

Install on Azure

 For supported software information, click [here](#).

This article describes how to install, or instantiate, a Versa branch device on Microsoft Azure. To perform the installation, you upload the Versa Operating System™ (VOS™) software image to the Azure portal and create an Azure Active Directory (AD) application for the software. Then, Versa Director does the following:

- Orchestrates the VOS software deployment.
- Applies and instantiates post staging configuration to the device to set it to be an SD-WAN gateway.
- Instantiates the device to set it to be a vCPE.

A Versa vCPE is a standalone virtual customer premises equipment device that performs Layer 3 through Layer 7 network functions.

An SD-WAN gateway is used as part of an SD-WAN branch to perform routing, firewall, and security functions as a part of an SD-WAN overlay network.

Releases 22.1.1 and later, which run on Ubuntu 18.04 (Bionic) platforms, support Azure accelerated networking. Releases 21.2 and earlier do not support Azure accelerated networking.

Upload Versa Image to Azure Portal

To install the VOS software on a branch device, you first upload the Versa software images to the Azure portal. To do this, follow the procedure in the [Upload Versa Images to Azure Portal](#) section in the Install Headend Components on Azure article.

Create an Azure AD Application

To allow the VOS software to access and modify Azure resources, you register the VOS software as an application in Azure AD, which is a cloud-based identity and access management service. In Azure AD, you define who can access the VOS software and which actions users are permitted to perform with the VOS software.

To create an Azure AD application for VOS software, first check that that you and your Azure subscription account have the proper permissions. Then create the Azure AD application.

Before you create an Azure AD application for the VOS software, ensure that you have the following:

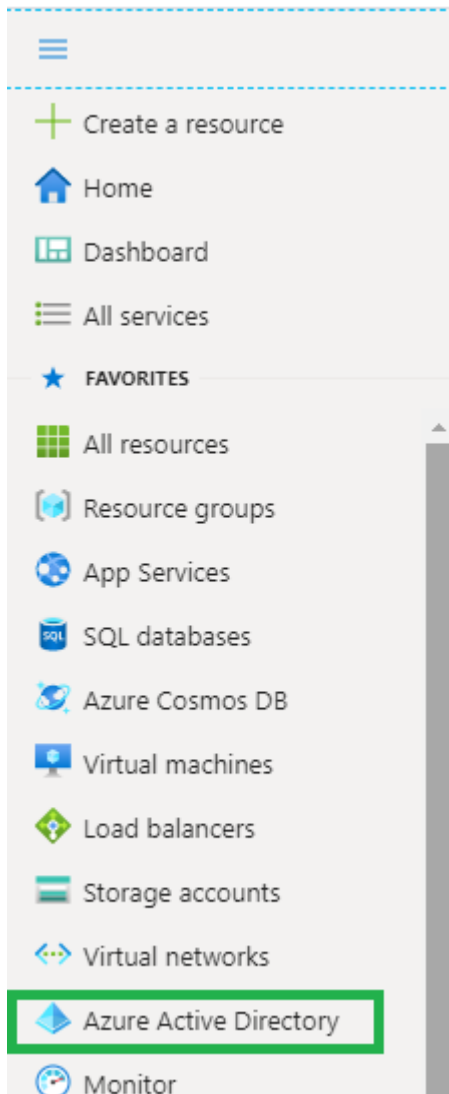
- Permissions to register an application with Azure AD tenant
- Permissions to assign a role to an application in Azure subscription

Check Azure AD and Subscription Permissions

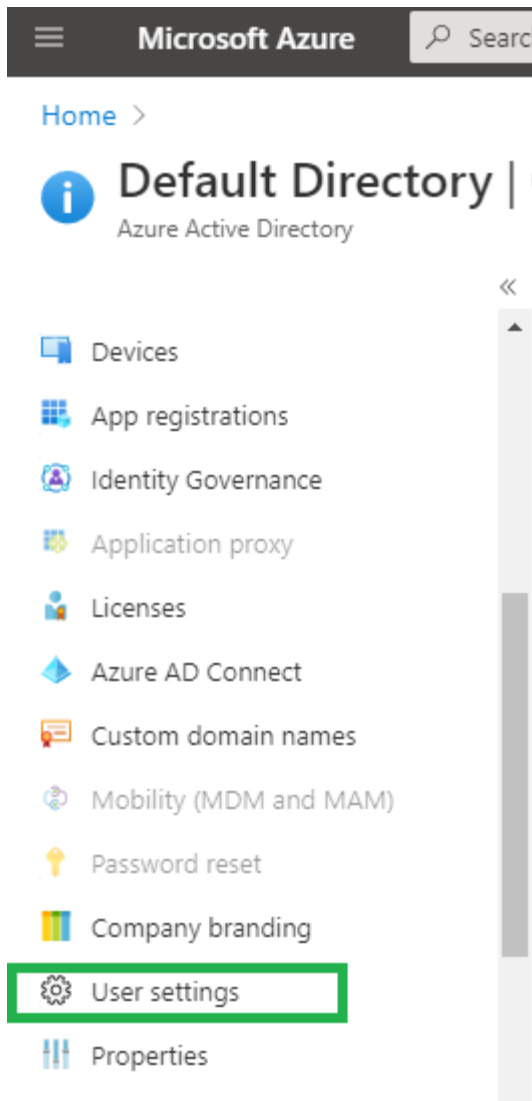
To create an Azure AD application, you must have an administrator role in Azure AD, and your Azure subscription account must have Microsoft.Authorization/*/*Write access so that you can assign an AD application to a role.

To check your Azure AD and subscription permissions:

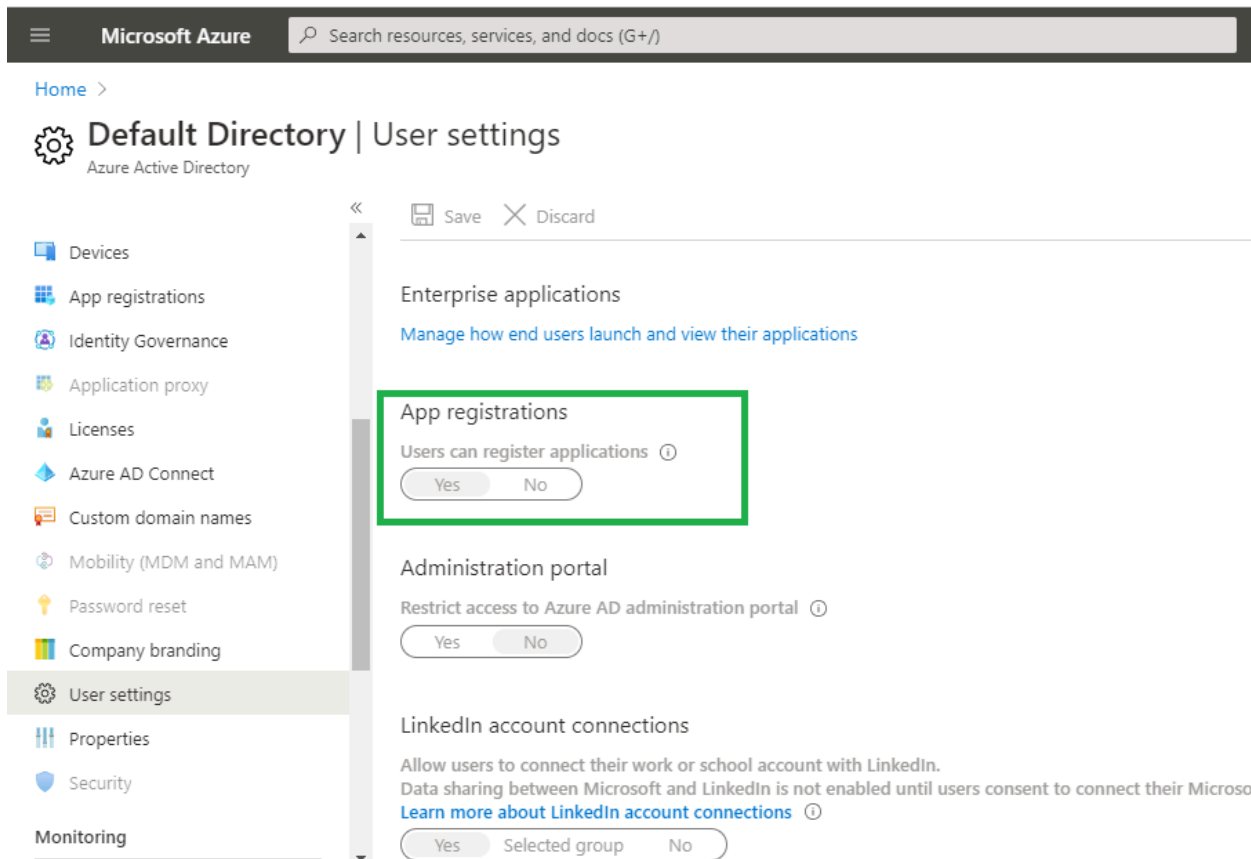
1. Log in to the Azure portal.
2. Select Azure Active Directory.



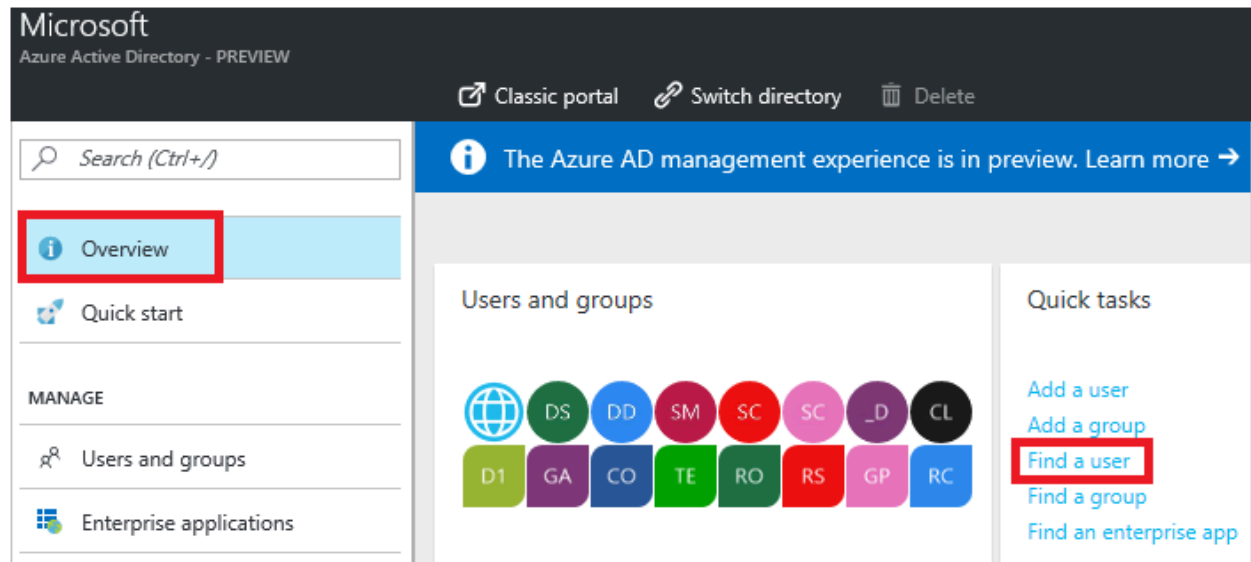
3. In the Azure Active Directory Preview window, select User Settings.



4. Check the setting in the App Registrations: Users Can Register Applications field.
If the field is set to Yes, any user in the Azure AD tenant can register an application. Continue with Step 11, to check your Azure subscription permissions.
If the field is set to No, only administrative users can register an application. Continue with Step 5, to assign permission to other users to register an application.



5. In the left navigation bar, click Overview.
6. In the Quick Tasks pane, click Find a User.




7. In the search box, type the name of the person you want to assign registration permission to, and then click the name.

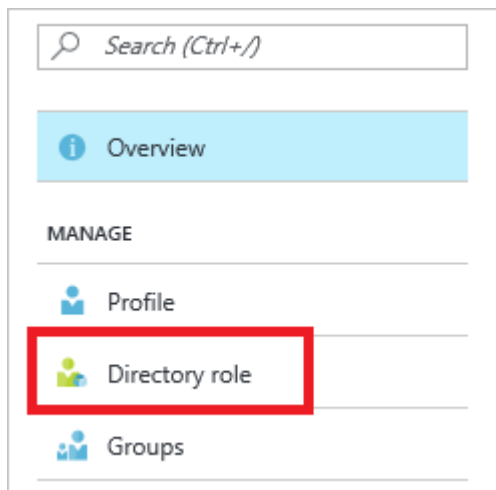
https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:16:50 GMT

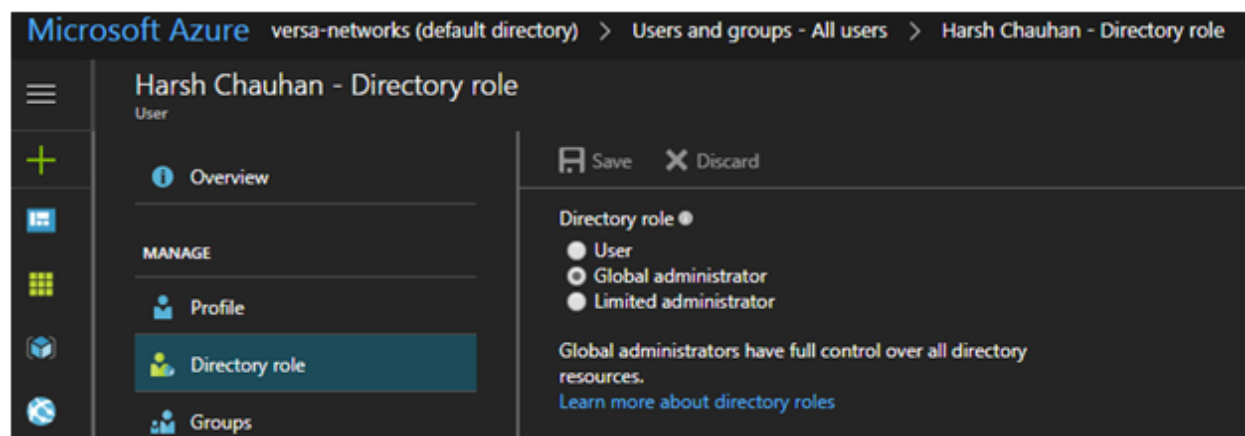
Copyright © 2024, Versa Networks, Inc.

+ Add Columns Multi-Factor A... Filter	
Example Person	
NAME	USER NAME
 Example Person	example@contoso.org

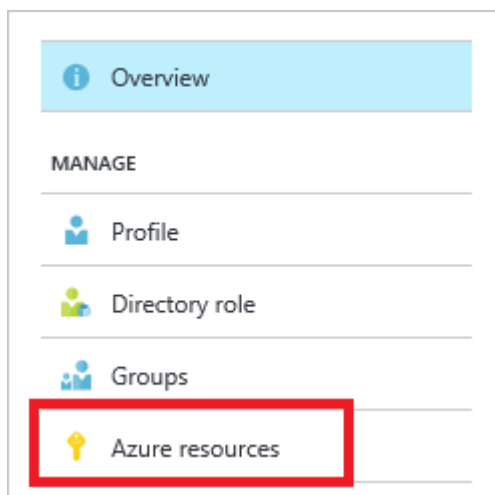
- In the left navigation bar, select Directory Role to view the Azure AD permissions for the user.



- Review the Azure AD permissions for the user. The user must have either the global administrator or limited administrator role. If they do not, ask your administrator to assign the user to one of the administrator roles or to set the permissions such that the user can register applications.




10. In the left navigation bar, select Azure Resources to view the role assigned to the subscription account.



11. Review the assigned role for the subscription account. The subscription account must have the role of either Owner or User Access Administrator. These roles grant Microsoft.Authorization/*/*Write access, which is required to assign an AD application to a role. If the account does not have the appropriate permission, ask your subscription administrator to add you to the User Access Administrator role. For information about Azure roles, see the Built-in Roles for Azure Resources article on the Microsoft Azure website.

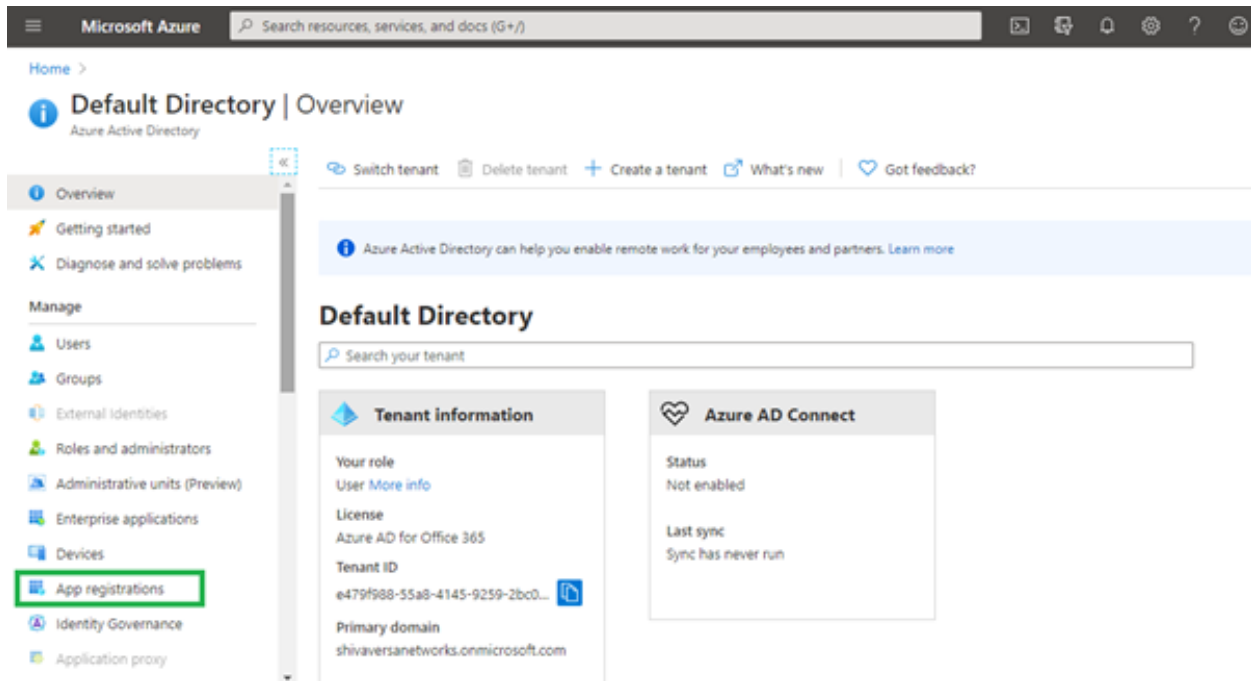
The following figure shows a user who is assigned Owner role:

RESOURCE NAME	RESOURCE TYPE	ROLE	ASSIGNED TO
 Pay-As-You-Go	Subscription	Owner	Subscription adm...

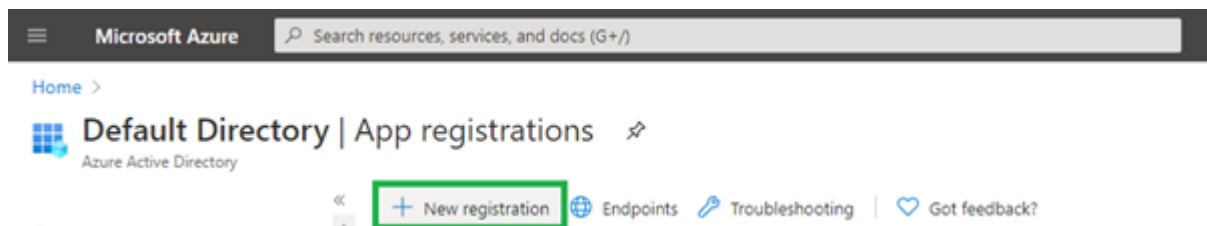
Create an Azure AD Application

To create the Azure AD application for the VOS software:

1. Log in to the Azure portal.
2. Select the Azure Active Directory.
3. In the left navigation bar, select App Registrations.



4. Click New Registration.



5. In the Register an Application pane, enter the following information:
 - a. In the Name field, enter name of the application.
 - b. In the Supported account types field, click Accounts in the organizational directory only (Default Directory Only—Single Tenant) option.
 - c. In the Redirect URI field, select Web from the drop-down list.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Default Directory | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Versa-LAB ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼ e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

6. Click Register.

Get the Application ID, Tenant ID, and Client Secret

To sign in to the VOS application in the Azure AD, you need an application ID, a tenant ID, and a client secret. To get these:

1. From App Registrations in Azure AD, select your application.

Microsoft Azure Search resources, services, and docs (G+)

Home > Default Directory | App registrations

Azure Active Directory

Users
Groups
External Identities
Roles and administrators
Administrative units (Preview)
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses

+ New registration Endpoints Troubleshooting Download (Preview) Got feedback?

Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library.

All applications Owned applications

Versa-LAB

Display name	Application (client) ID
VE Versa-LAB	45b6be

- Copy the application ID and directory ID, and save them for future use. Note that in Versa Director, the application ID is referred to as the client ID and the directory ID is referred to as the tenant ID.

Microsoft Azure Search resources, services, and docs (G+)

Home > Default Directory | App registrations > Versa-LAB

Search (Ctrl+F)

Delete Endpoints

Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Token configuration API permissions

Display name : Versa-LAB

Application (client) ID : 45b6be

Directory (tenant) ID : 502c0ff

Object ID : 656add01-1097-4cf9-884e-cb8985e17bc4

Supported account types : My organization only

Redirect URIs : Add a Redirect URI

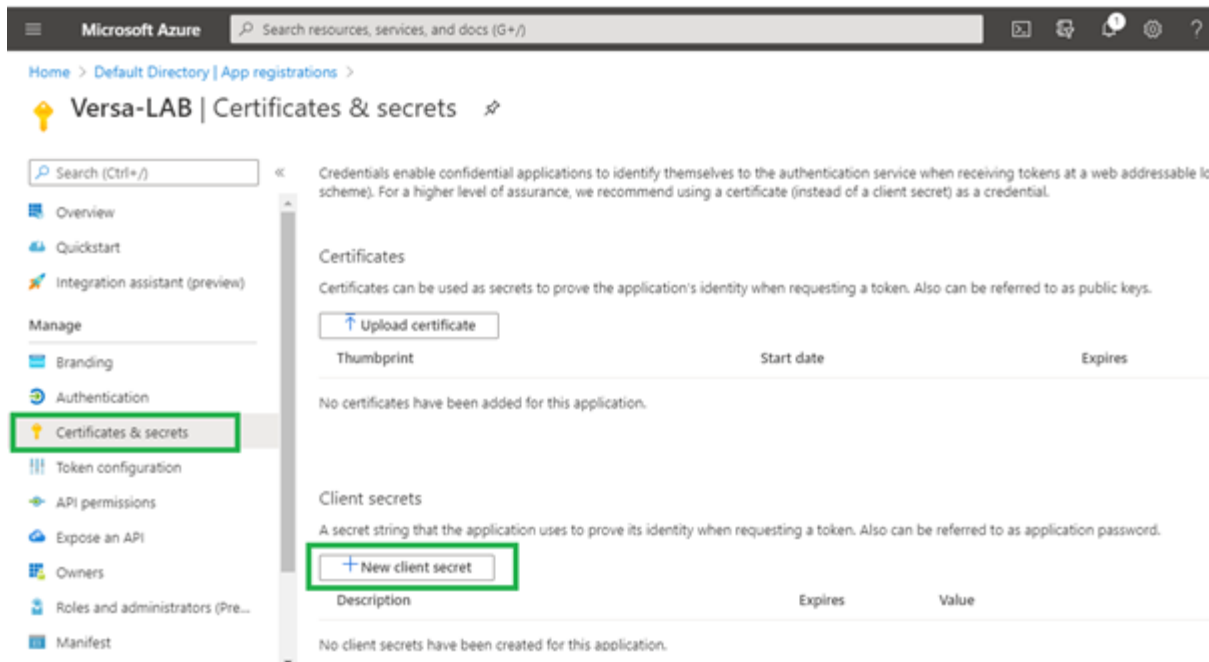
Application ID URI : Add an Application ID URI

Managed application in L... : Versa-LAB

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs Documentation Microsoft identity platform

- Select Certificates and Secrets, and then click New Client Secret to generate an authentication key.



4. In the Add a Client Secret pane, enter the following information:
 - a. In the Description field, enter a text description for the key.
 - b. In the Expires field, select the duration of the key.

Add a client secret

Description

Expires
☒ In 1 year
☐ In 2 years
☐ Never

- c. Click Add to generate the client secret value for the application, which is shown in the Value field.
- d. Copy the client secret value and store it in a safe place. You cannot retrieve the key at a later time.

Description	Expires	Value
Versa-LAB-Key	7/31/2021	VqoRbXH

Assign a Role to the Azure AD Subscription

To access the resources in your Azure AD using the application you created, you must assign a role at your Azure subscription level for the application. For information about Azure roles, see the [Built-in Roles for Azure Resources](#) article on the Microsoft Azure website.

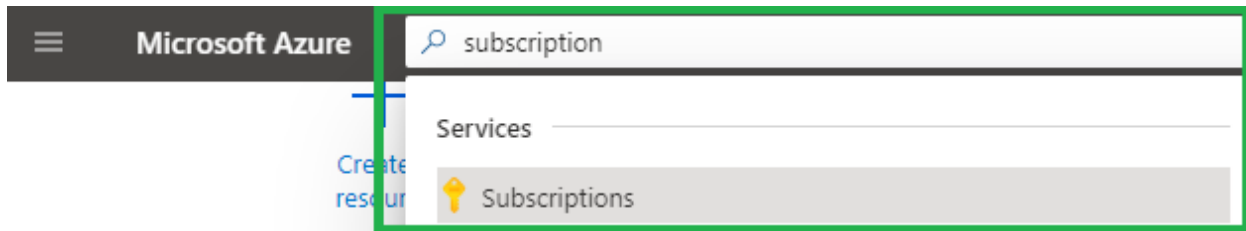
https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:16:50 GMT

Copyright © 2024, Versa Networks, Inc.

To assign a role to the Azure AD subscription:

1. Log in to Azure portal.
2. Select Subscriptions.



3. To retrieve the Azure subscription ID, click subscription name in the Subscriptions pane.

Subscriptions

Default Directory

+ Add

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for other directories, click [Switch directories](#).

My role ⓘ

8 selected

Status ⓘ

3 selected

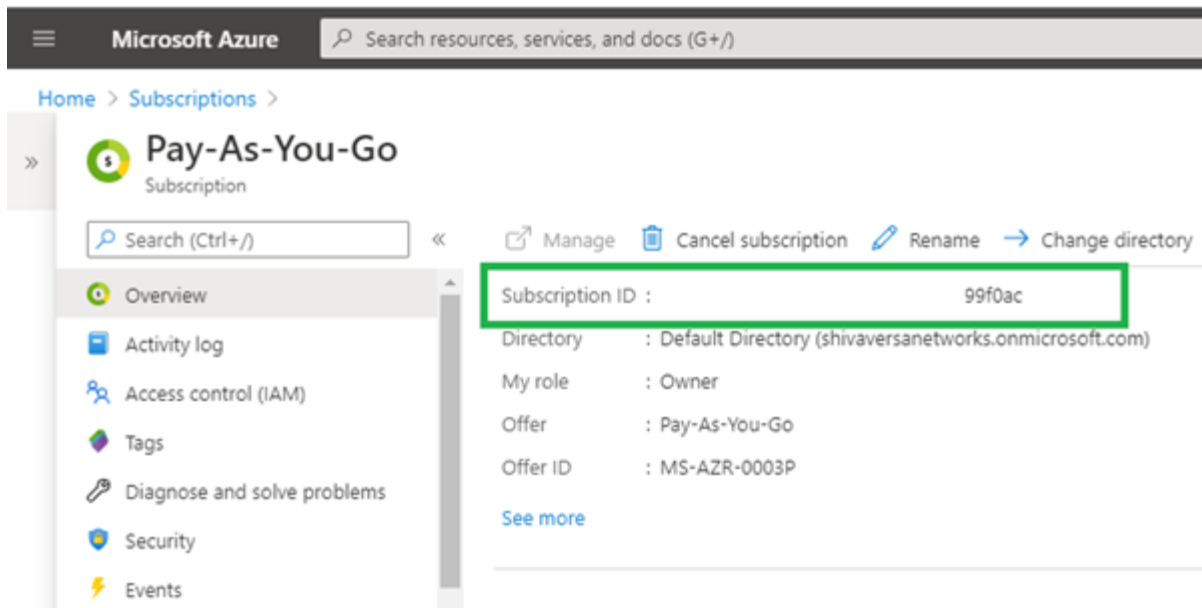
Apply

Showing 1 of 1 subscriptions ☒ Show only subscriptions selected in the [global subscriptions filter](#) ⓘ

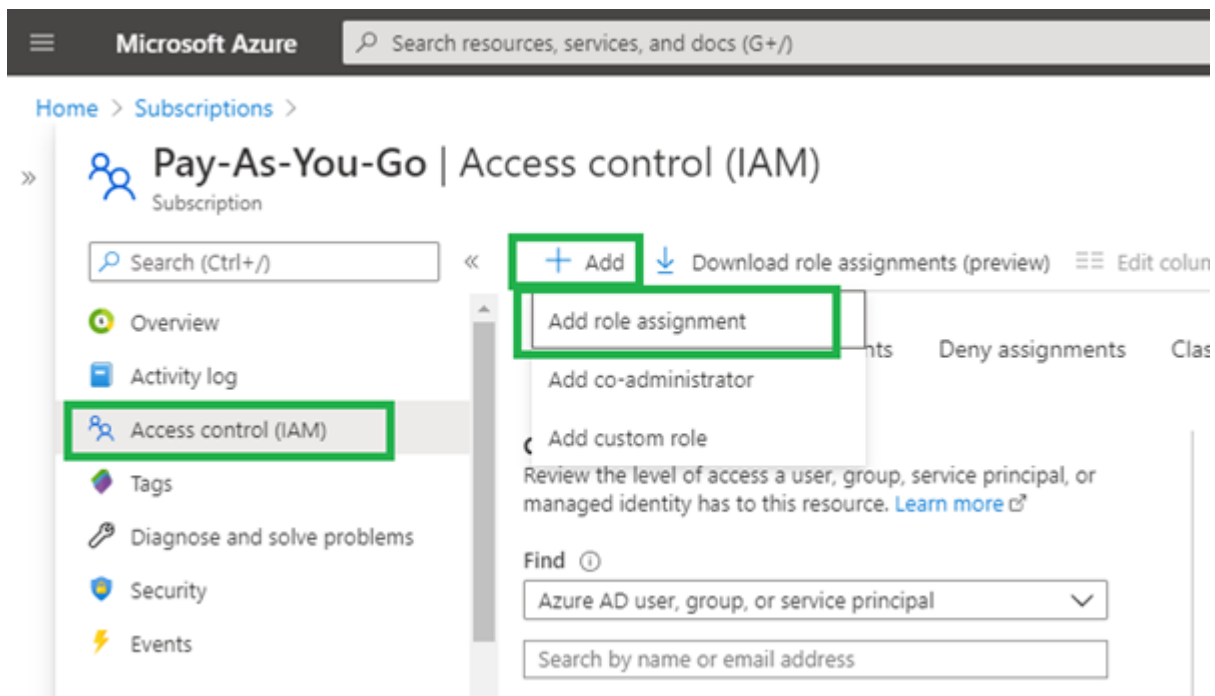
Search to filter items...

Subscription name	Subscription ID	My role
 Pay-As-You-Go	99f0ac	Owner

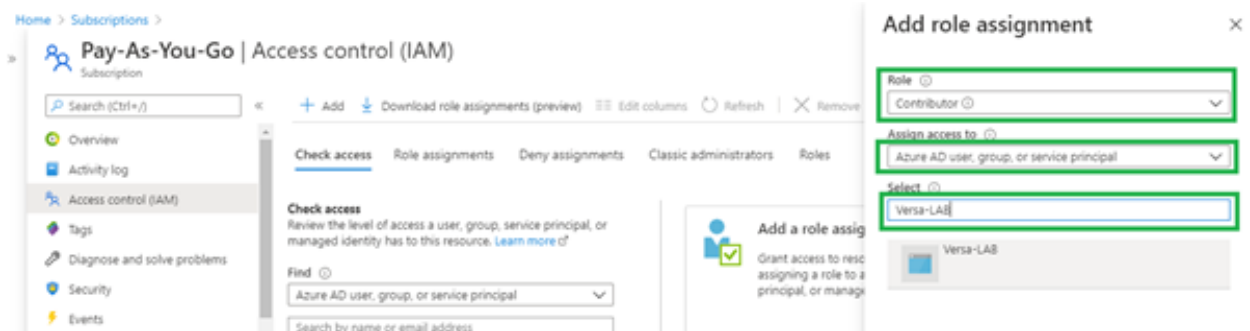
4. Select Overview in the left menu bar, and then copy the subscription ID.



5. Select Access Control (IAM), and then click the Add icon and select Add Role Assignment.



6. In the Add Role Assignment pane, enter the following information:
 - a. In the Role drop-down, select Contributor.
 - b. In the Assign access to drop-down, select Azure AD User, Group, or Service Principal.
 - c. In the Select field, search for the registered application and select the application.
 - d. Click Save.



Add role assignment

Role ⓘ

Contributor ⓘ

Assign access to ⓘ

Azure AD user, group, or service principal

Select ⓘ

Versa-LAB

No users, groups, or service principals found.

Selected members:

 Versa-LAB [Remove](#)

Save

Discard

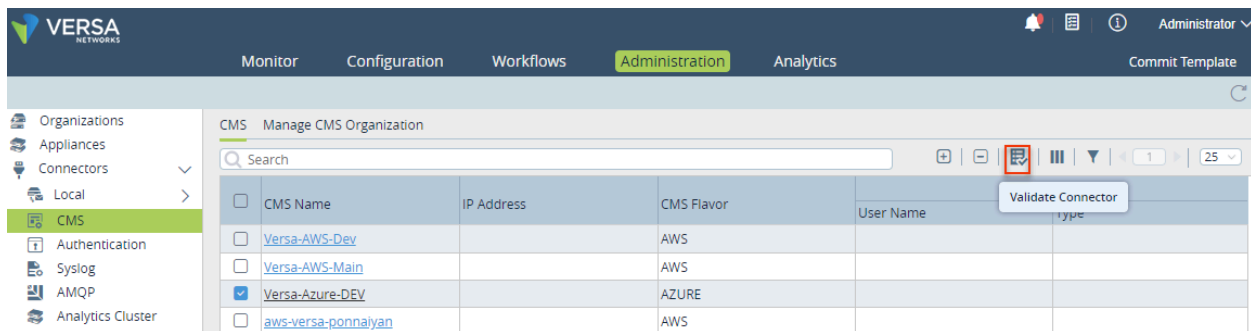
Field	Description
CMS Name	Enter the name of the CMS connector. The name is a text string.
Organization	(For Releases 21.1.1 and later.) Select the organization
CMS Flavor	Select Azure.
Environment	Select the environment. For more information, see Create an Azure AD Application , above.
Subscription ID	Enter the Azure subscription ID. For more information, see Create an Azure AD Application , above.
Client	Enter the Azure application ID. For more information, see Create an Azure AD Application , above.
Tenant ID	Enter the Azure directory ID. For more information, see Create an Azure AD Application , above.
Key	Enter the Azure authentication key. For more information, see Create an Azure AD Application , above.

5. Click OK.

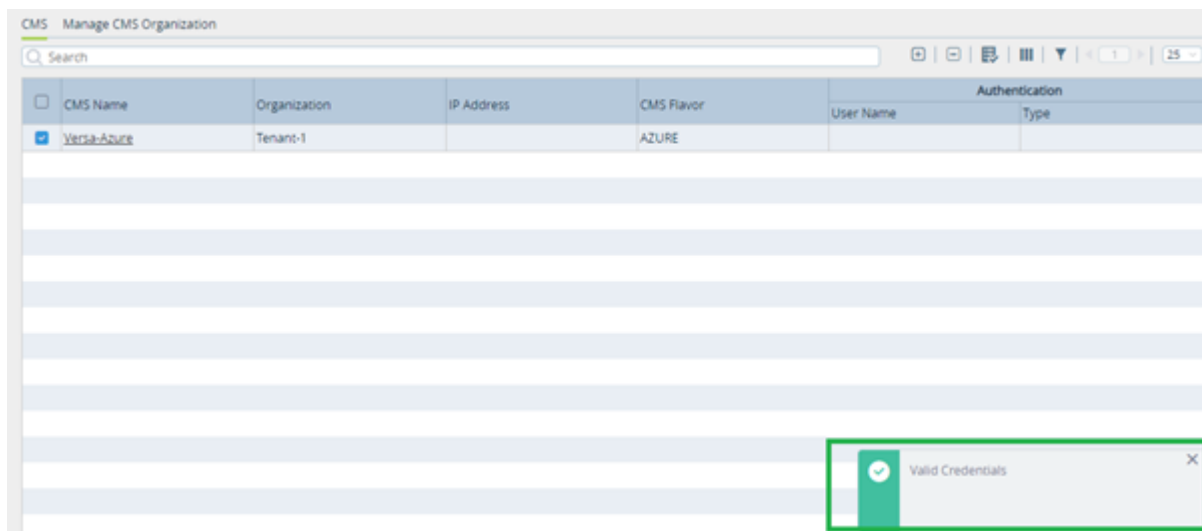
To test that the CMS connector is operating properly:

1. Log in to Versa Director.
2. In the top bar, click the Administration tab.
3. In the left navigation bar, select Connectors > CMS.
4. In the right pane, select the name of the CMS connector.

- Click the  Validate Connector icon.



- For valid credentials, the message "Valid Credentials" displays at the bottom of the pane.



Associate a CMS Connector with an Organization

After you have added a CMS connector, you associate it with an organization that you have already configured on the Versa Director. You can do this in one of two ways.

Method 1:

- Log in to Versa Director.
- Select the Administration tab in the top menu bar.
- Select Organizations in the left menu bar. The main pane displays the organizations.

The screenshot shows the Versa Networks Administration console. The left sidebar contains a navigation menu with items like Organizations, Appliances, Connectors, System, Notification Config, Entitlement Manager, Director User Mana, Inventory, and SDWAN. The main area displays a table of organizations. The table has columns for Organization Name, Parent Organization, CMS Connectors, CMS Organizations, Subscription Profile, and Global Organization ID. The table lists five organizations: Citi-Bank, CMPL, Coke, NOV, and Tesla.

Organization Name	Parent Organization	CMS Connectors	CMS Organizations	Subscription Profile	Global Organization ID
<input type="checkbox"/> Citi-Bank	Coke	Versa-AWS-Dev	-	Default-All-Services-Plan	3
<input type="checkbox"/> CMPL	Coke	Versa-AWS-Dev	-	Default-All-Services-Plan	5
<input type="checkbox"/> Coke	Tesla	Versa-AWS-Dev aws-versa-ponnaiyan	-	Default-All-Services-Plan	2
<input type="checkbox"/> NOV	Coke	Versa-Azure-DEV aws-versa-ponnaiyan	-	Default-All-Services-Plan	4
<input type="checkbox"/> Tesla	none	aws-versa-ponnaiyan	-	Default-All-Services-Plan	1

4. Select the organization you want to associate with the connector. In the Edit Organization window, enter the following information:
 - a. Select the CMS Connectors tab.
 - b. In the Available pane, click the Azure connector.
 - c. Click the > icon to add the connector to the Selected pane.
 - d. Click OK.

The screenshot shows the 'Edit Organization' window. The 'Name' field is set to 'NOV'. The 'Global Organization ID' is '4'. The 'Parent Organization' is 'Coke'. The 'Authentication Connector' is set to '--Select--'. The 'Subscription Profile' is 'Default-All-Services-Plan'. The 'CMS Connectors' tab is selected. The 'Available' pane shows 'Versa-Azure-DEV' highlighted with a red box. The 'Selected' pane shows 'Versa-AWS-Dev' and 'aws-versa-ponnaiyan'.

Method 2:

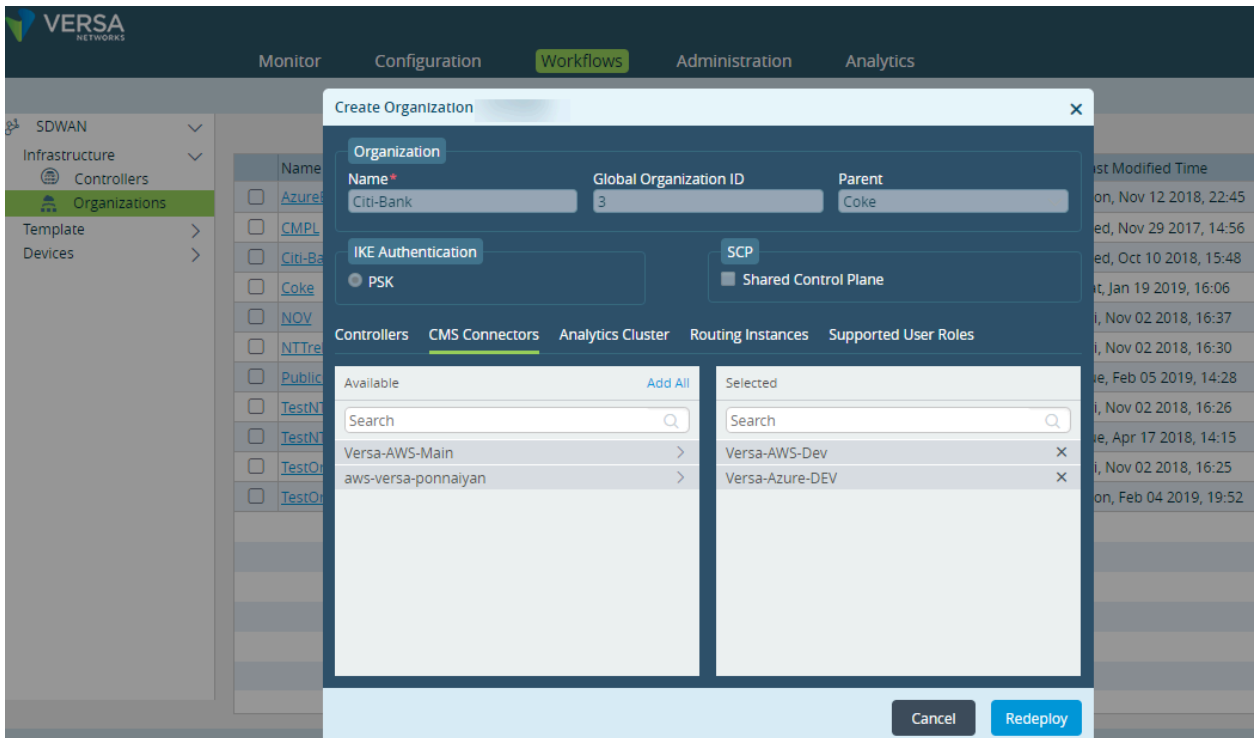
1. Log in to Versa Director.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:16:50 GMT

Copyright © 2024, Versa Networks, Inc.

2. Select the Workflows tab in the top menu bar.
3. Select Infrastructure > Organizations in the left menu bar. The Organizations table displays.
4. Select the organization you want to associate with the connector. In the Create Organization window, enter the following information:
 - a. Select the CMS Connectors tab.
 - b. In the Available pane, click the Azure connector to add it to the Selected pane.
 - c. Click Redeploy.



Make Azure VM Interface Addresses Persistent

The first time you onboard a VOS device in Azure, ensure that the MAC address is not changed on the VOS device.

To verify the MAC address of VOS device in Azure, click Virtual Machine > VM > Networking > Network Interface > Properties. For example:



To verify the MAC address of VOS device, issue the **show interfaces brief** CLI command. For example:

```
admin@VOS-cli> show interfaces brief
```

NAME	MAC	OPER	ADMIN	TENANT	VRF	IP
eth-0/0	52:54:00:39:fa:85	up	up	0	global	10.192.111.240/16 fe80::5054:ff:fe39:fa85/64
eth-0/1		down	up	0	global	
ptvi1039	n/a	up	up	2	Director-QA-Control-VR	11.1.0.6/32
ptvi1042	n/a	up	up	3	Director-QA-Tenant-1-Control-VR	11.1.0.6/32
ptvi527	n/a	up	up	2	Director-QA-Control-VR	11.1.0.2/32
ptvi530	n/a	up	up	3	Director-QA-Tenant-1-Control-VR	11.1.0.2/32
tvi-0/30	n/a	up	up	-	-	
tvi-0/30.0	n/a	up	up	2	Director-QA-Control-VR	11.1.0.253/32
tvi-0/31	n/a	up	up	-	-	
tvi-0/31.0	n/a	up	up	2	Director-QA-Control-VR	11.1.0.252/32
tvi-0/36	n/a	up	up	-	-	
tvi-0/36.0	n/a	up	up	3	Director-QA-Tenant-1-Control-VR	11.1.0.253/32
tvi-0/37	n/a	up	up	-	-	
tvi-0/37.0	n/a	up	up	3	Director-QA-Tenant-1-Control-VR	11.1.0.252/32
tvi-0/5602	n/a	up	up	-	-	
tvi-0/5602.0	n/a	pdown	up	3	Director-QA-Tenant-1-LAN-VR	169.254.19.138/31
tvi-0/5604	n/a	up	up	-	-	
tvi-0/5604.0	n/a	pdown	up	3	Director-QA-Tenant-1-LAN-VR	169.254.19.140/31
vni-0/0	52:54:00:95:53:f6	up	up	-	-	
vni-0/0.0	52:54:00:95:53:f6	up	up	2	WAN-Network-Transport-VR	75.75.75.222/24
vni-0/1	52:54:00:cb:10:cb	up	up	-	-	
vni-0/1.100	52:54:00:cb:10:cb	up	up	3	Director-QA-Tenant-1-LAN-VR	85.85.85.101/24
vni-0/1.2	52:54:00:cb:10:cb	up	up	3	Director-QA-Tenant-1-LAN-VR	85.85.85.3/24
vni-0/1.1	52:54:00:cb:10:cb	up	up	3	Director-QA-Tenant-1-LAN-VR	85.85.85.2/24
vni-0/1.0	52:54:00:cb:10:cb	up	up	3	Director-QA-Tenant-1-LAN-VR	85.85.85.1/24

If the MAC address has not changed on the VOS device, issue the following command to make the Azure VM interface

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:16:50 GMT

Copyright © 2024, Versa Networks, Inc.

addresses permanent:

```
| sudo touch /etc/cloud/cloud-init.disabled
```

If the MAC address has changed on the VOS device, do the following to make the Azure VM interface addresses permanent:

1. Log in to the VOS device.
2. Create the cloud-init.disabled file.

```
| sudo touch /etc/cloud/cloud-init.disabled
```

3. Delete the vinterfaces file.

```
| sudo rm -rf /var/run/vinterfaces
```

4. Check whether the **/etc/udev/rules.d/70-persistent-net.rules** file exists. In this file, verify that the mapping of MAC addresses to the eth interfaces has been updated. If there is a mismatch between the MAC address and eth interface naming, correct the mapping in the file.
5. Shut down the VM from Azure portal.
6. Restart the VM from Azure portal.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.1.1 adds the Organization field in the CMS Connector window.
- Release 22.1.1 adds support for Azure accelerated networking.

Additional Information

[Branch Hardware and Software Requirements](#)

[Branch Overview](#)

[Configure Basic Features](#)

[Configure VRRP](#)

[Initial Branch Software Configuration](#)

[Install Headend Components on Azure](#)

[Install on Azure without CMS](#)

[Qualified AWS and Azure Instances](#)