Setting up Point-to-Site (P2S) VPN in Azure

Objective:

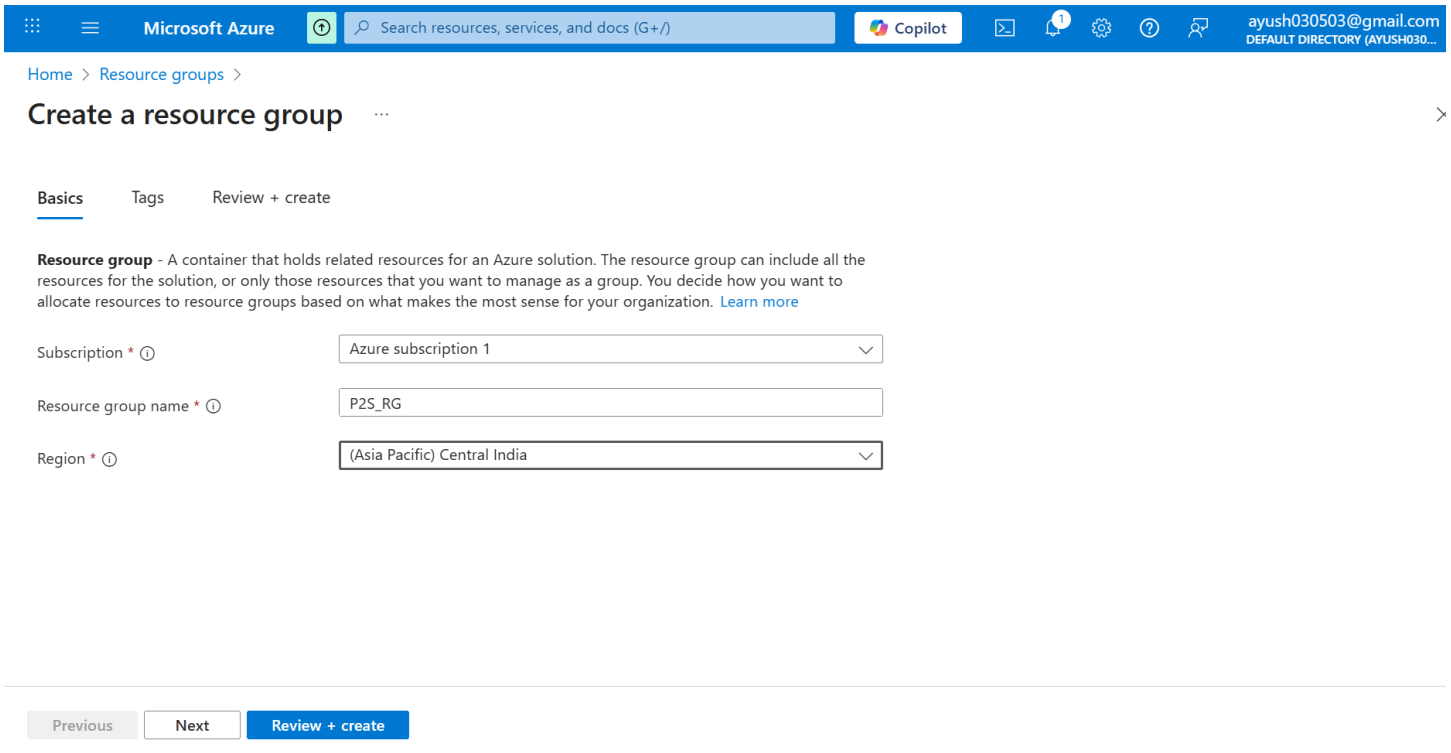
To enable secure remote access to an Azure Virtual Network (VNet) from individual machines (like laptops/desktops) using a Point-to-Site (P2S) VPN. This is especially useful for administrators or developers working from outside Azure.

1. Create a Resource Group

A resource group acts as a container for all the Azure resources you'll create.

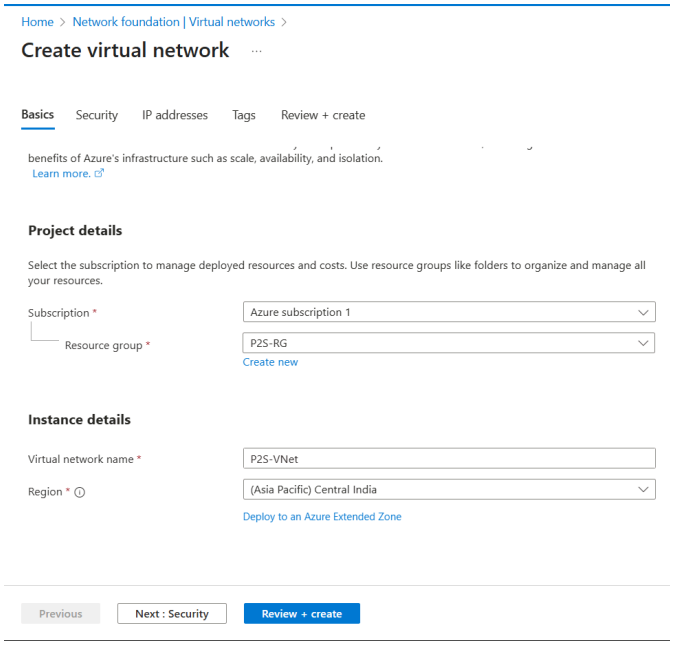
Steps:

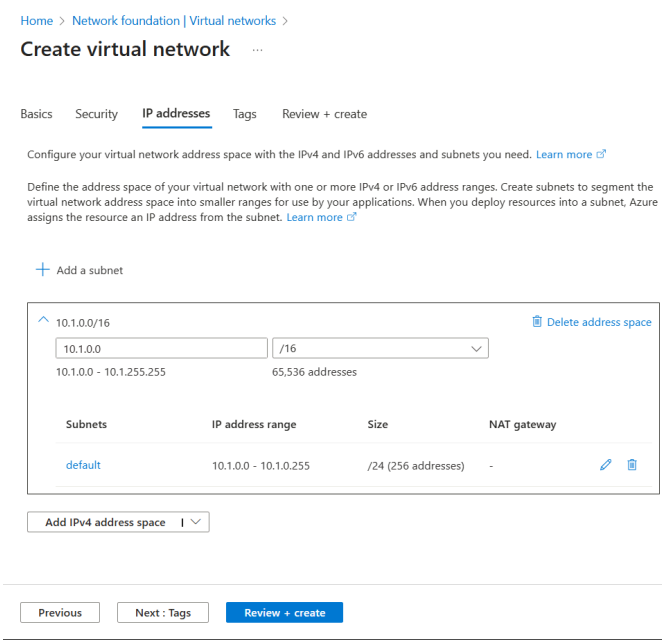
- Go to Azure Portal.
- Search for **Resource groups** and click **+ Create**.
- Enter:
  - **Subscription**: Use your current Azure subscription.
  - **Resource group name**: `P2S-RG`
  - **Region**: Choose one close to your location (e.g., `Central India` or `East US`)
- Click **Review + Create** → **Create**.



2. Create a Virtual Network (VNet)

- Search for **Virtual networks** → **+ Create**.
- Basics tab:
  - **Subscription**: Same as before.
    Resource group: `P2S-RG`
  - **Name**: `P2S-VNet`
  - **Region**: Same region as the resource group
- IP Addresses tab:
  - **IPv4 address space**: `10.1.0.0/16`
  - **Subnet name**: `default`
  - **Subnet address range**: `10.1.0.0/24`
- Leave other settings as default.
- Click **Review + Create** → **Create**.

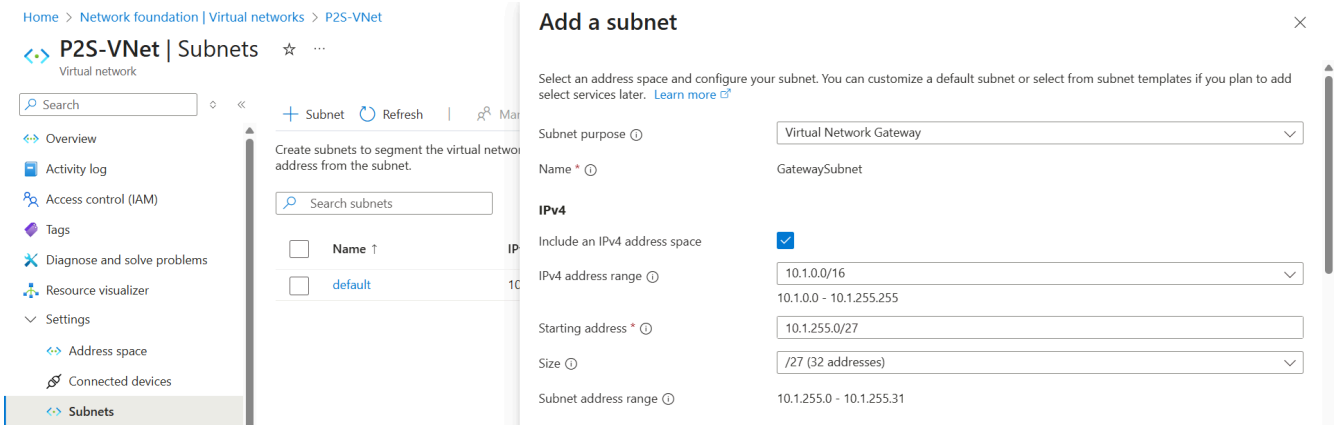




3. Add a Gateway Subnet

This is required for the VPN Gateway to function.

- Go to **P2S-VNet** > **Subnets** > **+ Gateway subnet**.
- Address range: `10.1.255.0/27` (must not overlap with other subnets)
- Click **Save**.

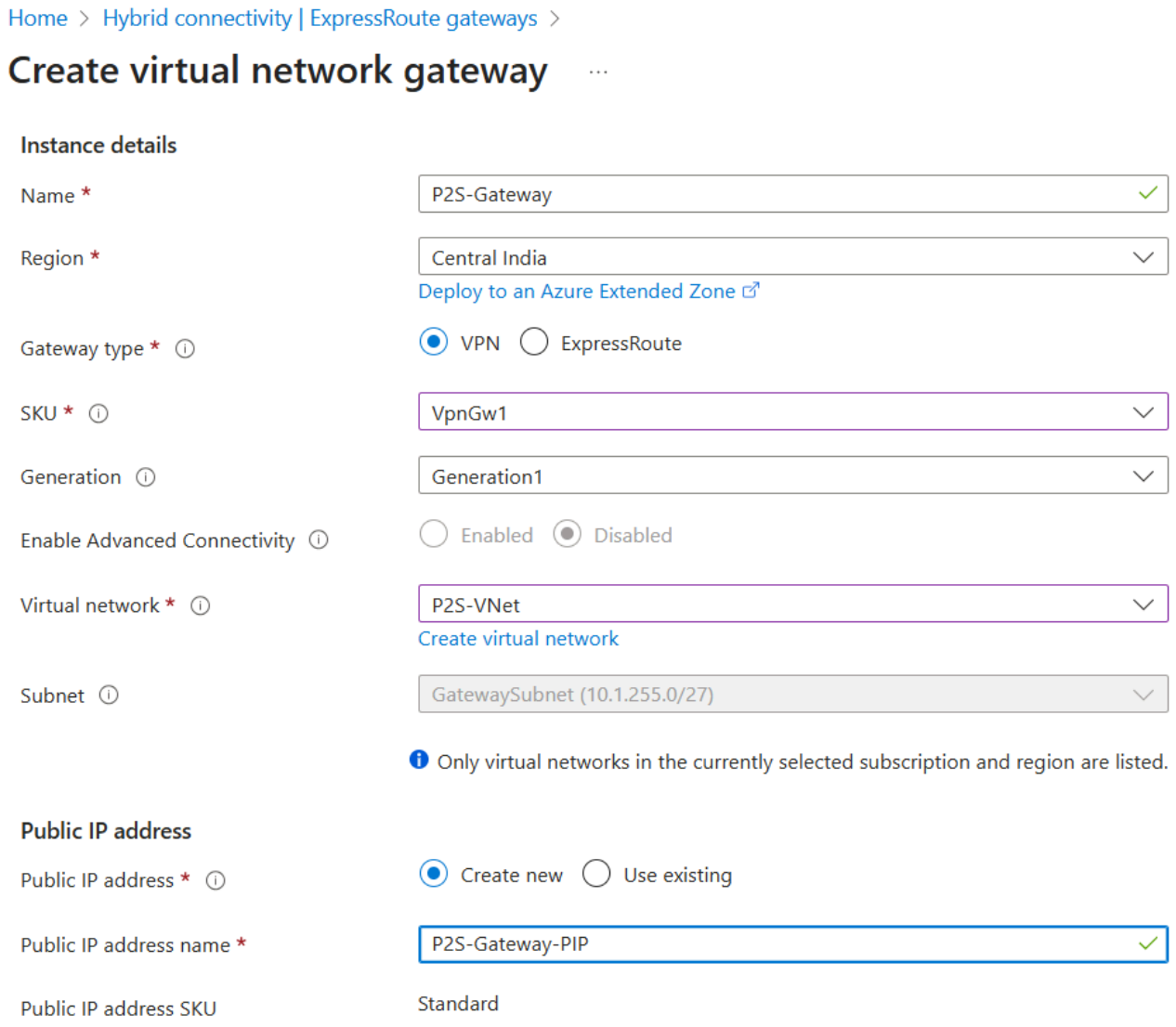


4. Create the VPN Gateway

The VPN gateway handles encrypted tunnels between Azure and your PC.

- Search **Virtual Network Gateways** > **+ Create**.
- Basics tab:
  - **Subscription**: Same
  - **Resource group**: `P2S-RG`
  - **Name**: `P2S-Gateway`
  - **Region**: Same as VNet
  - **Gateway type**: `VPN`
  - **VPN type**: `Route-based`
  - **SKU**: `VpnGw1` (Basic does not support P2S)
  - **Virtual network**: Select `P2S-VNet`
  - **Gateway subnet**: Auto-selected

- Public IP address:
  - Create new > Name: `P2S-Gateway-PIP`
- Click **Review + Create → Create**
  *Note: This step takes **30–45 minutes.***



5. Create a Self-Signed Root Certificate (on your PC)

You'll use this certificate to authenticate your client machine to Azure.

Steps (on Windows PowerShell):

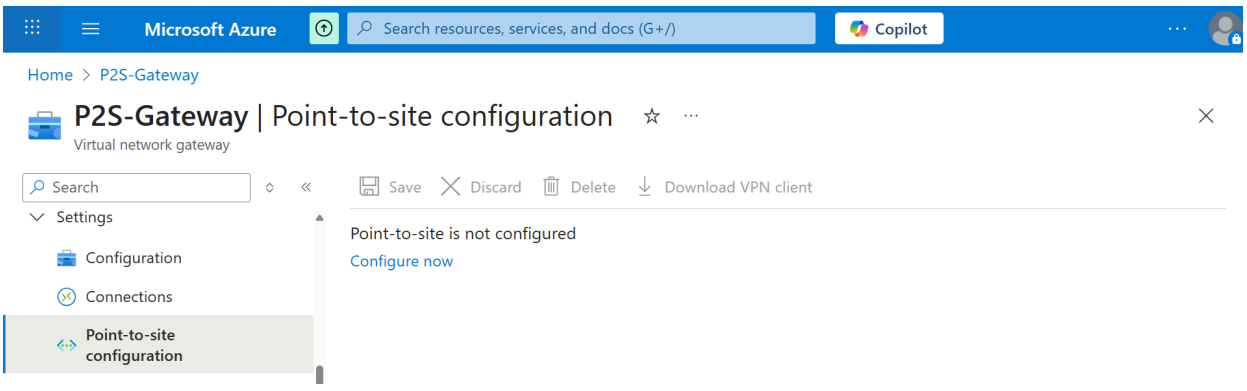
```
# Generate Root Certificate
$rootCert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

# Export Public Key (Base64)
Export-Certificate -Cert $rootCert -FilePath "<FILEPATH>\P2SRootCert.cer"
```

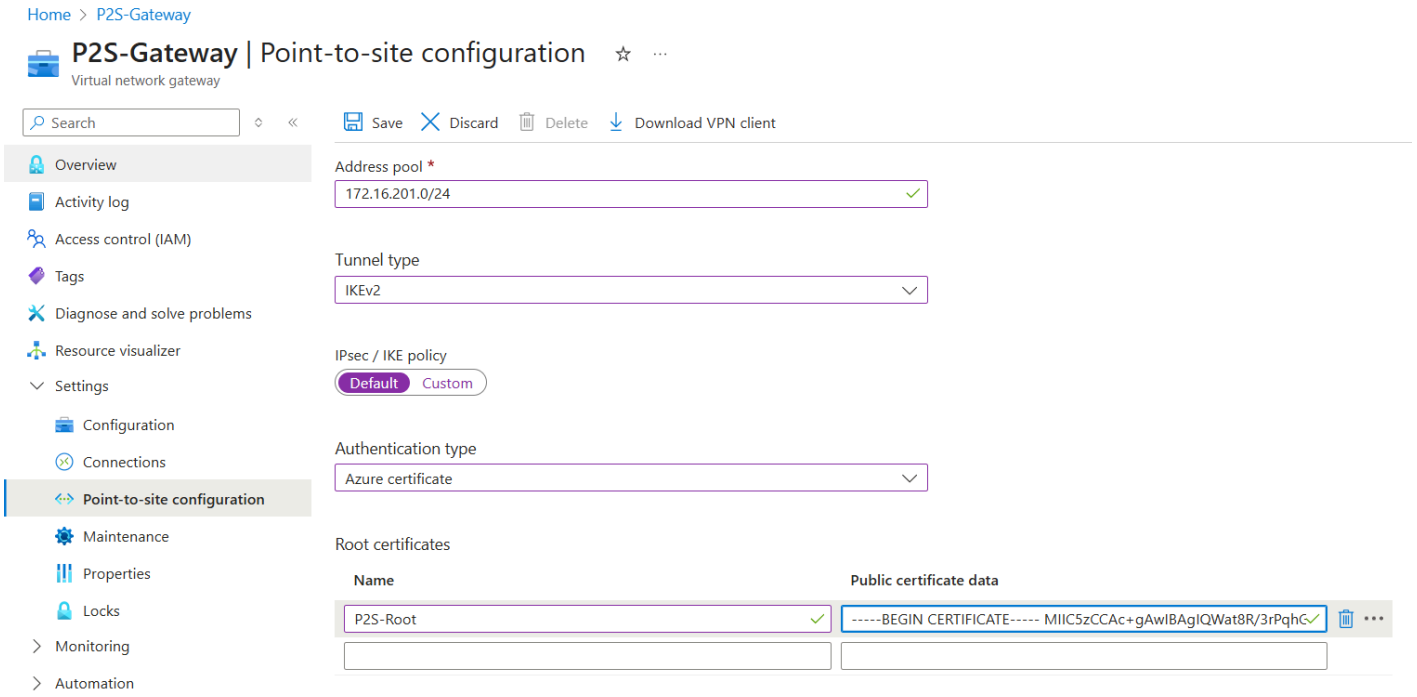
Now, open the file `P2SRootCert.cer` from your Desktop using Notepad, and copy the full **Base64-encoded text** (everything between and excluding `-----BEGIN CERTIFICATE-----` & `-----END CERTIFICATE-----`).

```
PS C:\WINDOWS\system32> $rootCert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\WINDOWS\system32> Export-Certificate -Cert $rootCert -FilePath "C:\Users\ayush\OneDrive\Desktop\P2SRootCert.cer" -Type CERT


    Directory: C:\Users\ayush\OneDrive\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        26-07-2025  03:01 PM            747 P2SRootCert.cer
```

6. Configure the Point-to-Site VPN

- Go to **P2S-Gateway** > **Point-to-site configuration** > **Configure now**.
- Input:
  - **Address pool**: `172.16.201.0/24`
  - **Tunnel type**: Select `IKEv2` and `OpenVPN` (select both if unsure)
  - **Authentication type**: Select `Azure certificate`
  - **Root certificate name**: `P2S-Root`
  - **Public certificate data**: Paste the Base64 content from `.cer` file
- Click **Save**.



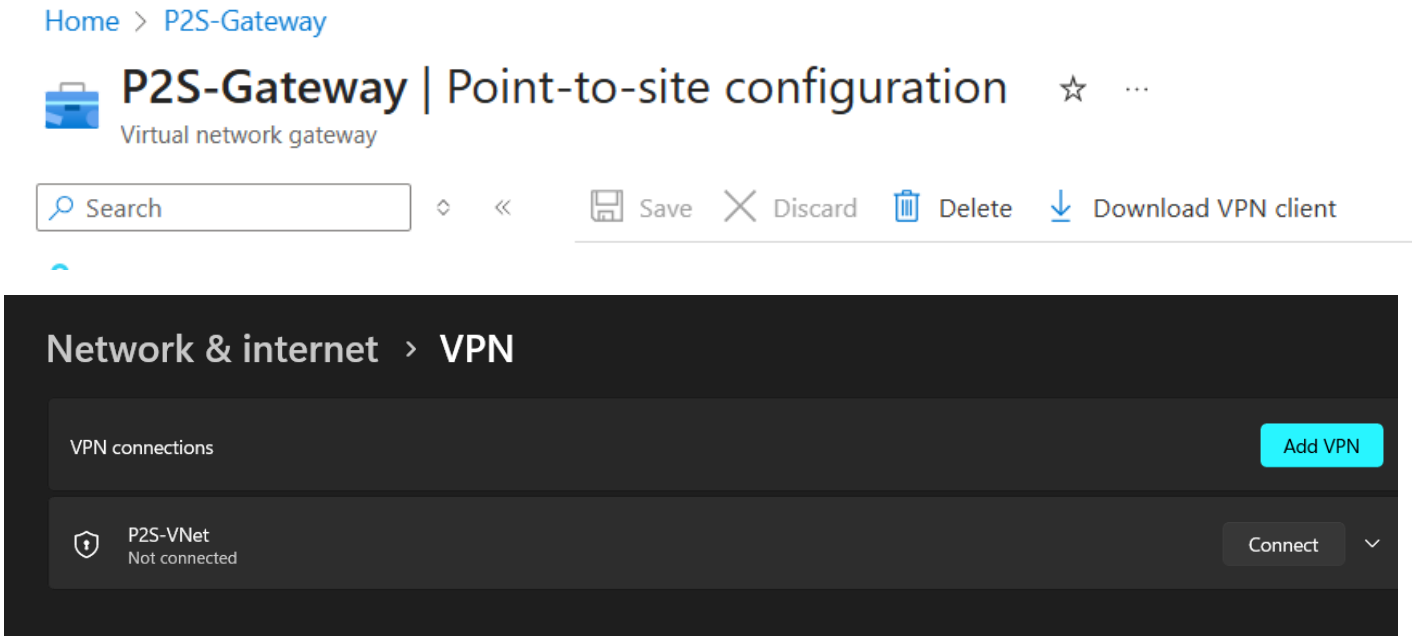


NOTE: If the certificate is in **Binary Format(DER)** , use this command to convert it to **BASE64**

```
certutil -encode "<FILEPATH>\P2SRootCert.cer" "<FILEPATH>\P2SRootCert-BASE64.cer"
```

7. Download and Install VPN Client

- Go to the Point-to-site configuration tab in the gateway.
- Click Download VPN client > Choose Windows x64 or your platform.
- Unzip the downloaded file.
- Run the appropriate installer inside the extracted folder.
- A new VPN profile will be added to your OS.



8. Connect to the VPN

- Open Settings > Network & Internet > VPN.
- You'll see a new connection named P2S-VNet or similar.
- Click Connect.
- You're now connected to Azure.

NOTE : If you get an error, "valid certificate not found", it might mean that the private certificate key for the certificate you generated is not yet installed on your machine, use the below code to generate the private certificate:-

```
# This pulls certs from the user's certificate store
Get-ChildItem -Path "Cert:\CurrentUser\My" | Select Subject

# Grab the certificate with subject CN=AzureP2SRootCert
$cert = Get-ChildItem -Path "Cert:\CurrentUser\My" | Where-Object { $_.Subject -eq
"CN=AzureP2SRootCert" }

# Export it as a PFX with a password
Export-PfxCertificate -Cert $cert `
  -FilePath "$env:USERPROFILE\Desktop\AzureP2SClientCert.pfx" `
  -Password (ConvertTo-SecureString -String "P@ssw0rd123" -Force -AsPlainText)
```