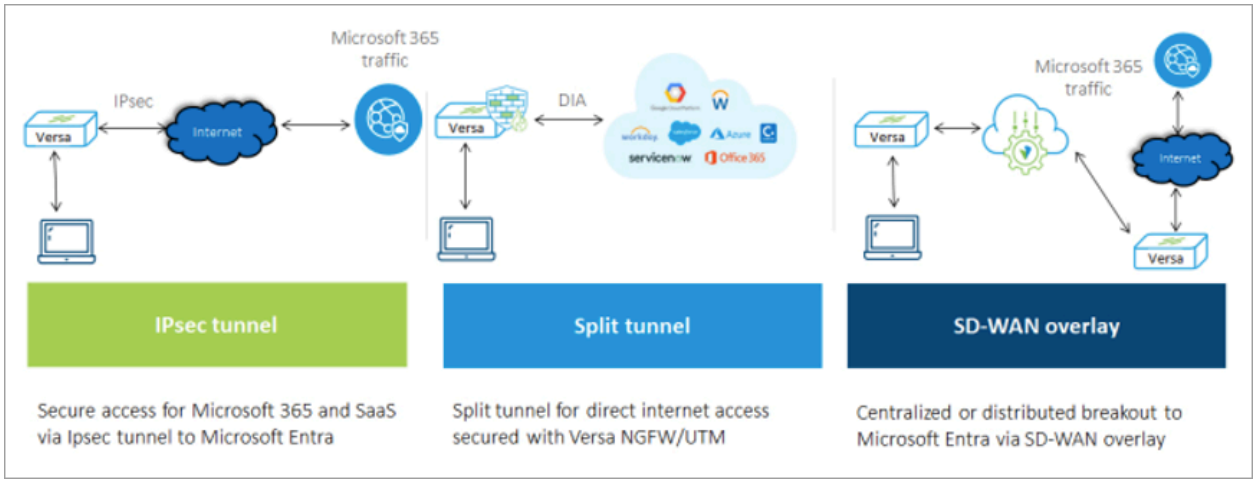
Versa Secure SD-WAN and Microsoft Entra Internet Access APIBased Integration

This article describes how to integrate Versa Secure SD-WAN with Microsoft Entra Internet Access. Versa uses workflows to automate the configuration and provisioning of the IPsec tunnels to Microsoft Entra Internet Access. The Versa secure SD-WAN integration creates two IPsec tunnels to Microsoft Entra Internet Access and both tunnels peer via BGP to two different zones for redundancy within Microsoft Entra. Equal Cost Multipath (ECMP) load balancing is enabled by default.

Versa's API-based integration with Microsoft Entra Internet Access focuses on simplicity and time to deployment. With this method, you can ensure a consistent and reliable connection to critical resources, all while ensuring the highest level of security across both solutions.



Prerequisites

The following prerequisites are required from Versa Networks setup and Microsoft Entra Internet Access.

Versa Networks set up:

- Versa Director and Versa Operating System™ (VOS™) Release 22.1.4 and later.
- Must have a public IP address on the physical interface where IPsec tunnels are terminating.

Microsoft Entra

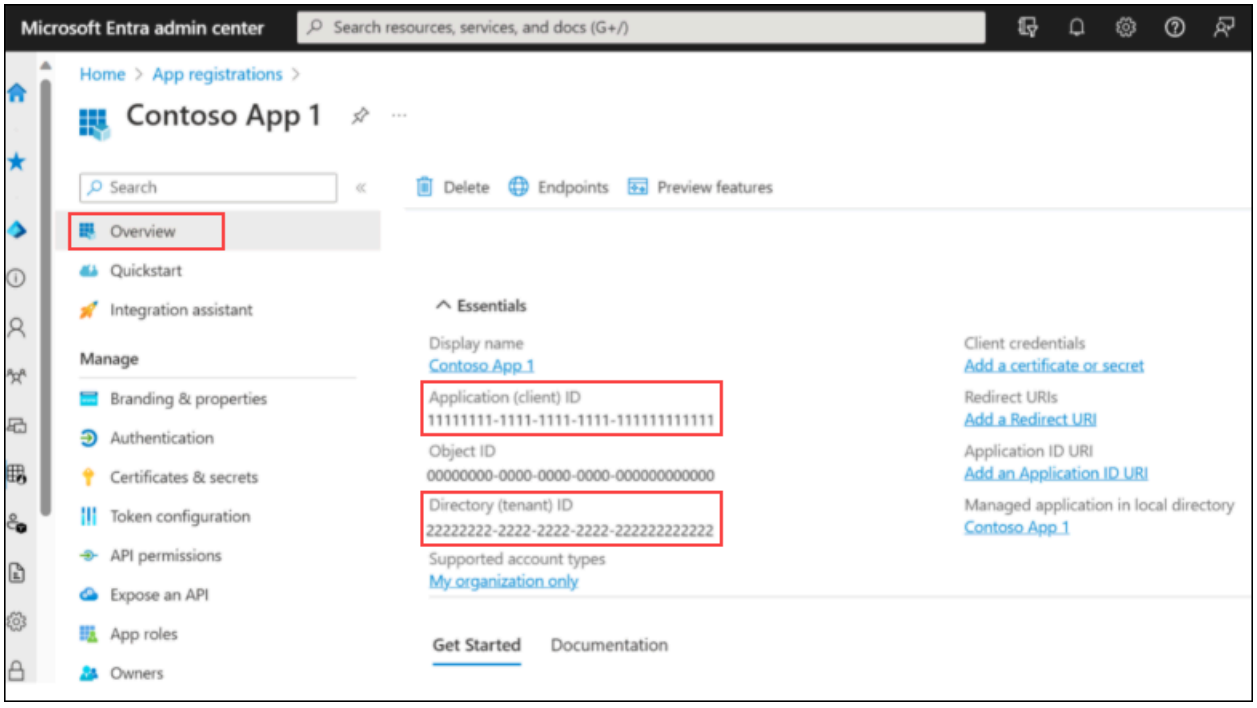
- Enable permissions on Microsoft Entra Admin Center.
- Create an application and service principal. See *Microsoft Entra Identity Platform* documentation.
- Add application permissions. See *Microsoft Entra Identity Platform* documentation.
- After creating permissions, obtain the following information from Microsoft Entra application:
  - Client ID
  - Tenant ID
  - Client Secret

Gather Information from the Microsoft Entra Application

In this procedure, you gather the Microsoft Entra client ID, tenant ID, and client secret, which you need to create the CMS cloud connector in Versa Director.

To gather the information from Microsoft Entra application:

1. Log in to Microsoft Entra Admin Center.
2. Navigate to Entra ID > App registrations, then select your application.
3. Select the Overview page and note the Directory (tenant) ID and Application (client) ID values.

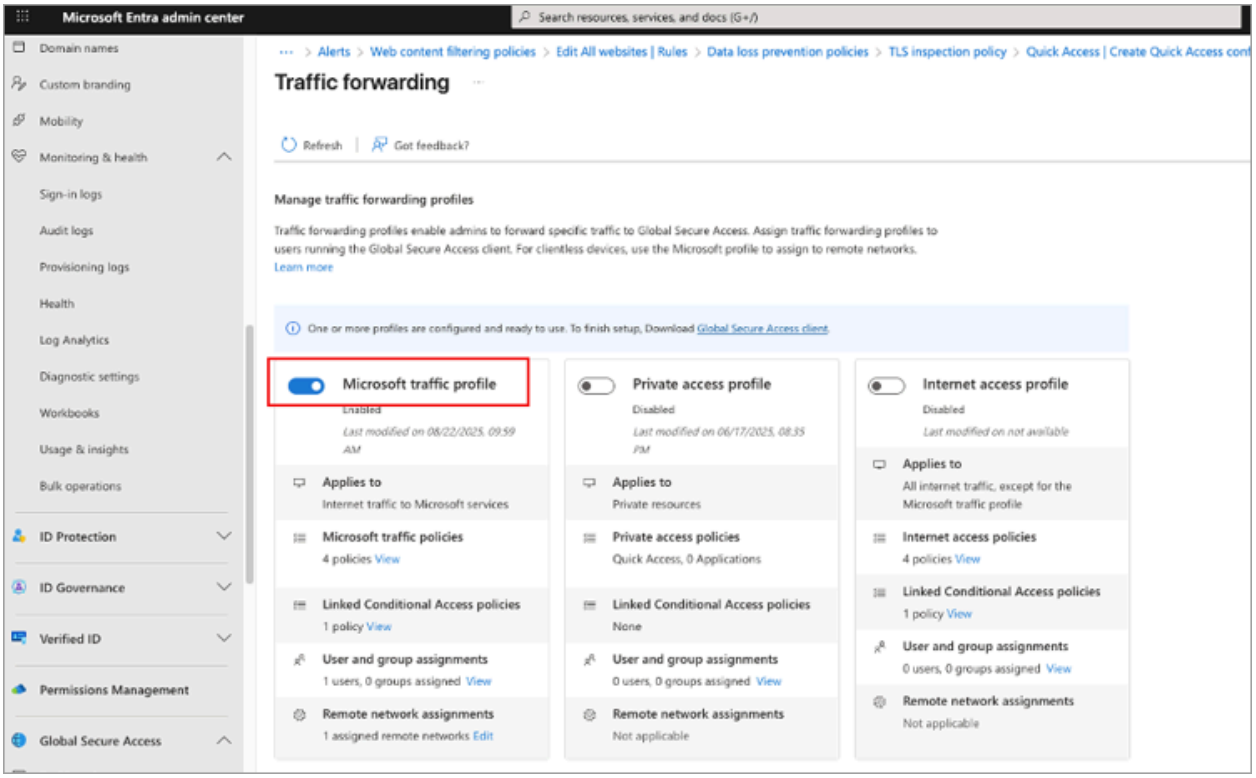


4. To create a client secret, see *Microsoft Entra Identity Platform* documentation. After you save the client secret, the value of the client secret is displayed. This is only displayed once, so copy this value and store it where you can retrieve it. You provide the secret value along with the application's client ID to sign in as the application.

Enable Microsoft Traffic Profile

To enable a traffic profile in Microsoft Entra admin center:

1. Log in to Microsoft Entra Admin Center.
2. Navigate to Global Secure Access > Connect > Traffic Forwarding.
3. Enable Microsoft traffic profile.



Supported Encryption Algorithms

Versa Networks supports the following IKE encryption algorithms in phase 1 and phase 2. The default values for phase 1 is MIX 8 and phase 2 is MIX 6.

Table 1: IKE Phase 1 Encryption Algorithms

IKEV2	MIX 1	MIX 2	MIX 3	MIX 4	MIX 5	MIX 6	MIX 7	MIX 8
Encryption	AES128	AES128	AES128	AES128	AES256	AES256	AES256	AES256
Integrity	SHA256	SHA256	SHA384	SHA384	SHA256	SHA256	SHA384	SHA384
DH Group	ECP256	ECP384	ECP256	ECP384	ECP256	ECP384	ECP256	ECP384

Table 2: IKE Phase 2 Encryption Algorithms

IPsec	MIX 1	MIX 2	MIX 3	MIX 4	MIX 5	MIX 6
Encryption	GCMAES128	GCMAES128	GCMAES128	GCMAES256	GCMAES256	GCMAES256
Integrity	GCMAES128	GCMAES128	GCMAES128	GCMAES256	GCMAES256	GCMAES256
PFS Group	PFS14	ECP256	ECP384	PFS14	ECP256	ECP384

Create a CMS Cloud Connector in Versa Director

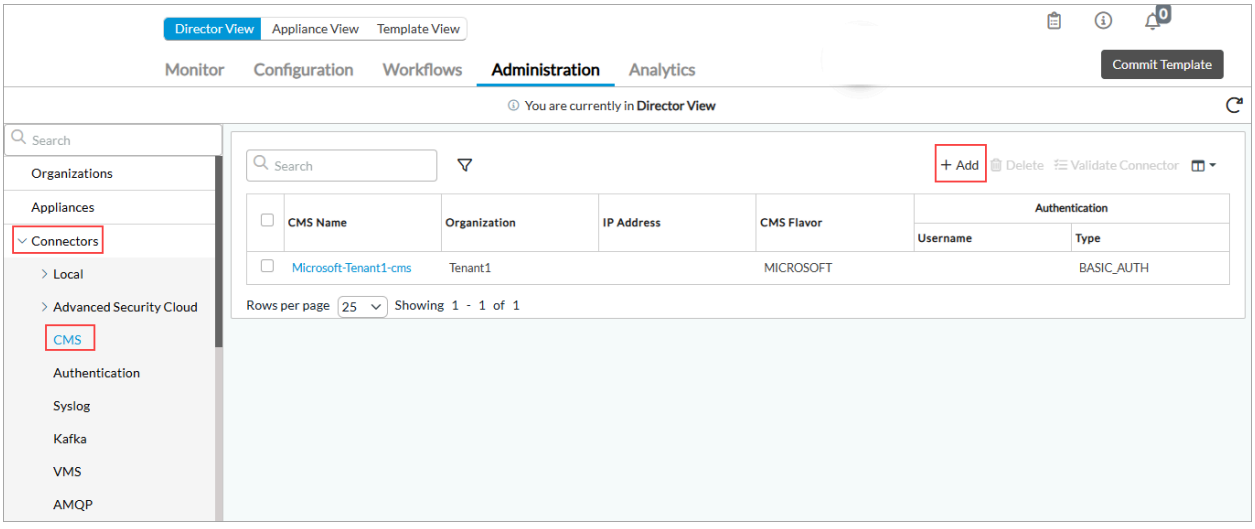
To establish a connection between a Versa Operating System™ (VOS™) device and Microsoft Entra, and manage that connection through Versa Director, you must first configure a CMS connector on Versa Director. Note that you can create only one CMS connector per tenant for Microsoft Entra API-based integration.

When you create the CMS cloud connector on Versa Director, you need the following information:

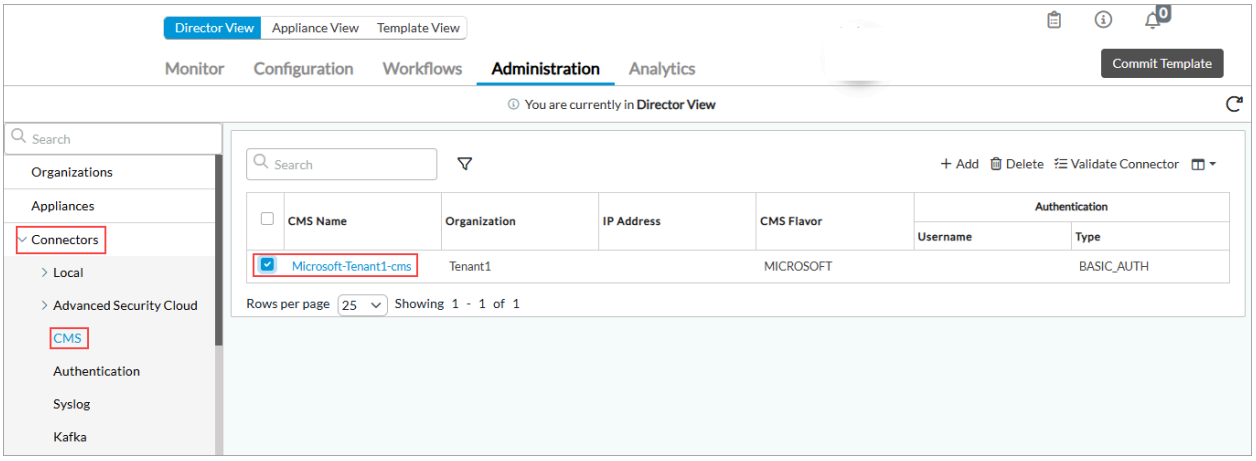
- Microsoft Entra application client ID, client secret, and tenant ID that you gathered in the Gather Information from Microsoft Entra Application, above.

To create a CMS cloud connector in Versa Director:

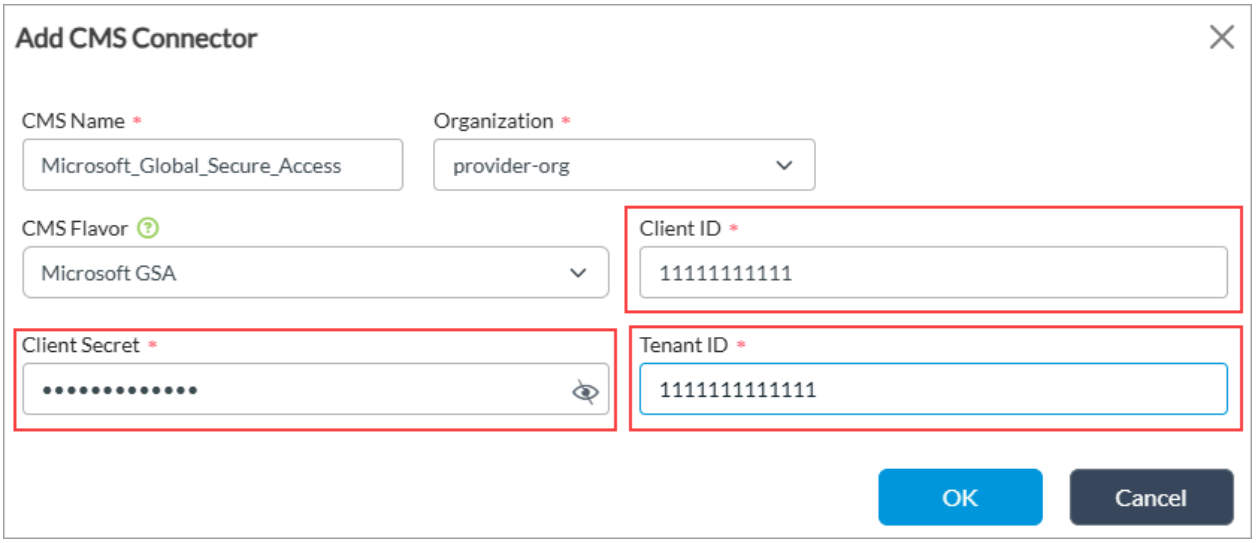
1. Log in to Versa Director.
2. In Director view, select the Administration tab in the top menu bar.
3. Select Connectors > CMS in the left menu bar:
   a. If you have already created a CMS connector, go to step 4.
   b. To create a CMS connector, go to step 5. Note that if you have already added a CMS connector, the + Add icon is not displayed. You can create only one CMS connector per tenant.



4. Click the CMS name to edit the CMS connector.



5. Click the + Add icon. In the Add CMS Connector window, enter information for the following fields.



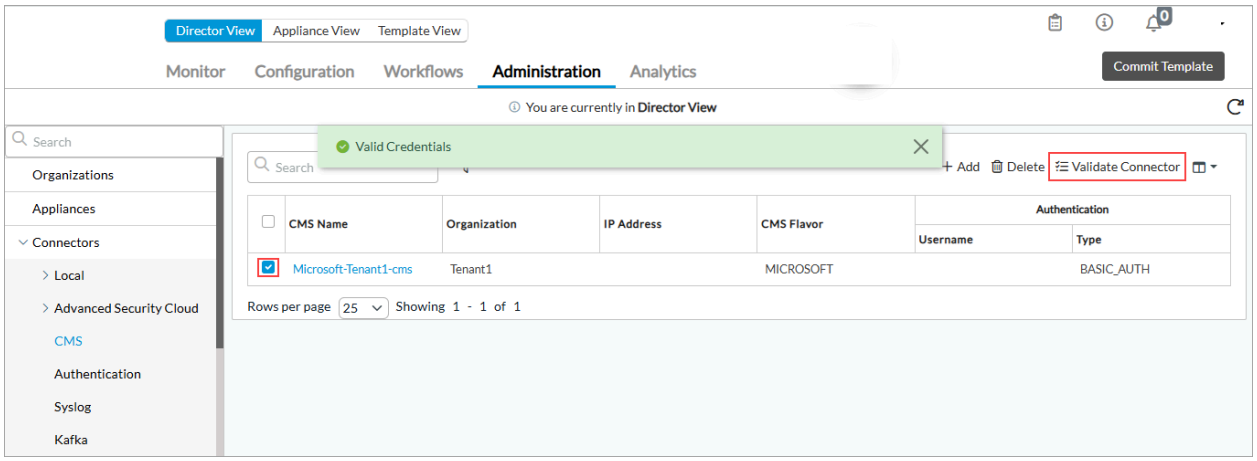
Field	Description
CMS Name (Required)	Enter the name of the CMS connector. The name is a text string.
Organization (Required)	Select the tenant organization, which should be present in the provider Versa Director.
CMS Flavor	Select Microsoft GSA for the type of cloud service.
Client ID (Required)	Enter the client ID obtained from the Microsoft Entra admin center.
Client Secret (Required)	Enter the client secret ID obtained from the Microsoft Entra admin center.
Tenant ID (Required)	Enter the tenant ID value obtained from the Microsoft Entra admin center.

6. Click OK.

Verify a CMS Cloud Connector

To verify that a CMS connector is working:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > CMS in the left menu bar. The main pane displays a table of CMS connectors.
3. Select the CMS connector to verify, and then click Validate Connector in the horizontal menu bar. This triggers an API call to the CMS connector to verify its Microsoft Intra user rights. If the validation is successful, the Valid Credentials popup message displays.



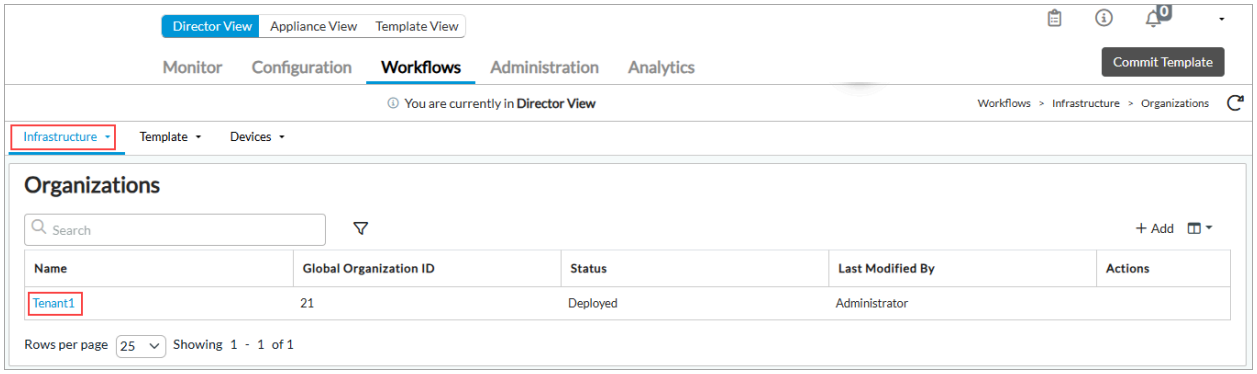
Updated: Fri, 12 Sep 2025 10:33:02 GMT

Associate a CMS Cloud Connector with an Organization

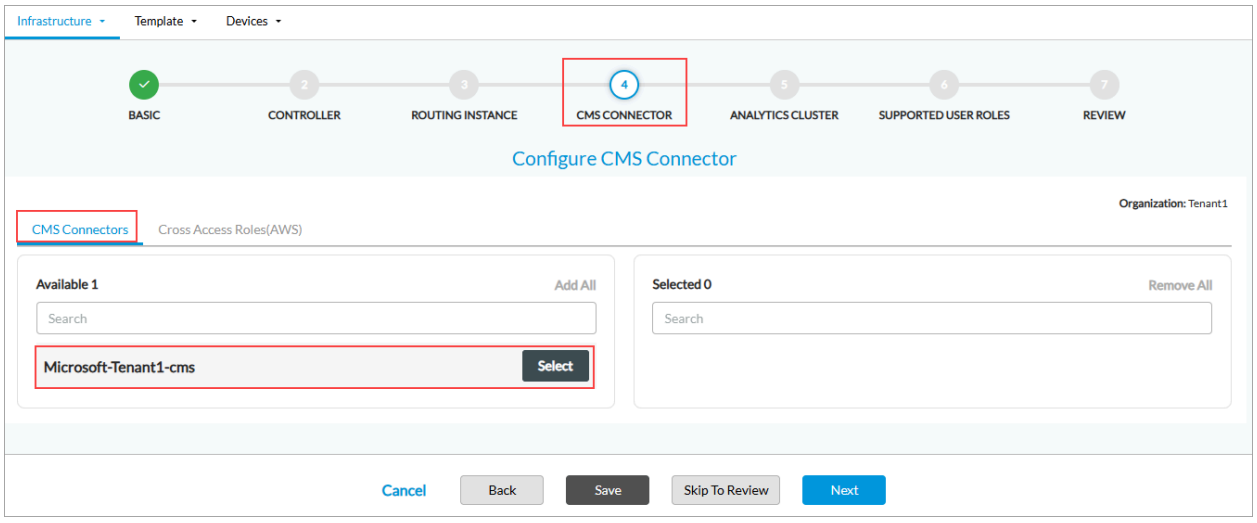
After you add a CMS cloud connector, you associate it with an organization that is already configured on the Director node.

To verify the workflow with an organization.

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Infrastructure > Organizations in the horizontal menu bar. The main pane displays a table of organizations.
3. Select the organization with which you want to associate the CMS connector. In this example, the organization is Tenant1.



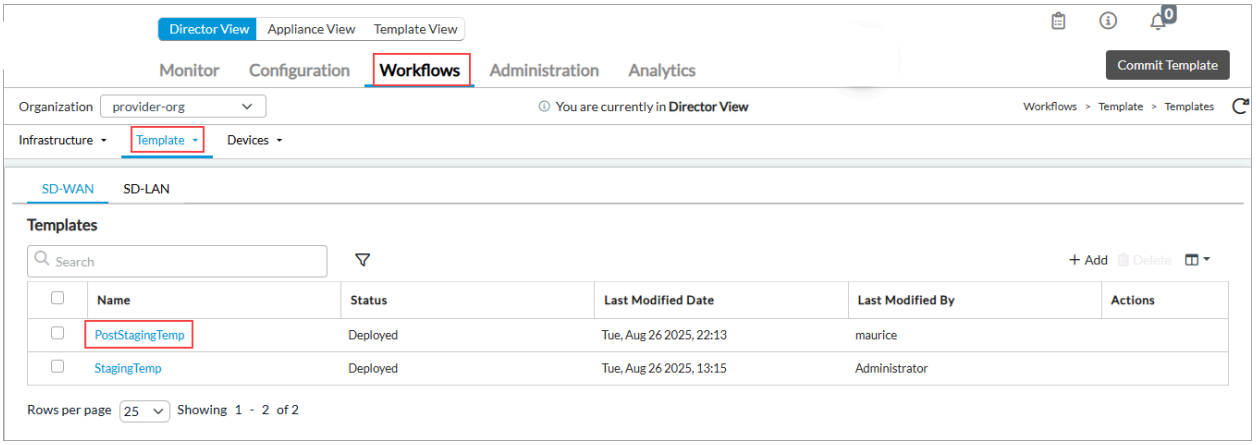
4. Select Step 4, CMS Connector. In the Available pane, click the Microsoft-Tenant1-cms connector to add it to the Selected pane.



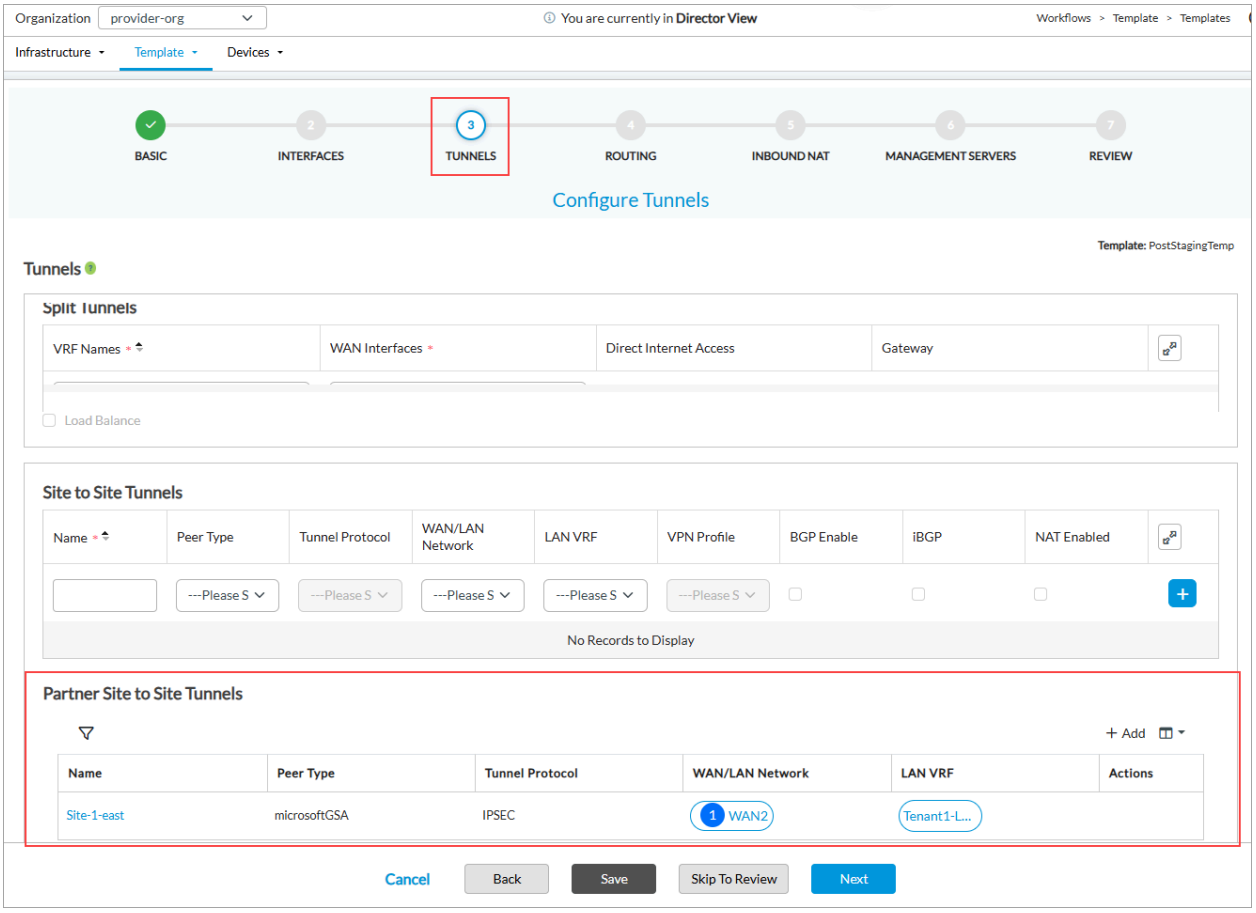
5. Select Step 7, Review, and then click Deploy.

Configure a Site-to-Site Tunnel in a Workflow Template for Microsoft Entra

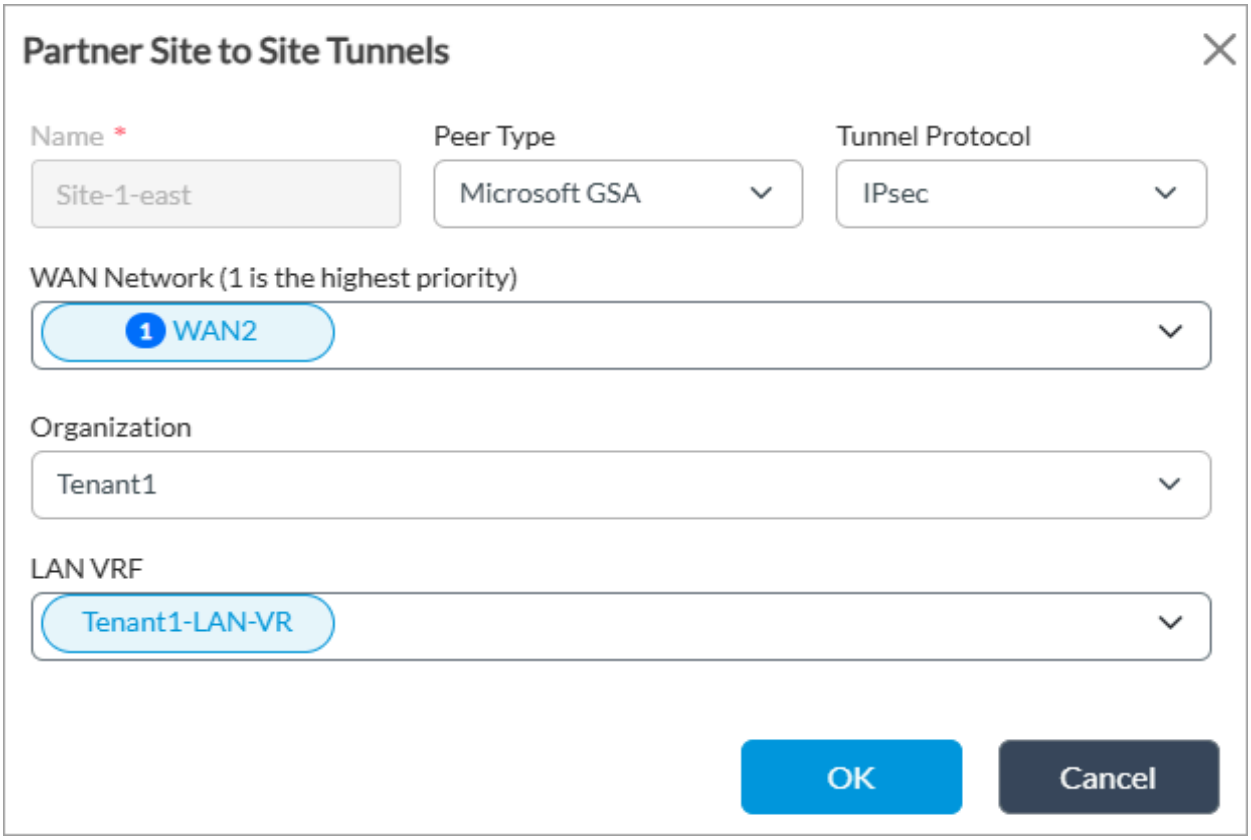
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. Select an SD-WAN post-staging template in the main pane. To create a new workflow template, see Create and Manage Staging and Post-Staging Templates.



4. Click Step 3, Tunnels. In the Partner Site-to-Site Tunnels section, click the + Add icon.



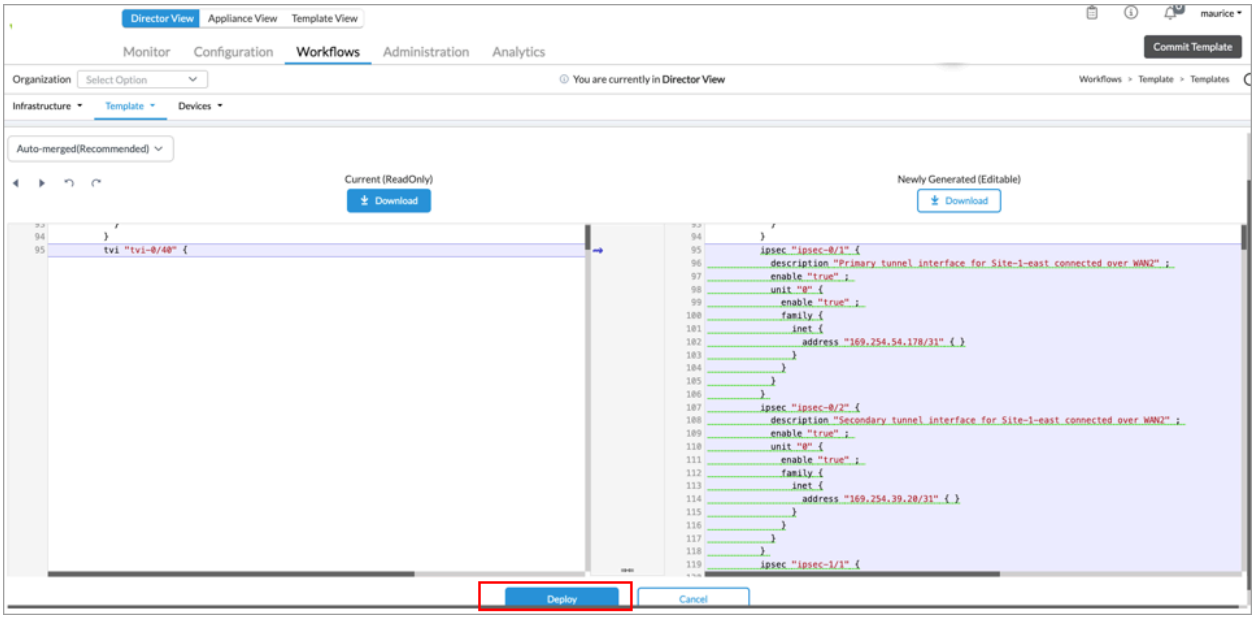
5. In the Partner Site to Site Tunnels page, enter the following information.



Field	Description
Name (Required)	Enter a name for the site-to-site tunnel.
Peer Type	Select the Microsoft GSA peer type.
Tunnel Protocol	Select the IPsec tunnel protocol to use to reach the peer.
WAN Network	Select one or more WAN networks to use. This network is the originating endpoint of the tunnel. The highest priority is 1.
Organization	Select the organization for which the site-to-site tunnel is created.
LAN VRF	Select one or more virtual routing instances to use to reach the LAN.

6. Click OK, and then click Save.
7. If modifying an existing device:
   a. Click Step 7, Review, and then click Re-Deploy.
   b. Commit the template.

Versa Director shows a diff with newly added changes for the tunnel to validate changes.



8. Click Deploy.
   For more information on template workflows, see Overview of Configuration Templates.

Configure a Site-to-Site Tunnel in a Device Workflow for Microsoft Entra

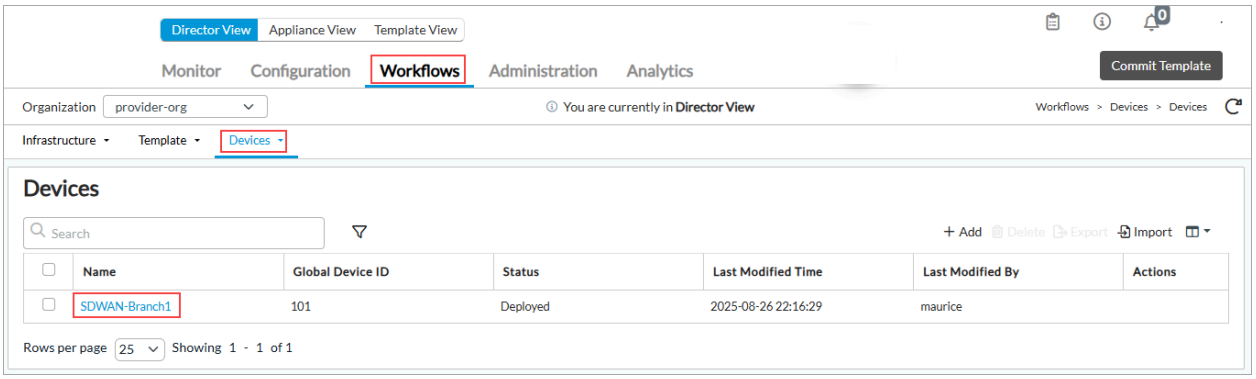
Versa Network's device workflow automates configuration or provisioning, attaching the device groups and bind data for each VOS instance. To configure the device workflow, you must attach the template workflow to the device group within the device workflow.

In the following example configuration, there are two Microsoft Entra BGP peers and one Versa BGP peer. Versa uses a local tunnel interface that can be viewed as a loopback. The Versa BGP local IP peer exchange information with the primary BGP peer (BGP peer IP) and the secondary BGP peer (BGP zone peer IP) through the IPsec tunnels. In this example, APIPA (RFC 3927) address space is used. You can also verify Microsoft Entra supported address space and ASNs here.

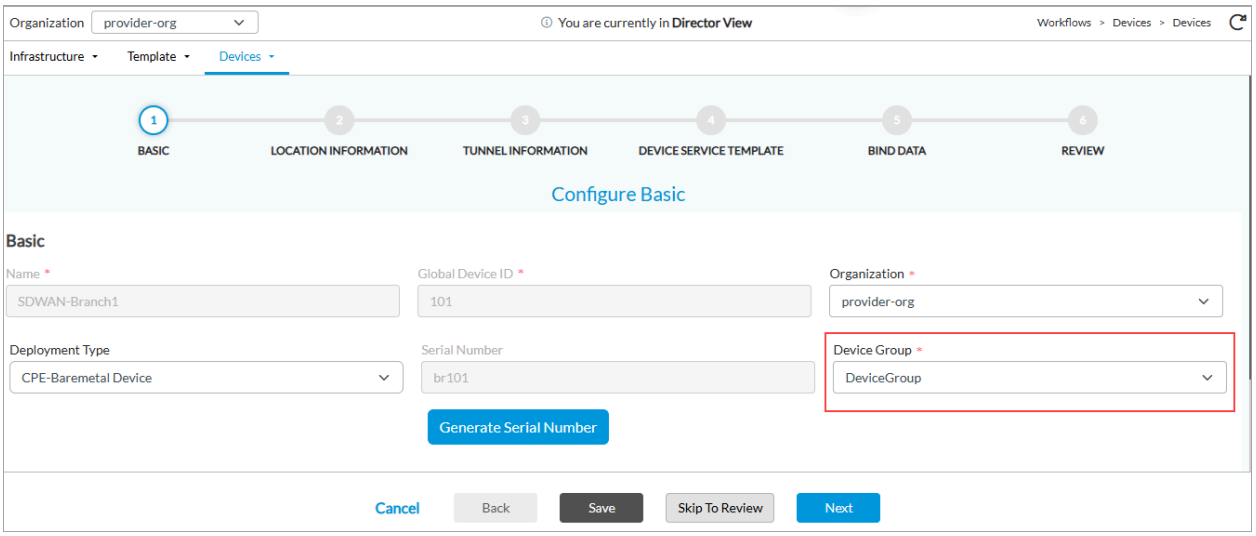
For more information on device workflows, see Overview of Configuration Templates.

To configure a Versa Director–Microsoft Entra IPsec site-to-site tunnel for a device:

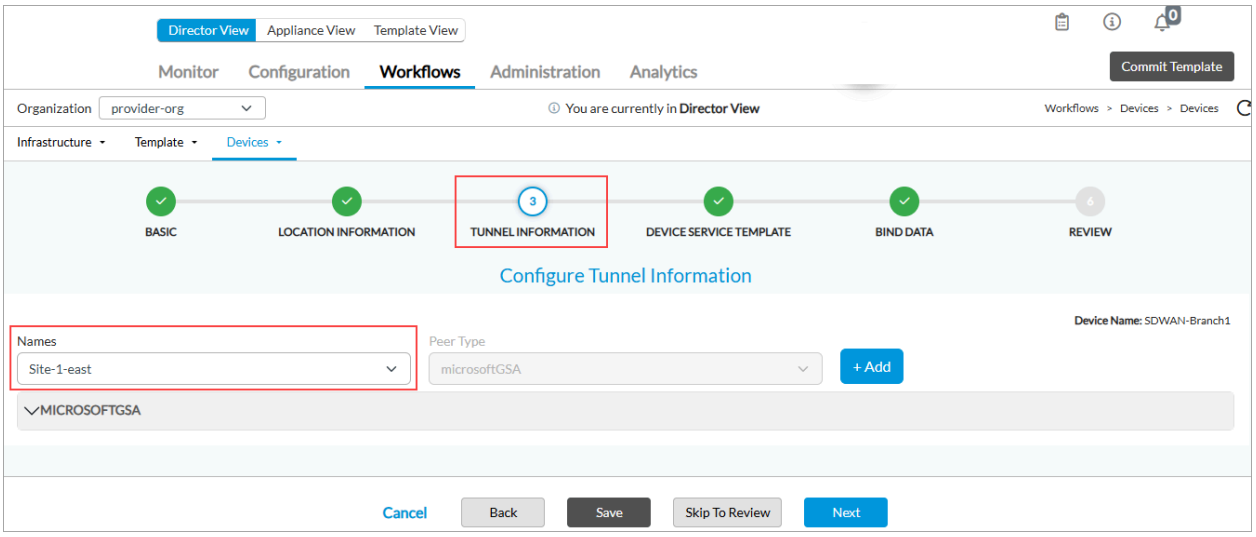
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the left menu bar.
3. Select a device in the main pane.



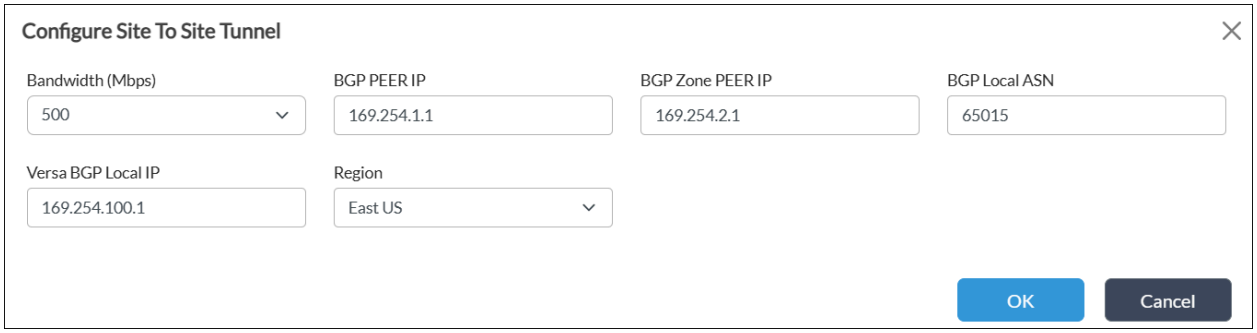
4. In Step 1, Basic, select a device group that has a template associated with it.



5. Click Step 3, Tunnel Information. Select the partner site-to-site tunnel created in the workflow template, and then click the + Add Add icon.

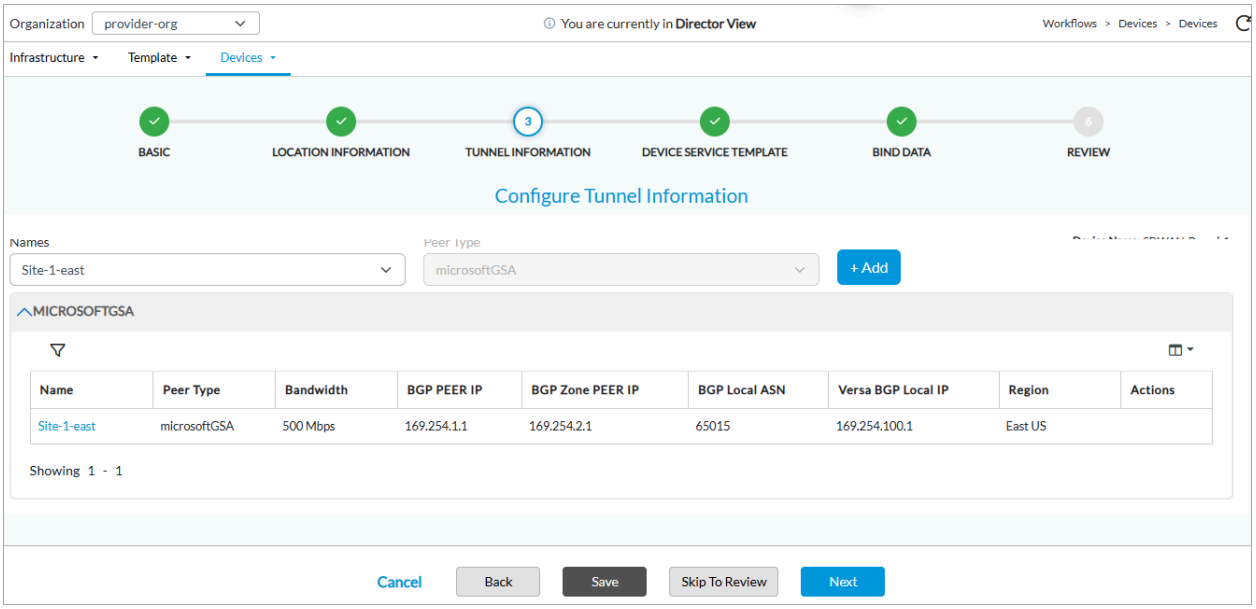


6. In the Configure Site-To-Site Tunnel popup window, enter information for the following fields.



Field	Description
Bandwidth (Mbps)	Select the tunnel bandwidth, in Mbps, for Microsoft Entra.
BGP Peer IP	Enter the IP address of primary BGP speaker on Microsoft Entra.
BGP Zone Peer IP	Enter the IP address of secondary BGP speaker on Microsoft Entra.
BGP Local ASN	Enter the Versa BGP local autonomous system number (ASN).
Versa BGP Local IP	Enter the VOS local ASN.
Region	Select the Microsoft Entra region.

7. Click OK. The tunnel information page displays the tunnel information for the device workflow.



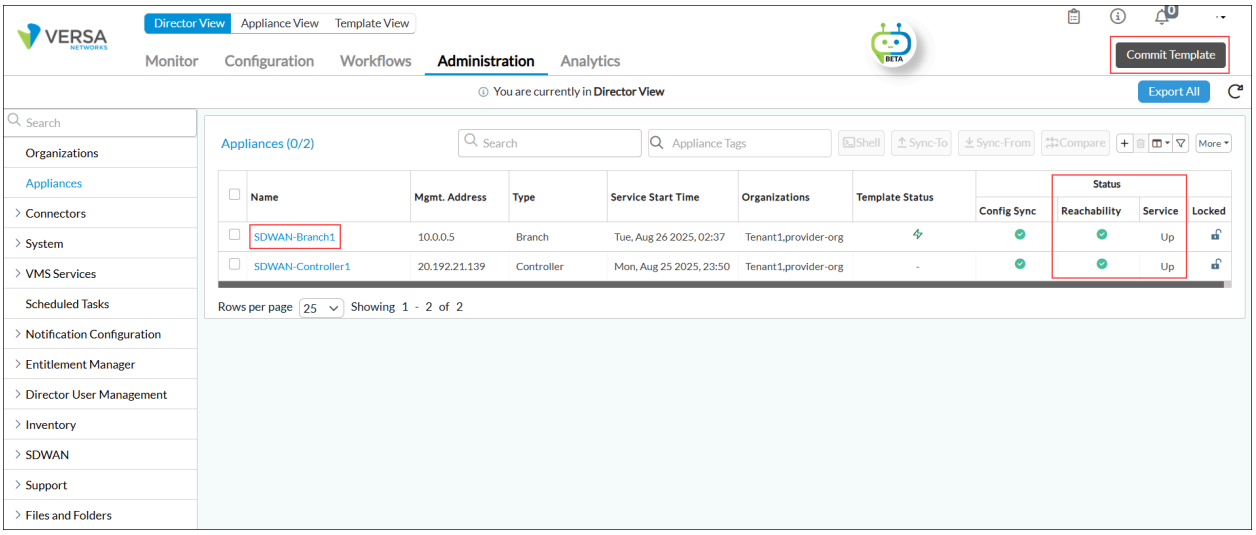
8. Click Save.
9. If modifying an existing device:
    a. Click Step 6, Review, and then click Re-Deploy.
    b. Commit the template.

Commit Template Modifications

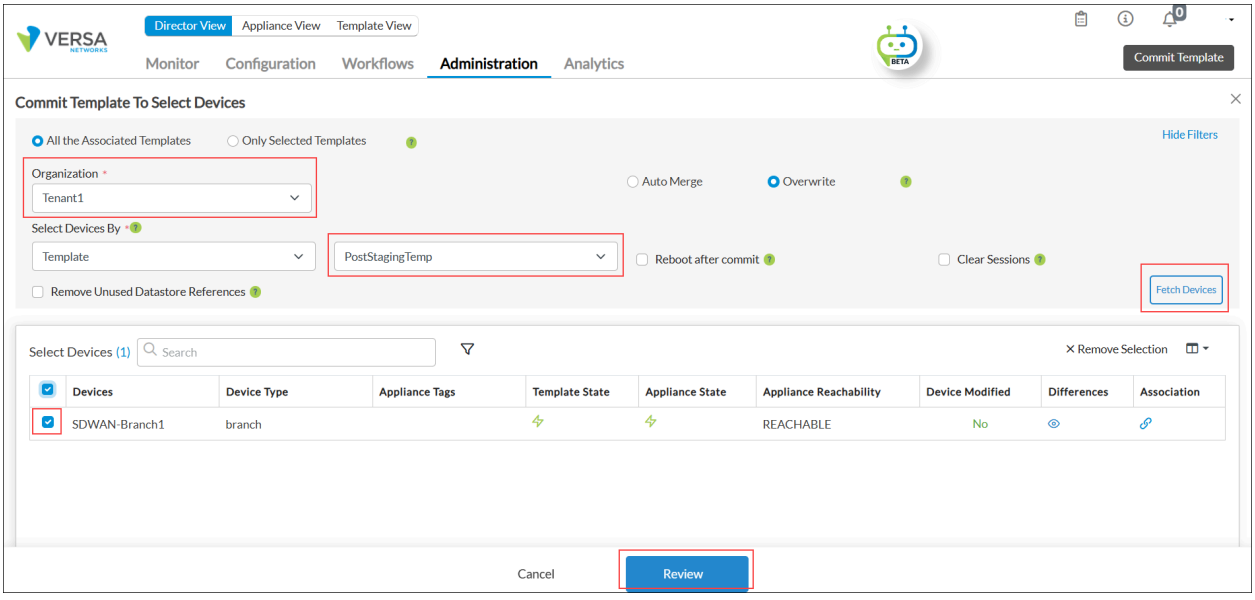
When you change the configuration in an existing configuration or service template, you must commit the changes so that the new configuration is deployed on the associated devices. You can commit all changes, and you can merge the changes into the existing configuration.

To commit a modified template:

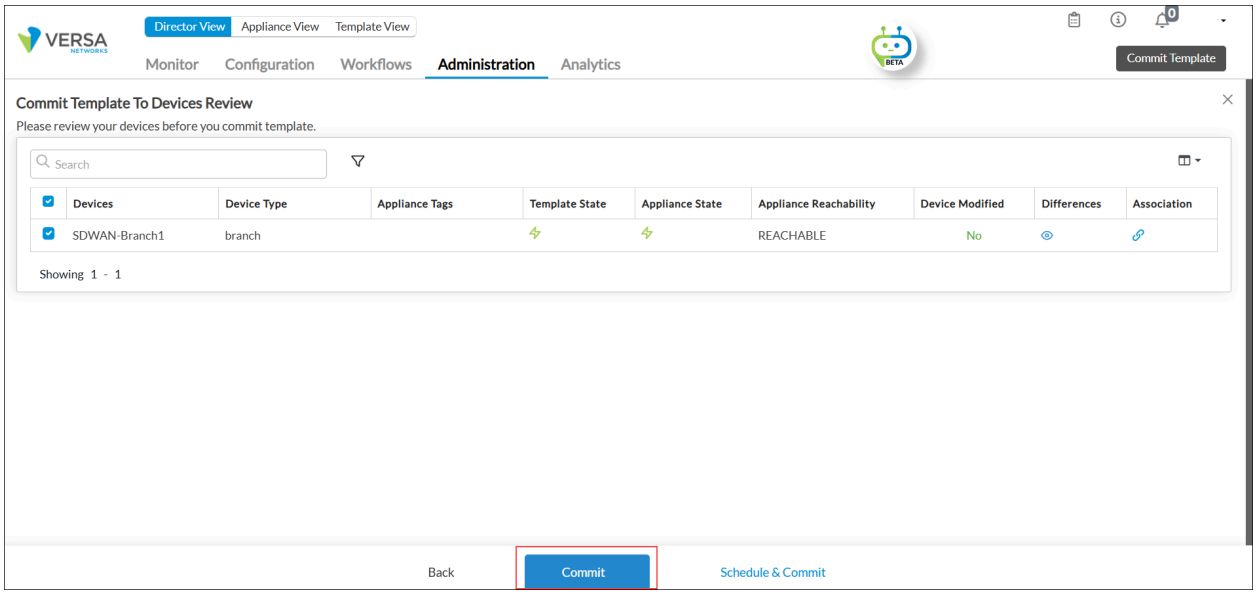
1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. In the Status column in the main pane, check whether Reachability is green and Service is Up, and then click Commit Template.



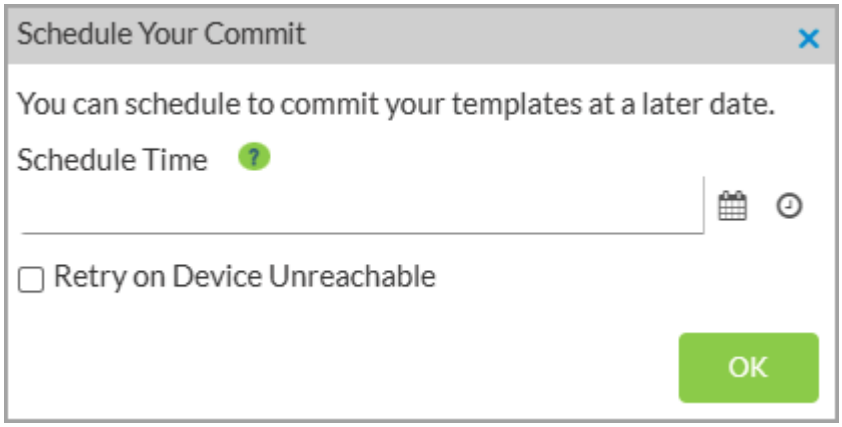
4. In the Commit Template To Select Devices window, select which templates to commit to which devices. You can select either All the Associated Templates or Only Selected Templates. The All the Associated Templates option is selected by default.
   a. Select the organization.
   b. Select a post-staging template
   c. Click Fetch Devices.
   d. Select the device and click Review.



5. The Commit Template to Devices Review window displays.



6. Click Commit to commit the template changes.
7. To schedule the commit for a later date or time, click Schedule & Commit. In the Schedule Your Commit popup window, set the schedule.



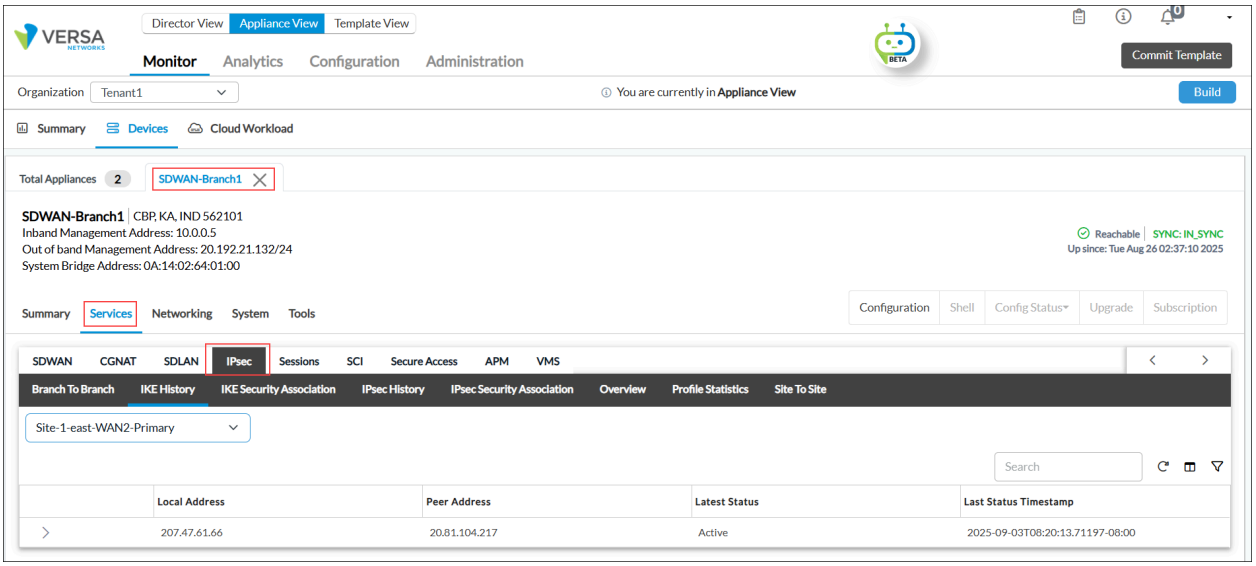
8. Click OK.

To view the details and progress of the commit template, click the Task icon. Expand an activity to view more information, which you can use to analyze and troubleshoot any issues.

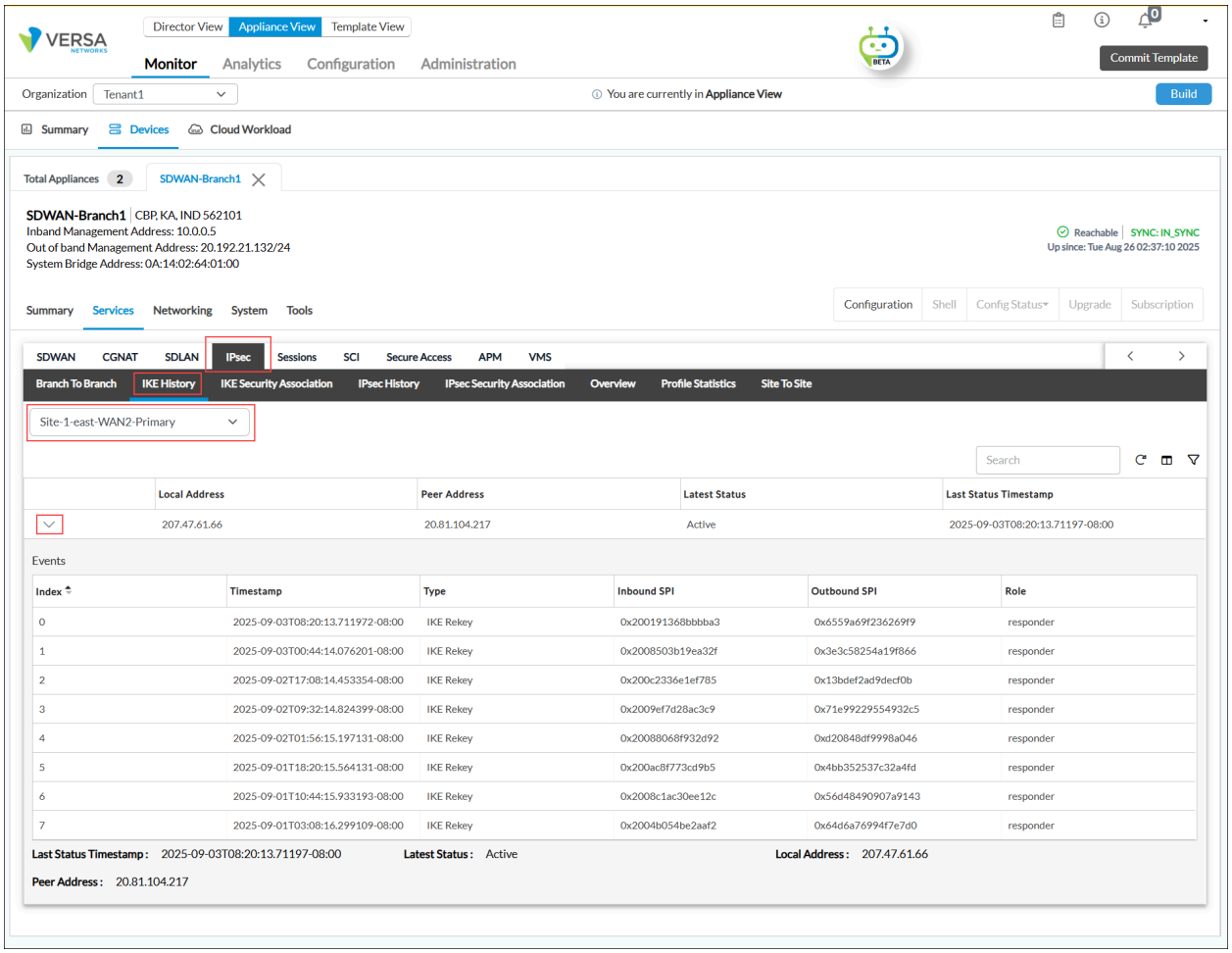
Verify IPsec Tunnel Services

To verify IPsec tunnel services for a site-to-site tunnel:

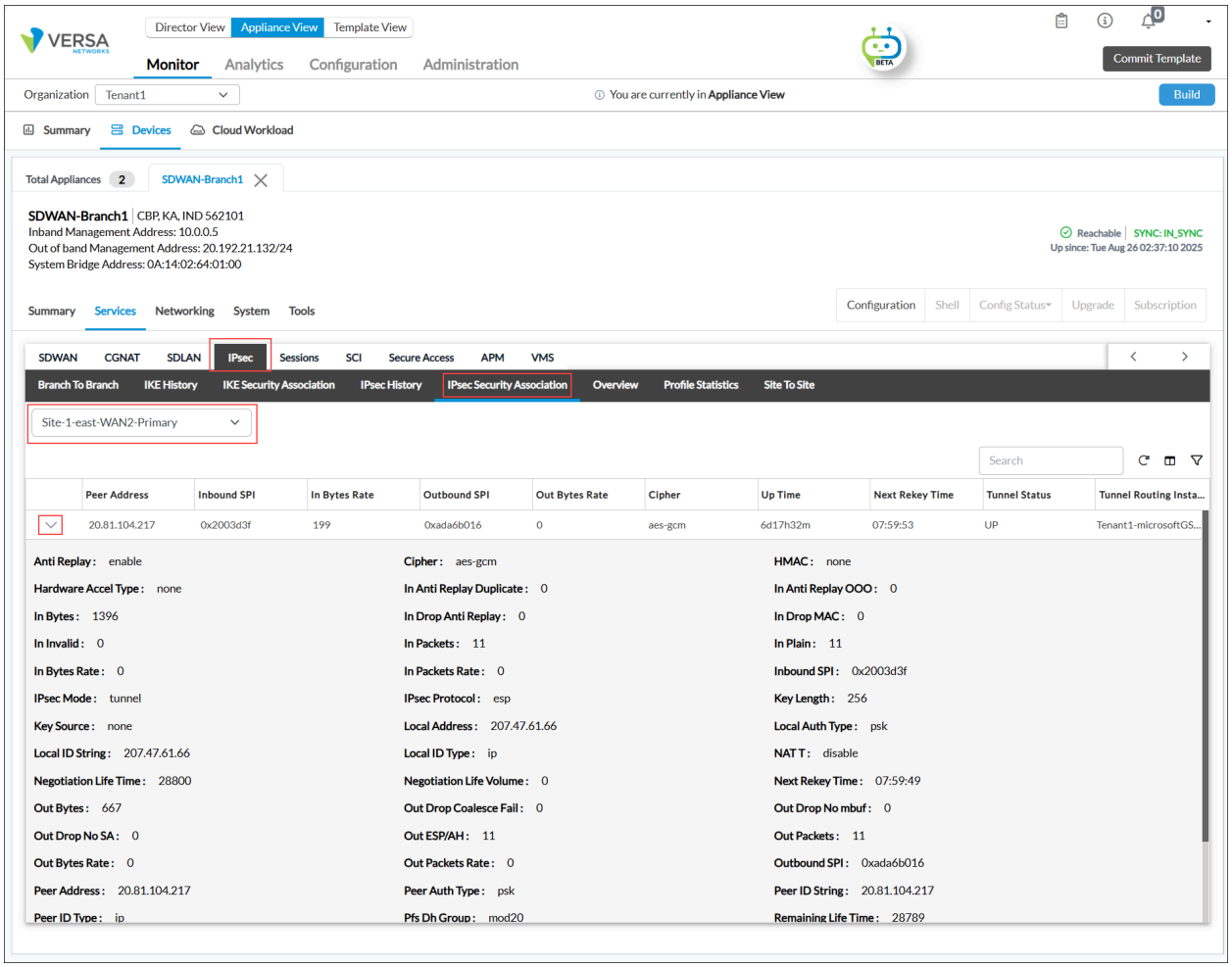
1. In Director view:
   a. Select the Monitor tab in the top menu bar.
   b. Select Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select Services > IPsec in the horizontal device menu bar.



3. On the IPsec tab, select IKE History, and then select the IPsec tunnel. Click an entity to view the IKE history.

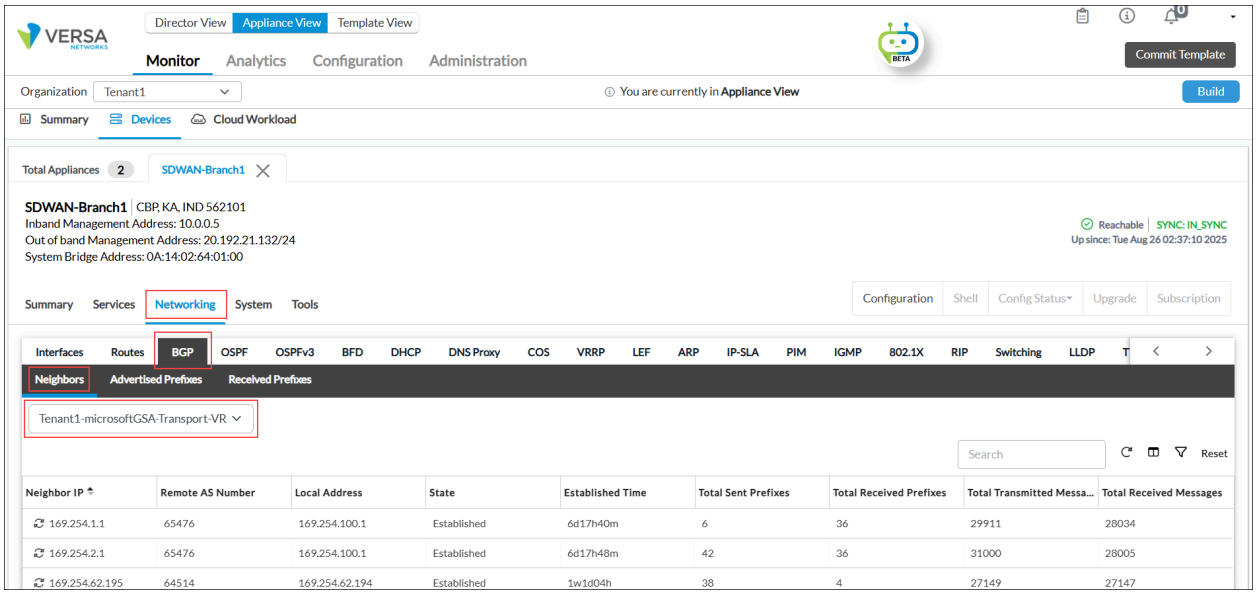


4. Select IPsec Security Association, and then select the IPsec tunnel. Click an entity to view the IPsec security details.

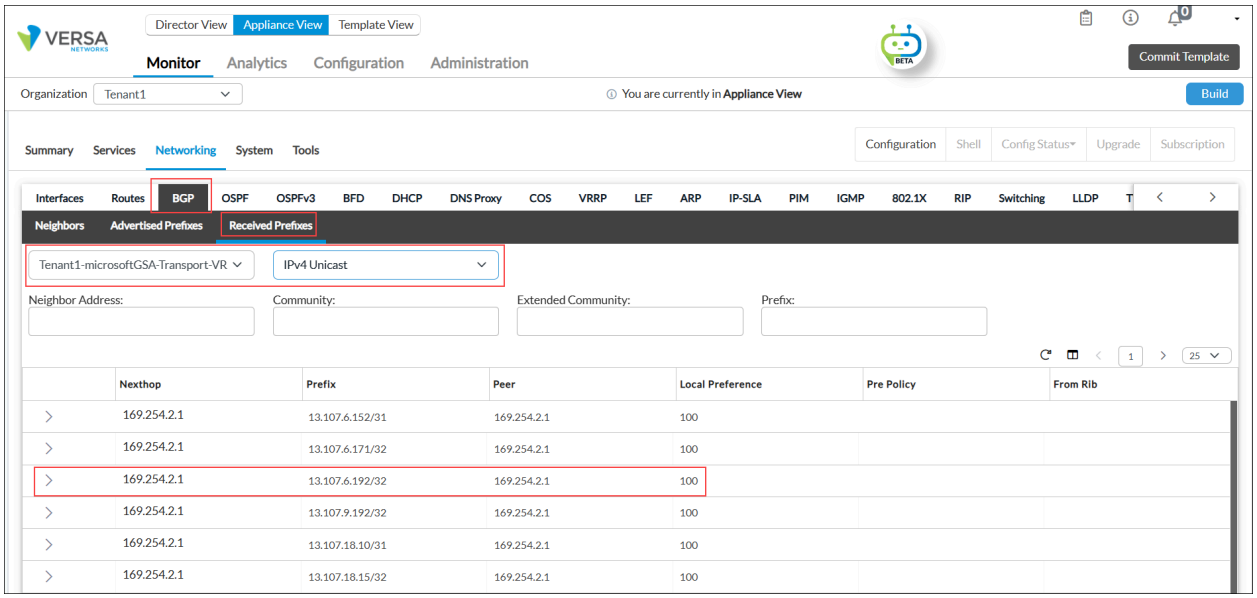


Verify Microsoft Entra BGP Peers in Versa Director

1. In Director view:
   a. Select the Monitor tab in the top menu bar.
   b. Select Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select Networking > BGP in the horizontal device menu bar.
3. On the BGP tab, select Neighbors, and then select Tenant1-microsoftGSA-Transport-VR to check neighbors for Microsoft Entra BGP Peers.

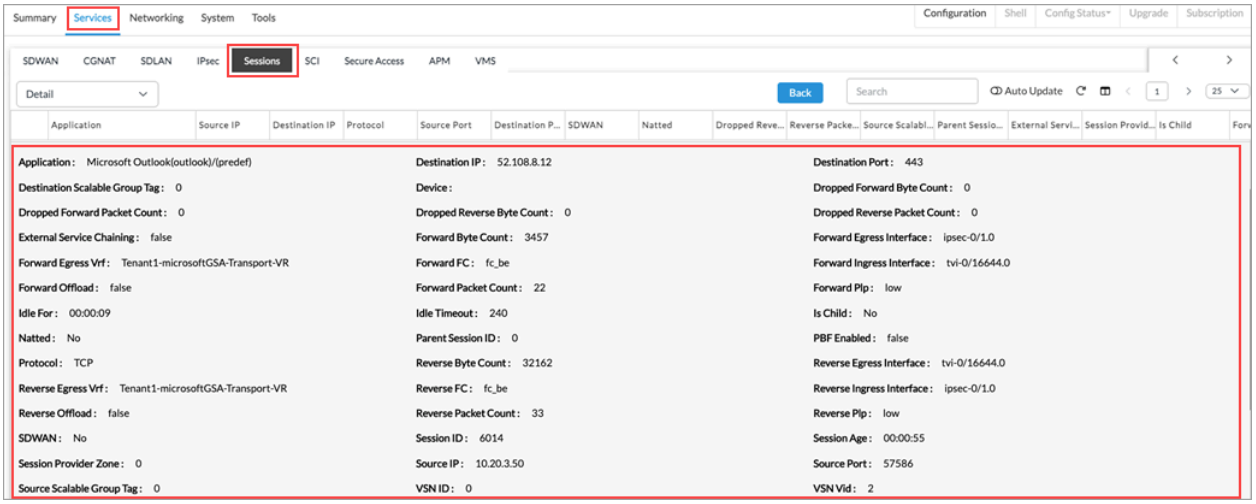


4. Select Received Prefixes to view the prefixes received from Microsoft Entra Intra Access.



Verify Traffic Through VOS to Microsoft Entra

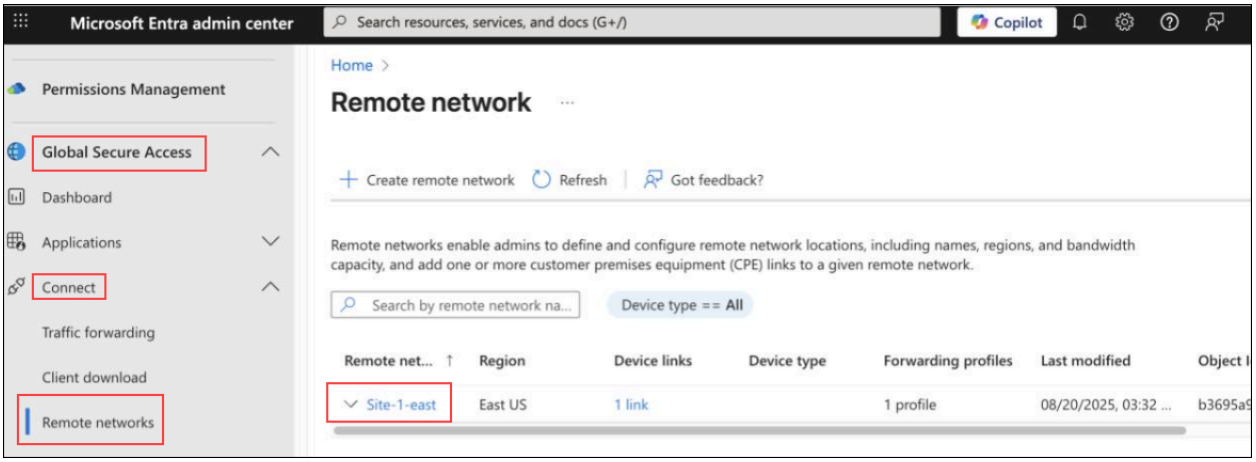
1. In Director view:
   a. Select the Monitor tab in the top menu bar.
   b. Select Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select Services > Session in the horizontal device menu bar to display the session information.



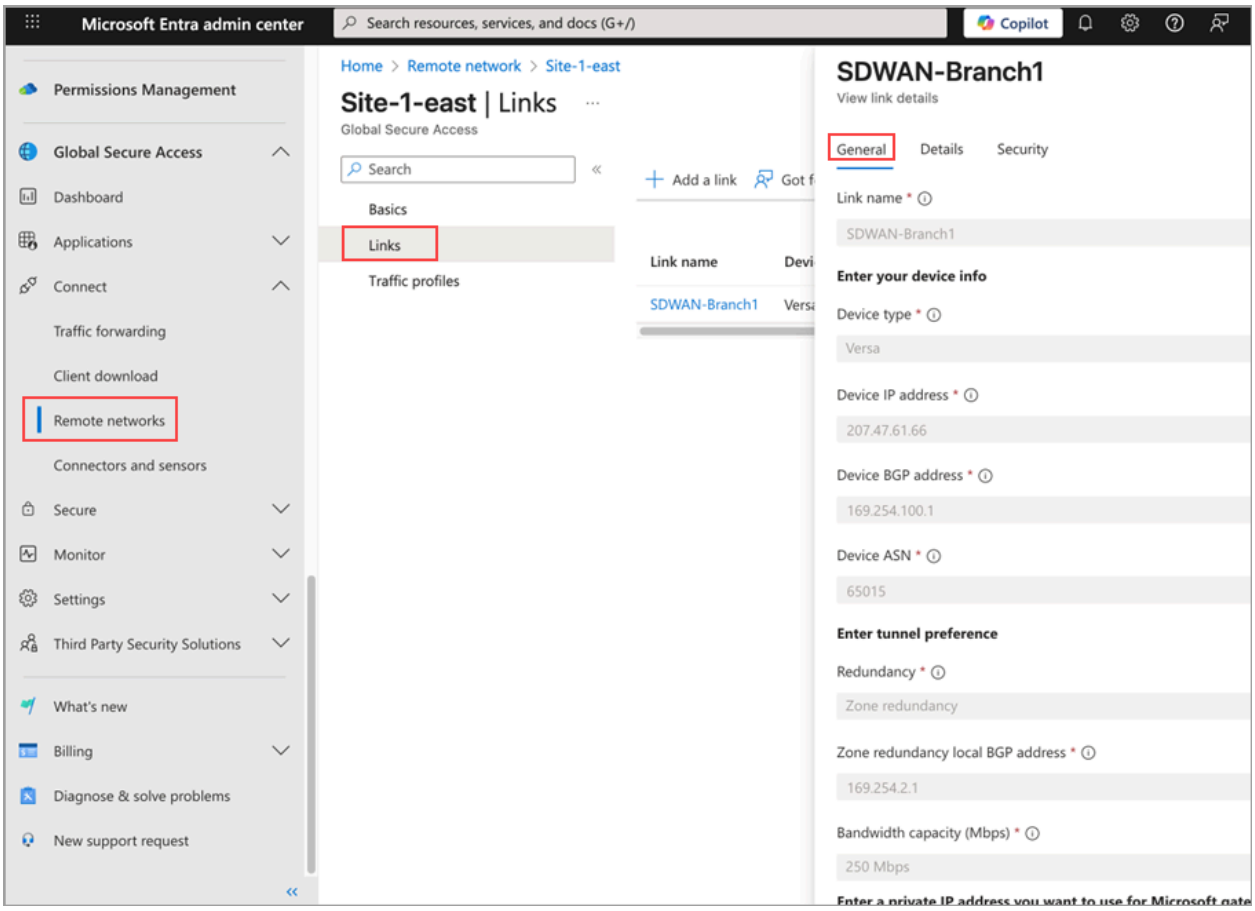
Verify Versa Director Device Information from Microsoft Entra

To verify the device information from Microsoft Entra:

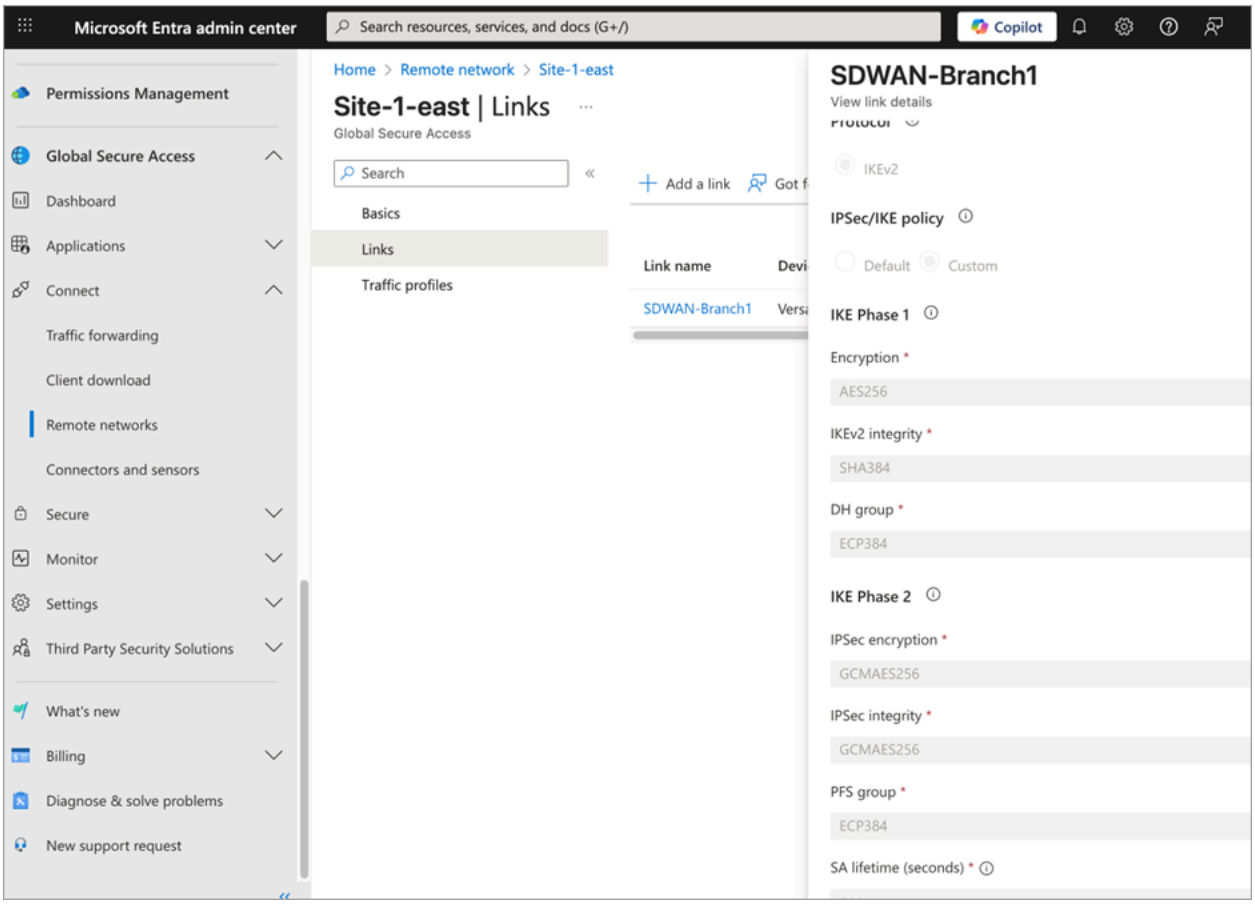
1. Log in to Microsoft Entra Admin Center.
2. Navigate to Global Secure Access > Connect > Remote Networks.
3. Click the remote network created by Versa Director.



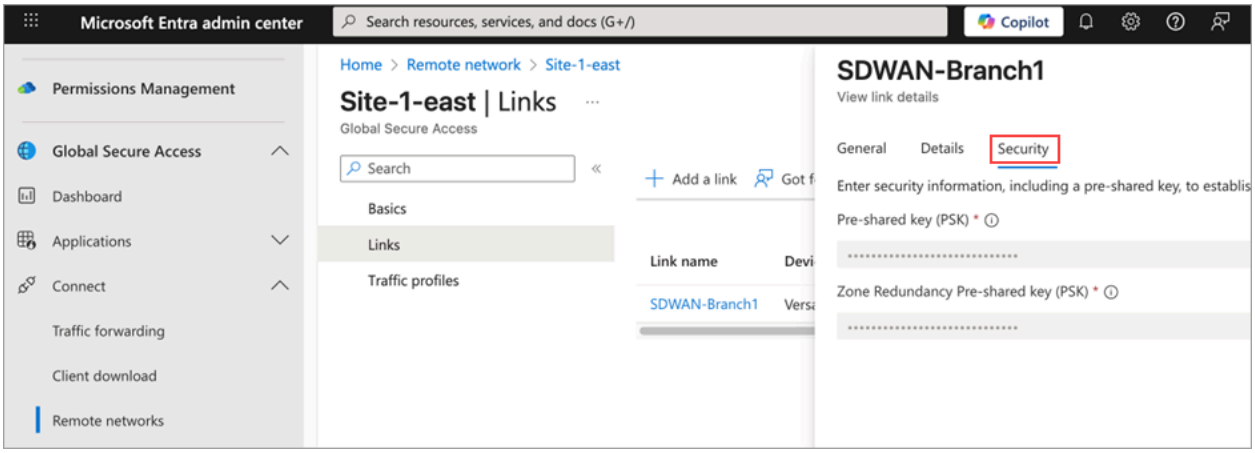
4. In the remote network details page, select Links. The view link details pane displays the device information.
    1. Select the General tab to view the device information.



2. Select the Details tab to view the IKE and IPsec information. For Versa supported IKE encryption algorithms, see Supported Encryption Algorithms.



3. Select the Security tab to view the randomly generated pre-shared keys.



View Versa Director Traffic Logs from Microsoft Entra

To view Versa Director traffic logs from Microsoft Entra:

1. Log in to Microsoft Entra Admin Center.
2. Navigate to Global Secure Access > Monitor > Traffic Logs.
3. Select the Connections tab.