



## Importing Existing Brownfield Azure Cloud VNets Into Cisco Cloud APIC

### [New and Changed Information](#) 2

[Benefits of Importing Existing Azure Brownfield Cloud VNets into Cisco Cloud APIC](#) 2

[Terminology Used In This Document](#) 3

[About VNet Peering for Unmanaged \(Brownfield\) VNets](#) 4

[What Cisco Cloud APIC Does and Does Not Do With Brownfield VNets](#) 5

[Guidelines and Restrictions](#) 7

[Workflow for Importing Existing Brownfield Cloud VNets Into Cisco Cloud APIC](#) 7

[Updates in Release 25.0\(4\)](#) 8

[Configuring Access Policies at Different Levels](#) 16

[Copying a Route Table Associated with a Brownfield VNet](#) 22

[Creating an Unmanaged \(Brownfield\) Cloud Context Profile](#) 24

[Adding Peering from Unmanaged VNet to Infra VNets in Azure](#) 31

[Creating an EPG Associated With the Brownfield Cloud Context Profile](#) 33

[Completing the Remaining Configurations for the Brownfield VNet in Azure](#) 39

[Verifying the Configurations](#) 44

[Trademarks](#) 44

Revised: July 13, 2022,

## New and Changed Information

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

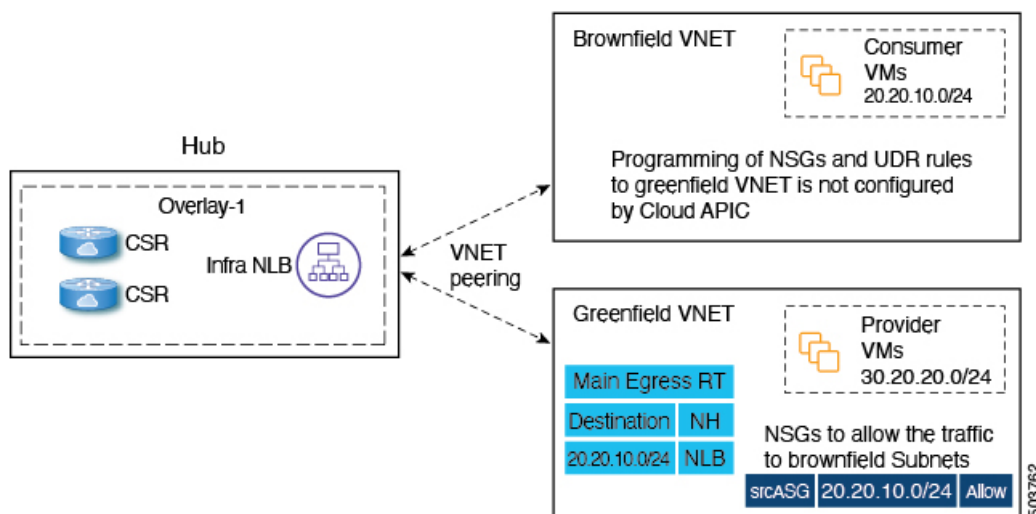
Cisco APIC Release Version	Feature	Description
25.0(4)	Updates to access policies	This release provides updates for access policies for Cisco Cloud APIC with Azure, where new access policies are available at different levels. See <a href="#">Updates to Access Policies in Release 25.0(4), on page 9</a> for more information.
25.0(4)	Route table copying	This release allows for route table copying when importing brownfield VNets into Cisco Cloud APIC. See <a href="#">About Route Table Copying, on page 13</a> for more information.
5.2(1)	Support for importing existing brownfield cloud VNets into Cisco Cloud APIC	This release provides support for importing existing brownfield cloud VNets into Cisco Cloud APIC

## Benefits of Importing Existing Azure Brownfield Cloud VNets into Cisco Cloud APIC

Prior to release 5.2(1), cloud deployments through Cisco Cloud APIC are considered greenfield deployments, where the configurations for the necessary components (resource groups, VNets, CIDRs, subnets, and so on) are done through the Cisco Cloud APIC. You would then deploy the services under these resource groups created through the Cisco Cloud APIC to bring up your applications.

Many users who have adopted Microsoft Azure Cloud for their data center extensions have hundreds of VNets and instances already deployed in the cloud. This results in having two different environments, one for the new greenfield configurations through Cisco Cloud APIC and existing brownfield configurations on Azure. This is not ideal if you don't want separate control points for your existing cloud resources once you adopt the Cisco Cloud APIC solution.

Prior to release 5.2(1), existing brownfield environments, where the resource groups and VNets were created without using Cisco Cloud APIC, were not able to coexist in a Cisco Cloud APIC-managed site. Beginning with release 5.2(1), support is now available for importing existing brownfield VNets into Cisco Cloud APIC. This enhancement uses VNet peering to provide communication between greenfield VNets configured through Cisco Cloud APIC and brownfield VNets that were configured outside of Cisco Cloud APIC.



In the figure above:

- The hub VNet and the greenfield VNet were created and are managed through Cisco Cloud APIC
- The brownfield VNet was created by you through Azure and is managed outside of Cisco Cloud APIC

Note that with this feature, Cisco Cloud APIC does not configure or provision anything in the existing brownfield resource groups. The regular route tables, UDR rules, NSGs and ASGs are not created through Cisco Cloud APIC for these brownfield resource groups. Cisco Cloud APIC will not manage security rules and routing for these existing brownfield deployments, so you will continue to manage security rules and routing for those existing brownfield deployments outside of Cisco Cloud APIC.

With this brownfield feature, you can import brownfield VNets into the Cisco Cloud APIC, where:

- The brownfield VNets belong to subscriptions pointing to the same Azure Active Directory (Azure AD) as the one associated with the infra tenant, or
- The brownfield VNets belong to subscriptions pointing to an Azure AD different from the Azure AD associated with the infra tenant. This is accomplished using the support for VNet peering across Azure ADs feature, available in release 5.2(1). For more information, see [Configuring VNet Peering for Cloud APIC for Azure](#).

## Terminology Used In This Document

This section introduces some of the key terminology and concepts used in this document:

### Greenfield VNet

A Virtual Network on Azure that is created by Cloud APIC based on the cloud context profile.

### Brownfield or unmanaged VNet

A Virtual Network on Azure that is created without using a policy through Cloud APIC.

### Greenfield resource group

A resource group on Azure that is created by Cloud APIC based on the cloud context profile.

### Brownfield or unmanaged resource group

A resource group on Azure that is created without using a policy through Cloud APIC.

### Access policy

Policies that are created on Cloud APIC that denote the respective privilege.

Prior to release 25.0(4), the access policies are:

- Default
- Read-Only
- Unmanaged

Beginning with release 25.0(4), the access policies are:

- Read Only
- Routing Only
- Routing & Security

Note that most of these access policies can be applied at the global, account/tenant, VNet, and subnet levels (Read Only is not supported at the global level). See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

### **Route table copying**

A new feature introduced in release 25.0(4). Describes the ability to copy routes from route tables that are associated with the subnets in a brownfield VNet when you import that brownfield VNet into Cisco Cloud APIC. Cisco Cloud APIC does not modify any existing route tables associated with a brownfield VNet, but rather copies all the routes from that route table into a Cisco Cloud APIC-created route table when you import a brownfield VNet into Cloud APIC.

## **About VNet Peering for Unmanaged (Brownfield) VNets**

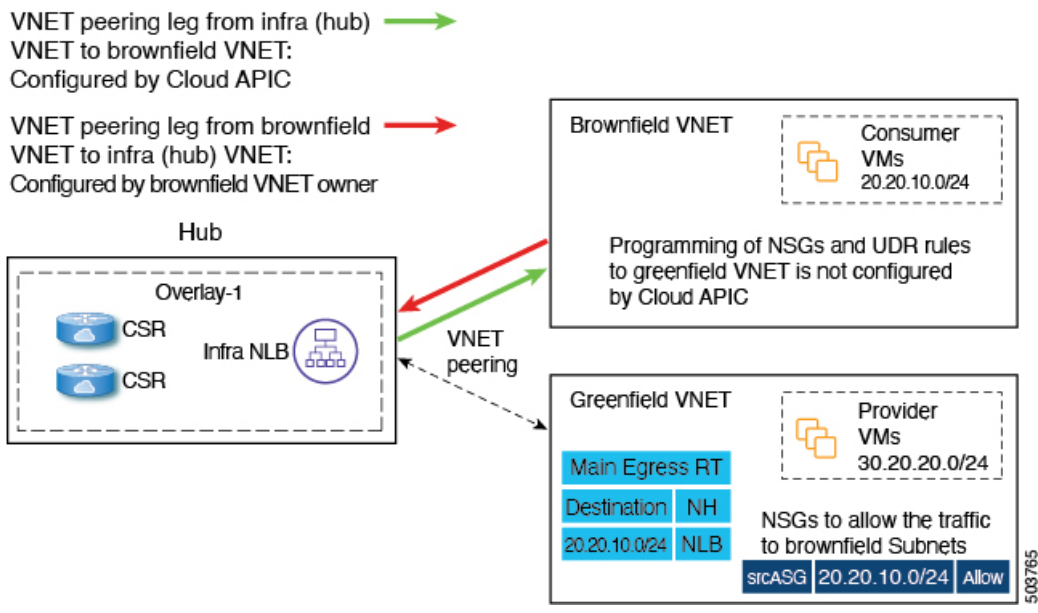
The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect how Cisco Cloud APIC configures VNet peering for brownfield VNets. See [How the Brownfield VNet Import Differs in Release 25.0\(4\), on page 15](#) for more information.

Typically, when Cisco Cloud APIC creates a greenfield VNet on the cloud, it creates a bidirectional VNet peering configuration from this spoke VNet to all of the infra (hub) VNets. For VNet peering configurations with greenfield VNets, Cisco Cloud APIC configures both legs of this peering configuration:

- Cisco Cloud APIC configures the first leg from the infra (hub) VNet to the spoke VNet
- Cisco Cloud APIC then configures the other leg from the spoke VNet to the infra VNet

However, when configuring VNet peering with an unmanaged (brownfield) VNet, some of the VNet peering configurations are done by Cisco Cloud APIC and other VNet peering configurations must be done manually by you:

- **First leg from the infra (hub) VNet to the unmanaged VNet:** Configured by Cisco Cloud APIC, where the Cisco Cloud APIC takes care of the programming of the UDR and NSG rules on greenfield NSGs on resource groups managed by Cisco Cloud APIC.
- **Other leg from the unmanaged VNet to the infra VNet:** As the owner of the unmanaged (brownfield) VNet, you must manually configure this leg of the VNet peering configuration. This leg of the VNet peering configuration is not done by Cisco Cloud APIC. You have to configure UDR and NSG rules on the brownfield VNet to communicate with the greenfield VNet.



In order to have communication between the greenfield VNet and the brownfield VNet, you must create these single-leg VNet peerings from the unmanaged VNet to all of the infra VNets. Without this, the packet flow will not occur between the greenfield VNet and the brownfield VNets.

In addition, beginning with release 5.2(1), support is also available for VNet peering across Azure active directories. Without this enhancement, you would be restricted to the same Azure active directory. With this enhancement, you are not restricted to importing brownfield VNets from the same Azure active directories as the infra VNet. Brownfield VNets present in different Azure active directories compared to the infra Azure active directory can be imported into Cisco Cloud APIC using this enhancement for VNet peering across Azure active directories.

For more information, see [Configuring VNet Peering for Cloud APIC for Azure](#).

## What Cisco Cloud APIC Does and Does Not Do With Brownfield VNets



**Note** The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect what Cisco Cloud APIC does and does not do with brownfield VNets. See [How the Brownfield VNet Import Differs in Release 25.0\(4\), on page 15](#) for more information.

With this enhancement as part of release 5.2(1), Cisco Cloud APIC is able to orchestrate the network connectivity and security required on the greenfield resource group/VNet side to be able to send and receive packets from a brownfield VNet.

Cisco Cloud APIC provides the following with regards to provisioning:

- Cisco Cloud APIC provisions the VNet peering from all of the infra VNets to the brownfield VNet.
- From the greenfield VNet side:
  - Cisco Cloud APIC provisions the route table entries for the brownfield VNet CIDRs with the next hop as the network load balancer in the infra VNet.

- Cisco Cloud APIC provisions the security group rules to allow packets coming in from or going out to the subnets or IP addresses of the brownfield VNet endpoints or subnets, depending on the configured contracts.

When you register a brownfield VNet with Cisco Cloud APIC, the following configurations take place:

- An inventory pull is performed on the brownfield resource group or VNet.
- Cisco Cloud APIC automatically configures unidirectional VNet peering from all of the infra VNets to the brownfield VNet. See [About VNet Peering for Unmanaged \(Brownfield\) VNets, on page 4](#) for more information.
- Based on the contracts with existing greenfield EPGs, UDR and NSG rules are set only on greenfield NSGs on resource groups managed by Cisco Cloud APIC.
- Once the contract is defined between the EPG associated with the greenfield VNet and the EPG associated with the brownfield cloud context profile, Cisco Cloud APIC will automatically program the CSR with the static routes. Cisco Cloud APIC also configures route leaking corresponding to the brownfield VNet CIDRs in the CSR.
- Cisco Cloud APIC automatically programs all the route entries corresponding to the brownfield VNet CIDRs on the greenfield VNet based on the contract between the EPGs.

Cloud EPGs associated with brownfield cloud context profiles through the VRF should have subnet-based endpoint selectors (tag-based EPGs will not be applicable on brownfield cloud context profiles).

For release 5.2(1), Cisco Cloud APIC will not configure or provision anything in the unmanaged resource groups. Cisco Cloud APIC does not create the regular route tables, UDR rules, NSGs, and ASGs in these unmanaged resource groups. You are responsible for the security and routing on these unmanaged resource groups, as Cisco Cloud APIC will not be managing them.

The following configurations do *not* take place when you register a brownfield VNet with Cisco Cloud APIC, so you must create these policies and apply them:

- Cisco Cloud APIC does not create route tables with the UDRs pointing to the infra NLB, based on the contracts with the greenfield EPGs. You must program the UDR rules in the route tables to send and receive packets from the external site subnets. These external subnets should be programmed with the next hop pointing to the private IP of one of the infra NLBs in the hub VNets.
- Cisco Cloud APIC does not create any NSGs or ASGs in the brownfield resource groups. You must program the NSG or ASG rules to allow the security rules to send or receive packets from the external site endpoints or subnets. See the following page on the Azure site for more information:

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group#work-with-application-security-groups>

- Cisco Cloud APIC does not program the VNet peering from the brownfield VNet to the infra VNets. You must program the VNet peering from the brownfield VNet to the infra VNets. See [About VNet Peering for Unmanaged \(Brownfield\) VNets, on page 4](#) for more information.
- There is no endpoint discovery done for the endpoints in these brownfield resource groups.

In addition, the following Cisco Cloud APIC components are affected or are not affected when you register a brownfield VNet with Cisco Cloud APIC:

- No changes take place with CSR programming for the brownfield VRF. From the CSR perspective, the brownfield VRF will behave like any other VRF. On the CSR, the brownfield VRF will be programmed along with the CIDRs (the CIDRs present on the unmanaged cloud context profile). Access lists will be programmed on the gigabit 1 interface to allow traffic coming in from these unmanaged VNet CIDRs. Based on the contracts, route leaking will occur between different VRFs, if necessary.

## Guidelines and Restrictions

The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect the guidelines and restrictions for importing brownfield VNETs. See [How the Brownfield VNet Import Differs in Release 25.0\(4\), on page 15](#) for more information.

Following are the guidelines and restrictions when importing existing brownfield cloud configurations into Cloud APIC.



---

**Note** In the following bullets, the term "infra NLB" is used to refer to the NLB in the infra VNet's Resource Group.

---

- As part of the process for importing existing brownfield cloud configurations into Cloud APIC, you will configure the following:
  - Route entry for the greenfield CIDR in the route table belonging to the brownfield resource group with the next-hop set to the infra NLB
  - Security rules to allow traffic from and to the greenfield EPG
  - VNet peering between brownfield VNETs and infra VNETs.

In a typical Cloud APIC multi-hub deployment, an infra NLB failure in one region is usually detected automatically, which results in the UDR being updated automatically with another available infra NLB as the next-hop in the route plane. However, when configuring the system to import existing brownfield cloud configurations into Cloud APIC as described above, this infra NLB failure detection and UDR update does not occur automatically as it normally would.

In this situation, it is your responsibility to detect the infra NLB failure and manually update the brownfield route table with an operating infra NLB IP address as the next-hop.

- The following guidelines and restrictions apply specifically for unmanaged (brownfield) cloud context profiles:
  - A given VNet ID of a brownfield VNet cannot be mapped to two different unmanaged cloud context profiles on a Cisco Cloud APIC. A given VNet ID can only be used once to create only one unmanaged cloud context profile on a Cisco Cloud APIC.
  - An unmanaged VNet mapped to a cloud context profile should reside in the same account (subscription) as the tenant that is associated with this cloud context profile. Random VNet IDs cannot be given while defining these unmanaged cloud context profiles on the Cisco Cloud APIC.
- A hosted VRF can't be used for importing a brownfield VNet.

## Workflow for Importing Existing Brownfield Cloud VNETs Into Cisco Cloud APIC



---

**Note** The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect the workflow for importing existing brownfield VNETs. See [How the Brownfield VNet Import Differs in Release 25.0\(4\), on page 15](#) for more information.

---

Following is the general workflow for importing existing brownfield cloud VNets into Cisco Cloud APIC:

1. Create a new tenant to be used with the unmanaged (brownfield) cloud context profile, if necessary.

If the unmanaged (brownfield) VNet is in a different subscription, then you must create a new tenant.

This new account created under the unmanaged tenant will also have a relation to a read-only policy, which will not trigger the creation of event collection or stat collection resources on these subscriptions. Only the inventory pull will be done for these subscriptions.

For instructions on creating a new tenant, see the following sections in the [Cisco Cloud APIC for Azure User Guide](#), Release 5.2(x) or later:

- "Understanding Tenants, Identities, and Subscriptions"
- "Creating a Tenant Using the Cisco Cloud APIC GUI"

2. Import the existing brownfield VNet, CIDR, and subnet configurations in to Cisco Cloud APIC.

You do this by creating a cloud context profile corresponding to the brownfield VNet, which creates an association between the brownfield VNet and a VRF. The cloud context profile in Cisco Cloud APIC is an object that is used to link between the brownfield VNet and a VRF. To import the brownfield VNet, you must first create a VRF object, which is a placeholder for the cloud context profile association that will be used later when importing the brownfield VNet.

See [Creating an Unmanaged \(Brownfield\) Cloud Context Profile, on page 24](#) for those procedures.

3. Configure VNet peering for the brownfield VNets.

- As the owner of the unmanaged (brownfield) VNet, you must manually configure one part of the VNet peering configuration, the leg from the unmanaged VNet to the infra VNet. Cisco Cloud APIC automatically configures the other part of the VNet peering configuration, the leg from the infra VNet to the unmanaged VNet.

For more information, see [About VNet Peering for Unmanaged \(Brownfield\) VNets, on page 4](#).

- If you want VNet peering across Azure ADs, you must configure that separately.

For more information, see [Configuring VNet Peering for Cloud APIC for Azure](#).

4. Create an EPG associated with the brownfield cloud context profile.

See [Creating an EPG Associated With the Brownfield Cloud Context Profile, on page 33](#) for those procedures.

## Updates in Release 25.0(4)



---

**Note** The information in this section describe updates that are available beginning in release 25.0(4).

To understand how certain configurations (such as access policies) were done prior to release 25.0(4), see [What Cisco Cloud APIC Does and Does Not Do With Brownfield VNets, on page 5](#) and [Workflow for Importing Existing Brownfield Cloud VNets Into Cisco Cloud APIC, on page 7](#).

---

- Following are the updates to the access policies beginning in release 25.0(4):
  - Prior to release 25.0(4), you can import a brownfield VNet into Cisco Cloud APIC only using a Read Only access policy (previously referred to as **unmanaged**), where the Cisco Cloud APIC has no write privileges on that brownfield VNet. With the Read Only access policy, the brownfield VNet co-exists in the Cisco Cloud APIC fabric with Cisco Cloud



APIC-created (greenfield) VNETs, but any security group or route table configurations that are required on the brownfield VNET are not done through the Cisco Cloud APIC.

Beginning with release 25.0(4), you can now apply the following additional access policies when you import a brownfield VNET into Cisco Cloud APIC:

- Routing & Security
- Routing Only

Based on the access policy that you apply, the Cloud APIC can take full ownership of that imported brownfield VNET.

- Beginning with release 25.0(4), support is also available for changing from one access policy to another access policy. For example, if you initially imported a brownfield VNET with a Routing & Security access policy, you can change the access policy for that imported brownfield VNET to Routing Only at a later date.
- In addition, prior to release 25.0(4), you could only apply access policies at the VNET level. Beginning with release 25.0(4), you can also apply access policies at the global (Cloud APIC), account/tenant, VNET, or subnet levels (note that the Read Only access policy is not supported at the global level).
- In the absence of an explicitly-applied access policy, an object will inherit the access policy from its parent. See [Hierarchy of Access Policies, on page 10](#) for more information.

See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

- When importing a brownfield VNET, you can also copy routes from route tables that are associated with the subnets in that brownfield VNET. Cisco Cloud APIC does not take over existing route tables that are already present in that brownfield VNET in this case. Instead, Cisco Cloud APIC copies the existing route tables that are associated with the subnets in the brownfield VNET that is being imported, then controls routes through Cloud APIC-created route tables that are copied from the brownfield VNET route tables.
- The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

## Updates to Access Policies in Release 25.0(4)

Following are the updates to the access policies that are available beginning in release 25.0(4):

- [About the New Access Policies, on page 9](#)
- [Hierarchy of Access Policies, on page 10](#)
- [When You Might Use Different Access Policies, on page 12](#)
- [Guidelines and Limitations, on page 13](#)

### About the New Access Policies

Prior to release 25.0(4), support was available only for the Read Only access policy. Beginning with release 25.0(4), the following access policies are now available, listed in order of greater privileges (least restrictive) to lesser privileges (more restrictive).

- **Routing & Security access policy:** The default access policy. If you do not assign an access policy to an object, then that object has a Routing & Security access policy applied to it by default.

Assigning a Routing & Security access policy to an object means that it has full permissions, where it is able to control Routing & Security. This is the typical access policy that would normally be applied to an object if you were to create that object through Cisco Cloud APIC (if this were a greenfield object created through Cisco Cloud APIC).

- **Routing Only access policy:** Assigning a Routing Only access policy to an object means that it can control only the routing policy and the network connectivity.
- **Read Only access policy:** The existing access policy that was available prior to release 25.0(4). Assigning a Read Only access policy to an object means that it does not have write permissions and can only read the inventory. Note that the Read Only access policy is not supported at the global (Cisco Cloud APIC) level.

## Hierarchy of Access Policies

Following is the hierarchy of the objects where access policies can be applied, in order from the highest level to the lowest level. Note that for each level, while the children objects under a parent object automatically inherit the access policy applied at the parent level, you can also manually change the access policy for any child under a parent object within the guidelines provided later in this section.

1. **Global Level:** Access policies applied at the global level (the `cloudDomP` level) are attached to a cloud account or cloud provider and affect the entire Cisco Cloud APIC system. All objects created or imported with the Inherit option under this Cisco Cloud APIC (such as tenants, VNets, and subnets) automatically inherit the access policy applied at this global level.

You can configure the access policy at the global level during the initial first time setup of the Cisco Cloud APIC.

- By default, the access policy at the global level will be set to Routing & Security.
- Routing Only is the only other valid alternate access policy at the global level. The Read Only access policy is not supported at the global level.

2. **Account/Tenant Level:** Access policies applied at the account/tenant level (the `cloudAccount` level) apply to all resources within that account. All objects created or imported with the Inherit option under the account or tenant (such as VNets and subnets) automatically inherit the access policy applied at the account or tenant level.

If the account is set to a Read Only access policy, then the extra resources are not created on the cloud in this account.

3. **VNet Level:** Access policies applied at the VNet level (the `cloudCtxProfile` level) apply to all resources within that VNet. All objects created or imported with the Inherit option under the VNet (such as subnets) automatically inherit the access policy applied at the VNet level.

Assigning an access policy at the VNet level affects the following resources within that VNet:

- Route tables in the VNet or resource group
- The ability to peer with the infra VNet
- Security groups and their rules

4. **Subnet Level:** Access policies applied at the subnet level (the `cloudSubnet` level) apply to all resources under that subnet.

Assigning an access policy at the subnet level affects the following resources under that subnet:

- Association of the subnet to the given routing table
- Association of the subnet to the NSG or the endpoints in that subnet that are associated with that security group

The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

In addition, following is a list of the access policies mentioned earlier, listed in order of greater privileges (least restrictive) to lesser privileges (more restrictive):

1. **Routing & Security access policy**
2. **Routing Only access policy**
3. **Read Only access policy**

For any of the levels listed above, the following rules apply:

- When you set an access policy at a parent level, any objects created or imported with the Inherit option underneath that level automatically inherit the access policy of the parent.
- However, policies can be overridden at any child level. At any child level in the hierarchy shown above, if you want a more restrictive policy than the policy set for the parent, setting a different policy at that child level will override the policy applied at parent level. Note that the policy applied at the child level (the overriding policy) must be more restrictive or equal to the policy applied at the parent level.
- If the children access policies are using the Inherit options and you change an access policy at a parent level at some point in the future, then the access policy for all of the children under that parent policy automatically change to match the parent at that point.

For example, assume the following scenario:

1. You set the access policy at the **global level** to a **Routing & Security** access policy. At this point, if you create or import objects under the global level with the Inherit option along with the access policy, all objects under that Cisco Cloud APIC is set with a Routing & Security access policy, which is the access policy with the greatest privileges (the least restrictive access policy).
2. You then manually change the access policy at the **subnet level** to a **Read Only** access policy. The access policies are then set for the objects within the Cisco Cloud APIC in this way:
  - All objects created or imported with the Inherit option under the global level, but above the subnet level, are set with a Routing & Security access policy.
  - All objects created or imported with the Inherit option under the subnet level are set with a Read Only access policy.

Note that the changes take effect only for the subnet where the access policy was changed. New subnets imported will continue to have the Inherit access policy by default unless otherwise changed.

3. Then, at some point in the future, you decide to change the access policy at the **global level** again, this time setting the global level access policy to a **Routing Only** access policy. At that point, all of the children objects under the global level, but above the subnet level, that are created or imported with the Inherit option are set to the parent's Routing Only access policy.

However, because you had manually set the access policy at the subnet level to the Read Only access policy, the access policy does not change at the subnet level, even though the access policy changed at the global level; this is because the access policy at the subnet level was not set to Inherit the access policy at the global level. All objects created or imported with the Inherit option under the subnet level remain with a Read Only access policy.

Following is a set of example scenarios and how access policies would be applied at various levels for each scenario.

**Table 1: Example Access Policy Scenarios**

Levels				
Global	Account/Tenant	VNet	Subnet	Notes
Routing & Security access policy	Inherit	Inherit	Inherit	Valid configuration <ul style="list-style-type: none"> <li>• Routing &amp; Security access policy applied at the global level by default</li> <li>• All objects created or imported with the Inherit option under global level (account/tenant, VNet, and subnet levels) inherit the Routing &amp; Security access policy that was applied at the global level</li> </ul>
Routing & Security access policy	Inherit	Routing Only access policy	Inherit	Valid configuration <ul style="list-style-type: none"> <li>• Routing &amp; Security access policy applied at global level and inherited at the account/tenant level</li> <li>• Routing Only access policy applied at VNet level and inherited at the subnet level</li> </ul>
Routing Only access policy	Routing & Security access policy (invalid configuration)	Inherit	Inherit	Invalid configuration <ul style="list-style-type: none"> <li>• Routing Only access policy is more restrictive than Routing &amp; Security access policy</li> <li>• Policy at child (account/tenant) level cannot be more restrictive than parent (global) level</li> <li>• As long as the access policy is set to Routing Only at the global level, the account/tenant and lower objects can have only the Routing Only or Read Only access policies</li> </ul>

### When You Might Use Different Access Policies

Following are several use cases where you might use different access policies:

- **Gradual migration of brownfield resources:** Assume that you have an existing brownfield VNet with a number of subnets and you want to migrate one subnet, leaving the remaining subnets untouched. You could accomplish this task using access policies in the following manner:
  - Assign a Routing & Security access policy for the one subnet that you want to migrate.
  - Assign a Read Only access policy for the remaining subnets that you want to leave untouched.
- **Granular control over what the Cisco Cloud APIC does to the cloud resources:** Using different access policies, you can have Cisco Cloud APIC-managed resources and brownfield resources co-existing in the same VNet.

For example, assigning a Routing Only access policy at any level means that you are entirely in control of the network at that level. Conversely, assigning a Routing & Security access policy at any level means that the Cisco Cloud APIC controls the Routing & Security at that level.

- **Having brownfield and greenfield VNETs co-exist in Cisco Cloud APIC fabric:** When importing a brownfield VNET into Cisco Cloud APIC, that brownfield VNET is able to co-exist with Cisco Cloud APIC-created and managed VNETs by using different access policies.
- **Determining overall functionality of Cisco Cloud APIC:** For example, if you wanted to use the Cisco Cloud APIC only for routing, and have the security policy managed outside of Cisco Cloud APIC. In that case, you would assign a Routing Only access policy at the Cisco Cloud APIC level.

## Guidelines and Limitations

Following are the guidelines and limitations for the new access policies that are available in release 25.0(4):

- Following are the restrictions for the access policies at various levels:
  - At the global level, only the Routing & Security and Routing Only access policies are supported; the Read Only access policy is not a valid option at the global level.
  - However, all three access policies (Routing & Security, Routing Only, and Read Only) are supported for all remaining levels (account/tenant, VNET, and subnet).
- For greenfield VNETs:
  - You can apply the Routing Only access policy if you want the Cisco Cloud APIC to manage only the routing and not the security.
  - The Read Only access policy is not supported for greenfield VNETs.

## About Route Table Copying

Beginning with release 25.0(4), support is available for copying routes from certain route tables that are created outside of Cisco Cloud APIC. This provides the ability to copy routes from route tables that are associated with the subnets in a brownfield VNET when you import that brownfield VNET into Cisco Cloud APIC.

In this situation, Cisco Cloud APIC does not modify any existing route tables that are associated with the subnets in a brownfield VNET, but rather copies the routes from that route table into a Cisco Cloud APIC-created route table when you import a brownfield VNET into Cloud APIC or when you use the **Copy Existing Routes** option in the Cloud APIC GUI. You can then make modifications to that Cloud APIC-created route table that is associated with the imported brownfield VNET, if necessary. An option is also available for you to select multiple route tables so that all of the routes from multiple route tables will be copied into this Cloud APIC-created route table.

In order to copy routes from route tables that are associated with the subnets in a brownfield VNET to a Cloud APIC-created route table:

1. You will be provided with an option to select one or more route tables that you can opt to copy and the source VRF that will be used for the brownfield VNET route table.
2. Select subnets corresponding to the route tables.
3. Cisco Cloud APIC then creates its own routing table and populates the routes from the route tables and associates all selected subnets with this table.

You can copy a route table at two different points in time:

- As part of the initial first time setup operation, where you are importing a brownfield VNet while you are setting up the Cisco Cloud APIC and you want to copy the routes in a route table that is associated with the subnets in that imported brownfield VNet.
- As an update operation at some point later on. Note that this applies only in the following situations:
  - If you imported a brownfield VNet as part of the initial first time setup operation and did not copy the route table associated with the subnets in that imported brownfield VNet at that time
  - If you imported only **some** of the subnets associated with a route table that you copied previously, or if that copied route table is associated with subnets in multiple VNets

Then you can copy that route table after the initial first time setup operation as long as there are still subnets in those VNets associated with that route table that have not been imported into Cloud APIC.

Routes are classified in the following manner in the inventory:

- **Cloud APIC-Owned:** Greenfield routes that are created through Cisco Cloud APIC
- **Cloud APIC-Copied:** Brownfield routes that were created outside of Cisco Cloud APIC but were copied into the Cisco Cloud APIC-created route table when you imported a brownfield VNet into Cloud APIC or when you used the **Copy Existing Routes** option in the Cloud APIC GUI.
- **Other:** Brownfield routes that were created outside of Cisco Cloud APIC but were not copied in the Cisco Cloud APIC-created route table.

## Guidelines and Limitations

Following are the guidelines and limitations for the route table copying feature in Cisco Cloud APIC:

- The copying feature applies only to routes. Cisco Cloud APIC does not copy existing security groups associated with the brownfield VNets. Cisco Cloud APIC creates its own security groups based on the contracts and associates those Cisco Cloud APIC-created security groups with the necessary subnets or endpoints.
- The Cisco Cloud APIC route-leak policy will always override any existing copied routes in the Cisco Cloud APIC-created route table. Cisco Cloud APIC will not delete any brownfield routes in the Cisco Cloud APIC-created route table.

For example, if existing brownfield routes that are copied in the Cloud APIC-created route table match the prefix for Cisco Cloud APIC-created routes, those matched routes are not deleted in the Cisco Cloud APIC-created route table; instead, the Cisco Cloud APIC-created routes take precedence.

- Prior to release 25.0(4), if you manually added a route on a Cloud APIC-created route table, Cisco Cloud APIC would automatically remove that route that you added. Beginning with release 25.0(4), this is no longer the case; any routes that you manually add to a Cloud APIC-created route table is no longer removed, as long as it does not conflict with a Cloud APIC-created route.
- When you copy routes from existing route tables that are associated with the subnets in a brownfield VNet, the existing route tables are affected in the following ways, depending on the access policy:
  - Read Only access policy: The existing route table is not impacted. The option to copy routing is not available. The Cisco Cloud APIC-created route table is not created.
  - Routing & Security access policy:
    - If you select **Copy Existing Routes** when you import a brownfield VNet:
      1. The Cisco Cloud APIC-created route table is created.
      2. The entries are copied from one or multiple route tables into one Cisco Cloud APIC-created route table.

3. Then the subnets are disassociated from the existing route table.
- If you select **Do Not Copy Existing Routes** when you import a brownfield VNet:
    1. The Cisco Cloud APIC-created route table is created.
    2. The entries are *not* copied from the existing route tables into the Cisco Cloud APIC-created route table.
    3. However, the subnets are still disassociated from the existing route table - in this case, you should expect traffic loss.

## How the Brownfield VNet Import Differs in Release 25.0(4)



---

**Note** The information in this section describe updates that are available beginning in release 25.0(4).

To understand how certain configurations (such as access policies) were done prior to release 25.0(4), see [What Cisco Cloud APIC Does and Does Not Do With Brownfield VNets, on page 5](#) and [Workflow for Importing Existing Brownfield Cloud VNets Into Cisco Cloud APIC, on page 7](#).

---

Beginning with release 25.0(4), the following things occur when you import a brownfield VNet into Cisco Cloud APIC:

- You select the subnets in the brownfield VNet that you want to bring under Cisco Cloud APIC ownership, and Cisco Cloud APIC takes ownership of the brownfield VNet and its subnets, based on the access policy that you apply. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.
- Cloud APIC does not take over existing route tables that are already present in that brownfield VNet in this case, and instead removes the associations with the subnets in the brownfield VNet from the brownfield route tables and controls routes through Cloud APIC-created route tables that are copied (see [About Route Table Copying, on page 13](#) for more information). You select the route tables that you want to copy that are present under the brownfield VNet. Routing is controlled through the Cisco Cloud APIC-created routing table, and existing subnets on the brownfield VNets are associated with these Cisco Cloud APIC-created routing tables.
- The brownfield VNet will be attached to the Cisco Cloud APIC-created infra network (the Cisco Cloud APIC-created peering to the Cisco Cloud APIC-created infra VNets). When you import a brownfield VNet with the corresponding access policy, Cisco Cloud APIC automatically attaches this VNet to the Azure VNet peering hub. However, Cisco Cloud APIC does not remove the existing peerings in this operation; instead, it creates a peering to the Cisco Cloud APIC-created routing table.
- A brownfield VNet might contain existing CIDRs and subnets, so you can import those existing CIDRs and subnets when you import a brownfield VNet into Cisco Cloud APIC. Additionally, you can also create new CIDRs or subnets in that brownfield VNet through the Cisco Cloud APIC, depending on the access policy. For example, if the access policy of a brownfield VNet that you are importing has Routing & Security access privileges, then you can create new CIDRs and subnets on that particular brownfield VNet through the Cisco Cloud APIC.

You can create or modify additional CIDRs or subnets on brownfield VNets by directly posting the configuration under the brownfield cloud context profile on the Cisco Cloud APIC. However, in order to create CIDRs, you must disable all peerings of the VNet.

## Configuring Access Policies at Different Levels

Following are the updates to the access policies beginning in release 25.0(4):

- Prior to release 25.0(4), you can import a brownfield VNet into Cisco Cloud APIC only using a Read Only access policy, where the Cisco Cloud APIC has no write privileges on that brownfield VNet. With the Read Only access policy, the brownfield VNet co-exists in the Cisco Cloud APIC fabric with Cisco Cloud APIC-created (greenfield) VNets, but any security group or route table configurations that are required on the brownfield VNet are not done through the Cisco Cloud APIC.

Beginning with release 25.0(4), you can now apply the following additional access policies when you import a brownfield VNet into Cisco Cloud APIC:

- Routing & Security
- Routing Only

Based on the access policy that you apply, the Cloud APIC can take full ownership of that imported brownfield VNet.

- Beginning with release 25.0(4), support is also available for changing from one access policy to another access policy. For example, if you initially imported a brownfield VNet with Security & Routing access, you can change the access policy for that imported brownfield VNet to Read Only at a later date.
- In addition, prior to release 25.0(4), you could only apply access policies at the VNet level. Beginning with release 25.0(4), you can also apply access policies at the global (Cloud APIC), account/tenant, VNet, or subnet levels (note that the Read Only access policy is not supported at the global level).
- In the absence of an explicitly-applied access policy, an object will inherit the access policy from its parent. See [Hierarchy of Access Policies, on page 10](#) for more information.

See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

## Configuring Access Policies at the Global Level

Access policies applied at the global level (the `cloudDomP` level) are attached to a cloud account or cloud provider and affect the entire Cisco Cloud APIC system. All objects configured under this Cisco Cloud APIC (such as tenants, VNets, and subnets) automatically inherit the access policy applied at this global level.

This topic describes how to configure access policies at the global level.

- For instructions on configuring access policies at the account or tenant level, see [Configuring Access Policies at the Account/Tenant Level, on page 17](#).
- For instructions on configuring access policies at the VNet level, see [Configuring Access Policies at the VNet Level, on page 18](#).
- For instructions on configuring access policies at the subnet level, see [Configuring Access Policies at the Subnet Level, on page 20](#).


### Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 9](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.



## Procedure

---

- Step 1** In the Cloud APIC GUI, click the Intent icon (  ) and select **Cloud APIC Setup**.
- Step 2** In the **Region Management** area, click **Edit Configuration**.  
The **Regions to Manage** screen appears.
- Step 3** Click **Next** to advance past the **Regions to Manage** screen.  
The **General Connectivity** screen appears.
- Step 4** In the **General Connectivity** screen, scroll down to the **Cloud APIC Access Privilege** area.
- Step 5** Click the scroll-down menu and choose one of the access policies to apply globally, to the entire Cisco Cloud APIC.
- **Routing & Security:** The default access policy. If you do not assign an access policy to the Cisco Cloud APIC, then the Cisco Cloud APIC has the Routing and Security access policy applied to it by default.  
  
Assigning a Routing and Security access policy to a Cisco Cloud APIC means that it has full permissions, where it is able to control routing and security.
  - **Routing Only:** Assigning a routing-only access policy to a Cisco Cloud APIC means that it can control only the routing policy and the network connectivity.

**Note** The Read Only access policy is not available at the global (Cisco Cloud APIC) level.

---

## Configuring Access Policies at the Account/Tenant Level

Access policies applied at the account/tenant level (the `cloudAccount` level) apply to all resources within that account. All objects under the account or tenant (such as VNETs and subnets) automatically inherit the access policy applied at the account or tenant level.

This topic describes how to configure access policies at the account/tenant level.

- For instructions on configuring access policies at the global level, see [Configuring Access Policies at the Global Level, on page 16](#).
- For instructions on configuring access policies at the VNet level, see [Configuring Access Policies at the VNet Level, on page 18](#).
- For instructions on configuring access policies at the subnet level, see [Configuring Access Policies at the Subnet Level, on page 20](#).

### Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 9](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

## Procedure

---

- Step 1** In the Cloud APIC GUI, click **Application Management > Tenants**.  
The **Tenants** screen appears.
- Step 2** In the **Tenants** screen, double-click on the tenant that you want to change the access policies for.  
The **Overview** screen appears for this tenant.

**Step 3** Scroll to the bottom of the screen and click **Advanced Settings** to expand that menu option.

**Step 4** Locate the **Cloud Access Privilege** area to see the current access policy setting.

The current access policy setting for the account/tenant is displayed in the following format:

*<inherit setting> (<current access policy>)*

For example, if you see this in the **Cloud Access Privilege** for a tenant:

Inherited (Routing & Security)

That means:

- The access policy for this account/tenant is set to the Routing & Security access policy
- This access policy was inherited from the parent level (in this case, the global, or Cisco Cloud APIC level), which was also set to the Routing & Security access policy

**Step 5** If you want to change the current access policy setting at the account/tenant level, click **Actions > Edit**. The Edit screen for the tenant appears.

**Step 6** Scroll to the bottom of the screen and, if necessary, click **Advanced Settings** again to expand that menu option.

**Step 7** In the **Cloud Access Privilege** area, click the scroll-down menu and choose the access policy for this account/tenant.

- **Routing & Security:** Assigning a Routing & Security access policy to an account/tenant means that it has full permissions, where it is able to control routing and security.
- **Routing Only:** Assigning a routing-only access policy to an account/tenant means that it can control only the routing policy and the network connectivity.
- **Read Only:** The existing access policy that was available prior to release 25.0(4). Assigning a read-only access policy to an account/tenant means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the account/tenant level are based on the access policy that was assigned at the parent level (in this case, at the global level). For example, if the access policy at the parent global level is set to Routing Only, then you will only see Routing Only and Read Only as options at the child account/tenant level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\)](#), on page 9 for more information.

**Step 8** Click **Save**.

---

## Configuring Access Policies at the VNet Level

Access policies applied at the VNet level (the `cloudCtxProfile` level) apply to all resources within that VNet. All objects under the VNet (such as subnets) automatically inherit the access policy applied at the VNet level.

Assigning an access policy at the VNet level affects the following resources within that VNet:

- Route tables in the VNet or resource group
- The ability to peer with the infra VNet
- Security groups and their rules

This topic describes how to configure access policies at the VNet level.

- For instructions on configuring access policies at the global level, see [Configuring Access Policies at the Global Level, on page 16](#).
- For instructions on configuring access policies at the account/tenant level, see [Configuring Access Policies at the Account/Tenant Level, on page 17](#).
- For instructions on configuring access policies at the subnet level, see [Configuring Access Policies at the Subnet Level, on page 20](#).

## Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 9](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

## Procedure

---

- Step 1** In the Cloud APIC GUI, click **Application Management > Cloud Context Profiles**.  
The **Cloud Context Profiles** screen appears.
- Step 2** In the **Cloud Context Profiles** screen, double-click on the cloud context profile that you want to change the access policies for.  
The **Overview** screen appears for this cloud context profile.
- Step 3** Scroll to the bottom of the screen and click **Advanced Settings** to expand that menu option.
- Step 4** Locate the **Cloud Access Privilege** area to see the current access policy setting.  
The current access policy setting for the cloud context profile is displayed in the following format:  
*<inherit setting> (<current access policy>)*  
For example, if you see this in the **Cloud Access Privilege** for a cloud context profile:  
*Inherited (Routing & Security)*  
That means:
- The access policy for this cloud context profile is set to the Routing & Security access policy
  - This access policy was inherited from the parent level (in this case, the account/tenant level), which was also set to the Routing & Security access policy
- Step 5** If you want to change the current access policy setting at the cloud context profile level, click **Actions > Edit**.  
The Edit screen for the cloud context profile appears.
- Step 6** Scroll to the bottom of the screen and, if necessary, click **Advanced Settings** again to expand that menu option.
- Step 7** In the **Cloud Access Privilege** area, click the scroll-down menu and choose the access policy for this account/tenant.
- **Routing & Security:** Assigning a Routing & Security access policy to a cloud context profile means that it has full permissions, where it is able to control routing and security.
  - **Routing-Only:** Assigning a routing-only access policy to a cloud context profile means that it can control only the routing policy and the network connectivity.
  - **Read-Only:** Assigning a read-only access policy to a cloud context profile means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the VNet (cloud context profile) level are based on the access policy that was assigned at the parent level (in this case, at the account/tenant level). For example, if the access policy at the parent account/tenant level is set to Read Only, then you will only see Read Only as an option at the child VNet (cloud context profile) level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

**Step 8** Click **Save**.

---

## Configuring Access Policies at the Subnet Level

Access policies applied at the subnet level (the `cloudSubnet` level) apply to all resources under that subnet. All objects under the subnet automatically inherit the access policy applied at the subnet level.

Assigning an access policy at the subnet level affects the following resources under that subnet:

- Association of the subnet to the given routing table
- Association of the subnet to the NSG or the endpoints in that subnet that are associated with that security group

The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

This topic describes how to configure access policies at the subnet level.

- For instructions on configuring access policies at the global level, see [Configuring Access Policies at the Global Level, on page 16](#).
- For instructions on configuring access policies at the account/tenant level, see [Configuring Access Policies at the Account/Tenant Level, on page 17](#).
- For instructions on configuring access policies at the VNet (cloud context profile) level, see [Configuring Access Policies at the VNet Level, on page 18](#).

### Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 9](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

### Procedure

---

- Step 1** In the Cloud APIC GUI, click **Application Management > Cloud Context Profiles**.  
The **Cloud Context Profiles** screen appears.
- Step 2** In the **Cloud Context Profiles** screen, double-click on the cloud context profile that you want to change the access policies for.  
The **Overview** screen appears for this cloud context profile.
- Step 3** Click **Actions > Edit**.  
The Edit screen for the cloud context profile appears.
- Step 4** Scroll down until you see the **CIDRs** area.  
The CIDRs and subnets associated with this cloud context profile are displayed.
- Step 5** Click on the pencil icon on the appropriate CIDR and subnet line.

**Step 6** Locate the **Cloud Access Privilege** column in the **Subnets** area to determine the current access policy setting for the subnet.

The current setting for the access policy for the subnet is displayed in the following format:

`<inherit setting>(<current access policy>)`

For example, if you see this in the **Cloud Access Privilege** column for a subnet:

`Inherited(Routing & Security)`

That means:

- The access policy for this subnet is set to the Routing & Security access policy
- This access policy was inherited from the parent level (in this case, the VNet, or cloud context profile, level), which was also set to the Routing & Security access policy

**Step 7** In the **Cloud Access Privilege** area, click the scroll-down menu and choose the access policy for this subnet.

- **Routing & Security:** Assigning a Routing & Security access policy to a cloud context profile means that it has full permissions, where it is able to control routing and security.
- **Routing Only:** Assigning a routing-only access policy to a cloud context profile means that it can control only the routing policy and the network connectivity.
- **Read Only:** Assigning a read-only access policy to a cloud context profile means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the subnet level are based on the access policy that was assigned at the parent level (in this case, at the VNet level). For example, if the access policy at the parent VNet level is set to Read Only, then you will only see Read Only as an option at the child subnet level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

**Step 8** Click **Done**, then click **Save** in the Edit screen for the cloud context profile.

---

## Configuring Access Policies Using the REST API

This topic describes how to configure the new access policies that are available in release 25.0(4). Following are the entries that you would use for the new access policies:

- Security & Routing: `accesspolicy-default`
- Routing Only: `accesspolicy-routing-only`
- Read Only: `accesspolicy-read-only` (not supported at global level)

### Before you begin

Review the information provided in [Updates in Release 25.0\(4\), on page 8](#) to better understand the new access policies and other update available in release 25.0(4).

### Procedure

---

**Step 1** To set the access policy at the global (Cisco Cloud APIC) level:

```
<polUni>
  <cloudDomP>
    <cloudRsDomPToAccessPolicy tDn="uni/tn-infra/accesspolicy-routing-only" />
  </cloudDomP>
</polUni>
```

**Step 2** To set the access policy at the account/tenant level:

```
<polUni>
  <fvTenant name="coke" status="">
    <cloudAccount name="insbu" id="<id>" vendor="azure" accessType="credentials" status="">
      <cloudRsAccountToAccessPolicy tDn="uni/tn-infra/accesspolicy-routing-only"/>
    </cloudAccount>
  </fvTenant>
</polUni>
```

**Step 3** To set the access policy at the cloud context profile and subnet levels:

```
<polUni>
  <fvTenant name="pepsi">
    <cloudCtxProfile name="c3" status="">
      <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-default"/>
      <cloudBrownfield status="">
        <cloudIDMapping cloudProviderId="vpc-0123456789abcd" status="" />
      </cloudBrownfield>
      <cloudCidr name="cidr1" addr="40.0.0.0/16" primary="yes" >
        <cloudSubnet ip="40.0.1.0/24" usage="gateway">
          <cloudRsSubnetToAccessPolicy tDn="uni/tn-infra/accesspolicy-routing-only"/>
          <cloudBrownfield status="">
            <cloudIDMapping cloudProviderId="subnet-0123456789abcd" status="" />
          </cloudBrownfield>
        </cloudSubnet>
        <cloudSubnet ip="40.0.2.0/24" usage="gateway">
          <cloudRsSubnetToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
          <cloudBrownfield status="">
            <cloudIDMapping cloudProviderId="subnet-dcba987654321" status="" />
          </cloudBrownfield>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>
```

---

## Copying a Route Table Associated with a Brownfield VNet

Beginning with release 25.0(4), support is available for copying routes from certain route tables that are created outside of Cisco Cloud APIC. This provides the ability to copy routes from route tables that are associated with the subnets in a brownfield VNet when you import that brownfield VNet into Cisco Cloud APIC.

In this situation, Cisco Cloud APIC does not modify any existing route tables that are associated with the subnets in a brownfield VNet, but rather copies the routes from that route table into a Cisco Cloud APIC-created route table when you import a brownfield VNet into Cloud APIC or when you use the **Copy Existing Routes** option in the Cloud APIC GUI. You can then make modifications to that Cloud APIC-created route table that is associated with the imported brownfield VNet, if necessary. An option is also available

for you to select multiple route tables so that all of the routes from multiple route tables will be copied into this Cloud APIC-created route table.

You can copy a route table at two different points in time:

- As part of the initial first time setup operation, where you are importing a brownfield VNet while you are setting up the Cisco Cloud APIC and you want to copy the routes in a route table that is associated with the subnets in that imported brownfield VNet. See [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#) for those instructions.
- As an update operation at some point later on. The procedures in this topic describe how to copy a route table after the initial first time setup operation.

Note that this applies only in the following situations:

- If you imported a brownfield VNet as part of the initial first time setup operation and did not copy the route table associated with the subnets in that imported brownfield VNet at that time
- If you imported only **some** of the subnets associated with a route table that you copied previously, or if that copied route table is associated with subnets in multiple VNets

Then you can copy that route table after the initial first time setup operation as long as there are still subnets in those VNets associated with that route table that have not been imported into Cloud APIC.

## Before you begin

You can copy a route table at two different points in time. The following sections describe how to copy a route table at either of those points in time:

- To copy a route table as part of the initial first time setup operation, go to [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#).
- To copy a route table after the initial first time setup operation, follow the procedures in this topic.

## Procedure

---

- Step 1** In the Cloud APIC GUI, click **Application Management > Cloud Context Profiles**.  
The **Cloud Context Profiles** screen appears.
- Step 2** In the **Cloud Context Profiles** screen, double-click on the cloud context profile that is associated with the brownfield VNet that you imported previously.  
The **Overview** screen appears for this cloud context profile.
- Step 3** Click **Actions > Edit**.  
The **Edit Cloud Context Profile** screen for the cloud context profile appears.
- Step 4** Locate the **Copy Existing Routing Tables from VNet** area and click **Copy Existing Routes**.  
The **Brownfield Route Tables** fields appear.
- Step 5** Click **Add Brownfield Route Tables**.  
The **Select Brownfield Route Tables** page appears, displaying a list of route tables associated with the subnets in the existing brownfield (unmanaged) VNet that you are importing.
- Step 6** Select the route tables that you want to copy, then click **Select**.  
You are returned to the **Edit Cloud Context Profile** screen for the cloud context profile.
- Step 7** Determine if you want import subnets from the VNet.

Make sure that all the desired subnets and their associated route tables are selected for import and copy in order to avoid traffic disruption.

**Note** The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

Follow these steps to import the subnets from this VNet.

- a) Scroll up to the CIDRs area and click on the pencil icon to edit a CIDR block range.  
The **Edit CIDR** page appears.
- b) In the **Import Subnets from VNet** area, click the box next to **Enabled**.  
The subnets available to import from this brownfield VNet are displayed.
- c) Select the subnets to import from this VNet, then click **Done**.  
You are returned to the **Edit Cloud Context Profile** page for the cloud context profile.

**Step 8** In the **Edit Cloud Context Profile** page, click **Save**.

---

## Creating an Unmanaged (Brownfield) Cloud Context Profile

The following topics provide information for creating an unmanaged (brownfield) cloud context profile.

### About Unmanaged (Brownfield) Cloud Context Profiles

An unmanaged (brownfield) cloud context profile refers to a configuration that is posted on the Cisco Cloud APIC that is associated with the unmanaged (brownfield) VNet.

- **VRF**: The VRF on the Cisco Cloud APIC where you want to associate the unmanaged VNet
- **Region**: The region where the unmanaged VNet is present on the cloud
- **VNet ID**: The cloud provider ID of this unmanaged VNet on the cloud
- **CIDRs**: The CIDRs that need to be referred to on the Cisco Cloud APIC

Following are the necessary parameters that you will have to configure for an unmanaged (brownfield) cloud context profile:

- **VRF**: The VRF on the Cisco Cloud APIC where you want to associate the unmanaged VNet
- **Region**: The region where the unmanaged VNet is present on the cloud
- **VNet ID**: The cloud provider ID of this unmanaged VNet on the cloud
- **CIDRs**: The CIDRs that need to be referred to on the Cisco Cloud APIC

The Cisco Cloud APIC will use these parameters to map the brownfield cloud context profile to the given VNet on the cloud.



# Creating an Unmanaged (Brownfield) Cloud Context Profile Using the GUI

## Before you begin

Review the information provided in [About Unmanaged \(Brownfield\) Cloud Context Profiles, on page 24](#) before going through these procedures.

## Procedure

**Step 1** Create a new tenant to be used with the unmanaged (brownfield) cloud context profile, if necessary. If the unmanaged (brownfield) VNet is in a different subscription, then you must create a new tenant. The new tenant to be used with the brownfield VNet can have the following characteristics:

- It can be configured as a Read Only account, if you have an account (subscription) on the cloud that has only unmanaged VNets and you are never going to use Cisco Cloud APIC to manage any VNets in this subscription on Azure.
- An unmanaged tenant with Read Only access can be configured in either of these modes:
  - Managed identity mode
  - Service Principle mode

For instructions on creating a new tenant, see the following sections in the [Cisco Cloud APIC for Azure User Guide, Release 5.2\(x\)](#) or later:

- "Understanding Tenants, Identities, and Subscriptions"
- "Creating a Tenant Using the Cisco Cloud APIC GUI"

Note that this tenant should use the same Azure subscription ID as the unmanaged (brownfield) VNet in Azure.

**Step 2** Create a VRF that will be associated with the cloud context profile for the brownfield VNet.

- In the Cisco Cloud APIC GUI, in the left nav bar, click **Application Management > VRFs**. A list of configure VRFs appears.
- Click **Actions > Create VRF**. The **Create VRF** page appears.
- Enter the appropriate values in each field as listed in the following *Create VRF Dialog Box Fields* table then continue.

**Table 2: Create VRF Dialog Box Fields**

Properties	Description
<b>General</b>	

Properties	Description
<b>Name</b>	Enter a name for the VRF in the <b>Name</b> field.  All VRFs are assigned a <i>vrfEncoded</i> value. If the Tenant and VRF name combination has more than 32 characters, then, a VRF name (which also contains the tenant name) is identified in the cloud router using the <i>vrfEncoded</i> value. To see the <i>vrfEncoded</i> value, navigate to <b>Application Management &gt; VRFs</b> subtab. Click a VRF on the right hand pane and look for <i>Encoded VRF Name in Cloud Router</i> .
<b>Tenant</b>	To choose a tenant:  1. Click <b>Select Tenant</b> . The <b>Select Tenant</b> dialog box appears.  2. From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column then click <b>Select</b> . You return to the <b>Create VRF</b> dialog box.
<b>Description</b>	Enter a description of the VRF.

d) When finished, click **Save**.

**Step 3** In the Cisco Cloud APIC GUI, click the Intent icon (  ).

A slide-in pane appears from the right of the window, asking **What would you like to do?**

**Step 4** Click the **Import Brownfield Virtual Network** option.

A setup wizard for creating an unmanaged cloud context profile appears.

**Step 5** In the **Import Brownfield Virtual Network** window, in the **Settings** area, click **Select Virtual Network**.

The **Select Virtual Network** window appears, with a list of all available brownfield VNets (VNets that are not managed by Cisco Cloud APIC) that are available in Azure under the subscription where you created the tenant. The list of VNets that is populated in this window is based on the inventory pull on this subscription.

**Step 6** Locate the unmanaged VNet from the list that you want to import and associate with the unmanaged cloud context profile.

In this window in the Cisco Cloud APIC GUI, the unmanaged VNets in this list are shown with this format:

**AZURE > {Azure\_subscription\_ID} > {Azure\_resource\_group}**

And the name of the brownfield VNet in the **Name** column in the Cisco Cloud APIC GUI page.

Return to the Azure portal and click on the unmanaged VNet in the Azure page, then locate the **Resource Group**, **Subscription ID**, and **Name** fields for this brownfield VNet to verify that the information matches with the information displayed in the Cisco Cloud APIC GUI page.

**Step 7** Click on the appropriate unmanaged VNet from the list.

The right pane in the window is populated with additional information about this unmanaged VNet.

**Step 8** Click **Select**.

You are returned to the main **Import Brownfield Virtual Network** window.

**Step 9** In the **Tenant** field, select the tenant under this subscription that will be associated with this unmanaged cloud context profile.

This unmanaged cloud context profile will be created under this tenant.

- Step 10** In the **VRF** field, select the VRF that will be associated with this unmanaged cloud context profile.
- Step 11** In the **Cloud Context Profile** field, enter a name for this unmanaged cloud context profile.
- Step 12** Click **Advanced Settings** to expand that menu option, if necessary.
- Step 13** In the **VNet Peering** field, click the box next to enable VNet peering for this unmanaged cloud context profile.
- Enabling this VNet peering field allows the Cisco Cloud APIC to create the peering from the infra VNets to the unmanaged VNet on the cloud. For more information, see the "Support for VNet Peering Across Azure Active Directories" section in the [Configuring VNet Peering for Cloud APIC for Azure](#) document.
- Step 14** In the **Cloud APIC Access Privilege** field, determine how the current access policy is set at the VNet (cloud context profile) level.
- Beginning with release 25.0(4), additional access policies are available at the VNet (cloud context profile) level. The access policy is set to Inherit by default, unless you explicitly change the access policy at this level. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.
- The current access policy setting for the cloud context profile is displayed in the following format:
- ```
<inherit setting>(<current access policy>)
```
- For example, if you see this in the **Cloud Access Privilege** for a cloud context profile:
- ```
Inherited(Routing & Security)
```
- That means:
- The access policy for this cloud context profile is set to the Routing & Security access policy
  - This access policy was inherited from the parent level (in this case, the account/tenant level), which was also set to the Routing & Security access policy
- Step 15** If you want to change the access policy, click the scroll-down menu in the **Cloud APIC Access Privilege** field and choose one of the access policies to apply at the VNet (cloud context profile) level.
- **Routing & Security:** The default access policy. If you do not assign an access policy to at the VNet level, then the VNet has the Routing & Security access policy applied to it by default.
- Assigning a Routing & Security access policy to a VNet means that it has full permissions, where it is able to control routing and security.
- **Routing Only:** Assigning a routing-only access policy at the VNet level means that it can control only the routing policy and the network connectivity.
  - **Read Only:** Assigning a read-only access policy at the VNet level means that it does not have write permissions and can only read the inventory.
- Keep in mind that the access policies available to you at the VNet (cloud context profile) level are based on the access policy that was assigned at the parent level (in this case, at the account/tenant level). For example, if the access policy at the parent account/tenant level is set to Read Only, then you will only see Read Only as an option at the child VNet (cloud context profile) level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.
- Step 16** Determine if you want to copy any route tables that are associated with the subnets in the existing VNet that you are importing.
- Beginning with release 25.0(4), you can copy route tables that are associated with the subnets in the existing brownfield (unmanaged) VNet that you are importing. See [About Route Table Copying, on page 13](#) for more information.

- If you do not want to copy any route tables that are associated with the subnets in the existing VNet that you are importing, in the **Copy Existing Routing Tables from VNet** area, click **Do Not Copy Existing Routes**, then go to [Step 17, on page 28](#).
- If you want to copy route tables that are associated with the subnets in the existing VNet that you are importing, in the **Copy Existing Routing Tables from VNet** area, click **Copy Existing Routes**.

The **Brownfield Route Tables** fields appear. Follow the steps below to copy the existing route tables from the brownfield VNet.

- a) Click **Add Brownfield Route Tables**.

The **Select Brownfield Route Tables** page appears, displaying a list of route tables associated with the subnets in the existing brownfield (unmanaged) VNet that you are importing.

- b) Select the route tables that you want to copy, then click **Select**.

### Step 17

In the **Resources to Import** area, select any additional CIDRs available inside the unmanaged VNet that you want to have imported into this unmanaged cloud context profile, if necessary.

The primary CIDR block range in the unmanaged VNet is imported automatically and is tagged as the primary CIDR.

### Step 18

In the **Resources to Import** area, select the subnets inside the unmanaged VNet that you want to have imported into this unmanaged cloud context profile.

If you are copying an existing route table from the brownfield VNet, select the necessary subnets that are associated with the route table that you are copying that you want to import. Make sure that all the desired subnets and their associated route tables are selected for import and copy in order to avoid traffic disruption.

**Note** The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

- a) Click the box in the **Subnet** column to import the corresponding subnets for an imported CIDR.
- b) Determine how the current access policy is set at the subnet level.

Beginning with release 25.0(4), additional access policies are available at the subnet level. The access policy is set to Inherit by default, unless you explicitly change the access policy at this level. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

The current access policy setting for the subnet is displayed in the following format:

```
<inherit setting>(<current access policy>)
```

For example, if you see this in the **Access Privilege** area for a subnet:

```
Inherited(Routing & Security)
```

That means:

- The access policy for this subnet is set to the Routing & Security access policy
- This access policy was inherited from the parent level (in this case, the VNet, or cloud context profile, level), which was also set to the Routing & Security access policy

- c) Click the pencil icon next to the entry in the **Subnet** column to change the access policy at the subnet level.

- **Routing & Security:** The default access policy. If you do not assign an access policy to at the subnet level, then the subnet has the Routing & Security access policy applied to it by default.

Assigning a Routing & Security access policy to a subnet means that it has full permissions, where it is able to control routing and security.

- **Routing Only:** Assigning a routing-only access policy at the subnet level means that it can control only the routing policy and the network connectivity.
- **Read Only:** Assigning a read-only access policy at the subnet level means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the subnet level are based on the access policy that was assigned at the parent level (in this case, at the VNet level). For example, if the access policy at the parent VNet level is set to Read Only, then you will only see Read Only as an option at the child subnet level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 9](#) for more information.

**Step 19** Click **Save** in the **Import Brownfield Virtual Network** window to save this cloud context profile.

A **What's Next** page is displayed.

**Step 20** Click **Go to Cloud Context Profile Details** at the bottom right of the window.

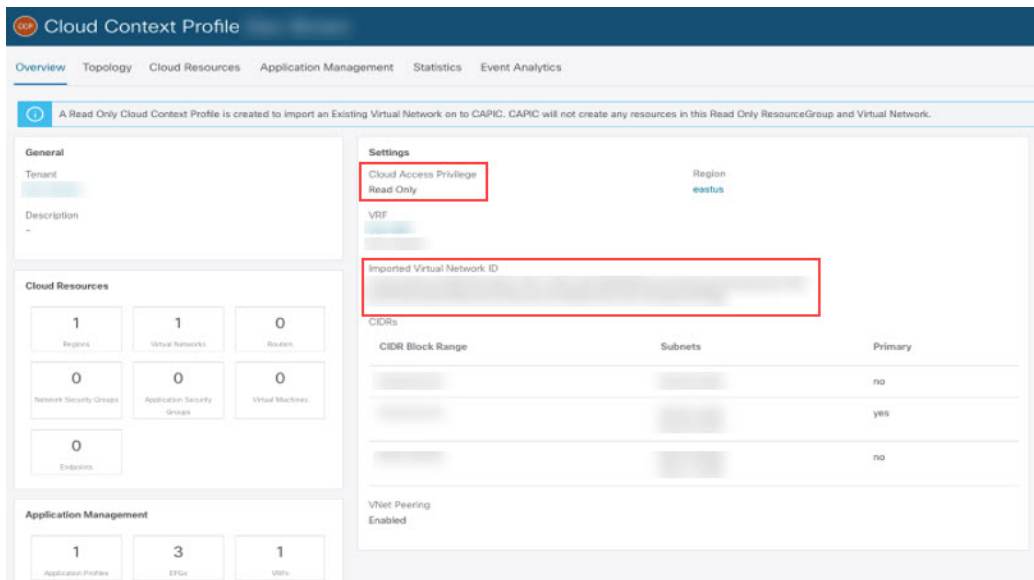
You are returned to the main **Cloud Context Profiles** page, with all the configured cloud context profiles listed.

**Step 21** Locate the unmanaged cloud context profile that you just created and verify that the access policy is displayed correctly in the **Cloud Access Privilege** column for this cloud context profile.

		Application Management					Cloud Resources		
Health	Name	Cloud Access Privilege	Primary CIDR Address	VRF	EPGs	Region	Virtual Networks	Routers	Endpoints
Major	cl_ctxprofile_centralus infra	Read and Write	/25	1	12	1	1	3	10
Healthy	Cto-Brown Dev-Tenant	Read Only	/16	1	0	1	1	1	0
Healthy	Dev-Ctx-EastUS Dev-Tenant	Read and Write	/16	1	1	1	1	1	0
Healthy	HR-CentralUS HR	Read and Write	/16	1	6	1	1	1	0
Healthy	HR-EastUS HR	Read and Write	/16	1	6	1	1	1	0
Healthy	HR-WestUS HR	Read and Write	/16	1	6	1	1	1	0

**Step 22** Click on the unmanaged cloud context profile that you just created to display additional information on this profile.

The following figure shows a configured unmanaged cloud context profile, with the Read Only flag enabled and the associated cloud provider ID.



**Step 23** In the Cisco Cloud APIC GUI, in the left nav bar, click **Application Management > VRFs**.

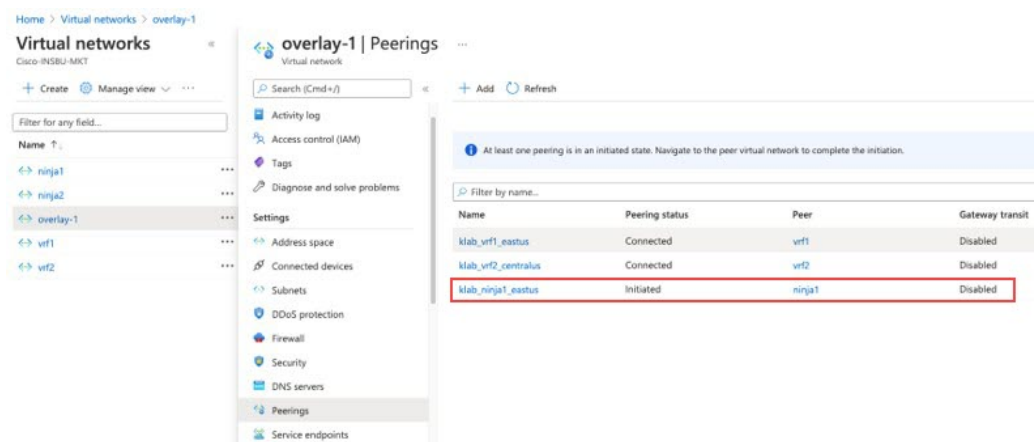
A list of configure VRFs appears.

**Step 24** Locate the VRF that you created earlier in these procedures that would be associated with the cloud context profile for the brownfield VNet and click that VRF.

Verify that the VRF is associated with the imported brownfield VNet.

**Step 25** In the Azure portal, navigate to the **Peerings** area in the **Virtual networks** page for the infra VNet and verify that the VNet peering from the infra (hub) VNet to the unmanaged (brownfield) VNet is configured.

As described in [About VNet Peering for Unmanaged \(Brownfield\) VNets, on page 4](#), because only the first leg of the VNet peering was configured by Cisco Cloud APIC (from the infra VNet to the unmanaged VNet), but the other leg is not yet configured (from the unmanaged VNet to the infra VNet), the **Peering status** will show as **initiated** for this VNet peering, with the unmanaged (brownfield) VNet shown in the **Peer** column.



## What to do next

Configure the other leg of the VNet peering (from the unmanaged VNet to the infra VNet) in Azure using the procedures provided in [Adding Peering from Unmanaged VNet to Infra VNets in Azure](#), on page 31.

## Creating an Unmanaged (Brownfield) Cloud Context Profile Using the REST API

### Before you begin



**Note** The information in this section is applicable if you are running on a release prior to release 25.0(4). For equivalent information for release 25.0(4) and later, including how to configure new access policies that are available beginning with release 25.0(4) see [Configuring Access Policies Using the REST API](#), on page 21.

Review the information provided in [About Unmanaged \(Brownfield\) Cloud Context Profiles](#), on page 24 before going through these procedures.

### Procedure

To create an unmanaged (brownfield) cloud context profile, post the following.

The text in bold shows the lines that are specific to creating an unmanaged cloud context profile, where:

- The `cloudRsCtxProfileToAccessPolicy` line sets the cloud context profile to be Read Only.
- The `cloudBrownfield` lines are used to import a brownfield VNet on the cloud with its cloud provider ID.

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

```
<fvTenant name="tn15">
  <cloudCtxProfile name="cProfilewestus151" status="" azVirtualNetwork="vnet1" status="">
    <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only" status="" />
    <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-westus" status="" />

    <cloudRsToCtx tnFvCtxName="ctx151" />
    <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status="" />
    <cloudBrownfield status="">
      <cloudIDMapping
cloudProviderId="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/BrownfieldResGrp/providers/Microsoft.Network/virtualNetworks/VNET1"
status="" />
      </cloudBrownfield>
    <cloudCidr name="cidr1" addr="xx.10.0.0/16" primary="yes" status="" />
    <cloudCidr name="cidr2" addr="xx.50.0.0/16" primary="no" status="" />
  </cloudCtxProfile>
</fvTenant>
```

## Adding Peering from Unmanaged VNet to Infra VNets in Azure

In this task, you will be programming the VNet peering from the unmanaged (brownfield) VNet to the infra VNets in Azure, as described in [About VNet Peering for Unmanaged \(Brownfield\) VNets](#), on page 4.





## What to do next

Create an EPG to be associated with the brownfield cloud context profile using the procedures provided in [Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI, on page 35](#).

# Creating an EPG Associated With the Brownfield Cloud Context Profile

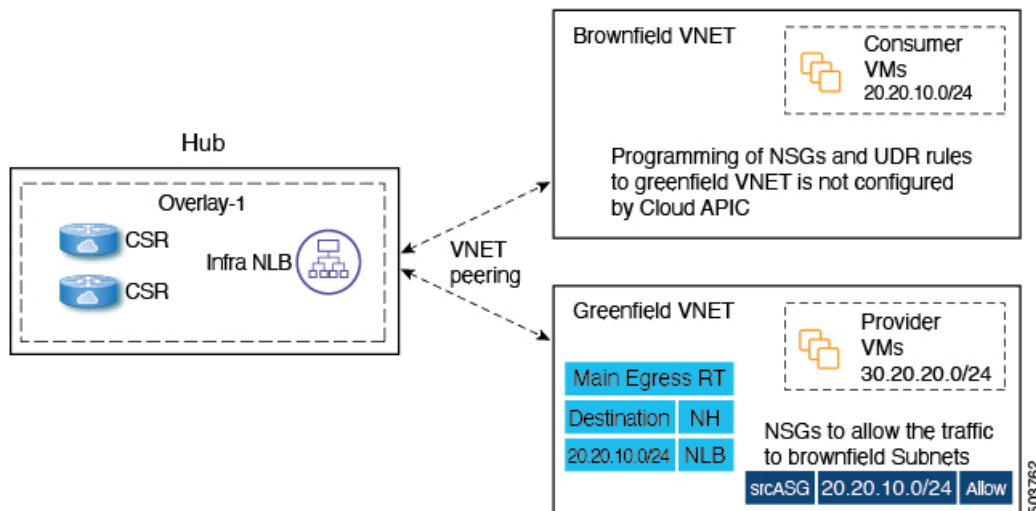
The following topics provide information on creating an EPG associated with the brownfield cloud context profile.

## How EPGs are Associated With Brownfield Cloud Context Profiles Through VRFs

In order to better understand how EPGs are associated with brownfield cloud context profiles through VRFs, it's helpful to compare it to how EPGs are mapped normally:

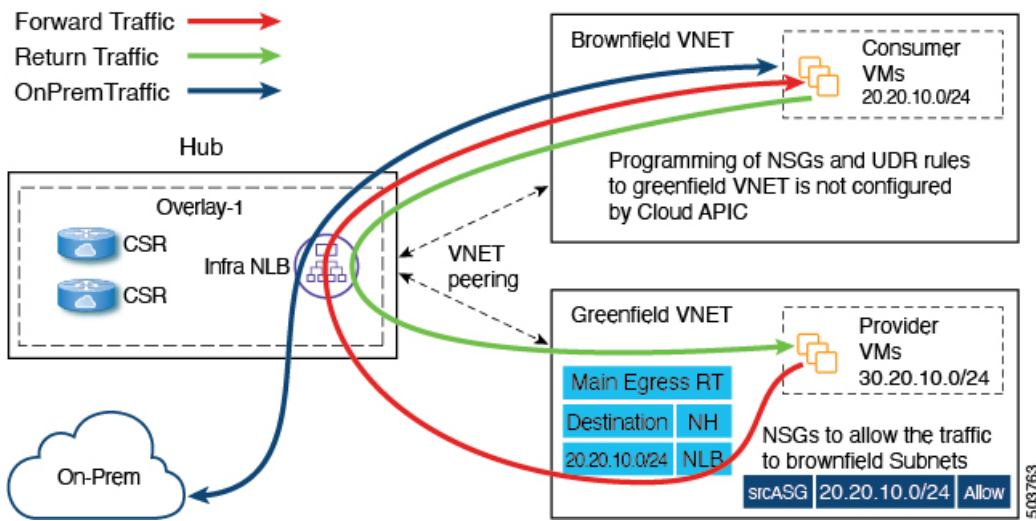
- **Regular EPG mapping:** Typically, when you define a regular cloud EPG, you associate the cloud EPG with a VRF. The cloud context profile also gets associated with the VRF as part of this process. Thus, when an EPG is defined, it gets translated into the appropriate security group under each and every cloud context profile (resource group/VNet), which then gets converted into an ASG in the Azure cloud.
- **EPGs associated with brownfield cloud context profiles:** When an unmanaged (brownfield) cloud context profile is defined and associated with a VRF, and when you define an EPG that is associated with this same VRF, then this EPG can be referred to as an **EPG associated with a brownfield cloud context profile**. The reason for creating an EPG associated with a brownfield cloud context profile is to orchestrate all the networking and security constructs on the greenfield VNet to allow the communication to the brownfield VNet, because everything in the Cisco Cloud APIC, such as security and routing, depends on EPG contracts.

For example, consider the configuration in the following figure:



In this configuration, the reason for creating the EPG that is associated with the brownfield cloud context profile and creating a contract is to provision the routing and security on the greenfield VNet side to allow the traffic to reach this unmanaged VNet.

In this example, the goal is to allow a packet flow on the greenfield VNet to send and receive the packets to 20.20.10.0/24 (rules) and to send the traffic destined to this subnet to the infra NLB and then program the CSR to send the packet to the brownfield VNETs. All of this is achieved using contracts.



Cisco Cloud APIC does not program the route entries or the security group rules on the brownfield VNet side. Instead, Cisco Cloud APIC programs only the greenfield VNet side to send packets to or receive packets from the brownfield VNet subnets, based on the contracts. Cisco Cloud APIC programs the CSR accordingly to make the routing occur between the greenfield VNet and the brownfield VNet.

This is why you create EPGs associated with the brownfield cloud context profiles, so that the other greenfield VNets can send and receive traffic to and from these brownfield VNets.

Note that EPGs associated with the brownfield cloud context profiles should only have subnet-based or exact IP-based endpoint selectors and not tag-based endpoint selectors. Cisco Cloud APIC won't recognize endpoints belonging to an unmanaged VNet. Because of this, Cisco Cloud APIC won't recognize tag-based endpoints belonging to an unmanaged (brownfield) VNet. If Cisco Cloud APIC can't detect the endpoints, then it can't find the IP addresses and therefore can't program the security rules on the greenfield VNet side to send/receive the packets to and from the brownfield VNet side.

The reason to create an EPG that is associated with the brownfield cloud context profile and then define a subnet-based or specific IP-based endpoint selector in that EPG is:

- When you create a contract from this EPG (associated with the brownfield cloud context profile) to another EPG (associated to the greenfield cloud context profile), this drives the programming of the route entries to the unmanaged VNet CIDRs in the route table on the greenfield VNet side.
- This also drives the programming of all the security group rules on the greenfield VNet side to allow the packets to be sent to or received from these subnets defined on the EPG's endpoint selector.
- If an EPG is configured with tag-based endpoint selectors and is associated with the brownfield cloud context profile, then a fault will be raised saying that this EPG cannot be used.

Event Analytics

Faults | Fault Records | Events | Audit Logs

Severity: Minor

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VNF]-addr-[redacted]/group-[uni/m-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudScaleSetNicGroup	Tag-Based EpSelector custom:tag=devmgr is not applicable on the EPG uni/m-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile uni/m-Dev-Tenant/cxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VNF]-addr-[redacted]/group-[uni/m-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudEndPoint	Tag-Based EpSelector custom:tag=devmgr is not applicable on the EPG uni/m-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile uni/m-Dev-Tenant/cxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00

## Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI

In this topic, you will be creating an EPG that is associated with the brownfield cloud context profile. For a better understanding of why you need to do this, see [How EPGs are Associated With Brownfield Cloud Context Profiles Through VRFs, on page 33](#).

### Before you begin

Verify that you have completed all of the previous necessary configurations before going through these procedures, including:

- [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#)
- [Adding Peering from Unmanaged VNet to Infra VNets in Azure, on page 31](#)

### Procedure

---

- Step 1** Click the **Intent** icon.  
The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Create EPG**.  
The **Create EPG** dialog box appears.
- Step 4** Enter the necessary general configurations for the EPG.

*Table 3: Create EPG Dialog Box Fields*

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the EPG.
<b>Tenant</b>	To choose a tenant: <ol style="list-style-type: none"><li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog box appears.</li><li>From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column.  Beginning with Release 5.0(2), you can select the infra tenant and can create cloud EPGs and cloud external EPGs in the infra tenant, as described earlier in this section.</li><li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li></ol>
<b>Application Profile</b>	To choose an application profile: <ol style="list-style-type: none"><li>Click <b>Select Application Profile</b>. The <b>Select Application Profile</b> dialog box appears.</li><li>From the <b>Select Application Profile</b> dialog, click to choose an application profile in the left column.</li><li>Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li></ol>

Properties	Description
<b>Description</b>	Enter a description of the EPG.
<b>Settings</b>	
<b>Type</b>	Because this will be an application EPG, choose <b>Application</b> as the EPG type.
<b>VRF</b>	To choose a VRF: <ul style="list-style-type: none"> <li>a. Click <b>Select VRF</b>. The <b>Select VRF</b> dialog box appears.</li> <li>b. From the <b>Select VRF</b> dialog, click to choose a VRF in the left column.</li> <li>c. Click <b>Select</b>. You return to the <b>Create EPG</b> dialog box.</li> </ul>

**Step 5** In the **Endpoint Selectors** field, define the subnet-based or specific IP-based endpoint selector corresponding to the Azure brownfield site.

For more information, see [How EPGs are Associated With Brownfield Cloud Context Profiles Through VRFs, on page 33](#).

- a) Click **Add Endpoint Selector** to add an endpoint selector.
- b) Enter a name in the **Name** field.
- c) Enter the following information in the **Match Expressions** area:

- **Key:** Choose **IP**.

- **Operator:** Choose **equals (==)**.

- **Value:** Enter the appropriate subnet-based or specific IP-based IP endpoint.

For example, this could be the **Private IP address** for the virtual machine in the resource group for the brownfield VNet that you want to import into Cloud APIC.

- d) Click the checkmark to accept these values for this match expression.
- e) Click **Add** to add this endpoint selector.

**Step 6** Click **Save** to save this EPG.

### What to do next

Configure a contract between the EPGs using the procedures provided in [Creating a Contract Between the EPGs Using the GUI, on page 36](#).

## Creating a Contract Between the EPGs Using the GUI

In this topic, you will be creating a contract to be used from the EPG associated with the brownfield cloud context profile to the EPG associated with the greenfield cloud context profile. This is done to drive the programming of the route entries to the unmanaged VNet CIDRs in the route table in the greenfield VNet side. This also drives the programming of all the security group rules on the greenfield VNet side to allow the packets to be sent to or received from these subnets defined on the EPG's endpoint selector.

## Before you begin

Create an EPG associated with the brownfield cloud context profile using the instructions provided in [Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI, on page 35](#).

## Procedure

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

**Table 4: Create Contract Dialog Box Fields**

Properties	Description
<b>Name</b>	Enter the name of the contract.
<b>Tenant</b>	To choose a tenant: <b>a.</b> Click <b>Select Tenant</b> . The <b>Select Tenant</b> dialog box appears. <b>b.</b> From the <b>Select Tenant</b> dialog, click to choose a tenant in the left column. <b>Note</b> Beginning in Release 5.0(2), you can create contracts in the infra tenant. You can also export contracts from and import contracts to the infra tenant for shared services use cases. <b>c.</b> Click <b>Select</b> . You return to the <b>Create Contract</b> dialog box.
<b>Description</b>	Enter a description of the contract.
<b>Settings</b>	
<b>Scope</b>	Choose <b>Global</b> from the drop-down menu. This enable EPGs in one tenant to communicate with EPGs in another tenant.
<b>Add Filter</b>	To choose a filter: <b>a.</b> Click <b>Add Filter</b> . The filter row appears with a <b>Select Filter</b> option. <b>b.</b> Click <b>Select Filter</b> . The <b>Select Filter</b> dialog box appears. <b>c.</b> From the <b>Select Filter</b> dialog, click to choose a filter in the left column then click <b>Select</b> . You return to the <b>Create Contract</b> dialog box.

- Step 5** Click **Save** when finished.
- Step 6** In the main **Create Contract** window, click **Configure EPG Communication**.

The **EPG Communication Configuration** window appears.

**Step 7** In the **Contract** area, click **Select Contract**.

The **Select Contract** window appears.

**Step 8** Choose the contract that you just created from the list of contracts and click **Select**.

You are returned to the **EPG Communication Configuration** window.

**Step 9** In the **Provider EPGs** area on the right side, click **Add Provider EPGs**.

The **Select Provider EPGs** window appears.

**Step 10** Choose the EPG associated with the greenfield cloud context profile and click **Select**.

You are returned to the **EPG Communication Configuration** window.

**Step 11** In the **Consumer EPGs** area on the right side, click **Add Consumer EPGs**.

The **Select Consumer EPGs** window appears.

**Step 12** Choose the EPG associated with the brownfield cloud context profile and click **Select**.

You are returned to the **EPG Communication Configuration** window.

**Step 13** Click **Save**.

---

## What to do next

Complete the remaining configuration tasks in Azure using the procedures provided in [Completing the Remaining Configurations for the Brownfield VNet in Azure](#), on page 39.

## Creating an EPG Associated With the Brownfield Cloud Context Profile Using the REST API

### Procedure

Create a cloud EPG for the brownfield VNet.

You will be creating a cloud EPG to allow an on-premises site or another cloud site to be able to send or receive the traffic to this unmanaged brownfield VNet.

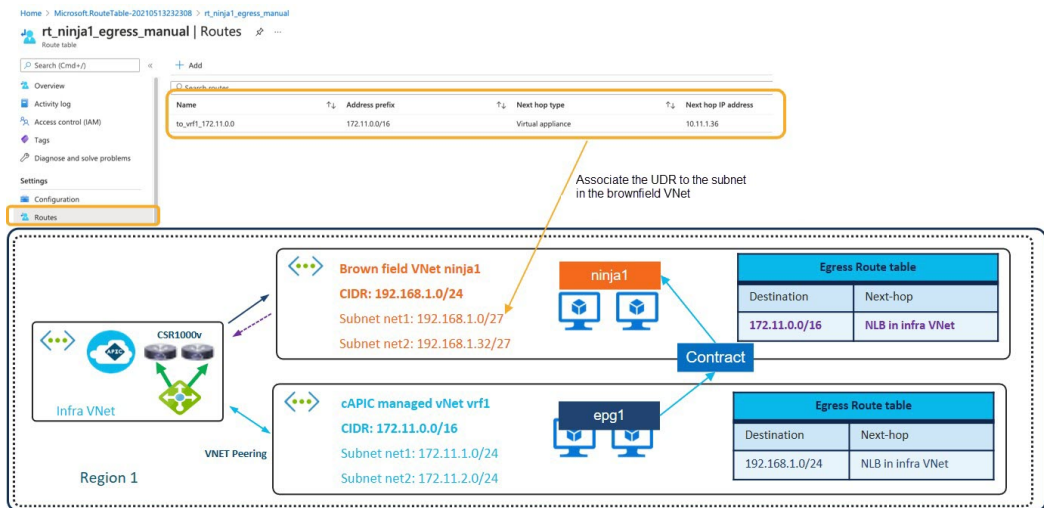
**Note** The endpoint selectors for these brownfield cloud EPGs must be subnet- or IP-based., not tag-based.

```
<fvTenant name="UnManagedTenant1">
  <fvCtx name="VRF" />
  <cloudApp name="UnManagedapp" status="">
    <cloudEPg name="Epg" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="VRF" />
      <cloudEPSelector name="1" subnet="20.0.0.0/24"/>
      <cloudEPSelector name="1" matchExpression="IP=='20.47.0.16/32'"/>
      <fvRsCons status="" tnVzBrCPName="http" />
      <fvRsCons tnVzBrCPName="contract_http_https_ssh" />
    </cloudEPg>
  </cloudApp>
</fvTenant>
```

# Completing the Remaining Configurations for the Brownfield VNet in Azure

In these procedures, you will complete these remaining configurations in Azure:

- Program the UDR rules in the route tables to send and receive packets from the external site subnets. These external subnets should be programmed with the next hop pointing to the private IP of one of the infra NLBs in the hub VNets.



- Program the NSG or ASG rules to allow the security rules to send or receive packets from the external site endpoints or subnets.

The following section provides the general instructions and example configurations to complete these remaining configurations in Azure, but keep in mind that your configuration might be different.

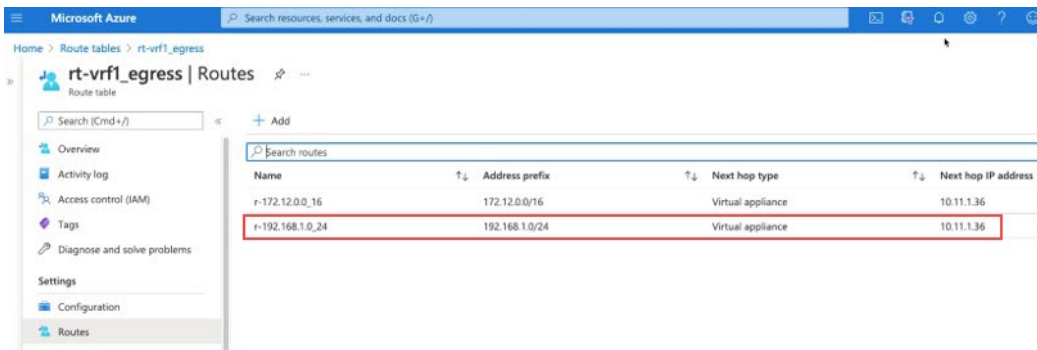
## Before you begin

Verify that you have completed all of the previous necessary configurations before going through these procedures, including:

- [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#)
- [Adding Peering from Unmanaged VNet to Infra VNets in Azure, on page 31](#)
- [Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI, on page 35](#)
- [Creating a Contract Between the EPGs Using the GUI, on page 36](#)

## Procedure

- Step 1** In the Azure portal, verify that the UDR from the Cisco Cloud APIC-managed VRF to the brownfield VRF was configured automatically by Cisco Cloud APIC.
- Search for `Route tables` in the Azure search bar and click the `Route tables` search result. A list of configured route tables appears.
  - Click the route table that was configured for the Cisco Cloud APIC-managed VRF to the brownfield VRF and verify that the UDR is configured correctly in that route table.



**Step 2** Create the UDR from the brownfield VRF to the Cisco Cloud APIC-managed VRF.

This will be a new route table in the brownfield VNet, different from the route table shown in the previous step that was configured for the Cisco Cloud APIC-managed VRF to the brownfield VRF.

- a) Go back a level to the list of route tables, then click + **New** to create a new route table.

The **Create route table** window appears.

- b) Enter the necessary information in the **Create route table** window, then click **Review + create**.

A **Validation Passed** screen appears if the information that you entered in the **Create route table** window was valid.

- c) Click **Create**.

The deployment is submitted, then a screen showing that the deployment is complete appears.

- d) Click **Go to resource**.

The page for the route table that you just created appears.

- e) In the left pane, click **Routes**, then click + **Add**.

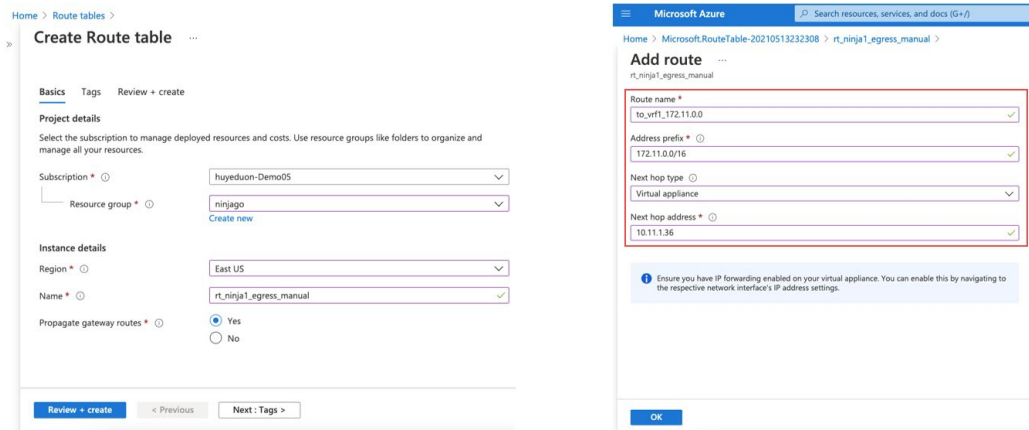
The **Add route** window appears.

- f) Enter the necessary information in the **Add route** window to create the UDR from the brownfield VRF to the Cisco Cloud APIC-managed VRF, then click **OK**.

In the **Add route** page:

- The entry in the **Address prefix** field is the Cisco Cloud APIC-managed VNet CIDR.
- The entry in the **Next hop address** field is the IP address of a properly provisioned NLB in the infra VNet.





### Step 3

Associate the UDR to the subnet in the brownfield VNet.

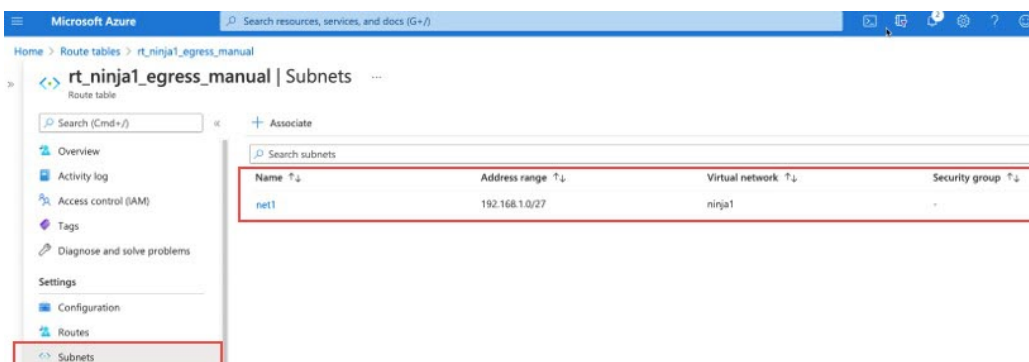
- a) Click **Subnets** in the left nav bar, then click + **Associate**.

The **Associate subnet** pane appears on the right side.

- b) Locate and select the brownfield VNet.

A list of subnets in that VNet appear.

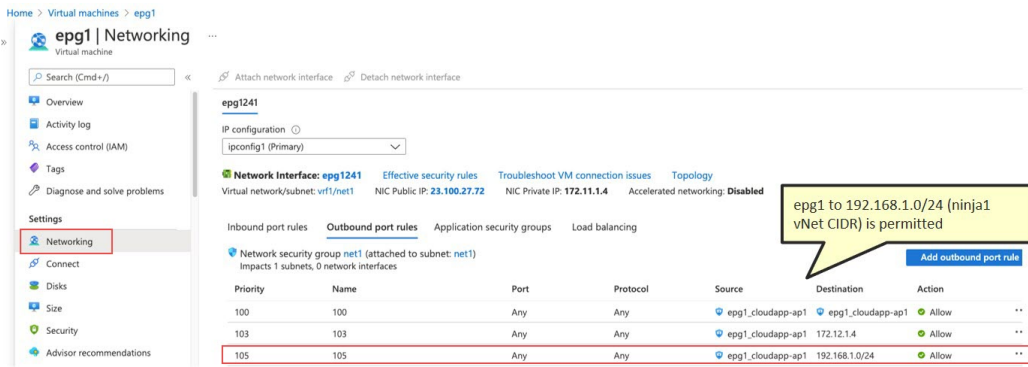
- c) Locate the appropriate subnet in the brownfield VNet that you want to use to associate with the UDR and select that subnet.



### Step 4

Verify the NSG rules for the endpoint associated with the Cisco Cloud APIC-managed VNet.

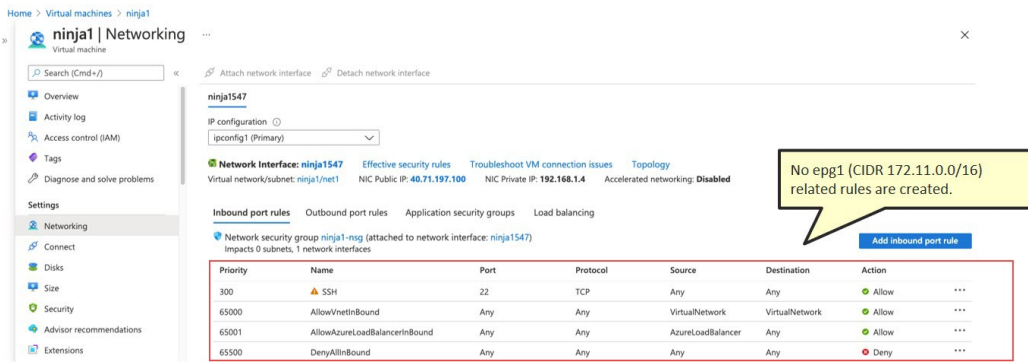
This rule is created for endpoints in the Cisco Cloud APIC-managed VNet automatically by the Cisco Cloud APIC after you applied the contract between the EPG for the Cisco Cloud APIC-managed VNet and the EPG for the brownfield VNet.



**Step 5** Manually configure the NSG rules for the brownfield endpoint.

You must perform a manual configuration for the brownfield VNet, and the method that you use will vary depending on the NSG rules that you are configuring. Following is one example way of manually configuring the NSG rules for the brownfield EPG. In this example, traffic is initiated from the greenfield (Cisco Cloud APIC-managed) EPG `epg1` (172.11.1.4) to the brownfield EPG `ninja1` (192.168.1.4).

In the following example, you can see that there are no rules configured yet for the greenfield (Cisco Cloud APIC-managed) EPG `epg1`.



Configure the inbound rules to permit traffic from the greenfield (Cisco Cloud APIC-managed) EPG.

In this example, we configure the inbound rules to permit traffic from the greenfield (Cisco Cloud APIC-managed) EPG `epg1` (172.11.1.4).

- a) With **Inbound port rules** selected in the area above the table, click **Add inbound port rule**.
- b) Enter the necessary information in the Add inbound security rule window to permit traffic from the greenfield (Cisco Cloud APIC-managed) EPG (in this example, 172.11.1.4 for the Cisco Cloud APIC-managed) EPG `epg1`.

## Add inbound security rule

ninja1-nsg

Source ⓘ

IP Addresses

Source IP addresses/CIDR ranges \* ⓘ

172.11.0.0/16

Source port ranges \* ⓘ

\*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges \* ⓘ

\*

Protocol

Any

TCP

UDP

This example is to permit traffic from 172.11.0.0/16.

- c) Verify that the inbound rules to permit traffic from the greenfield (Cisco Cloud APIC-managed) EPG were configured correctly.

Following is an example brownfield NSG rule after allowing the greenfield subnet.

Home > Virtual machines > ninja1

ninja1 | Networking

Virtual machine

Search (Cmd+I)

Attach network interface Detach network interface

ninja1547

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: **ninja1547** Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: ninja1/net1 NIC Public IP: 40.71.197.100 NIC Private IP: 192.168.1.4 Accelerated networking: Disabled

Manually add an inbound port rule.

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	allow_epg1	Any	Any	172.11.0.0/16	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

### What to do next

Verify the configurations using the procedures provided in [Verifying the Configurations, on page 44](#).

# Verifying the Configurations

## Procedure

---

- 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** Navigate to the resource group for the greenfield VNet.  
a) From the main Azure management portal page, click **Resource groups** in the left nav bar.  
A list of resource groups is displayed.  
b) Locate the resource group for the greenfield VNet and click that resource group.  
The overview information for that resource group is displayed.
- Step 3** Locate the appropriate network security group from the list and click that network security group.  
The overview page for that network security group is displayed.
- Step 4** Verify that the rules for reaching the brownfield site are displayed in the **Inbound Security Rules** and **Outbound Security Rules** tables.
- Step 5** Navigate back to the page for the resource group for the greenfield VNet.  
The overview information for that resource group is displayed.
- Step 6** Locate the entry for the route table from the list and click that route table field.  
The overview page for that route table is displayed.
- Step 7** Verify that the route entries are programmed in the route table to allow traffic to the CIDRs of the brownfield VNet.
- 

## Trademarks

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

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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

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

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

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

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





**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA 95134-1706  
USA

**Asia Pacific Headquarters**  
CiscoSystems(USA)Pte.Ltd.  
Singapore

**Europe Headquarters**  
CiscoSystemsInternationalBV  
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).