

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**.

Microsoft Azure

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

Copilot

ayush030503@gmail.com
DEFAULT DIRECTORY (AYUSH030...

Home > Resource groups >

Create a resource group

Basics

Tags

Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription * ⓘ

Azure subscription 1

Resource group name * ⓘ

P2S_RG

Region * ⓘ

(Asia Pacific) Central India

Previous

Next

Review + 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**.

Home > Network foundation | Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * P2S-RG [Create new](#)

Instance details

Virtual network name * P2S-VNet

Region * (Asia Pacific) Central India [Deploy to an Azure Extended Zone](#)

Previous Next: Security Review + create

Home > Network foundation | Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

+ Add a subnet

10.1.0.0/16 [Delete address space](#)

10.1.0.0 /16 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	10.1.0.0 - 10.1.0.255	/24 (256 addresses)	-

Add IPv4 address space

Previous Next: Tags Review + 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**.

Home > Network foundation | Virtual networks > P2S-VNet

P2S-VNet | Subnets

Virtual network

Search

+ Subnet Refresh

Create subnets to segment the virtual network address from the subnet.

Search subnets

Name	IP
default	10.1.0.0/24

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose Virtual Network Gateway

Name GatewaySubnet

IPv4

Include an IPv4 address space ☒

IPv4 address range 10.1.0.0/16 10.1.0.0 - 10.1.255.255

Starting address 10.1.255.0/27

Size /27 (32 addresses)

Subnet address range 10.1.255.0 - 10.1.255.31

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.

[Home](#) > [Hybrid connectivity | ExpressRoute gateways](#) >

Create virtual network gateway ...

Instance details

Name *	<input type="text" value="P2S-Gateway"/>
Region *	<input type="text" value="Central India"/> Deploy to an Azure Extended Zone
Gateway type *	<input checked="" type="radio"/> VPN <input type="radio"/> ExpressRoute
SKU *	<input type="text" value="VpnGw1"/>
Generation	<input type="text" value="Generation1"/>
Enable Advanced Connectivity	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Virtual network *	<input type="text" value="P2S-VNet"/> Create virtual network
Subnet	<input type="text" value="GatewaySubnet (10.1.255.0/27)"/>

i Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address *	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing
Public IP address name *	<input type="text" value="P2S-Gateway-PIP"/>
Public IP address SKU	Standard

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-----**).

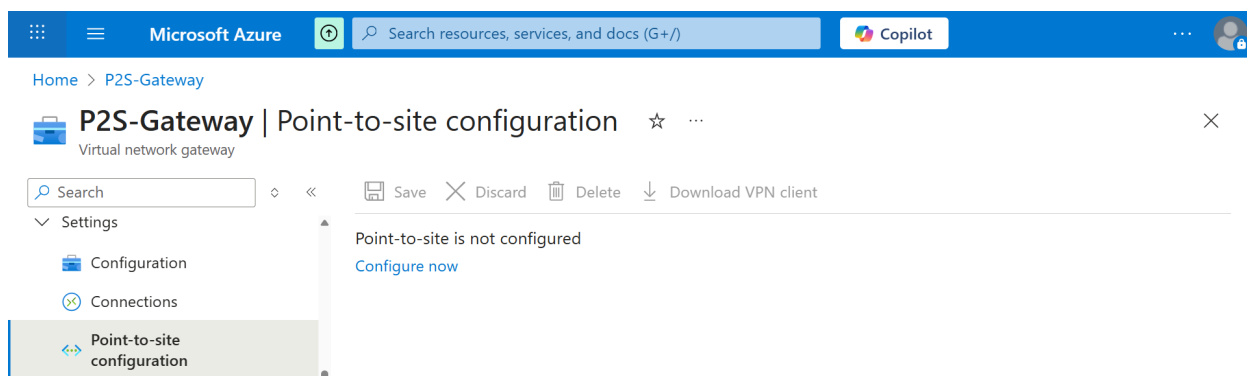
```
PS C:\WINDOWS\system32> $rootCert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\WINDOWS\system32> 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**.



Home > P2S-Gateway

P2S-Gateway | Point-to-site configuration

Virtual network gateway

Search Save Discard Delete Download VPN client

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
 - Configuration
 - Connections
 - Point-to-site configuration**
 - Maintenance
 - Properties
 - Locks
- Monitoring
- Automation

Address pool *
172.16.201.0/24 ✓

Tunnel type
IKEv2 ✓

IPsec / IKE policy
Default Custom

Authentication type
Azure certificate ✓

Root certificates

Name	Public certificate data
P2S-Root ✓	-----BEGIN CERTIFICATE----- MIIC5zCCAc+gAwIBAgIQWat8R/3rPqhC✓

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.

Home > P2S-Gateway

P2S-Gateway | Point-to-site configuration

Virtual network gateway

Search Save Discard Delete Download VPN client

Network & internet > VPN

VPN connections Add VPN

P2S-VNet Not connected	Connect ▼
----------------------------------	-----------

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)
```