



Configuring Infra for Cisco Cloud APIC Sites

- [Refreshing Cloud Site Connectivity Information, on page 1](#)
- [Configuring Infra: Cloud Site Settings, on page 1](#)

Refreshing Cloud Site Connectivity Information

Any infrastructure changes, such as CSR and Region addition or removal, require a Multi-Site fabric connectivity site refresh. This section describes how to pull up-to-date connectivity information directly from each site's APIC.

-
- Step 1** Log in to the Cisco Nexus Dashboard Orchestrator GUI.
- Step 2** In the Main menu, select Infrastructure > Infra Configuration.
- Step 3** In the top right of the main Infra Configuration view, click the Configure Infra button.
- Step 4** In the left pane, under Sites, select a specific site.
- Step 5** In the main window, click the Refresh button to discover any new or changed CSRs and regions.
- Step 6** Finally, click Yes to confirm and load the connectivity information.
- This will discover any new or removed CSRs and regions.
- Step 7** Click Deploy to propagate the cloud site changes to other sites that have connectivity to it.
- After you refresh a cloud site's connectivity and CSRs or regions are added or removed, you need to deploy infra configuration so other sites that have underlay connectivity to that cloud site get updated configuration.

Configuring Infra: Cloud Site Settings

This section describes how to configure site-specific Infra settings for Cloud APIC sites.

-
- Step 1** Log in to the Cisco Nexus Dashboard Orchestrator GUI.
- Step 2** In the Main menu, select Infrastructure > Infra Configuration.
- Step 3** In the top right of the main pane, click Configure Infra.

Step 4 In the left pane, under Sites, select a specific cloud site.

Step 5 Provide Inter-Site Connectivity information.

Provide the Overlay Configuration:

- a) In the right *<Site>* Settings pane, select the Inter-Site Connectivity tab.
- b) In the Overlay Configuration area, enable the Multi-Site knob.

This defines whether the overlay connectivity is established between this site and other sites.

- c) (Optional) Specify the BGP Password.

Provide Inter-Site Connectivity information.

- a) In the Underlay Configuration area, click Add Connectivity.
- b) From the Site dropdown, select the site to which you want to establish connectivity.
- c) From the Connection Type dropdown, choose the type of connection between the sites.

The following options are available:

- **Public Internet**—connectivity between the two sites is established via the Internet.
This type is supported between any two cloud sites or between a cloud site and an on-premises site.
- **Private Connection**—connectivity is established using a private connection between the two sites.
This type is supported between a cloud site and an on-premises site.
- **Cloud Backbone**—connectivity is established using cloud backbone.

This type is supported between two cloud sites of the same type, such as Azure-to-Azure or AWS-to-AWS.

If you have multiple types of sites (on-premises, AWS, and Azure), different pairs of site can use different connection type.

- d) (Optional) Enable IPsec.

The following options are available:

- For **Public Internet** connectivity, IPsec is always enabled.
- For **Cloud Backbone** connectivity, IPsec is always disabled.
- For **Private Connection**, you can choose to enable or disable IPsec.

- e) If IPsec is enabled, choose the IKE Version for it.

Internet Key Exchange (IKE) is a protocol used to establish security association for IPsec. You can choose which version of the protocol to use: IKEv1 (*Version 1*) or IKEv2 (*Version 1*) depending on your configuration.

- f) Click Save to save the inter-site connectivity configuration.

When you save connectivity information from *Site1* to *Site2*, the reverse connectivity is automatically created from *Site2* to *Site1*, which you can see by selecting the other site and checking the Underlay Configuration tab.

- g) Repeat this step to add inter-site connectivity for other sites.

When you establish underlay connectivity from *Site1* to *Site2*, the reverse connectivity is done automatically for you.

However, if you also want to establish inter-site connectivity from *Site1* to *Site3*, you must repeat this step for that site as well.

Step 6 Provide External Connectivity information.

If you do not plan to configure connectivity to external sites or devices that are not managed by NDO, you can skip this step. Otherwise, provide the following information:

a) In the right **<Site>** Settings pane, select the External Connectivity tab.

b) Click Add External Connection.

The Add External Connectivity dialog will open.

c) From the VRF dropdown, select the VRF you want to use for external connectivity.

This is the VRF which will be used to leak the cloud routes. The Regions section will display the cloud regions that contain the CSRs to which this configuration be applied.

d) From the Name dropdown in the External Devices section, select the external device.

This is the external device you added in the General Settings > External Devices list during general infra configuration and must already be defined as described in [Configuring Infra: General Settings](#).

e) From the Tunnel IKE Version dropdown, pick the IKE version that will be used to establish the IPSec tunnel between the cloud site's CSRs and the external device.

f) (Optional) From the Tunnel Subnet Pool dropdown, choose one of the named subnet pools.

Named subnet pool are used to allocate IP addresses for IPSec tunnels between cloud site CSRs and external devices. If you do not provide any named subnet pools here, the external subnet pool will be used for IP allocation.

Providing a dedicated subnet pool for external device connectivity is useful for cases where a specific subnet is already being used to allocate IP addresses to the external router and you want to continue to use those subnets for IPSec tunnels for NDO and cloud sites.

If you want to provide a specific subnet pool for this connectivity, it must already be created as described in [Configuring Infra: General Settings](#).

g) (Optional) In the Pre-Shared Key field, provide the custom keys you want to use to establish the tunnel.

h) If necessary, repeat the previous substeps for any additional external devices you want to add for the same external connection (same VRF).

i) If necessary, repeat this step for any additional external connections (different VRFs).

Note that there's a one-to-one relationship for tunnel endpoints between CSRs and external devices, so while you can create additional external connectivity using different VRFs, you cannot create additional connectivity to the same external devices.

What to do next

While you have configured all the required inter-site connectivity information, it has not been pushed to the sites yet. You need to deploy the configuration as described in [Deploying Infra Configuration](#)

