



Managing Cisco Cloud APIC Through Cisco ACI Multi-Site

- [About Cisco Cloud APIC and Cisco ACI Multi-Site, on page 1](#)
- [Adding the Cisco Cloud APIC Site to Cisco ACI Multi-Site, on page 2](#)
- [Configuring the Intersite Infrastructure, on page 2](#)
- [Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices, on page 3](#)
- [Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 8](#)
- [Configuring a Tenant, on page 8](#)
- [Adding a Role Assignment, on page 10](#)
- [Creating a Schema, on page 15](#)
- [Configuring an Application Profile and the EPGs, on page 15](#)
- [Creating and Associating a Bridge Domain with a VRF, on page 16](#)
- [Creating a Filter for a Contract, on page 16](#)
- [Creating a Contract, on page 16](#)
- [Adding Sites to the Schema, on page 17](#)
- [Adding an Endpoint Selector, on page 18](#)
- [Verifying the Cisco ACI Multi-Site Configurations, on page 21](#)

About Cisco Cloud APIC and Cisco ACI Multi-Site

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

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

If you are managing an on-premises site along with the Cisco Cloud APIC site, we recommend that you set up your on-premises site before beginning these procedures, if it is not set up already. See the *Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide* for those procedures, located here:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

Adding the Cisco Cloud APIC Site to Cisco ACI Multi-Site

- Step 1** Log in to the ACI Multi-Site Orchestrator, if you aren't already logged in.
- Step 2** In the Main menu, click **Sites**.
- Step 3** In the **Sites List** page, click **ADD SITE**.
- Step 4** In the **Connection Settings** page, perform the following actions:
- In the **NAME** field, enter the site name.
For example, `cloudsite1`.
 - (Optional) In the **LABELS** field, choose or create a label.
 - In the **APIC CONTROLLER URL** field, enter the URL of the Cloud APIC. This is the public IP address allocated by Azure, which will be the same public IP address that you used to log into the Cloud APIC at the beginning of the procedures for configuring Cisco Cloud APIC using the setup wizard.
For example, `https://192.0.2.1`.
 - In the **USERNAME** field, enter a username.
For example, `admin`. Note that you can also register with any account that has the same privilege as `admin`.
 - In the **PASSWORD** field, enter the password.
 - In the **APIC SITE ID** field, enter a unique site ID, if this field is not already populated automatically.
The site ID must be a unique identifier of the Cloud APIC site. The range must be from 1 to 127.
 - Click **SAVE**.
- Step 5** Verify that Cloud APIC site was added correctly.
- If you are managing multiple sites, all sites should be displayed in the Sites screen in the ACI Multi-Site Orchestrator. The ACI Multi-Site Orchestrator automatically detects if the site is an on-premises or a Cloud APIC site.
-

What to do next

Go to [Configuring the Intersite Infrastructure, on page 2](#).

Configuring the Intersite Infrastructure

- Step 1** In the **Sites** screen, click **CONFIGURE INFRA**.
The **Fabric Connectivity Infra** page appears.
- Step 2** In the left pane, under **SITES**, click on the cloud site.

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

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

- If you do *not* want to configure a password between your on-premises site and your cloud site, skip to [Step 4, on page 3](#).
- If you want to configure a password between your on-premises site and your cloud site:
 - a) In the right pane, click on the **BGP Password** field and enter a password.
 - b) Click the Refresh icon at the upper right corner of the CloudSite window.

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

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

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

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

- **Deploy Only:** Select this option if you are configuring Multi-Cloud (cloud site-to-cloud site) connectivity. This option pushes the configuration to the cloud sites and the Cloud APIC site and enables the end-to-end interconnect connectivity between the cloud sites.
- **Deploy & Download IPN Device config files:** Pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect connectivity between the on-premises and the cloud site. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.
- **Download IPN Device config files only:** Downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices



Note Follow the procedures in this section only if you are enabling connectivity between the on-premises site and the cloud site. Skip these procedures if you do not have an on-premises site and go to [Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 8](#).

Follow these procedures to manually enable connectivity between Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device.

By default, the Cisco Cloud APIC will deploy a pair of redundant Cisco Cloud Services Router 1000Vs. The procedures in this section creates two tunnels, one IPsec tunnel from the on-premises IPsec device to each of these Cisco Cloud Services Router 1000Vs.

The following information provides commands for Cisco Cloud Services Router 1000V as your on-premises IPsec termination device. Use similar commands if you are using a different device or platform.

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

- If you selected either the **Deploy & Download IPN Device config files** or the **Download IPN Device config files only** option in ACI Multi-Site Orchestrator as part of the procedures provided in [Configuring the Intersite Infrastructure, on page 2](#), locate the zip file that contains the configuration files for the ISN devices.
- If you are manually locating the information that you need to enable connectivity between the CSRs deployed in Azure and the on-premises IPsec termination device, gather the CSR and Tenant information, as described in the Appendix of the *Cisco Cloud APIC Installation Guide*.

Step 2 Log into the on-premises IPsec device.

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

If you downloaded the configuration files for the ISN devices through ACI Multi-Site Orchestrator, locate the configuration information for the first CSR and enter that configuration information.

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

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

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

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

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

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

interface tunnel <first-CSR-tunnel-ID>
  ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <interface>
```

```

tunnel destination <first-CSR-elastic-IP-address>
tunnel mode ipsec ipv4
tunnel protection ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
ip mtu 1476
ip tcp adjust-mss 1460
ip ospf <process-id> area <area-id>
no shut
exit

```

Where:

- <first-CSR-tunnel-ID> is a unique tunnel ID that you assign to this tunnel.
- <first-CSR-elastic-IP-address> is the elastic IP address of the third network interface of the first CSR.
- <first-CSR-preshared-key> is the preshared key of the first CSR.
- <interface> is the interface that is used for connecting to the Cisco Cloud Services Router 1000V deployed in Azure.
- <peer-tunnel-for-onprem-IPsec-to-first-CSR> is the peer tunnel IP address for the on-premises IPsec device to the first cloud CSR.
- <process-id> is the OSPF process ID.
- <area-id> is the OSPF area ID.

For example:

```

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

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

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

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

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

interface tunnel 1000
  ip address 30.29.1.2 255.255.255.252
  ip virtual-reassembly
  tunnel source GigabitEthernet1
  tunnel destination 192.0.2.20
  tunnel mode ipsec ipv4

```

```

    tunnel protection ipsec profile infra:overlay-1-1000
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit

```

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

If you downloaded the configuration files for the ISN devices through ACI Multi-Site Orchestrator, locate the configuration information for the second CSR and enter that configuration information.

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

```

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

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

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

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

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

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

```

For example:

```

crypto isakmp policy 1
  encryption aes
  authentication pre-share

```

```

    group 2
    lifetime 86400
    hash sha
exit

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

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

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

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

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

```

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

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

For example:

```

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

```

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

Creating a Security Domain Using the Cisco Cloud APIC GUI

A security domain restricts the tenant to the security domains that you add. If you do not add a security domain, all security domains will have access to this tenant. You will be given the choice of choosing these security domains when you configure a shared tenant using the procedures in [Configuring a Tenant, on page 8](#).

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

-
- Step 1** Log into your Cloud APIC system.
- Step 2** Click the **Intent** icon. The **Intent** menu appears.
- Step 3** Click the drop-down arrow below the **Intent** search box and choose **Administrative**.
A list of **Administrative** options appear in the **Intent** menu.
- Step 4** From the **Administrative** list in the **Intent** menu, click **Create Security Domain**. The **Create Security Domain** dialog box appears.
- Step 5** In the **Name** field, enter the name of the security domain.
- Step 6** In the **Description** field, enter a description of the security domain.
- Step 7** Click **Save** when finished.
-

Configuring a Tenant

When configuring a tenant, you can use either of these subscriptions:

- A new subscription specifically for this tenant.
- The already-existing infra tenant subscription where the Cloud APIC is currently running, because you can share subscriptions in Azure.
- Another user tenant subscription, because you can share with another user tenant subscription in Azure.

Use the procedures in this section to configure a tenant that is shared between the on-premises site and the Cloud APIC site.

-
- Step 1** Log in to your Multi-Site Orchestrator GUI.
- Step 2** In the left navigation menu, click **Tenants**.
- Step 3** In the main pane, click **Add Tenant**.
- Step 4** In the **Add Tenant** window, provide a name for the tenant.
You may also choose to provide a description of the tenant.
- Step 5** If the tenant needs to be deployed to an on-premises site, in the **Associated Sites** area, select the on-premises site by checking the check box next to it.
(Optional) You can also choose a security domain from the drop-down list for the site.

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

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

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

Step 8 Select the mode for the Azure account.

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

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

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

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

For more information, see [Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 8](#).

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

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

In this case, you must also provide the application's credentials to the Cloud APIC. Refer to the information that you saved at the end of the procedures in [Creating an Application in Azure](#):

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

Note You will also have to add a role assignment for the app in this case. More information on those steps are provided at the end of this procedure.

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

Note You will also have to add a role assignment for the VM in this case. More information on those steps are provided at the end of this procedure.

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

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

If you choose **Select Shared**, you can then select a cloud account from the drop-down list. The cloud accounts available in the drop-down list are based on the security domain that you selected in [Step 7, on page 9](#). Your new tenant will be associated with the same Azure subscription as the selected account.

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

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

Step 10 (Optional) Enable consistency checker.

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

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

What to do next

Go to [Adding a Role Assignment, on page 10](#) to determine if you need to add a role assignment for the VM or the application.

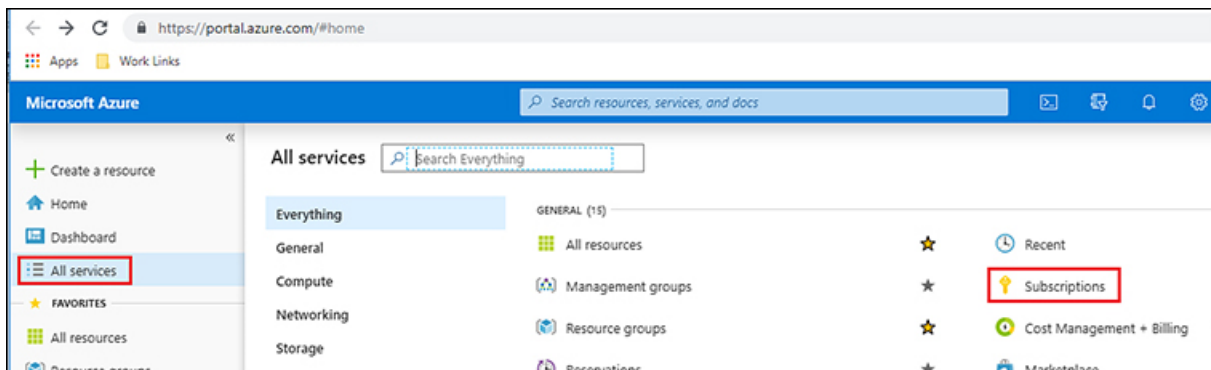
Adding a Role Assignment

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

- In the **Associate Account** page, if you made one of the following selections:
 - You chose **Mode: Create Own** and you selected **Managed Identity** in the **Associate Account** page, or
 - You chose **Mode: Select Shared** and you are sharing with the infra tenant
- Then you must also add a role assignment for the user tenant. Go to [Adding a Role Assignment for a VM, on page 12](#).
- If you selected **Unmanaged Identity** in the **Associate Account** page, then the cloud resources will be managed through a specific application. Go to [Adding a Role Assignment for an App, on page 10](#).

Adding a Role Assignment for an App

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



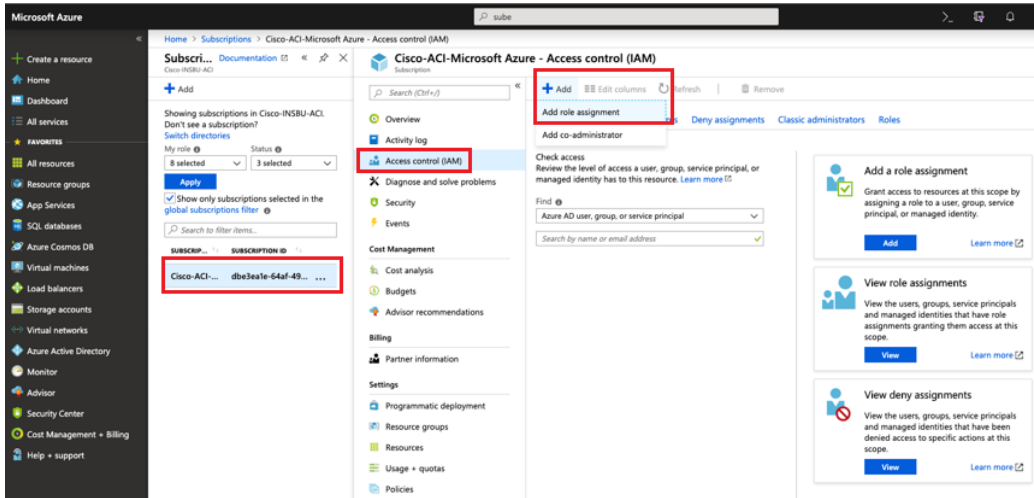
Step 2 In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

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

The Access Control page for that subscription is displayed.

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



Step 5 In the **Add role assignment** page, make the following selections:

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

Add role assignment ✕

Role ⓘ

Contributor ▼

Assign access to ⓘ

Azure AD user, group, or service principal ▼

Select ⓘ

App1 ✓

Selected members:

App1

Remove

Save

Discard

Step 6 Click **Save** at the bottom of the screen.

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

What to do next

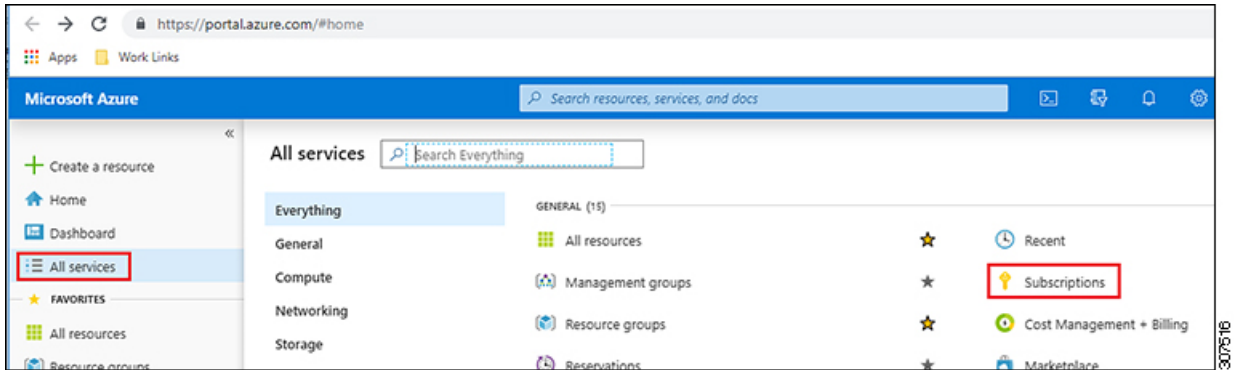
Go to [Creating a Schema, on page 15](#) to create a schema.

Adding a Role Assignment for a VM

- If you chose **Managed Identity** in the **Access Type** field in [Step 8, on page 9](#), then you must also add a role assignment for the user tenant using the procedures in this section.

- If you chose **Unmanaged Identity** in the **Access Type** field in [Step 8, on page 9](#), then you do *not* have to add a role assignment for the user tenant. Skip to [Creating a Schema, on page 15](#) in that case.

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

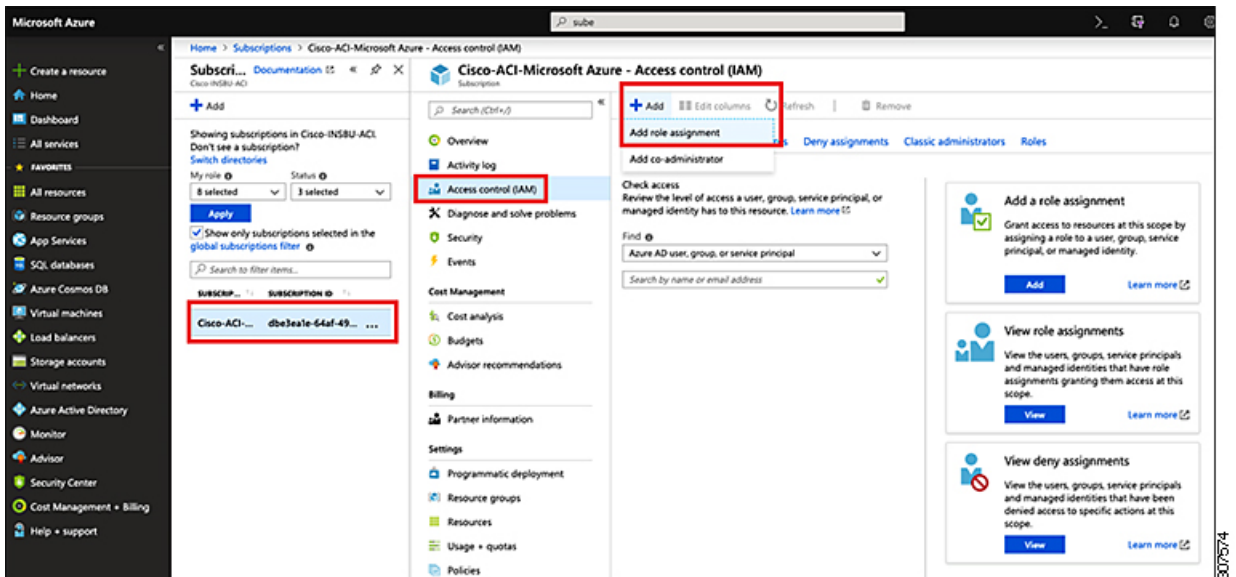


Step 2 In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

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

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



Step 5 In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **Contributor** from the drop-down menu.

- In the **Assign access to** field, select **Virtual Machine**.
- In the **Subscription** field, select the subscription where the Cloud APIC is deployed.
- Select the Cloud APIC virtual machine.


Add role assignment ✕

Role ⓘ
Contributor

Assign access to ⓘ
Virtual Machine

* Subscription
Azure-Demo

Select ⓘ
Search by name


CloudApic-4-2-0221
 /subscriptions/b01b49fb-18e4-4e8c-ac02-445cdfd2...

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

[Learn more about RBAC](#)

Save
Discard

307573

Step 6 Click **Save** at the bottom of the screen.

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

What to do next

Go to [Creating a Schema, on page 15](#) to create a schema.

Creating a Schema

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

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

If you already have a schema that you want to use for the Cisco Cloud APIC site, you can skip these steps and go straight to [Adding Sites to the Schema, on page 17](#).

-
- Step 1** In the Main menu, click **Schemas**.
 - Step 2** On the Schema page, click the **Add Schema** button.
 - Step 3** On the Untitled Schema page, replace the text `Untitled Schema` at the top of the page with a name for the schema that you intend to create (for example, `Cloudbursting-Schema`).
 - Step 4** In the left pane, click **Template 1**.
 - Step 5** In the middle pane, click the area **To build your schema please click here to select a tenant**.
 - Step 6** In the right pane, access the **Select A Tenant** dialog box and select the tenant that you created in [Configuring a Tenant, on page 8](#) from the drop-down menu.
-

Configuring an Application Profile and the EPGs

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

-
- Step 1** In the middle pane, locate the Application Profile area, then click + **Application Profile**.
 - Step 2** In the right pane, enter the Application Profile name in the **DISPLAY NAME** field.
 - Step 3** In the middle pane, click + **Add EPG** to create an EPG for the cloud site.
 - Step 4** In the right pane, enter an EPG name in the **DISPLAY NAME** field (for example, `epg1`).
 - Step 5** In the middle pane, click + **Add EPG** again, if you want to create an EPG for the on-premises site.
 - Step 6** In the right pane, enter an EPG name in the **DISPLAY NAME** field (for example, `epg2`).
 - Step 7** Create a VRF:
 - a) In the middle pane, scroll down until you see the VRF area, then click the + in the dotted box.
 - b) In the right pane, enter the VRF name in the **DISPLAY NAME** field (for example, `vrf1`).
 - Step 8** Click **SAVE**.
-

Creating and Associating a Bridge Domain with a VRF

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

-
- Step 1** In the middle pane, scroll back up to **EPG** and click on the EPG that you created earlier for the on-premises site.
 - Step 2** In the right pane, in the **ON-PREM PROPERTIES** area, under **BRIDGE DOMAIN**, create a new bridge domain by typing a name in the field (for example, bd1), then click the **Create** area.
 - Step 3** In the middle pane, click the bridge domain that you just created.
 - Step 4** In the **Virtual Routing & Forwarding** field, select the VRF that you created in [Configuring an Application Profile and the EPGs, on page 15](#).
 - Step 5** Scroll down to the **SUBNETS** area and click on the + next to **SUBNET** under the **GATEWAY** heading.
 - Step 6** On the **Add Subnet** dialog, enter the **Gateway IP** address and a description for the subnet you plan to add. The Gateway IP address is the on-premises subnet.
 - Step 7** In the **Scope** field, select **Advertised Externally**.
 - Step 8** Click **SAVE**.
-

Creating a Filter for a Contract

-
- Step 1** In the middle pane, scroll down until you see the Filter area, then click + in the dotted box.
 - Step 2** In the right pane, enter a name for the filter in the **DISPLAY NAME** field.
 - Step 3** Click + **Entry** to provide information for your schema filter on the **Add Entry** display:
 - a) Enter a name for the schema filter entry in the **Name** field on the **Add Entry** dialog.
 - b) Optional. Enter a description for the filter in the **Description** field.
 - c) Enter the details as appropriate to filter EPG communication.

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

 TYPE: IP, IP PROTOCOL: TCP, and DESTINATION PORT RANGE FROM and DESTINATION PORT RANGE TO: https.
 - d) Click **SAVE**.
-

Creating a Contract

-
- Step 1** In the middle pane, scroll down until you see the Contract area, then click + in the dotted box.
 - Step 2** In the right pane, enter a name for the contract in the **DISPLAY NAME** field.
 - Step 3** In the **SCOPE** area, leave the selection at VRF.

- Step 4** In the **FILTER CHAIN** area, click + **FILTER**.
The Add Filter Chain screen appears.
- Step 5** In the **NAME** field, select the filter that you created in [Creating a Filter for a Contract, on page 16](#).
- Step 6** In the middle pane, scroll back up to **EPG** and click on the EPG that you created for the cloud site.
- Step 7** In the right pane, click + **CONTRACT**.
The Add Contract screen appears.
- Step 8** In the **CONTRACT** field, select the contract that you created earlier in this procedure.
- Step 9** In the **TYPE** field, select either **CONSUMER** or **PROVIDER**.
- Step 10** Scroll to the **CLOUD PROPERTIES** area, then, in the **VIRTUAL ROUTING & FORWARDING** area, choose the VRF that you created in [Configuring an Application Profile and the EPGs, on page 15](#).
- Step 11** Click **SAVE**.
- Step 12** In the middle pane, scroll back up to **EPG** and click on the EPG that you created for the on-premises site.
- Step 13** In the right pane, click + **CONTRACT**.
The Add Contract screen appears.
- Step 14** In the **CONTRACT** field, select the same contract that you created earlier in this procedure.
- Step 15** In the **TYPE** field, select either **CONSUMER** or **PROVIDER**, whatever you did not select for the previous EPG.
For example, if you selected **PROVIDER** for the first EPG, select **CONSUMER** for the second EPG.
- Step 16** Scroll to the **CLOUD PROPERTIES** area, then, in the **VIRTUAL ROUTING & FORWARDING** area, choose the same VRF that you created in [Configuring an Application Profile and the EPGs, on page 15](#).

Adding Sites to the Schema

- Step 1** In the left pane, click the + next to **Sites**.
- Step 2** On the **Add Sites** page, add the on-premises and cloud sites to the schema by checking the box next to each, then click **Save**.
- Step 3** Click on the template underneath the cloud site in the left pane to configure the site local properties for the template.
- Step 4** In the middle pane, click on the VRF.
- Step 5** In the right pane, in the **SITE LOCAL PROPERTIES** area, enter the following information:
- In the **REGIONS** field, select the Azure region that this VRF will be deployed on.
 - In the **CIDRS** field, click +**CIDR**.
- The **ADD CLOUD CIDR** dialog appears. Enter the following information:
- **CIDR** — Enter the VNET CIDR information. For example, 11.11.0.0/16.
The CIDR includes the scope of all subnets that are going to be available to an Azure VNET.
 - **CIDR TYPE** — Select Primary or Secondary. If this is your first CIDR, select Primary for the CIDR type.
 - **ADD SUBNETS** — Enter the subnet information, then click the check mark. For example, 11.11.1.0/24.

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

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

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

Adding an Endpoint Selector

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

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

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

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

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

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

Step 2 Log into the ACI Multi-Site Orchestrator, if you aren't already logged in.

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

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

- If you want to create an endpoint selector that could be applied to any additional cloud site in the future, follow these procedures:
 1. In the left pane, leave the template selected.
Do not select a specific site for these procedures.
 2. In the middle pane, select the EPG that you created for the cloud site.
 3. In the right pane, in the **CLOUD PROPERITES** area, click + next to **SELECTORS** to configure the endpoint selector.
 4. In the **Add New End Point Selector** dialog, enter a name in the **END POINT SELECTOR NAME** field, based on the classification that you use for this endpoint selector.

5. Click + **Expression**, then select the type of endpoint selector.
For an endpoint selector created this way, the only option available under the Key field is EPG.
 6. Go to [Step 5, on page 19](#).
- If you want to create an endpoint selector specifically for this cloud site, follow these procedures:
 1. In the left pane, select the cloud site.
 2. In the middle pane, select the EPG that you created for the cloud site.
 3. In the right pane, in the **SITE LOCAL PROPERTIES** area, under the **SELECTORS** area, click + next to **SELECTOR** to configure the endpoint selector.
 4. In the **Add New End Point Selector** dialog, enter a name in the **END POINT SELECTOR NAME** field, based on the classification that you use for this endpoint selector.
For example, for an endpoint selector with the IP Subnet classification, you might use a name such as IP-Subnet-EPSelector.
 5. Click + **Expression**, then select the key that you want to use for the endpoint selector.
 - **IP Address:** Used to select by the IP address or subnet. The value for an IP address as an endpoint selector should fall under the user subnet created under the CIDR in [Adding Sites to the Schema, on page 17](#).
In addition, specifically for Azure scale set VMs, the value for an IP address as an endpoint selector must be a complete subnet that was configured in [Adding Sites to the Schema, on page 17](#) where that scale set resides. It cannot be an IP address within the subnet.
For example, if you used the following values in these fields for Azure scale set VMs:
 - **CIDR:** 10.1.0.0/16
 - **Subnet:** 10.1.0.0/24Then a valid value for an IP address as an endpoint selector would be 10.1.0.0/24. Entries of 10.1.0.1/32 or 10.1.0.0/16 would not be valid values for an IP address as an endpoint for Azure scale set VMs.
 - **Region:** Used to select by the Azure region of the endpoint.
 - If you want to create a custom tag for the endpoint selector, start typing in the **Type to search or create field** to enter the custom tag or label, then click **Create** on the new field to create a new custom tab or label.
Using the example earlier in these procedures when you were adding a tag in Azure, you might create the custom tag `Location` in this field, to match the `Location` tag that you added in Azure earlier.

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

The options are:

- **Equals:** Used when you have a single value in the Value field.
- **Not Equals:** Used when you have a single value in the Value field.
- **In:** Used when you have multiple comma-separated values in the Value field.

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

Step 6

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

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

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

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

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

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

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

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

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

In this situation, the EPG rules will be applied to all endpoints with the Azure tag key Location, regardless of the location value.

Step 7

Click the checkmark when you have finished creating this endpoint selector expression.

Step 8

Determine if you want to create additional endpoint selector expressions.

If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions. For example, assume you created two sets of expressions under a single endpoint selector:

- Endpoint selector 1, expression 1:
 - **Key:** Region
 - **Operator:** Equals
 - **Value:** eastus
- Endpoint selector 1, expression 2:
 - **Key:** IP

- **Operator:** Equals
- **Value:** 192.0.2.1/24

In this case, if *both* of these expressions are true (if the region is eastus AND if the IP address belongs to subnet 192.0.2.1/24), then that endpoint will be assigned to the Cloud EPG.

Click the checkmark after every additional expression that you want to create under this endpoint selector.

Step 9

When you have finished creating the expressions for this endpoint selector, click **SAVE** in the lower right corner of the **Add New End Point Selector**.

If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you had created endpoint selector 1 as described in the previous step, and then you created a second endpoint selector as described below:

- Endpoint selector 2, expression 1:
 - **Key:** Region
 - **Operator:** In
 - **Value:** centralus, eastus2

In this case:

- If the region is eastus AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions)
OR
- If the region is either centralus or eastus2 (endpoint selector 2 expression)

Then that end point is assigned to the Cloud EPG.

Step 10

When you have finished creating the endpoint selectors, click **SAVE** in the upper right corner.

Step 11

Click on the **DEPLOY TO SITES** button at the top right corner of the screen to deploy the schema to the sites.

You should see a message saying `Successfully Deployed` at this point.

What to do next

Verify that the Cisco ACI Multi-Site areas were configured correctly using the instructions in [Verifying the Cisco ACI Multi-Site Configurations, on page 21](#).

Verifying the Cisco ACI Multi-Site Configurations

Use the procedures in this topic to verify that the configurations that you entered in the ACI Multi-Site Orchestrator are applied correctly.

Step 1

Log into the Cloud APIC and verify the following:

- a) Click on Dashboard and use the information in the Inter-Site Connectivity Status and the Inter-Region Connectivity Status boxes to verify the following:
 - That the tunnels are up from the Cisco Cloud Services Router 1000V on Azure to the ISN (IPsec termination point) on-premises and to the VGWs in the user VNETs.
 - That the OSPF neighbors are coming up between the Cisco Cloud Services Router and the ISN on-premises devices.
 - That the BGP EVPN routes for the VRF show the cloud and on-premises routes, and that the cloud routes are populated through the BGP EVPN in the ACI spine switch.
- b) Click on Application Management → Tenants and verify that the tenants were configured correctly.
- c) Click on Application Management → Application Profiles and verify that the application profiles were configured correctly.
- d) Click on Application Management → EPGs and verify that the EPGs were configured correctly.
- e) Click on Application Management → Contracts and verify that the contracts were configured correctly.
- f) Click on Application Management → VRFs and verify that the VRFs were configured correctly.
- g) Click on Application Management → Cloud Context Profiles and verify that the cloud context profiles were configured correctly.
- h) Click on Cloud Resources → Regions and verify that the regions were configured correctly.
- i) Click on Cloud Resources → VNETs and verify that the VNETs were configured correctly.
- j) Click on Cloud Resources → Cloud Endpoints and verify that the cloud endpoints were configured correctly.
- k) Click on Cloud Resources → Routers and verify that the CSRs were configured correctly.

Step 2 Log into on-premises APIC site and verify the schema in APIC.

You should see the shared tenant that you configured in the ACI Multi-Site Orchestrator is displayed in the tenants area in APIC and the VRF and EPG deployed from the ACI Multi-Site Orchestrator schema is configured in the on-premises APIC.

Step 3 From a command line, verify that the VRFs were created properly on the Cisco Cloud Services Router 1000V on Azure:

```
show vrf
```

If the tenant `t1` and the VRF `v1` is deployed from the ACI Multi-Site Orchestrator, the CSR output will be similar to the following:

Name	Default RD	Protocols	Interfaces
t1:v1	64514:3080192	ipv4	BD1 Tu4 Tu5

Step 4 From a command line, verify that the tunnels are up between the Cisco Cloud Services Router 1000V on Azure and the ISN on-premises devices.

You can run the following command on either the Cisco Cloud Services Router 1000V on Azure or on the ISN on-premises devices.

```
show ip interface brief | inc Tunnel
```

Output similar to the following should appear:

Interface	IP-Address	OK?	Method	Status	Protocol
Tunnell	1.2.3.22	YES	manual	up	up

Tunnel2	1.2.3.30	YES	manual	up	up
Tunnel3	1.2.3.6	YES	manual	up	up
Tunnel4	1.2.3.14	YES	manual	up	up

Step 5 From a command line, verify that the OSPF neighbors are up between the Cisco Cloud Services Router 1000V on Azure and the ISN on-premises devices:

```
show ip ospf neighbor
```

Output similar to the following should appear:

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.200.10.201	0	FULL/ -	00:00:36	1.2.3.13	Tunnel4
20.30.40.50	0	FULL/ -	00:00:36	1.2.3.29	Tunnel2
10.202.101.202	0	FULL/ -	00:00:38	1.2.3.5	Tunnel3

Step 6 From a command line, verify that the on-premises BGP EVPN neighbors are present in the Cisco Cloud Services Router 1000V:

```
show bgp l2vpn evpn summary
```

Output similar to the following should appear:

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.2	4	100	139	137	99	0	0	01:30:36	6

Step 7 From a command line, verify that the BGP routes for the VRF show both the cloud and on-premises routes.

Note In the current Cloud APIC workflow, a VRF will not be configured on the Cisco Cloud Services Router 1000V until the corresponding VNET is created in Azure.

```
show ip route vrf t1:v1
```

Output similar to the following should appear:

```
B    129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B    130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```

