Configuring and Managing Sites

Pod Profile and Policy Group

In each site's APIC, you must have one Pod profile with a Pod policy group. If you site does not have a Pod policy group you must create one.

To check if the POD profile contains a POD policy group:

- Navigate to the Cisco APIC GUI, **Fabric** > **Fabric Policies** > **Pods** > **Profiles** > **Pod Profile default**.

To create a POD policy group:

- Navigate to the Cisco APIC GUI, **Fabric** > **Fabric Policies** > **Pods** > **Policy Groups**, right-click **Policy Groups** and click **Create Pod Policy Group**. Enter the appropriate information and click **Submit**.

To assign the new pod policy group to the default POD profile:

- Navigate to the Cisco APIC GUI, **Fabric** > **Fabric Policies** > **Pods** > **Profiles** > **Pod Profile default**. Click on the default, choose the new pod policy group and click **Update**.

Configuring Fabric Access Policies for All APIC Sites

Before your APIC fabrics can be added to and managed by the Multi-Site Orchestrator, there is a number of fabric-specific access policies that you must configure on each site.

Configuring Fabric Access Global Policies

This section describes the global fabric access policy configurations that must be created for each APIC site before it can be added to and managed by the Multi-Site Orchestrator.

Step 1 Log in directly to the site's APIC GUI.

Step 2 From the main navigation menu, select **Fabric** > **Access Policies**.

You must configure a number of fabric policies before the site can be added to the Multi-Site Orchestrator. From the APIC's perspective, this is something you do just like you would if you were connecting a bare-metal host, where you would configure domains, AEPs, policy groups, and interface selectors; you must configure the same options for connecting the spine switch interfaces to the inter-site network for all the sites that will be part of the same Multi-Site domain.

Step 3 Specify the VLAN pool.

The first thing you configure is the VLAN pool. We use Layer 3 sub-interfaces tagging traffic with VLAN-4 to connect the spine switches to the inter-site network.

a) In the left navigation tree, browse to **Pools** > **VLAN**.
b) Right-click the **VLAN** category and choose **Create VLAN Pool**.

In the **Create VLAN Pool** window, specify the following:

- For the **Name** field, specify the name for the VLAN pool, for example `msite`.
- For **Allocation Mode**, specify `Static Allocation`.
- And for the **Encap Blocks**, specify just the single VLAN 4. You can specify a single VLAN by entering the same number in both **Range** fields.

Step 4 Configure Attachable Access Entity Profiles (AEP).

a) In the left navigation tree, browse to **Global Policies** > **Attachable Access Entity Profiles**.
b) Right-click the **Attachable Access Entity Profiles** category and choose **Create Attachable Access Entity Profiles**.

In the **Create Attachable Access Entity Profiles** window, specify the name for the AEP, for example `msite-aep`.

c) Click **Next** and **Submit**

No additional changes, such as interfaces, are required.

Step 5 Configure domain.

The domain you configure is what you will select from the Multi-Site Orchestrator when adding this site.

a) In the left navigation tree, browse to **Physical and External Domains** > **External Routed Domains**.
b) Right-click the **External Routed Domains** category and choose **Create Layer 3 Domain**.

In the **Create Layer 3 Domain** window, specify the following:

- For the **Name** field, specify the name the domain, for example `msite-l3`.
- For **Associated Attachable Entity Profile**, select the AEP you created in Step 4.
- For the **VLAN Pool**, select the VLAN pool you created in Step 3.

c) Click **Submit**.

No additional changes, such as security domains, are required.

What to do next

After you have configured the global access policies, you must still add interfaces policies as described in Configuring Fabric Access Interface Policies, on page 3.

Configuring Fabric Access Interface Policies

This section describes the fabric access interface configurations that must be done for the Multi-Site Orchestrator on each APIC site.

Before you begin

You must have configured the global fabric access policies, such as VLAN Pool, AEP, and domain, in the site's APIC, as described in Configuring Fabric Access Global Policies, on page 2.

Step 1 Log in directly to the site's APIC GUI.

Step 2 From the main navigation menu, select **Fabric** > **Access Policies**.

In addition to the VLAN, AEP, and domain you have configured in previous section, you must also create the interface policies for the fabric's spine switch interfaces that connect to the Inter-Site Network (ISN).

Step 3 Configure a spine policy group.

a) In the left navigation tree, browse to **Interface Policies** > **Policy Groups** > **Spine Policy Groups**.

This is similar to how you would add a bare-metal server, except instead of a Leaf Policy Group, you are creating a Spine Policy Group.

b) Right-click the **Spine Policy Groups** category and choose **Create Spine Access Port Policy Group**.

In the **Create Spine Access Port Policy Group** window, specify the following:

- For the **Name** field, specify the name for the policy group, for example `Spine1-PolGrp`.
- For the **Link Level Policy** field, specify the link policy used between your spine switch and the ISN.
- For **CDP Policy**, choose whether you want to enable CDP.
- For the **Attached Entity Profile**, select the AEP you have configured in previous section, for example `msite-aep`.

c) Click **Submit**.

No additional changes, such as security domains, are required.

Step 4 Configure a spine profile.

a) In the left navigation tree, browse to **Interface Policies** > **Profiles** > **Spine Profiles**.

b) Right-click the **Spine Profiles** category and choose **Create Spine Interface Profile**.

In the **Create Spine Interface Profile** window, specify the following:

- For the **Name** field, specify the name for the profile, for example `Spine1-ISN`.

- For **Interface Selectors**, click the **+** sign to add the port on the spine switch that connects to the ISN. Then in the **Create Spine Access Port Selector** window, provide the following:
  - For the **Name** field, specify the name for the port selector, for example `Spine1-ISN`.
  - For the **Interface IDs**, specify the switch port that connects to the ISN, for example `5/32`.
  - For the **Interface Policy Group**, choose the policy group you created in the previous step, for example `Spine1-PolGrp`.

  Then click **OK** to save the port selector.

c) Click **Submit** to save the spine interface profile.

Step 5 Configure a spine switch selector policy.

a) In the left navigation tree, browse to **Switch Policies** > **Profiles** > **Spine Profiles**.

b) Right-click the **Spine Profiles** category and choose **Create Spine Profile**.

In the **Create Spine Profile** window, specify the following:

- For the **Name** field, specify the name for the profile, for example `Spine1`.
- For **Spine Selectors**, click the **+**to add the spine and provide the following:
  - For the **Name** field, specify the name for the selector, for example `Spine1`.
  - For the **Blocks** field, specify the spine node, for example `201`.

c) Click **Update** to save the selector.

d) Click **Next** to proceed to the next screen.

e) Select the interface profile you have created in the previous step

For example `Spine1-ISN`.

f) Click **Finish** to save the spine profile.

Configuring Sites That Contain Remote Leaf Switches

Starting with Release 2.1(2), the Multi-Site architecture supports APIC sites with Remote Leaf switches. The following sections describe guidelines, limitations, and configuration steps required to allow Multi-Site Orchestrator to manage these sites.

Multi-Site and Remote Leaf Guidelines and Limitations

If you want to add an APIC site with a Remote Leaf to be managed by the Multi-Site Orchestrator, the following restrictions apply:

- You must upgrade your Cisco APIC to Release 4.1(2) or later.
- You must upgrade your Multi-Site Orchestrator to Release 2.1(2) or later.
- Only physical Remote Leaf switches are supported in this release

- Only -EX and -FX or later switches are supported as Remote Leaf switches for use with Multi-Site:
- Remote Leaf is not supported with back-to-back connected sites without IPN switches
- Remote Leaf switches in one site cannot use another site's L3out
- Stretching a bridge domain between one site and a Remote Leaf in another site is not supported

You must also perform the following tasks before the site can be added to and managed by the Multi-Site Orchestrator:

- You must enable Remote Leaf direct communication and configure routable subnets directly in the site's APIC, as described in the following sections.
- You must add the routable IP addresses of Cisco APIC nodes in the DHCP-Relay configuration applied on the interfaces of the Layer 3 routers connecting to the Remote Leaf switches.

  The routable IP address of each APIC node is listed in the **Routable IP** field of the **System** > **Controllers** > **<controller-name>** screen of the APIC GUI.

Configuring Routable Subnets for Remote Leaf Switches

Before you can add a site that contains one or more Remote Leaf switches to the Multi-Site Orchestrator, you must configure routable subnets for the pod with which the Remote Leaf nodes are associated.

Step 1 Log in directly to the site's APIC GUI.

Step 2 From the menu bar, select **Fabric** > **Inventory**.

Step 3 In the Navigation pane, click **Pod Fabric Setup Policy**.

Step 4 In the main pane, double-click the pod where you want to configure the subnets.

Step 5 In the **Routable Subnets** area, click the **+** sign to add a subnet.

Step 6 Enter the **IP** and **Reserve Address Count**, set the state to `Active` or `Inactive`, then click **Update** to save the subnet.

When configuring routable subnets, you must provide a netmask between `/22` and `/29`.

Step 7 Click **Submit** to save the configuration.

Enabling Direct Communication for Remote Leaf Switches

Before you can add a site that contains one or more Remote Leaf switches to the Multi-Site Orchestrator, you must configure direct remote leaf communication for that site. Additional information about remote leaf direct communication feature is available in the *Cisco APIC Layer 3 Networking Configuration Guide*. This section outlines the steps and guidelines specific to the integration with Multi-Site.

Note Once you enable Remote Leaf switch direct communication, the switches will function in the new mode only

Step 1 Log in directly to the site's APIC.

Step 2 Enable direct traffic forwarding for Remote Leaf switches.

a) From the menu bar, navigate to **System** > **System Settings**.
b) From the left side bar, select **Fabric Wide Setting**.
c) Check the **Enable Remote Leaf Direct Traffic Forwarding** checkbox.

Note You cannot disable this option after you enable it.

d) Click **Submit** to save the changes.

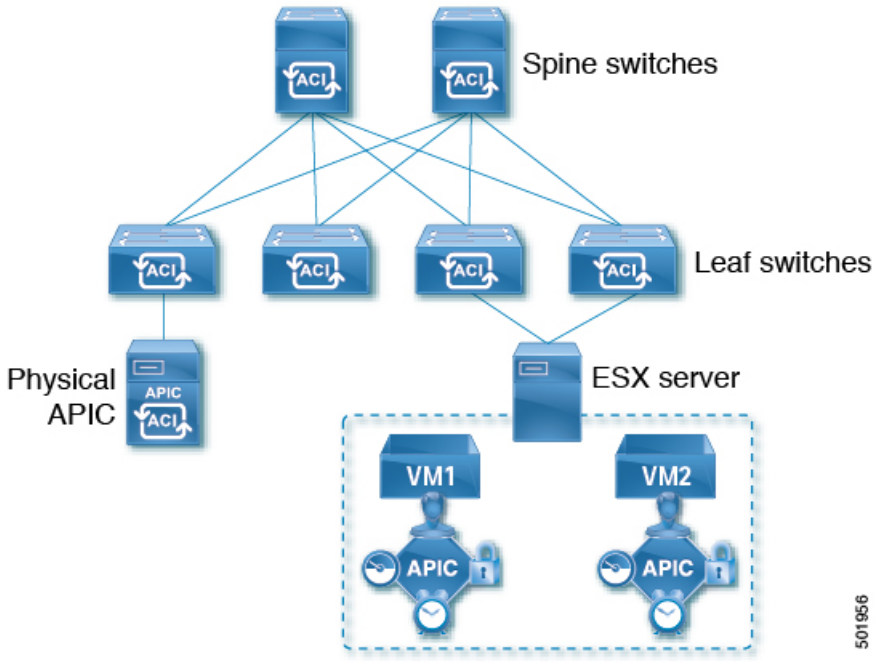
Cisco Mini ACI Fabrics

Cisco ACI Multi-Site supports Cisco Mini ACI fabrics as typical on-premises sites without requiring any additional configuration. This section provides brief overview of Mini ACI fabrics, detailed info on deploying and configuring this type of fabrics is available in *Cisco Mini ACI Fabric and Virtual APICs*.

Cisco ACI, Release 4.0(1) introduced Mini ACI Fabric for small scale deployment. Mini ACI fabric works with Cisco APIC cluster consisting of one physical APIC and two virtual APICs (vAPIC) running in virtual machines. This reduces the physical footprint and cost of the APIC cluster, allowing ACI fabric to be deployed in scenarios with limited rack space or initial budget, such as a colocation facility or a single-room data center, where a full-scale ACI installations may not be practical due to physical footprint or initial cost.

The following diagram shows an example of a mini Cisco ACI fabric with a physical APIC and two virtual APICs (vAPICs):

Figure 1: Cisco Mini ACI Fabric



Adding Sites

This section describes how to add sites using the Cisco ACI Multi-Site Orchestrator GUI.

Before you begin

You must have completed the site-specific configurations in each site's APIC, as decribed in previous sections in this chapter.

Step 1 Log in to the Multi-Site GUI, in the **Main menu**, click **Sites**.

If you are logging in for the first time, log in as the **admin** user with the default password **We1come2msc!**, you will then be prompted to change that default password. The new password requirements are:

- At least 12 characters
- At least 1 letter
- At least 1 number
- At least 1 special character apart from * and space

Step 2 In the **Main menu**, select **Infrastructure** > **Sites**.

Step 3 In the top right of the main pane, click **Add Site**.

Step 4 In the **Add Site** screen, provide the site's details.

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

b) In the **Labels** field, choose or create a label.

You can choose to provide multiple labels for the site.

c) In the **APIC Controller URL** field, enter the Cisco APIC URL.

For the APIC URL, you can use the `http` or `https` protocol and the IP address or the DNS hostname, such as`https://<ip-address>` or `https://<dns-hostname>`.

d) If you have a cluster of APICs in the fabric, click **+APIC Controller URL** and provide the additional URLs.

e) In the **Username** field, enter the admin user's username for the site's APIC.

f) In the **Password** field, enter the user's password.

g) You can turn on the **Specify Login Domain for Site** switch, if you want to specify a domain to be used for authenticating the user you provided.

If you turn on this option, enter the domain name in the **Domain Name** field.

h) In the **APIC Site ID** field, enter a unique site ID.

The site ID must be a unique identifier of the Cisco APIC site, ranged between `1` and `127`. Once specified, the site ID cannot be changed without factory resetting Cisco APIC.

Step 5 Click **Save** to add the site.

Step 6 If prompted, confirm proxy configuration update.

If you have configured the Orchestrator to use a proxy server and are adding an on-premises site that is not already part of the "no proxy" list, the Orchestrator will inform you of the proxy settings update.

For additional information on proxy configuration, see the "Administrative Operations" chapter in *Cisco ACI Multi-Site Configuration Guide*.

Step 7 Repeat these steps to add any additional sites.

Deleting Sites Using Multi-Site Orchestrator GUI

This section describes how to delete sites using the Multi-Site GUI.

Step 1 Log in to the Multi-Site GUI.

Step 2 Ensure you unbind the site from any Schema's before trying to delete the site.

Step 3 In the **Main menu**, click **Sites**.

Step 4 In the **Sites List** page, hover over the site you want to delete and choose **Action** > **Delete** .

Step 5 Click **YES**.

Multi-Site Cross Launch to Cisco APIC

Multi-Site currently supports the basic parameters to choose when creating a Tenant and setting up a site. Multi-Site supports most of the Tenant policies, but in addition to that you can configure some advanced parameters.

Use the Multi-Site GUI to manage the basic properties to configure. If you want to configure advanced properties, the capability to cross launch into Cisco APIC GUI directly from the Multi-Site GUI is provided. You can also configure the additional properties directly in Cisco APIC.

There are three different access points in Multi-Site GUI from where you can cross launch into APIC. From these access points in Multi-Site, you can open a new browser tab with access into Cisco APIC. You will log in to Cisco APIC at that point for the first time, and the associated screen is displayed in the Cisco APIC GUI.

Cross-Launch to Cisco APIC from Sites

Before you begin

- At least one site must be configured in Multi-Site.
- The site must contain at least one tenant with entities such as VRF and bridge domain configured.

Step 1 From the left-hand sidebar, open the **Sites** view.

Step 2 From the **Sites** list, hover over the name of the appropriate site, click the **Actions** icon at the end of the row, and choose **Open in APIC User Interface** to access the Cisco APIC GUI.

The APIC GUI login screen is displayed for logging in with APIC GUI credentials.

Cross-Launch to Cisco APIC from Schemas

Before you begin

- At least one site based on a template must be configured in Multi-Site.
- The site must contain at least one tenant with entities such as VRF and bridge domain configured.

Step 1 From the left-hand sidebar, open the **Schemas** view.

Step 2 From the **Schemas** list, click the appropriate <***schema-name***>.

Step 3 From the left-hand sidebar **Sites** list, hover over the name of the appropriate site, click the **Actions** icon at the end of the row, and choose **Open in APIC User Interface** to access the Cisco APIC GUI.

The APIC GUI login screen is displayed for logging in with APIC GUI credentials.

Cross-Launch to Cisco APIC from the Property Pane

Before you begin

- At least one site must be configured in Multi-Site.
- The site must contain at least one tenant with entities such as VRF and bridge domain configured.

Step 1 From the left-hand sidebar, open the **Schemas** view.

Step 2 From the **Schemas** list, click the appropriate <***schema-name***>.

Step 3 From the left-hand sidebar **Sites** list, choose the appropriate site.

Step 4 In the **Canvas**, choose the name of a specific entity.

For example, choose an available VRF, Contract, Bridge Domain, or another entity as appropriate.

The details for the specific entity are displayed in the **Property Pane** on the right.

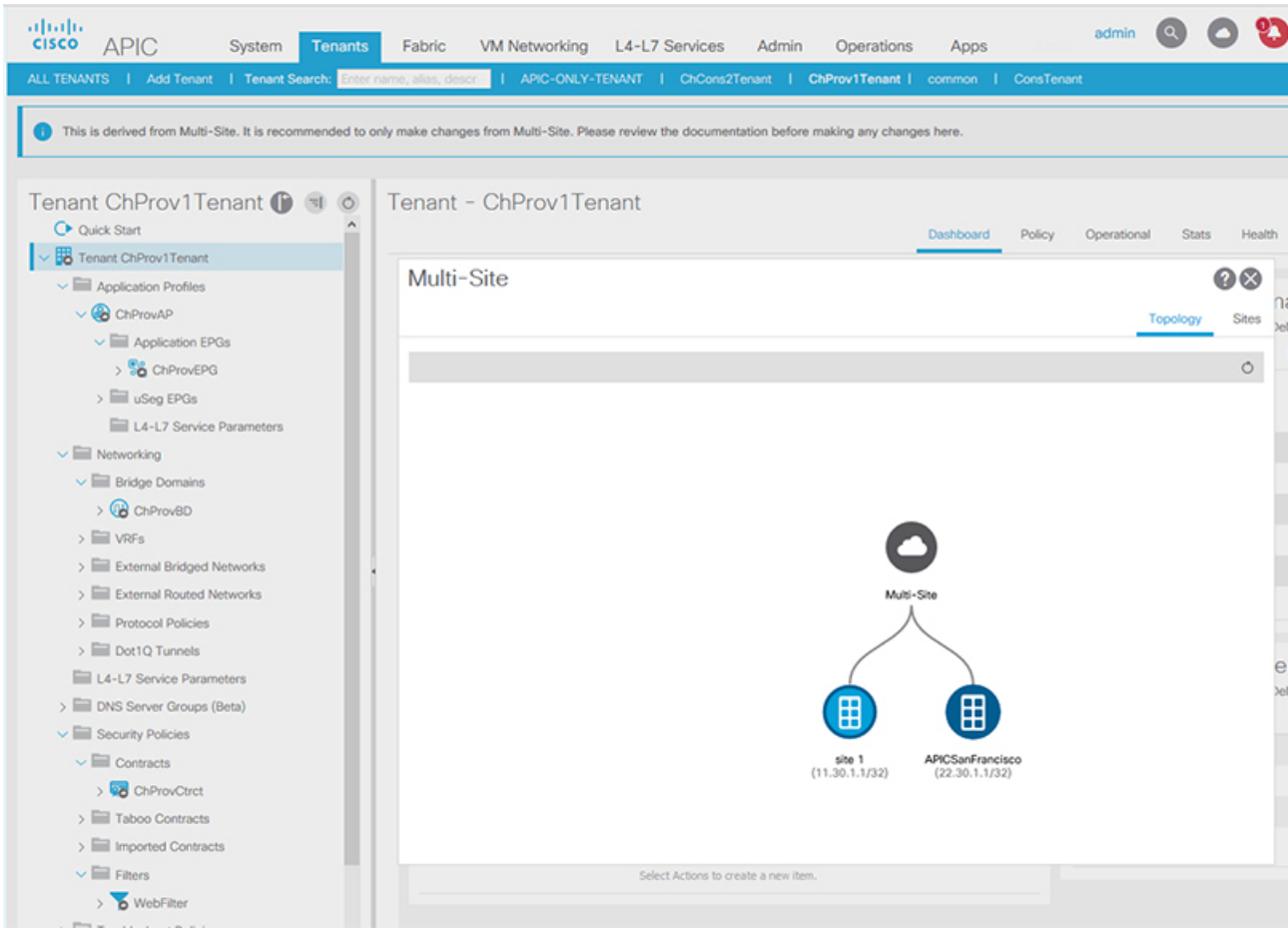
Step 5 In the top right of the **Property Pane**, click the **Open in APIC User Interface** icon to access the Cisco APIC GUI.

The APIC GUI login screen is displayed for logging in with APIC GUI credentials.

Viewing Cisco ACI Multi-Site-Managed Objects Using the Cisco APIC GUI

When an APIC cluster is managed by Multi-Site, cloud icons indicate the relationships with other sites.

Figure 2: Viewing Multi-Site-Managed Objects Using the APIC GUI



Before you begin

The APIC cluster/site must be set up to be managed by Cisco ACI Multi-Site.

Step 1 To view the relationship of the APIC site with other sites, click the cloud icon at the upper right, next to the settings icons.

In the diagram, hover over the light blue site icon to see the local site details, and hover over the dark blue icon to see the remote site details.

In the image, T1 and its Application Profile, EPG, BD, VRF, and contracts are marked with cloud icons. This indicates that they are managed by Multi-Site. We recommend that you only make changes to these objects in the Multi-Site GUI.

Step 2 To view the localized or stretched usage of a VRF, bridge domain, or other objects, where there is a **Show Usage** button on the information page, perform the following steps; for example for Bridge Domain and VRF:

a) On the menu bar, click **Tenants** and double-click on a tenant that is managed by Multi-Site.

b) Click **Networking** > **Bridge Domains** > ***BD-name*** or **Networking** > **VRFs** > ***vrf-name***.

Step 3 Click **Show Usage**.

Here you can view the nodes or policies using the object.

Note It is recommended to make changes to managed policies only in the Multi-Site GUI.

Step 4 To set the scope of deployment notification settings for this BD or VRF, click **Change Deployment Settings**. You can enable warnings to be sent for all deletions and modifications of the object on the **Policy** tab.

Step 5 To enable or disable Global warnings, check or uncheck the **(Global) Show Deployment Warning on Delete/Modify** check box.

Step 6 To enable or disable Local warnings, choose **Yes** or **No** on the **(Local) Show Deployment Warning on Delete/Modify** field.

Step 7 To view any past warnings, click the **History** tab **Events** or **Audit Logs**.