



# Deploying Infra Configuration for ACI Sites

---

- [Deploying Infra Configuration, on page 1](#)
- [Enabling Connectivity Between On-Premises and Cloud Sites, on page 2](#)

## Deploying Infra Configuration

This section describes how to deploy the Infra configuration to each APIC site.

---

- Step 1** In the top right of the main pane, click **Deploy** and choose the appropriate option to deploy the configuration. If you have configured only on-premises or only cloud sites, simply click **Deploy** to deploy the Infra configuration. However, if you have both, on-premises and cloud site, the following two additional options become available:
- **Deploy & Download IPN Device config files:** Pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect between the on-premises and the cloud sites. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router (CSR) deployed in your cloud sites and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.
  - **Download IPN Device config files only:** Downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router (CSR) without deploying the configuration.

- Step 2** In the confirmation window, click **Yes**. The Deployment started, refer to left menu for individual site deployment status message will indicate that Infra configuration deployment began and you can verify each site's progress by the icon displayed next to the site's name in the left pane.
- 

### What to do next

The Infra overlay and underlay configuration settings are now deployed to all sites' controllers and cloud CSRs. The last remaining step is to configure your IPN devices with the tunnels for cloud CSRs as described in [Refreshing Site Connectivity Information](#).

# Enabling Connectivity Between On-Premises and Cloud Sites

If you have only on-premises or only cloud sites, you can skip this section.

This section describes how to enable connectivity between on-premises APIC sites and Cloud APIC sites.

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

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

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

You can get the required configuration details using either the **Deploy & Download IPN Device config files** or the **Download IPN Device config files only** option in Nexus Dashboard Orchestrator as part of the procedures provided in [Deploying Infra Configuration, on page 1](#).

**Step 2** Log into the on-premises IPsec device.

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

Details for the first CSR are available in the configuration files for the ISN devices you downloaded from the Nexus Dashboard Orchestrator, but the following fields describe the important values for your specific deployment:

- `<first-csr-tunnel-ID>`—unique tunnel ID that you assign to this tunnel.
- `<first-csr-ip-address>`—public IP address of the third network interface of the first CSR.

The destination of the tunnel depends on the type of underlay connectivity:

- The destination of the tunnel is the public IP of the cloud router interface if the underlay is via public internet
- The destination of the tunnel is the private IP of the cloud router interface if the underlay is via private connectivity, such as DX on AWS or ER on Azure
- `<first-csr-preshared-key>`—preshared key of the first CSR.
- `<onprem-device-interface>`—interface that is used for connecting to the Cisco Cloud Services Router 1000V deployed in Amazon Web Services.
- `<onprem-device-ip-address>`—IP address for the `<interface>` interface that is used for connecting to the Cisco Cloud Services Router 1000V deployed in Amazon Web Services.
- `<peer-tunnel-for-onprem-IPsec-to-first-CSR>`—peer tunnel IP address for the on-premises IPsec device to the first cloud CSR.
- `<process-id>` —OSPF process ID.
- `<area-id>`—OSPF area ID.

The following example shows intersite connectivity configuration using the IKEv2 protocol supported starting with Nexus Dashboard Orchestrator, Release 3.3(1) and Cloud APIC, Release 5.2(1). If you are using IKEv1, the IPN configuration file you downloaded from NDO may look slightly differently, but the principle remains the same.

```
crypto ikev2 proposal ikev2-proposal-default
  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-policy-default
  proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
  peer peer-ikev2-keyring
    address <first-csr-ip-address>
    pre-shared-key <first-csr-preshared-key>
  exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
  match address local interface <onprem-device-interface>
  match identity remote address <first-csr-ip-address> 255.255.255.255
  identity local address <onprem-device-ip-address>
  authentication remote pre-share
  authentication local pre-share
  keyring local key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
  lifetime 3600
  dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-<first-csr-tunnel-id> esp-gcm 256
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-csr-tunnel-id>
  set pfs group14
  set ikev2-profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
  set transform-set infra:overlay-1-<first-csr-tunnel-id>
exit

interface tunnel 2001
  ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <onprem-device-interface>
  tunnel destination <first-csr-ip-address>
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-<first-csr-tunnel-id>
  ip mtu 1400
  ip tcp adjust-mss 1400
  ip ospf <process-id> area <area-id>
  no shut
exit
```

### Example:

```
crypto ikev2 proposal ikev2-proposal-default
  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-policy-default
  proposal ikev2-proposal-default
```

```

exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-2001
  peer peer-ikev2-keyring
    address 52.12.232.0
    pre-shared-key 1449047253219022866513892194096727146110
  exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-2001
  ! Please change GigabitEthernet1 to the appropriate interface
  match address local interface GigabitEthernet1
  match identity remote address 52.12.232.0 255.255.255.255
  identity local address 128.107.72.62
  authentication remote pre-share
  authentication local pre-share
  keyring local key-ikev2-infra:overlay-1-2001
  lifetime 3600
  dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-2001 esp-gcm 256
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-2001
  set pfs group14
  set ikev2-profile ikev2-infra:overlay-1-2001
  set transform-set infra:overlay-1-2001
exit

! These tunnel interfaces establish point-to-point connectivity between the on-prem device and the
! cloud Routers
! The destination of the tunnel depends on the type of underlay connectivity:
! 1) The destination of the tunnel is the public IP of the cloud Router interface if the underlay is
!    via internet
! 2) The destination of the tunnel is the private IP of the cloud Router interface if the underlay
!    is via private
!    connectivity like DX on AWS or ER on Azure

interface tunnel 2001
  ip address 5.5.1.26 255.255.255.252
  ip virtual-reassembly
  ! Please change GigabitEthernet1 to the appropriate interface
  tunnel source GigabitEthernet1
  tunnel destination 52.12.232.0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-2001
  ip mtu 1400
  ip tcp adjust-mss 1400
  ! Please update process ID according with your configuration
  ip ospf 1 area 0.0.0.1
  no shut
exit

```

**Step 4** Repeat the previous step for the 2nd and any additional CSRs that you need to configure.

**Step 5** Verify that the tunnels are up on your on-premises IPsec device.

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

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

---

