Cisco Cloud APIC for Azure Installation Guide, Release 25.0(1)-25.0(4)

First Published: 2021-09-20

Last Modified: 2022-12-30

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. 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

CHAPTER 1

New and Changed Information

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 PAYG Licensing Model on Cisco Catalyst 8000V in Cisco Cloud APIC	Cisco Cloud APIC supports Pay-As-You-Go (PAYG) Licensing Model on Cisco Catalyst 8000V which allows users to deploy a Catalyst 8000V instance in the cloud based on the VM size and purchase the usage on an hourly basis.	

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	The following terms are used for the two types of routers described above: • **CSR**: Short for Cloud Services Router. Refers to the Cisco Cloud Services Router 1000v, used in releases prior to release 25.0(3). • **CCR**: Short for Cisco Cloud Router. Refers to the Cisco Catalyst 8000V, used in release 25.0(3) and later. In addition, throughout this document, **CCR** is used as a generic term for either of the routers described above, depending on your release.	
Change in name of Multi-Site Orchestrator	Cisco ACI Multi-SiteOrchestrator (MSO) has changed to Cisco Nexus Dashboard Orchestrator (NDO) beginning with the MSO release 3.4.1 on August 15, 2021. Every instance of MSO is now NDO in this Cisco Cloud APIC documentation.	

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

Feature or Change	Description	Where Documented
Change in release numbering for Cisco Cloud APIC	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: • 4.1(x) (support for AWS only) • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(x) (this release)	

Feature or Change	Description	Where Documented
Updates to external connectivity options	Beginning with release 25.0(1), support is now available for IPv4 connectivity from the infra VPC/VNet CCRs and cloud native routers to any external device, including to another cloud native router. In addition, support is also available for external connectivity between cloud native routers in the same cloud or between two different cloud vendors.	
Support for configuring routing and security policies separately	Prior to release 25.0(1), routing and security policies are tightly coupled together through contracts. Beginning with release 25.0(1), support is now available for configuring routing and security policies separately.	

CHAPTER 2

Overview

Extending the Cisco ACI Fabric to the Public Cloud

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 Multi-Site fabric to Amazon Web Services (AWS) public clouds.

Beginning in APIC Release 4.2(1), Cisco ACI can also use Cisco Cloud APIC to extend a Multi-Site fabric to Microsoft Azure public clouds.

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 Amazon AWS or Microsoft Azure public clouds.
- Automates the deployment and configuration of cloud connectivity.
- Configures the cloud router control plane.
- Configures the data path between the on-premises Cisco ACI fabric and the cloud site.
- Translates Cisco ACI policies to cloud native policies.
- Discovers endpoints.

How Users Can Benefit from Cisco ACI Extension to the Public Cloud

Cisco Cloud APIC is a key part of Cisco ACI extension to the public cloud. Cisco Cloud APIC provides consistent policy, security, and analytics for workloads deployed either on or across on-premises data centers and the public cloud.

Cisco ACI extension to the public cloud also provides an automated connection between on-premises data centers and the public cloud with easy provisioning and monitoring. It also provides a single point for managing, monitoring, and troubleshooting policies across on-premises data centers and the public cloud or between cloud sites.

Azure Government Support

Starting with Release 4.2(3), Cisco Cloud APIC supports Azure Government for on-premises-to-cloud connectivity (Hybrid-Cloud and Hybrid Multi-Cloud), cloud site-to-cloud site connectivity (Multi-Cloud), and single-cloud configurations (Cloud First).

Cisco Cloud APIC supports the following Azure Government regions:

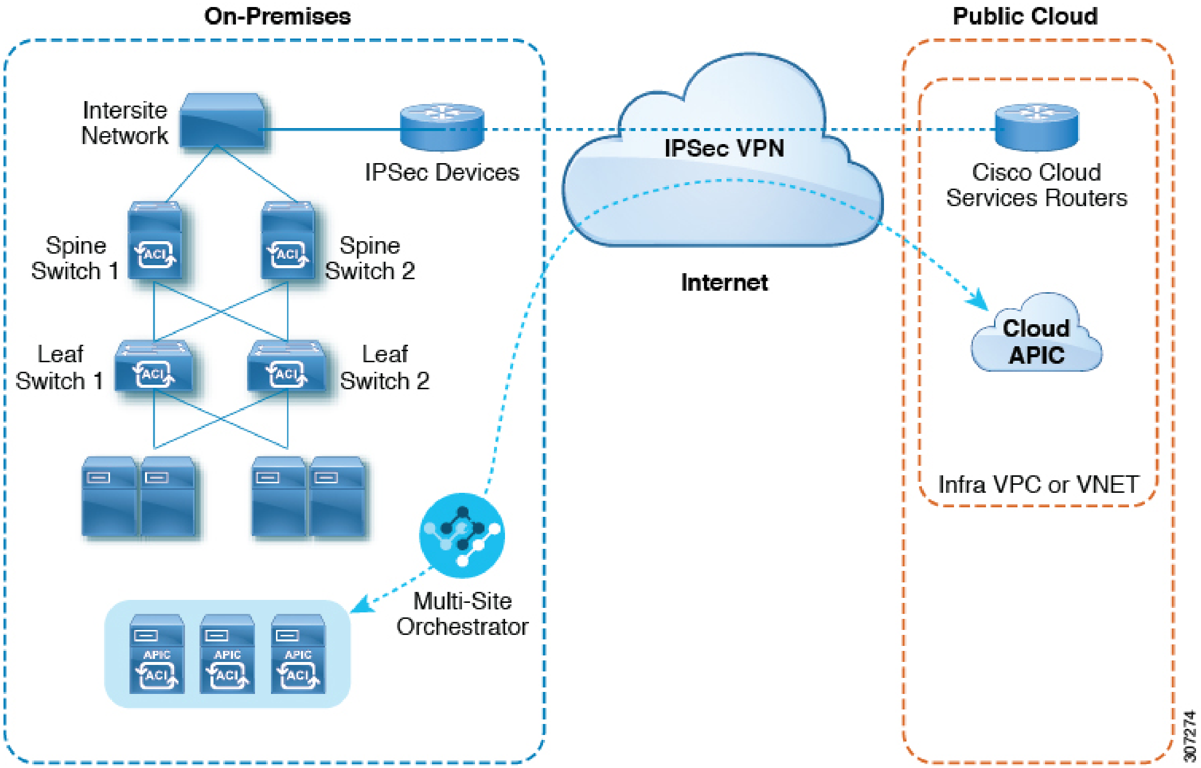
- US DoD Central
- US DoD East
- US Gov Arizona
- US Gov Texas
- US Gov Virginia

Components of Extending Cisco ACI Fabric to the Public Cloud

Several components, each with its specific role, are required to extend the Multi-Site fabric to the Microsoft Azure public cloud.

The following illustration shows the architecture of Cisco Cloud APIC.

Figure 1: Cisco Cloud APIC Architecture



On-Premises Data Center Components

Cisco ACI Fabric and Cisco APIC

The Cisco ACI allows application requirements to define the network. This architecture simplifies, optimizes, and accelerates the entire application deployment life cycle. Cisco Application Policy Infrastructure Controller (APIC) is a key component of Cisco ACI. It enables applications to directly connect with a secure, shared, high-performance resource pool that includes network, compute, and storage capabilities.

Multi-Site and Multi-Site Orchestrator/Cisco Nexus Dashboard Orchestrator

Multi-Site is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates application deployment. You must have Multi-Site installed to use Cisco Cloud APIC to extend the fabric into the public cloud.

For more information, see the Multi-Site documentation on Cisco.com and the configuration information for Multi-Site in this guide.

Cisco Nexus Dashboard Orchestrator (NDO) manages multiple instances of Cisco Application Policy Infrastructure Controller (APICs) in multiple fabrics (sites).

When extending the Cisco ACI fabric to the public cloud, Cisco Nexus Dashboard Orchestrator creates connectivity between the on-premises data center and the public cloud. Use Multi-Site to create tenants across the on-premises data center and the public cloud.

Note You must configure the on-premises Cisco ACI fabric: Create a Fabric Ext Connection Policy and define the overlay TEP and other information required for Multi-Site. You also must add the on-premises Cisco ACI fabric to the Multi-Site architecture. See the *Multi-Site Configuration Guide* on Cisco.com.

For more information, see the Multi-Site documentation on Cisco.com and the configuration information for Multi-Site in this guide.

IP Security (IPsec) Router

A router capable of Internet Protocol Security (IPsec) is required to establish IPsec connections between the on-premises site and the cloud site in Microsoft Azure.

Azure Public Cloud Components

Cisco Cloud APIC

Cisco Cloud APIC performs the following actions:

- Defines a site on the public cloud, provisions the cloud infra virtual networks (VNETs) and manages the CCR across all regions.
- Renders the Cisco ACI policy model in the public cloud, and manages cloud health.

For more information, see *Cisco Cloud APIC Release Notes*.

CCR

The CCR is a virtual router that delivers comprehensive WAN gateway and network services into virtual and cloud environments. The CCR enables enterprises to extend their WANs into provider-hosted clouds. Two CCRs are required for Cisco Cloud APIC solution.

The type of CCR that you will use with Cisco Cloud APIC varies depending on the release:

- For releases up to 25.0(3), Cisco Cloud APIC uses the **CSR 1000v** as the cloud services router. For more information on this CCR, see the Cisco CSR 1000v documentation.
- For release 25.0(3) and later, Cisco Cloud APIC uses the **Cisco Catalyst 8000V** as the cloud services router. For more information on this CCR, see the Cisco CCR 8000v documentation.

Microsoft Azure public cloud

Microsoft Azure is a cloud-based platform that provides on-demand services such as compute, storage, network, and databases. Subscribers to Azure have access through the Internet to virtual computers where they can run their workloads.

For more information, see the documentation on the Microsoft Azure website.

Connections Between the On-Premises Data Center and the Public Cloud

IPsec VPN

You need Internet connectivity with a VPN from the IPsec router, including a publicly routable IP address and with sufficient bandwidth for Microsoft Azure connectivity.

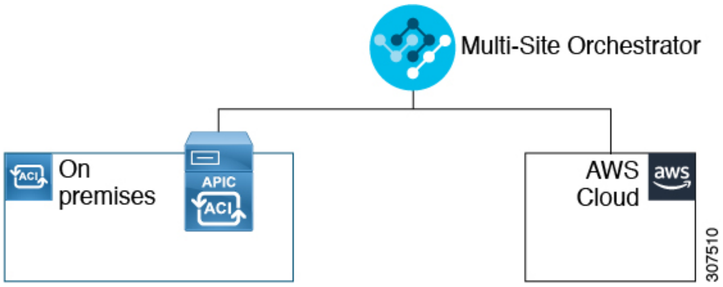
Management Connection

You need a management connection between the Nexus Dashboard Orchestrator in the on-premises data center and Cisco Cloud APIC in the Microsoft Azure public cloud.

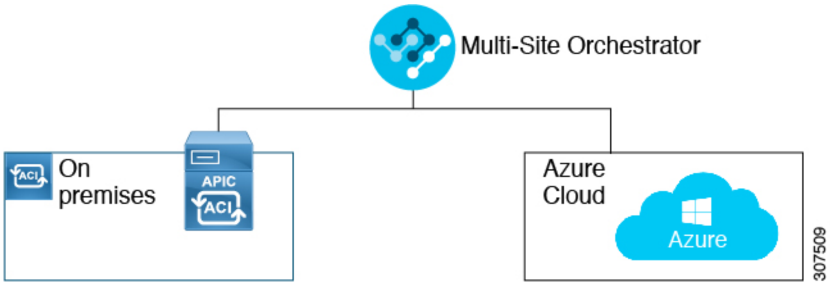
Supported Cloud Computing Platforms and Connectivity Options

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

- As part of the initial release of the Cisco Cloud APIC in release 4.1(1), support is provided for on-premises-to-cloud connectivity, or Hybrid-Cloud, where you could use the Cisco Cisco Nexus Dashboard Orchestrator to extend an on-premises Cisco ACI site to Amazon AWS public clouds.



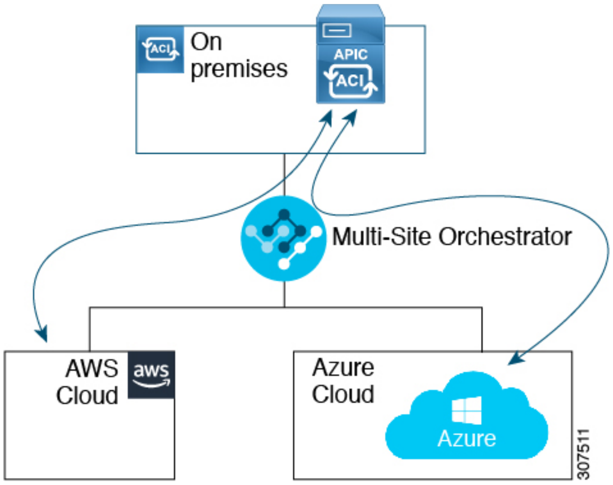
- Beginning in release 4.2(1), support is available for using the Cisco Cisco Nexus Dashboard Orchestrator to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.



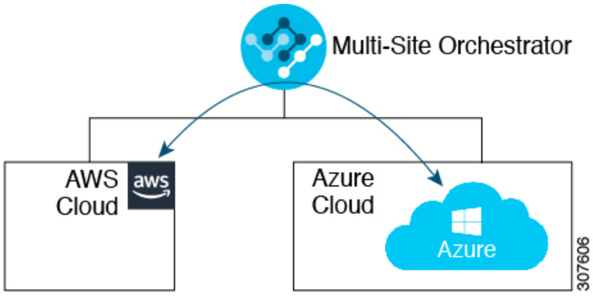
- Support is available for using the Cisco Cisco Nexus Dashboard Orchestrator to extend an on-premises Cisco ACI site to Google Cloud public clouds.

You can also use the Cisco Nexus Dashboard Orchestrator to establish connectivity between the following components:

- On-premises-to-cloud connectivity:
  - Connectivity for these public cloud sites:
    - On-premises Cisco ACI and Amazon AWS public cloud sites
    - On-premises Cisco ACI and Microsoft Azure public cloud sites
    - On-premises Cisco ACI and Google Cloud public cloud sites
  - On-premises-to-single cloud site connectivity (Hybrid-Cloud)
  - On-premises-to-multiple cloud sites connectivity (Hybrid Multi-Cloud)



- Cloud site-to-cloud site connectivity (Multi-Cloud):
    - Between Amazon AWS public cloud sites (Amazon AWS public cloud site-to-Amazon AWS public cloud site)
    - Between Microsoft Azure public cloud sites (Microsoft Azure public cloud site-to-Microsoft Azure public cloud site)
    - Between Google Cloud public cloud sites (Google Cloud public cloud site-to-Google Cloud public cloud site)
    - Between Amazon AWS, Microsoft Azure, and Google Cloud public cloud sites



In addition, support is also available for the single-cloud configuration (Cloud First).

Policy Terminology

A key feature of Cisco Cloud APIC is translation of Cisco Application Centric Infrastructure (ACI) policy to the native constructs of the public cloud.

Policy Mapping Between Cisco ACI and Microsoft Azure

The following table lists Cisco ACI policy terms and the equivalent terms in Microsoft Azure.

Cisco ACI	Azure
Tenant (Region, VRF)	Resource group
Virtual Routing and Forwarding (VRF)	Virtual network
BD subnet	Subnet
Contract, filter	Outbound rule, inbound rule
EP-to-EPG mapping	Application Security Group (ASG), Network Security Group (NSG)
Endpoint	Network adapter on VM instances

Understanding Tenants, Identities, and Subscriptions

Azure has an active directory structure. The top level structure is the organization, and underneath the organization are the directories (also known as Azure tenants). Inside the directories, you can have one or more Azure subscriptions.

The relationship between certain Azure components is as follows:

Tenants > **Subscriptions** > **Resource Groups** > **Resources**

Where:

- One tenant can have multiple subscriptions, but each subscription can belong to only one tenant.
- One subscription can have multiple resource groups, but each resource group can belong to only one subscription.
- One resource group can have multiple resources, but each resource can belong to only one subscription.

The following sections provide more detail about each of these components:

- Mapping Azure and Cloud APIC Components, on page 11
- About Azure Subscriptions, on page 12
- About Tenants and Identities, on page 12

Mapping Azure and Cloud APIC Components

In Cloud APIC, each Azure resource group is mapped to one Cloud APIC tenant, and one Cloud APIC tenant can have multiple Azure resource groups.

The relationship between certain Cloud APIC components is as follows:

Tenants > **VRFs** > **Regions**

When you create a VRF in Cloud APIC, a new resource group is also created on Azure.

About Azure Subscriptions

An Azure subscription is used to pay for Azure cloud services. An Azure subscription has a trust relationship with Azure Active Directories (Azure ADs), where the subscription uses the Azure AD to authenticate users, services, and devices. While multiple subscriptions can trust the same Azure AD, each subscription can trust only one Azure AD.

In Azure, the same Azure subscription ID can be used for multiple ACI fabric tenants. This means that you could configure the infra tenant using one Azure subscription, and then configure more user tenants in the same subscription. ACI tenants are tied to Azure subscriptions.

About Tenants and Identities

Following are the different types of tenants and identities available through Azure and Cloud APIC.

Note For releases prior to release 5.2(1), only managed identity was supported as the access type for infra tenants, while both managed identity and service principal was supported as the access type for user tenants.

Beginning with release 5.2(1), both managed identity and service principal is now supported as an access type for the infra tenants and the user tenants.

Managed Identity

Managed identities provide an identity for applications to use when connecting to resources that support Azure AD authentication. Applications can use the managed identity to obtain Azure AD tokens. For example, an application could use a managed identity to access resources like Azure Key Vault, where developers can store credentials in a secure manner or to access storage accounts.

Following are several benefits to using managed identities:

- You don't need to manage credentials, since credentials are not even accessible to you.
- You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.
- Managed identities can be used without any additional cost.

For additional information on managed identities in Azure, see:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

If you are configuring tenants in the Cloud APIC using **managed identity**, then you will make the following configurations in the Azure portal and in the Cloud APIC:

1. In the Azure portal, you will add a role assignment for a **virtual machine**. You use this option when the Azure subscriptions are in the same Azure directory (of the same organization).

   Note If your Azure subscriptions are in different directories and you want to configure tenants using **managed identity**, you can go to the Azure console and click on each of the subscriptions and move the subscriptions under the same Azure directory. You can only do this if the directories (containing the different subscriptions) are a child of the same parent organization.

The procedures for adding a role assignment in Azure for a virtual machine are provided in Adding a Role Assignment for a Virtual Machine, on page 39.

2. In the Cloud APIC, you will choose the **Create Your Own Managed Identity** option when configuring a tenant in Cloud APIC. You will configure this option in the Cloud APIC GUI using the procedures in Configuring a Tenant, on page 72.

Service Principal

An Azure **service principal** is an identity created for use with applications, hosted services, and automated tools to access Azure resources. You would use the service principal identity when you want to configure tenants in different subscriptions. The subscriptions are either in different Azure directories (Azure tenants) in the same organization, or the subscriptions can be in different organizations.

If you are configuring tenants in the Cloud APIC using **service principal**, then you will make the following configurations in the Azure portal and in the Cloud APIC:

1. In the Azure portal, you will be adding a role assignment for an **app**, where the cloud resources will be managed through a specific application.

   The procedures for adding a role assignment in Azure for an app are provided in Adding a Role Assignment for an App, on page 41.

2. In the Cloud APIC, you will choose the **Service Principal** option when configuring a tenant in Cloud APIC. The subscriptions that you enter in this page can be in different Azure directories (Azure tenants) in the same organization, or the subscriptions can be in different organizations. You will configure this option in the Cloud APIC GUI using the procedures in Configuring a Tenant, on page 72.

Shared Tenant

You will choose this option when you have already associated Azure subscriptions with either of the two methods above and want to create more tenants in that subscription.

If you are configuring a tenant in the Cloud APIC as **shared tenant**, then you will make the following configurations in the Azure portal and in the Cloud APIC:

1. You do not have to make any configurations in Azure specifically for a shared tenant, because you will have already associated Azure subscriptions with either of the two methods above. With the shared tenant, you will just create more tenants in that existing subscription.

2. In the Cloud APIC, you will choose the **Shared** option when configuring a tenant in Cloud APIC. You will configure this option in the Cloud APIC GUI using the procedures in Configuring a Tenant, on page 72.

Cisco Cloud APIC Licensing

This section lists the licensing requirements to use Cisco Cloud Application Policy Infrastructure Controller (APIC).

Cisco Cloud APIC and Cisco Cloud Router

Note The licensing information in this section applies specifically for the Cisco Cloud Services Router 1000v, which was used for releases prior to release 25.0(3). For licensing information for the Cisco Catalyst 8000V, which is used from release 25.0(3) and later, see Cisco Catalyst 8000V, on page 15.

Cisco licenses Cisco Cloud APIC by each virtual machine (VM) instance that it manages. The Cisco Cloud APIC binary images are available on Microsoft Azure portal and support the Bring Your Own License (BYOL) model.

The Essential Cloud tier includes licenses for a single policy domain or a single instance of Cisco Cloud APIC on a public cloud. If you deploy multiple instances of Cisco Cloud APIC, buy an Advantage Cloud license for each VM instance that Cisco Cloud APIC manages.

For licensing details, see the *Cisco Application Centric Infrastructure Ordering Guide*.

In addition to obtaining one or more Cisco Cloud APIC licenses, you must register your Cisco Cloud APIC and CCR with Cisco Smart Software Licensing.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Complete the following steps to register Cisco Cloud APIC and CCR:

1. Ensure that this product has access to the internet or a Smart Software Manager satellite that is installed on your network.
2. Log in to Smart Account:
   - **a.** Smart Software Manager: https://software.cisco.com/
   - **b.** Smart Software Manager Satellite: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
3. Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
4. Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

Note Cisco Cloud APIC deploys the appropriate size of CCRs based on the setting chosen in the **Throughput of the routers** field in the Cisco Cloud APIC setup wizard. See Requirements for the Azure Public Cloud, on page 18 and Configuring Cisco Cloud APIC Using the Setup Wizard, on page 53 for more information.

Note If you remove a CCR from deployment at some point in the future (by deleting the CCR through the Cisco Cloud APIC GUI or through the cloud console or portal), this results in the CCR smart license server getting severed from that CCR. The CCR instance that got deleted will get marked as stale for 90 days and the license cannot be reused by any other new CCRs for that period of time.

To avoid this situation, rehost the new CCR to the old license using the instructions in Rehosting the CSR 1000v License.

Cisco Catalyst 8000V

Beginning with release 25.0(4), the Cisco Catalyst 8000V on Cisco Cloud APIC supports the following licensing models:

1. **Bring Your Own License (BYOL)** Licensing Model
2. **Pay As You Go (PAYG)** Licensing Model

Note For releases prior to 25.0(4), the Cisco Catalyst 8000V on Cisco Cloud APIC supports only the **Bring Your Own License (BYOL)** licensing model.

BYOL Licensing Model

The Cisco Catalyst 8000V supports subscription-based licensing.

- For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see Cisco Catalyst 8000V Edge Software.
- For more information on different throughputs based on the tiers, see the "Throughput" section in "About the Cisco Catalyst 8000V" in the Cisco Cloud APIC for Azure User Guide, Release 25.0(1)-25.0(4) or later.

Cisco Cloud APIC makes use of the “Cisco DNA Advantage” subscription. For features supported by the “Cisco DNA Advantage” subscription, see Cisco DNA Software SD-WAN and Routing Matrices.

PAYG Licensing Model

Beginning with the 25.0(4) release, Cisco Cloud APIC supports Pay-As-You-Go (PAYG) Licensing Model on Cisco Catalyst 8000V which allows users to deploy a Catalyst 8000V instance in the cloud based on the VM size and purchase the usage on an hourly basis.

As you completely depend on the VM size to get the throughput, the PAYG licensing model can be enabled only by first un-deploying the current Cisco Catalyst 8000V and then re-deploying it using the First Time Set Up with the new VM size. For more information, see Configuring Cisco Cloud APIC Using the Setup Wizard, on page 45.

Note The procedure for enabling the PAYG license can also be used if you would like to switch between the two licensing types available.

Note There are two PAYG options for consuming licenses in the Azure marketplace: **Catalyst 8000V Cisco DNA Essentials** and **Catalyst 8000V Cisco DNA Advantage**. Cisco Cloud APIC will make use of **Catalyst 8000V Cisco DNA Advantage**. For features supported by the “Cisco DNA Advantage” subscription, see Cisco DNA Software SD-WAN and Routing Matrices.

Cisco Cloud APIC and On-Premises ACI Licensing Summary

- Licensing requirements for all leaf switches on the on-premises Cisco ACI sites:

    - If the Cisco ACI on-premises site is a single site, then use the Essentials license tier (or higher) for the on-premises leaf switches
    - If the Cisco ACI on-premises site is a multi-site, then use the Advantage license tier (or higher) for the on-premises leaf switches

- Licensing requirements for all VM instances managed by Cloud APIC instances:
    - If the Cisco ACI on the cloud has only one Cloud APIC, then use the Essentials Cloud license tier (or higher) for Cloud ACI
    - If the Cisco ACI on the cloud has more than one Cloud APIC, then use the Advantage Cloud license tier (or higher) for Cloud ACI

Microsoft Azure

You must subscribe through the Microsoft Azure Marketplace, depending on the release:

- For releases up to release 25.0(3), subscribe to **Cisco Cloud Services Router (CSR) 1000V - BYOL for Maximum Performance**.
- For release 25.0(3) and later, subscribe to **Cisco Catalyst 8000V Edge Software - BYOL**.
- For release 25.0(4) and later, subscribe to **Cisco Catalyst 8000V Edge Software - PAYG**.

To subscribe through the Microsoft Azure Marketplace, follow the instructions in Subscribing to the CCR, on page 23.

Cisco Cloud APIC-Related Documentation

You can find information about Cisco Cloud Application Policy Infrastructure Controller (APIC), Multi-Site, and Microsoft Azure from different resources.

Cisco Documentation

You can find documentation for Cisco products on Cisco.com:

- Cisco Cloud APIC Documentation Library

  Includes videos, release notes, fundamentals, installation, configuration, and user guides.

- Nexus Dashboard Documentation

  Includes videos, release notes, installation, configuration, and user guides.

- CCR Documentation

  Includes release notes, command reference, data sheets, installation, upgrade, and configuration guides.

Microsoft Azure Documentation

You can find documentation, including user guides, FAQs, case studies, and white papers, on the Microsoft Azure website.

CHAPTER 3

Preparing for Installing Cisco Cloud APIC

Requirements for Extending the Cisco ACI Fabric to the Public Cloud

Before you can extend the Cisco Application Centric Infrastructure (ACI) to the public cloud, you must meet requirements for the Cisco ACI on-premises datacenter and the Microsoft Azure deployment.

Requirements for the On-Premises Data Center

This section lists the on-premises data center requirements for extending the Cisco Application Centric Infrastructure (ACI) fabric to the public cloud.

- Ensure that the Cisco ACI fabric is installed with the following components:
  - At least two Cisco Nexus EX or FX spine switches, or Nexus 9332C and 9364C spine switches, running Cisco Nexus 9000 Series ACI Mode switch software release 14.1 or later.
  - At least two Cisco Nexus pre-EX, EX, or FX leaf switches running the Cisco Nexus 9000 Series ACI Mode switch software release 14.1 or later.

Note Even though Cisco Nexus pre-EX leaf switches are supported, we recommend using later-generation leaf switches, such as EX or FX leaf switches, due to the End-of-Life announcement for these older pre-EX leaf switches as described in End-of-Sale and End-of-Life Announcement for the Cisco Nexus 9372PX and 9372TX Switches.

  - At least one on-premises Cisco Application Policy Infrastructure Controller (APIC) running release 4.1 or later and Cisco Nexus Dashboard Orchestrator (NDO) Release 2.2(x) or later.
- Cisco Nexus Dashboard Orchestrator 2.2(x) deployed with basic configuration.

- A network device capable of terminating Internet Protocol Security (IPsec).
- Verify that you have enough bandwidth for tenant traffic between on-premises and cloud sites.
- Verify that all leaf switches on the on-premises sites have the appropriate Cisco ACI license:
  - If the Cisco ACI on-premises site is a single site, then use the Essentials license tier (or higher) for the on-premises leaf switches
  - If the Cisco ACI on-premises site is a multi-site, then use the Advantage license tier (or higher) for the on-premises leaf switches

Note These licensing requirements for the on-premises data center are independent of the number of Cloud APICs deployed on public clouds. For Cloud APIC licensing requirements, see Cisco Cloud APIC and On-Premises ACI Licensing Summary, on page 15.

- Workloads that are connected to the Cisco ACI fabric.
- An intersite network (ISN) that is configured between the Cisco ACI fabric (spine) and the IP Security (IPsec) termination device.

  For information about creating an ISN, see the "Multipod" chapter of the *Cisco APIC Layer 3 Networking Configuration Guide*.
- Certain firewall ports must be permitted if you are deploying firewalls between your on-premises and Azure deployments. These include HTTPS access for the Cisco Cloud APIC, IPsec ports for each Azure CCR, and SSH connectivity for Azure CCR remote management.

  These firewall ports are described in more detail in Cloud APIC Communication Ports, on page 21 in this guide.

Requirements for the Azure Public Cloud

This section lists the Microsoft Azure requirements for extending the Cisco Application Centric Infrastructure (ACI) fabric to the public cloud.

Azure Accounts

You must have at least one Azure account. You will then create a subscription in your Azure account, where you can choose to deploy multiple tenants within the same subscription or you can create multiple subscriptions for the tenants.

Azure Quota Limits

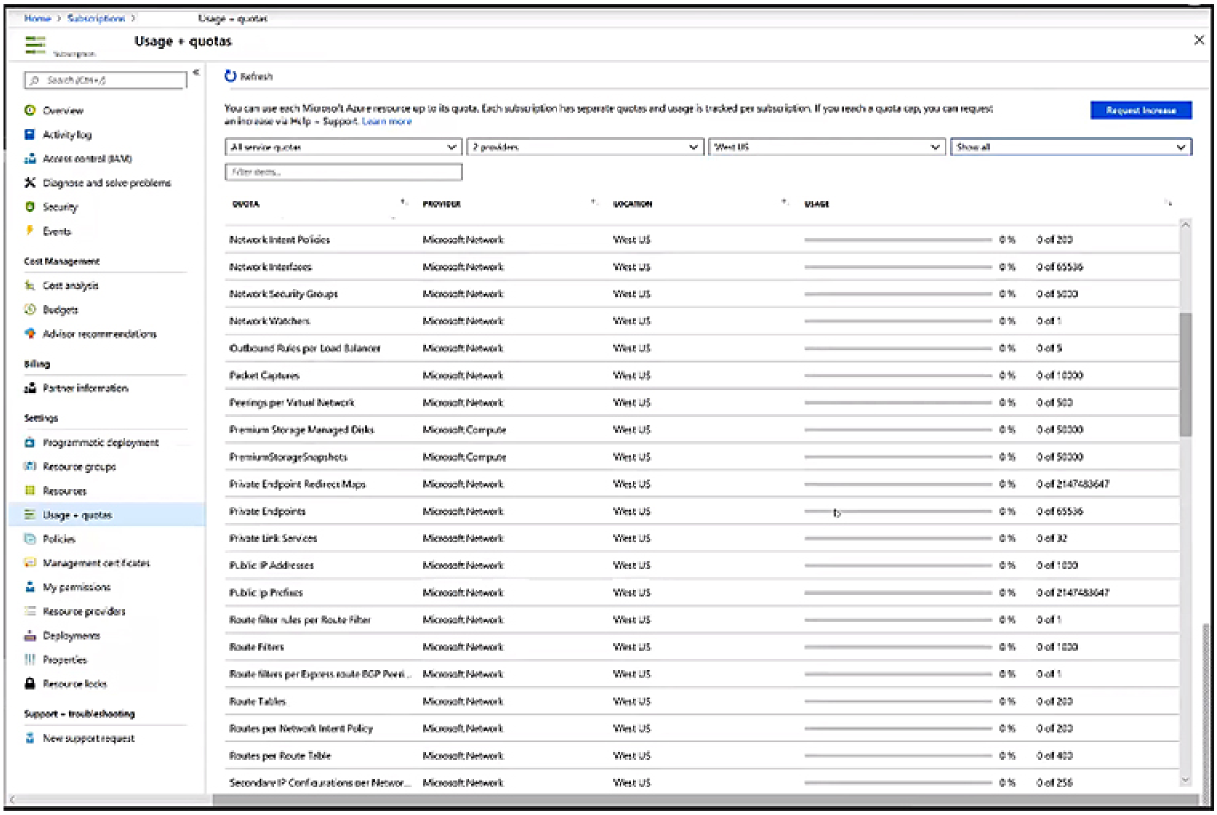
Verify that you have the appropriate Azure quota limits:

1. Navigate to **Subscriptions** > **Settings: Usage + quotas**.
2. In the **Select a provider** field, select:
   - Microsoft.Compute

- Microsoft.Network

3. In the **Select a location** field, select your region (for example, **West US**).
4. In the last field, change **Show only items with usage** to **Show all**.

Output similar to the following appears. Use this output to verify that you have the appropriate Azure quota limits.



You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more

All service quotas | 2 providers | West US | Show all

Filter items...

QUOTA	PROVIDER	LOCATION	USAGE	
Network Intent Policies	Microsoft.Network	West US	0 %	0 of 200
Network Interfaces	Microsoft.Network	West US	0 %	0 of 65536
Network Security Groups	Microsoft.Network	West US	0 %	0 of 5000
Network Watchers	Microsoft.Network	West US	0 %	0 of 1
Outbound Rules per Load Balancer	Microsoft.Network	West US	0 %	0 of 5
Packet Captures	Microsoft.Network	West US	0 %	0 of 10000
Peerings per Virtual Network	Microsoft.Network	West US	0 %	0 of 500
Premium Storage Managed Disks	Microsoft.Compute	West US	0 %	0 of 50000
PremiumStorageSnapshots	Microsoft.Compute	West US	0 %	0 of 50000
Private Endpoint Redirect Maps	Microsoft.Network	West US	0 %	0 of 2147483647
Private Endpoints	Microsoft.Network	West US	0 %	0 of 65536
Private Link Services	Microsoft.Network	West US	0 %	0 of 32
Public IP Addresses	Microsoft.Network	West US	0 %	0 of 1000
Public ip Prefixes	Microsoft.Network	West US	0 %	0 of 2147483647
Route filter rules per Route Filter	Microsoft.Network	West US	0 %	0 of 1
Route Filters	Microsoft.Network	West US	0 %	0 of 1000
Route filters per Express route BGP Peeri...	Microsoft.Network	West US	0 %	0 of 1
Route Tables	Microsoft.Network	West US	0 %	0 of 200
Routes per Network Intent Policy	Microsoft.Network	West US	0 %	0 of 200
Routes per Route Table	Microsoft.Network	West US	0 %	0 of 400
Secondary IP Configurations per Networ...	Microsoft.Network	West US	0 %	0 of 256

307588

Azure Resources

You need the following resources as part of the Azure deployment:

- Access to the Azure Marketplace offer. Locate the Cisco Cloud APIC offer on the Azure Marketplace and follow the steps in that page:

  https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-aci-cloud-apic

- The following cloud resource requirements (assumes one tenant, one VRF):

Resource Name	Resource Type	Minimum Requirement
Virtual Networks	Network	2
Static Public IP Addresses	Network	9
Network Security Groups	Network	5

Resource Name	Resource Type	Minimum Requirement
Application Security Groups	Network	5
Application Gateways	Network	1
Virtual Machines	Compute	3
Standard DSv2 Family vCPUs	Compute	16
Standard DSv3 Family vCPUs	Compute	8
Premium Storage Managed Disks	Compute	4

Azure Resource Providers

For every subscription that you use with the Cloud APIC, including for tenants that have subscriptions that you might add later, you must register the following resource providers:

- `microsoft.insights`
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

For more information, see Registering the Necessary Resource Providers, on page 25.

CCR

Deploy the CCRs in the appropriate size, depending on the bandwidth requirement defined during the Cisco Cloud APIC setup.

The value for the throughput of the routers determines the size of the CCR instance that you deploy; a higher value for the throughput results in the deployment of a larger VM. CCR licensing is based on the throughput configuration that you set as part of the Cisco Cloud APIC setup process. You need the equivalent or higher license in your Smart account and the AX feature set for compliance.

Cisco Cloud Services Router 1000v

The following table lists what Azure VM sizes are needed for different router throughput settings for the Cisco Cloud Services Router 1000v:

CSR Throughput	Azure VM Size	Premium Storage	Accelerated Networking
Up to 1 GB	DS3_v2	Yes	On
1 GB - 5 GB	DS4_v2	Yes	On

Beginning with Release 5.1(2), up to 40G throughput is supported by version 17.3 CSRs for the Cisco Cloud Services Router 1000v. The maximum throughput a CSR supports depends on the instance type. For achieving 40G throughput, a minimum of eight CSRs are required.

The following table lists the number of CSRs required and the instance type to achieve 40G throughput (per region):

Throughput per CSR	CSR Instance Type	Number of CSRs
5 Gbps	F16s_v2	8

Cisco Catalyst 8000V

The Cisco Catalyst 8000V supports tier-based (T0/T1/T2/T3) throughput options. The following table lists what Azure VM sizes are needed for different router throughput settings for the Cisco Catalyst 8000V:

CCR Throughput	Azure VM Size
T0 (up to 15M throughput)	DS3_v2
T1 (up to 100M throughput)	DS3_v2
T2 (up to 1G throughput)	DS3_v2
T3 (up to 10G throughput)	F16s_v2

Tier2 (T2) is the default throughput supported by Cisco Cloud APIC.

Cisco Cloud APIC

Cisco Cloud APIC is deployed using Standard_D8s_v3.

Cloud APIC Communication Ports

When configuring your Cloud APIC environment, keep in mind that the following ports are required for network communications:

- For communication between the Cisco Nexus Dashboard Orchestrator and the Cloud APIC: HTTPS (TCP Port 443 inbound/outbound)

  For the Cloud APIC, use the same Cloud APIC management IP address that you will use to log into the Cloud APIC at the beginning of Configuring Cisco Cloud APIC Using the Setup Wizard, on page 53.

- For communication between the on-premises IPsec device and the CCRs deployed by Cloud APIC in Azure: Standard IPsec ports (UDP ports 500 and 4500 should be open)

  For the two Azure CCRs, the public IPsec peering IP as provided if you download the ISN device configuration files using the instructions in Configuring the Intersite Infrastructure, on page 66.

- If you want to connect and manage the CCRs deployed by Cloud APIC in Azure, allow port TCP 22 inbound/outbound to the public IP address of each CCR.
- For license registration (towards `tools.cisco.com`): Port 443 (outbound) is required
- For DNS: UDP Port 53 outbound
- For NTP: UDP Port 123 outbound
- If remote authentication is used (LDAP, Radius, TACACS+, SAML), open the proper ports
- If a certificate authority is used, open the proper ports

Cisco Cloud APIC Installation Workflow

This section provides a high-level description of the tasks that are required to install and deploy Cisco Cloud APIC. You perform installation tasks through Azure management portal, the Azure Resource Manager (ARM) template, the Cloud APIC Setup Wizard, and Cisco Application Centric Infrastructure (ACI) Multi-Site.

1. Fulfill all prerequisites, which include tasks in the on-premises data center and the public cloud.

   See the section "Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 17."

2. Deploy Cisco Cloud APIC in Azure.

   This task includes subscribing to the CCR, registering the necessary resource providers, and creating an application in Azure.

   You also must create an Azure SSH keypair, deploy the Cisco Cloud APIC in Azure, and add a role assignment for a VM.

   See the section "Deploying the Cloud APIC in Azure, on page 23."

3. Configure Cisco Cloud APIC using the Setup Wizard.

   This task includes logging into Cisco Cloud APIC and configuring the Cisco Cloud ACI fabric for connecting to the public cloud. You also add the Azure region selection. You provide the Border Gateway Protocol (BGP) autonomous system number (ASN) and OSPF area ID for intersite network (ISN) peering and add an external subnet. You then add the IPsec peer address.

   See the section "Configuring Cisco Cloud APIC Using the Setup Wizard, on page 45."

4. Configure Cisco Cloud APIC using Multi-Site.

   - For on-premises-to-cloud connectivity, this task includes logging into the Cisco Nexus Dashboard Orchestrator GUI, adding the on-premises and cloud site, configuring the fabric connectivity infra, and configuring the properties for the on-premises site. You then configure the Cisco ACI spines, BGP peering, and enable the connectivity between the on-premises site and the Azure cloud sites.

   - For cloud-to-cloud connectivity, this task includes logging into the Cisco Nexus Dashboard Orchestrator GUI, adding the cloud sites, enabling the **Multi-Site** option and selecting the **Deploy Only** option when you are deploying the configuration.

   See the section "Managing Cisco Cloud APIC Through Multi-Site, on page 65."

5. Use Cisco Cloud APIC to extend Cisco ACI policy into the Azure public cloud.

   See the sections "Navigating the Cisco Cloud APIC GUI, on page 83" and "Configuring Cisco Cloud APIC Components, on page 83."

CHAPTER 4

Deploying the Cloud APIC in Azure

Subscribing to the CCR

The procedures for subscribing to the CCR vary depending on the release of the Cisco Cloud APIC software:

- For releases up to 25.0(3), Cisco Cloud APIC uses the **CSR 1000v** as the cloud services router, so refer to the procedures in Subscribing to the Cisco Cloud Services Router 1000V, on page 23.
- For release 25.0(3) and later, Cisco Cloud APIC uses the **CCR 8000v** as the cloud services router, so refer to the procedures in Subscribing to the Cisco Cloud Router 8000V, on page 25.

Subscribing to the Cisco Cloud Services Router 1000V

You must subscribe to the Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL) for Maximum Performance. To subscribe through the Microsoft Azure Marketplace:

Step 1 In the Azure Marketplace search text field, type *Cisco Cloud Services Router (CSR) 1000V* and select the option that appears.

The **Cisco Cloud Services Router (CSR) 1000V** option appears as a search suggestion.

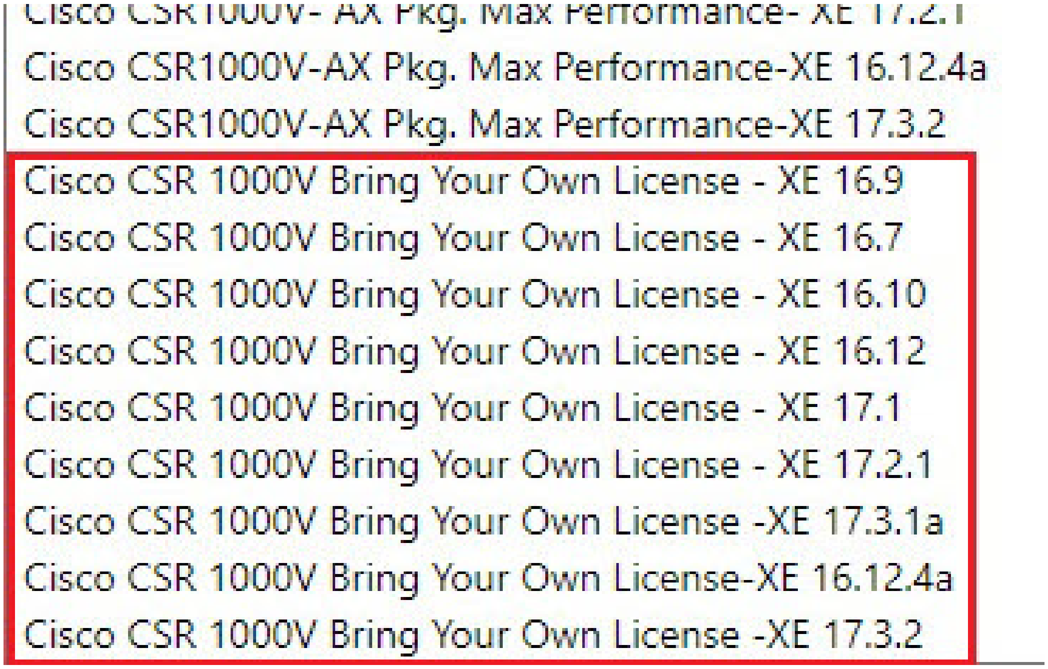
Step 2 Click the **Cisco Cloud Services Router (CSR) 1000V** option.

You should be redirected to the **Cisco Cloud Services Router (CSR) 1000V** page in the Microsoft Azure Marketplace.

Step 3 Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

Step 4 In the **Select a software plan** drop-down menu, locate the area that lists the **Cisco CSR 1000V Bring Your Own License** options.



Cisco CSR1000V- AX Pkg. Max Performance- XE 17.2.1

Cisco CSR1000V-AX Pkg. Max Performance-XE 16.12.4a

Cisco CSR1000V-AX Pkg. Max Performance-XE 17.3.2

Cisco CSR 1000V Bring Your Own License - XE 16.9

Cisco CSR 1000V Bring Your Own License - XE 16.7

Cisco CSR 1000V Bring Your Own License - XE 16.10

Cisco CSR 1000V Bring Your Own License - XE 16.12

Cisco CSR 1000V Bring Your Own License - XE 17.1

Cisco CSR 1000V Bring Your Own License - XE 17.2.1

Cisco CSR 1000V Bring Your Own License -XE 17.3.1a

Cisco CSR 1000V Bring Your Own License-XE 16.12.4a

Cisco CSR 1000V Bring Your Own License -XE 17.3.2

Step 5 Select the appropriate option, depending on the Cisco Cloud APIC software release:

For Cloud APIC Release	Select this specific option
Release 4.2x	Cisco CSR 1000V Bring Your Own License - XE **16.12**
Release 5.0(1)	Cisco CSR 1000V Bring Your Own License - XE **16.12**
Release 5.0(2)	Cisco CSR 1000V Bring Your Own License - XE **17.1**
• Release 5.1(2) • Release 5.2(1) • Release 25.0(1) • Release 25.0(2)	Cisco CSR 1000V Bring Your Own License - XE **17.3.1(a)**

Step 6 Locate the **Want to deploy programmability?** field and click **Get Started**.

Step 7 In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.

Step 8 Click **Save**.

What to do next

Go to Registering the Necessary Resource Providers, on page 25.

Subscribing to the Cisco Cloud Router 8000V

You must subscribe to the Cisco Cloud Router (CCR) 8000V - Bring Your Own License (BYOL) for Maximum Performance. To subscribe through the Microsoft Azure Marketplace:

Step 1 In the Azure Marketplace search text field, type *Cisco Catalyst 8000V Edge Software* and select the option that appears.

The **Cisco Catalyst 8000V Edge Software** option appears as a search suggestion.

Step 2 Click the **Cisco Catalyst 8000V Edge Software** option.

You should be redirected to the **Cisco Catalyst 8000V Edge Software** page in the Microsoft Azure Marketplace.

Step 3 Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

Step 4 In the **Select a software plan** drop-down menu, select the appropriate option, depending on the Cisco Cloud APIC software release:

For Cloud APIC Release	Select this specific option
• 25.0(3) • 25.0(4)	Cisco Catalyst 8000V Edge Software-BYOL-**17.07.01a**

Step 5 Locate the **Want to deploy programmability?** field and click **Get Started**.

Step 6 In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.

Step 7 Click **Save**.

What to do next

Go to Registering the Necessary Resource Providers, on page 25.

Registering the Necessary Resource Providers

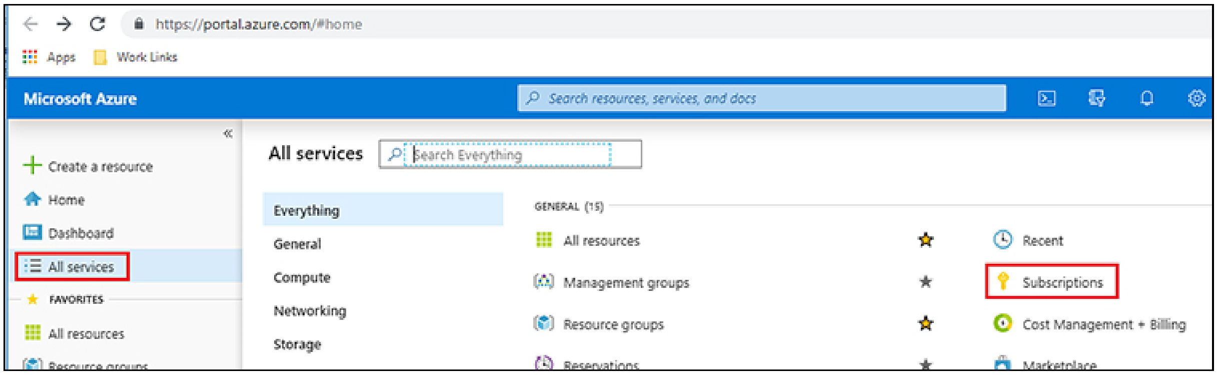
For every subscription that you use with the Cloud APIC, including for tenants that have subscriptions that you might add later, you must register the following resource providers:

- `microsoft.insights`
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

These procedures describe how to register these necessary resource providers for a subscription.

Step 1 Access the area in Azure where you can view the resource providers:

a) From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.

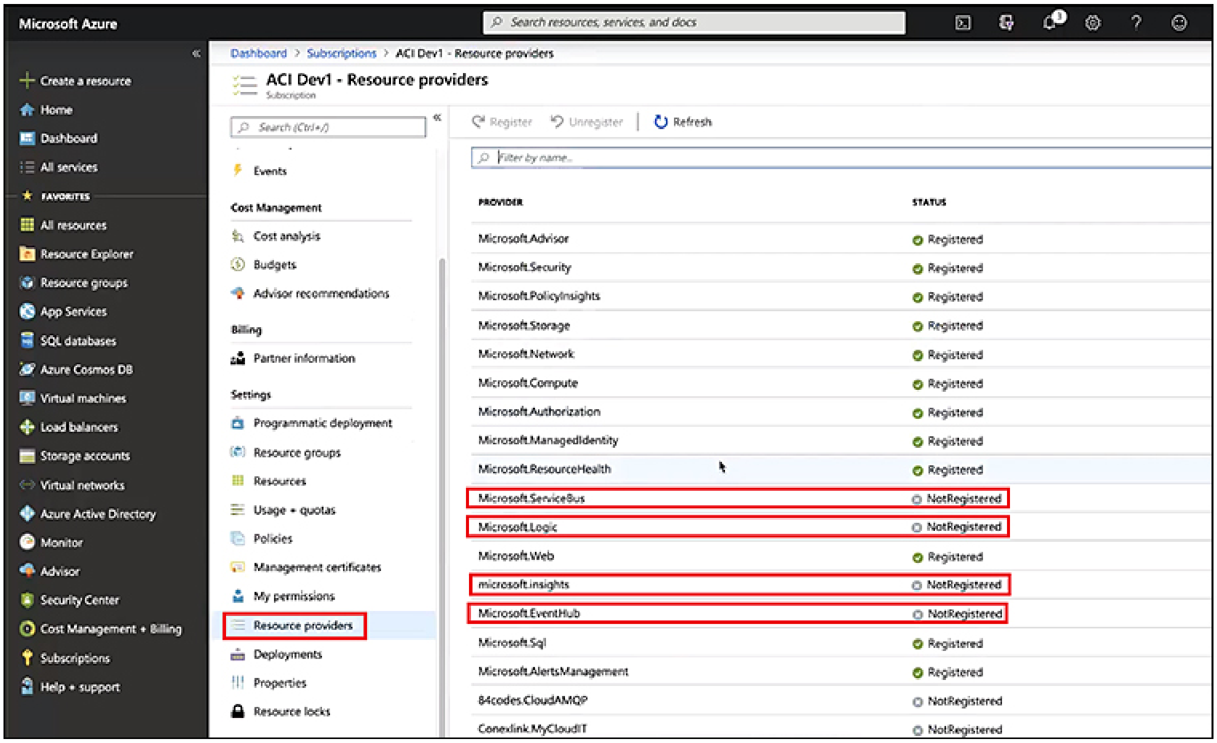


b) In the **Subscriptions** page in the Azure management portal, click the subscription account for your Microsoft account.

The overview information for that subscription is displayed.

c) From the overview page for that subscription, locate the **Resource providers** link in the left nav bar and click that link.

The Resource Providers page for that subscription is displayed.



PROVIDER	STATUS
Microsoft.Advisor	Registered
Microsoft.Security	Registered
Microsoft.PolicyInsights	Registered
Microsoft.Storage	Registered
Microsoft.Network	Registered
Microsoft.Compute	Registered
Microsoft.Authorization	Registered
Microsoft.ManagedIdentity	Registered
Microsoft.ResourceHealth	Registered
Microsoft.ServiceBus	NotRegistered
Microsoft.Logic	NotRegistered
Microsoft.Web	Registered
microsoft.insights	NotRegistered
Microsoft.EventHub	NotRegistered
Microsoft.Sql	Registered
Microsoft.AlertsManagement	Registered
84codes.CloudAMQP	NotRegistered
Conexlink.MyCloudIT	NotRegistered

Step 2 Locate the following four resource providers in the list of providers, as shown in the preceding screenshot:

- `microsoft.insights`

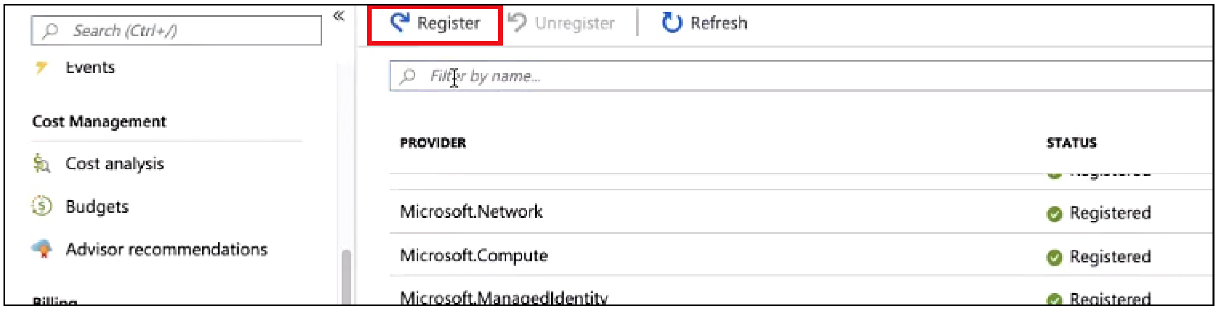
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

Step 3 Determine if all four of the resource providers are in the `Registered` or `NotRegistered` state.

- If all four of the resource providers are shown as `Registered` in the Status column, then you do not have to do anything further to register these resource providers for this subscription.
- For every resource provider that is shown as `NotRegistered` in the Status column:

  a. Click on that specific resource provider that is shown as `NotRegistered`.

  b. Click on Register at the top of the screen to register that resource provider.



PROVIDER	STATUS
Microsoft.Network	Registered
Microsoft.Compute	Registered
Microsoft.ManagedIdentity	Registered

  The Status will change from `NotRegistered` to `Registering`, then to `Registered` when the registration process is completed.

  c. Repeat these steps for every resource provider that is shown as `NotRegistered` until all four resource providers are shown as `Registered`.

Creating an Application in Azure

Follow these instructions to create an application in Azure, if necessary. You will need these procedures if you are creating a new subscription for the tenant and you are selecting **Unmanaged Identity** to manage the cloud resources through a specific application.

Note An application in Azure is also referred to as a Service Principal.

Step 1 Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

Step 2 From the main Azure management portal page, click the **Azure Active Directory** link in the left nav bar, then click the **App registrations** link.

Step 3 In the **App registrations** page, click **+ New registration**.

Step 4 Enter the necessary information in the **Register an application** page:

- **Name**
- **Supported Account Types**: Select the first option (Accounts in this organizational directory only)
- (Optional) **Redirect URI**

Then click **Register**.

The overview page for this application appears.

Step 5 Click **Certificates & secrets** in the left nav bar, then enter the necessary information in the **Add a client secret** area and click **Add**.

This generates the necessary information that you will need for the **Application Secret** field later on in these procedures.

Step 6 Open a text file and copy-and-paste the necessary information into the text file:

- **Client Secret**: Copy the text in the **Value** field in the **Client Secrets** area in the **Clients & Secrets** page.
- **Application ID**: Navigate to **Home** > **App registrations** > **<application-name>**, then, in the **Overview** page, copy the text from **Application (client) ID** field.
- **Azure Active Directory ID**: Navigate to **Home** > **App registrations** > **<application-name>**, then, in the **Overview** page, copy the text from **Directory (tenant) ID** field.

Step 7 Save the text file and note its location.

You will refer to this information when you are going through the procedures in Configuring a Tenant, on page 72 later on in this document.

Generating an SSH Key Pair for Azure

As part of the Cloud APIC setup process, you will be asked to provide the Admin Public Key (the SSH public key) in the Azure Resource Manager (ARM) template for your Cloud APIC. The following sections provide instructions for generating the SSH public and private key pair in Windows or Linux systems.

Generating an SSH Key Pair in Windows

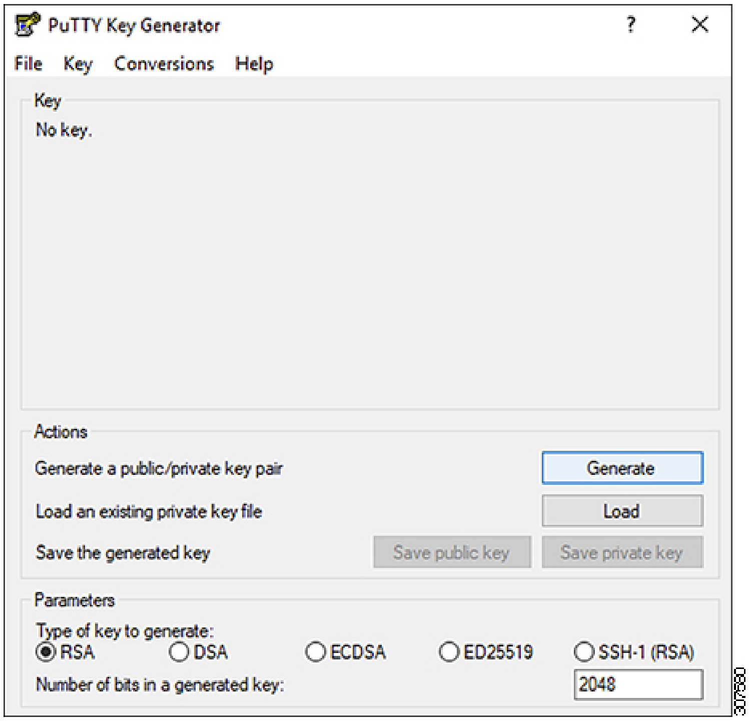
These procedures describe how to generate an SSH public and private key pair in Windows. For instructions on generate an SSH public and private key pair in Linux, see Generating an SSH Key Pair in Linux or MacOS, on page 31.

Step 1 Download and install the PuTTY Key Generator (puttygen):

https://www.puttygen.com/download-putty

Step 2 Run the PuTTY Key Generator by navigating to **Windows** > **Start Menu** > **All Programs** > **PuTTY** > **PuTTYgen**.

You will see a window for the PuTTY Key Generator on your screen.



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

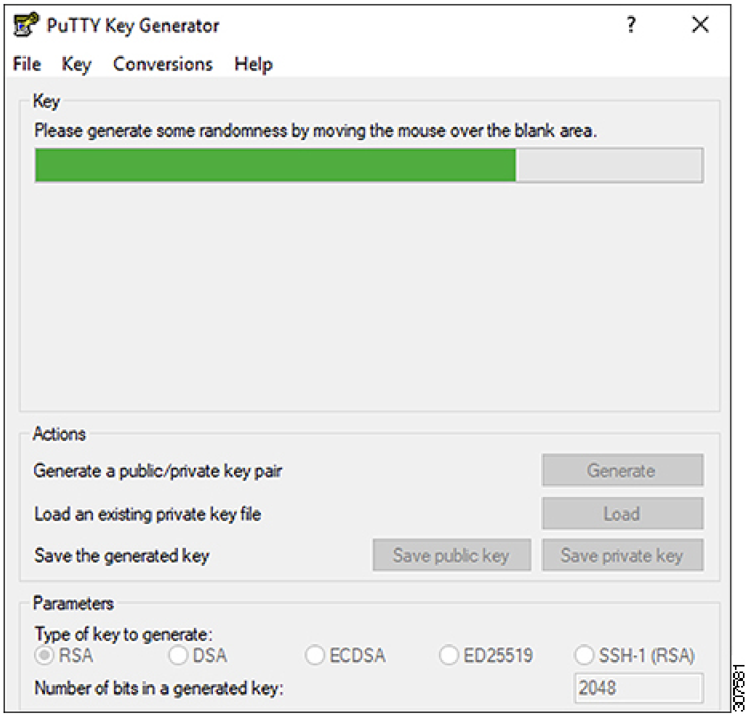
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Step 3 Click **Generate**.

A screen appears, asking you to move the mouse over the blank area to generate a public key.

Step 4 Move your cursor around the blank area to generate random characters for a public key.



Please generate some randomness by moving the mouse over the blank area.

Type of key to generate: ● RSA

Number of bits in a generated key: 2048

Step 5 Save the public key.

a) Navigate to a folder on your laptop where you want to save the public key file and create a text file for this public key.

b) Copy the information in the PuTTY Key Generator.

Copy the public key information in the window, with these inclusions and exclusions:

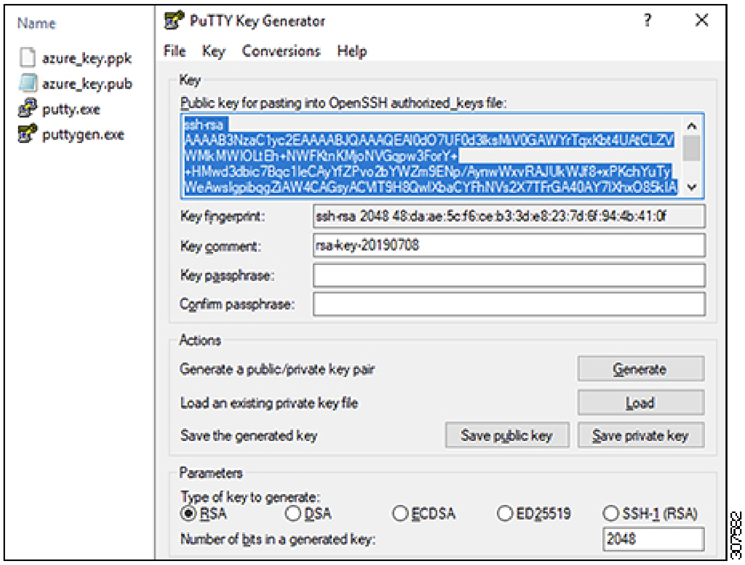
- Including the **ssh-rsa** text at the beginning of the public key.
- Excluding the following text string at the end:

```
== rsa-key-<date-stamp>
```

Truncate the key so that it does not include the == **rsa-key-<date-stamp>** text string at the end.

Note In the next set of procedures, you will paste the public key information into the Azure ARM template. If the form does not accept the key in this format, add == back to the end of the key, as this format is required in some regions.

If the key is not in the correct format, the Cloud APIC will not complete its installation.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEA0dO7UF0d3ksMiV0GAWYrTqxKbt4UAtCLZV
WMkMWIOLtEh+NWFKtnKMjoNVGqpw3ForY+
+HMwd3dbic7Bqc1leCAyYfZPvo2bYWZm9ENp/AynwWxvRAJUkWJf8+xPKchYuTy
WeAwslgpibqgZiAW4CAGsyACVlT9H8QwlXbaCYFhNVs2X7TFrGA40AY7lXhxO85kIA
```

Key fingerprint: ssh-rsa 2048 48:da:ae:5c:f6:ce:b3:3d:e8:23:7d:6f:94:4b:41:0f

Key comment: rsa-key-20190708

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

c) Paste the information in the public key text file that you created in 5.a, on page 30 and save the file, giving it a unique file name.

This public key text file will now contain a key that is on a single line of text. You will need the information in this public key text file in the next set of procedures.

Note Do not save the public key using the **Save public key** option in the PuTTY Key Generator. Doing so saves the key in a format that has multiple lines of text, which is not compatible with the Cloud APIC deployment process.

Step 6 Save the private key.

a) Click **Save private key**.

A screen appears, asking if you want to save the file without a passphrase. Click **Yes** on this screen.

b) Navigate to a folder on your laptop and save the private key file, giving it a unique file name.

Note The private key file is not used in the installation process. However, you might need it for other reasons, such as logging into your Cloud APIC through SSH, as described in Logging Into Cloud APIC Through SSH, on page 117.

What to do next

Follow the instructions in Deploying the Cloud APIC in Azure, on page 33 to continue the Azure configuration process, which includes pasting the public key information into the Azure ARM template.

Generating an SSH Key Pair in Linux or MacOS

These procedures describe how to generate an SSH public and private key pair in Linux or MacOS. For instructions on generate an SSH public and private key pair in Windows, see Generating an SSH Key Pair in Windows, on page 28.

Step 1 On your Linux virtual machine or Mac, create a public and private key pair using ssh-keygen, directing the output to a file.

```
# ssh-keygen -f filename
```

For example:

```
# ssh-keygen -f azure_key
```

Output similar to the following appears. Press the Enter key without entering any text when you are asked to enter a passphrase (leave the field empty so that there is no passphrase).

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXVV6U0dyBNs
...
```

Step 2 Locate the public and private key files that you saved.

```
# ls
```

Two files should be displayed, where:

- The file with the .pub suffix contains the public key information
- The file with the same name, but with no suffix, contains the private key information

For example, if you directed the output to a file named `azure_key`, you should see the following output:

```
# ls
azure_key
azure_key.pub
```

In this case:

- The `azure_key.pub` file contains the public key information
- The `azure_key` file contains the private key information

Step 3 Open the public key file and copy the public key information from that file, without the `username@hostname` information at the end.

Note The private key file is not used in the installation process. However, you might need it for other reasons, such as logging into your Cloud APIC through SSH, as described in Logging Into Cloud APIC Through SSH, on page 117.

What to do next

Follow the instructions in Deploying the Cloud APIC in Azure, on page 33 to continue the Azure configuration process, which includes pasting the public key information from the public key file into the Azure ARM template.

Deploying the Cloud APIC in Azure

Before you begin

- Verify that you have met the requirements outlined in Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 17 before proceeding with the tasks in this section. For example, verify that you have the correct number of elastic IP addresses and that you have checked the limits that are allowed to deploy the instances.

Step 1 Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

Step 2 From the main Azure management portal page, in the search text field, type *Cisco Cloud APIC*.

Step 3 In the **Cisco Cloud APIC** page, in the **Select a plan** field, select the appropriate release and click **Create**.

The **Basics** page for the **Cisco Cloud APIC** screen appears.

Step 4 Complete the necessary fields in the **Basics** page:

- **Subscription**: Select the Cloud APIC infra subscription account from the drop-down list.
- **Resource group**: Choose an existing resource group from the drop-down list or click **Create new** to enter a name for a new resource group.

  A resource group is a container that holds related resources for an Azure solution.

  You can define custom naming rules for most cloud resources created by the Cloud APIC, with the exception of the resource group for the Cloud APIC itself. Ensure that the resource group name you select here is correct.
- **Region**: Select the location from the drop-down list where you want to deploy the virtual machine for the Cloud APIC.
- **Virtual Machine name**: Enter a virtual machine name. This entry will be the name for the virtual machine for this Cloud APIC. The virtual machine name must be only alphanumeric characters, but can be separated by dashes (for example, `CloudAPIC`).
- **Password**: Enter an admin password. This entry is the password that you will use to log into the Cloud APIC after you have enabled SSH access.

  The password must have the following characteristics:

  - Must be between 12 and 72 characters in length
  - Must have three of the following:
    - 1 lower case letter
    - 1 upper case letter
    - 1 number
    - 1 of the following acceptable special characters:

      @$!%*#?&

- **Confirm Password**: Enter the admin password again.
- **SSH Public Key**: Paste the public key information that you copied at the end of one of these procedures:
    - Generating an SSH Key Pair in Windows, on page 28
    - Generating an SSH Key Pair in Linux or MacOS, on page 31

  You will use this SSH key pair to log into the Cloud APIC. Note that the **ssh-rsa** string should remain at the beginning of the public key string that you paste into this field.

  Note If you generated an SSH key pair in Windows, the key in the PuTTY Key Generator ends with == **rsa-key-<date-stamp>**. Truncate the key so that it does not include **== rsa-key-<date-stamp>**. If the form does not accept the key in this format, add == back to the end of the key, as this format is required in some regions.

  If the key is not in the correct format, the Cloud APIC will not complete its installation.

Step 5 When you have finished completing the fields in this page, click **Next: ACI Settings**.

The **ACI Settings** page for the **Cisco Cloud APIC** screen appears.

Step 6 Complete the necessary fields in the **ACI Settings** page:

- **ACI Fabric Name**: Leave the default value as-is or enter a fabric name. This entry will be the name for this Cloud APIC. The fabric name must be only alphanumeric characters, but can be separated by dashes (for example, `ACI-Cloud-Fabric`).
- **Virtual machine size**: The virtual machine size is automatically set to the default deployment size of Standard_D8s_v3. You cannot change the default virtual machine size setting.
- **Image Version**: Choose the appropriate release in this field.
- **Infra Subnet**: The infra pool for your Cloud APIC. This field is automatically populated with a default value of 10.10.0.0/24. Change the value in this field if the default value overlaps with your infra pool from your on-premises fabric. This entry must be a /24 subnet.

  Note We recommend that you do not use any subnet from 172.17.0.0/16 (for example, 172.17.10.0/24) as the infra subnet, as this might cause a conflict with the Docker bridge IP subnet, as described in Resolving Subnet Conflict Issue With Infra Subnet, on page 37.

- **Public IP Address**: Set the public IP address to **static**.

  a. In the **Public IP Address** field, click **Create New**.

  Note To assign a private IP address for Cloud APIC, select **none** from the drop-down list.

  The **Create public IP address** field appears on the right side of the page.

  b. In the **SKU** area, choose either the **Basic** or the **Standard** SKU.

  For more information on the differences between the Basic and the Standard SKU, see the *Public IP Addresses in Azure* document in the Microsoft documentation site.

  c. In the **Assignment** area, choose **Static**.

  Do not leave the setting as Dynamic in the **Assignment** area.

  d. Click **OK** in the **Create public IP address** area.

- **DNS Prefix for the public IP Address**: The Cloud APIC DNS name prefix. When the Cloud APIC is deployed, you can access the Cloud APIC using the DNS name.

  Note Due to an Azure restriction, you cannot use periods (.) in the Cloud APIC DNS name prefix that you enter in this field.

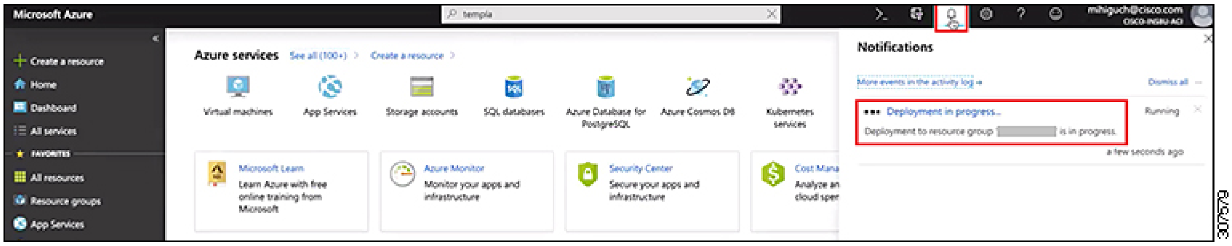
- **External Subnets**: Enter the IP addresses and subnets of the external networks that you will allow to connect to Cloud APIC (for example, 192.0.2.0/24). Only the IP addresses from this subnet are allowed to connect to Cloud APIC. Entering a value of `0.0.0.0/0` means that anyone is allowed to connect to Cloud APIC.
- **Virtual Network Name**: Leave the default entry for the virtual network name as-is or change the entry in this field, if desired.
- **Management NSG Name**: Leave the default entry for the management network security group name as-is or change the entry in this field, if desired.
- **Management ASG Name**: Leave the default entry for the management application security group name as-is or change the entry in this field, if desired.
- **Subnet Prefix**: Leave the default entry for the subnet prefix as-is or change the entry in this field, if desired.

Step 7 When you have finished completing the fields in this page, click **Next: Review + create**.

The **Review + create** page for the **Cisco Cloud APIC** screen appears.

Step 8 Review the information in the **Review + create** page, then click **Create**.

The system now uses the information that you provided in the template to create the Cloud APIC VM instance. This process takes 5-10 minutes to complete. Click the Notifications icon (the bell-shaped icon) to check the status of the deployment of your Cloud APIC.



••• Deployment in progress...

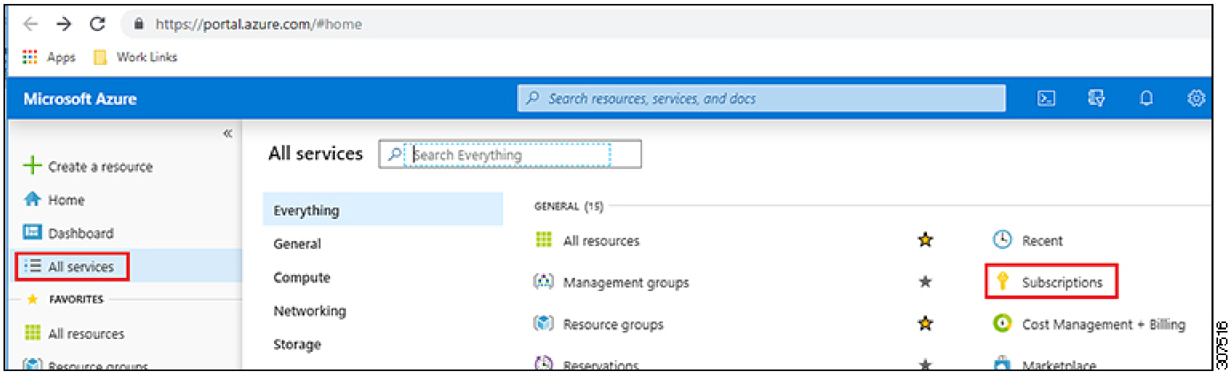
Deployment to resource group [redacted] is in progress.

Running

a few seconds ago

Step 9 When the deployment is complete, add a **User Access Administrator** role assignment.

a) From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.



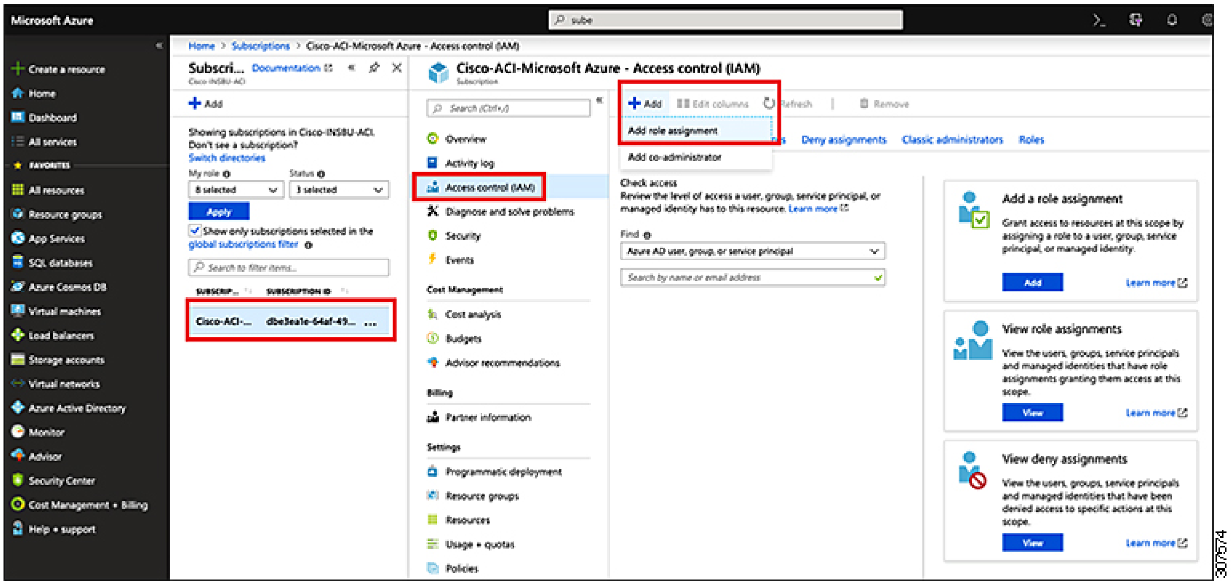
b) In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

c) From the overview page for that subscription, locate the **Access control (IAM)** link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

d) Click **+ Add**, then select **Add role assignment** from the drop-down menu.


Microsoft Azure
subs
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Home > Subscriptions > Cisco-ACI-Microsoft Azure - Access control (IAM)
Subscri... Documentation
Cisco-INSBU-ACI
+ Add
Showing subscriptions in Cisco-INSBU-ACI. Don't see a subscription? Switch directories
My role
8 selected
Status
3 selected
Apply
Show only subscriptions selected in the global subscriptions filter
Search to filter items...
SUBSCRIP...
SUBSCRIPTION ID
Cisco-ACI-...
dbe3ea1e-64af-49...
Cisco-ACI-Microsoft Azure - Access control (IAM)
Subscription
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Diagnose and solve problems
Security
Events
Cost Management
Cost analysis
Budgets
Advisor recommendations
Billing
Partner information
Settings
Programmatic deployment
Resource groups
Resources
Usage + quotas
Policies
+ Add
Edit columns
Refresh
Remove
Add role assignment
Add co-administrator
Deny assignments
Classic administrators
Roles
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Find
Azure AD user, group, or service principal
Search by name or email address
Add a role assignment
Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.
Add
Learn more
View role assignments
View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.
View
Learn more
View deny assignments
View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.
View
Learn more
307574

e) In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **User Access Administrator** from the drop-down menu.
- In the **Assign access to** field, select **Virtual Machine**.
- In the **Subscription** field, select the subscription where the Cloud APIC is deployed.
- Select the Cloud APIC virtual machine.

f) Click **Save** at the bottom of the screen.

What to do next

Go to Adding a Role Assignment, on page 39 to determine if you need to add a role assignment for a managed identity or unmanaged identity for the access type.

Resolving Subnet Conflict Issue With Infra Subnet

In some situations, you might encounter an issue with a subnet conflict with your Cloud APIC. This issue might occur when the following conditions are met:

- Your Cloud APIC is running on release 25.0(2)
- The infra subnet for your Cloud APIC is configured within the 172.17.0.0/16 CIDR (for example, if you entered `172.17.10.0/24` in the **Infra Subnet** field as part of the procedures in Deploying the Cloud APIC in Azure, on page 33)
- There is something else configured that overlaps with the 172.17.0.0/16 CIDR that you are using for the infra subnet for your Cloud APIC (for example, if the Docker bridge IP subnet is configured with `172.17.0.0/16`, which is the default subnet in Cloud APIC).

In this situation, your Cloud APIC might not be able to reach the CCR private IP address due to this subnet conflict and the Cloud APIC will raise an SSH connectivity fault for the affected CCR.

You could determine if there might be a possible conflict by logging in as root into the Cloud APIC and entering the `route -n` command:

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
```

Assume that you see output similar to the following:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.0.17     0.0.0.0         UG    16     0        0 oobmgmt
169.254.169.0   0.0.0.0         255.255.255.0   U     0      0        0 bond0
169.254.254.0   0.0.0.0         255.255.255.0   U     0      0        0 lxcbr0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.17.0.12     0.0.0.0         255.255.255.252 U     0      0        0 bond0
172.17.0.16     0.0.0.0         255.255.255.240 U     0      0        0 oobmgmt
```

In this example output, the highlighted text shows that a Docker bridge is configured with `172.17.0.0/16`.

Because this overlaps with the 172.17.0.0/16 CIDR that you used for the infra subnet for your Cloud APIC, you might see an issue where you lose connectivity to the CCR, where you are not able to SSH into the CCR, and you see a Host Unreachable message when you try to ping the CCR (such as in the following example, where 172.17.0.84 is the private IP address of the CCR):

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
From 172.17.0.1 icmp_seq=1 Destination Host Unreachable
From 172.17.0.1 icmp_seq=2 Destination Host Unreachable
From 172.17.0.1 icmp_seq=3 Destination Host Unreachable
From 172.17.0.1 icmp_seq=5 Destination Host Unreachable
From 172.17.0.1 icmp_seq=6 Destination Host Unreachable
```

```
^C
--- 172.17.0.84 ping statistics ---
9 packets transmitted, 0 received, +5 errors, 100% packet loss, time 8225ms
pipe 4
[root@ACI-Cloud-Fabric-1 ~]#
```

To resolve the conflict in this situation, enter a REST API post similar to the following to change the IP address for the other area that is causing the conflict:

```
https://{{apic}}/api/plgnhandler/mo/.xml
<apPluginPolContr>
    <apContainerPol containerBip="<new-IP-address>" />
</apPluginPolContr>
```

For example, to move the Docker bridge IP address out from under the 172.17.0.0/16 CIDR, which was shown in the example scenario above, you might enter a REST API post such as the following:

```
https://{{apic}}/api/plgnhandler/mo/.xml
<apPluginPolContr>
    <apContainerPol containerBip="172.19.0.1/16" />
</apPluginPolContr>
```

where `172.19.0.1/16` is the new subnet for the Docker bridge. This moves the Docker bridge IP address under the 172.19.0.0/16 CIDR, where there is no longer a conflict with the infra subnet for your Cloud APIC that is configured within the 172.17.0.0/16 CIDR.

You can use the same commands as before to verify that there is no longer a conflict:

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.0.17     0.0.0.0         UG    16     0        0 oobmgmt
169.254.169.0   0.0.0.0         255.255.255.0   U     0      0        0 bond0
169.254.254.0   0.0.0.0         255.255.255.0   U     0      0        0 lxcbr0
172.17.0.12     0.0.0.0         255.255.255.252 U     0      0        0 bond0
172.17.0.16     0.0.0.0         255.255.255.240 U     0      0        0 oobmgmt
172.19.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
```

In this example output, the highlighted text shows that a Docker bridge is configured with the IP address `172.19.0.0`. Because there is no overlap with the 172.17.0.0/16 CIDR that you are using for the infra subnet for your Cloud APIC, there is no issue with connectivity with the CCR:

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
64 bytes from 172.17.0.84: icmp_seq=1 ttl=255 time=1.15 ms
64 bytes from 172.17.0.84: icmp_seq=2 ttl=255 time=1.01 ms
64 bytes from 172.17.0.84: icmp_seq=3 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=4 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=5 ttl=255 time=1.09 ms
64 bytes from 172.17.0.84: icmp_seq=6 ttl=255 time=1.06 ms
64 bytes from 172.17.0.84: icmp_seq=7 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=8 ttl=255 time=1.05 ms
^C
--- 172.17.0.84 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7005ms
rtt min/avg/max/mdev = 1.014/1.061/1.153/0.046 ms
[root@ACI-Cloud-Fabric-1 ~]#
```

Adding a Role Assignment

The type of role assignment that you add depends on whether you have a managed identity or unmanaged identity for the access type:

- If you have a **managed** identity for the access type, then you must add a role assignment for the user tenant. Go to Adding a Role Assignment for a Virtual Machine, on page 39.

  Note that this access type would apply if you make either of the following selections when you are entering information in the **Associate Account** page in the Configuring a Tenant, on page 72 procedures later in this manual:

  - You choose **Mode: Create Own** and you selected **Managed Identity** in the **Associate Account** page, or
  - You choose **Mode: Select Shared** and you are sharing with the infra tenant

- If you have an **unmanaged** identity (service principal) for the access type, then the cloud resources will be managed through a specific application. Go to Adding a Role Assignment for an App, on page 41.

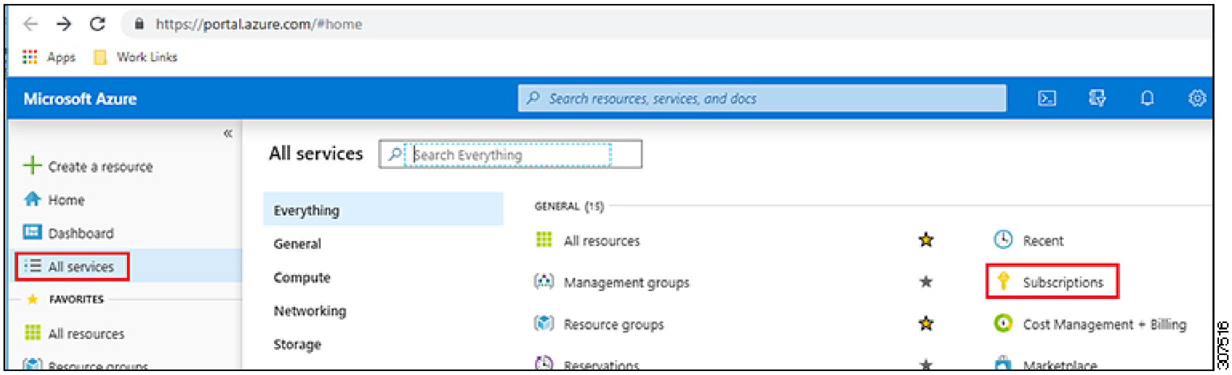
  Note that this access type would apply if you select **Unmanaged Identity** (service principal) in the **Associate Account** page in the Configuring a Tenant, on page 72 procedures later in this manual.

Adding a Role Assignment for a Virtual Machine

Follow the procedures in this section if you have a **managed** identity for the access type, where you must add a role assignment for the user tenant. See Understanding Tenants, Identities, and Subscriptions, on page 11 for more information about the relationship between Azure subscription types and Cloud APIC tenants.

Note If you have an **unmanaged** identity for the access type, where the cloud resources will be managed through a specific application, follow the procedures in Adding a Role Assignment for an App, on page 41 instead.

Step 1 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.



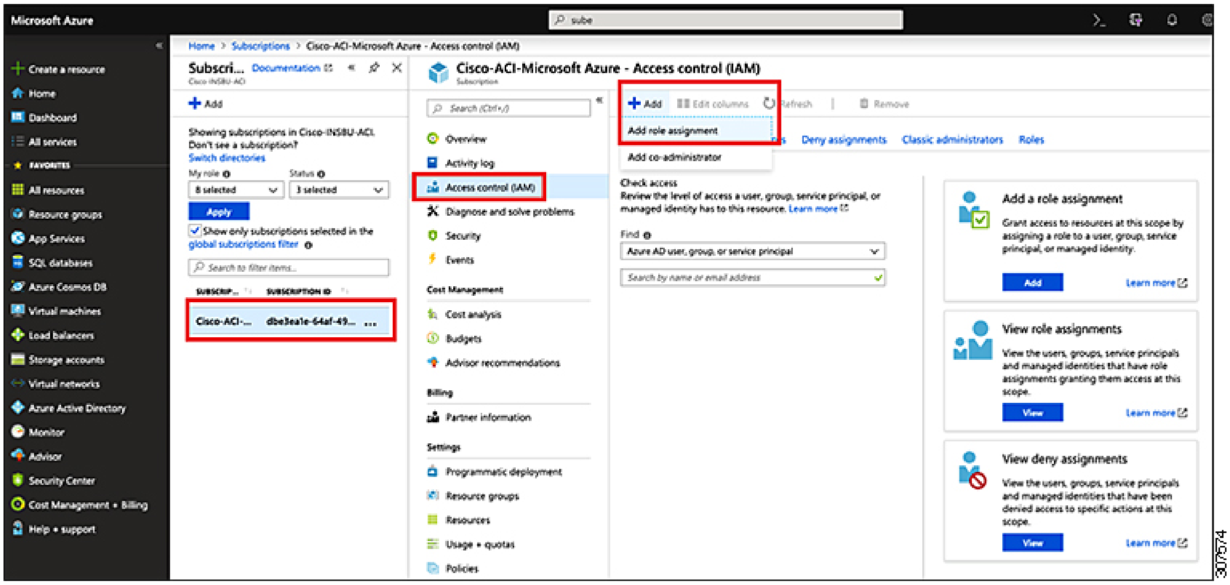
Step 2 In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

Step 3 From the overview page for that subscription, locate the **Access control (IAM)** link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

Step 4 Click **+ Add**, then select **Add role assignment** from the drop-down menu.



Showing subscriptions in Cisco-INSBU-ACI. Don't see a subscription? Switch directories

☑ Show only subscriptions selected in the global subscriptions filter

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

Step 5 Add a **Contributor** role assignment.

a) In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **Contributor** from the drop-down menu.
- In the **Assign access to** field, select **Virtual Machine**.
- In the **Subscription** field, select the subscription where the Cloud APIC is deployed.
- Select the Cloud APIC virtual machine.

b) Click **Save** at the bottom of the screen.

Step 6 Add a **User Access Administrator** role assignment.

a) In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **User Access Administrator** from the drop-down menu.
- In the **Assign access to** field, select **Virtual Machine**.
- In the **Subscription** field, select the subscription where the Cloud APIC is deployed.
- Select the Cloud APIC virtual machine.

b) Click **Save** at the bottom of the screen.

Note If you are sharing a subscription for the user tenant, it could take up to 30 minutes for a new IAM role assignment to take effect in Azure. Wait for at least 30 minutes before proceeding to the next section.

What to do next

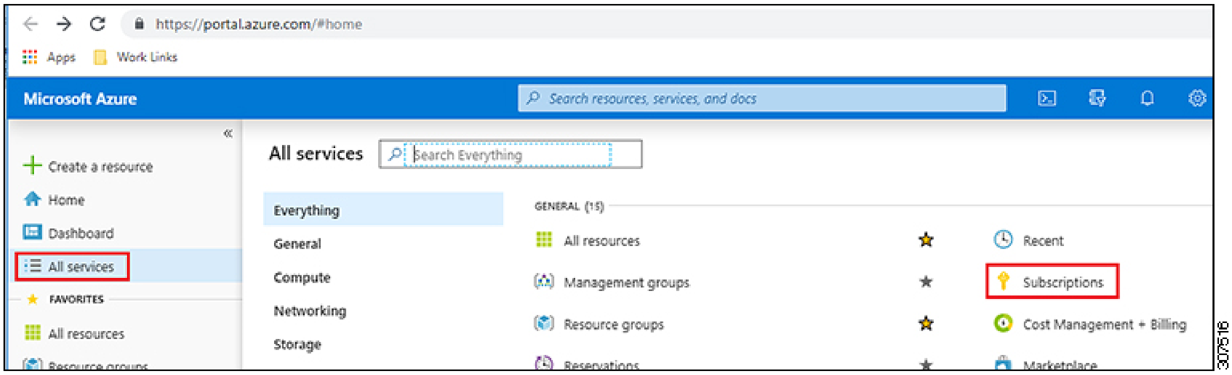
Go to Configuring Cisco Cloud APIC Using the Setup Wizard, on page 45 to continue setting up the Cloud APIC.

Adding a Role Assignment for an App

Follow the procedures in this section if you have an **unmanaged** identity for the access type, where the cloud resources will be managed through a specific application. See Understanding Tenants, Identities, and Subscriptions, on page 11 for more information about the relationship between Azure subscription types and Cloud APIC tenants.

Note If you have a **managed** identity for the access type, where you must add a role assignment for the user tenant, follow the procedures in Adding a Role Assignment for a Virtual Machine, on page 39 instead.

Step 1 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.



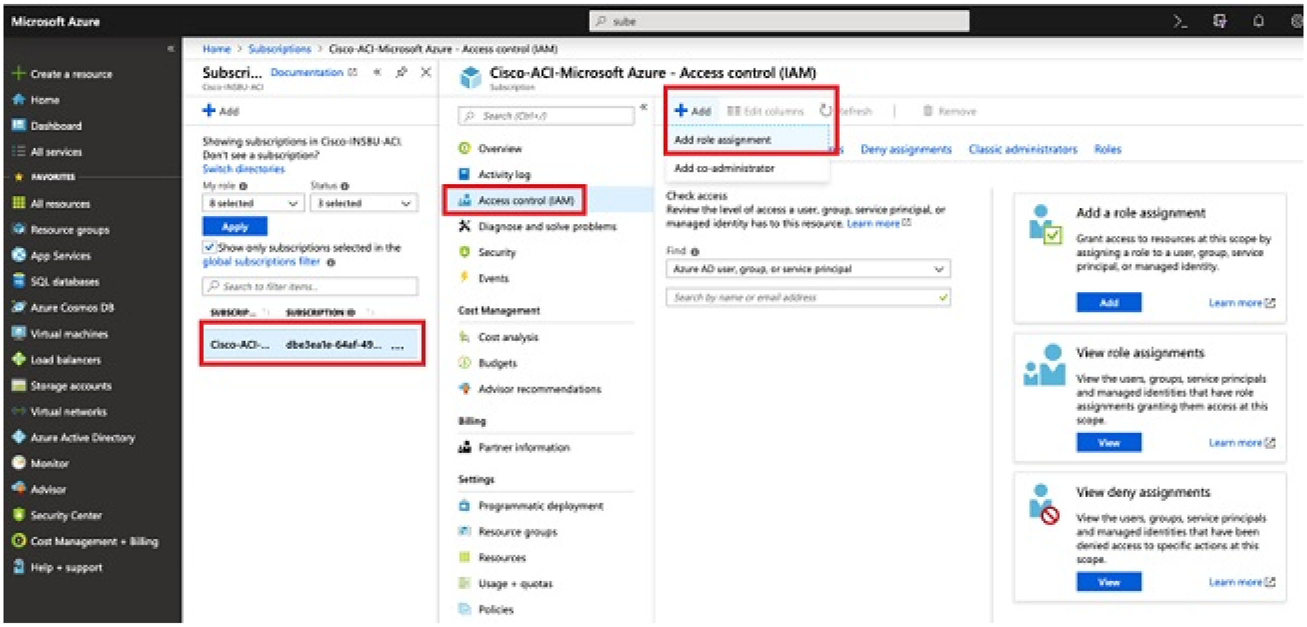
Step 2 In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

Step 3 From the overview page for that subscription, locate the **Access control (IAM)** link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

Step 4 Click **+ Add**, then select **Add role assignment** from the drop-down menu.



Showing subscriptions in Cisco-INSBU-ACI. Don't see a subscription?

My role: 8 selected

Status: 3 selected

☑ Show only subscriptions selected in the global subscriptions filter

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

Search by name or email address

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

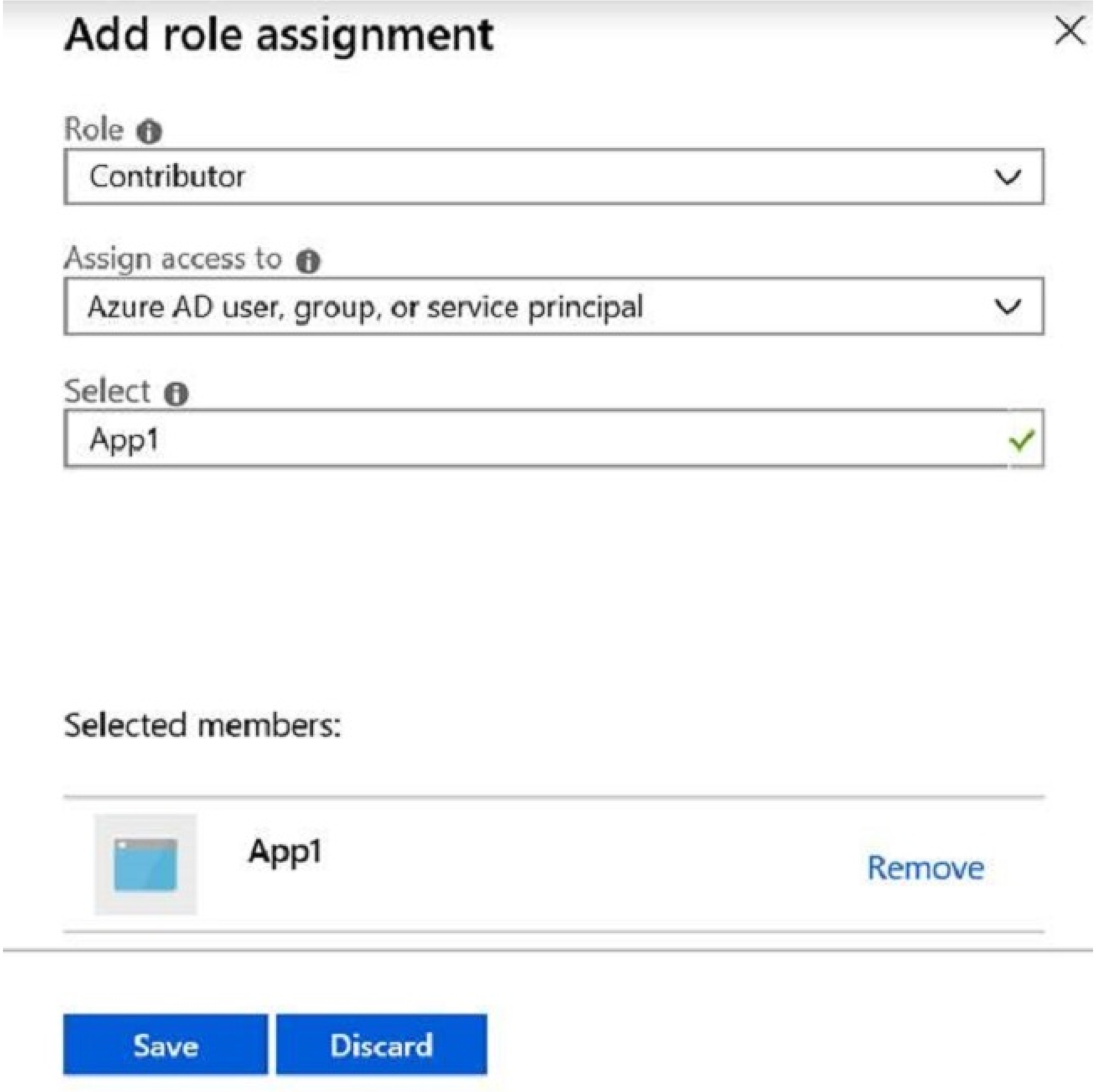
View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

Step 5 Add a **Contributor** role assignment.

a) In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **Contributor** from the drop-down menu.
- In the **Assign access to** field, select **Azure AD user, group, or service principal**.
- In the **Select** field, select the credentials that are associated with the Azure application.



Add role assignment

Role: Contributor

Assign access to: Azure AD user, group, or service principal

Select: App1

Selected members:

App1

b) Click **Save** at the bottom of the screen.

Step 6 Add a **User Access Administrator** role assignment.

a) In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **User Access Administrator** from the drop-down menu.
- In the **Assign access to** field, select **Azure AD user, group, or service principal**.
- In the **Select** field, select the credentials that are associated with the Azure application.

b) Click **Save** at the bottom of the screen.

Note It could take up to 30 minutes for a new IAM role assignment to take effect in Azure. Wait for at least 30 minutes before proceeding to the next chapter. If you attempt to configure the Cloud APIC using the setup wizard before the IAM role assignment takes effect in Azure, then the CCR deployment will fail.

What to do next

Go to Configuring Cisco Cloud APIC Using the Setup Wizard, on page 45 to continue setting up the Cloud APIC.

CHAPTER 5

Configuring Cisco Cloud APIC Using the Setup Wizard

Configuring and Deploying Inter-Site Connectivity

Before you can begin to configure and deploy your Cloud APIC, you must first configure and deploy your Multi-Site and your on-premises Cisco ACI, if you are connecting an on-premises site to cloud sites. The actual configuration for each varies, depending on your requirements and setup. If you are connecting an on-premises site to cloud sites, you will also need to configure and deploy an on-premises IPsec termination device to connect to the Cisco Cloud Routers deployed by Cloud APIC in Microsoft Azure. See Components of Extending Cisco ACI Fabric to the Public Cloud, on page 6 for more information.

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

- Cisco ACI documentation: Available at Cisco Application Policy Infrastructure Controller (APIC) documentation, such as Operating Cisco Application Centric Infrastructure and Cisco APIC Basic Configuration Guide.

- Nexus Dashboard documentation: Available at Nexus Dashboard documentation, such as Multi-Site Orchestrator Installation and Upgrade Guide.

- Cisco Cloud Routers (CCR):

  - Cloud Services Router 1000v: Available at Cisco CSR 1000v documentation.

  - Cisco Catalyst 8000v Edge Software: Available at Cisco Catalyst 8000v Edge software documentation.

Gathering On-Premises Configuration Information

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

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

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

Understanding Limitations for Number of Sites, Regions and CCRs

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

Sites

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

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

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

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

Regions

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

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

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

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

CCRs

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

- You must have at least one region with CCRs deployed to have inter-VNET (Azure), inter-VPC (AWS), or inter-VRF communications.
- You do not have to have CCRs in every region.
- For regions with CCRs deployed to enable connectivity:
    - CCRs can be deployed on all four managed regions.
    - The number of CCRs supported per managed region varies, depending on the release:
        - For releases prior to 5.1(2), a maximum of four CCRs per managed region is supported, for a total of 16 CCRs per cloud site.
        - For Release 5.1(2) and later, a maximum of eight CCRs per managed region is supported, for a total of 32 CCRs per cloud site. For more information on increasing the number of CCRs, see the *Cloud APIC for Azure User Guide*.

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

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

Cloud Resources Naming

Prior to Cloud APIC Release 5.0(2), the cloud resources created by the Cloud APIC in Azure were assigned names that were derived from the names of the ACI objects:

- Resource groups were created based on the Tenant, VRF, and region. For example, `CAPIC_<tenant>_<vrf>_<region>`.
- VNET names matched the name of the Cloud APIC VRF.
- Subnet names were derived from the CIDR address space. For example, `subnet-10.10.10.0_24` for the `10.10.10.0/24` cloud subnet.
- The cloud application name was derived from the EPG name and the application profile name. For example, `<epg-name>_cloudapp_<app-profile-name>`

This approach is not ideal for deployments with strict cloud resource naming conventions and it does not follow the Azure best practices for naming and tagging of cloud resources.

Starting with Cloud APIC Release 5.0(2), you can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud. You can define custom naming rules for all cloud resources during the first time setup wizard of the Cloud APIC, with the exception of the **Resource group** name used for the Cloud APIC ARM template deployment. The resource group name for the template is defined when you first deploy it and cannot be changed after. In addition to the global policy, you can also explicitly define the names of the cloud resources created from each Cloud APIC object using the REST API.

Starting with Cloud APIC Release 5.1(2), for Layer 4 to Layer 7 service deployments, you can provide custom names to cloud resources, such as, Network Load Balancers, Application Load Balancers and Device Application Security Groups.

Note Keep in mind that even with custom naming policy, once a cloud resource is created, you will not be able to modify the name. If you want to change the name of an existing cloud resource, you would need to delete all configured cloud resources and recreate them. Cloud resources to be deleted include overlay-2 CIDR and subnets, Cisco Cloud Router deployed by Cloud APIC and therefore IPSec tunnels from the CCRs to every remote site.

Variables Available for Naming Rules

When creating your cloud resources naming policy, you can use the following variables to dynamically define the name of the cloud resource based on the Cisco Cloud APIC objects:

- `${tenant}` – the resource will include the name of the Tenant
- `${ctx}` – the resource will include the name of the VRF
- `${ctxprofile}` – the resources will include the cloud context profile, which is a VRF deployed in a given cloud region
- `${subnet}` – the resource will include the string `subnet` followed by the subnet IP address

- `${app}` – the resource will include the name of the application profile.
- `${epg}` – the resource will include the name of the EPG.
- `${contract}` – the resource will include the name of the contract
- `${region}` – the resource will include the name of the cloud region
- `${priority}` – the resource will include the name of the network security group (NSG) rule priority. This number is allocated automatically to ensure that each NSG rule name is unique
- `${serviceType}` – the resource will include an abbreviation of the service Type (only valid for private endpoint resources)
- `${resourceName}` – the resource will include the name of the target resource (only valid for private endpoint resources)
- `${device}` – the resource will include the name of the Layer 4 to Layer 7 device.
- `${interface}` – the resource will include the name of the Layer 4 to Layer 7 device interface.
- `${deviceInterfaceDn}` – the resource will include the DN of the Layer to Layer 7 device interface.

For private endpoints, the combination of the `${app}-${svcepg}-${subnet}-${serviceType}-${resourceName}` makes the private endpoint name unique. Removing any of these variables might form a name of a private endpoint that already exists. This would result in a fault raised by the Cisco Cloud APIC. Also, the max length requirements vary from Azure service to service.

When you define a global naming policy using one or more of the above variables, Cisco Cloud APIC validates the string to ensure that all mandatory variables are present and no invalid string is specified.

There is a maximum name length limit in Azure. If the length of the name exceeds the length supported by the cloud provider, it rejects the config and Cisco Cloud APIC raises a fault that the resource creation failed. You can then check the fault for details and correct the naming rules. The maximum length limits at the time of Cisco Cloud APIC, Release 5.0(2) are listed below, for the latest up-to-date information and any changes to the length limit, consult the Azure documentation.

The following table provides a summary of which cloud resources support each of the naming variables above. Cells denoted with an asterisk (`*`) indicate variables that are mandatory for that type of cloud resource. Cells denoted with a plus sign (`+`) indicate that at least one of these variables is mandatory for that type of cloud resource; for example, for VNET resources you can provide `${ctx}`, or `${ctxprofile}`, or both.

Table 4: Supported Variables for Cloud Resources

Azure Resource	${tenant}	${ctx}	${ctxprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
Resource Group Max Length: 90	Yes*	Yes*						Yes*	

Azure Resource	`${tenant}`	`${ctx}`	`${ctxprofile}`	`${subnet}`	`${app}`	`${epg}`	`${contract}`	`${region}`	`${priority}`
Virtual Network (VNET) Max Length: 64	Yes	Yes+	Yes+					Yes	
Subnet Max Length: 80	Yes	Yes	Yes	Yes*				Yes	
Application Security Group (ASG) Max Length: 80	Yes				Yes*	Yes*		Yes	
Network Security Group (NSG) Max Length: 80	Yes				Yes*	Yes*		Yes	
Network Security Group Rule Max Length: 80	Yes						Yes		Yes* (auto)

Table 5: Supported Variables for Cloud Resources (Layer 4 to Layer 7 device services)

Azure Resource	`${tenant}`	`${region}`	`${ctxprofile}`	`${device}`	`${interface}`	`${deviceInterfaceDN}`
Internal Network Load Balancer Max Length: 80	Yes	Yes	Yes	Yes*		
Internet-facing Network Load Balancer Max Length: 80	Yes	Yes	Yes	Yes*		

Azure Resource	`${tenant}`	`${region}`	`${ctxprofile}`	`${device}`	`${interface}`	`${deviceInterfaceDN}`
Internal Application Load Balancer Max Length: 80	Yes	Yes	Yes	Yes*		
Internet-facing Application Load Balancer Max Length: 80	Yes	Yes	Yes	Yes*		
Device ASG Max Length: 80	Yes	Yes		Yes*	Yes*	Yes*

Naming Rules Guidelines and Limitations

When configuring custom rules for naming cloud resources, the following restrictions apply:

- You define global naming policy during the Cloud APIC's first time setup using two sets of naming rules:
  - **Hub Resource Naming Rules** define names for the Hub Resource Group, Hub VNET, Overlay-1 CIDR, Overlay-2 CIDR subnet in the Infra Tenant, as well as the subnet prefixes for subnets that are created automatically by the system in the Infra tenant.
  - **Cloud Resource Naming Rules** define the names of the Network Security Group (NSG), Application Security Group (ASG), Network Load Balancer, Application Load Balancer, Device Application Security Group, and subnets you create in the Infra Tenant, as well as the names of all resources (Resource Groups, Virtual Networks, Subnets, NSG, ASG, Network Load Balancer, Application Load Balancer) in user Tenants.

  After you define the naming rules, you will be required to review and confirm them. Keep in mind that you must confirm the naming rules before any cloud resources are deployed.

- Once a cloud resource is created, its name cannot be changed and the naming policy cannot be updated in the GUI. If you upgrade your Cloud APIC to Release 5.0(2) with some resources already deployed in Azure, you will also not be able to change the global custom naming rules.

  If you want to change the names of the existing cloud resources or the policy, you would need to delete the deployed resources before being able to update the global naming policy in the GUI.

  In these cases you can use the REST API to explicitly assign custom names to any new resources you create.

- When updating cloud resources naming via REST API, we recommend you do not import configuration at the same time.

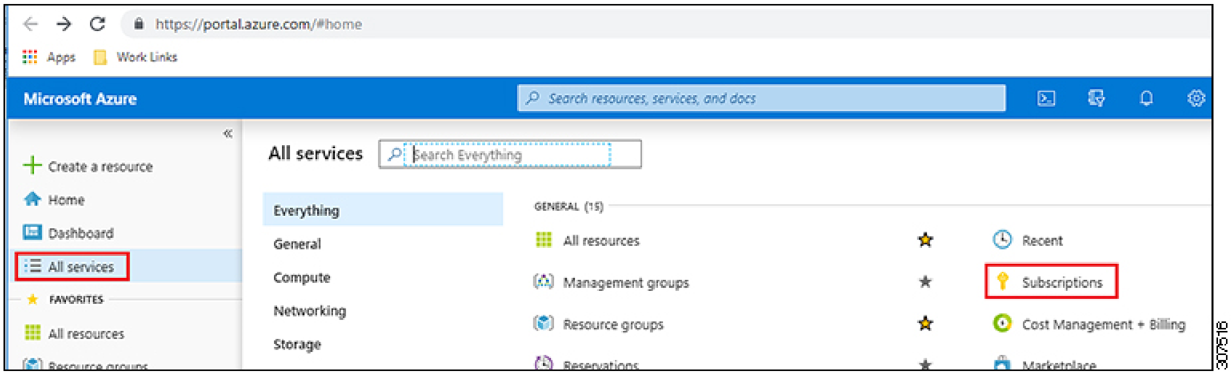
  We recommend you define any naming rules first. Then any tenant configuration.

  We recommend that you do not change the naming policy after the tenant configuration is deployed.

Locating the Cloud APIC IP Address

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

Step 1 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.



Step 2 In the **Subscriptions** page in the Azure management portal, click the subscription account that you just created.

The overview information for that subscription is displayed.

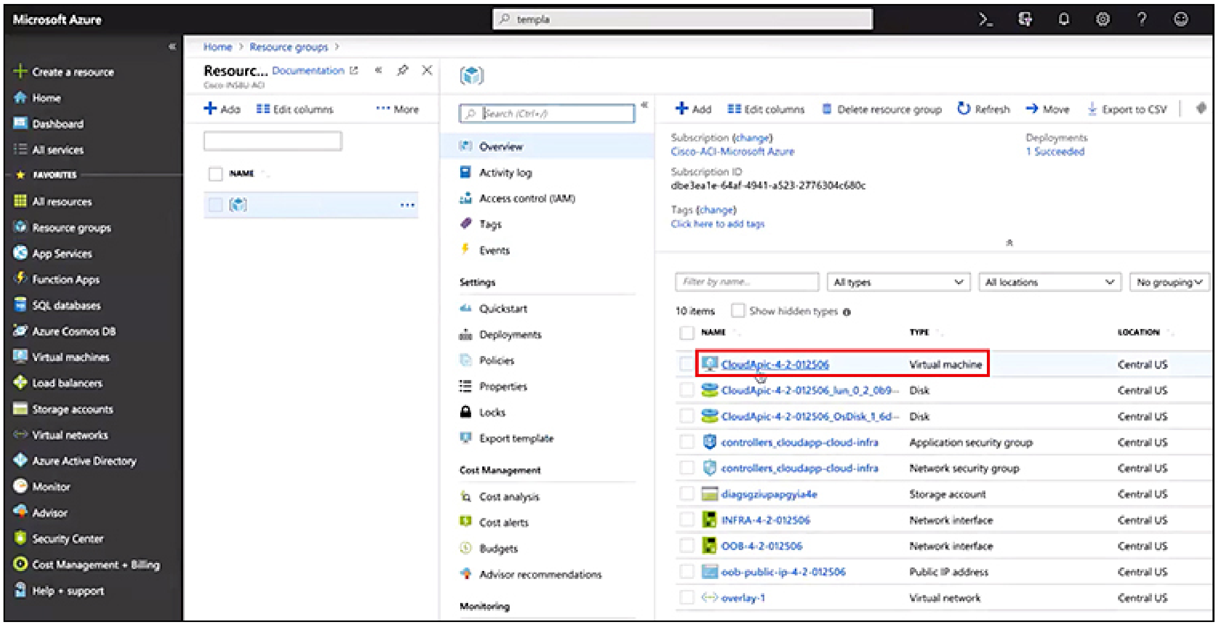
Step 3 From the overview page for that subscription, locate the **Resource groups** link in the left nav bar and click that link.

The resource groups for that subscription is displayed.

Step 4 Choose the resource group that you chose or created in Deploying the Cloud APIC in Azure, on page 33.

The overview information for that resource group is displayed.

Step 5 In the overview page for the resource group, locate your Cloud APIC VM instance (shown as **Virtual machine** under the TYPE column), and click the link for that VM instance.



Subscription (change): Cisco-ACI-Microsoft Azure

Deployments: 1 Succeeded

Subscription ID: dbe3ea1e-64af-4941-a523-2776304c680c

Tags (change): Click here to add tags

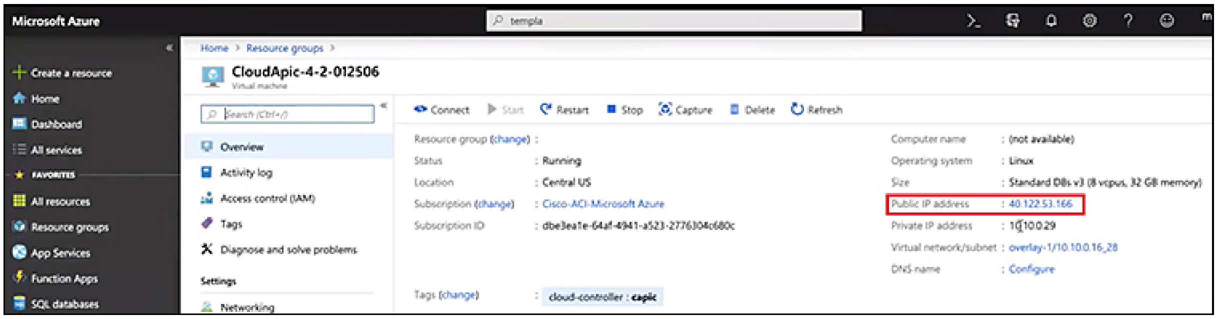
10 items

NAME	TYPE	LOCATION
CloudApic-4-2-012506	Virtual machine	Central US
CloudApic-4-2-012506_lun_0_2_0b9...	Disk	Central US
CloudApic-4-2-012506_OsDisk_1_6d...	Disk	Central US
controllers_cloudapp-cloud-infra	Application security group	Central US
controllers_cloudapp-cloud-infra	Network security group	Central US
diagsgziupapgyia4e	Storage account	Central US
INFRA-4-2-012506	Network interface	Central US
OOB-4-2-012506	Network interface	Central US
oob-public-ip-4-2-012506	Public IP address	Central US
overlay-1	Virtual network	Central US

307585

The overview information for the Cloud APIC VM instance is displayed.

Step 6 Locate the entry in the **Public IP address** field in this page and copy that IP address entry.



Resource group (change) :

Status : Running

Location : Central US

Subscription (change) : Cisco-ACI-Microsoft Azure

Subscription ID : dbe3ea1e-64af-4941-a523-2776304c680c

Tags (change) : cloud-controller : capic

Computer name : (not available)

Operating system : Linux

Size : Standard D8s v3 (8 vcpus, 32 GB memory)

Public IP address : 40.122.53.166

Private IP address : 10.10.0.29

Virtual network/subnet : overlay-1/10.10.0.16_28

DNS name : Configure

307576

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

Configuring Cisco Cloud APIC Using the Setup Wizard

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

Before you begin

Following are the prerequisites for this task:

- You have met the requirements that are outlined in Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 17 before proceeding with the tasks in this section.

- You have successfully completed the procedures that are provided in Deploying the Cloud APIC in Azure, on page 23.

Step 1 Locate the IP address for your Cloud APIC.

See Locating the Cloud APIC IP Address, on page 52 for those instructions.

Step 2 Open a browser window and, using the secure version of HTTP (`https://`), paste the IP address into the URL field, then press Return to access this Cloud APIC.

For example, `https://192.168.0.0`.

If you see a message asking you to **Ignore Risk and Accept Certificate**, accept the certificate to continue.

Step 3 Enter the following information in the login page for the Cloud APIC:

- **Username:** Enter **admin** for this field.
- **Password:** Enter the password that you provided to log into the Cloud APIC.
- **Domain:** If you see the **Domain** field, leave the default Domain entry as-is.

Step 4 Click **Login** at the bottom of the page.

Note If you see an error message when you try to log in, such as `REST Endpoint user authentication datastore is not initialized - Check Fabric Membership Status of this fabric node`, wait for several minutes, then try again after a few minutes. You might also have to refresh the page in order to log in.

The Welcome to Cloud APIC setup wizard page appears.

Step 5 Click **Begin Set Up**.

The **Let's Configure the Basics** page appears, with these areas to be configured:

- **DNS and NTP Servers**
- **Region Management**
- **Smart Licensing**

Step 6 In the **DNS and NTP Servers** row, click **Edit Configuration**.

The **DNS and NTP** page appears.

Step 7 In the **DNS and NTP** page, add the DNS, if necessary, and NTP servers.

- A DNS server is already configured by default. Add a DNS server if you want to use a specific DNS server.
- An NTP server is not configured by default, however, so we recommend that you configure an NTP server. Skip to 7.d, on page 54 if you want to configure an NTP server and you do not want to configure a DNS server.

a) If you want to use a specific DNS server, under the **DNS Servers** area, click **+Add DNS Provider**.
b) Enter the IP address for the DNS servers and, if necessary, check the box next to Preferred DNS Provider.
c) Click the check mark next to the DNS server, and repeat for any additional DNS servers that you want to add.
d) Under the **NTP Servers** area, click **+Add Providers**.

e) Enter the IP address for the NTP servers and, if necessary, check the box next to Preferred NTP Provider.

f) Click the check mark next to the NTP server, and repeat for any additional NTP servers that you want to add.

Step 8 When you have finished adding the DNS and NTP servers, click **Save and Continue**.

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

Step 9 In the **Region Management** row, click **Begin**.

The **Region Management** page appears.

Step 10 Set the type of connectivity that you want for the internal network in the **Connectivity for Internal Network** area, if necessary.

VNet peering at the global level is set in the **Connectivity for Internal Network** area, which enables VNet peering at the Cloud APIC level, deploying NLBs in all the regions with a CCR. For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document in the Cisco Cloud APIC documentation page.

- For release 5.1(2) and later, VNet peering at the global level is enabled by default and cannot be disabled.
- For releases prior to release 5.1(2), you can set the type of connectivity that you want for the internal network in the **Connectivity for Internal Network** area.
  - To enable Azure VNet peering at the global level, click **Virtual Network Peering**.
  - To enable the traditional VPN connectivity through the CCRs instead of through VNet peering, click **VPN Connectivity via CCR**.

Step 11 If you want connectivity to the on-premises site or another cloud site—in addition to connectivity within a region—check the **Inter-Site Connectivity** check box.

Step 12 Verify that the Cloud APIC home region is selected.

The region that you selected when you were configuring your cloud site is the home region and should be selected already in this page. This is the region where the Cloud APIC is deployed (the region that will be managed by Cloud APIC), and will be indicated with the text `Cloud APIC Deployed` in the Region column.

Note If you enabled Azure VNet peering in Step 10, on page 55, you must also check the box in the **Cloud Routers** column for the Cloud APIC home region, if it is not checked already.

Step 13 Select additional regions if you want the Cloud APIC to manage additional regions, and to possibly deploy CCRs to have inter-VNET communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

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

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

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

- **Cloud Routers:** Select this option if you want to deploy CCRs in this region. You must have at least one region with CCRs deployed to have inter-VNET or inter-VPC communications. However, if you choose multiple regions in this page, you do not have to have CCRs in every region that you choose. See Understanding Limitations for Number of Sites, Regions and CCRs, on page 46 for more information.

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

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

The **General Connectivity** page appears.

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

a) Under the **General** area, in the **Subnet Pools for Cloud Routers** field, click **Add Subnet Pool for Cloud Routers** if you want to add additional subnets for CCRs.

The first subnet pool is automatically populated (shown as `System Internal`). Addresses from this subnet pool will be used for inter-region connectivity for any additional regions that are added that need to be managed by the Cloud APIC. Subnet pools added in this field must be a valid IPv4 subnet with mask /24.

Add additional subnets for CCRs in this step in these situations:

- If you have a CCR deployed in the Cloud APIC home region, add one additional subnet pool in addition to the `System Internal` subnet pool that is automatically generated
- If you selected additional regions to be managed by Cloud APIC in the previous page:
  - Add *one* additional subnet pool for every managed region with 2-4 CCRs per managed region (if you enter **2**, **3**, or **4** in the **Number of Routers Per Region** field in 15.f, on page 58)
  - Add *two* additional subnet pools for every managed region with five or more CCRs per managed region (if you enter between **5** and **8** in the **Number of Routers Per Region** field in 15.f, on page 58)

For example:

- Assume you have only the Cloud APIC home region selected in the previous page, and you have a CCR deployed in the Cloud APIC home region. You will need two subnet pools (the automatically-populated **System Internal** subnet pool and one additional subnet pool that is created by you).
- Next, assume you selected two additional regions for Cloud APIC to manage in the previous page, and you have CCRs deployed in both additional regions. In addition, assume you select between 2-4 CCRs to be deployed in each managed region in the **Number of Routers Per Region** field (15.f, on page 58). In this case, you would need to add two additional subnet pools (one subnet pool for every region with CCRs that you selected in the previous page), for a total of four subnet pools (one automatically populated as **System Internal** and three additional ones that are created by you).
- Finally, assume that you decide to increase the number of CCRs in each managed region to eight at a later date, where you return to this page and you change the value to **8** in the **Number of Routers Per Region** field (15.f, on page 58). Because you have three regions selected in the previous screen (the Cloud APIC home region and two additional regions that you selected to have the Cloud APIC to manage), and you increased the number of CCRs per managed region above four, you would need to add three additional subnet pools again, one for every managed region that has more than four CCRs, for a total of seven subnet pools:
  - One automatically populated as **System Internal**
  - Two for the CCRs in the home region (one subnet pool created by you previously, and the other one created by you here when you increased the number of CCRs to 8 per managed region)

- Four for the CCRs in the two additional regions that you selected to have managed by the Cloud APIC (two subnet pools created by you previously, and the other two created by you here when you increased the number of CCRs to 8 per managed region)

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

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

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

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

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

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

d) Under the **CCRs** area, in the **BGP Autonomous System Number for CCRs** field, enter the BGP autonomous system number (ASN) that is unique to this site.

The BGP autonomous system number can be in the range of 1 - 65534.

Note the following Microsoft Azure ASN restrictions:

- Do not use 64518 as the autonomous system number in this field.
- Do not use 32-bit ASNs. Azure VPN Gateways support 16-Bit ASNs at this time.
- The following ASNs are reserved by Azure for both internal and external peerings:
  - Public ASNs: 8074, 8075, 12076
  - Private ASNs: 65515, 65517, 65518, 65519, 65520

  You cannot specify these ASNs for your on-premises VPN devices when connecting to Azure VPN gateways.
- The following ASNs are reserved by IANA and cannot be configured on your Azure VPN Gateway: 23456, 64496-64511, 65535-65551 and 429496729

e) In the **Assign Public IP to CCR Interface** field, determine if you want to assign public IP addresses or private IP addresses to the CCR interfaces.

The CCR interface IP addresses are used for the following purposes:

- Allows you to configure the CCR through the Management Interface in the Cloud APIC GUI
- Allows you to cross-program the interfaces across sites for multi-cloud and hybrid cloud connectivity through the Cisco Nexus Dashboard Orchestrator
- For the CCRs for both control plane and data plane traffic

By default, the **Enabled** check box is checked. This means that public IP addresses can be assigned to the CCRs.

- If you want *public* IP addresses assigned to the CCRs, leave the check in the box next to **Enabled**.
- If you want *private* IP addresses assigned to the CCRs, remove the check in the box next to **Enabled**.

Note that changing the CCR connectivity from private to public, or vice versa, may cause disruption in your network.

Note Beginning with release 5.1(2), both the public and private IP addresses assigned to a CCR are displayed with the other details of the router in the Cloud Resources area. If a public IP is not assigned to a CCR, only the private IP is displayed.

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

See Understanding Limitations for Number of Sites, Regions and CCRs, on page 46 for more information on any limitations on the number of CCRs per region.

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

Note Do not use `admin` as a username for the Cisco Cloud Router when connecting to an Azure cloud site.

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

Enter the password again in the **Confirm Password** field.

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

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

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

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

1. In the **Throughput of the routers** field, choose the throughput of the Cisco Cloud Router.

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

   Note the following:

   - The licensing of the CCR is based on this setting. You will need the equivalent or higher license in your Smart account for it to be compliant. See Requirements for the Azure Public Cloud, on page 18 for more information.
   - Cloud routers should be undeployed from all regions before changing the router throughput or login credentials.

     If you wish to change this value at some point in the future, you must delete the CCR, then repeat the processes in this chapter again and select the new value that you would like in the same **Throughput of the routers** field.

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

   Beginning with Release 5.0(2i), the **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied to all cloud router interfaces, including data Gigabit Ethernet interfaces, IPSec tunnel interfaces of cloud routers, and VPN tunnel interfaces toward cloud, on-premises, or other cloud sites. For VPN tunnels towards the cloud, if the cloud provider's MSS value is less than the value that you enter in this field, then the lower value is used; otherwise, the value that you enter in this field is used.

The MSS value affects only TCP traffic, and has no impact on other types of traffic, such as ping traffic.

3. In the **License Token** field, enter the license token for the Cisco Cloud Router.

   This is the Product Instance Registration token from your Cisco Smart Software Licensing account. To get this license token, go to http://software.cisco.com, then navigate to **Smart Software Licensing** > **Inventory** > **Virtual Account** to find the Product Instance Registration token. See Cisco Cloud APIC Licensing, on page 13 for more information.

   Note If you assigned private IP addresses to the CCRs in 15.e, on page 57, the only supported option is **Direct connect to Cisco Smart Software Manager (CSSM)** when registering smart licensing for CCRs with private IP addresses. You must provide reachability to the CSSM through express route in this case.

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

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

   Cisco Cloud APIC supports a range of VM types. The table below shows the various instances of the VM types available along with their capacity.

VmName on Azure	Memory	vCPUs	NetworkBw
DS3V2	14GiB	4	Up to 3 Gigabit
DS4V2	28GiB	8	Up to 6 Gigabit
F16SV2	32GiB	16	Up to 12.5 Gigabit
F32SV2	64GiB	32	Up to 16 Gigabit

   Note If you wish to change this value at some point in the future, you must delete the CCR, then repeat the processes in this chapter again and select the new value that you would like in the same VM field.

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

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

   Beginning with Release 5.0(2l), the **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied all cloud router interfaces, including VPN tunnels towards the cloud and external tunnels towards the on-premises site or other cloud sites. For VPN tunnels towards the cloud, if the cloud provider's MSS value is less than the value that you enter in this field, then the lower value is used; otherwise, the value that you enter in this field is used.

   The MSS value affects only TCP traffic, and has no impact on other types of traffic, such as ping traffic.

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

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

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

- If you are not configuring inter-site connectivity (if you did not select **Inter-Site Connectivity** when you were selecting regions to manage in the **Region Management** page), click **Save and Continue**. The **Let's Configure the Basics** page appears again. Skip to Step 22, on page 61.

- If you are configuring inter-site connectivity (if you selected **Inter-Site Connectivity** when you were selecting regions to manage in the **Region Management** page), click **Next** at the bottom of the page. The **Inter-Site Connectivity** page appears.

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

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

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

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

- **OSPF Area for Inter-Site Connectivity**: Enter the underlay OSPF area ID that will be used with on-premises ISN peering (for example, `0.0.0.1`)

- Under the **External Subnets for Inter-Site Connectivity** heading, click the **+** button next to the **+Add External Subnet** field.

  - Enter the subnet tunnel endpoint pool (the cloud TEP) that will be used in Azure. It must be a valid IPv4 subnet with a mask between /16 and /22 (for example, `30.29.0.0/16`). This subnet will be used to address the IPsec tunnel interfaces and loopbacks of the Cloud Routers used for on-premises connectivity, and cannot overlap with other on-premises TEP pools.
  - Click the check mark after you have entered in the appropriate subnet pools.

Step 18 When you have configured all the connectivity options, click **Next** at the bottom of the page.

The **Cloud Resource Naming Rules** page appears.

Step 19 Choose **Cloud Resource Naming** mode.

Starting with Release 5.0(2), you can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud. Additional details about naming rules, available object name variables, guidelines, and limitations are available in the earlier Cloud Resources Naming, on page 48 section of this chapter.

You can choose one of the following:

- **Default**, in which case the cloud resources created by the Cloud APIC in Azure will be assigned names that are derived from the names of the ACI objects. For example, resource groups' names will be based on the Tenant, VRF, and region: `CAPIC_<tenant>_<vrf>_<region>`.

- **Custom**, in which case you can define your own rules for how each of the cloud resources is named.

  When you select the custom naming, an **Edit** icon appears next to each cloud resource. You can click the edit icon to define the naming convention for one or more of the displayed resources.

  The variables that are available for this type of resource are listed under the naming rule text box. The variables are divided into the **Required Keyword** and **Optional Keywords**, you must include all the required keywords for the rule you are updating. For example, when defining the naming rule for Azure's Resource Groups, you must include the Tenant name, VRF name, and the Region keywords.

Step 20 Confirm you have reviewed and accept the global resource naming policy.

Once a cloud resource is created, its name cannot be changed. As such, you must review and accept the global naming policy you have defined in the previous step before any cloud resources can be deployed. When ready, enable the **Deploy cloud resources based on these naming rules** checkbox.

Note that you can leave the checkbox unchecked and choose to proceed, in which case any changes you have made will be saved but no configuration will be deployed. You would need to come back to this screen to accept the naming policy to deploy.

Step 21 When you have entered all the necessary information on this page, click **Save and Continue** at the bottom of the page.

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

Step 22 In the **Smart Licensing** row, click **Register**.

The **Smart Licensing** page appears.

Step 23 Enter the necessary information in the **Smart Licensing** page.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To register your Cloud APIC with Cisco Smart Software Licensing, do the following

- Ensure that this product has access to the internet or a Smart Software Manager satellite installed on your network.
- Log in to Smart Account:
  - Smart Software Manager: https://software.cisco.com/
  - Smart Software Manager Satellite: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
- Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Step 24 Click **Register** at the bottom of the page if you entered the necessary licensing information on this page, or click **Continue in Evaluation Mode** if you want to continue in evaluation mode instead.

The **Summary** page appears.

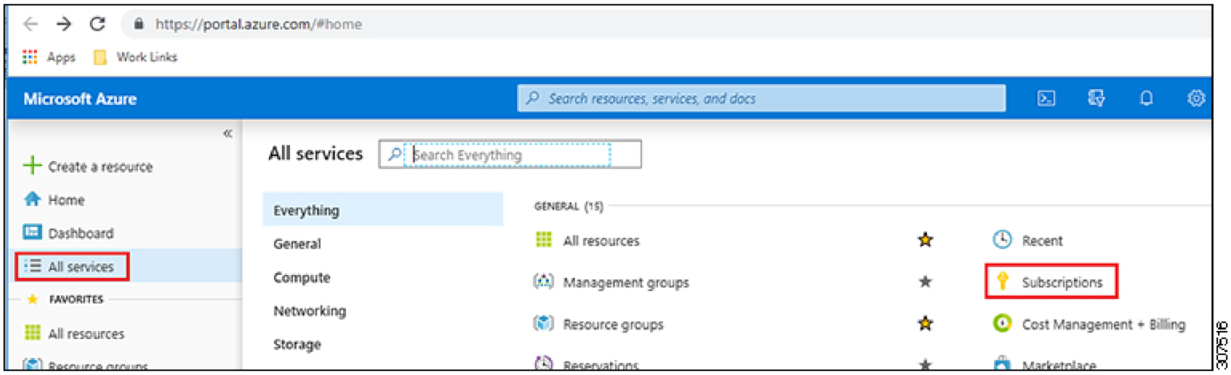
Step 25 Verify the information on the **Summary** page, then click **Finish**.

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

If this is the first time that you are deploying your Cloud APIC, this process might take quite a bit of time, possibly 30 minutes or so before the process is successfully completed.

Step 26 Verify that the CCRs were successfully deployed.

a) From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.



b) In the **Subscriptions** page in the Azure management portal, click the subscription account that you created.

The overview information for that subscription is displayed.

c) From the overview page for that subscription, locate the **Resource groups** link in the left nav bar and click that link.

The resource groups for that subscription is displayed.

d) Choose the resource group that you chose or created in the **Custom deployment** page in Deploying the Cloud APIC in Azure, on page 33.

The overview information for that resource group is displayed.

e) In the overview page for the resource group, locate your CCR VM instance (shown as **Virtual machine** under the TYPE column), and click the link for that VM instance.

The CCR VM instance will have a name with a `ct_routerp_`*`region`*`_`*`x`*`_0` format, where:

- *region* is the managed region (for example, `westus`, `westus2`, `centralus`, or `eastus`)
- *x* is the CCR count, starting from zero

For example: `ct_routerp_centralus_0_0` or `ct_routerp_centralus_1_0`

The overview information for the CCR VM instance is displayed.

f) Locate the **Status** field at the top left area in the page.

- If you see the text **Creating** in the **Status** field, then the CCRs are not fully deployed yet.
- If you see the text **Running** in the **Status** field, then the CCRs are fully deployed.

What to do next

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

- If you are managing additional sites (an on-premises site or cloud sites) along with the Cisco Cloud APIC site (if you selected the **Inter-Site Connectivity** option in the **Region Management** page), go to Managing Cisco Cloud APIC Through Multi-Site, on page 65.
- If you are setting up a Cloud First configuration, where you are not managing any other sites along with the Cisco Cloud APIC site (if you selected only the **Cloud Routers** option in the **Region Management**

page), you will not need to use the Multi-Site for additional configurations. However, you will have additional configurations that you must perform in the Cisco Cloud APIC GUI in this case.

You also need to create a tenant using the Cisco Cloud APIC GUI using the instructions in Creating a Tenant Using the Cisco Cloud APIC GUI, on page 83.

Use the Global Create option in the Cisco Cloud APIC GUI to configure the following components:

- Tenant
- Application Profile
- EPG

See Navigating the Cisco Cloud APIC GUI, on page 83 and Configuring Cisco Cloud APIC Components, on page 83 for more information.

Verifying the Cisco Cloud APIC Setup Wizard Configurations

Use the procedures in this topic to verify that the configuration information that you entered in the Cloud APIC Setup Wizard are applied correctly.

In Cisco Cloud APIC, verify the following settings:

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

What to do next

Complete the multi-site configuration using the procedures provided in Managing Cisco Cloud APIC Through Multi-Site, on page 65.

CHAPTER 6

Managing Cisco Cloud APIC Through Multi-Site

About Cisco Cloud APIC and Multi-Site

If you selected the **Inter-Site Connectivity** option in the **Region Management** page when configuring Cisco Cloud APIC using the setup wizard, you will use Multi-Site to manage another site, such as an on-premises site or cloud sites, along with the Cisco Cloud APIC site. You do not need the Multi-Site if you selected only the **Cloud Routers** option in the **Region Management** page in the Setup Wizard for Cisco Cloud APIC.

Several new pages have been introduced in the Cisco Nexus Dashboard Orchestrator that are used specifically for the management of the Cisco Cloud APIC. The topics in this chapter provide information on these new Cisco Cloud APIC management pages. Once you have entered the necessary information in these Cisco Cloud APIC management pages, the Cisco Cloud APIC essentially becomes another site that you manage through the Multi-Site.

If you are managing an on-premises site along with the Cisco Cloud APIC site, we recommend that you set up your on-premises site before beginning these procedures, if it is not set up already. See the *Multi-Site Orchestrator Installation and Upgrade Guide* for those procedures, located here: https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Adding the Cisco Cloud APIC Site to Multi-Site

Step 1 Log in to the Cisco Nexus Dashboard Orchestrator, if you aren't already logged in.

Step 2 In the Main menu, click **Sites**.

Step 3 In the **Sites List** page, click **ADD SITE**.

Step 4 In the **Connection Settings** page, perform the following actions:

a) In the **NAME** field, enter the site name.

   For example, `cloudsite1`.

b) (Optional) In the **LABELS** field, choose or create a label.

c) In the **APIC CONTROLLER URL** field, enter the URL of the Cloud APIC. This is the public IP address allocated by Azure, which will be the same public IP address that you used to log into the Cloud APIC at the beginning of the procedures for configuring Cisco Cloud APIC using the setup wizard.

   For example, `https://192.0.2.1`.

d) In the **USERNAME** field, enter a username.

   For example, `admin`. Note that you can also register with any account that has the same privilege as `admin`.

e) In the **PASSWORD** field, enter the password.

f) In the **APIC SITE ID** field, enter a unique site ID, if this field is not already populated automatically.

   The site ID must be a unique identifier of the Cloud APIC site. The range must be from 1 to 127.

g) Click **SAVE**.

Step 5 Verify that Cloud APIC site was added correctly.

If you are managing multiple sites, all sites should be displayed in the Sites screen in the Cisco Nexus Dashboard Orchestrator. The Cisco Nexus Dashboard Orchestrator automatically detects if the site is an on-premises or a Cloud APIC site.

What to do next

Go to Configuring the Intersite Infrastructure, on page 66.

Configuring the Intersite Infrastructure

Step 1 In the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

Step 2 In the left pane, under **SITES**, click on the cloud site.

Almost all of the information in the cloud site area is automatically populated and cannot be changed, with the exception of the BGP Password field, described in the next step.

Step 3 Determine if you want to configure a password between your on-premises site and your cloud site:

- If you do *not* want to configure a password between your on-premises site and your cloud site, skip to Step 4, on page 67.
- If you want to configure a password between your on-premises site and your cloud site:

a) In the right pane, click on the **BGP Password** field and enter a password.

b) Click the Refresh icon at the upper right corner of the CloudSite window.

All of the cloud properties are automatically fetched from the Cloud APIC. A `Site refreshed successfully` message appears, verifying that all the cloud properties were successfully fetched from the Cloud APIC.

Step 4 Click the **Multi-Site** button to toggle this on to enable Multi-Site connectivity in the cloud site.

Step 5 Choose the type of deployment that you would like to use to configure the intersite infrastructure.

When you click the **Deploy** button at the top right of the screen, it shows the following scroll-down menu options:

- **Deploy Only:** Select this option if you are configuring Multi-Cloud (cloud site-to-cloud site) connectivity.

  This option pushes the configuration to the cloud sites and the Cloud APIC site and enables the end-to-end interconnect connectivity between the cloud sites.

- **Deploy & Download IPN Device config files:** Pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect connectivity between the on-premises and the cloud site. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Router (CCR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

- **Download IPN Device config files only:** Downloads a zip file that contains configuration information that you will use to enable connectivity between the CCR deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices

Note Follow the procedures in this section only if you are enabling connectivity between the on-premises site and the cloud site. If you do not have an on-premises site, skip these procedures and go to Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 71.

Follow these procedures to manually enable connectivity between Cisco Cloud Router (CCR) deployed in Azure and the on-premises IPsec termination device.

By default, the Cisco Cloud APIC will deploy a pair of redundant CCRs. The procedures in this section creates two tunnels, one IPsec tunnel from the on-premises IPsec device to each of these CCRs.

The following information provides commands for CCR as your on-premises IPsec termination device. Use similar commands if you are using a different device or platform.

Step 1 Gather the necessary information that you will need to enable connectivity between the CCRs deployed in Azure and the on-premises IPsec termination device.

- If you selected either the **Deploy & Download IPN Device config files** or the **Download IPN Device config files only** option in Cisco Nexus Dashboard Orchestrator as part of the procedures provided in Configuring the Intersite Infrastructure, on page 66, locate the zip file that contains the configuration files for the ISN devices.
- If you are manually locating the information that you need to enable connectivity between the CCRs deployed in Azure and the on-premises IPsec termination device, gather the CCR and Tenant information, as described in the Appendix of the *Cisco Cloud APIC Installation Guide*.

Step 2 Log into the on-premises IPsec device.

Step 3 Configure the tunnel for the *first* CCR.

If you downloaded the configuration files for the ISN devices through Cisco Nexus Dashboard Orchestrator, locate the configuration information for the first CCR and enter that configuration information.

Following is an example of what the configuration information for the first CCR might look like:

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<first-CCR-tunnel-ID>
    pre-shared-key address <first-CCR-elastic-IP-address> key <first-CCR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CCR-tunnel-ID>
    local-address <interface>
    match identity address <first-CCR-elastic-IP-address>
    keyring infra:overlay-1-<first-CCR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CCR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CCR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <first-CCR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CCR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <first-CCR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<first-CCR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
```

```
exit
```

Where:

- <first-CCR-tunnel-ID> is a unique tunnel ID that you assign to this tunnel.
- <first-CCR-elastic-IP-address> is the elastic IP address of the third network interface of the first CCR.
- <first-CCR-preshared-key> is the preshared key of the first CCR.
- <interface> is the interface that is used for connecting to the CCR deployed in Azure.
- <peer-tunnel-for-onprem-IPsec-to-first-CCR> is the peer tunnel IP address for the on-premises IPsec device to the first cloud CCR.
- <process-id> is the OSPF process ID.
- <area-id> is the OSPF area ID.

For example:

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1000
    pre-shared-key address 192.0.2.20 key 123456789009876543211234567890
exit

crypto isakmp profile infra:overlay-1-1000
    local-address GigabitEthernet1
    match identity address 192.0.2.20
    keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1000
    ip address 30.29.1.2 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.20
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1000
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

Step 4 Configure the tunnel for the *second* CCR.

If you downloaded the configuration files for the ISN devices through Cisco Nexus Dashboard Orchestrator, locate the configuration information for the second CCR and enter that configuration information.

Following is an example of what the configuration information for the second CCR might look like:

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<second-CCR-tunnel-ID>
    pre-shared-key address <second-CCR-elastic-IP-address> key <second-CCR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<second-CCR-tunnel-ID>
    local-address <interface>
    match identity address <second-CCR-elastic-IP-address>
    keyring infra:overlay-1-<second-CCR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CCR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CCR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <second-CCR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-second-CCR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <second-CCR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<second-CCR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

For example:

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1001
    pre-shared-key address 192.0.2.21 key 123456789009876543211234567891
exit
```

```
crypto isakmp profile infra:overlay-1-1001
    local-address GigabitEthernet1
    match identity address 192.0.2.21
    keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1001
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1001
    ip address 30.29.1.6 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.21
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1001
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

Step 5 Repeat these steps for any additional CCRs that you need to configure.

Step 6 Verify that the tunnels are up on your on-premises IPsec device.

For example:

```
ISN_CCR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1000             30.29.1.2         YES manual up                    up
Tunnel1001             30.29.1.4         YES manual up                    up
```

If you do not see that both tunnels are shown as up, verify the information that you entered in the steps in this section to determine where you might have an issue. Do not proceed to the next section until you see that both tunnels are shown as up.

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. You will be given the choice of choosing these security domains when you configure a shared tenant using the procedures in Configuring a Tenant, on page 72.

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

Step 1 Log into your Cloud APIC system.

Step 2 Click the **Intent** icon. The **Intent** menu appears.

Step 3 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

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

Step 4 From the **Administrative** list in the **Intent** menu, click **Create Security Domain**. The **Create Security Domain** dialog box appears.

Step 5 In the **Name** field, enter the name of the security domain.

Step 6 In the **Description** field, enter a description of the security domain.

Step 7 Click **Save** when finished.

Configuring a Tenant

Use the procedures in this section to configure a tenant that is shared between the on-premises site and the Cloud APIC site. See Understanding Tenants, Identities, and Subscriptions, on page 11 for more information about the relationship between Azure subscription types and Cloud APIC tenants.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 In the left navigation menu, click **Tenants**.

Step 3 In the main pane, click **Add Tenant**.

Step 4 In the **Add Tenant** window, provide a name for the tenant.

You may also choose to provide a description of the tenant.

Step 5 If the tenant needs to be deployed to an on-premises site, in the **Associated Sites** area, select the on-premises site by checking the check box next to it.

(Optional) You can also choose a security domain from the drop-down list for the site.

Step 6 To add an Azure cloud site to the tenant, in the **Associated Sites** area, select the Azure cloud site by checking the check box next to it.

When associating an Azure cloud site with a tenant, you must also provide the Azure subscription information.

Step 7 After you check an Azure site, select the security domain from the drop-down list, if available, then click **Associate Account** next to it.

Step 8 Select the mode for the Azure account.

- Choose **Mode: Create Own** if you want to associate the tenant with a new Azure subscription, then enter information in the following fields:

  a. In the **Azure Subscription ID** field, provide the ID of the Azure subscription.

  You can obtain the subscription ID by logging into your Azure account and navigating to **Home** > **Subscriptions**. You must use the **Subscription ID** and not **Subscription Name** as listed in the Azure portal.

  b. (Optional) In the **Security Domain** field, select the security domains under the cloud account if you want to share this cloud account with other security domains.

  For more information, see Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 71.

  c. In the **Access Type** field, choose the access type between the Cloud APIC VM and the tenant.

Note For releases prior to release 5.2(1), only managed identity was supported as the access type for infra tenants, while both managed identity and unmanaged identity/service principal was supported as the access type for user tenants. Unmanaged identity/service principal was not supported as the access type for infra tenants for releases prior to release 5.2(1).

Beginning with release 5.2(1), both managed identity and unmanaged identity/service principal is now supported as an access type for the infra tenants and the user tenants.

- Select **Unmanaged Identity** to manage the cloud resources through a specific application.

  This can be used when you want to configure tenants in different subscriptions. The subscriptions are either in different Azure directories (Azure tenants) in the same organization, or the subscriptions can be in different organizations.

  In this case, you must also provide the application's credentials to the Cloud APIC. Refer to the information that you saved at the end of the procedures in Creating an Application in Azure, on page 27:

  - **Application ID:** Enter the application ID for the Azure application. This ID is listed in **Home** > **App registrations** > **<application-name>**, in the **Application (client) ID** field.
  - **Client Secret:** Enter the application secret. You can create a secret under **Home** > **App registrations** > **<application-name>** > **Certificates & secrets** > **New client secret**.
  - **Azure Active Directory ID:** Enter the application directory ID for the Azure application. This ID is listed in **Home** > **App registrations** > **<application-name>**, in the **Directory (tenant) ID** field.

  Note You will also have to add a role assignment for the app in this case. See Adding a Role Assignment for an App, on page 41 for those procedures.

- Select **Managed Identity** to allow the Cloud APIC VM to manage the cloud resources.

  This can be used when the Azure subscriptions are in the same directory (of the same organization).

  Note You will also have to add a role assignment for the VM in this case. See Adding a Role Assignment for a Virtual Machine, on page 39 for those procedures.

- Choose **Mode: Select Shared** if you want to use an existing subscription that is shared with an existing tenant.

  Azure allows you to create multiple tenants using the same subscription.

  If you choose **Select Shared**, you can then select a cloud account from the drop-down list. The cloud accounts available in the drop-down list are based on the security domain that you selected in Step 7, on page 72. Your new tenant will be associated with the same Azure subscription as the selected account.

  Note If you configured a security domain, then the cloud account that you select must have been shared with the same security domain that you selected for the tenant. All tenants sharing the same Azure subscription must be in the same security domain.

Step 9 If necessary, in the **Associated Users** area, select which users have access to the tenant.

Step 10 (Optional) Enable consistency checker.

You may choose to enable scheduled consistency checker for this tenant. Additional information about consistency check is available in the *Multi-Site Configuration Guide*.

Step 11 Click **Save** to add the tenant.

What to do next

Go to Creating a Schema, on page 74 to create a schema.

Creating a Schema

There are several general Multi-Site procedures that are not specific to the Cisco Cloud APIC, but that must be performed as part of the overall Cisco Cloud APIC setup if you are managing an on-premises site and a Cisco Cloud APIC site through Multi-Site. The following topics provide these general Multi-Site procedures that are part of the overall Cisco Cloud APIC setup.

Follow the instructions in this section if you want to create a new schema for the Cisco Cloud APIC site.

If you already have a schema that you want to use for the Cisco Cloud APIC site, you can skip these steps and go straight to Adding Sites to the Schema, on page 76.

Step 1 In the Main menu, click **Schemas**.

Step 2 On the Schema page, click the **Add Schema** button.

Step 3 On the Untitled Schema page, replace the text `Untitled Schema` at the top of the page with a name for the schema that you intend to create (for example, `Cloudbursting-Schema`).

Step 4 In the left pane, click **Template 1**.

Step 5 In the middle pane, click the area **To build your schema please click here to select a tenant**.

Step 6 In the right pane, access the **Select A Tenant** dialog box and select the tenant that you created in Configuring a Tenant, on page 72 from the drop-down menu.

Configuring an Application Profile and the EPGs

This procedure describes how to configure an application profile and add two EPGs, one for cloud site and one for the on-premises site, where the provider contract is associated with one EPG and the consumer contract is associated with the other EPG.

Step 1 In the middle pane, locate the Application Profile area, then click **+ Application Profile**.

Step 2 In the right pane, enter the Application Profile name in the **DISPLAY NAME** field.

Step 3 In the middle pane, click **+ Add EPG** to create an EPG for the cloud site.

Step 4 In the right pane, enter an EPG name in the **DISPLAY NAME** field (for example, `epg1`).

Step 5 In the middle pane, click **+ Add EPG** again, if you want to create an EPG for the on-premises site.

Step 6 In the right pane, enter an EPG name in the **DISPLAY NAME** field (for example, `epg2`).

Step 7 Create a VRF:

a) In the middle pane, scroll down until you see the VRF area, then click the **+** in the dotted box.

b) In the right pane, enter the VRF name in the **DISPLAY NAME** field (for example, `vrf1`).

Step 8 Click **SAVE**.

Creating and Associating a Bridge Domain with a VRF

Follow the procedures in this section to create a bridge domain for the on-premises site and associate it with the VRF. Note that these procedures are not necessary for a cloud-only schema.

Step 1 In the middle pane, scroll back up to **EPG** and click on the EPG that you created earlier for the on-premises site.

Step 2 In the right pane, in the **ON-PREM PROPERTIES** area, under **BRIDGE DOMAIN**, create a new bridge domain by typing a name in the field (for example, `bd1`), then click the **Create** area.

Step 3 In the middle pane, click the bridge domain that you just created.

Step 4 In the **Virtual Routing & Forwarding** field, select the VRF that you created in Configuring an Application Profile and the EPGs, on page 74.

Step 5 Scroll down to the **SUBNETS** area and click on the **+** next to **SUBNET** under the **GATEWAY** heading.

Step 6 On the **Add Subnet** dialog, enter the **Gateway IP** address and a description for the subnet you plan to add. The Gateway IP address is the on-premises subnet.

Step 7 In the **Scope** field, select **Advertised Externally**.

Step 8 Click **SAVE**.

Creating a Filter for a Contract

Step 1 In the middle pane, scroll down until you see the Filter area, then click **+** in the dotted box.

Step 2 In the right pane, enter a name for the filter in the **DISPLAY NAME** field.

Step 3 Click **+ Entry** to provide information for your schema filter on the **Add Entry** display:

a) Enter a name for the schema filter entry in the **Name** field on the **Add Entry** dialog.

b) Optional. Enter a description for the filter in the **Description** field.

c) Enter the details as appropriate to filter EPG communication.

For example, to add an entry allowing HTTPS traffic through a filter, choose:

TYPE: IP, IP PROTOCOL: TCP, and DESTINATION PORT RANGE FROM and DESTINATION PORT RANGE TO: https.

d) Click **SAVE**.

Creating a Contract

Step 1 In the middle pane, scroll down until you see the Contract area, then click + in the dotted box.

Step 2 In the right pane, enter a name for the contract in the **DISPLAY NAME** field.

Step 3 In the **SCOPE** area, leave the selection at VRF.

Step 4 In the **FILTER CHAIN** area, click **+ FILTER**.

The Add Filter Chain screen appears.

Step 5 In the **NAME** field, select the filter that you created in Creating a Filter for a Contract, on page 75.

Step 6 In the middle pane, scroll back up to **EPG** and click on the EPG that you created for the cloud site.

Step 7 In the right pane, click **+ CONTRACT**.

The Add Contract screen appears.

Step 8 In the **CONTRACT** field, select the contract that you created earlier in this procedure.

Step 9 In the **TYPE** field, select either **CONSUMER** or **PROVIDER**.

Step 10 Scroll to the **CLOUD PROPERTIES** area, then, in the **VIRTUAL ROUTING & FORWARDING** area, choose the VRF that you created in Configuring an Application Profile and the EPGs, on page 74.

Step 11 Click **SAVE**.

Step 12 In the middle pane, scroll back up to **EPG** and click on the EPG that you created for the on-premises site.

Step 13 In the right pane, click **+ CONTRACT**.

The Add Contract screen appears.

Step 14 In the **CONTRACT** field, select the same contract that you created earlier in this procedure.

Step 15 In the **TYPE** field, select either **CONSUMER** or **PROVIDER**, whatever you did not select for the previous EPG.

For example, if you selected **PROVIDER** for the first EPG, select **CONSUMER** for the second EPG.

Step 16 Scroll to the **CLOUD PROPERTIES** area, then, in the **VIRTUAL ROUTING & FORWARDING** area, choose the same VRF that you created in Configuring an Application Profile and the EPGs, on page 74.

Adding Sites to the Schema

Step 1 In the left pane, click the + next to **Sites**.

Step 2 On the **Add Sites** page, add the on-premises and cloud sites to the schema by checking the box next to each, then click **Save**.

Step 3 Click on the template underneath the cloud site in the left pane to configure the site local properties for the template.

Step 4 In the middle pane, click on the VRF.

Step 5 In the right pane, in the **SITE LOCAL PROPERITES** area, enter the following information:

a) In the **REGIONS** field, select the Azure region that this VRF will be deployed on.

b) In the **CIDRS** field, click **+CIDR**.

The **ADD CLOUD CIDR** dialog appears. Enter the following information:

- **CIDR** — Enter the VNET CIDR information. For example, `11.11.0.0/16`.

  The CIDR includes the scope of all subnets that are going to be available to an Azure VNET.

  Note The VNET CIDR information that you enter in this field cannot overlap with the infra pool. Verify that the CIDR information that you enter in this field does not overlap with the infra pool information that you entered in the **Infra Subnet** field in Step 6, on page 34 in Deploying the Cloud APIC in Azure, on page 33.

- **CIDR TYPE** — Select Primary or Secondary. If this is your first CIDR, select Primary for the CIDR type.
- **ADD SUBNETS** — Enter the subnet information, then click the check mark. For example, `11.11.1.0/24`.

  For the Cisco Cloud APIC, the subnet should be a valid subnet with subnet mask, and not an IP address with a subnet mask. For example, `11.11.0.0/24` is a valid subnet and subnet mask, whereas `11.11.0.1` is an IP address and subnet mask, but is not a valid subnet to use with the Cisco Cloud APIC.

  Note You must add one subnet specifically for the VGW. Select **Used by VGW** for this particular subnet.

c) Click **SAVE** in the window.

Adding an Endpoint Selector

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 Azure VNET 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.

You can configure the endpoint selector either through the Cisco Cloud APIC GUI or through the Cisco Nexus Dashboard Orchestrator GUI. There are slight differences in the options available between the two GUIs, but the general concept and overall procedures to add endpoint selectors is essentially the same between the two.

The procedures in this section describe how to set up the endpoint selectors using the Cisco Nexus Dashboard Orchestrator GUI. For information on setting up the endpoint selectors using the Cisco Cloud APIC GUI, see the *Cisco Cloud APIC User Guide, Release 4.2(x)*.

Step 1 Gather the necessary information from the Azure site that you could use for your Cisco Cloud APIC endpoint selector.

Note These steps assume that you are configuring the instance in Azure first, then adding an endpoint selector for Cisco Cloud APIC afterward; however, you can also add an endpoint selector in Cisco Cloud APIC first, then perform this Azure instance configuration step afterward, at the end of these endpoint selector procedures.

Step 2 Log into the Cisco Nexus Dashboard Orchestrator, if you aren't already logged in.

Step 3 In the left pane, click **Schemas**, then select the schema that you created earlier.

Step 4 Determine how you want to create the endpoint selector.

- If you want to create an endpoint selector that could be applied to any additional cloud site in the future, follow these procedures:

  a. In the left pane, leave the template selected.

  Do not select a specific site for these procedures.

  b. In the middle pane, select the EPG that you created for the cloud site.

  c. In the right pane, in the **CLOUD PROPERITES** area, click **+** next to **SELECTORS** to configure the endpoint selector.

  d. In the **Add New End Point Selector** dialog, enter a name in the **END POINT SELECTOR NAME** field, based on the classification that you use for this endpoint selector.

  e. Click **+ Expression**, then select the type of endpoint selector.

  For an endpoint selector created this way, the only option available under the Key field is `EPG`.

  f. Go to Step 5, on page 79.

- If you want to create an endpoint selector specifically for this cloud site, follow these procedures:

  a. In the left pane, select the cloud site.

  b. In the middle pane, select the EPG that you created for the cloud site.

  c. In the right pane, in the **SITE LOCAL PROPERITES** area, under the **SELECTORS** area, click **+** next to **SELECTOR** to configure the endpoint selector.

  d. In the **Add New End Point Selector** dialog, enter a name in the **END POINT SELECTOR NAME** field, based on the classification that you use for this endpoint selector.

  For example, for an endpoint selector with the IP Subnet classification, you might use a name such as `IP-Subnet-EPSelector`.

  e. Click **+ Expression**, then select the key that you want to use for the endpoint selector.

  - **IP Address**: Used to select by the IP address or subnet. The value for an IP address as an endpoint selector should fall under the user subnet created under the CIDR in Adding Sites to the Schema, on page 76.

    In addition, specifically for Azure scale set VMs, the value for an IP address as an endpoint selector must be a complete subnet that was configured in Adding Sites to the Schema, on page 76 where that scale set resides. It cannot be an IP address within the subnet.

    For example, if you used the following values in these fields for Azure scale set VMs:

    - **CIDR**: `10.1.0.0/16`
    - **Subnet**: `10.1.0.0/24`

    Then a valid value for an IP address as an endpoint selector would be `10.1.0.0/24`. Entries of `10.1.0.1/32` or `10.1.0.0/16` would not be valid values for an IP address as an endpoint for Azure scale set VMs.

    Note IPv6 is not supported for Cisco Cloud APIC in Azure. You must use a valid IPv4 address for this field.

- **Region**: Used to select by the Azure region of the endpoint.
- If you want to create a custom tag for the endpoint selector, start typing in the **Type to search or create field** to enter the custom tag or label, then click **Create** on the new field to create a new custom tab or label.

  Using the example earlier in these procedures when you were adding a tag in Azure, you might create the custom tag `Location` in this field, to match the Location tag that you added in Azure earlier.

Step 5 In the **Operator** field, choose the operator that you want to use for the endpoint selector.

The options are:

- **Equals**: Used when you have a single value in the Value field.
- **Not Equals**: Used when you have a single value in the Value field.
- **In**: Used when you have multiple comma-separated values in the Value field.
- **Not In**: Used when you have multiple comma-separated values in the Value field.
- **Has Key**: Used if the expression contains only a key.
- **Does Not Have Key**: Used if the expression contains only a key.

Step 6 In the **Value** field, choose which value that you want to use for the endpoint selector, based on the choices that you made for the two previous fields. You can have multiple comma-separated entries in the **Value** field, where a logical OR exists between the entries in this field.

Note The Value field is not displayed if **Has Key** or **Key Not Exist** is selected for the Operator field.

For example, if you want to have a specific Azure region for the endpoint selector, such as `westus`, you might make the following selections in this screen:

- **Key:** Region
- **Operator:** Equals
- **Value:** westus

As another example, assume that you used the following values in these fields:

- **Key:** IP
- **Operator:** Has Key
- **Value:** Not available because Has Key was used in the Operator field.

The EPG rules will be applied to all endpoints with an IP address in this situation.

As a final example, assume that you used the following values in these fields:

- **Key:** custom tag: Location
- **Operator:** Has Key
- **Value:** Not available because Has Key was used in the Operator field.

In this situation, the EPG rules will be applied to all endpoints with the Azure tag key Location, regardless of the location value.

Step 7 Click the checkmark when you have finished creating this endpoint selector expression.

Step 8 Determine if you want to create additional endpoint selector expressions.

If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions. For example, assume you created two sets of expressions under a single endpoint selector:

- Endpoint selector 1, expression 1:
  - **Key:** Region
  - **Operator:** Equals
  - **Value:** eastus
- Endpoint selector 1, expression 2:
  - **Key:** IP
  - **Operator:** Equals
  - **Value:** 192.0.2.1/24

In this case, if *both* of these expressions are true (if the region is eastus AND if the IP address belongs to subnet 192.0.2.1/24), then that endpoint will be assigned to the Cloud EPG.

Click the checkmark after every additional expression that you want to create under this endpoint selector.

Step 9 When you have finished creating the expressions for this endpoint selector, click **SAVE** in the lower right corner of the **Add New End Point Selector**.

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:

- Endpoint selector 2, expression 1:
  - **Key:** Region
  - **Operator:** In
  - **Value:** centralus, eastus2

In this case:

- If the region is eastus AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions)

  OR
- If the region is either centralus or eastus2 (endpoint selector 2 expression)

Then that end point is assigned to the Cloud EPG.

Step 10 When you have finished creating the endpoint selectors, click **SAVE** in the upper right corner.

Step 11 Click on the **DEPLOY TO SITES** button at the top right corner of the screen to deploy the schema to the sites.

You should see a message saying `Successfully Deployed` at this point.

What to do next

Verify that the Multi-Site areas were configured correctly using the instructions in Verifying the Multi-Site Configurations, on page 81 .

Verifying the Multi-Site Configurations

Use the procedures in this topic to verify that the configurations that you entered in the Cisco Nexus Dashboard Orchestrator are applied correctly.

Step 1 Log into the Cloud APIC and verify the following:

a) Click on Dashboard and use the information in the Inter-Site Connectivity Status and the Inter-Region Connectivity Status boxes to verify the following:

- That the tunnels are up from the CCR on Azure to the ISN (IPsec termination point) on-premises and to the VGWs in the user VNETs.
- That the OSPF neighbors are coming up between the CCR and the ISN on-premises devices.
- That the BGP EVPN routes for the VRF show the cloud and on-premises routes, and that the cloud routes are populated through the BGP EVPN in the ACI spine switch.

b) Click on Application Management → Tenants and verify that the tenants were configured correctly.

c) Click on Application Management → Application Profiles and verify that the application profiles were configured correctly.

d) Click on Application Management → EPGs and verify that the EPGs were configured correctly.

e) Click on Application Management → Contracts and verify that the contracts were configured correctly.

f) Click on Application Management → VRFs and verify that the VRFs were configured correctly.

g) Click on Application Management → Cloud Context Profiles and verify that the cloud context profiles were configured correctly.

h) Click on Cloud Resources → Regions and verify that the regions were configured correctly.

i) Click on Cloud Resources → VNETs and verify that the VNETs were configured correctly.

j) Click on Cloud Resources → Cloud Endpoints and verify that the cloud endpoints were configured correctly.

k) Click on Cloud Resources → Routers and verify that the CCRs were configured correctly.

Step 2 Log into on-premises APIC site and verify the schema in APIC.

You should see the shared tenant that you configured in the Cisco Nexus Dashboard Orchestrator is displayed in the tenants area in APIC and the VRF and EPG deployed from the Cisco Nexus Dashboard Orchestrator schema is configured in the on-premises APIC.

Step 3 From a command line, verify that the VRFs were created properly on the CCR on Azure:

```
show vrf
```

If the tenant `t1` and the VRF `v1` is deployed from the Cisco Nexus Dashboard Orchestrator, the CCR output will be similar to the following:

```
Name                              Default RD             Protocols   Interfaces
t1:v1                             64514:3080192          ipv4        BD1
                                                                     Tu4
                                                                     Tu5
```

Step 4 From a command line, verify that the tunnels are up between the CCR on Azure and the ISN on-premises devices.

You can run the following command on either the CCR on Azure or on the ISN on-premises devices.

`show ip interface brief | inc Tunnel`

Output similar to the following should appear:

```
Interface         IP-Address        OK?        Method        Status        Protocol
Tunnel1           1.2.3.22          YES        manual        up            up
Tunnel2           1.2.3.30          YES        manual        up            up
Tunnel3           1.2.3.6           YES        manual        up            up
Tunnel4           1.2.3.14          YES        manual        up            up
```

Step 5 From a command line, verify that the OSPF neighbors are up between the CCR on Azure and the ISN on-premises devices:

`show ip ospf neighbor`

Output similar to the following should appear:

```
Neighbor ID       Pri               State      Dead Time     Address       Interface
10.200.10.201     0                 FULL/ -    00:00:36      1.2.3.13      Tunnel4
20.30.40.50       0                 FULL/ -    00:00:36      1.2.3.29      Tunnel2
10.202.101.202    0                 FULL/ -    00:00:38      1.2.3.5       Tunnel3
```

Step 6 From a command line, verify that the on-premises BGP EVPN neighbors are present in the CCR:

`show bgp l2vpn evpn summary`

Output similar to the following should appear:

```
Neighbor     V     AS    MsgRcvd    MsgSent    TblVer    InQ    OutQ    Up/Down    State/PfxRcd
10.1.1.2     4     100   139        137        99        0      0       01:30:36   6
```

Step 7 From a command line, verify that the BGP routes for the VRF show both the cloud and on-premises routes.

Note In the current Cloud APIC workflow, a VRF will not be configured on the CCR until the corresponding VNET is created in Azure.

`show ip route vrf t1:v1`

Output similar to the following should appear:

```
B      129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B      130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```

CHAPTER 7

Understanding the Cisco Cloud APIC GUI

Navigating the Cisco Cloud APIC GUI

After you install Cisco Cloud APIC, you can use it for extending Cisco Application Centric Infrastructure (ACI) policy to the Amazon Web Services (AWS) or Microsoft Azure public cloud. You do so through the Cisco Cloud APIC GUI.

In the Cisco Cloud APIC GUI, you can create a tenant, configure application profiles, endpoint groups (EPGs), contracts, filters, and VRFs. You can also view Cisco Cloud APIC topology, configurations, and resources.

You perform configuration steps with the. **Intent** feature. For instructions on using the **Intent** feature, see the section Configuring Cisco Cloud APIC Components, on page 83. Also see the section "Understanding the Cisco Cloud APIC GUI Icons" in the *Cisco Cloud APIC User Guide*.

The steps for performing basic tasks in Cisco Cloud APIC differ from the steps in regular Cisco APIC. However, the functions of the tenant, application profile, and other elements of Cisco APIC are the same. For more information, see the *Cisco Application Centric Infrastructure Fundamentals Guide* on Cisco.com.

You view configurations and other information with the left navigation pane. You can choose **Dashboard** (the default view), **Topology**, **Application Management**, **Cloud Resources**, **Operations**, **Infrastructure**, and **Administrative**.

For information abut the icons, see the section "Understanding the Cisco Cloud APIC GUI Icons" in the *Cisco Cisco Cloud APIC User Guide* on Cisco.com.

Creating a Tenant Using the Cisco Cloud APIC GUI

The following sections describe how to create a tenant using the Cisco Cloud APIC GUI.

Configuring Cisco Cloud APIC Components

This section provides an overview of performing key tasks in Cisco Cloud APIC, including creating a tenant, application profile, and endpoint group (EPG).

Before you begin

You must have installed Cisco Cloud APIC. See the previous installation sections in this guide.

Step 1 Log into Cisco Cloud APIC.

Step 2 At the upper right of the **Dashboard** pane, click the icon with an arrow pointing to a bull's-eye.

This icon might be referred to as the **Intent** icon or feature.

Step 3 In the **What do you want to do?** window, type a term in the search window to bring up a list of options.

For example, if you want to configure a tenant, type the word tenant in the search window. The search returns a list of tasks that are related to creating and configuring tenants.

Step 4 Click a task and perform the configuration steps in the windows that open.

What to do next

You can view the configuration in the left navigation pane. Expand the pane by clicking the hamburger icon at the upper left of the **Dashboard** pane. Expand the appropriate heading to view the configurations.

For example, if you've configured a tenant, expand **Application Management** and click **Tenants**. Information about tenants appears in the central work pane.

CHAPTER 8

Performing a System Upgrade, Downgrade or Recovery

Important Notes

Important Notes For Release 25.0(3)

Following are important notes for release 25.0(3) regarding the installation, upgrade or downgrade procedures for the Cisco Cloud APIC:

- The Cisco Catalyst 8000V supports subscription-based licensing. Before upgrading from a release prior to 25.0(3) to release 25.0(3), you must first subscribe to one of the tier-based Cisco Catalyst 8000V licenses.

  - For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see Cisco Catalyst 8000V Edge Software.

  - For more information on different throughputs based on the tiers, see Requirements for the Azure Public Cloud, on page 18.

  Cisco Cloud APIC makes use of the "Cisco DNA Advantage" subscription. For features supported by the "Cisco DNA Advantage" subscription, see Cisco DNA SoftwareSD-WAN and Routing Matrices.

- When you upgrade your Cisco Cloud APIC to release 25.0(3), you should then upgrade the CCRs as soon after the Cisco Cloud APIC upgrade as possible. For those instructions, see:

  - Upgrading the Software, on page 88

  - Triggering an Upgrade of the CCRs, on page 111

Following are examples of how you would go through these upgrade processes:

- **Single-Site Upgrade**: You normally would have CCRs for a single-site Azure deployment. Once the Cisco Cloud APIC has completed the upgrade to release 25.0(3) and reached the ready state, you must then start the upgrade of the older CCRs (the Cisco Cloud Services Router 1000v) to the newer CCRs (the Cisco Catalyst 8000V) before making any configuration changes.

- **Multi-Cloud/Hybrid-Cloud Upgrade**: As an example of this upgrade process, assume that you have the following setup:

  - Site 1: AWS

  - Site 2: Azure

  - Site 3: On-premises site

  You would then upgrade these sites the following way:

  1. Upgrade Nexus Dashboard Orchestrator to the 3.7(1) release.

  2. Upgrade site 1 (AWS site) to the Cisco Cloud APIC release 25.0(3) using the procedures in Upgrading the Software, on page 88.

     Wait until this upgrade has reached the steady state before proceeding to the next step.

  3. Upgrade the CCRs on site 1 (AWS site) from the older CCRs (the Cisco Cloud Services Router 1000v) to the newer CCRs (the Cisco Catalyst 8000V) using the procedures in Triggering an Upgrade of the CCRs, on page 111.

     Wait until the CCRs are fully upgraded to the newer Cisco Catalyst 8000Vs before proceeding to the next step.

  4. Once the CCRs on site 1 (AWS site) are fully upgraded, repeat these steps for site 2 (Azure site), where you will first upgrade the Cisco Cloud APIC software to release 25.0(3). After that upgrade has reached the steady state, then you will upgrade the CCRs on site 2 to the newer Cisco Catalyst 8000Vs.

- Prior to Cisco Cloud APIC release 25.0(3), the older Cisco Cloud Services Router 1000v routers were configured with number-based throughput, as described in Requirements for the Azure Public Cloud, on page 18. Since the Cisco Catalyst 8000V routers will only support tier-based throughput options, during upgrades to release 25.0(3), the Cisco Cloud APIC will map the throughput values from the number-based throughput used by the older Cisco Cloud Services Router 1000v routers to the tier-based throughput used by the newer Cisco Catalyst 8000V routers.

  The following table shows the mapping of throughput from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade:

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
10M	T0 (up to 15M throughput)
50M	T1 (up to 100M throughput)
100M	T1 (up to 100M throughput)
250M	T2 (up to 1G throughput)

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
500M	T2 (up to 1G throughput)
1G	T2 (up to 1G throughput)
2.5G	T3 (up to 10G throughput)
5G	T3 (up to 10G throughput)
7.5G	T3 (up to 10G throughput)
10G	T3 (up to 10G throughput)

When migrating from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade, the Cisco Cloud APIC will migrate the comparable bandwidth as described above. When these Cisco Catalyst 8000V routers come up, they will try to register for that bandwidth to the smart licensing account. If the smart licensing server does not have these licenses, then the Cisco Catalyst 8000V will fall back to the default bandwidth and will fail to service the existing workload traffic. So you must procure and provision the required Cisco Catalyst 8000V licenses in your smart account before migrating from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade.

- Similarly, when downgrading from release 25.0(3) to an earlier release, the Cisco Cloud APIC will map the throughput values from the tier-based throughput used by the newer Cisco Catalyst 8000V routers to the number-based throughput used by the older Cisco Cloud Services Router 1000v routers.

  The following table shows the mapping of throughput from the newer Cisco Catalyst 8000V routers to the number-based throughput used by the older Cisco Cloud Services Router 1000v routers during a downgrade:

Throughput on Cisco Catalyst 8000V	Throughput on Cisco Cloud Services Router 1000v
T0 (up to 15M throughput)	10M
T1 (up to 100M throughput)	100M
T2 (up to 1G throughput)	1G
T3 (up to 10G throughput)	10G

Note Do not make any configuration changes when the Cisco Cloud APIC and the CCRs are in incompatible mode. When upgrading to release 25.0(3), verify that both the Cisco Cloud APIC and the CCRs are upgraded to that latest release before making any configuration changes.

General Important Notes

Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths:

- Release 5.2(1) to 25.0(2), 25.0(3), or 25.0(4)

- Release 25.0(1) to 25.0(2), 25.0(3), or 25.0(4)
- Release 25.0(2) to 25.0(3) or 25.0(4)
- Release 25.0(3) to 25.0(4)

Upgrading the Software

The following sections provide information on upgrading the Cisco Cloud APIC software using either a migration-based upgrade or a policy-based upgrade. Before upgrading your Cisco Cloud APIC software, review the information provided in Guidelines and Limitations For Upgrading the Software, on page 89.

The method that you use to upgrade your Cisco Cloud APIC software varies, depending on the situation:

- If you are upgrading from a pre-5.0(x) release to release 5.1(2) or later, you will use a migration-based process to upgrade your software. Go to Migration-Based Upgrade, on page 89 for those instructions.

Note The same migration-based procedures used for an upgrade can also be used for a system recovery, as described in Performing a System Recovery, on page 111.

- If you are upgrading from release 5.0(x) or later to release 5.1(2) or later, you will use a policy-based process to upgrade your software.

  For example, Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths:

  - Release 5.2(1) to 25.0(2), 25.0(3), or 25.0(4)
  - Release 25.0(1) to 25.0(2), 25.0(3), or 25.0(4)
  - Release 25.0(2) to 25.0(3) or 25.0(4)
  - Release 25.0(3) to 25.0(4)

  Go to Policy-Based Upgrade, on page 101 for those procedures.

Note If the policy-based upgrade does not work for some reason, you can upgrade using the migration-based process as described in Migration-Based Upgrade, on page 89.

Upgrading the CCRs

Regardless of the method that you use to upgrade your Cisco Cloud APIC software, the Cloud Routers (CCRs) must also be upgraded whenever the Cloud APIC software is upgraded.

- Prior to release 5.2(1), the CCRs are upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC.

- Beginning with release 5.2(1), you can trigger upgrades to the CCRs and monitor those CCR upgrades, independent from the Cisco Cloud APIC upgrades. This is useful to reduce traffic loss by allowing you to split up the upgrades for the management plane (Cisco Cloud APIC) and the data plane (CCRs).

See Triggering an Upgrade of the CCRs, on page 111 for more information.

Guidelines and Limitations For Upgrading the Software

Following are the guidelines and limitations that you must be aware of before upgrading the Cisco Cloud APIC software:

Beginning with release 5.0(2), the configuration drift feature became available as described in the "Configuration Drifts" chapter in the Cisco Cloud APIC for Azure User Guide, Release 5.0(x) or later. After you upgrade your Cisco Cloud APIC, if you had configuration drifts enabled prior to the upgrade, you will see that the configuration drift feature is restarted after the upgrade is completed. When the feature is restarted, the previous configuration drift analysis is cleared (no configuration drifts are shown after the upgrade) and a fresh analysis is started for the configuration drift when the feature is restarted after the upgrade. This is expected behavior.

Migration-Based Upgrade

Follow these procedures to use a migration-based process to upgrade your software.

Review the information provided in Guidelines and Limitations For Upgrading the Software, on page 89 before performing the procedures in this section.

Note These migration-based procedures used for an upgrade can also be used for a system recovery, as described in Performing a System Recovery, on page 111.

Gathering Existing Cloud APIC Configuration Information

Before upgrading or downgrading your Cisco Cloud APIC software, follow the instructions in this topic to locate the existing configuration information for certain fields and make a note of the entries for each of these fields. You will use the same entries for these fields below, in a step later in the following procedures, when you use the recovery template to upgrade your Cisco Cloud APIC.

For each of the following fields, make a note of the entries that you entered as part of the original deployment that you performed in Deploying the Cloud APIC in Azure, on page 33:

- Subscription, on page 90
- Resource Group, on page 90
- Location, on page 90
- Fabric Name, on page 90
- External Subnets, on page 91
- Virtual Machine Name, on page 91
- Infra VNET Pool, on page 92

- Storage Account Name, on page 92

Subscription

1. Navigate to **Application Management** > **Tenants**.
2. Locate the row for the tenant that has **infra** underneath the name in the **Name** column.
3. Note the value in the **Azure Subscription** column.

   This is the **Subscription** entry for your Cisco Cloud APIC.

Resource Group

1. Navigate to **Cloud Resources** > **Virtual Machines**.

   The **Virtual Machines** window appears.
2. Locate and note the Cisco Cloud APIC VM in the VM list.

   The value for the VM is typically shown with the format <*vm_name*>(<*resource_group*>), where:

   - <*vm_name*> is the virtual machine name, as described in Virtual Machine Name, on page 91.
   - (<*resource_group*>) is the **Resource Group** entry for your Cisco Cloud APIC.

Location

1. Navigate to **Cloud Resources** > **Virtual Machines**.

   The **Virtual Machines** window appears.
2. Locate the Cisco Cloud APIC VM in the VM list.
3. Click the value for the Cisco Cloud APIC VM in the VM list.

   A nav panel with details about the Cisco Cloud APIC VM slides in from the right side of the screen.
4. In the **General** area, locate and note the value in the **Region** field.

   This is the **Location** entry for your Cisco Cloud APIC.

Fabric Name

1. SSH to your Cisco Cloud APIC through the CLI:

   ```
   # ssh admin@<cloud_apic_ip_address>
   ```

   Enter the password if prompted.
2. Enter the following in the CLI:

   ```
   ACI-Cloud-Fabric-1# acidiag avread
   ```
3. Locate the **FABRIC_DOMAIN** area in the output:

   ```
   Local appliance ID=1 ADDRESS=10.100.0.13 TEP ADDRESS=10.100.0.12/30 ROUTABLE IP
   ADDRESS=0.0.0.0
   CHASSIS_ID=afe36d66-042a-11eb-ab21-7b2dc494b182
   ```

```
Cluster of 1 lm(t):1(zeroTime) appliances (out of targeted 1
lm(t):1(2020-10-01T21:15:48.743+00:00))
with FABRIC_DOMAIN name=ACI-Cloud-Fabric set to version=5.0(2i)
lm(t):1(2020-10-01T21:15:48.746+00:00);
discoveryMode=PERMISSIVE lm(t):0(zeroTime); drrMode=OFF lm(t):0(zeroTime); kafkaMode=OFF
 lm(t):0(zeroTime)

appliance id=1 address=10.100.0.13 lm(t):1(2020-10-01T21:14:23.001+00:00) tep
address=10.100.0.12/30
lm(t):1(2020-10-01T21:14:23.001+00:00) routable address=0.0.0.0 lm(t):1(zeroTime)
oob address=10.100.0.29/28 lm(t):1(2020-10-01T21:14:26.723+00:00) version=5.0(2i)
lm(t):1(2020-10-01T21:14:26.841+00:00) chassisId=afe36d66-042a-11eb-ab21-7b2dc494b182
lm(t):1(2020-10-01T21:14:26.841+00:00) capabilities=0X7EEFFFFFFFFF--0X2020--0X1
lm(t):1(2020-10-01T21:20:27.483+00:00) rK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) aK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobrK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobaK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) cntrlSbst=(APPROVED, E8E6DDB1D800)
lm(t):1(2020-10-01T21:14:26.841+00:00) (targetMbSn= lm(t):0(zeroTime),
failoverStatus=0 lm(t):0(zeroTime)) podId=1 lm(t):1(2020-10-01T21:14:23.001+00:00)
commissioned=YES lm(t):1(zeroTime) registered=YES lm(t):1(2020-10-01T21:14:23.001+00:00)

standby=NO lm(t):1(2020-10-01T21:14:23.001+00:00) DRR=NO lm(t):0(zeroTime) apicX=NO
lm(t):1(2020-10-01T21:14:23.001+00:00) virtual=YES lm(t):1(2020-10-01T21:14:23.001+00:00)

active=YES(2020-10-01T21:14:23.001+00:00) health=(applnc:255
lm(t):1(2020-10-01T21:16:16.514+00:00) svc's)
---------------------------------------------
clusterTime=<diff=-1 common=2020-10-02T07:46:19.717+00:00
local=2020-10-02T07:46:19.718+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):1(2020-10-01T21:15:50.026+00:00)>>
---------------------------------------------
```

This is the **Fabric Name** entry for your Cisco Cloud APIC.

External Subnets

1. Navigate to **Application Management** > **EPGs**.
2. Locate the EPG with the name **ext-networks** and click that EPG.

   A nav panel slides in from the right side of the screen.

3. In the nav panel, click the **Details** icon (↗).

   The **Overview** page for this EPG appears.

4. In the **Endpoints** area, locate the row for **ext-Network1** and note the value in the **Subnet** column.

   This is the **External Subnets** entry for your Cisco Cloud APIC. Note that a value of `0.0.0.0/0` meant that anyone is allowed to connect to your Cisco Cloud APIC.

Virtual Machine Name

1. Navigate to **Cloud Resources** > **Virtual Machines**.

   The **Virtual Machines** window appears.

2. Locate and note the value for the Cisco Cloud APIC VM in the list.

The value for the VM is typically shown with the format <*vm_name*>(<*resource_group*>), where:

- <*vm_name*> is the **Virtual Machine Name** entry for your Cisco Cloud APIC.
- (<*resource_group*>) is the resource group, as described in Resource Group, on page 90.

Infra VNET Pool

For the infra VNET pool, you might have multiple infra subnet pools, so be sure to locate the information for the infra subnet that was used when you launched the original Cisco Cloud APIC through the ARM template as part of the procedures in Deploying the Cloud APIC in Azure, on page 33.

1. In your Cisco Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.
2. In the Region Management area, click **Edit Configuration**.

   The **Regions to Manage** window appears.
3. Click **Next**.

   The **General Connectivity** window appears.
4. In the **Subnet Pools for Cloud Routers** area underneath **General**, locate the row that has a **System Internal** value in the **Created By** column and note the value in the **Subnet** column.

   This is the **Infra VNET Pool** entry for your Cisco Cloud APIC.

Storage Account Name

Navigate to the **Storage accounts** page in Azure under the resource group where the Cisco Cloud APIC was deployed previously:

1. Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

   https://portal.azure.com/#home
2. Under **Services**, select **Storage accounts**.

   The **Storage accounts** page appears.
3. Locate and note the storage account name for your Cisco Cloud APIC resource group.

   This is the **Storage Account Name** entry for your Cisco Cloud APIC.

Backing Up Your Existing Configuration

We recommend that you back up your existing configuration before performing a migration-based upgrade, in case you decide to roll back to the previous release for any reason afterwards.

Before you begin

Complete the procedures in Gathering Existing Cloud APIC Configuration Information, on page 89 before proceeding with these procedures.

Step 1 Enable Global AES encryption before performing the backup.

a) In your Cisco Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

   You should see the **General** tab selected by default; if not, click the **General** tab.

b) Click the pencil icon at the upper right part of the **Global AES Encryption** area.

   The **Global AES Encryption Settings** window appears.

c) Click the box next to the **Encryption: Enabled** area, enter a passphrase in the **Passphrase/Confirm Passphrase** fields, then click **Save** at the bottom of the window.

   Make a note of the passphrase that you entered in this step, as you will need it if you need as part of the backup restoration process.

Step 2 Back up your existing configuration.

a) Navigate to **Operations** > **Backup & Restore**.
b) Click the **Backup Policies** tab.
c) Click **Actions** > **Create Backup Configuration**.
d) Back up your existing configuration.

   For more information on the options available in the **Create Backup Configuration**, see the "Creating a Backup Configuration Using the Cisco Cloud APIC GUI" procedure in the *Cisco Cloud APIC for Azure User Guide*.

Step 3 Delete the Cisco Cloud APIC VM.

a) In the Microsoft Azure portal, navigate to **Services** > **Virtual Machines**.
b) Locate the Cisco Cloud APIC VM in the **Virtual Machines** window and click on the Cloud APIC VM.

   The **Overview** page for the Cisco Cloud APIC VM appears.

c) Click **Delete**, then click **Yes** when asked for confirmation of this action.

   You can view the deletion process in the Notifications area.

Downloading and Deploying the Recovery Template

Before you begin

Complete the procedures in Backing Up Your Existing Configuration, on page 92 before proceeding with these procedures.

Step 1 Download the appropriate recovery template for your release for Cisco Cloud APIC.

Contact Cisco TAC to get the appropriate recovery template:

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Step 2 Deploy the recovery template in the Azure portal.

a) In the Azure portal, go to the **All Services** page:

   https://portal.azure.com/#allservices

b) In the **General** area, click **Templates**.
c) In the **Templates** page, click Add.

The **Add Template** page appears.

d) Enter the necessary information in the **Add Template** page.

- **Name**: Enter a unique name that will identify this template as a release-specific recovery template (for example, for the release 25.0(1) recovery template, you might use `template-2501-recovery` as the release-specific unique name).
- **Description**: Enter descriptive text for this template, if necessary.

e) Click **OK**.

The **ARM Template** page appears.

f) In the **ARM Template** page, delete the default text that is automatically added in the template.
g) Navigate to the area where you downloaded the recovery template in Step 1, on page 93.
h) Using a text editor, open the recovery template and copy the contents in the template.
i) In the Azure portal window, paste the contents into the **ARM Template** page.
j) Click **OK**.

The **Add Template** page appears again.

k) Click **Add**.

The new recovery template is added to the **Templates** page. If you do not see the new recovery template in the **Templates** page, click **Refresh** to refresh the page.

Step 3 Use the recovery template to deploy the Cisco Cloud APIC VM in the same resource group.

a) In the Templates page, click the new recovery template that you just added.
b) Click **Deploy**.

The **Custom Deployment** page appears.

c) Enter the necessary information in the recovery template.

- **Basics**:
  - **Subscription**: Choose the same subscription that you used when you first deployed your Cisco Cloud APIC, as described in Subscription, on page 90.
  - **Resource Group**: You must choose the same resource group that you used when you first deployed your Cisco Cloud APIC, as described in Resource Group, on page 90.
  - **Location**: Select the same region that you used when you first deployed your Cisco Cloud APIC, as described in Location, on page 90.

    Note The **Location** option might not be available when you are using the same resource group.
- **Settings**:
  - **Vm Name**: Enter the same VM name that was used previously, as described in Virtual Machine Name, on page 91.
  - **Vm Size**: Select the size for the VM.
  - **Image Sku**: Select the appropriate image SKU. For example, for release 25.0(1), select `25_0_1_byol`.

- **Admin Username**: Leave the default entry for this field as-is. The admin username login will work once the Cisco Cloud APIC is up.
- **Admin Password or Key**: Enter an admin password.
- **Admin Public Key**: Enter the admin public key (the ssh key).
- **Fabric Name**: Enter the same fabric name that was used previously, as described in Fabric Name, on page 90.
- **Infra VNET Pool**: Enter the same infra subnet pool that was used previously, as described in Infra VNET Pool, on page 92.
- **External Subnets**: Enter the IP addresses and subnets of the external networks that were used previously to allow access to the Cisco Cloud APIC, as described in External Subnets, on page 91. This would be the same external subnet pool for Cisco Cloud APIC access that you entered as part of the original deployment that you performed in Deploying the Cloud APIC in Azure, on page 33.
- **Storage Account Name**: Enter the same storage account name that was used previously, as described in Storage Account Name, on page 92.
- **Virtual Network Name**: Verify that the virtual network name in this field matches the virtual network name that was originally used to deploy the Cisco Cloud APIC.
- **Mgmt Nsg Name**: Verify that the management network security group name in this field matches the management network security group name that was originally used to deploy the Cisco Cloud APIC.
- **Mgmt Asg Name**: Verify that the management application security group name in this field matches the management application security group name that was originally used to deploy the Cisco Cloud APIC.
- **Subnet Prefix**: The entry for this field will be the subnet prefix that needs to be used for the automatically-configured infra subnet.

  Verify that the subnet prefix in this field matches the subnet prefix that was originally used to deploy the Cisco Cloud APIC. You can check that prefix by looking at the format of the subnet names on the Cisco Cloud APIC Virtual Network. For example, if subnet names shown there are **subnet-10.10.0.0_28**, then the subnet prefix for this field should be **subnet-**.erify that the subnet prefix in this field matches the subnet prefix that was originally used to deploy the Cisco Cloud APIC. You can check that prefix by looking at the format of the subnet names on the Cisco Cloud APIC Virtual Network. For example, if subnet names shown there are **subnet-10.10.0.0_28**, then the subnet prefix for this field should be **subnet-**.

d) Click the box next to the agreement statement, then click **Purchase**.

The **Azure services** window appears, with a small popup window saying **Deployment in progress**. Click the Notifications icon to continue to monitor the progress of the deployment. The deployment usually takes roughly five or so minutes to complete.

After a period of time, you will see the **Deployment succeeded** window.

What to do next

Follow the procedures in Performing Post-Upgrade Procedures, on page 96.

Performing Post-Upgrade Procedures

Before you begin

Complete the procedures in Downloading and Deploying the Recovery Template, on page 93 before proceeding with these procedures.

Step 1 Give the contributor role to the Cisco Cloud APIC VM on the infra subscription.

a) In the Microsoft Azure portal, under **Services**, select **Subscription**.
b) Select the subscription where Cisco Cloud APIC was deployed.
c) Select **Access Control (IAM)**.
d) On the top menu, click **Add** > **Add role assignment**.
e) In the **Role** field, select **Contributor**.
f) In the **Assign access to** field, select **Virtual Machine**.
g) In the **Subscription** field, select the subscription where the Cisco Cloud APIC was deployed.
h) In **Select**, click on the Cisco Cloud APIC Virtual Machine.
i) Click **Save**.

Note Also give the contributor role to the Cisco Cloud APIC VM if you have managed user tenants. You must do this on user subscriptions that are used to deploy the user tenants. See Understanding Tenants, Identities, and Subscriptions, on page 11 and Adding a Role Assignment for a Virtual Machine, on page 39 for more information.

Step 2 Enable the same encryption passphrase.

a) In the Microsoft Azure portal, under **Services**, select **Virtual machines**.
b) In the **Virtual machines** window, click the Cisco Cloud APIC.

   The **Overview** page for the Cisco Cloud APIC appears.

c) Locate the **Public IP address** field and copy the IP address.
d) In another browser window, enter the IP address and hit Return:

   ```
   https://<IP_address>
   ```

   The **Welcome to Cloud APIC** screen appears after logging in for the first time.

e) Click **Begin First Time Setup**.

   The **Let's Configure the Basics** window appears. Click the **X** in the upper right corner to exit out of this window to proceed with procedures to enable the same encryption passphrase.

f) In your Cisco Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

   It should be underneath the **General** tab by default; if not, click the **General** tab.

   After first login, welcome screen appears. Click begin first time setup.first time setup page opens, close the first time setup pagethen user can proceed to setting the pass phrase.

g) In the **Global AES Encryption** area, click the pencil icon at the upper right part of the **Global AES Encryption** area.

   The **Global AES Encryption Settings** window appears.

h) Click the box next to the **Encryption: Enabled** area, enter the same passphrase in the **Passphrase/Confirm Passphrase** fields that you used in Backing Up Your Existing Configuration, on page 92, then click **Save** at the bottom of the window.

Step 3 If you are performing a migration-based upgrade to release 25.0(1), run the Python script to clean up the necessary configuration before importing the configuration that you backed up earlier.

Contact Cisco TAC to get the Python script to address the issue raised in CSCvy42684 to clean up the necessary configuration:

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Step 4 Import the configuration that you backed up in Backing Up Your Existing Configuration, on page 92.

If you configured a remote location when you backed up your configuration, you might have to create the remote location again to access the backup.

a) In your Cisco Cloud APIC GUI, navigate to **Operations** > **Backup & Restore**.
b) In the **Backup & Restore** window, click the **Backups** tab.
c) Click the **Actions** scrolldown menu, then choose **Restore Configuration**.

The **Restore Configuration** window appears.

d) Enter the necessary information to restore the configuration that you backed up in Backing Up Your Existing Configuration, on page 92.

Use the following settings:

- In the **Restore Type** field, choose **Merge**.
- In the **Restore Mode** field, choose **Best Effort**.

Click **Restore Configuration** when you have entered the necessary information in this window.

e) Wait until the restore process is complete before proceeding to the next step.

Click the **Job Status** tab in the **Backup & Restore** window to get the status of the restore process and verify that the restore process was successful.

Step 5 Review the naming policy.

a) In your Cisco Cloud APIC GUI, click the Intent icon ( ) and choose **Cloud APIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Verify that the selections that you had prior to the migration were transferred over successfully with the backup import, then click **Next**.

Note Do not modify the managed region or CCR configuration at this point.

d) Navigate to the last page in the setup and review the information in the **Cloud Resource Naming Rules** area.

Verify that the cloud resource naming rules match the cloud resource naming rules that were originally used to deploy the Cisco Cloud APIC.

Click the box next to **Deploy cloud resources based on these naming rules**, then click **Save and Continue** after reviewing the information in this screen. Resources will not be deployed to the cloud until the naming rules have been reviewed and accepted.

At this point in the process, the non-home region CCRs will be deployed automatically with the new CCR image.

Note Allow for some time to pass for the Cisco Cloud APIC to clear all of the faults before proceeding to the next step. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 6 Wait for the non-home region CCRs to come up on the cloud, and ensure that all of the VGW tunnels are up with the newly-created CCRs and the configuration reconciliation is complete.

In addition, you may see that the home region CCR is deleted and recreated at this point in the process if a CCR upgrade is required. Ignore these actions and any faults that might appear as a result, as they will clear up when you complete the following steps in this procedure.

Wait until the home region CCRs are upgraded to the latest CCR version in this case.

Step 7 (Optional) If you have intersite connectivity and you want to avoid a complete intersite traffic drop, reconfigure the non-home region intersite tunnels and bring up the tunnels through the Cisco Nexus Dashboard Orchestrator before bringing down the home region CCRs in the next step.

This step is not necessary if you do not have intersite connectivity or if you have intersite connectivity but you're not concerned with traffic loss.

a) In the Cisco Nexus Dashboard Orchestrator, in the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

b) In the left pane, under **SITES**, click on the cloud site.
c) Click **Reload Site Data**.
d) Verify that the new CCRs are added in the UI.
e) Click the **Deploy** button at the top right of the screen, then choose the **Deploy & Download IPN Device config files** option.

This action pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect connectivity between the on-premises and the cloud site. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the CCR deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

Note If you delete and recreate intersite tunnels on the cloud CCRs from the Cisco Cloud APIC in this step, and you need to program the new keys on the on-premises IPsec termination device, where you are going to change the key for the same public IP address of the cloud CCRs, you must first manually delete the existing keys on the on-premises IPsec termination device and add a new key. There should be only one matching IPsec pre-shared key for a given cloud CCR destination IP address on the on-premises IPsec termination device.

Step 8 Undeploy the home region CCRs.

a) In your Cisco Cloud APIC GUI, click the Intent icon (⊛) and choose **cAPIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate the home region (the region that has the text **Cloud APIC Deployed**) and unselect the boxes in the **Cloud Routers** column for the home region.
d) Click **Save**.

This removes the old CCRs for the home region.

e) Wait for home region CCR VMs, CCR NICs, and CCR public IP addresses to get deleted on the cloud.

Once the home region CCR VMs, CCR NICs, and CCR public IP addresses are deleted on the cloud, you can redeploy the CCRs back in the home region.

Step 9 Redeploy the home region CCRs.

The previously-configured home region CCRs are deleted and the new home region CCRs are re-created in this step.

a) Click **Previous** to return to the **Regions to Manage** screen, then click the boxes in the **Cloud Routers** column for the home region to re-enable the CCRs for the home region.
b) Click **Save**.

Step 10 (Optional) Complete the procedures in this step if intersite connectivity is required.

- If intersite connectivity is not required, then you do not have to complete the procedures in this step. Skip to Migrating to VNet Peering (Optional), on page 99 in that case.

- If intersite connectivity is required, then complete the following procedures:

a) Once the new home region CCRs come up, in the Cisco Nexus Dashboard Orchestrator, in the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

b) In the left pane, under **SITES**, click on the cloud site.
c) Click **Reload Site Data**.
d) Verify that the new CCRs are added in the UI.
e) Click the **Deploy** button at the top right of the screen, then choose the **Deploy & Download IPN Device config files** option.
f) Reconfigure the IPN IPsec tunnels on the on-premises CCR with the downloaded IPN configuration.

See Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices, on page 67.

Note If you delete and recreate intersite tunnels on the cloud CCRs from the Cisco Cloud APIC for any reason, and you need to program the new keys on the on-premises IPsec termination device, where you are going to change the key for the same public IP address of the cloud CCRs, you must first manually delete the existing keys on the on-premises IPsec termination device and add a new key. There should be only one matching IPsec pre-shared key for a given cloud CCR destination IP address on the on-premises IPsec termination device.

What to do next

If you want to migrate to Azure VNet peering for inter-VNet connectivity, follow the procedures in Migrating to VNet Peering (Optional), on page 99.

Migrating to VNet Peering (Optional)

Follow the procedures in this task if you want to migrate to Azure VNet peering for inter-VNet connectivity rather than using the traditionial tunnel-based VPN connectivity through the CCRs. For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document.

Note Migrating to VNet peering mode is a disruptive operation. Be aware that there will be traffic loss during the process.

Before you begin

Complete the procedures in Performing Post-Upgrade Procedures, on page 96 before proceeding with these procedures.

Step 1 In your Cisco Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.

Step 2 In the **Region Management** area, click **Edit Configuration**.

The **Regions to Manage** window appears.

Step 3 Locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.

Step 4 Click **Virtual Network Peering** to enable the Azure VNet peering feature.

This enables VNet peering at the Cisco Cloud APIC level, deploying NLBs in all the regions with CCRs in the infra VNet.

After you have enabled VNet peering at the Cisco Cloud APIC level, on each user cloud context profile, you will have to enable the **VNet Peering** option and disable the **VNet Gateway Router** option.

Note The following steps describe now to enable VNet peering on each cloud context profile through the Cisco Cloud APIC GUI. You can also perform the following steps through the Cisco Nexus Dashboard Orchestrator, if you want.

Step 5 In the left navigation bar, navigate to **Application Management** > **Cloud Context Profiles**.

The existing cloud context profiles are displayed.

Step 6 Click Actions and choose **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

Step 7 Locate the **VNet Gateway Router** field and click to uncheck (disable) the **VNet Gateway Router** check box.

Step 8 Locate the **VNet Peering** field and click to check (enable) the **VNet Peering** check box.

Step 9 Click **Save** when finished.

Step 10 Configure the Network Contributor role for both the infra and user tenant subscriptions.

For example, assume the following:

- The infra tenant is using subscription **S1** with access credentials/service principal **C1**
- The user tenant is using subscription **S2** with access credentials/service principal **C2**

In this situation, you will have to configure the following for peering to work between the user tenant and the infra VNets:

- You will have to give C1 Network Contributor role permissions to S2 for the hub to spoke peering link
- You will have to give C2 Network Contributor role permissions to S1 for the spoke to hub peering link

a) In the yellow window that appears, copy the **az** command provided.

- If you have configure the Network Contributor role for the user tenant, copy the text in the area **Command to run for User Subscription**.

- If you have configure the Network Contributor role for the infra tenant, copy the text in the area **Command to run for Infra Subscription**.

b) Return to the Azure management portal and click **Registrations** in the left navigation bar.
c) Open the Cloud Shell.
d) Select **Bash**.
e) Paste the **az** command that you copied in 10.a, on page 101.

Policy-Based Upgrade

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software.

Review the information provided in Guidelines and Limitations For Upgrading the Software, on page 89 before performing the procedures in this section.

Downloading an Image

Step 1 Log in to your Cisco Cloud APIC, if you aren't logged in already.

Step 2 From the **Navigation** menu, choose **Operations** > **Firmware Management**.

The **Firmware Management** window appears.

Step 3 Click the **Images** tab in the **Firmware Management** window.

Step 4 Click **Actions**, then choose **Add Firmware Image** from the scroll-down menu.

The **Add Firmware Image** pop-up appears.

Step 5 Determine if you want to add the firmware image from a local or a remote location.

- If you want to add the firmware image from a *local* location, click the **Local** radio button in the **Image Location** field. Click the **Choose File** button, then navigate to the folder on your local system with the firmware image that you want to import and select the file. Go to Step 6, on page 102.

- If you want to import the firmware image from a *remote* location, click the **Remote** radio button in the **Image Location** field, then perform the following actions:

a) In the **Protocol** field, click either the **HTTP** or the **SCP** radio button.
b) In the **URL** field, enter the URL from where the image will be downloaded.

- If you selected the **HTTP** radio button in the previous step, enter the http source that you want to use to download the software image. An example URL is `10.67.82.87:/home/<username>/ACI/aci-capic-dk9.25.0.2f.iso`. Go to Step 6, on page 102.

- If you selected the **SCP** radio button in the previous step, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image, using the format `<SCP server>:/<path>`. An example URL is `10.67.82.87:/home/<username>/ACI/aci-capic-dk9.25.0.2f.iso`.

c) In the **Username** field, enter your username for secure copy.

d) In the **Authentication Type** field, select the type of authentication for the download. The type can be:

- **Password**
- **SSH Key**

The default is **Password**.

e) If you selected **Password**, in the **Password** field, enter your password for secure copy. Go to Step 6, on page 102.

f) If you selected **SSH Key**, enter the following information:

- **SSH Key Content** — The SSH Key Content is used to create the SSH Key File which is required when creating a Remote location for the download.

  Note The public key is generated at the time of the transfer. After the transfer the key files that were generated in the background are deleted. The temporary key files are stored in dataexport directory of the Cisco Cloud APIC.

- **SSH Key Passphrase** — The SSH Key Passphrase is used to create the SSH Key File which is required when creating a Remote location for the download.

  Note The Passphrase field can remain empty.

Step 6 Click **Select**.
Wait for the Cisco Cloud APIC firmware images to download.

Upgrading the Software Using the Policy-Based Upgrade Process

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software.

Before you begin

- You have downloaded an image using the procedures provided in Downloading an Image, on page 101.

Step 1 Subscribe to the correct image for the CCR.

- For releases prior to release 25.0(3), to subscribe to the image for the **Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL)**:

a) In the Azure Marketplace search text field, type *Cisco Cloud Services Router (CSR) 1000V* and select the option that appears.

The **Cisco Cloud Services Router (CSR) 1000V** option appears as a search suggestion.

b) Click the **Cisco Cloud Services Router (CSR) 1000V** option.

You should be redirected to the **Cisco Cloud Services Router (CSR) 1000V** page in the Microsoft Azure Marketplace.

c) Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

d) In the **Select a software plan** drop-down menu, select the **Cisco CSR 1000V Bring Your Own License - XE 17.3.1a** option.
e) Locate the **Want to deploy programmability?** field and click **Get Started**.
f) In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.
g) Click **Save**.

- For release 25.0(3) or later, to subscribe to the image for the **Cisco Catalyst 8000V Edge Software - Bring Your Own License (BYOL)**:

a) In the Azure Marketplace search text field, type *Cisco Catalyst 8000V Edge Software* and select the option that appears.

The **Cisco Catalyst 8000V Edge Software** option appears as a search suggestion.

b) Click the **Cisco Catalyst 8000V Edge Software** option.

You should be redirected to the **Cisco Catalyst 8000V Edge Software** page in the Microsoft Azure Marketplace.

c) Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

d) In the **Select a software plan** drop-down menu, select the **Cisco Catalyst 8000V Edge Software-BYOL-17.7.1** option.
e) Locate the **Want to deploy programmability?** field and click **Get Started**.
f) In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.
g) Click **Save**.

Step 2 If you are upgrading from **release 5.0(1)**, remove the CCRs from all regions *except the home region*.

Note If you are upgrading from **release 5.0(2)** or later, do not remove any CCRs. Go to Step 3, on page 104 in this case.

Do not remove the CCR from the home region at this point. Removing the CCR for the home region at this point will cause an outage.

a) In your Cloud APIC GUI, click the Intent icon (⊛) and choose **cAPIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.

You will be unselecting the boxes in the **Cloud Routers** column in the next step, so make sure you know which regions will need to selected again at the end of this procedure.

d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).

e) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

The process of removing the CCRs might take roughly a half hour. You can monitor the process of the CCR removal by looking at the virtual machines for the resource group in the Azure portal.

Do not proceed to the next step until the necessary CCRs have been completely removed.

Step 3 From the **Navigation** menu, choose the **Operations** > **Firmware Management**.

The **Firmware Management** window appears.

Step 4 Click **Schedule Upgrade**.

The **Schedule Upgrade** pop-up appears.

If you see a message that says that faults are present in your fabric, we recommend that you resolve these faults before performing a upgrade. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 5 In the **Target Firmware** field, choose a firmware image from the scroll-down menu.

Step 6 In the **Upgrade Start Time** field, determine if you want to begin the upgrade now or later.

- Click **Now** if you want to schedule the upgrade for now. Go to Step 7, on page 104.
- Click **Later** if you want to schedule the upgrade for a later date or time, then select the date and time from the pop-up calendar for the scheduled upgrade.

Step 7 In the **Ignore Compatibility Check** field, leave the setting in the default off (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

In Cloud APIC, there is a compatibility check feature that verifies if an upgrade path from the currently-running version of the system to a specific newer version is supported or not. The **Ignore Compatibility Check** setting is set to off by default, so the system automatically checks the compatibility for possible upgrades by default.

Note If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Ignore Compatibility Check** field, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

Step 8 Click **Schedule Upgrade**.

You can monitor the progress of the upgrade in the main **Firmware Management** window, under the **Upgrade Status** area.

Step 9 If you are upgrading from **release 5.0(1)**, when the upgrade is completed, add the necessary CCRs back again.

Note This step is necessary only if you are upgrading from **release 5.0(1)**. If you are upgrading from **release 5.0(2)**, you do not have to perform any more steps in this section.

Verify that the home region CCR is stabilized before adding the CCRs in the other regions back again.

a) In your Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.

b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate all of the regions that had CCRs and check the boxes in the **Cloud Routers** column for each of those regions to add the CCRs back again.

d) Click Next, then enter the necessary information in the following page and click **Save and Continue**.

Step 10 Verify that all of the CCRs (home region CCR and non-home region CCRs) have come up with release 17.7.1.

Do not power off your Cisco Cloud APIC VM until all of the CCRs have come up with release 17.7.1.

Step 11 If you are upgrading from release 5.0(1) to release 5.1(2) or later, determine if you want to migrate to Azure VNet peering for inter-VNet connectivity rather than using the traditional tunnel-based VPN connectivity through the CCRs.

For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document.

Note Migrating to VNet peering mode is a disruptive operation. Be aware that there will be traffic loss during the process.

Follow these instructions to enable the VNet peering feature:

a) In your Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.

b) In the **Region Management** area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.

- If the **Virtual Network Peering** is available, then the home region CCR has already been successfully migrated from the basic SKU to the standard SKU. Go to 11.i, on page 105 in this case.
- If the **Virtual Network Peering** is not available, that means that the home region CCR is still set to the basic SKU rather than the updated standard SKU. Continue to 11.d, on page 105 to migrate the home region CCR to the standard SKU.

d) Locate the home region (the region that has the text **Cloud APIC Deployed**) and unselect the box in the **Cloud Routers** column for the home region.

e) Click **Save**.

This action removes the CCR with the basic SKU for the home region.

f) Click **Previous** to return to the **Regions to Manage** screen, then click the box in the **Cloud Routers** column for the home region to re-enable the CCR for the home region.

g) Click **Save**.

This action adds the CCR with the standard SKU for the home region.

h) Click **Previous** to return to the **Regions to Manage** screen, then locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.

i) Click **Virtual Network Peering** to enable the Azure VNet peering feature.

This enables VNet peering at the Cloud APIC level, deploying NLBs in all the regions with CCRs in the infra VNet.

Note The **VPN Connectivity via CCR** option is used to enable the traditional VPN connectivity through the overlay IPsec tunnels between CCRs and Azure VPN Gateway routers, instead of using VNet peering.

After you have enabled VNet peering at the Cloud APIC level, on each user cloud context profile, you will have to enable the **VNet Peering** option and disable the **VNet Gateway Router** option.

j) In the left navigation bar, navigate to **Application Management** > **Cloud Context Profiles**.

The existing cloud context profiles are displayed.

k) Click Actions and choose **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

l) Locate the **VNet Gateway Router** field and click to uncheck (disable) the **VNet Gateway Router** check box.
m) Locate the **VNet Peering** field and click to check (enable) the **VNet Peering** check box.
n) Click **Save** when finished.

Downgrading the Software

The following sections provide the necessary information that you will need to successfully downgrade your Cisco Cloud APIC software.

Prerequisites for Downgrading the Software

Following are prerequisites that you must follow before downgrading the Cisco Cloud APIC software:

- If your Cisco Cloud APIC is part of a Cisco Multi-Site ACI fabric, where it is orchestrated with Cisco Multi-Site, you must first downgrade the Cisco Cloud APIC software to an equivalent or earlier release before you can downgrade the Cisco Nexus Dashboard Orchestrator software. In other words, the release of the Cisco Nexus Dashboard Orchestrator software should always be equal to or later than the release of the Cisco Cloud APIC software.

  - To determine the release date for the Cisco Nexus Dashboard Orchestrator software, go to Multi-Site Software in the Software Download site, then select the appropriate release in the left nav bar to see the release date for that release

  - To determine the release date for the Cisco Cloud APIC software, go to Cloud Application Policy Infrastructure Controller in the Software Download site, then select the appropriate release in the left nav bar to see the release date for that release

  For example, if you are downgrading to Cisco Cloud APIC Release 5.0(2i):

  1. Determine the release date for Cisco Cloud APIC Release 5.0(2i) using the information in Cloud Application Policy Infrastructure Controller in the Software Download site (in this case, 25-Sep-2020), then go to Multi-Site Software in the Software Download site to find the equivalent or later release of the Cisco Nexus Dashboard Orchestrator software (in this case, Multi-Site Release 3.0(2k), which was released on 02-Oct-2020).

  2. First downgrade the Cisco Cloud APIC software to the Cloud APIC Release 5.0(2i) using the instructions in this document.

  3. After you have downgraded the Cisco Cloud APIC software, then downgrade the Cisco Nexus Dashboard Orchestrator software to the Multi-Site Release 3.0(2k). See Multi-Site Orchestrator Installation and Upgrade Guide, Release 3.1(x) for those instructions.

Downgrading the Software

These procedures describe how to downgrade the software.

These procedures assume the following scenario:

1. At some point previously, you were running one version of the software, such as release 5.2(1), and you decided to upgrade to a later release, such as release 25.0(2). Before you performed that upgrade, however, you backed up your existing configuration and saved that backed-up configuration file, as described in Backing Up Your Existing Configuration, on page 92.
2. You then performed the software upgrade and, at some pointer later on, decided to revert back to that previous release again.

These procedures describe how to revert back to that previous release, but you will need that backed-up configuration file for that previous release in order for these downgrade procedures to work.

Step 1 Verify that you have the backed-up configuration file for the previous release, as described in Backing Up Your Existing Configuration, on page 92.

Do not use these procedures to downgrade your software if you do not have that backed-up configuration file from the previous release available. You will need that backup configuration file for these downgrade procedures.

Step 2 Download the recovery template for Cisco Cloud APIC.

Contact Cisco TAC to get the recovery template:

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Step 3 Deploy the recovery template in the Azure portal.

a) In the Azure portal, go to the **All Services** page:

   https://portal.azure.com/#allservices

b) In the **General** area, click **Templates**.

c) In the **Templates** page, click Add.

   The **Add Template** page appears.

d) Enter the necessary information in the **Add Template** page.

   - **Name**: Enter a unique name that will identify this template as the recovery template (for example, `template-521-recovery`).
   - **Description**: Enter descriptive text for this template, if necessary.

e) Click **OK**.

   The **ARM Template** page appears.

f) In the **ARM Template** page, delete the default text that is automatically added in the template.

g) Navigate to the area where you downloaded the recovery template in Step 2, on page 107.

h) Using a text editor, open the recovery template and copy the contents in the template.

i) In the Azure portal window, paste the contents into the **ARM Template** page.

j) Click **OK**.

The **Add Template** page appears again.

k) Click **Add**.

The new recovery template is added to the **Templates** page. If you do not see the new recovery template in the **Templates** page, click **Refresh** to refresh the page.

Step 4 Use the recovery template to deploy the Cisco Cloud APIC VM in the same resource group.

a) In the **Templates** page, click the new recovery template that you just added.

b) Click **Deploy**.

The **Custom Deployment** page appears.

c) Enter the necessary information in the recovery template.

- **Basics**:
  - **Subscription**: Choose the same subscription that you used when you first deployed your Cisco Cloud APIC, as described in Subscription, on page 90.
  - **Resource Group**: You must choose the same resource group that you used when you first deployed your Cisco Cloud APIC, as described in Resource Group, on page 90.
  - **Location**: Select the same region that you used when you first deployed your Cisco Cloud APIC, as described in Location, on page 90.

    Note The **Location** option might not be available when you are using the same resource group.
- **Settings**:
  - **Vm Name**: Enter the same VM name that was used previously, as described in Virtual Machine Name, on page 91.
  - **Vm Size**: Select the size for the VM.
  - **Image Sku**: Select the appropriate image SKU (for example, `5_2_1_byol`).
  - **Admin Username**: Leave the default entry for this field as-is. The admin username login will work once the Cisco Cloud APIC is up.
  - **Admin Password or Key**: Enter an admin password.
  - **Admin Public Key**: Enter the admin public key (the ssh key).
  - **Fabric Name**: Enter the same fabric name that was used previously, as described in Fabric Name, on page 90.
  - **Infra VNET Pool**: Enter the same infra subnet pool that was used previously, as described in Infra VNET Pool, on page 92.
  - **External Subnets**: Enter the IP addresses and subnets of the external networks that were used previously to allow access to the Cisco Cloud APIC, as described in External Subnets, on page 91. This would be the same external subnet pool for Cisco Cloud APIC access that you entered as part of the original deployment that you performed in Deploying the Cloud APIC in Azure, on page 33.
  - **Storage Account Name**: Enter the same storage account name that was used previously, as described in Storage Account Name, on page 92.

- **Virtual Network Name**: Verify that the virtual network name in this field matches the virtual network name that was originally used to deploy the Cisco Cloud APIC.
- **Mgmt Nsg Name**: Verify that the management network security group name in this field matches the management network security group name that was originally used to deploy the Cisco Cloud APIC.
- **Mgmt Asg Name**: Verify that the management application security group name in this field matches the management application security group name that was originally used to deploy the Cisco Cloud APIC.
- **Subnet Prefix**: The entry for this field will be the subnet prefix that needs to be used for the automatically-configured infra subnet.

  Verify that the subnet prefix in this field matches the subnet prefix that was originally used to deploy the Cisco Cloud APIC. You can check that prefix by looking at the format of the subnet names on the Cisco Cloud APIC Virtual Network. For example, if subnet names shown there are **subnet-10.10.0.0_28**, then the subnet prefix for this field should be **subnet-**.Verify that the subnet prefix in this field matches the subnet prefix that was originally used to deploy the Cisco Cloud APIC. You can check that prefix by looking at the format of the subnet names on the Cisco Cloud APIC Virtual Network. For example, if subnet names shown there are **subnet-10.10.0.0_28**, then the subnet prefix for this field should be **subnet-**.

d) Click the box next to the agreement statement, then click **Purchase**.

The **Azure services** window appears, with a small popup window saying **Deployment in progress**. Click the Notifications icon to continue to monitor the progress of the deployment. The deployment usually takes roughly five or so minutes to complete.

After a period of time, you will see the **Deployment succeeded** window.

What to do next

Follow the procedures in Performing Post-Downgrade Procedures, on page 109.

Performing Post-Downgrade Procedures

Before you begin

Complete the procedures in Downgrading the Software, on page 107 before proceeding with these procedures.

Step 1 Give the contributor role to the Cisco Cloud APIC VM on the infra subscription.

a) In the Microsoft Azure portal, under **Services**, select **Subscription**.
b) Select the subscription where Cisco Cloud APIC was deployed.
c) Select **Access Control (IAM)**.
d) On the top menu, click **Add** > **Add role assignment**.
e) In the **Role** field, select **Contributor**.
f) In the **Assign access to** field, select **Virtual Machine**.
g) In the **Subscription** field, select the subscription where the Cisco Cloud APIC was deployed.
h) In **Select**, click on the Cisco Cloud APIC Virtual Machine.
i) Click **Save**.

Note Also give the contributor role to the Cisco Cloud APIC VM if you have managed user tenants. You must do this on user subscriptions that are used to deploy the user tenants. See Understanding Tenants, Identities, and Subscriptions, on page 11 and Adding a Role Assignment for a Virtual Machine, on page 39 for more information.

Step 2 If you are downgrading from release 25.0(3) to an earlier release, trigger a CCR downgrade to the older Cisco Cloud Services Router 1000v.

As part of the upgrade to 25.0(3), you also moved from the older Cisco Cloud Services Router 1000v to the newer Cisco Catalyst 8000V. Downgrading from 25.0(3) to an earlier release therefore requires downgrading the CCR back to the older Cisco Cloud Services Router 1000v.

When the downgrade is completed, the system will recognize that the CCRs are now incompatible with the Cisco Cloud APIC. You will see a message saying that the CCRs and the Cisco Cloud APIC are incompatible and that any new policies configured for the Cisco Cloud APIC will not be applied to the CCRs until you've downgraded the CCRs.

You can begin the process of triggering the CCR downgrade using either of the following methods. Note that while the menu option is shown as **Upgrade CCRs** in both methods, you are actually downgrading the CCRs in this situation by selecting this option.

- In the banner at the top of the screen when your first log into the Cisco Cloud APIC, click on the **Upgrade CCRs** link, or
- Through the **CCRs** area in the **Firmware Management** page by navigating to:

  Operations > **Firmware Management**

  Click the **CCRs** tab, then choose **Upgrade CCRs**.

Step 3 Enable the same encryption passphrase.

a) In the Microsoft Azure portal, under **Services**, select **Virtual machines**.
b) In the **Virtual machines** window, click the Cisco Cloud APIC.

   The **Overview** page for the Cisco Cloud APIC appears.

c) Locate the **Public IP address** field and copy the IP address.
d) In another browser window, enter the IP address and hit Return:

```
https://<IP_address>
```

   The **Welcome to Cloud APIC** screen appears after logging in for the first time.

e) Click **Begin First Time Setup**.

   The **Let's Configure the Basics** window appears. Click the **X** in the upper right corner to exit out of this window to proceed with procedures to enable the same encryption passphrase.

f) In your Cisco Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

   It should be underneath the **General** tab by default; if not, click the **General** tab.

   After first login, welcome screen appears. Click begin first time setup.first time setup page opens, close the first time setup pagethen user can proceed to setting the pass phrase.

g) In the **Global AES Encryption** area, click the pencil icon at the upper right part of the **Global AES Encryption** area.

   The **Global AES Encryption Settings** window appears.

h) Click the box next to the **Encryption: Enabled** area, enter the same passphrase in the **Passphrase/Confirm Passphrase** fields that you used in Backing Up Your Existing Configuration, on page 92, then click **Save** at the bottom of the window.

Step 4 Import the configuration that you backed up in Backing Up Your Existing Configuration, on page 92.

If you configured a remote location when you backed up your configuration, you might have to create the remote location again to access the backup.

a) In your Cisco Cloud APIC GUI, navigate to **Operations** > **Backup & Restore**.
b) In the **Backup & Restore** window, click the **Backups** tab.
c) Click the **Actions** scrolldown menu, then choose **Restore Configuration**.

The **Restore Configuration** window appears.

d) Enter the necessary information to restore the configuration that you backed up in Backing Up Your Existing Configuration, on page 92.

Use the following settings:

- In the **Restore Type** field, choose **Merge**.
- In the **Restore Mode** field, choose **Best Effort**.

Click **Restore Configuration** when you have entered the necessary information in this window.

e) Wait until the restore process is complete before proceeding to the next step.

Click the **Job Status** tab in the **Backup & Restore** window to get the status of the restore process and verify that the restore process was successful.

Performing a System Recovery

The procedures for performing a system recovery is identical to the procedures for performing a migration-based upgrade. Refer to the section Migration-Based Upgrade, on page 89 for those procedures.

Triggering an Upgrade of the CCRs

The following topics provide information and procedures for triggering an upgrade of the CCRs.

Triggering an Upgrade of the CCRs

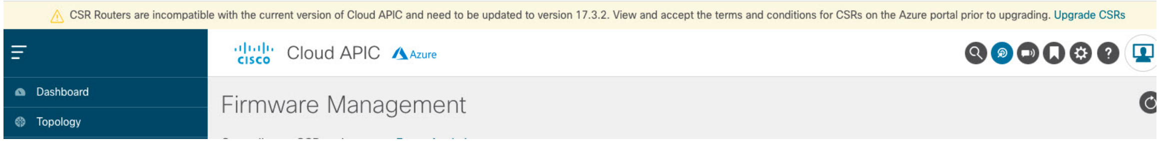
Prior to Release 5.2(1), the CCRs are upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC. Beginning with Release 5.2(1), you can trigger upgrades to the CCRs and monitor those CCR upgrades, independent from the Cisco Cloud APIC upgrades. This is useful to reduce traffic loss by allowing you to split up the upgrades for the management plane (Cisco Cloud APIC) and the data plane (CCRs).

Beginning with Release 5.2(1), this feature is enabled by default, where the default assumption is that you will be triggering the upgrades to the CCRs after you trigger an upgrade to the Cisco Cloud APIC. You cannot disable this feature once it's enabled.

When this feature is enabled, the proper upgrade sequence for the Cisco Cloud APIC and the CCRs is as follows.

Note Following are upper-level steps to describe the overall process for triggering upgrades to the CCRs. For specific step-by-step instructions, see Triggering an Upgrade of the CCRs Using the Cisco Cloud APIC GUI, on page 113.

1. Upgrade Cisco Cloud APIC using the instructions provided in this chapter.
2. Wait for the Cisco Cloud APIC upgrade process to complete. When that upgrade is completed, the system will recognize that the CCRs are now incompatible with the Cisco Cloud APIC. You will then see a message saying that the CCRs and the Cisco Cloud APIC are incompatible and that any new policies configured for the Cisco Cloud APIC will not be applied to the CCRs until you've upgraded the CCRs.



⚠ CSR Routers are incompatible with the current version of Cloud APIC and need to be updated to version 17.3.2. View and accept the terms and conditions for CSRs on the Azure portal prior to upgrading. Upgrade CSRs

3. View and accept the terms and conditions for the CCRs on the Azure portal.
4. Trigger the CCR upgrade so that it is now at a compatible version as the Cisco Cloud APIC.

   You can begin the process of triggering the CCR upgrade using either of these two methods:

   - In the banner at the top of the screen, click on the **Upgrade CCRs** link, or
   - Through the **CCRs** area in the **Firmware Management** page. Navigate to:

     Operations > **Firmware Management**

     Click the **CCRs** tab, then choose **Upgrade CCRs**.

You can also trigger the CCR upgrade through the REST API. See Triggering an Upgrade of the CCRs Using the REST API, on page 114 for those instructions.

Guidelines and Limitations

- After you have upgraded the Cisco Cloud APIC, if you do not see the message saying that the CCRs and the Cisco Cloud APIC are incompatible, you might have to refresh the browser for that message to appear.
- Trigger an upgrade to the CCRs *after* you have upgraded the Cisco Cloud APIC. Do not trigger an upgrade to the CCRs before you have upgraded the Cisco Cloud APIC.
- Once you have triggered an upgrade to the CCRs, it cannot be stopped.
- If you see any errors after you trigger an upgrade to the CCRs, check and resolve those errors. The CCR upgrade will continue automatically once those CCR upgrade errors have been resolved.

Triggering an Upgrade of the CCRs Using the Cisco Cloud APIC GUI

This section describes how to trigger an upgrade to the CCRs using the Cisco Cloud APIC GUI. For more information, see Triggering an Upgrade of the CCRs, on page 111.

Step 1 If the CCR software version is incompatible with the Cisco Cloud APIC software version, first view and accept the terms and conditions for the CCRs on the Azure portal.

- For releases prior to release 25.0(3), for the **Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL)**:

a) In the Azure Marketplace search text field, type *Cisco Cloud Services Router (CSR) 1000V* and select the option that appears.

The **Cisco Cloud Services Router (CSR) 1000V** option appears as a search suggestion.

b) Click the **Cisco Cloud Services Router (CSR) 1000V** option.

You should be redirected to the **Cisco Cloud Services Router (CSR) 1000V** page in the Microsoft Azure Marketplace.

c) Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

d) In the **Select a software plan** drop-down menu, select the **Cisco CSR 1000V Bring Your Own License - XE 17.3.1a** option.

e) Locate the **Want to deploy programmability?** field and click **Get Started**.

f) In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.

g) Click **Save**.

- For release 25.0(3) or later, for the **Cisco Catalyst 8000V Edge Software - Bring Your Own License (BYOL)**:

a) In the Azure Marketplace search text field, type *Cisco Catalyst 8000V Edge Software* and select the option that appears.

The **Cisco Catalyst 8000V Edge Software** option appears as a search suggestion.

b) Click the **Cisco Catalyst 8000V Edge Software** option.

You should be redirected to the **Cisco Catalyst 8000V Edge Software** page in the Microsoft Azure Marketplace.

c) Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

d) In the **Select a software plan** drop-down menu, select the **Cisco Catalyst 8000V Edge Software-BYOL-17.7.1** option.

e) Locate the **Want to deploy programmability?** field and click **Get Started**.

f) In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.

g) Click **Save**.

Step 2 Begin the process of triggering the CCR upgrade to a compatible CCR version.

You can begin the process of triggering the CCR upgrade using either of these two methods:

- In the banner at the top of the screen, click on the **Upgrade CCRs** link, or
- Through the **CCRs** area in the **Firmware Management** page. Navigate to:

  Operations > **Firmware Management**

  Click the **CCRs** tab, then choose **Upgrade CCRs**.

A warning appears after clicking **Upgrade CCRs**, stating that upgrading the CCRs will cause the CCRs to reboot, which may cause temporary disruption in traffic.

Step 3 If this is a good time to upgrade the CCRs and have a temporary disruption in traffic, click **Confirm Upgrade** in the warning message.

The CCR software upgrade begins. A banner appears at the top of the screen, saying that the CCR upgrade is in process. Click **View CCR upgrade status** in the message to view the status of the CCR upgrade.

Step 4 Fix any faults that might occur during the upgrade of the CCRs.

If a fault occurs during the upgrade, you can get more information on the fault by navigating to:

Operations > **Event Analytics** > **Faults**

Triggering an Upgrade of the CCRs Using the REST API

This section describes how to trigger an upgrade to the CCRs using the REST API. For more information, see Triggering an Upgrade of the CCRs, on page 111.

Set the value for the `routerUpgrade` field to `"true"` in the cloud template to trigger an upgrade to the CCRs through the REST API (`routerUpgrade="true"`).

```
<polUni>
<fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
       <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName" routerPassword="SomePass"
 routerUpgrade="true">
        </cloudtemplateProfile>
        <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
        <cloudtemplateIntNetwork name="default">
            <cloudRegionName provider="azure" region="westus"/>
            <cloudRegionName provider="azure" region="westus2"/>
        </cloudtemplateIntNetwork>
        <cloudtemplateExtNetwork name="default">
            <cloudRegionName provider="aws" region="us-west-2"/>
            <cloudtemplateVpnNetwork name="default">
                <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />
                <cloudtemplateOspf area="0.0.0.1"/>
            </cloudtemplateVpnNetwork>
           <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
 />
        </cloudtemplateExtNetwork>
    </cloudtemplateInfraNetwork>
```

```
</fvTenant>
</polUni>
```

APPENDIX A

Logging Into Cloud APIC Through SSH

Normally, you will log into your Cloud APIC through a browser, as described in Configuring Cisco Cloud APIC Using the Setup Wizard, on page 53. If you need to log into your Cloud APIC through SSH for any reason, however, the following sections describe how to log into the Cloud APIC using the SSH keys that you generated in the previous sections or using SSH password authentication.

Log Into Cloud APIC Using SSH Keys

Step 1 Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

Step 2 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Virtual Machines** link.

Step 3 Locate the Cloud APIC system in the Virtual Machines page, then locate the IP address shown in the Public IP address column.

Step 4 Log into your Cloud APIC using the SSH keys.

- For Linux systems, enter the following to log into your Cloud APIC:

```
# ssh -i private-key-file admin@public-IP-address
```

  where the private-key-file is the private key file that you created in Generating an SSH Key Pair in Linux or MacOS, on page 31.

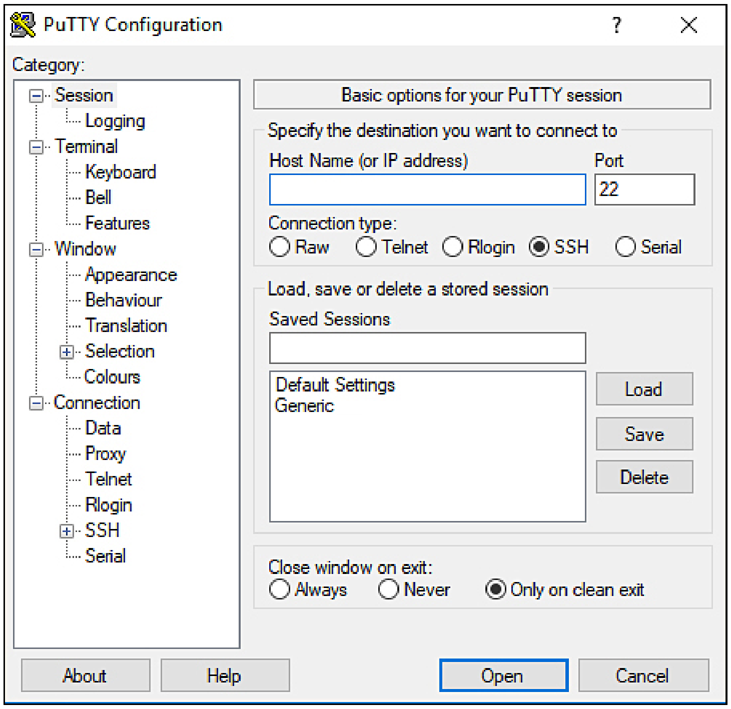
  For example:

```
# ssh -i azure_key admin@192.0.2.1
```

- For Windows systems, use PuTTY to log into your Cloud APIC:

  a. Run the PuTTY Configuration program by navigating to **Windows** > **Start Menu** > **All Programs** > **PuTTY** > **PuTTY**.

  b. In the left nav bar, click **Session**, then enter the public IP address for the Cloud APIC.



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
Generic

Close window on exit: ○ Always ○ Never ● Only on clean exit

c. In the left nav bar, click **Connection** > **SSH** > **Auth**.

d. In the Authentication parameters area, locate the Private key file for authentication field and click the **Browse...** button.

e. Navigate to the private key file that you created in Generating an SSH Key Pair in Windows, on page 28 and click **Open**.

f. In the main PuTTY window, click **Open** to log into the Cloud APIC. A login prompt appears.

g. Log into the Cloud APIC as `admin`.

Log Into Cloud APIC Using SSH Password Authentication

Unlike SSH using a public key, SSH Password Authentication is disabled by default. Use these procedures to enable SSH Password Authentication so that you can SSH into your Cloud APIC with a username and password.

Step 1 Open a browser window and, using the secure version of HTTP (`https://`), paste the IP address into the URL field, then press Return to access this Cloud APIC.

For example, `https://192.0.2.1`.

Step 2 Enter the following information in the login page for the Cloud APIC:

- **Username**: Enter admin for this field.

- **Password**: Enter the password that you provided to log into the Cloud APIC.
- **Domain**: If you see the Domain field, leave the default Domain entry as-is.

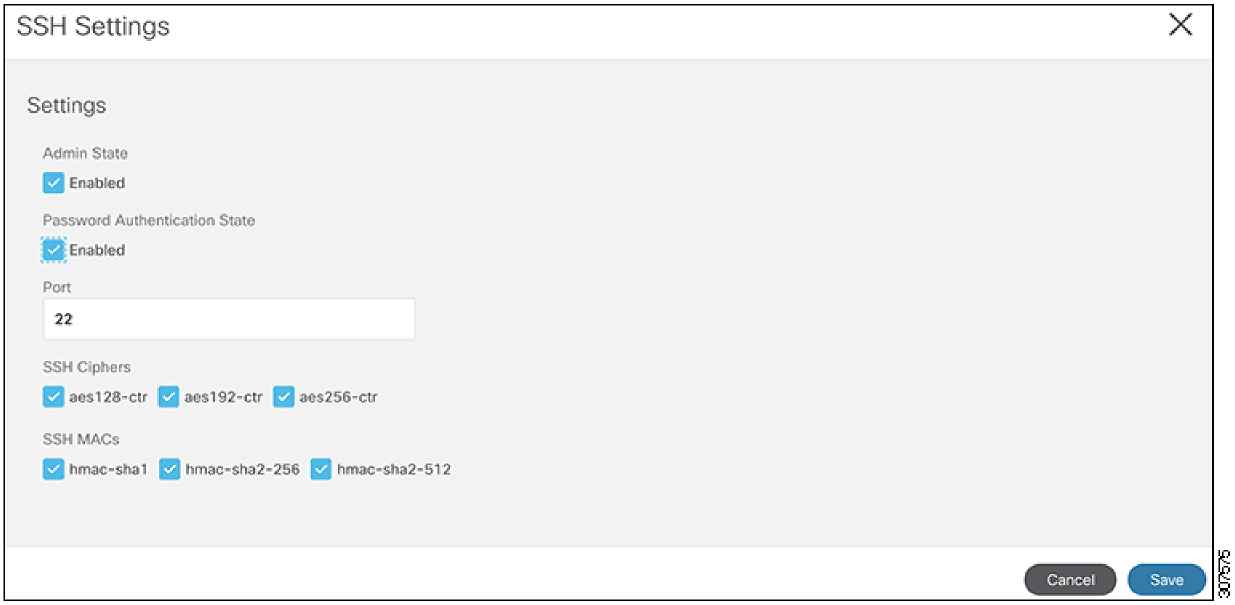
Step 3 Click **Login** at the bottom of the page.

Step 4 Navigate to **Infrastructure** > **System Configuration**, then click the **Management Access** tab in the **System Configuration** page.

Step 5 Click the pencil icon in the upper right corner of the screen to edit the SSH settings.

The Settings page appears for SSH.

Step 6 In the Password Authentication State field, select Enabled.



SSH Settings

Settings

Admin State

☑ Enabled

Password Authentication State

☑ Enabled

Port

22

SSH Ciphers

☑ aes128-ctr ☑ aes192-ctr ☑ aes256-ctr

SSH MACs

☑ hmac-sha1 ☑ hmac-sha2-256 ☑ hmac-sha2-512

Step 7 Click **Save**.

You can now SSH into your Cloud APIC without having to access the public and private key files:

```
# ssh admin@192.0.2.1
```