b>Privilege Type</b> drop-down list and choose <b>Read Privilege</b> or <b>Write Privilege</b>.</li> <li>5. Click the check mark on the right side of the <b>Privilege Type</b> drop-down list to confirm.</li> <li>6. Click <b>Add</b> when finished. You return to the <b>Create Local User</b> dialog box where you can add another security domain.</li> </ol> </li> </ol>

**Step 5** Click **Advanced Settings** and enter the appropriate values in each field as listed in the following *Create Local User Dialog Box Fields: Advanced Settings* table then continue.

**Table 26: Create Local User Dialog Box Fields: Advanced Settings**

Property	Description
<b>Account Expires</b>	If you choose <b>Yes</b> , the account is set to expire at the time that you choose.

Property	Description
<b>Password Update Required</b>	If you choose <b>Yes</b> , the user must change the password upon the next login.
<b>OTP</b>	Put a check in the box to enable the one-time password feature for the user.
<b>User Certificate Attribute</b>	The attribute for the user certificate.
<b>User Certificates</b>	To add a user certificate: <ul style="list-style-type: none"> <li>a. Click <b>Add X509 Certificate</b>. The <b>Add X509 Certificate</b> dialog box appears.</li> <li>b. Enter a name in the <b>Name</b> field.</li> <li>c. Enter the X509 certificate in the <b>User X509 Certificate</b> text box.</li> <li>d. Click <b>Add</b>. The <b>X509 certificate in the User X509 Certificate</b> dialog box closes. You return to the <b>Local User</b> dialog box.</li> </ul>
<b>SSH Keys</b>	To add an SSH key: <ul style="list-style-type: none"> <li>a. Click <b>Add SSH Key</b>. The <b>Add SSH Key</b> dialog box appears.</li> <li>b. Enter a name in the <b>Name</b> field.</li> <li>c. Enter the SSH key in the <b>Key</b> text box.</li> <li>d. Click <b>Add</b>. The <b>Add SSH Key</b> dialog box closes. You return to the <b>Local User</b> dialog box.</li> </ul>

**Step 6** Click **Save** when finished.

## Managing Regions (Configuring a Cloud Template) Using the Cisco Cloud APIC GUI

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 and inter-region connectivity is present. Cisco Cloud APIC manages all 25 Google Cloud regions.

**Step 1** Click the **Intent** icon.  
The **Intent** menu appears.

**Step 2** In the **Workflows** area, click **Cloud APIC Setup**.  
The **Set up - Overview** dialog box appears with options for **DNS and NTP Servers**, **Region Management**, and **Smart Licensing**.

- Step 3** For **Region Management**, click **Edit Configuration**.  
The **Region Management** window appears.
- Step 4** Determine if you want to configure external connectivity.  
Click the box next to **Enable** to enable external connectivity.
- Step 5** Verify that all of the regions in the page are selected.  
This page shows all of the regions that are supported by Google Cloud. All of the regions are managed by Cisco Cloud APIC.
- Step 6** Click **Next** at the bottom of the page.  
If you enabled external connectivity, the **General Connectivity** page appears.
- Step 7** Enter the necessary information in the **Hub Network** area.  
Hub network management is used to deploy cloud routers on specific managed regions. Configure the fabric infra connectivity for the cloud site and define the configuration template used for the cloud routers in the cloud site in this area.  
Note the following restrictions:
- You can create only one hub network in Google Cloud.
  - Under the hub network, only one cloud router is created in Google Cloud.
- 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) Enter a value in the **BGP Autonomous System Number** field.  
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, then click the check mark next to the field.
- d) In the **Region** field, select the appropriate regions.  
You can add up to four regions to deploy hub network in this area. The hub network will create one cloud router in each region selected.
- e) In the **VPN Router** field, enter a name for the VPN router.  
The infra VPC uses the cloud router and VPN Gateway to create IPsec tunnels and BGP sessions to on-premises sites or other cloud sites. The spoke VPCs peer with the infra VPC to share the VPN connections to external sites.
- Step 8** 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 existing 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 9** 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 [Creating an External Network Using Cloud Native Routers Using the Cisco Cloud APIC GUI, on page 51](#) for those procedures.

## Configuring Cisco Cloud APIC Using the REST API

### Creating a Tenant Using the REST API

#### Before you begin

Review the information provided in [Understanding Google Cloud Deployments with Cisco Cloud APIC, on page 10](#) before proceeding with the procedures in this section.

- Step 1** Enter the following POST to share the same credentials across multiple tenants, where you are duplicating the `cloudCredentials` object in each tenant and specifying the same Google Cloud Service Account.

Note the following:

- Tenant `T1` defines the `cloudCredentials` object that carries the private key for the Service Account.
- Both tenant `T1` and `T2` then refer to this `cloudCredentials` object through the `cloudRsCredentials` relation.
- The Service Account defined by tenant `T1` must be a member of Google Cloud Projects `project1` and `project2` in this scenario.
- The highlighted areas in the POST for tenant `T2` show the credentials that are shared with the first user tenant

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="T1">
  <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
    <cloudRsCredentials tDn="uni/tn-T1/credentials-creds1" />
  </cloudAccount>
  <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN ... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
  <fvRsCloudAccount tDn="uni/tn-T1/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
  <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
    <cloudRsCredentials tDn="uni/tn-T2/credentials-creds1" />
  </cloudAccount>
```

```

    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
    rsaPrivateKey="-----BEGIN ... -----END PRIVATE KEY-----\n" clientId="28763876"
    email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
  </fvTenant>

```

- Step 2** To create a user tenant where the Cisco Cloud APIC runs outside of Google Cloud (the infra tenant with credentials):  
Note that the new properties added specifically for Google Cloud are highlighted below.

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml
```

```

<fvTenant name="infra">
  <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
    <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
  </cloudAccount>
  <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
  rsaPrivateKey="-----BEGIN ... -----END PRIVATE KEY-----\n" clientId="28763876"
  email="capic-395@project2.iam.gserviceaccount.com"/>
  <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
  <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
    <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
  </cloudAccount>
  <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>

```

- Step 3** To create a managed user tenant where the user shares the infra service account across multiple Google Cloud projects:

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml
```

```

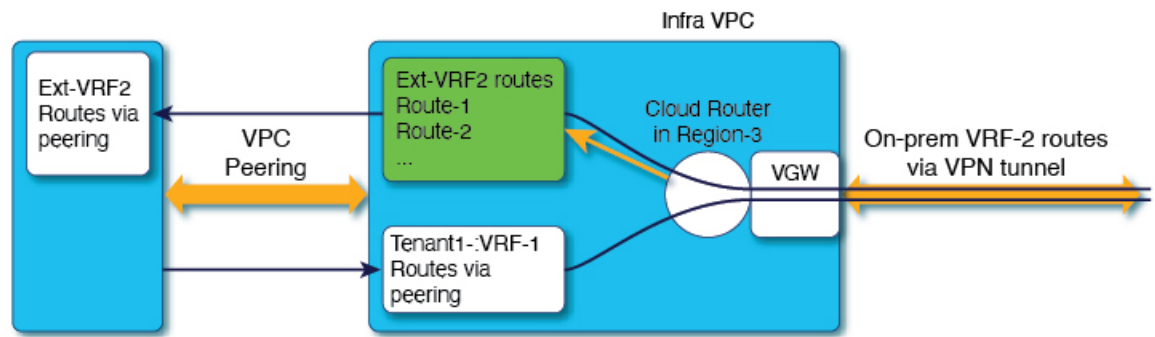
<fvTenant name="infra">
  <cloudAccount id="project1" vendor="gcp" accessType="managed" />
  <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
  <cloudAccount id="project2" vendor="gcp" accessType="managed" />
  <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>

```

## Configuring Inter-VRF Route Leaking Using the REST API

This example demonstrates how to configure leak routes for the Cisco Cloud APIC using the REST API. This example shows how to configure inter-VRF route leaking, between an external VRF and a cloud VRF, as shown in the following figure.



**Subnet1 (Region-1) Route-Table**

CIDR1 (Region-1) - 100.100.0.0/16  
 Subnet1 - 100.100.100.0/24

100.100.0.0/16 -> Local  
 50.50.0.0/16 -> Infra-VPC

Leak-All-routes to  
 Tenant-Infra:Ext-RF-2

503853

To configure inter-VRF route leaking for this example:

**Example:**

```
<polUni>
  <fvTenant name="t1">
    <fvCtx name="VRF1">
      <leakRoutes>
        <leakInternalPrefix ip="0.0.0.0/0" status="">
          <leakTo tenantName="infra" ctxName="Ext-VRF2" scope="public" status=""/>
        </leakInternalPrefix>
      </leakRoutes>
    </fvCtx>
    <cloudCtxProfile name="v1-us-west1" type="regular" vpcGroup="one" status="">
      <cloudRsToCtx tnFvCtxName="VRF1"/>
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
      <cloudCidr addr="100.100.0.0/16" primary="yes">
        <cloudSubnet ip="100.100.100.0/20" scope="public,shared" subnetGroup="one">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
  <fvTenant name="infra" status="">
    <fvCtx name="Ext-VRF2">
      <leakRoutes>
        <leakExternalPrefix ip="0.0.0.0/0" status="">
          <leakTo tenantName="t1" ctxName="VRF1" scope="public" status=""/>
        </leakExternalPrefix>
      </leakRoutes>
    </fvCtx>
  </fvTenant>
</polUni>
```

## Creating a Filter Using the REST API

This section demonstrates how to create a filter using the REST API.

To create a filter:

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="t15">
    <vzFilter name="rule1">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>
    <vzFilter name="rule2">
      <vzEntry etherT="ip" dToPort="http" prot="tcp" dFromPort="http" name="http"/>
    </vzFilter>
    <vzFilter name="rule3">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
    </vzFilter>
    <vzFilter name='all_rule'>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>

    <vzBrCP name="c1">
      <vzSubj name="c1">
        <vzRsSubjFiltAtt tnVzFilterName="rule2"/>
        <vzRsSubjGraphAtt tnVnsAbsGraphName="c13_g1"/>
        <vzRsSubjFiltAtt tnVzFilterName="rule3"/>
        <vzRsSubjFiltAtt tnVzFilterName="all_rule"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

## Creating a Contract Using the REST API

This example demonstrates how to create a contract for the Cisco Cloud APIC using the REST API.

### Before you begin

Create filters.

To create a contract:

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
```

```

    <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
      <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
    </vzSubj>
  </vzBrCP>
</fvTenant>
</polUni>

```

Note the following restrictions for the name of the contract (the `vzBrCP` entry):

- Match the regular expression:

```
[a-z]([-a-z0-9]*[a-z0-9])?
```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to [Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24](#) to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

## Creating a Cloud Context Profile Using the REST API

This section demonstrates how to create a cloud context profile.

### Before you begin

Create a VRF.

**Step 1** To create a basic cloud context profile:

#### Example:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <cloudCtxProfile name="cProfilewest1151">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
      <cloudRsToCtx tnFvCtxName="ctx151"/>
      <cloudCidr addr="15.151.0.0/16" primary="true" status="">
        <cloudSubnet ip="15.151.1.0/24" name="GatewaySubnet" usage="gateway">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>

```

**Step 2** To create a cloud context profile where you are adding a secondary VRF, CIDR, and subnet for a VNet:

#### Example:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tenant1" status="">
    <fvCtx name="VRF1" />
    <fvCtx name="VRF2" />
    <cloudCtxProfile name="vpcl" status="">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-central1" status=""/>
      <cloudRsToCtx tnFvCtxName="VRF1" />
      <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
      <cloudCidr name="cidr1" addr="192.0.2.0/16" primary="yes" status="">
        <cloudSubnet ip="192.0.3.0/24" usage="gateway" status="">
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-gcp/region-us-central1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
      <cloudCidr name="cidr1" addr="193.0.2.0/16" primary="no" status="">
        <cloudSubnet ip="193.0.3.0/24" usage="" status="">
          <cloudRsSubnetToCtx tnFvCtxName="VRF2"/>
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-gcp/region-us-central1/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>

```

## Creating an Application Profile Using the REST API

This section demonstrates how to create an application profile using the REST API.

### Before you begin

Create a tenant.

To create an application profile:

```

https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act- [<gcp-id>]-vendor-gcp" />

    <fvCtx name="ctx151"/>

    <cloudVpnGwPol name="VgwPol1"/>
    <cloudApp name="a1">

  </cloudApp>

</fvTenant>
</polUni>

```

For the application profile name, note the following restrictions:

- Match the regular expression:

```
[a-z]([-a-z0-9]*[a-z0-9])?
```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to [Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24](#) to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

## Creating an EPG Using the REST API

Use the procedures in this section to create an application EPG or an external EPG using the REST API.

### Creating a Cloud EPG Using the REST API

This example demonstrates how to create a cloud EPG using the REST API.

#### Before you begin

Create an application profile and a VRF.

To create a cloud EPG:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<gcp-id>]-vendor-gcp" />

    <fvCtx name="ctx151"/>

    <cloudVpnGwPol name="VgwPol1"/>
    <cloudApp name="a1">

      <cloudEPg name="epg1">
        <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
        <cloudEPSelector matchExpression="custom:tag1=='value1'" name="selector-1"/>
      </cloudEPg>

    </cloudApp>

  </fvTenant>
</polUni>
```

Note the following restrictions:

- Match the regular expression:

```
[a-z]([-a-z0-9]*[a-z0-9])?
```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to [Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24](#) to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

## Creating an External Cloud EPG Using the REST API

This example demonstrates how to create an external cloud EPG using the REST API.

For the name of the external EPG, note the following restrictions:

- Match the regular expression:

```
[a-z]([-a-z0-9]*[a-z0-9])?
```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name, if possible, due to the restrictions imposed by the Google Cloud firewall rules. Refer to [Naming Length Restrictions Imposed By Google Cloud Firewall Rules, on page 24](#) to better understand the restriction and the total number of characters allowed for each of the Cisco Cloud APIC components that make up the firewall rule name.

### Before you begin

Create an application profile and a VRF.

**Step 1** To create an external cloud EPG:

#### Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<gcp-id>-vendor-gcp" />
    <fvCtx name="ctx151"/>
    <cloudVpnGwPol name="VgwPol1"/>
    <cloudApp name="a1">
      <cloudExtEPg routeReachability="internet" name="extEpg-1">
        <fvRsCons tnVzBrCPName="extEpg-1"/>
        <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
        <cloudExtEPSelector name="extSelector1" subnet="0.0.0.0/0"/>
      </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

**Step 2** To create an external cloud EPG with type **site-external**, or an infra L3Out EPG:

#### Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
```



```

<polUni>
  <fvTenant name="infra">
    <cloudApp name="a1">
      <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
        <fvRsCons tnVzBrCPName="extEpg-1"/>
        <cloudRsCloudEPgCtx tnFvCtxName="ctx152"/>
        <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
      </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>

```

## Creating Cloud Routers, External Networks, and External VRFs Using the REST API

This section demonstrates how to create cloud routers, external networks, and external VRFs using the REST API.

Following is an example POST that shows how to bring up the cloud router in four regions and add an external network with an external VRF in each region.

```

<polUni>
  <fvTenant name="infra" status="">
    <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
    <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
    <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1" hostRouterMode="manual"
status="">
      <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24" poolname="pool1" />
      <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24" poolname="pool2" />
      <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24" poolname="pool3" />

      <cloudtemplateHubNetwork name="default" status="" >
        <cloudtemplateHubNetworkName name="fool" asn="64514" status="">
          <cloudRegionName provider="gcp" region="us-west4" status="" />
          <cloudRegionName provider="gcp" region="us-west2" status="" />
          <cloudRegionName provider="gcp" region="us-east1" status="" />
          <cloudRegionName provider="gcp" region="us-west1" status=""/>
        </cloudtemplateHubNetworkName>
      </cloudtemplateHubNetwork>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="gcp" region="us-west1">
          <cloudtemplateVpnRouter name="default" status=""/>
        </cloudRegionName>
        <cloudRegionName provider="gcp" region="us-west2">
          <cloudtemplateVpnRouter name="default" status=""/>
        </cloudRegionName>
        <cloudRegionName provider="gcp" region="us-east1">
          <cloudtemplateVpnRouter name="default" status=""/>
        </cloudRegionName>
        <cloudRegionName provider="gcp" region="us-west4">
          <cloudtemplateVpnRouter name="default" status=""/>
        </cloudRegionName>
      </cloudtemplateIntNetwork>

```

```

    <cloudtemplateExtNetwork name="default">
  </cloudtemplateExtNetwork>
    <cloudtemplateExtNetwork name="extnwfoo1" vrfName="extv1" hubNetworkName="foo1"
vpnRouterName="default" status="">
      <cloudRegionName provider="gcp" region="us-west1" status=""/>
      <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">
    <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd" poolname="pool1"
status="">
      <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
    </cloudtemplateIpSecTunnel>
  </cloudtemplateVpnNetwork>
</cloudtemplateExtNetwork>
  <cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
vpnRouterName="default" status="">
    <cloudRegionName provider="gcp" region="us-west2" status=""/>
    <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
  <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
poolname="pool2" status="">
    <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
  </cloudtemplateIpSecTunnel>
</cloudtemplateVpnNetwork>
</cloudtemplateExtNetwork>
  <cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3" hubNetworkName="foo1"
vpnRouterName="default" status="">
    <cloudRegionName provider="gcp" region="us-east1" status=""/>
    <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
  <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
poolname="pool3" status="">
    <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
  </cloudtemplateIpSecTunnel>
</cloudtemplateVpnNetwork>
</cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
</fvTenant>
</polUni>

```

---



## CHAPTER 6

# Viewing System Details

---

- [Monitoring VM Host Metrics, on page 107](#)
- [Viewing Application Management Details, on page 110](#)
- [Viewing Cloud Resource Details, on page 111](#)
- [Viewing Operations Details, on page 112](#)
- [Viewing Infrastructure Details, on page 114](#)
- [Viewing Administrative Details, on page 114](#)
- [Viewing Health Details Using the Cisco Cloud APIC GUI, on page 116](#)

## Monitoring VM Host Metrics

Beginning with release 25.0(1), support is available for monitoring metrics for the VM host where the Cisco Cloud APIC is deployed using the Prometheus Node Exporter. The Prometheus Node Exporter provides visibility to a wide variety of hardware and kernel-related metrics, where it collects technical information from Linux nodes, such as CPU, disk, and memory statistics. For overview information on the Prometheus Node Exporter, see:

<https://prometheus.io/docs/introduction/overview/>

If your Cisco Cloud APIC is running on release 25.0(1) or later, the Prometheus Node Exporter is automatically available by default.

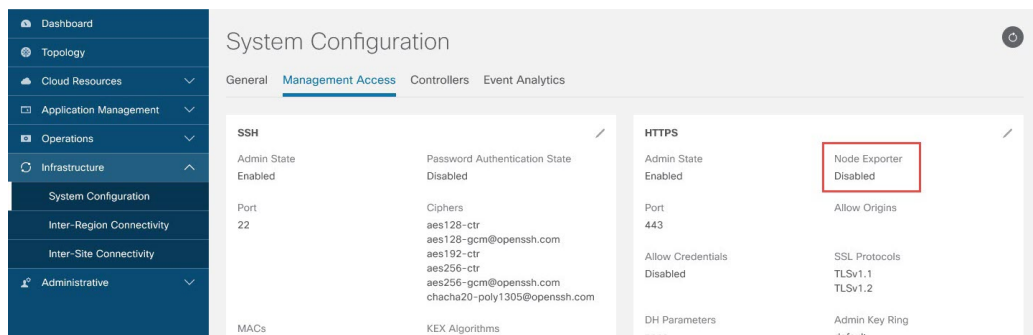
### Guidelines and Limitations

HTTP is not supported for monitoring metrics using the Prometheus Node Exporter. Only HTTPS is supported for monitoring metrics using the Prometheus Node Exporter.

## Monitoring VM Host Metrics Using the GUI

These procedures describe how to enable the Prometheus Node Exporter to monitor VM host metrics using the GUI.

- 
- Step 1** In the Cisco Cloud APIC GUI, navigate to **Infrastructure > System Configuration**, then click on the **Management Access** tab.
- Step 2** In the **HTTPS** area to the right of the window, note the entry in the **Node Exporter** field.

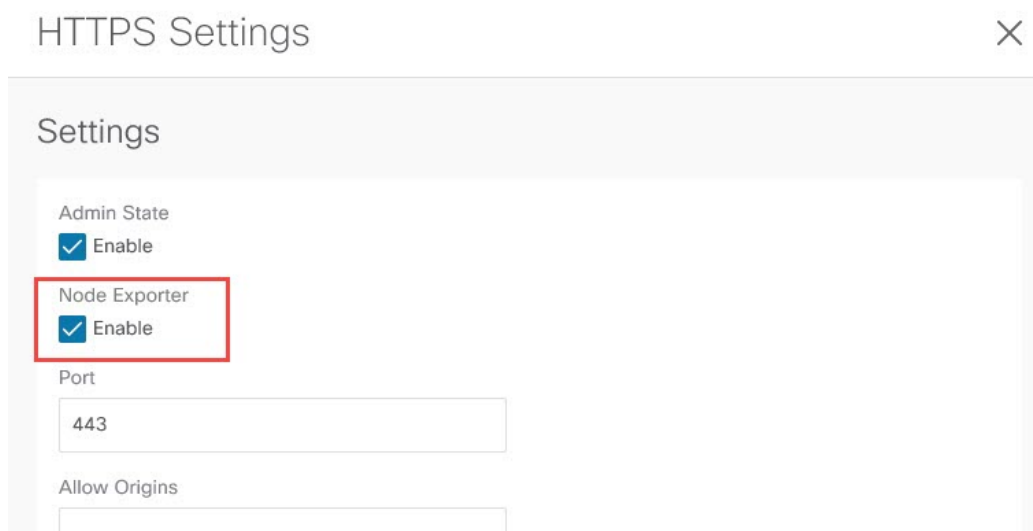


- **Enabled:** The Prometheus Node Exporter has already been enabled. You do not have to continue with these instructions in that case.
- **Disabled:** The Prometheus Node Exporter is not enabled yet. Proceed with these instructions to enable the Prometheus Node Exporter.

**Step 3** Click the pencil icon in the **HTTPS** area to edit the HTTPS settings.

The **HTTPS Settings** window appears.

**Step 4** Locate the **Node Exporter** field and click **Enable**.



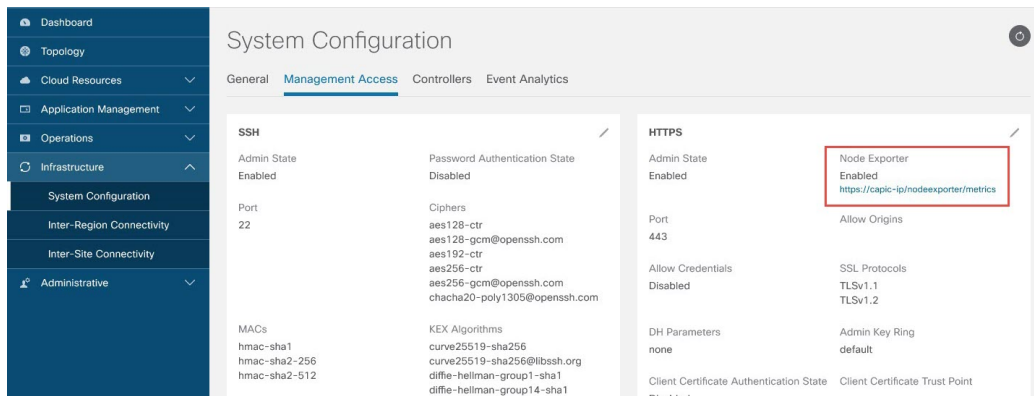
A warning message appears, telling you that saving these settings will restart the web service, and that it will take a moment for it to resume responding to requests. Click **OK** to confirm these changes.

**Step 5** At the bottom of the window, click **Save**.

You are returned to the **System Configuration/Management Access** window. The web service reboots and comes back online in a few seconds.

**Step 6** In the **HTTPS** area to the right of the window, verify that the entry in the **Node Exporter** field is set to **Enabled**.

This verifies that the Prometheus Node Exporter is enabled.



**Step 7** Click the link under the **Enabled** text in the **Node Exporter** area.

Another tab in your browser appears, showing the metrics for the VM host where the Cisco Cloud APIC is deployed.

## Monitoring VM Host Metrics Using the REST API

These procedures describe how to enable the Prometheus Node Exporter to monitor VM host metrics using the REST API.

**Step 1** To determine if the Prometheus Node Exporter is enabled or not, send the following GET call:

```
GET https://<cloud-apic-ip-address>/api/mo/uni/fabric/comm-default/https.xml
```

Locate the `nodeExporter` field to determine if it is set to `enabled` or `disabled`.

**Step 2** To monitor VM host metrics, send the following post to enable the Prometheus Node Exporter:

```
POST https://<cloud-apic-ip-address>/api/mo/uni/fabric/comm-default/https.xml
<commHttps nodeExporter="enabled" />
```

The metrics are displayed for the VM host where the Cisco Cloud APIC is deployed.

**Step 3** To view the metrics using REST API, send the following GET call:

```
GET https://<cloud-apic-ip-address>/nodeexporter/metrics
```

**Step 4** To disable the Prometheus Node Exporter, send the following post:

```
POST https://<cloud-apic-ip-address>/api/mo/uni/fabric/comm-default/https.xml
<commHttps nodeExporter="disabled" />
```

# Viewing Application Management Details

This section explains how to view application management details using the Cisco Cloud APIC GUI. The application management details include the information of a specific tenant, application profile, EPG, contract, filter, VRF, cloud context profile, or external network.

**Step 1** From the **Navigation** menu, choose the **Application Management** tab.

When the **Application Management** tab expands, a list of subtab options appear. See the *Application Management Options* table for more information.

**Table 27: Application Management Subtabs**

Subtab Name	Description
<b>Tenants</b>	Displays tenants as rows in a summary table.
<b>Application Profiles</b>	Displays application profiles as rows in a summary table.
<b>EPGs</b>	Displays an EPGs as rows in a summary table.
<b>Contracts</b>	Displays a contracts as rows in a summary table.
<b>Filters</b>	Displays filters as rows in a summary table.
<b>VRFs</b>	Displays VRFs as rows in a summary table.
<b>Cloud Context Profiles</b>	Displays cloud context profiles as rows in a summary table.
<b>External Networks</b>	Displays external networks as rows in a summary table.

**Step 2** Click the tab that represents the component with the details you want to view.

A summary table appears with items as rows in the table. For example, if you chose the **Tenants** subtab, a list of tenants appear as rows in a summary table

You can filter the rows by clicking the *Filter by Attributes* bar. Choose the attribute, operator and filter-value. For example, for filtering based on a tenant, choose Name == T1 (where T1 is the name of a tenant).

**Step 3** To view a summary pane, click the row that represents the specific component you want to view.

**Step 4** For more information, double-click the summary table row that represents the specific component you want to view.

A new dialog box appears over the **work** pane with any of the following tabs:

**Note** The tabs that appear differ between components and configurations.

- **Overview**—Provides a general overview of cloud resources, configuration relationships, and settings of the component.
- **Topology**—Provides visual relationship between an object and other related objects. The chosen object is displayed at the center.
- **Cloud Resources**—Contains a list of subtabs that display the cloud resource information related to the component.

- **Application Management**—Contains a list of subtabs that display the ACI relation information related to the component.
- **Event Analytics**—Contains a list of subtabs that display faults, events, and audit logs.

**Note** The dialog box that appears over the **work** pane contains an **edit** button in the top-right corner between the **refresh** button and the **Actions** button. When clicked, the **edit** button enables you to edit the chosen component.

## Viewing Cloud Resource Details

This section explains how to view cloud resource details using the Cisco Cloud APIC GUI. The cloud resource details include the information about a specific region, VPC, router, security group (application security group/network security group), endpoint, VM, and cloud service.

**Step 1** From the **Navigation** menu, choose the **Cloud Resources** tab.

When the **Cloud Resources** tab expands, a list of subtab options appear. See the *Cloud Resource Options* table for more information.

**Table 28: Cloud Resource Subtabs**

Subtab Name	Description
<b>Regions</b>	Displays regions as rows in a summary table.
<b>VPCs</b>	Displays VPCs as rows in a summary table.
<b>Routers</b>	Displays routers as rows in a summary table.
<b>Endpoints</b>	Displays endpoints as rows in a summary table.
<b>Instances</b>	Displays instances as rows in a summary table.

**Step 2** Click the tab that represents the component with the details you want to view.

A summary table appears with items as rows in the table. For example, if you chose the **Endpoints** subtab, a list of endpoints appear as rows in a summary table.

You can filter the rows by selecting an attribute from the drop-down menu when you click the *Filter by attributes* bar. The attributes displayed in the drop-down menu depend on the selected subtab.

For the **Endpoints** subtab, you can narrow down the search based on a cloud tag, by entering a **key** or **value** term. If you want to search based on both terms, click the (+) displayed as a superscript to the **key** or **value** term (depending on which was entered first). Cloud tag filters cannot be edited. To modify a search, first delete the filters, and then enter the desired **key** or **value** term again. Search based on multiple cloud tag filters is supported.

**Step 3** To view a summary pane, click the row that represents the specific component you want to view.

**Step 4** For more information, double-click the summary table row that represents the specific component you want to view.

A new dialog box appears over the **work** pane with any of the following tabs:

**Note** The tabs that appear differ between components and configurations.

- **Overview**—Provides a general overview of cloud resources, configuration relationships, and settings of the component, including the cloud tags associated with endpoints.
- **Cloud Resources**—Contains a list of subtabs that display the cloud resource information related to the component.
- **Application Management**—Contains a list of subtabs that display the ACI relation information related to the component.
- **Event Analytics**—Contains a list of subtabs that display faults, events, and audit logs.

## Viewing Operations Details

This section explains how to view operations details using the Cisco Cloud APIC GUI. The operations details include the information of a specific fault, event, audit log, active sessions, backup and restore policies, tech support policies, firmware management, scheduler policies, and remote locations.

**Step 1** From the **Navigation** menu, choose the **Operations** tab.

When the **Operations** tab expands, a list of subtab options appear. See the *Operations Options* table for more information.

**Table 29: Operations Subtabs**

Subtab Name	Description
<b>Event Analytics</b>	Contains the following subtabs: <ul style="list-style-type: none"> <li>• <b>Faults</b> Tab—Displays faults as rows in a summary table.</li> <li>• <b>Fault Records</b> Tab—Displays fault records as rows in a summary table.</li> <li>• <b>Events</b> Tab—Displays events as rows in a summary table.</li> <li>• <b>Audit Logs</b> Tab—Displays audit logs as rows in a summary table.</li> </ul>
<b>Active Sessions</b>	Displays a list of active users who are logged into Cloud APIC.



Subtab Name	Description
<b>Backup &amp; Restore</b>	Contains the following subtabs: <ul style="list-style-type: none"> <li>• <b>Backups</b> Tab—Displays backup as rows in a summary table.</li> <li>• <b>Backup Policies</b> Tab—Displays backup policies as rows in a summary table.</li> <li>• <b>Job Status</b> Tab—Displays the job status as rows in a summary table.</li> <li>• <b>Event Analytics</b> Tab—Contains the following subtabs:               <ul style="list-style-type: none"> <li>• <b>Faults</b> Tab—Displays faults as rows in a summary table.</li> <li>• <b>Events</b> Tab—Displays events as rows in a summary table.</li> <li>• <b>Audit Logs</b> Tab—Displays audit logs as rows in a summary table.</li> </ul> </li> </ul>
<b>Tech Support</b>	Contains the following subtabs: <ul style="list-style-type: none"> <li>• <b>Tech Support</b> Tab—Displays tech support policies as rows in a summary table.</li> <li>• <b>Core Logs</b> Tab—Displays core logs as rows in a summary table.</li> </ul>
<b>Firmware Management</b>	Contains the following subtabs: <ul style="list-style-type: none"> <li>• <b>Controllers</b> Tab—Displays general firmware management information, such as Current Firmware Version, Upgrade Status, and so on.</li> <li>• <b>Images</b> Tab—Displays a list of images.</li> <li>• <b>Event Analytics</b> Tab—Contains the following subtabs:               <ul style="list-style-type: none"> <li>• <b>Faults</b> Tab—Displays faults as rows in a summary table.</li> <li>• <b>Events</b> Tab—Displays events as rows in a summary table.</li> <li>• <b>Audit Logs</b> Tab—Displays audit logs as rows in a summary table.</li> </ul> </li> </ul>
<b>Schedulers</b>	Displays scheduler policies as rows in a summary table.
<b>Remote Locations</b>	Displays remote locations as rows in a summary table.

**Step 2** Click the tab that represents the component you want to view.

A summary table appears with items as rows in the table. For example, if you chose the **Active Sessions** subtab, a list of active sessions appear as rows in a summary table.

You can filter the rows by clicking the *Filter by Attributes* bar. Choose the attribute, operator and filter-value. For example, for filtering based on a username, choose username == user1 (where user1 is a user logged into Cloud APIC).

**Step 3** To view a summary pane, click the row that represents the specific component you want to view.

**Step 4** For more information, double-click the summary table row that represents the specific item you want to view.

A new dialog box appears over the **work** pane that displays additional information about the item you chose from the summary table.

## Viewing Infrastructure Details

This section explains how to view infrastructure details using the Cisco Cloud APIC GUI. The infrastructure details include information about system configuration, inter-region connectivity, and external connectivity.

**Step 1** From the **Navigation** menu, choose the **Infrastructure** tab.

When the **Infrastructure** tab expands, a list of subtab options appear. See the *Infrastructure Options* table for more information.

*Table 30: Infrastructure Subtabs*

Subtab Name	Description
<b>System Configuration</b>	Displays <b>General</b> system configuration information, <b>Management Access</b> information, <b>Controllers</b> , and <b>Event Analytics</b> .
<b>External Connectivity</b>	Displays one pane with a map that contains the inter-region connectivity view.

**Step 2** Click the tab that represents the component with the details you want to view.

## Viewing Administrative Details

This section explains how to view administrative details using the Cisco Cloud APIC GUI. The administrative details include the information about authentication, security, users, and smart licensing..

**Step 1** From the **Navigation** menu, choose the **Administrative** tab.

When the **Administrative** tab expands, a list of subtab options appear. See the *Administrative Options* table for more information.

Table 31: Administrative Subtabs

Subtab Name	Description
<b>Authentication</b>	<p>Displays the <b>Authentication Default Settings</b>, <b>Login Domains</b>, <b>Providers</b> and <b>Event Analytics</b> subtabs, which contain the information described below:</p> <ul style="list-style-type: none"> <li>• <b>Authentication Default Settings</b> Tab—Displays settings information.</li> <li>• <b>Login Domains</b> Tab—Displays the login domains as rows in a summary table.</li> <li>• <b>Providers</b> Tab—Displays the providers as rows in a summary table.</li> <li>• <b>Event Analytics</b> Tab—Displays the <b>Faults</b>, <b>Events</b>, and <b>Audit Logs</b> subtabs, each with the corresponding information displayed as rows in a summary table.</li> </ul>
<b>Security</b>	<p>Contains the following list of subtabs:</p> <ul style="list-style-type: none"> <li>• <b>Security Default Settings</b> Tab—Enables you to view the default security settings information.</li> <li>• <b>Security Domains</b> Tab—Enables you to view security domain information in a summary table.</li> <li>• <b>Roles</b> Tab—Enables you to view the role information in a summary table.</li> <li>• <b>RBAC Rules</b> Tab—Enables you to view RBAC rule information in a summary table.</li> <li>• <b>Certificate Authorities</b> Tab—Enables you to view the certificate authority information in a summary table.</li> <li>• <b>Key Rings</b> Tab—Enables you to view key ring information in a summary table.</li> <li>• <b>User Activity</b> Tab—Enables you to view user activity.</li> </ul>
<b>Users</b>	<p>Contains the following subtabs:</p> <ul style="list-style-type: none"> <li>• <b>Local</b> Tab—Displays local users as rows in a summary table.</li> <li>• <b>Remote</b> Tab—Displays remote users as rows in a summary table.</li> </ul>

Subtab Name	Description
Smart Licensing	<p>Contains the following subtabs:</p> <ul style="list-style-type: none"> <li>• <b>General</b> Tab—Displays the licenses as rows in a summary table.</li> <li>• <b>CSRs</b> Tab—Displays CSRs as rows in a summary table.</li> <li>• <b>Faults</b> Tab—Displays faults as rows in a summary table.</li> </ul>

**Step 2** Click the tab that represents the component you want to view.

For some options, a summary table appears with items as rows in the table (For example, if you choose the **Users** tab, a list of users appear as rows in a summary table). To view a summary pane, click the row that represents the specific component you want to view. To view more information, double-click the summary table row that represents the specific item you want to view. A new dialog box appears over the **work** pane that displays additional information about the item you chose from the summary table.

You can filter the rows by clicking the *Filter by Attributes* bar. Choose the attribute, operator and filter-value. For example, for filtering based on a user, choose User ID == admin (where admin is a user ID. ).

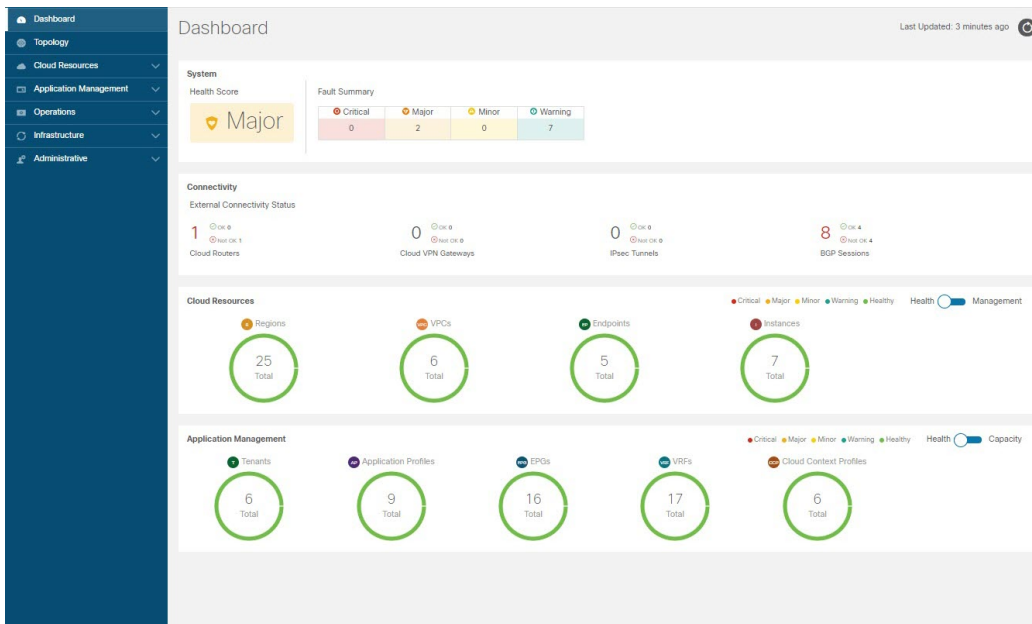
## Viewing Health Details Using the Cisco Cloud APIC GUI

This section explains how to view health details using the Cisco Cloud APIC GUI. You can view health details for any object that you can see in the Cloud Resources area in the Cisco Cloud APIC GUI, such as the following:

- Regions
- VPCs
- Endpoints
- Instances

**Step 1** From the **Navigation** menu, choose the **Dashboard** tab.

The **Dashboard** window for the Cisco Cloud APIC system appears. From this window, you can view the overall health status of your system.



**Step 2** Click within the Fault Summary area in the **Dashboard** window.

The **Event Analytics** window appears, showing more detailed information for the specific fault level that you clicked. The following screen shows an example **Event Analytics** window for the faults listed with critical severity.

The screenshot shows the Cisco Cloud APIC GUI Event Analytics window. The left sidebar is the same as in the dashboard. The main content area is titled 'Event Analytics' and has tabs for Faults, Fault Records, Events, and Audit Logs. The 'Faults' tab is selected, and the severity is set to 'Major'. The table below shows two fault records:

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Major	F3881	failedoperholder/failedoper-[acct-tenant1]/region-[global]/ctxprofile-[tenant1]/vrf/peer-[acc-[int]/region-[global]/ctxprofile-[overlay-1]]/ctxpeeroper	Operational State of hcloud.CtxPeer: json: invalid use of string struct tag, trying to unmarshal "project/gcp-ganandkcapic-nprd-67033/global/networks/" into uint84	raised	Aug 28 2021 01:04:51pm -07:00
<input type="checkbox"/>	Major	F3553	failedoperholder/failedoper-[acct-tenant1]/region-[global]/ctxprofile-[tenant1]/vrf/peer-[acc-[int]/region-[global]/ctxprofile-[overlay-1]]/ctxpeeroper	Operational error from Event Channel driver: unable to initialize Event Driver Topic: rpc error: code = PermissionDenied desc = User not authorized to perform this action.	raised	Sep 02 2021 08:52:34pm -07:00

**Step 3** Click the **X** next to the Severity level to display Event Analytics information for all faults.

The information provided in the **Event Analytics** window changes to show the events with critical, major, and warning levels of severity.

## Viewing Health Details Using the Cisco Cloud APIC GUI

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Major	F3881	failedoperholder/failedoper-[acct-tenant1]region-[global]chprofile-[tenant1vrf]cxpPeer-[acct-tenant1]region-[global]chprofile-[overlay-1]]cxpPeeroper	Operational State of hcloud.CtxPeer: json: invalid use of string struct tag, trying to unmarshal 'projects/gcp-gandalfacp-nprid-67033/global/networks/' into uint64	raised	Aug 28 2021 01:04:51pm -07:00
<input type="checkbox"/>	Major	F3553	failedoperholder/failedoper-[acct-TenantTest]igenericerror	Operational error from Event Channel driver: unable to initialize Event Driver Topic: rpc error: code = PermissionDenied desc = User not authorized to perform this action.	raised	Sep 02 2021 08:52:34pm -07:00
<input type="checkbox"/>	Warning	F3057	licensecont/manager	APIC is in 90 days evaluation period. Navigate to System -> Smart Licensing to register.	raised	Sep 07 2021 11:21:47am -07:00
<input type="checkbox"/>	Warning	F0967	uri/tn-tenant1/cloudapp-external-ap/cloudextepg-internet/rscons-Allow_access-to_Wordpress	Failed to form relation to MO brc-Allow_access-to_Wordpress of class vzbRCP in context	raised	Sep 07 2021 11:18:21am -07:00
<input type="checkbox"/>	Warning	F0974	uri/tn-tenant1/cloudapp-external-ap/cloudextepg-internet/rsprov-allow-linux-app-http-https-access	Failed to form relation to MO brc-allow-linux-app-http-https-access of class vzbRCP in context	raised	Sep 07 2021 11:18:21am -07:00
<input type="checkbox"/>	Warning	F0967	uri/tn-tenant1/cloudapp-linuxapp-ap/cloudextepg-app2/rscons-allow-linux-app-http-https-access	Failed to form relation to MO brc-allow-linux-app-http-https-access of class vzbRCP in context	raised	Sep 07 2021 11:18:21am -07:00
<input type="checkbox"/>	Warning	F0967	uri/tn-tenant1/cloudapp-linuxapp-ap/cloudextepg-app1/rscons-allow-linux-app-http-https-access	Failed to form relation to MO brc-allow-linux-app-http-https-access of class vzbRCP in context	raised	Sep 07 2021 11:18:21am -07:00
<input type="checkbox"/>	Warning	F0974	uri/tn-tenant2/cloudapp-frontent/cloudapp-frontent/rsprov-allow-nodejs-app-access	Failed to form relation to MO brc-allow-nodejs-app-access of class vzbRCP in context	raised	Sep 07 2021 11:18:19am -07:00
<input type="checkbox"/>	Warning	F0967	uri/tn-tenant2/cloudapp-external/cloudextepg-external-epg/rscons-allow-nodejs-app-access	Failed to form relation to MO brc-allow-nodejs-app-access of class vzbRCP in context	raised	Sep 07 2021 11:18:19am -07:00

**Step 4** From the **Navigation** menu, choose the **Cloud Resources** tab.

When the **Cloud Resources** tab expands, a list of subtab options appear. See the *Administrative Options* table for more information.

**Step 5** Choose any item under the **Cloud Resources** tab to display health information for that component.

For example, the following figure shows health information that might be displayed when you click on **Cloud Resources > Regions**. The health of each region is displayed in the left column of the table in the **Regions** window.

Health	Name	Admin State	Application Management			Cloud Resources	
			Tenants	EPGs	VPCs	Routers	Endpoints
Healthy	asia-east1	managed	0	0	0	0	0
Healthy	asia-east2	managed	0	0	0	0	0
Healthy	asia-northeast1	managed	0	0	0	0	0
Healthy	asia-northeast2	managed	0	0	0	0	0
Healthy	asia-northeast3	managed	0	0	0	0	0
Healthy	asia-south1	managed	0	0	0	0	0
Healthy	asia-southeast1	managed	0	0	0	0	0
Healthy	asia-southeast2	managed	0	0	0	0	0
Healthy	australia-southeast1	managed	0	0	0	0	0
Healthy	europa-central2	managed	0	0	0	0	0
Healthy	europa-north1	managed	0	0	0	0	0
Healthy	europa-west1	managed	0	0	0	0	0
Healthy	europa-west2	managed	0	0	0	0	0
Healthy	europa-west3	managed	0	0	0	0	0
Healthy	europa-west4	managed	0	0	0	0	0
Healthy	europa-west6	managed	0	0	0	0	0
Healthy	northamerica-northeast1	managed	0	0	0	0	0
Healthy	southamerica-east1	managed	0	0	0	0	0
Healthy	us-central1	managed	4	0	0	5	0



## CHAPTER 7

# Cisco Cloud APIC Statistics

---

- [About Google Cloud Statistics, on page 119](#)
- [Guidelines and Limitations For Configuring Google Cloud Statistics, on page 120](#)
- [Enabling Flow Log Statistics, on page 120](#)
- [Viewing Flow Log Statistics, on page 121](#)
- [Enabling VPC Flow Log Statistics Using the REST API, on page 123](#)

## About Google Cloud Statistics

Beginning in Cisco Cloud APIC Release 25.0(4), you can view statistics that are derived by processing Google Cloud flow logs.

### Flow Log Statistics

Cisco Cloud APIC allows you to enable flow log statistics for individual cloud context profiles within a tenant. When statistics are enabled for a cloud context profile, statistics are collected for every IP address within the corresponding VPCs. Available statistics include ingress and egress bytes and packets, internal and external, for VPCs, regions, and endpoints.

The collected statistics are aggregated through the following hierarchy:

- IP statistics are aggregated to determine endpoint statistics.
- Endpoint statistics are aggregated to determine zone statistics.
- Zone statistics are aggregated to determine subnet statistics.
- Subnet statistics are aggregated to determine region statistics.
- Region statistics are aggregated to determine VPC statistics.

The Cisco Cloud APIC GUI displays the collected statistics for VPCs, regions, and endpoints.

For more information about Google Cloud flow logs, see "VPC Flow Logs" on the Google Cloud website.

# Guidelines and Limitations For Configuring Google Cloud Statistics

Following are the guidelines and limitations when configuring Cisco Cloud APIC to collect Google Cloud statistics:

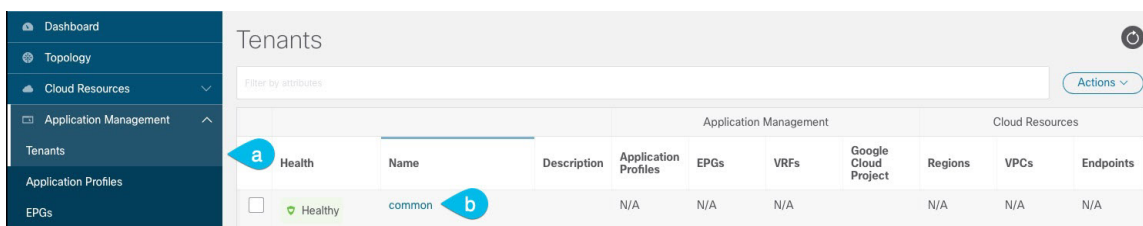
- The flow log statistics feature is not enabled by default.
- Flow log statistics can be enabled for individual context profiles within a tenant. In this case, flow logs are enabled on all subnets belonging to the corresponding VPC.
- Flow logs are aggregated at one minute intervals. The aggregation interval and sample rate are not configurable.
- Statistics for dropped traffic are not supported by flow logs.
- Statistics filters are not supported.
- Zone and subnet statistics are not displayed.

## Enabling Flow Log Statistics

You can enable the collection of Google Cloud flow log statistics for individual context profiles within a tenant. Statistics can then be viewed for VPCs, regions, and endpoints in their respective **Cloud Resources** GUI menus.

To enable flow log statistics using the Cisco Cloud APIC GUI:

**Step 1** Select the tenant containing the resource for which flow log statistics will be enabled.



a) From the navigation menu, select **Application Management > Tenants**.

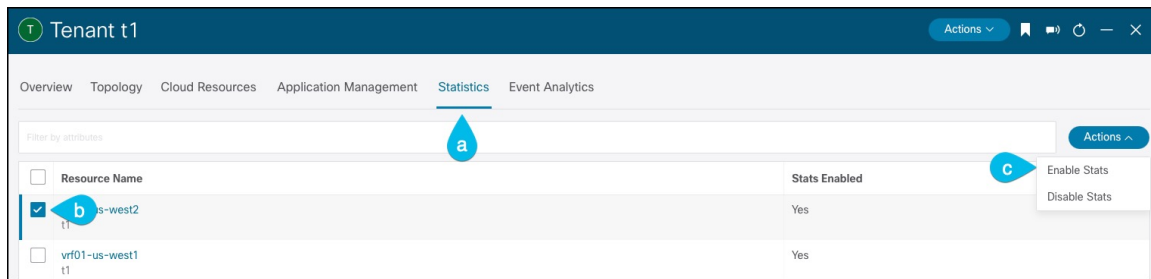
A **Tenants** summary table appears in the work pane.

b) In the summary table, double-click the name of the tenant.

The tenant dialog box appears over the work pane. The tenant dialog box displays the **Overview**, **Topology**, **Cloud Resources**, **Application Management**, **Statistics**, and **Event Analytics** tabs.

**Step 2** Enable flow log statistics collection on the desired resource.





a) In the tenant dialog box, select the **Statistics** tab.

A **Resource Name** table appears with context profiles listed as rows in the table. The **Stats Enabled** column indicates whether flow log statistics are enabled for each resource.

b) Check the checkbox next to the desired resource.

c) In the top right of the tenant dialog box, click the **Actions** menu and select **Enable Stats**.

## Viewing Flow Log Statistics

In the Cisco Cloud APIC GUI, you can view graphed statistics for VPCs, regions, and endpoints. Available statistics for each include ingress and egress bytes and packets. For VPCs and regions, the statistics are further separated into the following categories:

- **Statistics:** All traffic counters extracted from the flow logs records.
- **Inter-Region Statistics:** For a particular region, all ingress and egress traffic to or from other regions within the VPC.
- **External Statistics:** All ingress and egress traffic with a source or destination outside of the VPC.
- **Inter-Zone Statistics:** For a particular zone, all ingress and egress traffic to or from other zones within the same region and VPC. These aggregated statistics are available on the region page and on the VPC page.

Peak values for each counter are displayed with a timestamp that shows when the peak value occurred.

This example procedure shows you how to view the flow log statistics for VPCs in the Cisco Cloud APIC GUI. You can also view the statistics for regions or endpoints in the same manner by selecting **Regions** or **Endpoints** instead of **VPCs** in the following steps.

### Before you begin

Enable Google Cloud flow log statistics for the desired cloud context profile using the procedure in [Enabling Flow Log Statistics, on page 120](#).

**Step 1** Select the resource whose statistics you would like to view.

## Viewing Flow Log Statistics

Filter by attributes		Application Management							Cloud Resources		
Name	Cloud Access Privilege	Cloud Provider ID	Oper State	Cloud Context Profile	EPGs	VRFs	VPC peers	Routers	Endpoints		
Healthy vpc-3 t1 > global	Not Applicable	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		
Healthy vpc-4 t1 > global	Not Applicable	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		

a) From the navigation menu, select **Cloud Resources > VPCs**.

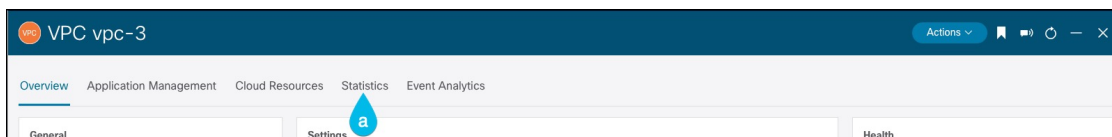
A **VPCs** summary table appears in the work pane.

b) In the summary table, double-click the name of the VPC.

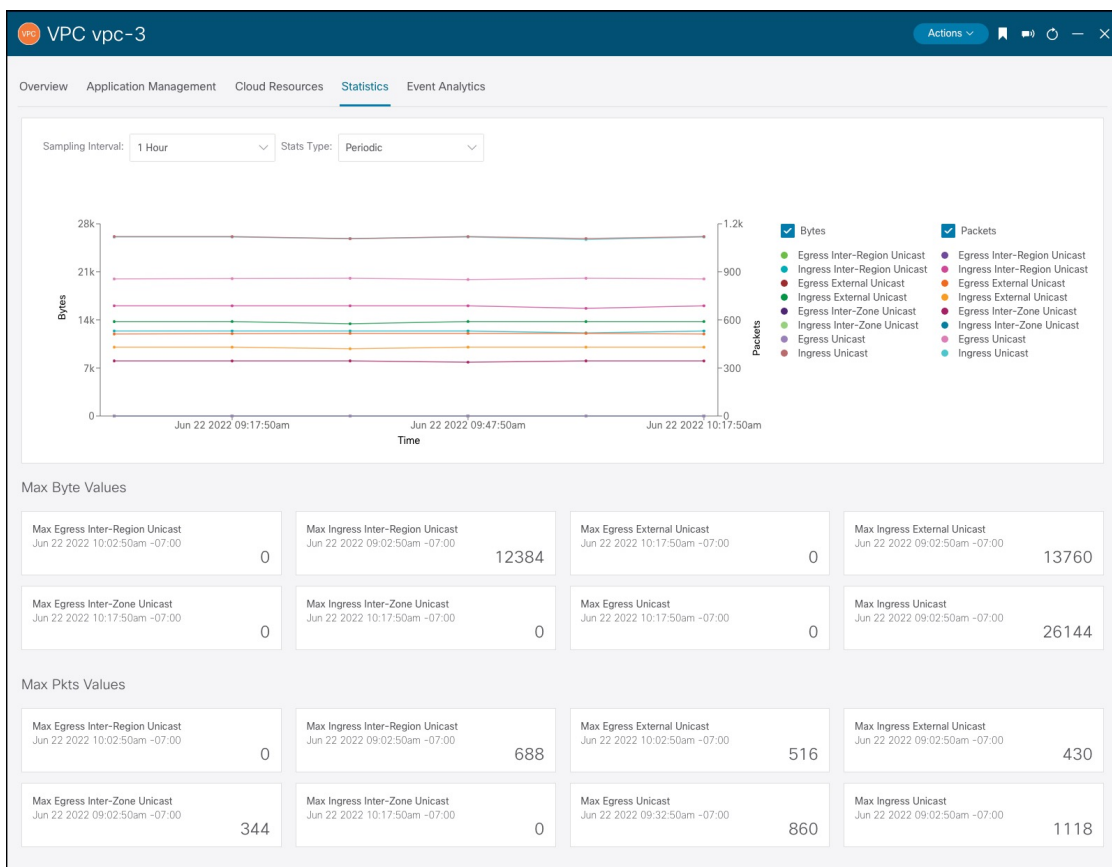
The VPC dialog box appears over the work pane. The VPC dialog box displays the **Overview**, **Application Management**, **Cloud Resources**, **Statistics**, and **Event Analytics** tabs.

## Step 2

Click the **Statistics** tab.



A graphical view of the VPC statistics appears along with a table of maximum values.



**Step 3** Configure the display of the statistics.

To configure the parameters of the displayed statistics, you can modify the following settings:

Properties	Description
<b>Sampling Interval</b>	Choose the interval: <ul style="list-style-type: none"> <li>• 1 hour</li> <li>• 12 Hours</li> <li>• 1 Day</li> <li>• 1 Week</li> <li>• 1 Month</li> </ul>
<b>Stats Type</b>	Choose the display type: <ul style="list-style-type: none"> <li>• Periodic</li> <li>• Cumulative</li> <li>• Trend</li> <li>• Rate</li> </ul>
<b>Bytes</b>	Check the checkbox to display the byte counter graph. The vertical axis on the left side of the graph indicates the byte count.
<b>Packets</b>	Check the checkbox to display the packet counter graph. The vertical axis on the right side of the graph indicates the packet count.

## Enabling VPC Flow Log Statistics Using the REST API

Google Cloud flow log statistics can be enabled for individual context profiles within a tenant.

**Step 1** Define a flow log policy (`cloudGcpFlowLogPol`) under the tenant.

No configuration settings are needed except for the name.

**Note** For the name of the flow log policy, note the following restrictions:

- Match the regular expression:

```
[a-z]([-a-z0-9]*[a-z0-9])?
```

This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name.

**Example:**

```

<polUni>
  <fvTenant name="tenant1" status="">
    <cloudGcpFlowLogPol name="myFlowLogPol1" status="">
    </cloudGcpFlowLogPol>
    <cloudCtxProfile name="ctxProfile2" status="" vpcGroup="vpc-4">
    .
    .
    .

```

**Step 2** Within the cloud context profile, add a reference to the flow log policy.

Flow log statistics for the cloud context profile are enabled by the presence of the reference object (`cloudRsCtxToGcpFlowLog`). To disable flow log statistics for the cloud context profile, remove the reference object.

**Example:**

```

.
.
.
    <cloudRsCtxToGcpFlowLog tnCloudGcpFlowLogPolName="myFlowLogPol1" status=""/>
  </cloudCtxProfile>
</fvTenant>
</polUni>

```

---



## CHAPTER 8

# Cisco Cloud APIC Security

---

This chapter contains the following sections:

- [Access, Authentication, and Accounting, on page 125](#)
- [Configuring TACACS+, RADIUS, LDAP and SAML Access, on page 126](#)
- [Configuring HTTPS Access, on page 134](#)

## Access, Authentication, and Accounting

Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) policies manage the authentication, authorization, and accounting (AAA) functions. The combination of user privileges, roles, and domains with access rights inheritance enables administrators to configure AAA functions at the managed object level in a granular fashion. These configurations can be implemented using the REST API or the GUI.



---

**Note** There is a known limitation where you cannot have more than 32 characters for the login domain name. In addition, the combined number of characters for the login domain name and the user name cannot exceed 64 characters.

---

For more access, authentication, and accounting configuration information, see *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

## Configuration

The admin account is configured in the initial configuration script, and the admin is the only user when the system starts.

### Configuring a Local User

Refer to [Creating a Local User Using the Cisco Cloud APIC GUI, on page 93](#) to configure a Local User and associate it to the OTP, SSH Public Key, and X.509 User Certificate using the Cisco Cloud APIC GUI.

# Configuring TACACS+, RADIUS, LDAP and SAML Access

The following topics describe how to configure TACACS+, RADIUS, LDAP and SAML access for the Cisco Cloud APIC.

## Overview

This topic provides step-by-step instructions on how to enable access to the Cisco Cloud APIC for RADIUS, TACACS+, LDAP, and SAML users, including ADFS, Okta, and PingID.

For additional TACACS+, RADIUS, LDAP, and SAML information, see *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

## Configuring Cloud APIC for TACACS+ Access

### Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.
- The TACACS+ server host name or IP address, port, and key are available.
- The Cloud APIC management endpoint group is available.

**Step 1** In the Cloud APIC, create the **TACACS+ Provider**.

- On the menu bar, choose **Administrative > Authentication**.
- In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

- In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.
- In the **Description** field, enter a description of the provider.
- Click the **Type** drop-down list and choose **TACACS+**.
- In **Settings** section, specify the **Key** and **Confirm Key**, **Port**, **Authentication Protocol**, **Timeout**, **Retries**, **Management EPG**. Select either **Enabled** or **Disabled** for **Server Monitoring**.

**Step 2** Create the **Login Domain** for TACACS+.

- On the menu bar, choose **Administrative > Authentication**.
- In the Work pane, click on **Login Domains** tab and then click on the **Actions** drop-down and select **Create Login Domain**.

The **Create Login Domain** dialog box appears.

- Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
General	

Properties	Description
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
<b>Settings</b>	
Realm	Choose <b>TACACS+</b> from the dropdown menu
Providers	To choose a Provider(s): <ol style="list-style-type: none"> <li>1. Click <b>Add Providers</b>. The <b>Select Providers</b> dialog appears.</li> <li>2. Click to choose a provider(s) in the column on the left.</li> <li>3. Click <b>Select</b>. You return to the <b>Create Login Domain</b> dialog box.</li> </ol>

- d) Click **Save** to save the configuration.

#### What to do next

This completes the TACACS+ configuration steps. Next, if a RADIUS server will also be used, configure the Cisco Cloud APIC for RADIUS.

## Configuring Cloud APIC for RADIUS Access

#### Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.
- The RADIUS server host name or IP address, port, and key are available.
- The Cloud APIC management endpoint group is available.

#### Step 1

In the Cloud APIC, create the **RADIUS Provider**.

- On the menu bar, choose **Administrative > Authentication**.
- In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

- In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.
- In the **Description** field, enter a description of the provider.
- Click the **Type** drop-down list and choose **RADIUS**.
- In the **Settings** section, specify the **Key** and **Confirm Key**, **Port**, **Authentication Protocol**, **Timeout**, **Retries**, **Management EPG**. Select either **Enabled** or **Disabled** for **Server Monitoring**.

**Step 2** Create the **Login Domain** for **RADIUS**.

- a) On the menu bar, choose **Administrative > Authentication**.
- b) In the Work pane, click on **Login Domains** tab and then click on the **Actions** drop-down and select **Create Login Domain**.

The **Create Login Domain** dialog box appears.

- c) Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
<b>General</b>	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
<b>Settings</b>	
Realm	Choose <b>RADIUS</b> from the dropdown menu
Providers	To choose a Provider(s): <ol style="list-style-type: none"> <li>1. Click <b>Add Providers</b>. The <b>Select Providers</b> dialog appears.</li> <li>2. Click to choose a provider(s) in the column on the left.</li> <li>3. Click <b>Select</b>. You return to the <b>Create Login Domain</b> dialog box.</li> </ol>

- d) Click **Save** to save the configuration.

**What to do next**

This completes the Cloud APIC RADIUS configuration steps. Next, configure the RADIUS server.

## Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the Cloud APIC

Refer to the section *Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the APIC* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.



## Configuring LDAP Access

There are two options for LDAP configurations:

- Configure a Cisco AVPair
- Configure LDAP group maps in the cloud APIC

The following sections contain instructions for both configuration options.

### Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair

---

Refer to the section *Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

---

### Configuring Cloud APIC for LDAP Access

#### Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.
- The LDAP server host name or IP address, port, bind DN, Base DN, and password are available.
- The cloud APIC management endpoint group is available.

#### Step 1

In the Cloud APIC, create the **LDAP Provider**.

- a) On the menu bar, choose **Administrative > Authentication**.
- b) In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

- c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.
- d) In the **Description** field, enter a description of the provider.
- e) Click the **Type** drop-down list and choose **LDAP**.
- f) Specify the **Bind DN**, **Base DN**, **Password**, **Confirm Password**, **Port**, **Timeout**, **Retries**, **SSL**, **SSL Certificate Validation Level**, **Attribute**, **Filter Type**, **Management EPG**, and **Server Monitoring**.

In the **SSL Certificate Validation Level** field, you have the following options:

- **Permissive**: A debugging knob to help diagnose DUO LDAP SSL Certificate issues.
- **Strict**: A level that should be used when in production.

- Note**
- The bind DN is the string that the Cloud APIC uses to log in to the LDAP server. The Cloud APIC uses this account to validate the remote user attempting to log in. The base DN is the container name and path in the LDAP server where the Cloud APIC searches for the remote user account. This is where the password is validated. Filter is used to locate the attribute that the Cloud APIC requests to use for the *cisco-av-pair*. This contains the user authorization and assigned RBAC roles for use on the Cloud APIC. The Cloud APIC requests the attribute from the LDAP server.
  - **Attribute** field—Enter one of the following:
    - For LDAP server configurations with a Cisco AVPair, enter **CiscoAVPair**.
    - For LDAP server configurations with an LDAP group map, enter **memberOf**.

**Step 2** Create the **Login Domain** for LDAP.

- On the menu bar, choose **Administrative > Authentication**.
- In the Work pane, click on **Login Domains** tab and then click on the **Actions** drop-down and select **Create Login Domain**.
- Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
<b>Settings</b>	
Realm	Choose <b>LDAP</b> from the dropdown menu
Providers	<p>To choose a Provider(s):</p> <ol style="list-style-type: none"> <li>1. Click <b>Add Providers</b>. The <b>Select Providers</b> dialog appears.</li> <li>2. Click to choose a provider(s) in the column on the left.</li> <li>3. Click <b>Select</b>. You return to the <b>Create Login Domain</b> dialog box.</li> </ol>

Properties	Description
Authentication Type	<ol style="list-style-type: none"> <li>1. Select <b>Cisco AV Pairs</b>, if provider(s) was configured with <b>CiscoAVPair</b> as the <b>Attribute</b>.</li> <li>2. Select <b>LDAP Group Map Rules</b>, if provider(s) was configured with <b>memberOf</b> as the <b>Attribute</b>. <ol style="list-style-type: none"> <li>a. Click <b>Add LDAP Group Map Rule</b>. The dialog box appears.</li> <li>b. Specify the map rule <b>Name</b>, <b>Description</b> (optional), and <b>Group DN</b>.</li> <li>c. Click the + next to <b>Add Security Domain</b>. The dialog box appears.</li> <li>d. Select the security domain using the <b>Select Security Domain</b> option.</li> <li>e. Click the + to access the <b>Role</b> name and <b>Role Privilege Type</b> (<b>Read</b> or <b>Write</b>) fields. Click check mark.</li> <li>f. If necessary, repeat the previous step to add more roles. Then click <b>Add</b>.</li> <li>g. If you want to add more security domains, click the + next to <b>Add Security Domain</b>, then follow those steps again. Then click <b>Add</b>.</li> </ol> </li> </ol>

d) Click **Save** on Create Login Domain dialog box.

## Configuring Cloud APIC for SAML Access

The following sections provide detailed information on configuring Cloud APIC for SAML access.

### About SAML

Refer to the section *About SAML* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

### Basic Elements of SAML

Refer to the section *Basic Elements of SAML* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

### Supported IdPs and SAML Components

Refer to the section *Supported IdPs and SAML Components* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

## Configuring Cloud APIC for SAML Access




---

**Note** SAML based Authentication is only for Cloud APIC GUI and not for REST.

---

### Before you begin

- The SAML server host name or IP address, and the IdP's metadata URL are available.
- The Cloud APIC management endpoint group is available.
- Set up the following:
  - Time Synchronization and NTP
  - Configuring a DNS Provider Using the GUI
  - Configuring a Custom Certificate for Cisco ACI HTTPS Access Using the GUI

### Step 1

In the Cloud APIC, create the **SAML Provider**.

- a) On the menu bar, choose **Administrative > Authentication**.
- b) In the **Work** pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.
- c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.
- d) In the **Description** field, enter a description of the provider.
- e) Click the **Type** drop-down list and choose **SAML**.
- f) In **Settings** pane, perform following:
  - Choose the **Identity Provider** option (**ADFS**, **OKTA**, or **PING IDENTITY**).
  - Specify the IdP metadata URL:
    - In case of AD FS, IdP Metadata URL is of the format *https://<FQDN ofADFS>/FederationMetadata/2007-06/FederationMetadata.xml*.
    - In case of Okta, to get the IdP Metadata URL, copy the link for **Identity Provider Metadata URL** in the **Sign On** section of the corresponding SAML Application from the Okta server.
  - Specify the **Entity ID** for the SAML-based service.
  - Configure the **HTTPS Proxy for Metadata URL** if it is needed to access the IdP metadata URL.
  - Enter a value in the **GUI Redirect Banner Message (URL)** field.
  - Select the **Certificate Authority** if IdP is signed by a Private CA.
  - Enter a value in the **Timeout (sec)** field.

- Enter a value in the **Retries** field.
- Select the **Signature Algorithm Authentication User Requests** from the drop-down.
- Select checkbox to enable **Sign SAML Authentication Requests, Sign SAML Response Message, Sign Assertions in SAML Response, Encrypt SAML Assertions**.

g) Click **Save** to save the configuration.

## Step 2

Create the login domain for SAML.

- On the menu bar, choose **Administrative > Authentication**.
- In the **Work** pane, click on the **Login Domains** tab and then click on the **Actions** drop-down and select **Create Login Domain**.
- Enter the appropriate values in each field as listed in the following Create Login Domain Dialog Box Fields table then continue.

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
<b>Settings</b>	
Realm	Choose <b>SAML</b> from the dropdown menu
Providers	<p>To choose a Provider(s):</p> <ol style="list-style-type: none"> <li>1. Click <b>Add Providers</b>. The <b>Select Providers</b> dialog appears.</li> <li>2. Click to choose a provider(s) in the column on the left.</li> <li>3. Click <b>Select</b>. You return to the <b>Create Login Domain</b> dialog box.</li> </ol>

d) Click **Save** to save the configuration.

## Setting Up a SAML Application in Okta

Refer to the section *Setting Up a SAML Application in Okta* of *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

## Setting Up a Relying Party Trust in AD FS

---

Refer to the section *Setting Up a Relying Party Trust in AD FS* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

---

## Configuring HTTPS Access

The following sections describe how to configure HTTPS access.

### About HTTPS Access

This article provides an example of how to configure a custom certificate for HTTPS access when using Cisco ACI.

For more information, see the section *HTTPS Access* in the *Cisco APIC Security Configuration Guide, Release 4.0(1)* at <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html>.

### Guidelines for Configuring Custom Certificates

- Wild card certificates (such as \*.cisco.com, which is used across multiple devices) and its associated private key generated elsewhere are not supported on the Cisco Cloud APIC as there is no support to input the private key or password in the Cisco Cloud APIC. Also, exporting private keys for any certificates, including wild card certificates, is not supported.
- You must download and install the public intermediate and root CA certificates before generating a Certificate Signing Request (CSR). Although a root CA Certificate is not technically required to generate a CSR, Cisco requires the root CA certificate before generating the CSR to prevent mismatches between the intended CA authority and the actual one used to sign the CSR. The Cisco Cloud APIC verifies that the certificate submitted is signed by the configured CA.
- To use the same public and private keys for a renewed certificate generation, you must satisfy the following guidelines:
  - You must preserve the originating CSR as it contains the public key that pairs with the private key in the key ring.
  - The same CSR used for the originating certificate must be resubmitted for the renewed certificate if you want to re-use the public and private keys on the Cisco Cloud APIC.
  - Do not delete the original key ring when using the same public and private keys for the renewed certificate. Deleting the key ring will automatically delete the associated private key used with CSRs.
- Only one Certificate Based Root can be active per pod.
- Client Certificate based authentication is not supported for this release.

# Configuring a Custom Certificate for Cisco Cloud APIC HTTPS Access Using the GUI

Determine from which authority you will obtain the trusted certification so that you can create the appropriate Certificate Authority.

## Before you begin

CAUTION: PERFORM THIS TASK ONLY DURING A MAINTENANCE WINDOW AS THERE IS A POTENTIAL FOR DOWNTIME. Expect a restart of all web servers on Cloud APIC during this operation.

- 
- Step 1** On the menu bar, choose **Administrative > Security**.
- Step 2** In the Work pane, click on **Certificate Authorities** tab and then click on the **Actions** drop-down and select **Create Certificate Authority**.
- Step 3** In the **Create Certificate Authority** dialog box, in the **Name** field, enter a name for the certificate authority and in the **Description** field, enter a description.
- Step 4** Select **System** in the **Used for** field.
- Step 5** In the **Certificate Chain** field, copy the intermediate and root certificates for the certificate authority that will sign the Certificate Signing Request (CSR) for the Cloud Application Policy Infrastructure Controller (Cloud APIC). The certificate should be in Base64 encoded X.509 (CER) format. The intermediate certificate is placed before the root CA certificate. It should look similar to the following example:
- ```
-----BEGIN CERTIFICATE-----  
<Intermediate Certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root CA Certificate>  
-----END CERTIFICATE-----
```
- Step 6** Click **Save**.
- Step 7** On the menu bar, choose **Administrative > Security**.
- Step 8** In the Work pane, click on the **Key Rings** tab, then click on the **Actions** drop-down and select **Create Key Ring**.
- Step 9** In the **Create Key Ring** dialog box, enter a name for the key ring in the **Name** field and a description in the **Description** field.
- Step 10** Select **System** in the **Used for** field.
- Step 11** For the **Certificate Authority** field, click on **Select Certificate Authority** and select the Certificate Authority that you created earlier.
- Step 12** Select either **Generate New Key** or **Import Existing Key** for the field **Private Key**. If you select **Import Existing Key**, enter a private key in the **Private Key** text box.
- Step 13** Select modulus from the **Modulus** drop-down menu.
- Step 14** In the **Certificate** field, do not add any content.
- Step 15** Click **Save**.
- In the **Work** pane, in the **Key Rings** area, the **Admin State** for the key ring created displays **Started**.
- Step 16** Double-click on the created Key Ring to open **Key Ring** *key\_ring\_name* dialog box from the **Work** pane.
- Step 17** In the **Work** pane, click on **Create Certificate Request**.
- Step 18** In the **Subject** field, enter the fully qualified domain name (FQDN) of the Cloud APIC.

**Step 19** Fill in the remaining fields as appropriate.

**Step 20** Click **Save**.

The **Key Ring** *key\_ring\_name* dialog box appears.

**Step 21** Copy the contents from the field Request to submit to the **Certificate Authority** for signing.

**Step 22** From the **Key Ring** *key\_ring\_name* dialog box, click on edit icon to display the **Key Ring** *key\_ring\_name* dialog box.

**Step 23** In the **Certificate** field, paste the signed certificate that you received from the certificate authority.

**Step 24** Click **Save** to return to the **Key Rings** work pane.

The key is verified, and in the **Work** pane, the **Admin State** changes to **Completed** and is now ready for use in the HTTPS policy.

**Step 25** Navigate to **Infrastructure > System Configuration**, then click the **Management Access** tab.

**Step 26** Click the edit icon on the **HTTPS** work pane to display the **HTTPS Settings** dialog box.

**Step 27** Click on **Admin Key Ring** and associate the Key Ring that you created earlier.

**Step 28** Click **Save**.

All web servers restart. The certificate is activated, and the non-default key ring is associated with HTTPS access.

---

### What to do next

You must remain aware of the expiration date of the certificate and take action before it expires. To preserve the same key pair for the renewed certificate, you must preserve the CSR, as it contains the public key that pairs with the private key in the key ring. Before the certificate expires, the same CSR must be resubmitted. Do not delete or create a new key ring, as deleting the key ring will delete the private key stored internally on the Cloud APIC.