
How to Create a Service Principal for Azure Virtual WAN

<https://campus.barracuda.com/doc/89621222/>

For the firewall to authenticate to the Azure Virtual WAN APIs that enable automated connectivity, a registered app must be created. The registered app requires the following information:

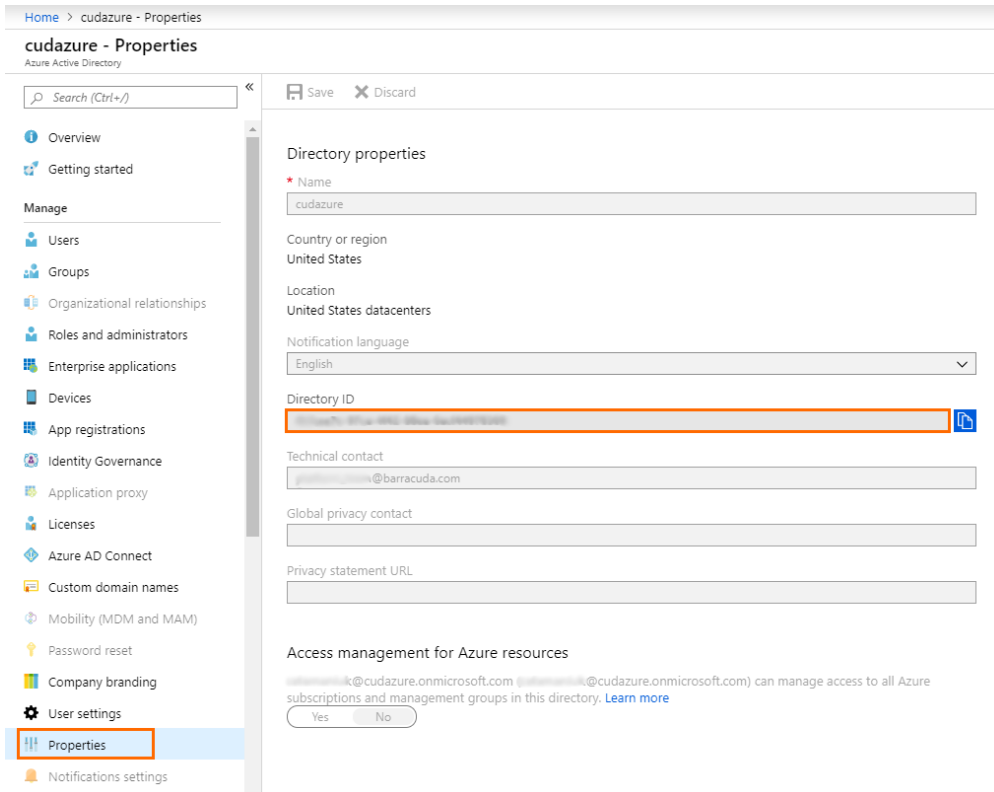
- Tenant ID
- Subscription ID
- User ID / Application ID / Client ID
- Key / Client Password

Before You Begin

- Create a resource group in Microsoft Azure. This resource group must contain your virtual WAN later. Otherwise, the firewall will not have sufficient permissions to authenticate to Azure Virtual WAN APIs that enable automated connectivity.

Step 1. Get the Tenant ID

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Azure Active Directory**.
3. Click **Azure Active Directory**.
4. In the left menu of the **Azure Active Directory** blade, click **Properties**.
5. Copy the **Directory ID**. This is the tenant ID of your service principal.

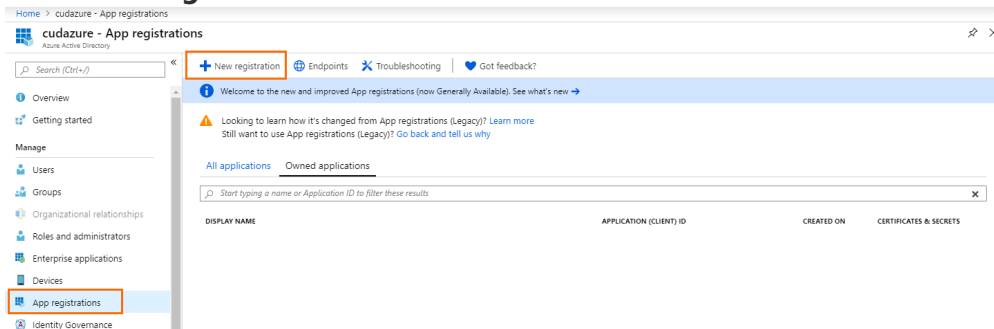


The screenshot shows the 'cudazure - Properties' page in the Azure portal. The left-hand navigation pane is visible, with 'Properties' highlighted. The main content area shows the following fields:

- Directory properties**
 - Name: cudazure
 - Country or region: United States
 - Location: United States datacenters
 - Notification language: English
 - Directory ID: [Redacted]
 - Technical contact: [Redacted]@barracuda.com
 - Global privacy contact: [Redacted]
 - Privacy statement URL: [Redacted]
- Access management for Azure resources**
 - Text: [Redacted]@cudazure.onmicrosoft.com ([Redacted]@cudazure.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)
 - Buttons: Yes, No

Step 2. Create New App Registration

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Azure Active Directory**.
3. Click **Azure Active Directory**.
4. In the left menu of the **Azure Active Directory** blade, click **App registrations**.
5. Click **New registration**.



The screenshot shows the 'cudazure - App registrations' page. The left-hand navigation pane has 'App registrations' highlighted. The main content area shows a '+ New registration' button highlighted in orange. Below it, there is a welcome message and a table with columns: DISPLAY NAME, APPLICATION (CLIENT) ID, CREATED ON, and CERTIFICATES & SECRETS.

6. The **Register an application** blade opens.
 - o **Name** - Enter a name for the application registration.
 - o **Supported account types** - Select **Accounts in this organizational directory only (<your_directory_name> only - Single tenant)**.
 - o **Redirect URI (optional)** - Select **Web** from the drop-down menu, and enter a random, unique URI. E.g., <https://localhost:432>

Home > cudazure - App registrations > Register an application

Register an application

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

doc-vwan-sp ✓

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (cudazure 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 | https://localhost:432 ✓

7. Click **Register**.

Copy the **Application (client) ID**: This is the **user ID** for your service principal information.

Home > cudazure - App registrations > doc-vwan-sp

doc-vwan-sp

Search (Ctrl+V) | Delete | Endpoints

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

Display name	doc-vwan-sp	Supported account types	My organization only
Application (client) ID	81c3c70d-9b11-4000-8000-000000000000	Redirect URIs	1 web, 0 public client
Directory (tenant) ID	72f988bf-86f1-41af-91ab-2d7cd011db47	Application ID URI	Add an Application ID URI
Object ID	72f988bf-86f1-41af-91ab-2d7cd011db47	Managed application in ...	doc-vwan-sp

Step 3. Create the Service Principal Key

For the app registration, create a service principal key to authenticate.

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Azure Active Directory**.
3. Click **Azure Active Directory**.
4. In the left menu of the **Azure Active Directory** blade, click **App registrations**.
5. Click on the registered app created in Step 2. The **Registered app** blade opens.
6. Click **Certificates & secrets**. The **Certificates & secrets** blade opens.
7. In the **Client secrets** section, click **New client secret**.

Home > azure - App registrations > doc-vwan-sp - Certificates & secrets

doc-vwan-sp - Certificates & secrets

Search (Ctrl+/)

Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.
[Upload certificate](#)
No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES
No certificates have been added for this application.		

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
[New client secret](#)


DESCRIPTION	EXPIRES	VALUE
No client secrets have been created for this application.		

8. The **Add a client secret** blade opens.
 - o **Description** – Enter a name for the service principal key.
 - o **Expires** – Select **Never expires**.
9. Click **Add**.
10. The key is now displayed in the **Value** column. Click on the copy icon to copy the key to your clipboard.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[New client secret](#)

DESCRIPTION	EXPIRES	VALUE
Service_Principal_key_doc	9/2/2020	

Note that you must copy the key before reloading the page because it is no longer displayed afterwards.

Step 4. Assign the Appropriate Roles to the Registered App

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Resource groups**.
3. Click **Resource groups**.
4. Select the resource group that will contain your virtual WAN later.
5. Click **Access control (IAM)**

All services > Resource groups > RG-Campus-VWAN

RG-Campus-VWAN
Resource group

Search (Ctrl+/)

+ Add Edit columns Delete resource group Refresh Move Export to CSV As

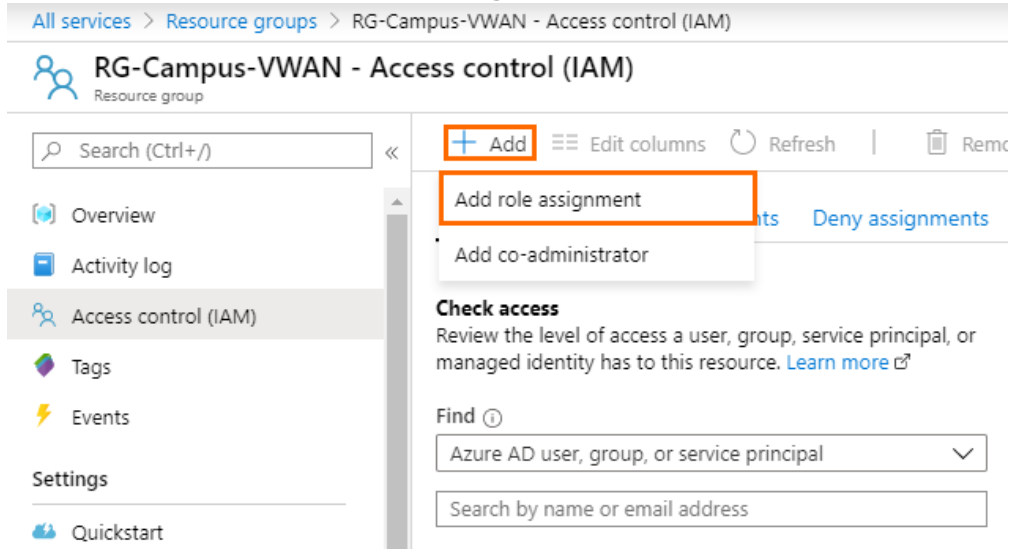
Subscription (change): Sandbox Deployments
Subscription ID : 25ebdaeb-a9a8-4b24-9164-1879a0661ae9
Tags (change) : [Click here to add tags](#)

Filter by name... Type == all Location == all Add filter

Showing 1 to 1 of 1 records. Show hidden types

Name	Type
Campus-VWAN	Virtual WAN

6. Click **+Add** and select **Add role assignment** from the list.



The screenshot shows the Azure portal interface for the 'RG-Campus-VWAN - Access control (IAM)' resource group. The breadcrumb trail is 'All services > Resource groups > RG-Campus-VWAN - Access control (IAM)'. The left-hand navigation pane includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Events', 'Settings', and 'Quickstart'. The main content area features a search bar and a '+ Add' button. A dropdown menu is open from the '+ Add' button, with 'Add role assignment' highlighted. Other options in the menu include 'Add co-administrator'. Below the menu, there is a 'Check access' section with a description and a 'Find' section with a search box containing the text 'Azure AD user, group, or service principal' and a 'Search by name or email address' input field.


7. For **Role**, select **Storage Blob Data Owner** from the list.
8. For **Assign access to**, select **Azure AD user, group, or service principal**.
9. For **Select** enter the name of the registered app created in Step 2 (doc-vwan-sp) and click on the corresponding entry of the list.


Add role assignment ✕

Role ⓘ
Storage Blob Data Owner


Assign access to ⓘ
Azure AD user, group, or service principal

Select ⓘ
doc- Ⓟ ✓

 ██████████

 ██████████

Selected members:

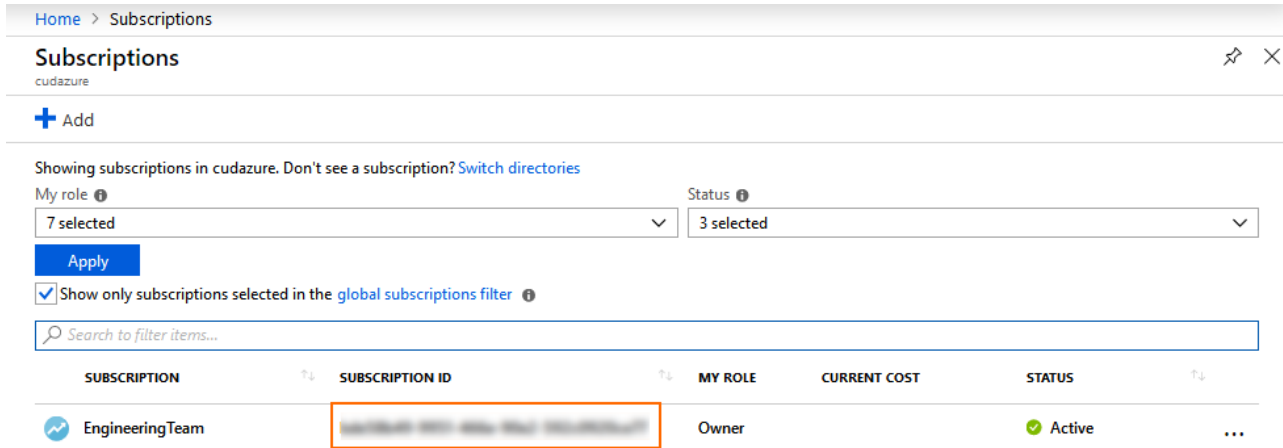
 doc-vwan-sp	Remove
---	------------------------

[Save](#) [Discard](#)

10. Click **Save** to save your configuration.
11. Repeat Step 4 and add the following roles:
 1. **Network Contributor.**
 2. **Storage Account Key Operator Service Role.**
 3. **Storage Account Contributor.**
12. Continue with Step 5 .

Step 5. Get the Subscription ID

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **Subscriptions**.
3. Copy the **Subscription ID** in the **Subscription ID** column.



Home > Subscriptions

Subscriptions

Subscriptions in cudazure

+ Add

Showing subscriptions in cudazure. Don't see a subscription? [Switch directories](#)

My role **7 selected** Status **3 selected**

Apply

Show only subscriptions selected in the [global subscriptions filter](#)

Search to filter items...

SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
EngineeringTeam	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	Owner		Active

Next Steps

You can now configure automated connectivity for Azure Virtual WAN.

For more information, see [How to Configure Automatic Connectivity to Azure Virtual WAN](#).

Figures

1. directory_properties.png
2. app_registrations.png
3. register_an_app.png
4. app_id.png
5. certificate_and_secrets.png
6. key.png
7. rg_IAM.png
8. rg_iam_add1.png
9. service_principal_role_assignment_assign_role_to_service_principal_and_save.png
10. vwan_sp_06.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.