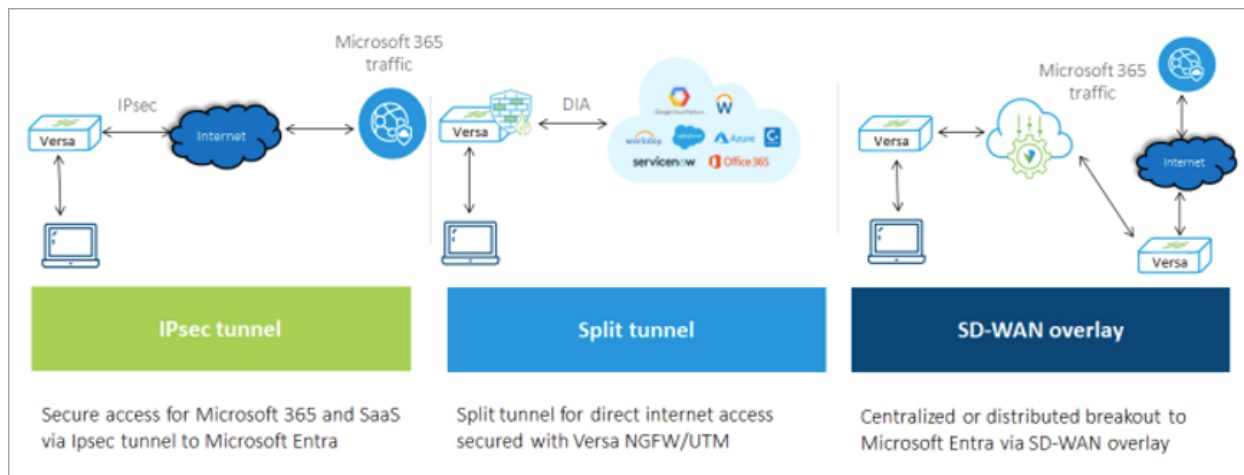


Versa Secure SD-WAN and Microsoft Entra Internet Access API Based Integration

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

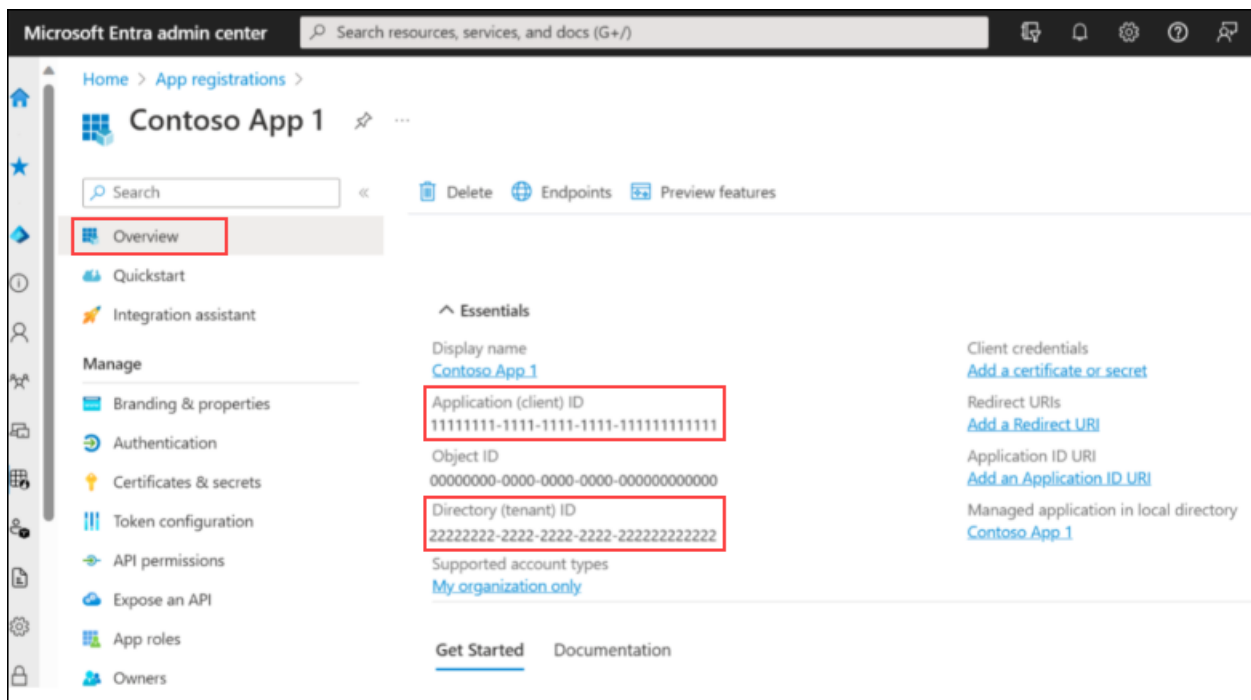
- Enable permissions on Microsoft Entra Admin Center.
- Create an application and service principal. See *Microsoft Entra Identity Platform* documentation.
- Add application permissions. See *Microsoft Entra Identity Platform* documentation.
- After creating permissions, obtain the following information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

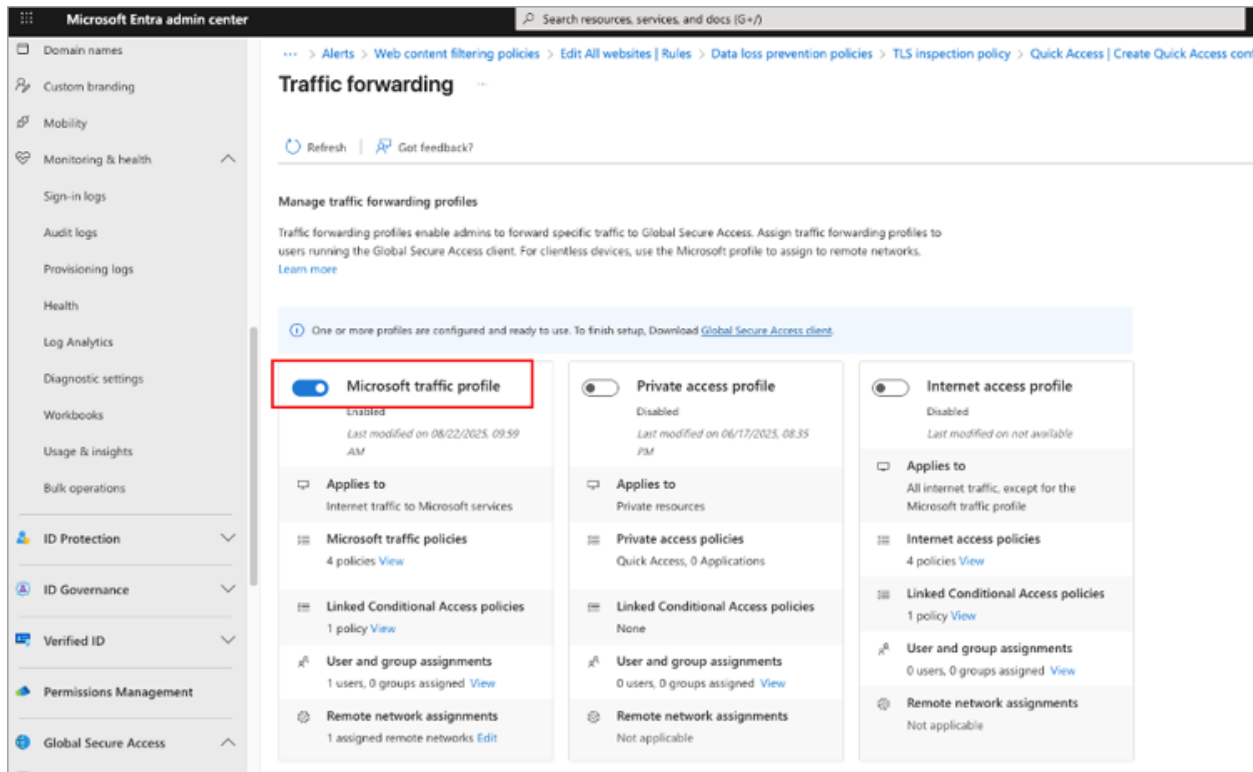


4. To create a client secret, see *Microsoft Entra Identity Platform* documentation. After you save the client secret, the value of the client secret is displayed. This is only displayed once, so copy this value and store it where you can retrieve it. You provide the secret value along with the application's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

https://docs.versa-networks.com/Versa_Internal/WIP/Suby/Draft%3A_Versa_Secure_SD-WAN_and_Microsoft_Entra_Internet...

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

Copyright © 2025, Versa Networks, Inc.

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

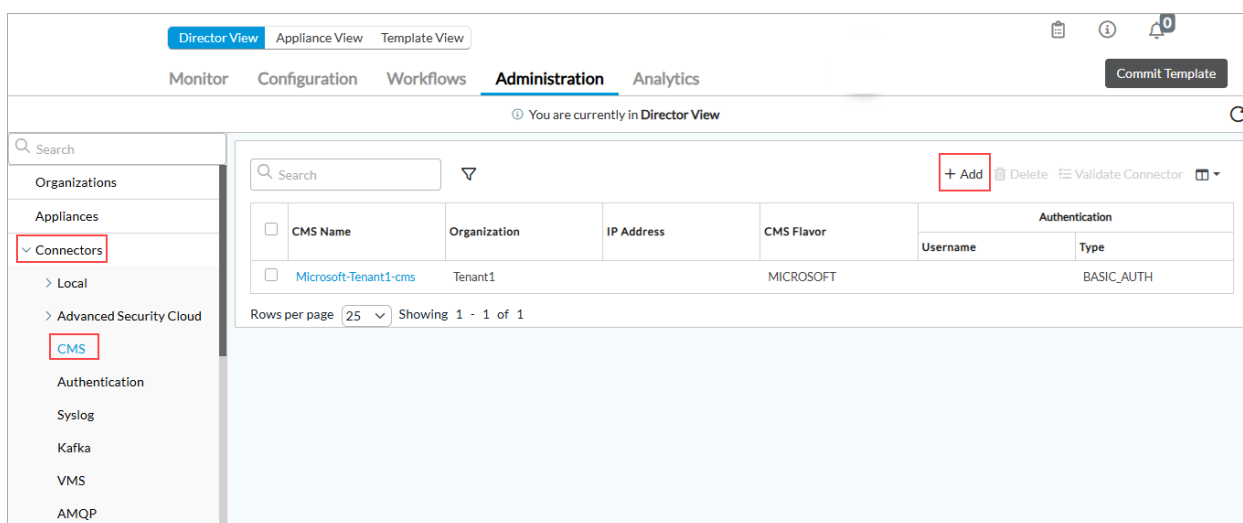
To establish a connection between a Versa Operating System™ (VOS™) device and Microsoft Entra, and manage that connection through Versa Director, you must first configure a CMS connector on Versa Director. Note that you can create only one CMS connector per tenant for Microsoft Entra API-based integration.

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

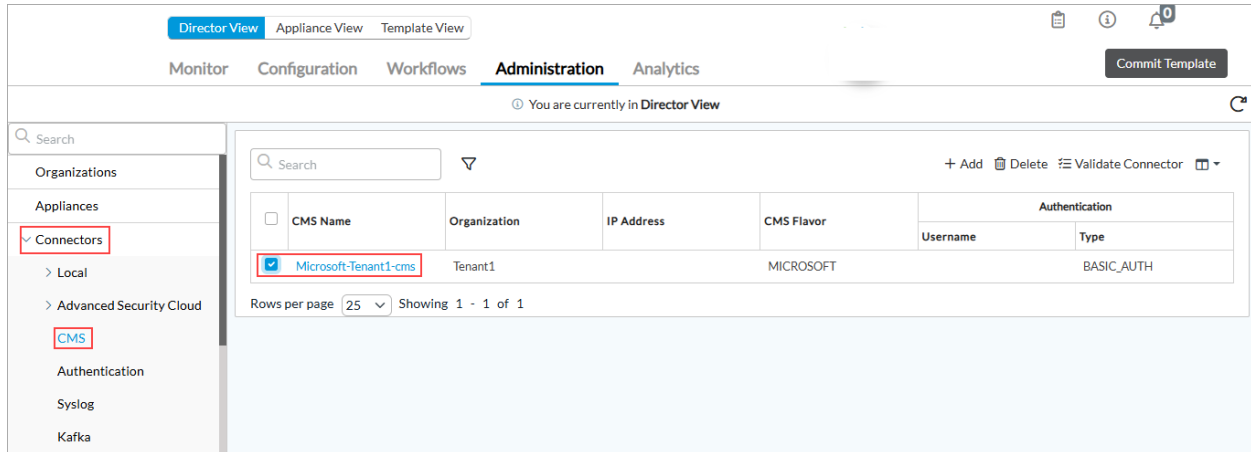
- Microsoft Entra application client ID, client secret, and tenant ID that you gathered in the [Gather Information from Microsoft Entra Application](#), above.

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.

The 'Add CMS Connector' dialog box is shown. It contains several input fields. The 'CMS Name' field is filled with 'Microsoft_Global_Secure_Access'. The 'Organization' dropdown is set to 'provider-org'. The 'CMS Flavor' dropdown is set to 'Microsoft GSA'. The 'Client ID' field is filled with '1111111111'. The 'Client Secret' field is filled with a series of dots and has a red box around it. The 'Tenant ID' field is filled with '111111111111' and also has a red box around it. At the bottom right, there are 'OK' and 'Cancel' buttons.

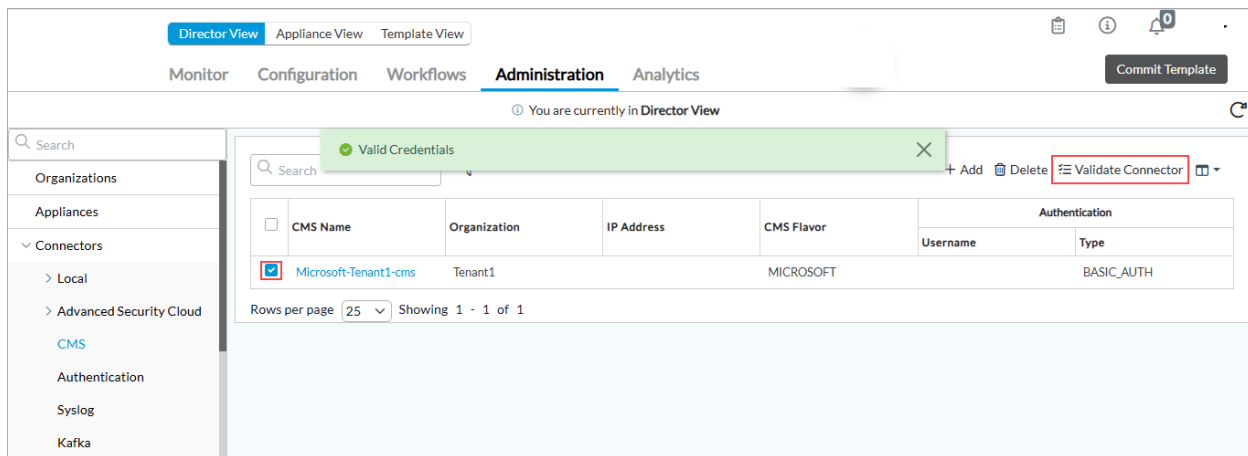
Field	Description
CMS Name (Required)	Enter the name of the CMS connector. The name is a text string.
Organization (Required)	Select the tenant organization, which should be present in the provider Versa Director.
CMS Flavor	Select Microsoft GSA for the type of cloud service.
Client ID (Required)	Enter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

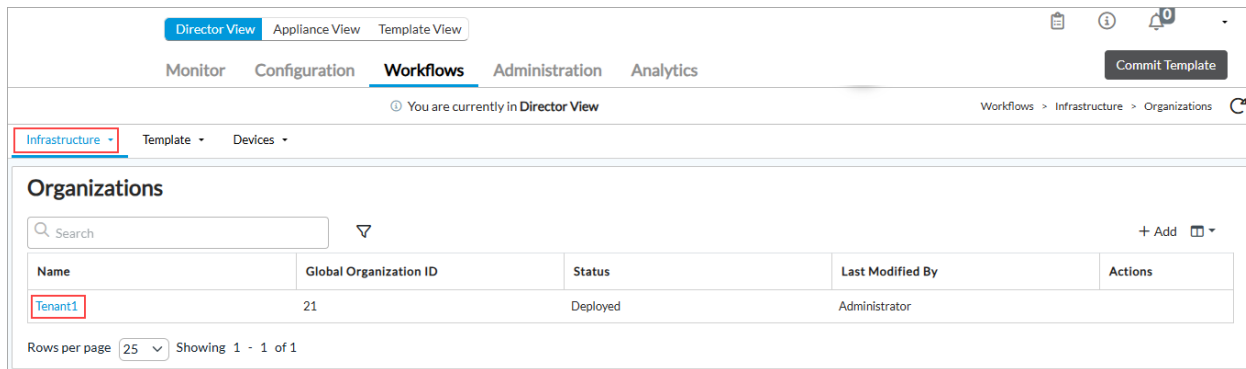


Associate a CMS Cloud Connector with an Organization

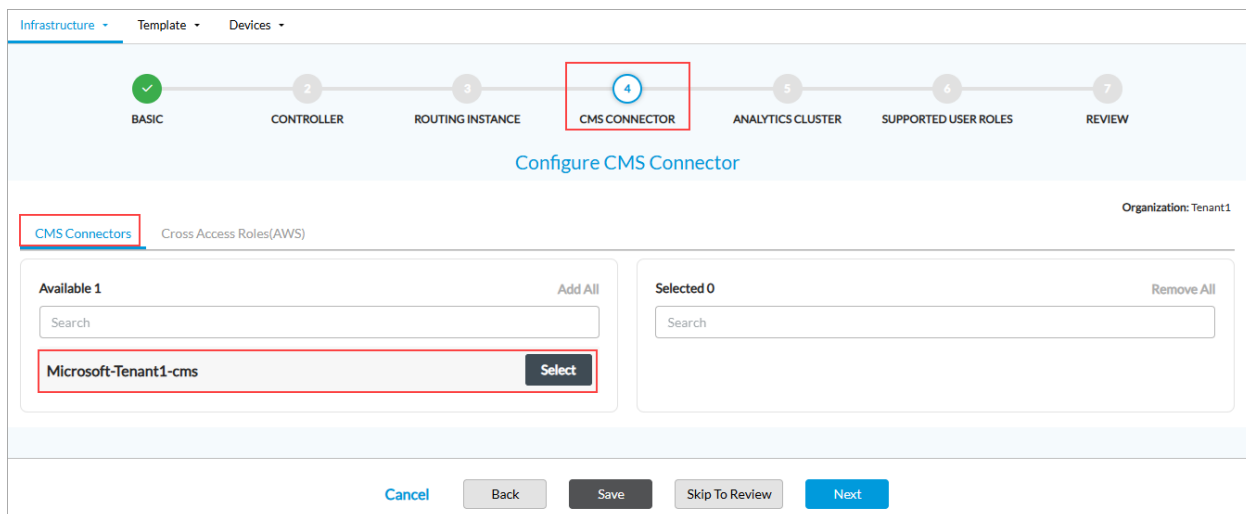
After you add a CMS cloud connector, you associate it with an organization that is already configured on the Director node.

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](#).

The screenshot shows the Versa Networks Director View interface. At the top, there are tabs for 'Director View', 'Appliance View', and 'Template View'. Below these are navigation tabs: 'Monitor', 'Configuration', 'Workflows' (highlighted with a red box), 'Administration', and 'Analytics'. A 'Commit Template' button is visible in the top right. The main content area shows the 'Workflows' tab selected, with a sub-tab 'Template' also highlighted. Below this, there's a 'Templates' section with a search bar and a table of templates. The table has columns for 'Name', 'Status', 'Last Modified Date', 'Last Modified By', and 'Actions'. Two templates are listed: 'PostStagingTemp' and 'StagingTemp'. The 'PostStagingTemp' row is highlighted with a red box. At the bottom, there's a 'Rows per page' dropdown set to 25 and a 'Showing 1 - 2 of 2' indicator.

☐	Name	Status	Last Modified Date	Last Modified By	Actions
☐	PostStagingTemp	Deployed	Tue, Aug 26 2025, 22:13	maurice	
☐	StagingTemp	Deployed	Tue, Aug 26 2025, 13:15	Administrator	

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

Organization: provider-org You are currently in Director View Workflows > Template > Templates

Infrastructure > Template > Devices

1 BASIC 2 INTERFACES 3 TUNNELS 4 ROUTING 5 INBOUND NAT 6 MANAGEMENT SERVERS 7 REVIEW

Configure Tunnels

Template: PostStagingTemp

Tunnels

Split tunnels

VRF Names * WAN Interfaces * Direct Internet Access Gateway

☐ Load Balance

Site to Site Tunnels

Name *	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	iBGP	NAT Enabled	
	---Please S v	---Please S v	---Please S v	---Please S v	---Please S v	☐	☐	☐	+

No Records to Display

Partner Site to Site Tunnels

▽ + Add

Name	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	Actions
Site-1-east	microsoftGSA	IPSEC	1 WAN2	Tenant1-L...	

Cancel Back Save Skip To Review Next

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

Partner Site to Site Tunnels

Name *

Site-1-east

Peer Type

Microsoft GSA

Tunnel Protocol

IPsec

WAN Network (1 is the highest priority)

1 WAN2

Organization

Tenant1

LAN VRF

Tenant1-LAN-VR

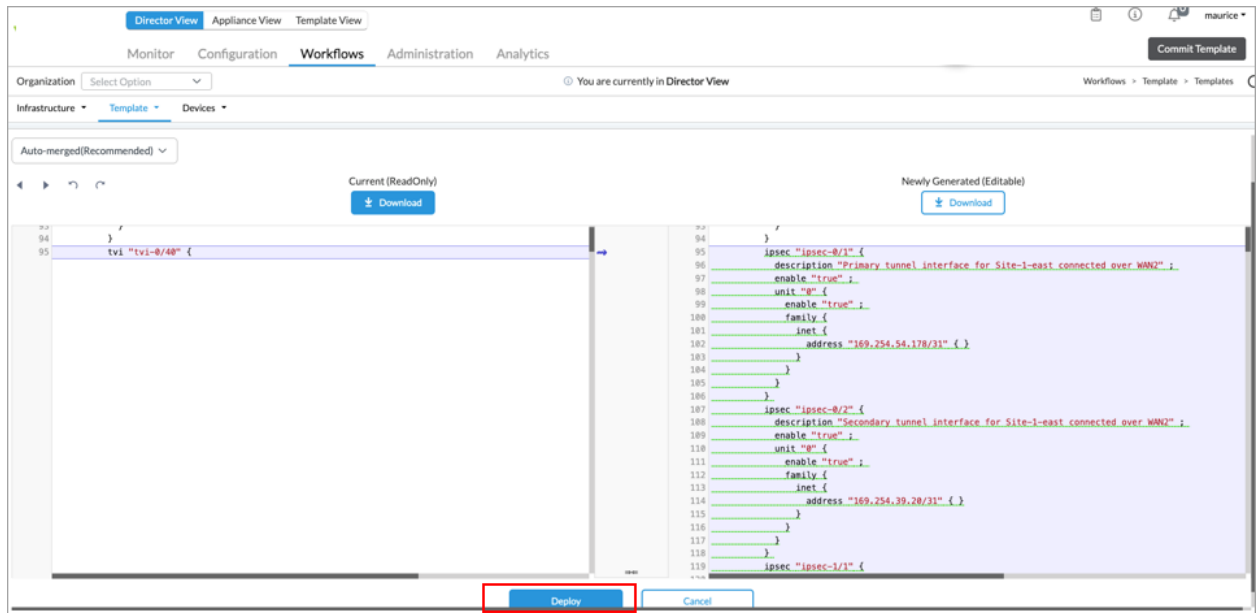
OK

Cancel

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

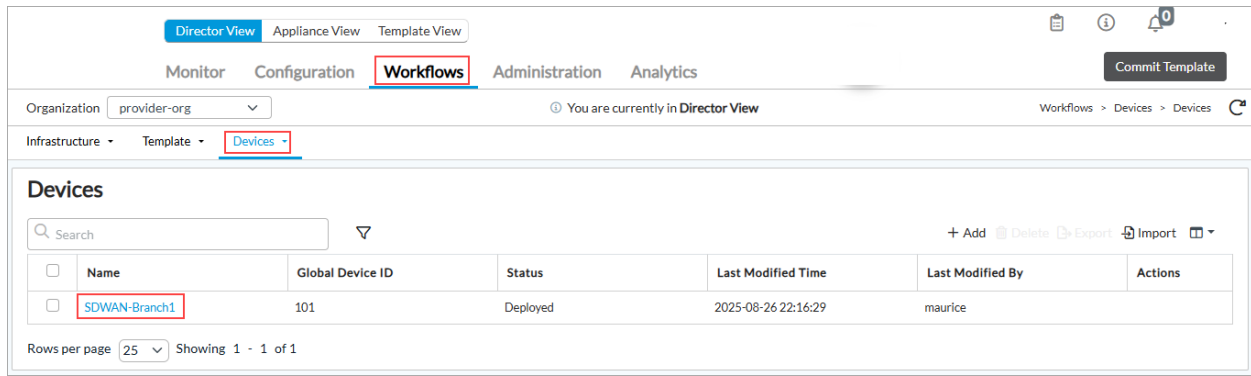
Versa Network's device workflow automates configuration or provisioning, attaching the device groups and bind data for each VOS instance. To configure the device workflow, you must attach the template workflow to the device group within the device workflow.

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](#).

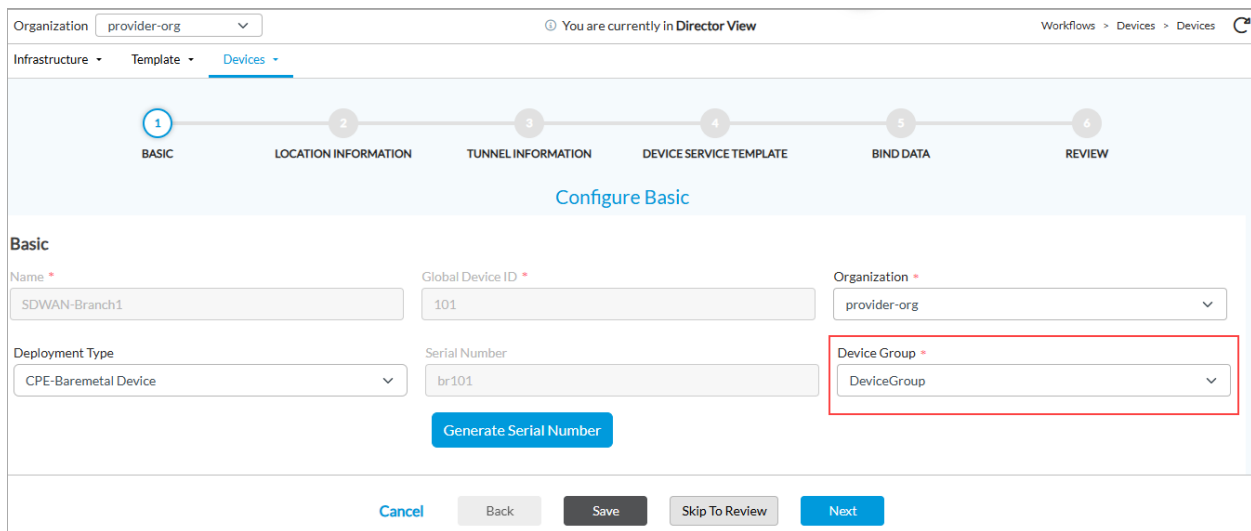
For more information on device workflows, see [Overview of Configuration Templates](#).

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

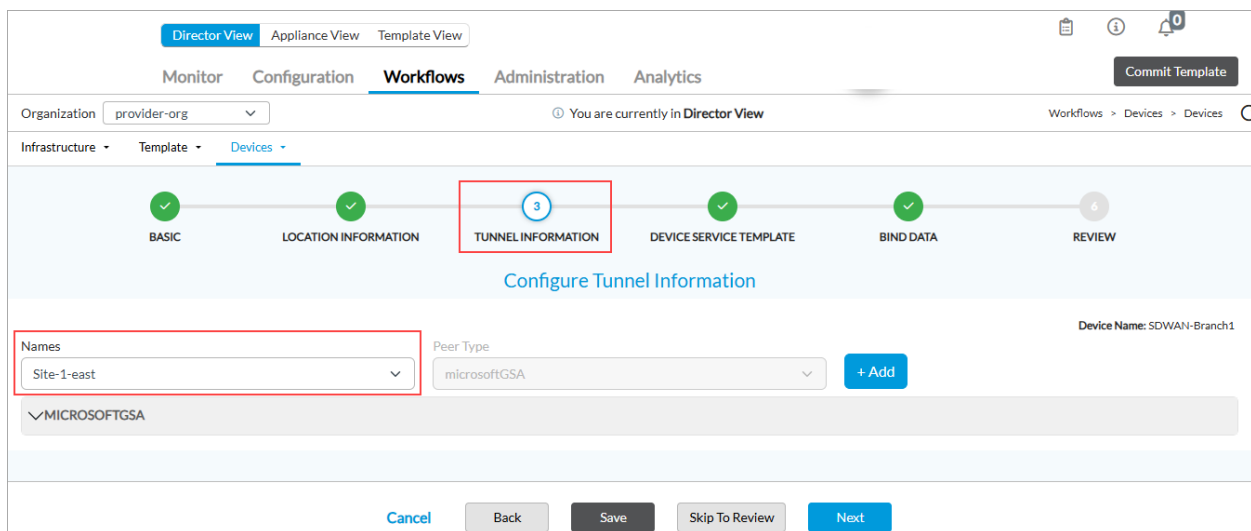
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the left menu bar.
3. Select a device in the main pane.



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.

Configure Site To Site Tunnel

Bandwidth (Mbps)

500

BGP PEER IP

169.254.1.1

BGP Zone PEER IP

169.254.2.1

BGP Local ASN

65015

Versa BGP Local IP

169.254.100.1

Region

East US

OK

Cancel

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.

Organization: provider-org You are currently in Director View Workflows > Devices > Devices

Infrastructure ▾ Template ▾ **Devices ▾**

✓ BASIC
✓ LOCATION INFORMATION
3 TUNNEL INFORMATION
✓ DEVICE SERVICE TEMPLATE
✓ BIND DATA
6 REVIEW

Configure Tunnel Information

Names: Site-1-east Peer type: microsoftGSA + Add

^ MICROSOFTGSA

Name	Peer Type	Bandwidth	BGP PEER IP	BGP Zone PEER IP	BGP Local ASN	Versa BGP Local IP	Region	Actions
Site-1-east	microsoftGSA	500 Mbps	169.254.1.1	169.254.2.1	65015	169.254.100.1	East US	

Showing 1 - 1

Cancel
Back
Save
Skip To Review
Next

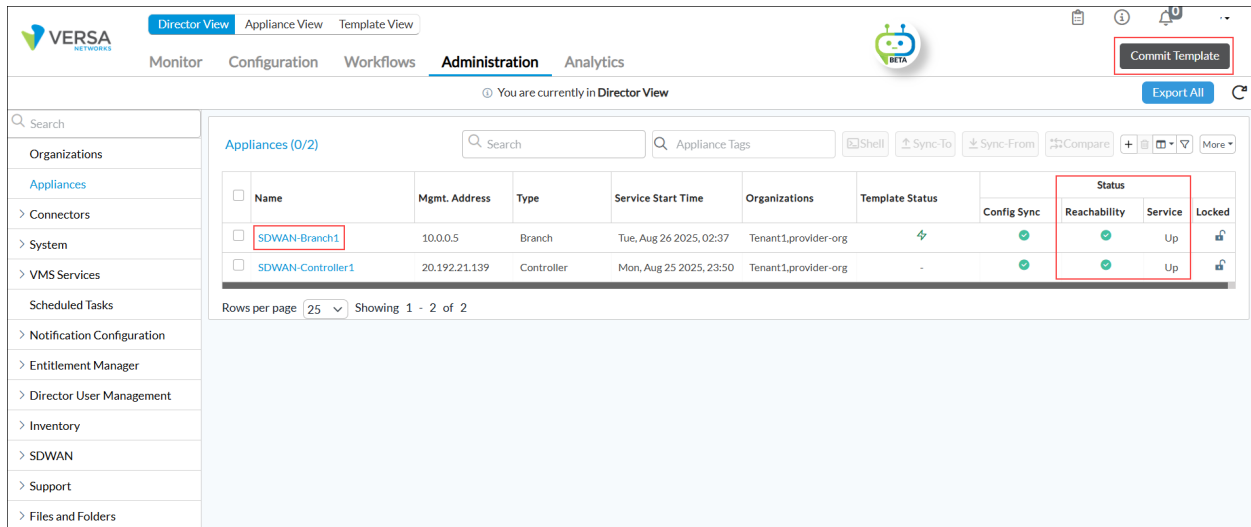
8. Click Save.
9. If modifying an existing device:
 - a. Click Step 6, Review, and then click Re-Deploy.
 - b. Commit the template.

Commit Template Modifications

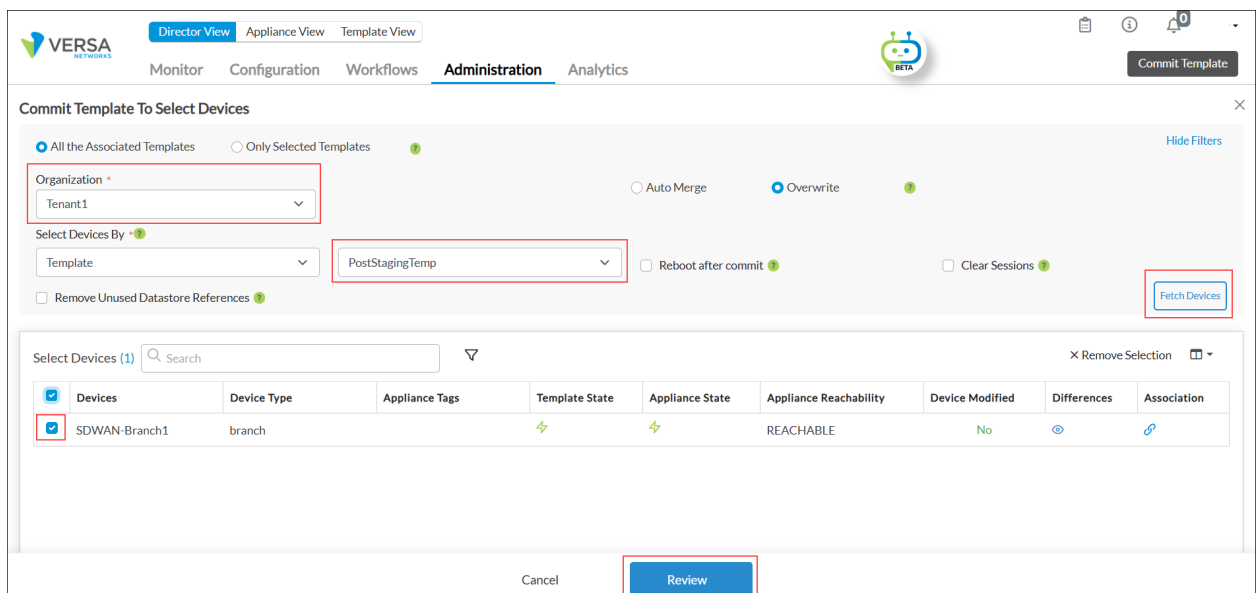
When you change the configuration in an existing configuration or service template, you must commit the changes so that the new configuration is deployed on the associated devices. You can commit all changes, and you can merge the changes into the existing configuration.

To commit a modified template:

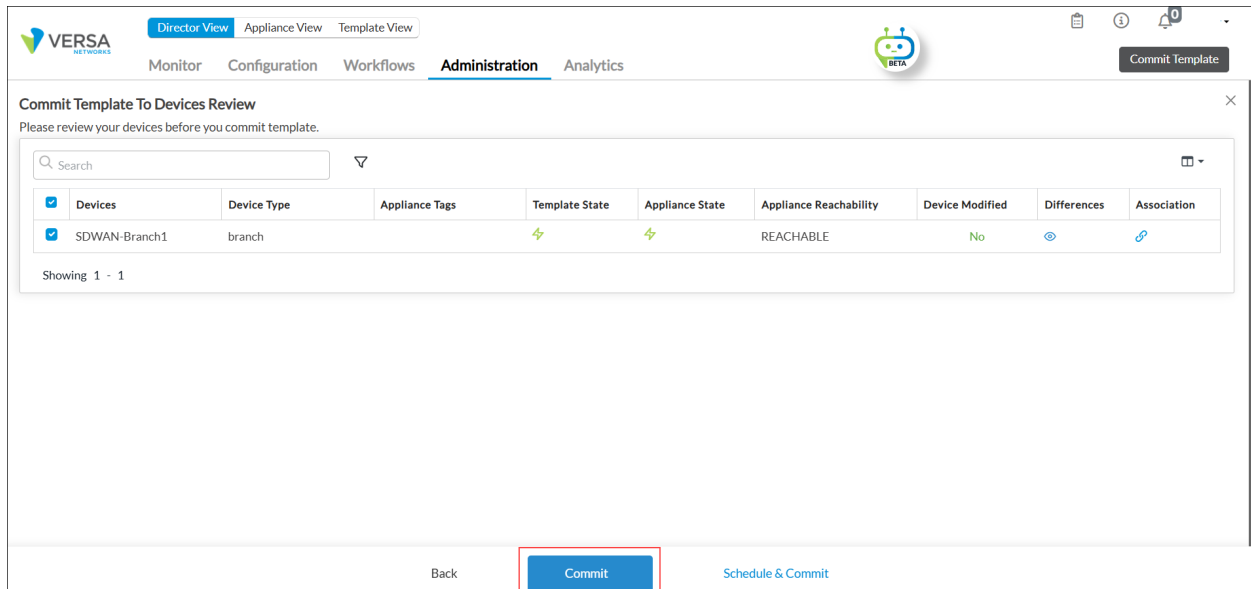
1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. In the Status column in the main pane, check whether Reachability is green and Service is Up, and then click Commit Template.



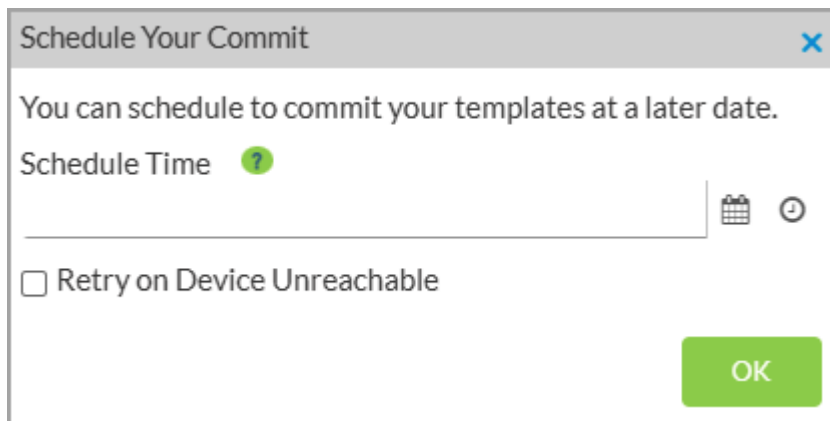
4. In the Commit Template To Select Devices window, select which templates to commit to which devices. You can select either All the Associated Templates or Only Selected Templates. The All the Associated Templates option is selected by default.
 - a. Select the organization.
 - b. Select a post-staging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

Tasks						
Failed 7 Pending 0 In Progress 0 Success 26 Total 33						
		ID	User	Activity	Time	Description
					Start Time End Time	
☐	>	33	maurice	Apply-Template-Devices	Wed, ... Wed, ...	Apply Template to devices [SDWAN...
Description : Apply Template to devices [SDWAN-Branch1], apply mode = overwrite Initiated by : maurice Running Messages : - Started - Applying template to [SDWAN-Branch1] - Loaded up Device Group [DeviceGroup] and number of appliance in this group is 1 - Checking all Devices for connectivity... - All Device(s) are online. Template commit will be applied to ALL. - Starting to build Merged Template - Finished building Merged Template - Starting to Apply Template to All Devices. - Applying-Template [PostStagingTemp] [SDWAN-Branch1] Result=Success - Updating Organization Association for All Appliances - Finished Updating Organization Association for All Appliances - Successfully attempted to apply template to All Appliance.						

Verify IPsec Tunnel Services

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

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

The screenshot shows the Versa Networks Director interface. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The 'Monitor' tab is selected. The main pane displays the configuration for 'SDWAN-Branch1'. The 'Services' tab is selected, and the 'IPsec' sub-tab is active. The 'IKE History' section shows a table with columns: Local Address, Peer Address, Latest Status, and Last Status Timestamp. The table contains one entry for the IPsec tunnel.

Local Address	Peer Address	Latest Status	Last Status Timestamp
207.47.61.66	20.81.104.217	Active	2025-09-03T08:20:13.71197-08:00

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

https://docs.versa-networks.com/Versa_Internal/WIP/Suby/Draft%3A_Versa_Secure_SD-WAN_and_Microsoft_Entra_Internet...

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

Copyright © 2025, Versa Networks, Inc.

Director View
Appliance View
Template View

Monitor
Analytics
Configuration
Administration

Organization: Tenant1
You are currently in Appliance View
Build

Summary
Devices
Cloud Workload

Total Appliances: 2
SDWAN-Branch1

SDWAN-Branch1 | CBP, KA, IND 562101
Inband Management Address: 10.0.0.5
Out of band Management Address: 20.192.21.132/24
System Bridge Address: 0A:14:02:64:01:00

Reachable | SYNC: IN_SYNC
Up since: Tue Aug 26 02:37:10 2025

Summary
Services
Networking
System
Tools

Configuration
Shell
Config Status
Upgrade
Subscription

SDWAN
CGNAT
SDLAN
IPsec
Sessions
SCI
Secure Access
APM
VMS

Branch To Branch
IKE History
IKE Security Association
IPsec History
IPsec Security Association
Overview
Profile Statistics
Site To Site

Site-1-east-WAN2-Primary

Search

	Local Address	Peer Address	Latest Status	Last Status Timestamp
☒	207.47.61.66	20.81.104.217	Active	2025-09-03T08:20:13.71197-08:00

Events

Index	Timestamp	Type	Inbound SPI	Outbound SPI	Role
0	2025-09-03T08:20:13.711972-08:00	IKE Rekey	0x200191368bbba3	0x6559a69f236269f9	responder
1	2025-09-03T00:44:14.076201-08:00	IKE Rekey	0x2008503b19ea32f	0x3e3c58254a19866	responder
2	2025-09-02T17:08:14.453354-08:00	IKE Rekey	0x200c2336e1ef785	0x13bdef2ad9decf0b	responder
3	2025-09-02T09:32:14.824399-08:00	IKE Rekey	0x2009ef7d28ac3c9	0x71e99229554932c5	responder
4	2025-09-02T01:56:15.197131-08:00	IKE Rekey	0x20088068f932d92	0xd20848df9998a046	responder
5	2025-09-01T18:20:15.564131-08:00	IKE Rekey	0x200ac8f773cd9b5	0x4bb352537c32a4fd	responder
6	2025-09-01T10:44:15.933193-08:00	IKE Rekey	0x2008c1ac30ee12c	0x56d48490907a9143	responder
7	2025-09-01T03:08:16.299109-08:00	IKE Rekey	0x2004b054be2aaf2	0x64d6a76994f7e7d0	responder

Last Status Timestamp: 2025-09-03T08:20:13.71197-08:00
Latest Status: Active
Local Address: 207.47.61.66
Peer Address: 20.81.104.217

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

The screenshot displays the Versa Director interface in Appliance View. The top navigation bar includes tabs for Director View, Appliance View (selected), and Template View. The main menu shows Monitor, Analytics, Configuration, and Administration. The Organization is set to Tenant1. The left sidebar shows Summary, Devices (selected), and Cloud Workload. The main pane shows the configuration for SDWAN-Branch1, including its management addresses and status (Reachable, SYNC: IN_SYNC). The IPsec tab is selected, showing the IPsec Security Association configuration for Site-1-east-WAN2-Primary. The configuration details are as follows:

Peer Address	Inbound SPI	In Bytes Rate	Outbound SPI	Out Bytes Rate	Cipher	Up Time	Next Rekey Time	Tunnel Status	Tunnel Routing Insta...
20.81.104.217	0x2003d3f	199	0xada6b016	0	aes-gcm	6d17h32m	07:59:53	UP	Tenant1-microsoftGS...

Additional configuration details for the selected peer:

- Anti Replay: enable
- Hardware Accel Type: none
- In Bytes: 1396
- In Invalid: 0
- In Bytes Rate: 0
- IPsec Mode: tunnel
- Key Source: none
- Local ID String: 207.47.61.66
- Negotiation Life Time: 28800
- Out Bytes: 667
- Out Drop No SA: 0
- Out Bytes Rate: 0
- Peer Address: 20.81.104.217
- Peer ID Type: ip
- Cipher: aes-gcm
- In Anti Replay Duplicate: 0
- In Drop Anti Replay: 0
- In Packets: 11
- In Packets Rate: 0
- IPsec Protocol: esp
- Local Address: 207.47.61.66
- Local ID Type: ip
- Negotiation Life Volume: 0
- Out Drop Coalesce Fail: 0
- Out ESP/AH: 11
- Out Packets Rate: 0
- Peer Auth Type: psk
- Pfs Dh Group: mod20
- HMAC: none
- In Anti Replay OOO: 0
- In Drop MAC: 0
- In Plain: 11
- Inbound SPI: 0x2003d3f
- Key Length: 256
- Local Auth Type: psk
- NAT T: disable
- Next Rekey Time: 07:59:49
- Out Drop No mbuf: 0
- Out Packets: 11
- Outbound SPI: 0xada6b016
- Peer ID String: 20.81.104.217
- Remaining Life Time: 28789

Verify Microsoft Entra BGP Peers in Versa Director

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

Organization: Tenant1

SDWAN-Branch1

SDWAN-Branch1 | CBR KA, IND 562101
Inband Management Address: 10.0.0.5
Out of band Management Address: 20.192.21.132/24
System Bridge Address: 0A:14:02:64:01:00

Reachable | SYNC-IN SYNC
Up since: Tue Aug 26 02:37:10 2025

Summary Services **Networking** System Tools

Configuration Shell Config Status* Upgrade Subscription

Interfaces Routes **BGP** OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP 802.1X RIP Switching LLDP

Neighbors **Advertised Prefixes** Received Prefixes

Tenant1-microsoftGSA-Transport-VR

Neighbor IP	Remote AS Number	Local Address	State	Established Time	Total Sent Prefixes	Total Received Prefixes	Total Transmitted Messages	Total Received Messages
169.254.1.1	65476	169.254.100.1	Established	6d17h40m	6	36	29911	28034
169.254.2.1	65476	169.254.100.1	Established	6d17h48m	42	36	31000	28005
169.254.62.195	64514	169.254.62.194	Established	1w1d04h	38	4	27149	27147

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

Organization: Tenant1

SDWAN-Branch1

SDWAN-Branch1 | CBR KA, IND 562101
Inband Management Address: 10.0.0.5
Out of band Management Address: 20.192.21.132/24
System Bridge Address: 0A:14:02:64:01:00

Reachable | SYNC-IN SYNC
Up since: Tue Aug 26 02:37:10 2025

Summary Services **Networking** System Tools

Configuration Shell Config Status* Upgrade Subscription

Interfaces Routes **BGP** OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP 802.1X RIP Switching LLDP

Neighbors **Advertised Prefixes** Received Prefixes

Tenant1-microsoftGSA-Transport-VR IPv4 Unicast

Neighbor Address: Community: Extended Community: Prefix:

	Nexthop	Prefix	Peer	Local Preference	Pre Policy	From Rib
>	169.254.2.1	13.107.6.152/31	169.254.2.1	100		
>	169.254.2.1	13.107.6.171/32	169.254.2.1	100		
>	169.254.2.1	13.107.6.192/32	169.254.2.1	100		
>	169.254.2.1	13.107.9.192/32	169.254.2.1	100		
>	169.254.2.1	13.107.18.10/31	169.254.2.1	100		
>	169.254.2.1	13.107.18.15/32	169.254.2.1	100		

Verify Traffic Through VOS to Microsoft Entra

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

https://docs.versa-networks.com/Versa_Internal/WIP/Suby/Draft%3A_Versa_Secure_SD-WAN_and_Microsoft_Entra_Internet...

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

Copyright © 2025, Versa Networks, Inc.

Summary	Services	Networking	System	Tools	Configuration	Shell	Config Status*	Upgrade	Subscription
SDWAN	CGNAT	SDLAN	IPsec	Sessions	SCI	Secure Access	APM	VMS	
Detail									
Application	Source IP	Destination IP	Protocol	Source Port	Destination P...	SDWAN	Natted	Dropped Reverse...	Reverse Packe...
Application: Microsoft Outlook(outlook)/(predef)	Destination Scalable Group Tag: 0	Dropped Forward Packet Count: 0	External Service Chaining: false	Forward Egress Vrf: Tenant1-microsoftGSA-Transport-VR	Forward Offload: false	Idle For: 00:00:09	Natted: No	Protocol: TCP	Reverse Egress Vrf: Tenant1-microsoftGSA-Transport-VR
Reverse Offload: false	SDWAN: No	Session Provider Zone: 0	Source Scalable Group Tag: 0	Destination IP: 52.108.8.12	Device:	Dropped Reverse Byte Count: 0	Forward Byte Count: 3457	Forward FC: fc_be	Forward Packet Count: 22
Idle Timeout: 240	Parent Session ID: 0	Reverse Byte Count: 32162	Reverse FC: fc_be	Reverse Packet Count: 33	Session ID: 6014	Source IP: 10.20.3.50	VSN ID: 0	Destination Port: 443	Dropped Forward Byte Count: 0
Dropped Reverse Packet Count: 0	Forward Egress Interface: ipsec-0/1.0	Forward Ingress Interface: tvi-0/16644.0	Forward P1p: low	Is Child: No	PBF Enabled: false	Reverse Egress Interface: tvi-0/16644.0	Reverse Ingress Interface: ipsec-0/1.0	Reverse P1p: low	Session Age: 00:00:55
Source Port: 57586	VSN Vid: 2								

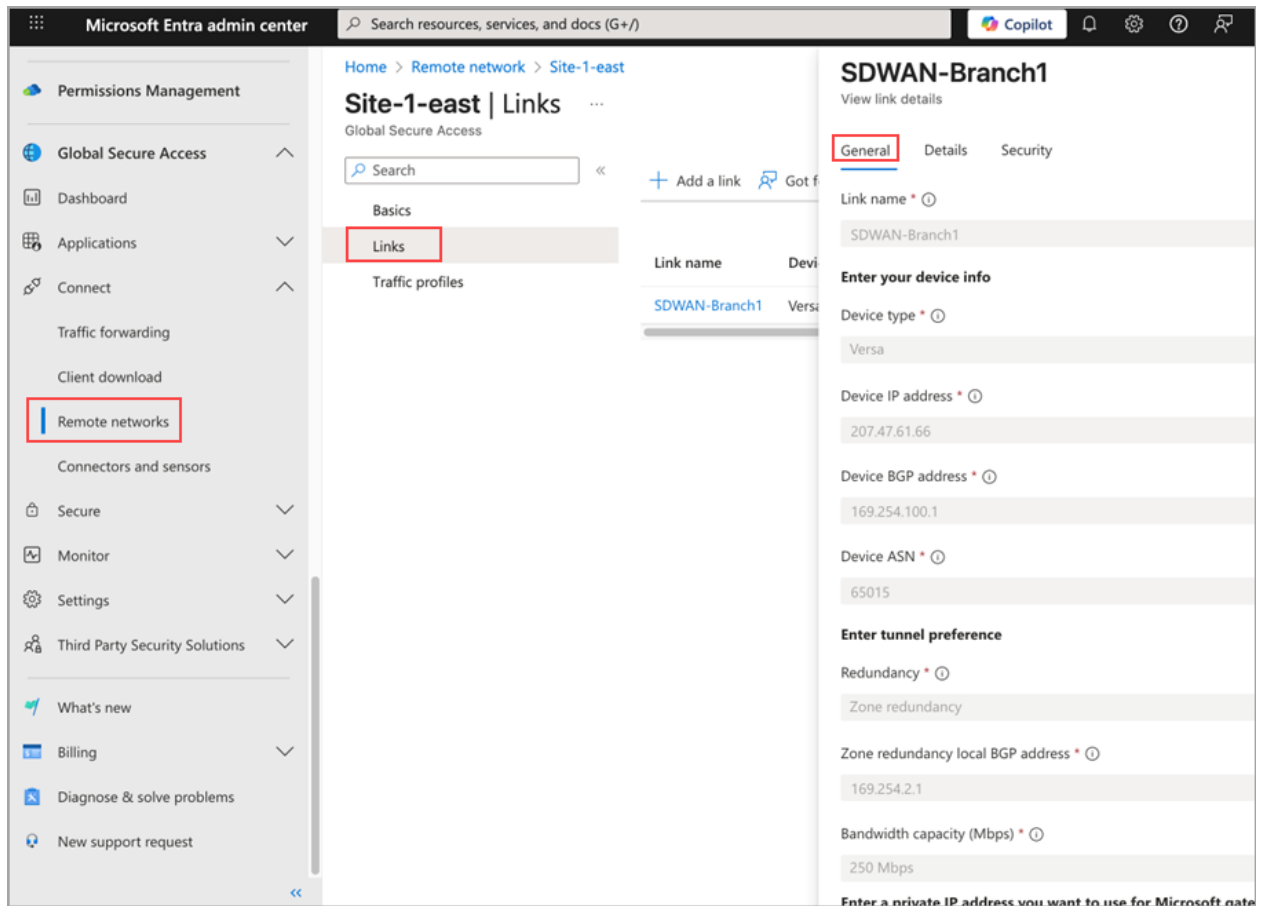
Verify Versa Director Device Information from Microsoft Entra

To verify the device information from Microsoft Entra:

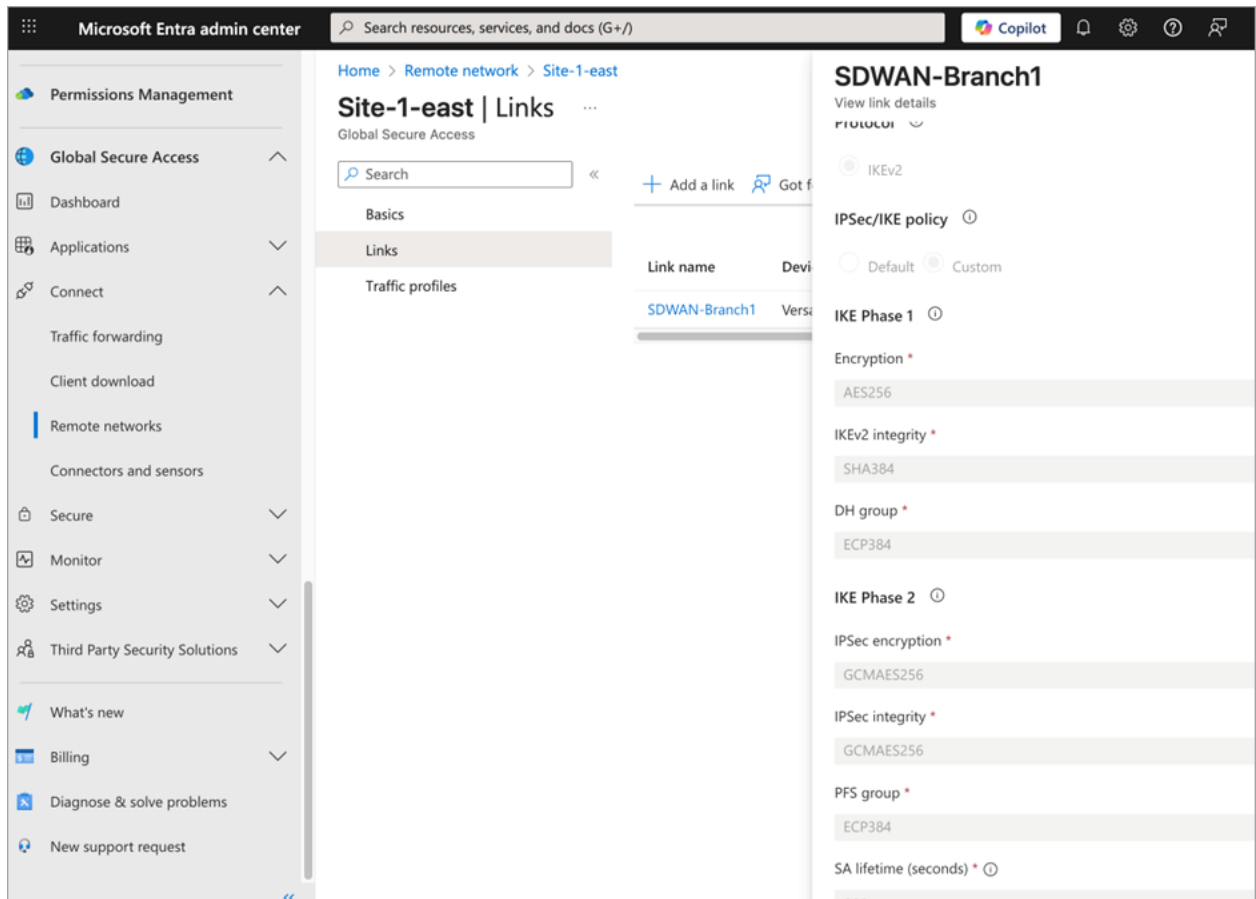
1. Log in to Microsoft Entra Admin Center.
2. Navigate to Global Secure Access > Connect > Remote Networks.
3. Click the remote network created by Versa Director.

Microsoft Entra admin center	Search resources, services, and docs (G+/)	Copilot	Home >
Permissions Management	Global Secure Access	Dashboard	Applications
Connect	Traffic forwarding	Client download	Remote networks
Remote network	Create remote network	Refresh	Got feedback?
Remote networks enable admins to define and configure remote network locations, including names, regions, and bandwidth capacity, and add one or more customer premises equipment (CPE) links to a given remote network.	Search by remote network na...	Device type == All	
Remote net...	Region	Device links	Device type
Site-1-east	East US	1 link	1 profile
			08/20/2025, 03:32 ...
			b3695a5

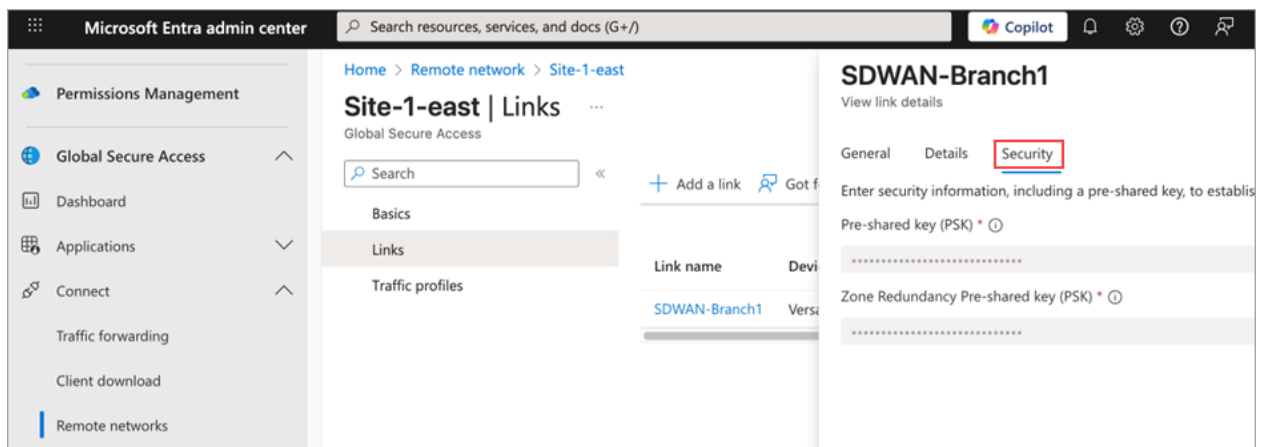
4. In the remote network details page, select Links. The view link details pane displays the device information.
 1. Select the General tab to view the device information.



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:

https://docs.versa-networks.com/Versa_Internal/WIP/Suby/Draft%3A_Versa_Secure_SD-WAN_and_Microsoft_Entra_Internet...

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

Copyright © 2025, Versa Networks, Inc.

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

Microsoft Entra admin center

Home > Traffic logs (Preview) > Versa ASC > Conditional Access | Policies > Create new policy from templates > Traffic forwarding >

Traffic logs (Preview)

Download Refresh Columns Got feedback?

All Connections: 31 Internet Access: 0 Private Access: 0 Microsoft 365 Access: 31

Timespan: Last 24 hours Add filter

Connections Transactions

Created date time	Id	Status	Traffic type	Destination FQDN	User principal name	Action	Sour...	Destination IP	Sent bytes	Received bytes	Transaction count	Tra
08/22/2025, 11:02:38.632 AM	d6...	Active	Microsoft 365	login.live.com		Allow	207...	40.126.62.129	0 bytes	0 bytes	1	0
08/22/2025, 11:02:38.346 AM	82...	Active	Microsoft 365	login.live.com		Allow	207...	40.126.62.129	0 bytes	0 bytes	1	0
08/22/2025, 11:02:29.138 AM	c1...	Closed	Microsoft 365	onedrive.live.com		Allow	207...	13.107.139.11	0 bytes	0 bytes	1	0
08/22/2025, 11:02:15.359 AM	7d...	Active	Microsoft 365	login.live.com		Allow	207...	20.190.190.130	0 bytes	0 bytes	1	0
08/22/2025, 11:02:14.960 AM	c2...	Active	Microsoft 365	owl.officeapps.live...		Allow	207...	52.108.9.12	0 bytes	0 bytes	1	0
08/22/2025, 11:01:53.766 AM	47...	Active	Microsoft 365	word.cloud.micros...		Allow	207...	52.108.8.12	0 bytes	0 bytes	1	0
08/22/2025, 11:01:41.249 AM	6c...	Active	Microsoft 365	myapplications.mic...		Allow	207...	20.190.151.71	0 bytes	0 bytes	1	0
08/21/2025, 06:59:20.873 PM	32...	Closed	Microsoft 365	safelinks.protectio...		Allow	207...	52.102.98.160	0 bytes	0 bytes	1	0
08/21/2025, 06:59:20.620 PM	25...	Closed	Microsoft 365	safelinks.protectio...		Allow	207...	52.102.98.160	0 bytes	0 bytes	1	0