



# Configure an Always-On VPN device tunnel using Azure VPN on Windows 10

This document provides a step-by-step guide on how to Configure an Always-On VPN device tunnel using Azure VPN on Windows 10.

## Prerequisite:

1. Configure the point-to-site VPN tunnel using this article <https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-certificate-gateway>
2. The device must be a domain joined computer running Windows 10 Enterprise or Education version 1809 or later.
3. Only one device tunnel can be configured per device.
4. Allow Port 4500,500 (IKEv2) and 443 (SSTP- if using) outbound Rules.

## Steps to be followed:

### Install client certificates on the Windows 10 or later client

#### Certificate:

1. Copy the client certificate file into the VPN client device and click to install PFX to install the certificate.
2. Select Store Location as Current User and click on next.  
**Note: After the certificate has been installed with the current user, again install the certificate with the store location as Local Machine.**
3. Click on **Next**
4. Enter the password for the private key
5. Click on **Next**
6. The certificate has been installed.

### Setting up the DNS for Ethernet

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("10.0.0.4","168.63.129.16")

### Install the Azure Point-To-Site VPN on the VPN client device:

1. Install the VpnClientAmd64.exe package on the client device
2. Open VPN settings and connect the VPN
3. Click on Connect in the Azure VPN and continue to establish the connection

### Setting up the DNS for VPNProfile of VNG

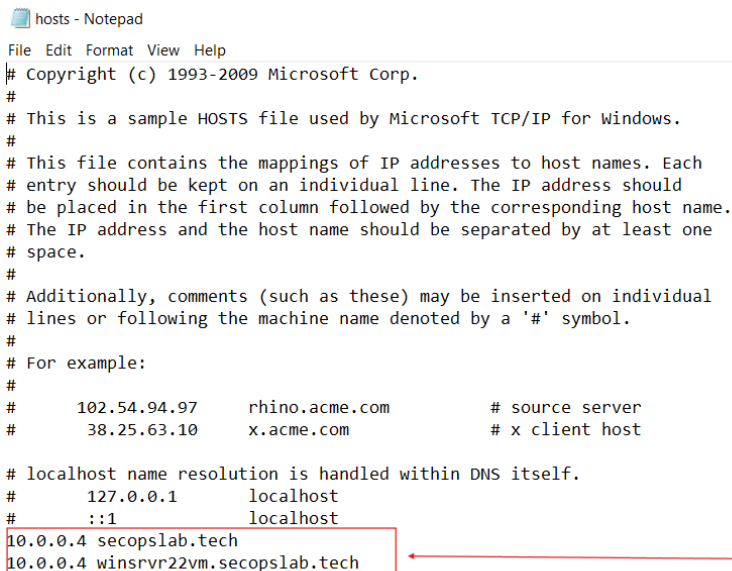
Set-DnsClientServerAddress -InterfaceAlias "aovpn-vnet" -ServerAddresses 10.0.0.4



## Steps to domain join the VPN client device

Do the Entry of the Private IP and Host name of the AD under the Host file Navigating the below path

C:\Windows\System32\drivers\etc\hosts



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com           # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
10.0.0.4 secopslab.tech
10.0.0.4 winsrvr22vm.secopslab.tech
```

1. Select **Advanced system settings** in the Properties of **This PC**
2. Click on Rename this PC (Advanced) and enter the domain name and the logins.
3. The Device will be Domain Joined it will Prompt for a Restart click ok and Select Restart Later.

## Configurations for Device tunnel

We have completed pre-requisites before, now we will setup Always-On Device Tunnel.

1. Copy the following text and save it as devicecert.ps1 provided under below reference link  
<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-always-on-device-tunnel>
2. Copy the following text and save it as **VPNProfile.xml** in the same folder as **devicecert.ps1** provided in below reference link.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-always-on-device-tunnel>

## Replace the following text to match your environment under VPNProfile.xml

<Servers>azuregateway-1234-56-78dc.cloudapp.net</Servers> <= Can be found in the VpnSettings.xml in the downloaded profile zip file

<Address>192.168.3.5</Address> <= IP of resource in the vnet or the vnet address space



<Address>192.168.3.4</Address> <= IP of resource in the vnet or the vnet address space

3. Download PsExec (PS Tools) from the below link and extract the files to C:\PSTools.

<https://learn.microsoft.com/en-us/sysinternals/downloads/psexec>

4. Open Command Prompt, change the path where the PS Tools file is present, and execute the below command:

For 32-bit Windows: **PsExec.exe -s -i powershell**

For 64-bit Windows: **PsExec64.exe -s -i powershell**

```
Administrator: Command Prompt - PsExec64.exe Powershell

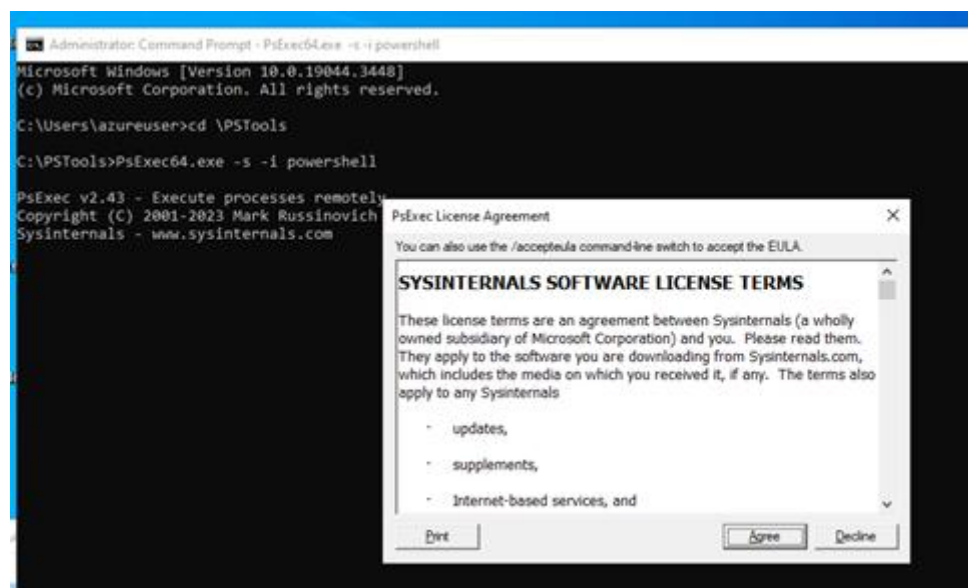
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \PSTools

C:\PSTools>PsExec64.exe Powershell

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

After clicking on the Agree, PowerShell will appear.





In PowerShell, switch to the folder where devicecert.ps1 and VPNProfile.xml are located, and run the following command:

**.\devicecert.ps1 .\VPNProfile.xml MachineCertTest**

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Windows\system32> cd "C:\Users\azureuser\Desktop\New folder"
PS C:\Users\azureuser\Desktop\New folder> ls

Directory: C:\Users\azureuser\Desktop\New folder

Mode                LastWriteTime         Length Name
----                -
-a----          9/27/2023   6:02 PM             1433 devicecert.ps1
-a----          9/27/2023   6:32 PM             1058 VPNProfile.xml

PS C:\Users\azureuser\Desktop\New folder> .\devicecert.ps1 .\VPNProfile.xml MachineCertTest
True

AlwaysOn                :
ByPassForLocal           :
DeviceTunnel             :
DnsSuffix                :
EdpModeId               :
InstanceID               : MachineCertTest
LockDown                :
ParentID                 : ./Vendor/MSFT/VPNv2
ProfileXML               :
RegisterDNS              :
RememberCredentials      :
TrustedNetworkDetection  :
PSComputerName           :

Created MachineCertTest profile.
Complete.

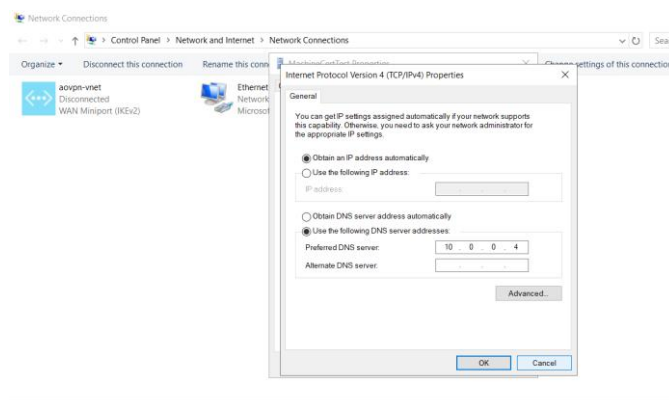
PS C:\Users\azureuser\Desktop\New folder> _
```

**Note:** If facing any issue with policies then Run the below command:

Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Force

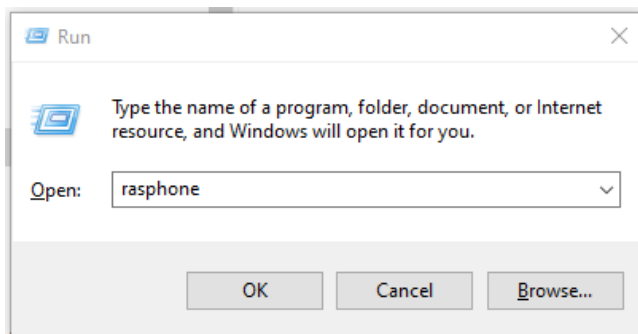
### Setting up the DNS for MachineCertTest

Set-DnsClientServerAddress -InterfaceAlias "MachineCertTest" -ServerAddresses 10.0.0.4

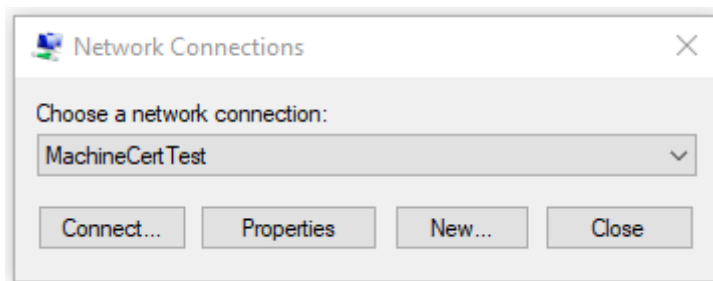




Now to test the connection, open Run and type **rasphone** and hit enter



Look for the **MachineCertTest** connection entry and click **Connect** (If you see Hang-up option instead of Connect then you are already connected)



Remove the earlier created P2S Connection to join the Client Machine to the Domain.