# Configuring Cisco Cloud APIC Components



# About Configuring the Cisco Cloud APIC

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

**Note**

- For information about configuring a load balancer and service graph, see Deploying Layer 4 to Layer 7 Services.
- For information about the GUI, such as navigation and a list of configurable components, see About the Cisco Cloud APIC GUI.

# Configuring the Cisco Cloud APIC Using the GUI

## Creating a Tenant Using the Cisco Cloud APIC GUI For Release 4.2(2) and Earlier

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

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

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

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

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

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

*Table 1: Create Tenant Dialog Box Fields*

| Properties | Description |
|---|---|
| **Name** | Enter the name of the tenant. |
| **Description** | Enter a description of the tenant. |
| **Settings** | |
| **Add Security Domain** | To add a security domain:<br>**a.** Click **Add Security Domain**. The **Select Security Domains** dialog appears with a list of security domains in the left pane.<br>**b.** Click to choose a security domain.<br>**c.** Click **Select** to add the security domain to the tenant. |
| **Trusted Tenant** | Click to check (default) or uncheck the **Enabled** check box. **Trusted Tenant** is enabled when checked. |
| **Cloud Account ID** | Enter the cloud account ID. |

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

# Creating a Tenant Using the Cisco Cloud APIC GUI For Release 4.2(3) and Later

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

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

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

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

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

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

*Table 2: Create Tenant Dialog Box Fields*

| Properties | Description |
|---|---|
| **Name** | Enter the name of the tenant. |
| **Description** | Enter a description of the tenant. |
| **Settings** | |

| Properties | Description |
|---|---|
| **Add Security Domain** | To add a security domain:<br>**a.** Click **Add Security Domain**. The **Select Security Domains** dialog appears with a list of security domains in the left pane.<br>**b.** Click to choose a security domain.<br>**c.** Click **Select** to add the security domain to the tenant. |
| **AWS Account ID** | Enter the cloud account ID. |
| **Access Type** | Click to enable the tenant type:<br>• **Untrusted**<br>• **Trusted**<br>• **Organization** |

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

# Configure a Tenant AWS Provider For Release 4.2(2) and Earlier

### Before you begin

- AWS Provider is auto-configured for Infra tenant. You do not need to do anything to configure the AWS provider for the infra tenant.
- For all non-infra tenants, the AWS provider is configured either as a trusted tenant or as untrusted tenant. Our recommendation is to use trusted tenants because managing credentials is not easy. Also, each tenant must be in a separate AWS account. Sharing the same AWS account for multiple tenants is not allowed.

  For a trusted tenant, establish the trust relationship first with the account in which Cisco Cloud APIC is deployed (the account for the infra tenant). To establish the trust relation and give all the required permissions to the Cisco Cloud APIC for accessing the tenant account, run the tenant role cloud-formation template in the tenant account. This template is available as a tenant-cft.json object in the S3 bucket that is named capic-common-[capicAccountId]-data in the infra tenant's AWS account. For security reasons, public access to this S3 bucket is not allowed, so the S3 bucket owner needs to download this file and use it in the tenant account.
- Untrusted tenants - use the account access and secret keys. The access and secret keys being used must be for an IAM user having these permissions at a minimum. The IAM role created must be named `ApicTenantRole`.

**Note** Cloud APIC does not disturb AWS resources created by other applications or users. It only manages the AWS resources created by itself.

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "events:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "logs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudtrail:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "resource-groups:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "sqs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "elasticloadbalancing:*",
            "Resource": "*",
           "Effect": "Allow"
        }, {
            "Action": [
                "config:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::<account-id>:role/ApicTenantRole",
```

```
            "Effect": "Allow"
        }
    ]
}
```

- Add trust relationship:

```
 {
    "Version": "2012-10-17",
    "Statement": [
       {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpc-flow-logs.amazonaws.com",
                "AWS": "arn:aws:iam::<account-d>:root"
            },
            "Action": "sts:AssumeRole"
       }
    ]
}
```

- Cloud APIC enforces ownership checks to prevent deployment of policies in the same tenant-region combination done either intentionally or by mistake. For example, assume that Cloud APIC is deployed in AWS account IA1 in region R1. Now you want to deploy a tenant TA1 in region R2. This tenant deployment i.e. account-region combination TA1-R2 is now owned by IA1-R1. If another Cloud APIC attempts to manage the same tenant-region combination later (say Capic2 in AWS account IA2 deployed in region R3), this will not be allowed because the current owner for the deployment TA1-R2 is IA1-R1. In other words, only one account in one region can be managed by one Cloud APIC. Example below shows some valid and wrong deployment combinations.

```
Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- Ownership enforcement is done using AWS Resource Groups. When a new tenant in account TA1 in region R2 is managed by Cloud APIC, a Resource Group CAPIC_TA1_R2 (e.g. CAPIC_123456789012_us-east-2) is created in the tenant account. This Resource Group has a resource tag AciOwnerTag with value IA1_R1_TA1_R2, assuming it was managed by Cloud APIC in account IA1 and deployed in region R1. If the AciOwnerTag mismatch happens, tenant-region management is aborted.

  Here is a summary of AciOwnerTag mismatch cases:

  - Initially Cloud APIC is installed in an account, and then taken down and Cloud APIC is installed in a different account. All existing tenant-region deployment will fail.
  - Another Cloud APIC is managing the same tenant-region.

  In ownership mismatch cases, **retry** (to setup tenant-region again) is not currently supported. As a workaround, if you are certain that no other Cloud APIC is managing the same tenant-region combination, logon to the tenant's AWS account and manually remove the affected Resource Group (e.g. CAPIC_123456789012_us-east-2). Next, reload Cloud APIC or delete and add the tenant again.

**Step 1** In the Cloud APIC, configure the AWS Provider.

a) On the **Intent** menu, choose **Tenants** > ***tenant_name*** from the drop-down.

b) In the **Intent** pane, choose **Application Management** > ***tenant_name*** .

**Step 2** Perform the following actions:

a) Confirm there is a check in the **Trusted** Tenant checkbox.

The AWS account must be a Trusted account for the user tenant using the cloud.

b) In the **Cloud Account ID** field, provide the Cloud account ID.

c) Run the tenant role cloud-formation template available at the URL https://capic-common-<infraAccountId>-data.s3.amazonaws.com/tenant-cft.json which is in a s3 bucket in the infra tenant's AWS account.

**Note** Alternatively, keep the trusted flag unchecked and provide the access and secret keys as done normally for any tenant.

**Step 3** Click **Save**.

# Configuring a Tenant AWS Provider For Release 4.2(3) and Later

### Before you begin

- AWS Provider is auto-configured for Infra tenant. You do not need to do anything to configure the AWS provider for the infra tenant.
- For all non-infra tenants, the AWS provider is configured either as a trusted tenant, untrusted tenant, or organization tenant. Our recommendation is to use trusted tenants because managing credentials is not easy. Also, each tenant must be in a separate AWS account. Sharing the same AWS account for multiple tenants is not allowed.

  For a trusted tenant, establish the trust relationship first with the account in which Cisco Cloud APIC is deployed (the account for the infra tenant). To establish the trust relation and give all the required permissions to the Cisco Cloud APIC for accessing the tenant account, first create a tenant and assign the Trusted tag to that tenant as the Access Type. Then, bring up that new trusted tenant again by clicking on the tenant name in the Tenants page, and in the AWS Account area in the tenant window, click the Run the CloudFormation template link.
- Organization tenants are for adding tenant accounts that are part of the organization. This requires deploying the Cisco Cloud APIC in the master account of the organization.
- Untrusted tenants use the account access and secret keys. The access and secret keys being used must be for an IAM user having these permissions at a minimum. The IAM role created must be named `ApicTenantRole`.

**Note** Cloud APIC does not disturb AWS resources created by other applications or users. It only manages the AWS resources created by itself.

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "events:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "logs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudtrail:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "resource-groups:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "sqs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "elasticloadbalancing:*",
            "Resource": "*",
           "Effect": "Allow"
        }, {
            "Action": [
                "config:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::<account-id>:role/ApicTenantRole",
```

```
            "Effect": "Allow"
        }
    ]
}
```

- Add trust relationship:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpc-flow-logs.amazonaws.com",
                "AWS": "arn:aws:iam::<infra-account-id>:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- The Cloud APIC uses the OrganizationAccountAccessRole IAM role to manage policies for AWS Organization tenants.
  - If you created an AWS account within the existing organization in the master account, the OrganizationAccountAccessRole IAM role is automatically assigned to that created AWS account. You do not have to manually configure the OrganizationAccountAccessRole IAM role in AWS in this case.
  - If the master account invited an existing AWS account to join the organization, then you must manually configure the OrganizationAccountAccessRole IAM role in AWS. Configure the OrganizationAccountAccessRole IAM role in AWS for the organization tenant and verify that it has Cloud APIC-related permissions available.

    The OrganizationAccountAccessRole IAM role, together with the SCP (Service Control Policy) used for the organization or the account, must have the minimum permissions that are required by the Cloud APIC to manage policies for the tenants. The access policy requirement is the same as the requirement for the trusted or untrusted tenants.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "events:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "logs:*"
```

```
                ],
                "Resource": "*",
                "Effect": "Allow"
            }, {
                "Action": [
                    "cloudtrail:*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }, {
                "Action": [
                    "cloudwatch:*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }, {
                "Action": [
                    "resource-groups:*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }, {
                "Action": [
                    "sqs:*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }, {
                "Action": "elasticloadbalancing:*",
                "Resource": "*",
               "Effect": "Allow"
            }, {
                "Action": [
                    "config:*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }, {
               "Action": "iam:PassRole",
               "Resource": "*",
               "Effect": "Allow"
              }

        ]
    }
```

To add a trust relationship for an Organization tenant:

```
 {
    "Version": "2012-10-17",
    "Statement": [
       {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpc-flow-logs.amazonaws.com",
                "AWS": "arn:aws:iam::<infra-account-id>:root"
            },
            "Action": "sts:AssumeRole"
       }
    ]
}
```

- Cloud APIC enforces ownership checks to prevent deployment of policies in the same tenant-region combination done either intentionally or by mistake. For example, assume that Cloud APIC is deployed

in AWS account IA1 in region R1. Now you want to deploy a tenant TA1 in region R2. This tenant deployment i.e. account-region combination TA1-R2 is now owned by IA1-R1. If another Cloud APIC attempts to manage the same tenant-region combination later (say Capic2 in AWS account IA2 deployed in region R3), this will not be allowed because the current owner for the deployment TA1-R2 is IA1-R1. In other words, only one account in one region can be managed by one Cloud APIC. Example below shows some valid and wrong deployment combinations.

```
Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- Ownership enforcement is done using AWS Resource Groups. When a new tenant in account TA1 in region R2 is managed by Cloud APIC, a Resource Group CAPIC_TA1_R2 (e.g. CAPIC_123456789012_us-east-2) is created in the tenant account. This Resource Group has a resource tag AciOwnerTag with value IA1_R1_TA1_R2, assuming it was managed by Cloud APIC in account IA1 and deployed in region R1. If the AciOwnerTag mismatch happens, tenant-region management is aborted.

  Here is a summary of AciOwnerTag mismatch cases:

  - Initially Cloud APIC is installed in an account, and then taken down and Cloud APIC is installed in a different account. All existing tenant-region deployment will fail.
  - Another Cloud APIC is managing the same tenant-region.

  In ownership mismatch cases, **retry** (to setup tenant-region again) is not currently supported. As a workaround, if you are certain that no other Cloud APIC is managing the same tenant-region combination, logon to the tenant's AWS account and manually remove the affected Resource Group (e.g. CAPIC_123456789012_us-east-2). Next, reload Cloud APIC or delete and add the tenant again.

**Step 1** In the Cloud APIC, configure the AWS Provider.

a) On the **Intent** menu, choose **Tenants** > ***tenant_name*** from the drop-down.
b) In the **Intent** pane, choose **Application Management** > ***tenant_name*** .

**Step 2** Perform the following actions:

a) In the **AWS Account ID** field, provide the cloud account ID.
b) In the **Access Type** area, choose **Trusted**.

   The AWS account must be a Trusted account for the user tenant that is using the cloud.

c) Click **Save**.
d) Bring up the new trusted tenant again by clicking on the tenant name in the **Tenants** page.

   In the **AWS Account** area in the tenant **Overview** page, you will see the following message: "In order to deploy any configuration from this tenant, you must create a trusted role in the tenant AWS account which will establish trust with the AWS infra account. To do so, open the link below to run the CloudFormation template."

e) Click the **Run the CloudFormation** template link.

This returns you to the AWS sign in page, which should be pre-populated with the necessary AWS account information that you entered earlier in these procedures in the Cloud APIC GUI.

f) Click **Next** in the AWS sign in page after verifying that the sign-in information is correct.

g) Run the tenant role cloud-formation template in the tenant account.

**Note** Alternatively, keep the trusted flag unchecked and provide the access and secret keys as done normally for any tenant.

**Step 3** Click **Save**.

# Creating an Application Profile Using the Cisco Cloud APIC GUI

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

### Before you begin

Create a tenant.

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

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

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

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

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

**Step 5** Choose a tenant:

a) Click **Select Tenant**.

The **Select Tenant** dialog box appears.

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

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

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

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

# Creating a VRF Using the Cisco Cloud APIC GUI

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

### Before you begin

Create a tenant.

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

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

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

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

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

***Table 3: Create VRF Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter a name for the VRF in the **Name** field.<br>All VRFs are assigned a *vrfEncoded* 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 *vrfEncoded* value. To see the *vrfEncoded* value, navigate to **Application Management** > **VRFs** subtab. Click a VRF on the right hand pane and look for *Encoded VRF Name in Cloud Router*. |
| **Tenant** | To choose a tenant:<br>**a.** Click **Select Tenant**. The **Select Tenant** dialog box appears.<br>**b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create VRF** dialog box. |
| **Description** | Enter a description of the VRF. |
| **Settings > IPv4 unicast address family BGP targets** | |
| **Add Filter** | **a.** Click the **Add Route Target** option for the unicast address family BGP target you want to configure.<br>**b.** Click to choose the following options for the **Type** field:<br>• **Export**—The route target can be exported to other VRFs<br>• **Import**—The route target is imported from other VRFs<br>• Enter the route target that can be exported from the current VRF or imported into the current VRF in the **Route Target** text box. |

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

# Creating an External Network Using the Cisco Cloud APIC GUI

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

### Before you begin

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

**Step 1** In the left navigation bar, navigate to **Application Management** > **External Networks**.
The configured external networks are displayed.

**Step 2** Click **Actions**, then choose **Create External Network**.
The **Create External Network** window appears.

**Step 3** Enter the appropriate values in each field as listed in the following *Create External Network Dialog Box Fields* table then continue.

***Table 4: Create External Network Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter the name for the external network. |
| **VRF** | This external VRF will be used for external connectivity with external non-ACI devices. You can create multiple external VRFs for this purpose.<br>This VRF will be identified as an external VRF if the VRF has all three of the following characteristics:<br>• Configured under the infra tenant<br>• Associated with an external network<br>• Not associated with a cloud context profile<br>Any VRF that is associated with an external network becomes an external VRF. The external VRF is not allowed to be associated with a cloud context profile or subnet.<br>To choose an external VRF:<br>**a.** Click **Select VRF**.<br>The **Select VRF** dialog box appears.<br>**b.** From the **Select VRF** dialog, click to choose a VRF in the left column.<br>You can also create a VRF using the **+ Create VRF** option.<br>**c.** Click **Select**.<br>You return to the **Create External Network** dialog box. |

| Properties | Description |
|---|---|
| **Router Type** | Choose the router type:<br>• **CCR**:<br>• For releases prior to 25.0(3), the Cisco Cloud Services Router 1000V<br>• For release 25.0(3) and later, the Cisco Catalyst 8000V<br>• **TGW**: An AWS transit gateway router |
| **Host Router Name** | This field appears if you select **CCR** as the **Router Type**.<br>This field is not editable. The default host router is automatically selected. |
| **Hub Network** | This field appears if you select **TGW** as the **Router Type**.<br>To choose a hub network:<br>**a.** Click **Select Hub Network**.<br>The **Select Hub Network** dialog box appears.<br>**b.** In the **Select Hub Network** dialog box, click the desired hub network from the list and then click **Select**.<br>You are returned to the **Create External Network** page. |
| **Settings** | |
| **Regions** | To choose a region:<br>**a.** Click **Add Regions**.<br>The **Select Regions** dialog box appears.<br>The regions that you selected as part of the First Time Setup are displayed here.<br>**b.** From the **Select Regions** dialog, click to choose a region in the left column then click **Select**.<br>You return to the **Create External Network** dialog box. |

| Properties | Description |
| --- | --- |
| VPN Networks | |

| Properties | Description |
|---|---|
| | The VPN networks entries are used for external connectivity. All configured VPN networks will be applied to all the selected regions.<br><br>To add a VPN network:<br><br>**a.** Click **Add VPN Network**.<br><br>The **Add VPN Network** dialog box appears.<br><br>**b.** In the **Name** field, enter a name for the VPN network.<br><br>**c.** Click **+ Add IPsec Peer**.<br><br>The **Add IPsec Tunnel Destination** window appears.<br><br>**d.** Enter values for the following fields for the IPsec tunnel destination that you want to add:<br><br>• **Public IP of IPSec Tunnel Peer**<br><br>• **Pre-Shared Key**<br><br>• **IKE Version**: Select **ikev1** or **ikev2** for IPsec tunnel connectivity<br><br>• **BGP Peer ASN**<br><br>• **Subnet Pool Name**: Click **Select Subnet Pool Name**.<br><br>The **Select Subnet Pool Name** dialog box appears. Select one of the available subnet pools that are listed, then click **Select**.<br><br>**Note** Additional IPsec tunnel subnet pools can be added in the **External Networks** page, or through the Cloud APIC First Time Set Up, if necessary. For more information on adding additional subnet pools through the Cloud APIC First Time Set Up, see the chapter "Configuring Cisco Cloud APIC Using the Setup Wizard" in the *Cisco Cloud APIC for AWS Installation Guide*, Release 25.0(1)-25.0(4) and later. The subnet pool size should be large enough to accommodate the number of IPsec tunnels that will get created.<br><br>• **IPsec Tunnel Source Interfaces**: Using the entries in this field, the Cisco Cloud APIC creates one IPsec tunnel from each selected source interface to the destination IP address.<br><br>**Note** **ikev2** is the default option in this field. The IPsec tunnel source interfaces feature is supported only with the IKEv2 configuration.<br><br>**gig3** is selected by default. Choose one or more from the following interfaces:<br><br>• **gig2**: The GigabitEthernet2 interface<br><br>• **gig3**: The GigabitEthernet3 interface<br><br>• **gig4**: The GigabitEthernet4 interface<br><br>**Note** After you have configured the IPsec tunnel source interfaces in this external network, you can then configure IPsec tunnel source interfaces in additional networks where tunnels to the same destination can be formed, as described in Routing Policies: Release 25.0(2). |

| Properties | Description |
|---|---|
| | **e.** Click **Add** to add this IPsec tunnel destination.<br>You return to the **Add VPN Network** window.<br>Click **+ Add IPsec Peer** if you want to add another IPsec tunnel destination.<br>**f.** Click **Add** in the **Add VPN Network** dialog box.<br>You return to the **Create External Network** dialog box. |

**Step 4** When you have finished creating the external network, click **Save**.
After you click **Save** in the **Create External Network** window, cloud routers are then configured in AWS.

# Configuring the Global Inter-VRF Route Leak Policy

The global inter-VRF route leak policy feature is introduced in release 25.0(2).

### Before you begin

Review the information provided in Global Inter-VRF Route Leak Policy before making any changes in the **Contract Based Routing** area in the **Cloud APIC Setup** window.

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

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

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

**Step 3** From the **Configuration** list in the **Intent** menu, click **Cloud APIC Setup**.
The **Set up - Overview** dialog box appears.

**Step 4** In the **Contract Based Routing** area, note the current setting for the **Contract Based Routing** field.

The **Contract Based Routing** setting reflects the current internal VRF route leak policy, which is a global policy under the infra tenant where a Boolean flag is used to indicate whether contracts can drive routes in the absence of route maps:

- **Off**: Default setting. Indicates that routes are not leaked based on contracts, and are leaked based on route maps instead.
- **On**: Indicates that routes are leaked based on contracts in the absence of route maps. When enabled, contracts drive routing when route maps are not configured. When route maps exist, route maps always drives routing.

**Step 5** Determine if you want to change the current setting for the **Contract Based Routing** field.

Follow these procedures if you toggle from one setting to another:

- **Toggling from On setting to Off (disabling contract-based routing)**: In this situation, the assumption is that you have contract-based routing configured currently and you want to toggle over to route map-based routing. This can be disruptive if the route map-based routing is not configured before you toggle from contract-based routing to route map-based routing.

  Before toggling from the **On** setting to the **Off** setting in this situation, make the following changes:

a. Between all pairs of VRFs that have existing contracts, enable route map-based route leaking.

   Follow the procedures provided in Configuring Leak Routes Using the Cisco Cloud APIC GUI, on page 18.

b. Disable the contract-based route policy in the global policy.

   Toggle the switch in the **Contract Based Routing** field from the **On** setting to the **Off** setting to toggle from contract-based routing to route map-based routing.

c. Change the routing to reflect any granularity that is required based on the new route map-based routing that you enabled.

- **Toggling from Off setting to On (enabling contract-based routing)**: In this situation, the assumption is that you have route map-based routing configured currently and you want to toggle over to contract-based routing. This is not a disruptive operation, but rather is an additive operation, since both contracts and route maps can be enabled between a pair of VRFs. In that situation, route maps take precedence over contracts when enabling routing. With route map-based routing enabled, adding contract-based routing should be non-disruptive.

  For that reason, you do not have to make any changes before toggling from the **Off** setting to the **On** setting in this situation. However, if you do not want to have both contracts and route maps enabled between a pair of VRFs, and you want to move completely to contract-based routing, you should completely set up contracts between the VRFs and delete the route maps between the VRFs before toggling to the **On** setting in the **Contract Based Routing** field.

**Step 6** If you want to change the current setting for the **Contract Based Routing** area, toggle the setting based on the type of routing that you want.

**Step 7** Click **Done** when you have finished the **Cloud APIC Setup** configurations.

# Configuring Leak Routes Using the Cisco Cloud APIC GUI

The procedures for configuring leak routes using the Cisco Cloud APIC GUI will vary slightly, depending on the release:

- For releases prior to 25.0(2), you can configure an independent routing policy to specify which routes to leak between internal and external VRFs when you are setting up routing between an ACI cloud site and an external destination using the external connectivity feature. See Configuring Inter-VRF Route Leaking Using the Cisco Cloud APIC GUI, on page 18 for those procedures.
- For releases 25.0(2) and later, support is available for route maps-based route leaking between a pair of internal VRFs. See Configuring Leak Routes for Internal VRFs Using the Cisco Cloud APIC GUI, on page 21 for those procedures.

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

Configuring leak routes is part of the release 25.0(1) update where routing and security policies are configured separately. Using inter-VRF routing, you can configure an independent routing policy to specify which routes to leak between internal and external VRFs when you are setting up routing between an ACI cloud site and an external destination using the external connectivity feature. See Understanding Supported Routing and Security Policies for more information.

The external destination must be configured manually using the Enabling Connectivity From the AWS Site to External Devices, on page 23 procedures. The external destination could be another cloud site, an ACI on-premises site or a branch office.

**Note**

- Use these procedures to configure routing policies independent of security policies only between internal and external VRFs, based on updates provided in release 25.0(1).
- Do not use these procedures to configure routing between a pair of internal VRFs; use contracts as you normally would prior to release 25.0(1) in that case.

**Step 1** In the left navigation bar, navigate to **Application Management** > **VRFs**.
The configured VRFs are displayed.

**Step 2** Click the **Leak Routes** tab.
Any already-configured leak routes are displayed.

**Step 3** Click **Actions**, then choose **Create Leak Route**.
The **Create Leak Route** window appears.

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

***Table 5: Create Leak Routes Dialog Box Fields***

| Properties | Description |
|---|---|
| **Source VRF** | To choose a source VRF:<br>**a.** Click **Select a Source VRF**.<br>The **Select a VRF** dialog box appears.<br>**b.** From the **Select a VRF** dialog, click to choose a VRF in the left column to use for the source VRF.<br>Note that the source VRF can be an internal or an external VRF.<br>**c.** Click **Select** to select this source VRF.<br>You return to the **Create Leak Route** dialog box. |
| **Destination VRF** | To choose a destination VRF:<br>**a.** Click **Select a Destination VRF**.<br>The **Select a VRF** dialog box appears.<br>**b.** From the **Select a VRF** dialog, click to choose a VRF in the left column to use for the destination VRF.<br>Note that the destination VRF cannot be an internal VRF if the source VRF is also internal VRF.<br>**c.** Click **Select** to select this destination VRF.<br>You return to the **Create Leak Route** dialog box. |

| Properties | Description |
|---|---|
| **Type** | Choose the type of leaked route that you want to configure:<br>• **Leak All**: Select to configure all routes to leak from the source VRF to the destination VRF.<br>The entry `0.0.0.0/0` is entered automatically in the subnet IP area by default in this case.<br>• **Subnet IP**: Select to configure a specific subnet IP address as the route to leak from the source VRF to the destination VRF. The **Subnet IP** box appears.<br>In the **Subnet IP** box, enter a subnet IP address as the route to leak between VRFs. |

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

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

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

  You are returned to the **Add Leak Route** window. Repeat Step 4, on page 19 through Step 5, on page 20 to configure another route to leak between a pair of VRFs.

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

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

  You are returned to the **Add Leak Route** window. Repeat Step 4, on page 19 through Step 5, on page 20 to configure another route, but this time:
  - In the **Source VRF** field, select the VRF that you had selected as a destination VRF in the previous configuration.
  - In the **Destination VRF** field, select the VRF that you had selected as a source VRF in the previous configuration.

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

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

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

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

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

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

  The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in Step 4, on page 19. Note that the entry in the **Source VRF** is pre-selected and cannot be changed in this situation.

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

  The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in Step 4, on page 19. Note that the entry in the **Destination VRF** is pre-selected and cannot be changed in this situation.

### What to do next

You have now configured the routing policy. Since the routing and security policies are separate, you now need to configure the security policy separately:

- Creating an EPG Using the Cisco Cloud APIC GUI, on page 27: Use these procedures to create an external EPG.
- Creating a Contract Using the Cisco Cloud APIC GUI, on page 32: Use these procedures to create a contract between the external EPG and the cloud EPG.

## Configuring Leak Routes for Internal VRFs Using the Cisco Cloud APIC GUI

Beginning with release 25.0(2), support is available for route maps-based route leaking between a pair of internal VRFs, as described in Route Leaking Between Internal VRFs. This feature is an extension of the routing and security split update provided in release 25.0(1), where routing and security policies are configured separately.

**Step 1** In the left navigation bar, navigate to **Application Management** > **VRFs**.
The configured VRFs are displayed.

**Step 2** Click the **Leak Routes** tab.
Any already-configured leak routes are displayed.

**Step 3** Click **Actions**, then choose **Create Leak Route**.
The **Create Leak Route** window appears.

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

***Table 6: Create Leak Routes Dialog Box Fields***

| Properties | Description |
|---|---|
| **Source VRF** | To choose a source VRF:<br>**a.** Click **Select a Source VRF**.<br>The **Select a VRF** dialog box appears.<br>**b.** From the **Select a VRF** dialog, click to choose a VRF in the left column to use for the source VRF.<br>Because this procedure is for route maps-based route leaking between a pair of internal VRFs, choose an internal VRF for the source VRF.<br>**c.** Click **Select** to select this source VRF.<br>You return to the **Create Leak Route** dialog box. |

| Properties | Description |
|---|---|
| **Destination VRF** | To choose a destination VRF:<br>**a.** Click **Select a Destination VRF**.<br>The **Select a VRF** dialog box appears.<br>**b.** From the **Select a VRF** dialog, click to choose a VRF in the left column to use for the destination VRF.<br>Because this procedure is for route maps-based route leaking between a pair of internal VRFs, choose an internal VRF for the destination VRF.<br>**c.** Click **Select** to select this destination VRF.<br>You return to the **Create Leak Route** dialog box. |
| **Type** | Choose the type of leaked route that you want to configure:<br>• **Leak All**: Select to configure all routes to leak from the source VRF to the destination VRF.<br>The entry `0.0.0.0/0` is entered automatically in the subnet IP area by default in this case.<br>• **Subnet IP**: Select to configure a specific subnet IP address as the route to leak from the source VRF to the destination VRF. The **Subnet IP** box appears.<br>In the **Subnet IP** box, enter a subnet IP address as the route to leak between VRFs. |

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

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

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

  You are returned to the **Add Leak Route** window. Repeat Step 4, on page 21 through Step 5, on page 22 to configure another route to leak between a pair of VRFs.

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

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

  You are returned to the **Add Leak Route** window. Repeat Step 4, on page 21 through Step 5, on page 22 to configure another route, but this time:
  - In the **Source VRF** field, select the VRF that you had selected as a destination VRF in the previous configuration.
  - In the **Destination VRF** field, select the VRF that you had selected as a source VRF in the previous configuration.

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

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

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

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

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

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

  The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in Step 4, on page 21. Note that the entry in the **Source VRF** is pre-selected and cannot be changed in this situation.

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

  The **Add Leak Route** window appears. Enter the necessary information as you did previously using the information in Step 4, on page 21. Note that the entry in the **Destination VRF** is pre-selected and cannot be changed in this situation.

# Enabling Connectivity From the AWS Site to External Devices

Follow these procedures to manually enable IPv4 connectivity from the infra VPC CCRs to any external device with IPSec/BGP.

## Downloading the External Device Configuration Files

**Step 1** In the Cisco Cloud APIC GUI, click on **Dashboard**.
The **Dashboard** view for the Cisco Cloud APIC appears.

**Step 2** Navigate to **Infrastructure** > **External Connectivity**.
The **External Connectivity** window appears.

**Step 3** Click **Actions** > **Download External Device Configuration Files**.
The **Download External Device Configuration Files** pop-up appears.

**Step 4** Select the external device configuration files to download and click **Download**.
This action downloads a zip file that contains configuration information that you will use to manually configure the external device for IPv4 connectivity to the CCRs.

## Enabling Connectivity From the AWS Site to External Devices

**Step 1** Gather the necessary information that you will need to manually enable IPv4 connectivity from the infra VPC CCRs to any external device without EVPN.

**Step 2** Log into the external device.

**Step 3** Enter the configuration information to connect an external networking device.

If you downloaded the external device configuration files using the instructions in Downloading the External Device Configuration Files, on page 23, locate the configuration information for the first tunnel and enter that configuration information.

Following is an example of what the external device configuration file might look like for the first tunnel:

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

! Tunnel to 128.107.72.122 1.100 [ikev2] for
hctunnIf.acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! USER-DEFINED: please define GigabitEthernet2 if required
! USER-DEFINED: please define tunnel-id: 100 if required
! USER-DEFINED: please define vrf-name: infra:externalvrf1 if required
! USER-DEFINED: please define gig3-public-ip: 13.88.168.176 if 0.0.0.0 ip still not provided by AWS.
! Device:            128.107.72.122
! Tunnel ID:         100
! Tunnel counter:    1
! Tunnel address:    5.16.1.9
! Tunnel Dn:
acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! VRF name:          infra:externalvrf1
! ikev:              ikev2
! Bgp Peer addr:     5.16.1.10
! Bgp Peer asn:      65015
! Gig3 Public ip:    13.88.168.176
! PreShared key:     device1azure
! ikev profile name: ikev2-100

vrf definition infra:externalvrf1
    rd 1:1

    address-family ipv4
        route-target export 64550:1
        route-target import 64550:1
    exit-address-family
exit

crypto ikev2 proposal ikev2-infra:externalvrf1
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-infra:externalvrf1
    proposal ikev2-infra:externalvrf1
exit

crypto ikev2 keyring keyring-ikev2-100
    peer peer-ikev2-keyring
        address 13.88.168.176
        pre-shared-key device1azure
    exit
exit

crypto ikev2 profile ikev2-100
    match address local interface GigabitEthernet2
    match identity remote address 13.88.168.176 255.255.255.255
    identity local address 128.107.72.122
```

```
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-ikev2-100
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set ikev2-100 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev2-100
    set transform-set ikev2-100
    set pfs group14
    set ikev2-profile ikev2-100
exit

interface Tunnel100
    vrf forwarding infra:externalvrf1
    ip address 5.16.1.10 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GigabitEthernet2
    tunnel mode ipsec ipv4
    tunnel destination 13.88.168.176
    tunnel protection ipsec profile ikev2-100
exit

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

address-family ipv4 vrf infra:externalvrf1
    redistribute connected
    maximum-paths eibgp 32

    neighbor 5.16.1.9 remote-as 65008
    neighbor 5.16.1.9 ebgp-multihop 255
    neighbor 5.16.1.9 activate
    neighbor 5.16.1.9 send-community both

    distance bgp 20 200 20
exit-address-family
```

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

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

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

VRF Definition

IPSec Global Configurations

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

```
!
crypto keyring Ext-V1-1000-ike
  pre-shared-key address <50.18.55.126>[cAPIC CSR Gig3 public IP] key <abcdefg12345>
!
crypto isakmp profile Ext-V1-1000-ike
   keyring Ext-V1-1000-ike
   match identity address <50.18.55.126>[cAPIC CSR1 gig3 Public IP] 255.255.255.255
!
crypto ipsec transform-set Ext-V1-1000-ike esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile Ext-V1-1000-ike
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set Ext-V1-1000-ike
set pfs group14
!
interface Tunnel1000
vrf forwarding Ext-V1
ip address 50.50.0.2[cAPIC CSR BGP Peer Addr] 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1400
tunnel source GigabitEthernet2
tunnel mode ipsec ipv4
tunnel destination <50.18.55.126>[cAPIC CSR1 gig3 Public IP]
tunnel protection ipsec profile Ext-V1-1000-ike
!
router bgp 64550
!
address-family ipv4 vrf Ext-V1
  redistribute connected
  neighbor <50.50.0.1>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.1 ebgp-multihop 255
  neighbor 50.50.0.1 activate
  neighbor 50.50.0.1 send-community both
  neighbor <50.50.0.5>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.5 ebgp-multihop 255
  neighbor 50.50.0.5 activate
  neighbor 50.50.0.5 send-community both
  distance bgp 20 200 20
!
ip route 50.18.55.126[cAPIC CSR1 gig3 Public IP] 255.255.255.255 GigabitEthernet2 10.10.0.103
```

IPSec and Ikev1
Per Tunnel Configurations

BGP Configurations for VRF Neighbor

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

```
crypto ikev2 proposal ikev2-1
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1
 group 24 21 20 19 16 15 14 2
!
crypto ikev2 policy ikev2-1
 proposal ikev2-1
!
crypto ikev2 keyring keyring-ikev2-2000
 peer peer-ikev2-keyring
  address 35.81.94.248 [cAPIC CSR1 gig3 Public IP]
  pre-shared-key abcdefg12345
!
crypto ikev2 profile ikev2-2000
 match address local interface GigabitEthernet3
 match identity remote address 35.81.94.248[cAPIC CSR1 gig3 Public IP] 255.255.255.255
 identity local address 52.53.49.193 [Local Device tunnel source interface Public IP (Gig3 public IP)]
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-ikev2-2000
 lifetime 3600
 dpd 10 5 on-demand
!
crypto ipsec transform-set ikev2-2000 esp-gcm 256
 mode tunnel
!
crypto ipsec profile ikev2-2000
 set transform-set ikev2-2000
 set pfs group14
 set ikev2-profile ikev2-2000
!
interface Tunnel2000
 vrf forwarding Ext-V1
 ip address 50.50.0.14 [cAPIC CSR1 BGP Peer Addr] 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel destination 35.81.94.248[cAPIC CSR1 gig3 Public IP]
 tunnel protection ipsec profile ikev2-2000
```

Ikev2 Global Configurations

IPSec and Ikev2
Per Tunnel Configurations

**Step 4** Repeat the previous step to configure additional tunnels.

# Creating an EPG Using the Cisco Cloud APIC GUI

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

### Before you begin

Create an application profile and a VRF.

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

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

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

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

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

***Table 7: Create EPG Dialog Box Fields***

| Properties | Description |
|---|---|
| **Name** | Enter the name of the EPG. |

| Properties | Description |
|---|---|
| **Tenant** | To choose a tenant:<br>**a.** Click **Select Tenant**. The **Select Tenant** dialog box appears.<br>**b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create EPG** dialog box. |
| **Application Profile** | To choose an application profile:<br>**a.** Click **Select Application Profile**. The **Select Application Profile** dialog box appears.<br>**b.** From the **Select Application Profile** dialog, click to choose an application profile in the left column then click **Select**. You return to the **Create EPG** dialog box. |
| **Description** | Enter a description of the EPG. |
| **Settings** | |
| **Type** | Choose the EPG type:<br>• **Cloud** - Click to create the EPG in the cloud.<br>• **External** - Click to create an external EPG. |
| **Route Reachability** | (Visible when creating an external EPG) Click the **Route Reachability** drop-down list and choose:<br>• **On Premises**<br>• **Internet**<br>• **Unspecified** |
| **VRF** | To choose a VRF:<br>**a.** Click **Select VRF**. The **Select VRF** dialog box appears.<br>**b.** From the **Select VRF** dialog, click to choose a VRF in the left column then click **Select**. You return to the **Create EPG** dialog box. |

| Properties | Description |
| --- | --- |
| **Endpoint Selectors** | |

| Properties | Description |
| --- | --- |
| | **Note** See Configuring Instances in AWS, on page 38 for instructions on configuring instances in AWS as part of the endpoint selector configuration process.<br><br>To add an endpoint selector:<br>**a.** Click **Add Endpoint Selector** to open the **Add Endpoint Selector** dialog.<br>**b.** In the **Add Endpoint Selector** dialog, enter a name in the **Name** field.<br>**c.** Click **Selector Expression**. The **Key**, **Operator**, and **Value** fields are enabled.<br>**d.** Click the **Key** drop-down list to choose a key. The options are:<br>• Choose **IP** if you want to use an IP address or subnet for the endpoint selector.<br>• Choose **Zone** if you want to use an availability zone for the endpoint selector.<br>• Choose **Region** if you want to use the Amazon Web Services region for the endpoint selector.<br>• Choose **Custom** if you want to create a custom key for the endpoint selector.<br>**Note** When choosing the **Custom** option, the drop-down list becomes a text box. You need to enter a name for the key in the spaces after **custom:** (for example, **custom: Location**).<br>**e.** Click the **Operator** drop-down list to choose an operator. The options are:<br>• **equals**: Used when you have a single value in the Value field.<br>• **not equals**: Used when you have a single value in the Value field.<br>• **in**: Used when you have multiple comma-separated values in the Value field.<br>• **not in**: Used when you have multiple comma-separated values in the Value field.<br>• **has key**: Used if the expression contains only a key. |

| Properties | Description |
| --- | --- |
| | • **does not have key**: Used if the expression contains only a key.<br><br>**f.** Enter a value in the **Value** field then click the check mark to validate the entries. The value you enter depends on the choices you made for the **Key** and **Operator** fields. For example, if the **Key** field is set to **IP** and the **Operator** field is set to **equals**, the **Value** field must be an IP address or subnet. However, if the **Operator** field is set to **has key**, the **Value** field is disabled.<br><br>**g.** When finished, click the check mark to validate the selector expression.<br><br>**h.** Determine if you want to create additional endpoint selector expressions to the endpoint selector. If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions.<br><br>For example, assume you created two sets of expressions under a single endpoint selector:<br><br>• Endpoint selector 1, expression 1:<br>• **Key:** Zone<br>• **Operator:** equals<br>• **Value:** us-west-1a<br><br>• Endpoint selector 1, expression 2:<br>• **Key:** IP<br>• **Operator:** equals<br>• **Value:** 192.0.2.1/24<br><br>In this case, if *both* of these expressions are true (if the availability zone is us-west-1a AND if the IP address belongs to subnet 192.0.2.1/24), then that endpoint is assigned to the Cloud EPG. |

| Properties | Description |
|---|---|
| | **i.** Click the check mark after every additional expression that you want to create under this endpoint selector then click **Add** when finished.<br><br>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:<br><br>• Endpoint selector 2, expression 1:<br>  • **Key:** Region<br>  • **Operator:** in<br>  • **Value:** us-east-1, us-east-2<br><br>In this case:<br><br>• If the availability zone is us-west-1a AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions)<br><br>OR<br><br>• If the region is either us-east-1 or us-east-2 (endpoint selector 2 expression)<br><br>Then that end point is assigned to the Cloud EPG. |

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

# Creating a Contract Using the Cisco Cloud APIC GUI

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

### Before you begin

Create filters.

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

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

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

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

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

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

| Properties | Description |
|---|---|
| **Name** | Enter the name of the contract. |
| **Tenant** | To choose a tenant:<br>**a.** Click **Select Tenant**. The **Select Tenant** dialog box appears.<br>**b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Contract** dialog box. |
| **Description** | Enter a description of the contract. |
| **Settings** | |
| **Scope** | The scope limits the contract to any endpoint groups within the same application profile, within the same VRF instance, throughout the fabric (globally), or within the same tenant.<br>**Note** Shared services enables communication between EPGs in different tenants and between EPGs in different VRFs.<br>To enable EPGs in one tenant to communicate with EPGs in another tenant, choose **Global** scope.<br>To enable an EPG in one VRF to communicate with another EPG in a different VRF, choose **Global** or **Tenant** scope.<br>For more information about shared services, see Shared Services<br>Click the drop-down arrow to choose from the following scope options:<br>• **Application Profile**<br>• **VRF**<br>• **Global**<br>• **Tenant** |
| **Apply Filter in Both Directions** | Put a check in the box to apply the same filters to traffic from consumer-to-provider and provider-to-consumer. Do not put a check in the box if you want to apply different filters for each direction of traffic.<br>The check box is enabled by default. |

| Properties | Description |
|---|---|
| **Add Filter** | To choose a filter:<br>**a.** Click **Add Filter**. The filter row appears with a **Select Filter** option.<br>**b.** Click **Select Filter**. The **Select Filter** dialog box appears.<br>**c.** From the **Select Filter** dialog, click to choose a filter in the left column then click **Select**. You return to the **Create Contract** dialog box. |

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

# Specifying Consumer and Provider EPGs Using the Cisco Cloud APIC

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

### Before you begin

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

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

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

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

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

**Step 4** To choose a contract:

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

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

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

**Step 6** To add a provider EPG:

a) Click **Add Provider EPGs**. The **Select Provider EPGs** dialog appears.
b) In the pane on the left side of the **Select Provider EPGs** dialog, click to place a check in a check box to choose a provider EPG.

c) When finished, click **Select**. The **Select Provider EPGs** dialog box closes.

# Creating a Filter Using the Cisco Cloud APIC GUI

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

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

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

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

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

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

***Table 9: Create Filter Dialog Box Fields***

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

| Properties | Description |
|---|---|
| **Add Filter** | To add a filter:<br>**a.** Click **Add Filter Entry**. The **Create Filter Entry** dialog box appears.<br>**b.** Enter a name for the filter entry in the **Name** field.<br>**c.** From the **Select Filter** dialog, click to choose a filter in the left column then click **Select**. You return to the **Create Contract** dialog box.<br>**d.** Click the **Ethernet Type** drop-down list to choose an ethernet type. The options are:<br>• **IP**<br>• **Unspecified**<br>**Note** When **Unspecified** is chosen, the remaining fields are disabled.<br>**e.** Click the **IP Protocol** drop-down menu to choose a protocol. The options are:<br>• **icmp**<br>• **tcp**<br>• **udp**<br>• **Unspecified**<br>**Note** The remaining fields are enabled only when **tcp** or **udp** is chosen.<br>**f.** Enter the appropriate port information in the **Origin Port from** and **to** fields.<br>**g.** Enter the appropriate port information in the **Destination Port from** and **to** fields.<br>**h.** When finished entering filter entry information, click **Add**. You return to the **Create Filter** dialog box where you can repeat the steps to add another filter entry. |

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

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

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

### Before you begin

Create a VRF.

**Step 1** Navigate to **Application Management** > **Cloud Context Profiles**.

The list of configure cloud context profiles appears.

**Step 2** Click **Actions** > **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

**Step 3** Enter the appropriate values in each field as listed in the following *Cloud Context Profile Dialog Box Fields* table then continue.

***Table 10: Create Cloud Context Profile Dialog Box Fields***

| Properties | Description |
|---|---|
| **Name** | Enter the name of the cloud context profile. |
| **Tenant** | To choose a tenant:<br>**a.** Click **Select Tenant**. The **Select Tenant** dialog box appears.<br>**b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Cloud Context Profile** dialog box. |
| **Description** | (Optional) Enter a description of the cloud context profile. |
| **Settings** | |
| **Select Region** | To choose a region:<br>**a.** Click **Select Region**. The **Select Region** dialog box appears.<br>**b.** From the **Select Region** dialog, click to choose a region in the left column then click **Select**. You return to the **Create Cloud Context Profile** dialog box. |
| **Select VRF** | To choose a VRF:<br>**a.** Click **Select VRF**. The **Select VRF** dialog box appears.<br>**b.** From the **Select VRF** dialog box, click to choose a VRF in the left column then click **Select**. You return to the **Create Cloud Context Profile** dialog box. |

| Properties | Description |
|---|---|
| **Add CIDR** | **Note** The following subnets are reserved and should not be used in this **Add CIDR** field:<br>• 169.254.0.0/16 (reserved for VPN tunnel to the transit gateway)<br>• 192.168.100.0/24 (reserved by the CCR for the bridge domain interface)<br><br>To add a CIDR:<br>**a.** Click **Add CIDR**. The **Add CIDR** dialog box appears.<br>**b.** Enter the address in the **Address** field.<br>**c.** Click **Add Subnet** and enter the subnet address in the **Address** field.<br>**d.** To add availability zones:<br>**1.** Click **Select Availability Zone**. The **Select Availability Zone** dialog box appears.<br>**2.** From the **Select Availability Zone** dialog box, click to choose an availability zone in the left column.<br>Beginning with release 25.0(2), the type of availability zone shown in this window varies depending on the type of tenant that you selected for this cloud context profile.<br>**Note** If you are creating a cloud context profile in a **user** tenant, you are restricted to only **cloud** availability zones in this window.<br>See Availability Zones for more information.<br>**3.** Click **Select**<br>You return to the **Create Cloud Context Profile** dialog box.<br>**e.** Click to check (enabled) or uncheck (disabled) the **Primary** check box.<br>**f.** When finished, click **Add**. |
| **VPN Gateway Router** | (Optional) Click to check (enabled) or uncheck (disabled) in the **VPN Gateway Router** check box. |
| **TGW Attachment** | (Optional) Click to check (enabled) or uncheck (disabled) in the **TGW Attachment** check box. |

**Step 4** Click **Save** when finished.

# Configuring Instances in AWS

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

This topic provides the instructions for configuring the instances in AWS. You can use these procedures to configure the instances in AWS either before you configure the endpoint selectors for Cisco Cloud APIC or afterward. For example, you might go to your account in AWS and create a custom tag or label in AWS first, then create an endpoint selector using a custom tag or label in Cisco Cloud APIC afterward. Or you might create an endpoint selector using a custom tag or label in Cisco Cloud APIC first, then go to your account in AWS and create a custom tag or label in AWS afterward.

**Step 1** Review your cloud context profile configuration settings and determine which settings you will use with your AWS instance.

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

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

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

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

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

c) Select the cloud context profile that you will use as part of this AWS instance configuration process.

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

**Step 2** Log in to the Amazon Web Services account for the Cisco Cloud APIC user tenant, if you are not logged in already.

**Step 3** Go to **Services** > **EC2** > **Instances** > **Launch Instance**.

**Step 4** In the **Choose an Amazon Machine Image (AMI)** page, select an Amazon Machine Image (AMI).

**Step 5** In the **Choose an Instance Type** page, select an instance type, then click **Configure Instance Details**.

**Step 6** In the **Configure Instance Details** page, enter the necessary information in the appropriate fields.

- In the **Network** field, select your Cisco Cloud APIC VRF.

  This would be the VRF that is associated with the cloud context profile that you are using as part of this AWS instance configuration process.

- In the **Subnet** field, select the subnet.
- In the **Auto-assign Public IP** field, if you want to have a public IP, select **Enable** from the scroll-down menu.

**Step 7** When you have finished entering the necessary information into the **Configure Instance Details** page, click **Add Storage**.

**Step 8** In the **Add Storage** page, accept the default values or configure the storage in this page, if necessary, and click **Add Tags**.

**Step 9** In the **Add Tags** page, click **Add Tag** and enter the necessary information in the appropriate fields in this page.

**Note** If you will be using IP Address, Region or Zone for the type of endpoint selector later in these procedures, you do not have to enter any information in this page. In those situations, when you start the instance in AWS, the IP address, region or zone will be discovered by the Cisco Cloud APIC and the endpoint will be assigned to the EPG.

- **Key:** Enter the key that you will use when you create a custom tag for the type of endpoint selector that you are adding later in these procedures.

- **Value:** Enter the value that you will be using for this key.
- **Instances:** Check the box for this field.
- **Volumes:** Check the box for this field.

For example, if you are planning on creating a custom tag for a specific building for your endpoint selector later in these procedures (such as building6), you might enter the following values in these fields on this page:

- **Key:** Location
- **Value:** building6

**Step 10** Click **Review and Launch**.

The **Select an existing key pair or create a new key pair** page appears. Use the information in this page if you want to ssh to the instance later on.

# Creating a Backup Configuration Using the Cisco Cloud APIC GUI

This section explains how to create a backup configuration.

### Before you begin

Create a remote location and a scheduler, if needed.

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

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

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

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

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

***Table 11: Create Backup Configuration Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter the name of the backup configuration. |
| **Description** | Enter a description of the backup configuration. |
| **Settings** | |
| **Backup Destination** | Choose a backup destination.<br>• **Local**<br>• **Remote** |

| Properties | Description |
| --- | --- |
| **Backup Object** | |

| Properties | Description |
| --- | --- |
| | Choose the root hierarchical content to consider for the backup<br>• **Policy Universe**<br>• **Selector Object**—When chosen, this option adds the **Object Type** drop-down list and **Object DN** field.<br>**a.** From the **Object Type** drop-down list, choose from the following options:<br>• **Tenant**—When chosen the **Select Tenant** option appears.<br>• **Application Profile**—When chosen the **Select Application Profile** option appears.<br>• **EPG**—When chosen the **Select EPG** option appears.<br>• **Contract**—When chosen the **Select Contract** option appears.<br>• **Filter**—When chosen the **Select Filter** option appears.<br>• **VRF**—When chosen the **Select VRF**option appears.<br>• **Device**—When chosen the **Select fvcloudLBCtx**option appears.<br>• **Service Graph**—When chosen the **Select Service Graph** option appears.<br>• **Cloud Context Profile**—When chosen the **Select Cloud Context Profile** option appears.<br>**b.** Click the **Select <object_name>**. The **Select <object_name>** dialog appears.<br>**c.** From the **Select <object_name>** dialog, click to choose from the options in the left column then click **Select**. You return to the **Create Backup Configuration** dialog box.<br>**Note** The **Object DN** field is automatically populated with the DN of the object it will use as root of the object tree to backup<br>• **Enter DN**—When chosen, this option displays the **Object DN** field.<br>**a.** From the **Object DN** field, enter the DN of a |

| Properties | Description |
|---|---|
| | specific object to use as the root of the object tree to backup. |
| **Scheduler** | **a.** Click **Select Scheduler** to open the **Select Scheduler** dialog and choose a scheduler from the left-side column.<br>**b.** Click the **Select** button at the bottom-right corner when finished. |
| **Trigger Backup After Creation** | Choose one of the following:<br>• **Yes**—(Default) Trigger a backup after creating the backup configuration.<br>• **No**—Do not trigger a backup after creating the backup configuration. |

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

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

This section explains how to create a tech support policy.

### Before you begin

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

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

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

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

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

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

***Table 12: Create Tech Support Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter the name of the tech support policy. |
| **Description** | Enter a description of the tech support. |
| **Settings** | |

| Properties | Description |
|---|---|
| **Export Destination** | Choose an export destination.<br>• **Controller**<br>• **Remote Location**—When chosen the **Select Remote Location** option appears.<br>a. Click **Select Remote Location**. The **Select Remote Location** dialog box appears.<br>b. From the **Select Remote Location** dialog, click to choose a remote location in the left column then click **Select**. You return to the **Create Tech Suport** dialog box. |
| **Include Pre-Upgrade Logs** | Click to place a check in the **Enabled** check box if you want to include pre-upgrade logs in the tech support policy. |
| **Trigger After Creation** | Click to place a check in the **Enabled** (the default) check box if you want to create the tech support policy after the policy creation. To disable, click the check box to uncheck. |

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

# Creating a Trigger Scheduler Using the Cisco Cloud APIC GUI

This section explains how to create a trigger scheduler.

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

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

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

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

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

***Table 13: Create Trigger Scheduler Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter the name of the trigger scheduler policy. |
| **Description** | Enter a description of the trigger scheduler. |
| **Settings** | |

| Properties | Description |
|---|---|
| **Recurring Windows** | Click **Add Recurring Window**. The **Add Recurring Window** dialog appears.<br>**a.** From the **Schedule** drop-down list, choose from the following.<br>• **every-day**<br>• **Monday**<br>• **Tuesday**<br>• **Wednesday**<br>• **Thursday**<br>• **Friday**<br>• **Saturday**<br>• **Sunday**<br>• **odd-day**<br>• **even-day**<br>**b.** From the **Start Time** field, enter a time.<br>**c.** From the **Maximum Concurrent Tasks** field, enter a number or leave the field empty to specify unlimited.<br>**d.** From the **Maximum Running Time**, click to choose **Unlimited** or **Custom**.<br>**e.** Click **Add** when finished. |
| **Add One Time Window** | Click **Add One Time Window**. The **Add One Time Window** dialog appears.<br>**a.** From the **Start Time** field, enter a date and time.<br>**b.** From the **Maximum Concurrent Tasks** field, enter a number or leave the field blank to specify unlimited.<br>**c.** From the **Maximum Running Time**, click to choose **Unlimited** or **Custom**.<br>**d.** Click **Add** when finished. |

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

# Creating a Remote Location Using the Cisco Cloud APIC GUI

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

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

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

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

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

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

***Table 14: Create Remote Location Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter the name of the remote location policy. |
| **Description** | Enter a description of the remote location policy. |
| **Settings** | |
| **Hostname/IP Address** | Enter the hostname or IP address of the remote location |
| **Protocol** | Choose a protocol:<br>• **FTP**<br>• **SFTP**<br>• **SCP** |
| **Path** | Enter the path for the remote location. |
| **Port** | Enter the port for the remote location. |
| **Username** | Enter a username for the remote location. |
| **Authentication Type** | When using SFTP or SCP, choose the authentication type:<br>• **Password**<br>• **SSH Key** |
| **SSH Key Content** | Enter the SSH key content. |
| **SSH Key Passphrase** | SSH key passphrase. |
| **Password** | Enter a password for accessing the remote location. |
| **Confirm Password** | Reenter the password for accessing the remote location. |

| Properties | Description |
|---|---|
| **Management EPG** | **a.** Click **Select Management EPG**. The **Select Management EPG** dialog appears.<br>**b.** From the column on the left, click to choose a management EPG.<br>**c.** Click **Select**. |

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

# Creating a Login Domain Using the Cisco Cloud APIC GUI

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

### Before you begin

Create a provider before creating a non-local domain.

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

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

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

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

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

***Table 15: Create Login Domain Dialog Box Fields***

| Properties | Description |
|---|---|
| **Name** | Enter the name of the login domain. |
| **Description** | Enter a description of the login domain. |
| **Realm** | Choose a realm:<br>• **Local**<br>• **LDAP**—Requires adding providers and choosing an authenication type.<br>• **RADIUS**—Requires adding providers.<br>• **TACACS+**—Requires adding providers.<br>• **SAML**—Requires adding providers. |

| Properties | Description |
|---|---|
| **Providers** | To add a provider:<br>**a.** Click **Add Providers**. The **Select Providers** dialog appears with a list of providers in the left pane.<br>**b.** Click to choose a provider.<br>**c.** Click **Select** to add the provider. |
| **Advanced Settings** | Displays the **Authentication Type** and **LDAP Group Map Rules** fields. |
| **Authentication Type** | When LDAP is chosen for realm option, choose one of the following authentication types:<br>• **Cisco AV Pairs**—(Default)<br>• **LDAP Group Map Rules**—Requires adding LDAP group map rules. |

| Properties | Description |
|---|---|
| **LDAP Group Map Rules** | To add an LDAP group map rule:<br>**a.** Click **Add LDAP Group Map Rule**. The **Add LDAP Group Map Rule** dialog appears with a list of providers in the left pane.<br>**b.** Enter a name for the rule in the **Name** field.<br>**c.** Enter a description for the rule in the **Description** field.<br>**d.** Enter a group DN for the rule in the **Group DN** field.<br>**e.** Add security domains:<br>**1.** Click **Add Security Domain**. The **Add Security Domain** dialog box appears.<br>**2.** Click **Select Security Domain**. The **Select Security Domain** dialog box appears with a list of security domains in the left pane.<br>**3.** Click to choose a security domain.<br>**4.** Click **Select** to add the security domain. You return to the **Add Security Domain** dialog box.<br>**5.** Add a user role:<br>**a.** From the **Add Security Domain** dialog box, click **Select Role**. The **Select Role** dialog box appears with a list of roles in the left pane.<br>**b.** Click to choose a role.<br>**c.** Click **Select** to add the role. You retun to the **Add Security Domain** dialog box.<br>**d.** From the **Add Security Domain** dialog box, click the **Privilege Type** drop-down list and choose **Read Privilege** or **Write Privilege**.<br>**e.** Click the check mark on the right side of the **Privilege Type** drop-down list to confirm.<br>**f.** Click **Add** when finished. You return to the **Add LDAP Group Map Rule** dialog box where you can add another security domain. |

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

# Creating a Provider Using the Cisco Cloud APIC GUI

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

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

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

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

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

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

***Table 16: Create Provider Dialog Box Fields***

| Properties | Description |
|---|---|
| **Hostname/IP Address** | Enter the hostname or IP address of the provider. |
| **Description** | Enter a description of the provider. |
| **Type** | Click the **Type** drop-down list and choose one of the following types:<br>• **LDAP**<br>• **RADIUS**<br>• **TACACS+**<br>• **SAML**<br>**Note** A set of fields will appear based on the type that you choose. |
| **[LDAP] Settings** | |
| **Bind DN** | Enter the LDAP bind DN. |
| **Base DN** | Enter the LDAP base DN. |
| **Password** | Enter a password for the LDAP settings. |
| **Confirm Password** | Reenter the password for the LDAP settings. |
| **Port** | Enter the port number for the provider type. |
| **Advanced Settings** | Displays additional fields in the **Settings** section of the provider dialog box. |
| **Timeout (sec)** | Enter the number of seconds allowed before a timeout occurs. The default is 30. |
| **Retries** | Enter the number of allowed retries. The default is 1. |

| Properties | Description |
|---|---|
| **SSL** | To enable SSL, click to place a check in the **SSL** check box. To disable SSL, click to remove the check from the **SSL** check box. The default is enabled. |
| **SSL Certificate Validation Level** | Choose one of the following:<br>• **Permissive**<br>• **Strict** |
| **Attribute** | Enter an LDAP attribute in the **Attribute** text box. |
| **Filter Type** | Choose a filter type:<br>• **Default**<br>• **Microsoft AD**<br>• **Custom** |
| **Filter** | Enter an LDAP filter in the text box. This option only appears when the **Custom** filter type is chosen. |
| **Select Management EPG** | To add a management EPG:<br>**a.** Click **Select Management EPG**. The **Select Management EPG** dialog appears with a list of EPGs in the left pane.<br>**b.** Click to choose an EPG.<br>**c.** Click **Select** to add the management EPG to the LDAP. |
| **Server Monitoring** | To enable server monitoring, click to place a check in the **Enabled** check box. To disable server monitoring, click to remove the check from the **Enabled** check box. The default is disabled. |
| **[RADIUS] Settings** | |
| **Key** | Enter the RADIUS key. |
| **Confirm Key** | Reenter the RADIUS key. |
| **Advanced Settings** | Displays additional fields in the **Settings** section of the provider dialog box. |
| **Port** | Enter the port number for the RADIUS settings. The default is 1812. |

| Properties | Description |
|---|---|
| **Authentication Protocol** | Choose from the following:<br>• **PAP**—(Default)<br>• **CHAP**<br>• **MS-CHAP** |
| **Timeout (sec)** | Enter the number of seconds allowed before a timeout occurs. The default is 5. |
| **Retries** | Enter the number of allowed retries. The default is 1. |
| **Select Management EPG** | To add a management EPG:<br>**a.** Click **Select Management EPG**. The **Select Management EPG** dialog appears with a list of EPGs in the left pane.<br>**b.** Click to choose an EPG.<br>**c.** Click **Select** to add the management EPG to the RADIUS. |
| **Server Monitoring** | To enable server monitoring, click to place a check in the **Enabled** check box. To disable server monitoring, click to remove the check from the **Enabled** check box. The default is disabled. |
| **[TACACS+] Settings** | |
| **Key** | Enter the TACACS+ key. |
| **Confirm Key** | Reenter the TACACS+ key. |
| **Advanced Settings** | Displays additional fields in the **Settings** section of the provider dialog box. |
| **Port** | Enter the port number for the TACACS+ settings. The default is 1812. |
| **Authentication Protocol** | Choose from the following:<br>• **CHAP**<br>• **MS-CHAP**<br>• **PAP**—(Default) |
| **Timeout (sec)** | Enter the number of seconds allowed before a timeout occurs. The default is 5. |
| **Retries** | Enter the number of allowed retries. The default is 1. |

| Properties | Description |
|---|---|
| **Select Management EPG** | To add a management EPG:<br>**a.** Click **Select Management EPG**. The **Select Management EPG** dialog appears with a list of EPGs in the left pane.<br>**b.** Click to choose an EPG.<br>**c.** Click **Select** to add the management EPG to the TACACS+. |
| **Server Monitoring** | To enable server monitoring, click to place a check in the **Enabled** check box. To disable server monitoring, click to remove the check from the **Enabled** check box. The default is disabled. |
| **[SAML] Settings** | |
| **Identity Provider** | Choose from the following identity providers:<br>• **ADFS**—(default)<br>• **OKTA**<br>• **PING IDENTITY** |
| **Identity Provider Metadata URL** | Enter the metatdata URL provided by the identity provider. |
| **Entity ID** | Enter a unique ID as the SAML entity identifier. |
| **HTTPS Proxy for Metadata URL** | Enter the HTTPS proxy used to reach the identity provider's metadata URL. |
| **Advanced Settings** | Displays additional fields in the **Settings** section of the provider dialog box. |
| **GUI Redirect Banner Message (URL)** | Enter the GUI redirect banner message. |
| **Certificate Authority** | To choose a certificate authority:<br>**a.** Click **Select Certificate Authoriy**. The **Select Certificate Authoriy** dialog appears with a list of certificates in the left pane.<br>**b.** Click to choose a certificate.<br>**c.** Click **Select** to add the certificate. You return to the **Create Provider** dialog box. |
| **Timeout (sec)** | Enter the number of seconds allowed before a timeout occurs. The default is 5. |
| **Retries** | Enter the number of allowed retries. The default is 1. |

| Properties | Description |
|---|---|
| **Signature Algorithm Authentication User Requests*** | Click the **Signature Algorithm for Requests** drop-down list and choose one of the following:<br>• **RSA SHA1**<br>• **RSA SHA224**<br>• **RSA SHA256** (Default)<br>• **RSA SHA384**<br>• **RSA SHA512** |
| **Sign SAML Authentication Requests** | To enable, click to place a check in the check box. To disable, click to remove the check from the check box. The default is enabled. |
| **Sign SAML Response Message** | To enable, click to place a check in the check box. To disable, click to remove the check from the check box. The default is enabled. |
| **Sign Assertions in SAML Response** | To enable, click to place a check in the check box. To disable, click to remove the check from the check box. The default is enabled. |
| **Encrypt SAML Assertions** | To enable, click to place a check in the check box. To disable, click to remove the check from the check box. The default is enabled. |

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

# Creating a Security Domain Using the Cisco Cloud APIC GUI

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

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

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

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

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

**Step 4** In the **Name** field, enter the name of the security domain.

**Step 5** In the **Description** field, enter a description of the security domain.

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

# Creating a Role Using the Cisco Cloud APIC GUI

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

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

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

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

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

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

***Table 17: Create Role Dialog Box Fields***

| Properties | Description |
|---|---|
| **General** | |
| **Name** | Enter a name for the role in the **Name** field. |
| **Description** | Enter a description of the role. |
| **Settings** | |

| Properties | Description |
| --- | --- |
| Privilege | |

| Properties | Description |
| --- | --- |
| | Click to place a check mark in the check boxes of the privileges you want to assign the user. The privileges are:<br>• **aaa**—Used for configuring authentication, authorization, accouting and import/export policies.<br>• **access-connectivity-l1**Used for Layer 1 configuration under infra. Example: selectors and port Layer 1 policy configurations.<br>• **access-connectivity-l2**—Used for Layer 2 configuration under infra. Example: Encap configurations on selectors, and attachable entity.<br>• **access-connectivity-l3**—Used for Layer 3 configuration under infra and static route configurations under a tenant's L3Out.<br>• **access-connectivity-mgmt**—Used for management infra policies.<br>• **access-connectivity-util**—Used for tenant ERSPAN policies.<br>• **access-equipment**—Used for access port configuration.<br>• **access-protocol-l1**—Used for Layer 1 protocol configurations under infra.<br>• **access-protocol-l2**—Used for Layer 2 protocol configurations under infra.<br>• **access-protocol-l3**—Used for Layer 3 protocol configurations under infra.<br>• **access-protocol-mgmt**—Used for fabric-wide policies for NTP, SNMP, DNS, and image management.<br>• **access-protocol-ops**—Used for operations-related access policies such as cluster policy and firmware policies.<br>• **access-protocol-util**—Used for tenant ERSPAN policies.<br>• **access-qos**—Used for changing CoPP and QoS-related policies.<br>• **admin**—Complete access to everything (combine ALL roles)<br>• **fabric-connectivity-l1**—Used for Layer 1 configuration under the fabric. Example: selectors and port Layer 1 policy and vPC protection. |

| Properties | Description |
| --- | --- |
| | • **fabric-connectivity-l2**—Used in firmware and deployment policies for raising warnings for estimating policy deployment impact.<br>• **fabric-connectivity-l3**—Used for Layer 3 configuration under the fabric. Example: Fabric IPv4 and MAC protection groups.<br>• **fabric-connectivity-mgmt**—Used for atomic counter and diagnostic policies on leaf switches and spine switches.<br>• **fabric-connectivity-util**—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches.<br>• **fabric-equipment**—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches.<br>• **fabric-protocol-l1**—Used for Layer 1 protocol configurations under the fabric.<br>• **fabric-protocol-l2**—Used for Layer 2 protocol configurations under the fabric.<br>• **fabric-protocol-l3**—Used for Layer 3 protocol configurations under the fabric.<br>• **fabric-protocol-mgmt**—Used for fabric-wide policies for NTP, SNMP, DNS, and image management.<br>• **fabric-protocol-ops**—Used for ERSPAN and health score policies.<br>• **fabric-protocol-util**—Used for firmware management traceroute and endpoint tracking policies.<br>• **none**—No privilege.<br>• **nw-svc-device**—Used for managing Layer 4 to Layer 7 service devices.<br>• **nw-svc-devshare**—Used for managing shared Layer 4 to Layer 7 service devices.<br>• **nw-svc-params**—Used for managing Layer 4 to Layer 7 service policies.<br>• **nw-svc-policy**—Used for managing Layer 4 to Layer 7 network service orchestration. |

| Properties | Description |
| --- | --- |
| | • **ops**—Used for operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies.<br>• **tenant-connectivity-l1**—Used for Layer 1 connectivity changes, including bridge domains and subnets.<br>• **tenant-connectivity-l2**—Used for Layer 2 connectivity changes, including bridge domains and subnets.<br>• **tenant-connectivity-l3**—Used for Layer 3 connectivity changes, including VRFs.<br>• **tenant-connectivity-mgmt**—Used for tenant in-band and out-of-band management connectivity configurations and for debugging/monitoring policies such as atomic counters and health score.<br>• **tenant-connectivity-util**—Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches.<br>• **tenant-epg**—Used for managing tenant configurations such as deleting/creating endpoint groups, VRFs, and bridge domains.<br>• **tenant-ext-connectivity-l2**—Used for managing tenant L2Out configurations.<br>• **tenant-ext-connectivity-l3**—Used for managing tenant L3Out configurations.<br>• **tenant-ext-connectivity-mgmt**—Used as write access for firmware policies.<br>• **tenant-ext-connectivity-util**—Used for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk.<br>• **tenant-ext-protocol-l1**—Used for managing tenant external Layer 1 protocols. Generally only used for write access for firmware policies.<br>• **tenant-ext-protocol-l2**—Used for managing tenant external Layer 2 protocols. Generally only used for write access for firmware policies.<br>• **tenant-ext-protocol-l3**—Used for managing tenant external Layer 3 protocols such as BGP, OSPF, PIM, and IGMP.<br>• **tenant-ext-protocol-mgmt**—Used as write access for firmware policies. |

| Properties | Description |
|---|---|
| | • **tenant-ext-protocol-util**—Used for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk.<br>• **tenant-network-profile**—Used for managing tenant configurations, such as deleting and creating network profiles, and deleting and creating endpoint groups.<br>• **tenant-protocol-l1**—Used for managing configurations for Layer 1 protocols under a tenant.<br>• **tenant-protocol-l2**—Used for managing configurations for Layer 2 protocols under a tenant.<br>• **tenant-protocol-l3**—Used for managing configurations for Layer 3 protocols under a tenant.<br>• **tenant-protocol-mgmt**—Only used as write access for firmware policies.<br>• **tenant-protocol-ops**—Used for tenant traceroute policies.<br>• **tenant-protocol-util**—Used for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk.<br>• **tenant-qos**—Only used as Write access for firmware policies.<br>• **tenant-security**—Used for Contract related configurations for a tenant.<br>• **vmm-connectivity**—Used to read all the objects in APIC's VMM inventory required for VM connectivity.<br>• **vmm-ep**—Used to read VM and Hypervisor endpoints in the APIC's VMM inventory.<br>• **vmm-policy**—Used for managing policies for VM networking.<br>• **vmm-protocol-ops**—Not used by VMM policies.<br>• **vmm-security**—Used for Contract related configurations for a tenant. |

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

# Creating an RBAC Rule Using the Cisco Cloud APIC GUI

This section explains how to create an RBAC rule using the GUI.

### Before you begin

Create a security domain.

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

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

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

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

**Step 4** In the **DN** field, enter the DN for the rule.

**Step 5** Choose a security domain:

a) Click **Select Security Domain**. The **Select Security Domain** dialog box appears.

b) From the **Select Security Domain** dialog box, click to choose a security domain from the column on the left then click **Select**. You return to the **Create RBAC Rule** dialog box.

**Step 6** From the **Allow Writes** field, click **Yes** to allow writes or **No** to not allow writes.

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

# Creating a Certificate Authority Using the Cisco Cloud APIC GUI

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

### Before you begin

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

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

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

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

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

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

***Table 18: Create Certificate Authority Dialog Box Fields***

| Properties | Description |
|---|---|
| **Name** | Enter the name of the certificate authority. |
| **Description** | Enter a description of the certificate authority. |

| Properties | Description |
|---|---|
| **Used for** | Choose from the following options:<br>• **Tenant**—Choose if the certificate authority is for a specific tenant. When chosen, the **Select Tenant** option appears in the GUI.<br>• **System**—Choose if the certificate authority is for the system. |
| **Select Tenant** | To choose a tenant:<br>**a.** Click **Select Tenant**. The **Select Tenant** dialog box appears.<br>**b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Certificate Authority** dialog box. |
| **Certificate Chain** | Enter the certificate chain in the **Certificate Chain** text box.<br>**Note** Add the certificates for a chain in the following order:<br>**a.** CA<br>**b.** Sub-CA<br>**c.** Subsub-CA<br>**d.** Server |

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

# Creating a Key Ring Using the Cisco Cloud APIC GUI

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

### Before you begin

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

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

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

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

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

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

***Table 19: Create Key Ring Dialog Box Fields***

| Properties | Description |
|---|---|
| **Name** | Enter the name of the key ring. |
| **Description** | Enter a description of the key ring. |
| **Used for** | • **System**—The key ring is for the system.<br>• **Tenant**—The key ring is for a specific tenant. Displays a **Tenant** field for specifying the tenant. |
| **Select Tenant** | To choose a tenant:<br>**a.** Click **Select Tenant**. The **Select Tenant** dialog box appears.<br>**b.** From the **Select Tenant** dialog, click to choose a tenant in the left column then click **Select**. You return to the **Create Key Ring** dialog box. |
| **Settings** | |
| **Certificate Authority** | To choose a certificate authority:<br>**a.** Click **Select Certificate Authority**. The **Select Certificate Authority** dialog appears.<br>**b.** Click to choose a certificate authority in the column on the left.<br>**c.** Click **Select**. You return to the **Create Key Ring** dialog box. |
| **Private Key** | Choose one of the following:<br>• **Generate New Key**—Generates a new key.<br>• **Import Existing Key**—Displays the **Private Key** text box and enables you to use an existing key. |
| **Private Key** | Enter an existing key in the **Private Key** text box (for the **Import Existing Key** option). |

| Properties | Description |
|---|---|
| **Modulus** | Click the **Modulus** drop-down list to choose from the following:<br>• **MOD 512**<br>• **MOD 1024**<br>• **MOD 1536**<br>• **MOD 2048**—(Default) |
| **Certificate** | Enter the certificate information in the **Certificate** text box. |

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

# Creating a Local User Using the Cisco Cloud APIC GUI

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

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

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

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

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

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

***Table 20: Create Local User Dialog Box Fields***

| Properties | Description |
|---|---|
| **Name** | Enter the username of the local user. |
| **Password** | Enter the password for the local user. |
| **Confirm Password** | Reenter the password for the local user. |
| **Description** | Enter a description of the local user. |
| **Settings** | |
| **Account Status** | To choose the account status:<br>• **Active**—Activates the local user account.<br>• **Inactive**—Deactivates the local user account. |
| **First Name** | Enter the first name of the local user. |

| Properties | Description |
|---|---|
| **Last Name** | Enter the last name of the local user. |
| **Email Address** | Enter the email address of the local user. |
| **Phone Number** | Enter the phone number of the local user. |
| **Security Domains** | To add a security domain:<br>**a.** Click **Add Security Domain**. The **Add Security Domain** dialog box appears.<br>**b.** Click **Select Security Domain**. The **Select Security Domain** dialog box appears with a list of security domains in the left pane.<br>**c.** Click to choose a security domain.<br>**d.** Click **Select** to add the security domain. You return to the **Add Security Domain** dialog box.<br>**e.** Add a user role:<br>**1.** From the **Add Security Domain** dialog box, click **Select Role**. The **Select Role** dialog box appears with a list of roles in the left pane.<br>**2.** Click to choose a role.<br>**3.** Click **Select** to add the the role. You retun to the **Add Security Domain** dialog box.<br>**4.** From the **Add Security Domain** dialog box, click the **Privilege Type** drop-down list and choose **Read Privilege** or **Write Privilege**.<br>**5.** Click the check mark on the right side of the **Privilege Type** drop-down list to confirm.<br>**6.** Click **Add** when finished. You return to the **Create Local User** dialog box where you can add another security domain. |

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

***Table 21: Create Local User Dialog Box Fields: Advanced Settings***

| Property | Description |
|---|---|
| **Account Expires** | If you choose **Yes**, the account is set to expire at the time that you choose. |
| **Password Update Required** | If you choose **Yes**, the user must change the password upon the next login. |

| Property | Description |
|---|---|
| **OTP** | Put a check in the box to enable the one-time password feature for the user. |
| **User Certificates** | To add a user certificate:<br>**a.** Click **Add X509 Certificate**. The **Add X509 Certificate** dialog box appears.<br>**b.** Enter a name in the **Name** field.<br>**c.** Enter the X509 certificate in the **User X509 Certificate** text box.<br>**d.** Click **Add**. The **X509 certificate in the User X509 Certificate** dialog box closes. You return to the **Local User** dialog box. |
| **SSH Keys** | To add a an SSH key:<br>**a.** Click **Add SSH Key**. The **Add SSH Key** dialog box appears.<br>**b.** Enter a name in the **Name** field.<br>**c.** Enter the SSH key in the **Key** text box.<br>**d.** Click **Add**. The **Add SSH Key** dialog box closes. You return to the **Local User** dialog box. |

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

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

Regions are configured during the first-time setup. When configured, you specify the regions that are managed by Cisco Cloud APIC and the region's inter-site and inter-region connectivity. This section explains how to manage regions with the cloud template using the Cisco Cloud APIC GUI after the initial installation.

For more information about cloud templates, see About the Cloud Template.

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

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

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

**Step 3** From the **Configuration** list in the **Intent** menu, click **Cloud APIC Setup**.
The **Set up - Overview** dialog box appears.

**Step 4** In the **Region Management** area, click **Edit Configuration**.

The **Setup - Region Management** dialog box appears. and the first step in the **Setup - Region Management** series of steps appears, **Regions to Manage**, with a list of managed regions.

**Step 5** If you want inter-site connectivity, click to place a check mark in the **Enabled** box in the **Inter-Site Connectivity** area. The **Inter-Site Connectivity** step is added in the **Setup - Region Management** steps at the top of the page.

**Step 6** To choose a region that you want to be managed by the Cisco Cloud APIC, click to place a check mark in check box of that region.

**Step 7** To deploy cloud routers locally to this region, click to place a check mark in the **Cloud Routers** check box for that region.

**Step 8** To configure the fabric infra connectivity for the cloud site, click **Next**.
The next step in the **Setup - Region Management** series of steps appears, **General Connectivity**

**Step 9** To add a subnet pool for the CCRs, click **Add Subnet Pool for Cloud Router** and enter the subnet in the text box.

**Note** The /24 subnet provided during the Cloud APIC deployment would be sufficient for up to two cloud sites. If you need to manage more than two cloud sites, you need to add more subnets.

**Step 10** Enter a value in the **BGP Autonomous System Number for CCRs** field.

The BGP ASN can be in the range of 1 - 65534.

**Step 11** In the **Assign Public IP to CCR Interface** field, determine if you want to have a public or a private IP address assigned to the CCR interface.

- To have a public IP address assigned to the CCR interface, leave the check in the **Enabled** check box. By default, the **Enabled** check box is checked.
- To have public IP disabled to the CCR interfaces, uncheck the **Enabled** check box. A private IP address is used for connectivity in this case.

**Note** Disabling or enabling a public IP address is a disruptive operation and can result in traffic loss.

Beginning with release 5.2(1), both the public and private IP addresses assigned to a CCR are displayed with the other details of the router in the Cloud Resources area. If a public IP is not assigned to a CCR, only the private IP is displayed.

**Step 12** To chose the number of routers per region, click the **Number of Routers Per Region** drop-down list and click **2**, **3**, or **4**.

**Step 13** Enter a username in the **Username** text box.

**Step 14** Enter a password in the **Password** and **Confirm Password** text boxes.

**Step 15** To choose the throughput value, click the **Throughput of the routers** drop-down list.

**Note**
- Cloud routers should be undeployed from all regions before changing the throughput or login credentials.
- Beginning with release 25.0(3), Cisco Cloud APIC moves from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V. For information on the throughput values for the Cisco Catalyst 8000V, see About the Cisco Catalyst 8000V.

**Step 16** (Optional) To specify the license token, enter the product instance registration token in the **License Token** text box.

**Note**

- Beginning with release 25.0(3), Cisco Cloud APIC moves from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V. For licensing information for the Cisco Catalyst 8000V, see About the Cisco Catalyst 8000V.
- If no token is entered, the CCR will be in EVAL mode.
- If the public IP addresses are disabled to the CCRs in Step 11, on page 67, the only supported option is **AWS Direct Connect or Azure Express Route to Cisco Smart Software Manager (CSSM)** when registering smart licensing for CCRs with private IP addresses (available by navigating to **Administrative** > **Smart Licensing**). You must provide reachability to the CSSM through AWS Direct Connect or Azure Express Route in this case. When the public IP addresses are disabled, public internet cannot be used because private IP addresses are being used. The connectivity should therefore use Private Connection, which is AWS Direct Connect or Azure Express Route.

**Step 17** Click **Next**.

- If you placed a check mark in the **Enabled** box in the **Inter-Site Connectivity** area earlier in these procedures, **Inter-Site Connectivity** appears as the next step in the **Setup - Region Management** series of steps. Go to Step 18, on page 68.
- If you did not place a check mark in the **Enabled** box in the **Inter-Site Connectivity** area earlier in these procedures, go to Step 22, on page 68.

**Step 18** To enter a peer public IP address of the IPsec Tunnel peer on-premises in the text box, click **Add Public IP of IPSec Tunnel Peer**.

**Step 19** Enter the OSPF area ID in the **OSPF Area Id** text box.

**Step 20** To add an external subnet pool, click **Add External Subnet** and enter a subnet pool in the text box.

**Step 21** When you have configured all the connectivity options, click **Next** at the bottom of the page.

**Step 22** Click **Save and Continue** when finished.

# Configuring Cisco Cloud APIC Using the REST API

## Creating a Tenant Using the REST API

This section demonstrates how to create a tenant and assigns using the REST API.

To create a tenant:

```
<polUni>
  <fvTenant name="infra">
    <cloudAwsProvider region="us-east-1" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"
 status=""/>
  </fvTenant>
</polUni>
```

# Creating a Contract Using the REST API

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

### Before you begin

Create filters.

To create a contract:

**Example:**

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

# Creating a Cloud Context Profile Using the REST API

This section demonstrates how to create a cloud context profile.

### Before you begin

Create a VRF.

**Step 1** For releases prior to release 25.0(2), enter a post similar to the following to create a cloud context profile:

**Example:**

```
<polUni>
<fvTenant name="Corp1" status="">
 <cloudAwsProvider accessKeyId="" secretAccessKey="" providerId="aws" status="" accountId=""/>

   <fvCtx name="prod-1" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

   <fvCtx name="prod-2" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="import"/>
    </bgpRtTargetP>
  </fvCtx>
```

```
  <cloudVpnGwPol name="VgwPol" status=""/>

  <cloudApp name="payment" status="">
    <cloudEPg  name="web" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-1" />
    </cloudEPg>
  </cloudApp>
  <cloudApp name="billing">
    <cloudEPg  name="app">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-2" />
    </cloudEPg>
  </cloudApp>

  <cloudCtxProfile name="prod-web-east-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-1"/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1"/>
    </cloudRouterP>

    <cloudCidr addr="60.10.10.1/16" primary="true">
        <cloudSubnet ip="60.10.10.1/24">
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-aws/region-us-east-1/zone-us-east-1a"/>
        </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>

  <cloudCtxProfile name="prod-payment-east-1" status="">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-2" status=""/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1" status=""/>
    </cloudRouterP>

    <cloudCidr addr="70.10.10.1/16" primary="true" status="">
       <cloudSubnet ip="70.10.10.1/24" status="">
           <cloudRsZoneAttach tDn="uni/clouddomp/provp-aws/region-us-east-1/zone-us-east-1a"/>
       </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>

</fvTenant>
</polUni>
```

**Step 2** To create a cloud context profile using the **cloud** availability zones supported beginning with release 25.0(2), enter a post such as the following example.

Beginning with release 25.0(2), if you are creating a cloud context profile in a **user** tenant, you are restricted to only **cloud** availability zones. The cloud availability zones are created through the `zone` field highlighted below. For more information on the cloud availability zones, see Availability Zones.

**Example:**

```
<polUni>
<fvTenant name="Corp1" status="">
 <cloudAwsProvider accessKeyId="" secretAccessKey="" providerId="aws" status="" accountId=""/>

   <fvCtx name="prod-1" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="import"/>
```

```
    </bgpRtTargetP>
  </fvCtx>

   <fvCtx name="prod-2" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <cloudVpnGwPol name="VgwPol" status=""/>

  <cloudApp name="payment" status="">
    <cloudEPg  name="web" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-1" />
    </cloudEPg>
  </cloudApp>
  <cloudApp name="billing">
    <cloudEPg  name="app">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-2" />
    </cloudEPg>
  </cloudApp>

  <cloudCtxProfile name="prod-web-east-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-1"/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1"/>
    </cloudRouterP>
    <cloudCidr addr="10.10.0.0/16" primary="yes">
        <cloudSubnet ip="10.10.1.0/24" usage="gateway" scope="public" zone=”us-west-1a"/>
        <cloudSubnet ip="10.10.2.0/24" scope="public" zone=”us-west-1b"/>
    </cloudCidr>
  </cloudCtxProfile>

  <cloudCtxProfile name="prod-payment-east-1" status="">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-2" status=""/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1" status=""/>
    </cloudRouterP>
    <cloudCidr addr="20.10.0.0/16" primary="yes">
        <cloudSubnet ip="20.10.1.0/24" scope="public" zone=”us-west-1a"/>
    </cloudCidr>
  </cloudCtxProfile>

</fvTenant>
</polUni>
```

# Managing a Cloud Region Using the REST API

This section demonstrates how to manage a cloud region using the REST API.

To create a cloud region:

```
<polUni>
```

```
  <cloudDomP name="dom-us-east-2">
    <cloudBgpAsP asn="64513"/>
    <cloudProvP vendor="aws">
      <cloudRegion name="us-east-2" adminSt="managed">
        <cloudZone name="us-east-2a"/>
        <cloudZone name="us-east-2b"/>
      </cloudRegion>
    </cloudProvP>
  </cloudDomP>
</polUni>
```

# Creating a Filter Using the REST API

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

To create a filter:

```
https://<IP_Address>/api/node/mo/.xml
<polUni>
<fvTenant name="intervpc" >
<fvCtx name="VRF1"/>
    <cloudApp name="CloudAP1" >
    <cloudEPg name="CloudEPG1" >
        <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
        <fvRsProv tnVzBrCPName="Contract2” > </fvRsProv>
        <cloudEPSelector name="sel1" matchExpression="custom:epgtag=='cloudepg1'" />
      </cloudEPg>
     </cloudApp>

      <vzFilter name="http" annotation="orchestrator:msc" >
      <vzEntry name="Entry3" prot="tcp" etherT="ipv4" arpOpc="unspecified" stateful="no"
applyToFrag="no" sFromPort="unspecified" sToPort="unspecified" dFromPort="80" dToPort="80" > </vzEntry>

    </vzFilter>

   <vzBrCP name="Contract2" scope="global">
      <vzSubj name="test-subj" >


        <vzRsSubjFiltAtt action="permit" tnVzFilterName="http" directives="none" />


      </vzSubj>
    </vzBrCP>
   </fvTenant>
</polUni>
```

# Creating an Application Profile Using the REST API

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

### Before you begin

Create a tenant.

To create an application profile:

```
https://<IP_Address>/api/node/mo/.xml
<polUni>
<fvTenant name="intervpc" >
<fvCtx name="VRF1"/>
    <cloudApp name="CloudAP1" >

    <cloudEPg name="CloudEPG1" >
        <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
        <fvRsProv tnVzBrCPName="Contract2” > </fvRsProv>
        <cloudEPSelector name="sel1" matchExpression="custom:epgtag=='cloudepg1'" />
      </cloudEPg>

     </cloudApp>

      <vzFilter name="http" annotation="orchestrator:msc" >
      <vzEntry name="Entry3" prot="tcp" etherT="ipv4" arpOpc="unspecified" stateful="no"
applyToFrag="no" sFromPort="unspecified" sToPort="unspecified" dFromPort="80" dToPort="80" > </vzEntry>

    </vzFilter>
   <vzBrCP name="Contract2" scope="global">
      <vzSubj name="test-subj" >
        <vzRsSubjFiltAtt action="permit" tnVzFilterName="http" directives="none" />
        </vzSubj>
    </vzBrCP>
   </fvTenant>
</polUni>
```

# Creating a Cloud EPG Using the REST API

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

### Before you begin

Create an application profile and a VRF.

To create a cloud EPG:

**Example:**

```
<polUni>
  <fvTenant name="t2" status="">
    <!-- Tenant provide AWS credentials -->
   <cloudAwsProvider region="us-east-2" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"/>

    <fvCtx name="v1" status=""/>
    <cloudApp name="ap">
      <cloudEPg name="provEPG" status="">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='provfoo'"/>
```

```
        <cloudEPSelector name="2" matchExpression="custom:tag=='provbaz'"/>
        <fvRsProv tnVzBrCPName="httpFamily"/>
      </cloudEPg>
      <cloudEPg name="consEPG">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='consfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='consbaz'"/>
        <fvRsCons tnVzBrCPName="httpFamily"/>
      </cloudEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

# Creating an External Cloud EPG Using the REST API

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

### Before you begin

Create an application profile and a VRF.

To create an external cloud EPG:

**Example:**

```
<polUni>
  <fvTenant name="t2" status="">
    <!-- Tenant provide AWS credentials -->
   <cloudAwsProvider region="us-east-2" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"/>

    <fvCtx name="v1" status=""/>
    <cloudApp name="ap">
      <cloudEPg name="provEPGInternet" status="">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='provfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='provbaz'"/>
        <fvRsProv tnVzBrCPName="httpFamily"/>
      </cloudEPg>
      <cloudExtEPg name="consInternetEPG">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
        <fvRsCons tnVzBrCPName="httpFamily"/>
      </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

# Creating a Cloud Template Using the REST API

This section demonstrates how to create a cloud template using the REST API. For more information about cloud templates, see About the Cloud Template.

The REST API will change depending on the type of Licensing model selected. The license type of the Cisco Catalyst 8000V is captured by the property `routerThroughput` in the `cloudtemplateProfile` managed object .

If the `routerThroughput` value belongs to **T0/T1/T2/T3** then **BYOL** Cisco Catalyst 8000V is deployed on Cisco Cloud APIC. If `routerThroughput` value is **PAYG** then **PAYG** Cisco Catalyst 8000V is deployed on Cisco Cloud APIC.

**Step 1** To create a cloud template post to deploy a **BYOL** Cisco Catalyst 8000V:

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerUsername="admin" routerPassword="rtpssw"
routerThroughput="15"
              routerLicenseToken="hYjZhYjItYTg0mrtrL15ocStS%0AUzRSZz0%3"
routerMgmtInterfacePublicIp="yes" routerDataInterfacePublicIp="yes"/>

      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-1"/>
        <cloudRegionName provider="aws" region="us-west-2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

       <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234" />


      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

**Note** Beginning with release 25.0(3), tier2 (T2) is the default throughput supported by Cisco Cloud APIC, which is indicated by the property `routerThroughput` in the `cloudtemplateProfile` managed object above.

**Step 2** To create a cloud template post to deploy a **PAYG** Cisco Catalyst 8000V:

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerUsername="admin" routerPassword="rtpssw"
routerThroughput="PAYG"
             vmName="c5.4xlarge" routerMgmtInterfacePublicIp="yes" routerDataInterfacePublicIp="yes"/>


      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
```

```
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-1"/>
        <cloudRegionName provider="aws" region="us-west-2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

       <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234" />


      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

On selecting PAYG throughput the user must also select the **vmName** from a list of vmNames which is created by Cloud APIC and represented by the managed object `vmName`.

The following table lists the vmNames that are indicated by the property `vmName` in the `cloudtemplateProfile`.

| AWS EC2 Instance | CCR Throughput | vCPUs | Memory |
|---|---|---|---|
| c5.xlarge | up to 5 Gigabit throughput | 4 | 8 GiB |
| c5.2xlarge | up to 10 Gigabit throughput | 8 | 16 GiB |
| c5.4xlarge | up to 10 Gigabit throughput | 16 | 32 GiB |
| c5.9xlarge | up to 10 Gigabit throughput | 36 | 72 GiB |
| c5n.xlarge | up to 25 Gigabit throughput | 4 | 10.5 GiB |
| c5n.2xlarge | up to 25Gigabit throughput | 8 | 21 GiB |
| c5n.4xlarge | up to 25 Gigabit throughput | 16 | 42 GiB |
| c5n.9xlarge | up to 50 Gigabit throughput | 36 | 96 GiB |

# Configuring VRF Leak Routes Using the REST API

### Before you begin

Review the information provided in Route Leaking Between Internal VRFs and Global Inter-VRF Route Leak Policy before proceeding with the instructions in this section.

**Step 1** Enter a post similar to the following to enable or disable contract-based routing.

```
<fvTenant name=”infra”>
    <cloudVrfRouteLeakPol name="default" allowContractBasedRouting=”true”/>
</fvTenant>
```

Where the `allowContractBasedRouting` field has either of the following settings:

- **true**: Indicates that routes are leaked based on contracts in the absence of route maps. When enabled, contracts drive routing when route maps are not configured. When route maps exist, route maps always drives routing.
- **false**: Default setting. Indicates that routes are not leaked based on contracts, and are leaked based on route maps instead.

**Step 2** Enter a post similar to the following to use the `leakInternalPrefix` field to configure route leaking for all cloud CIDRs associated with the VRFs.

```
<fvTenant name=”t1”>
  <fvCtx name="v1">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t2" ctxName="v2" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>

<fvTenant name=”t2”>
  <fvCtx name="v2">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t1" ctxName="v1" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>
```

**Step 3** Enter a post similar to the following to use the `leakInternalSubnet` field to leak specific routes between a pair of VRFs.

```
<fvTenant name=”anyTenant" status="">
    <fvCtx name="VRF1" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.1.0/24" >
                <leakTo ctxName=”VRF2" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
    <fvCtx name="VRF2" status="" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.2.0/24" >
                <leakTo ctxName=”VRF1" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
</fvTenant>
```

# Configuring the Source Interface Selection for Tunnels Using the REST API

### Before you begin

Review the information provided in Source Interface Selection for Tunnels before proceeding with these instructions.

Enter a post similar to the following to configure the source interface selection for tunnels.

```
<cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
  <cloudtemplateProfile name="defaultxyz" routerUsername="james" routerPassword="bond@@7" />

  <cloudtemplateIpSecTunnelSubnetPool subnetpool="10.20.0.0/16" poolname="pool1" />

  <cloudtemplateIntNetwork name="default">
    <cloudRegionName provider="aws" region="us-west-1"/>
    <cloudRegionName provider="aws" region="us-west-2"/>
  </cloudtemplateIntNetwork>

  <cloudtemplateExtNetwork name="something" vrfName="xyz" >
    <cloudRegionName provider="aws" region="us-west-2"/>
    <cloudtemplateVpnNetwork name="default">
      <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" poolname="" presharedkey="abcd"
ikeVersion="v1|v2">
          <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId="2" />
      </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
```