POINT TO SITE

Prepare R&D Document on How to setup Point to Site.

Objective

Set up a Point-to-Site VPN in Azure to securely connect a client computer (like your laptop) to an Azure Virtual Network (VNet) over the internet.

What is Point-to-Site VPN?

- A VPN (Virtual Private Network) creates a secure, encrypted connection between your computer and another network.
- A Point-to-Site (P2S) VPN allows a single client device to securely connect to a Virtual Network in Azure from a remote location.
- P2S is ideal for remote workers or developers who need secure access to Azure resources (VMs, databases, etc.).

Step-by-Step Setup

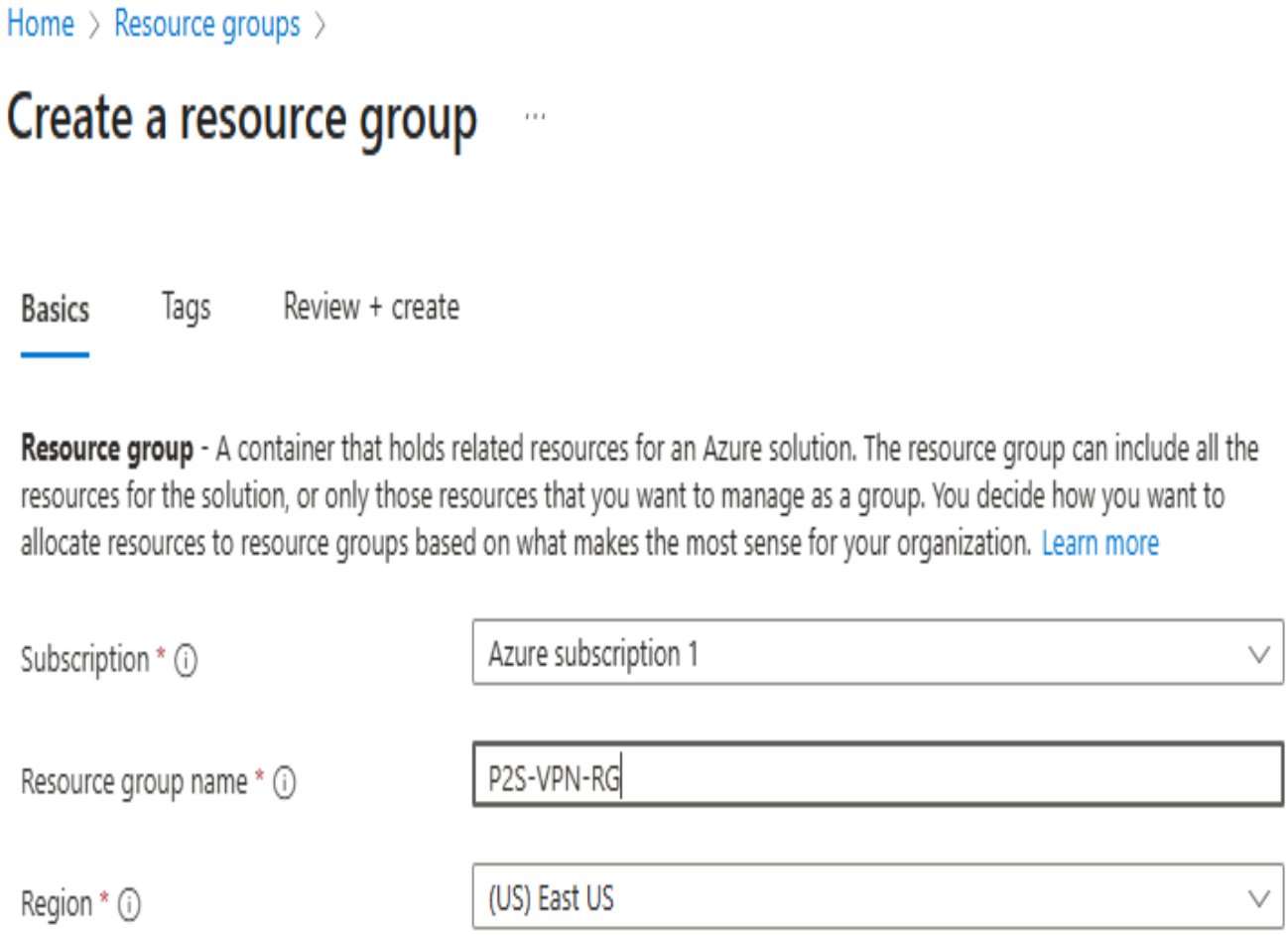
Step 1: Create a Resource Group

A Resource Group is a container that holds related Azure resources.

1. Go to https://portal.azure.com
2. Search for "Resource groups"
3. Click “+ Create”
4. Fill in:
    - Subscription: Choose your subscription

- Resource Group Name: P2S-VPN-RG
- Region: e.g., East US

5. Click Review + Create, then Create



Home > Resource groups >

Create a resource group ...

Basics Tags Review + create

Automation Link

Basics

Subscription	Azure subscription 1
Resource group name	P2S-VPN-RG
Region	East US

Tags

None

Home >

Resource groups ...

Default Directory (tanishkadeepakkadamgmail.onmicrosoft.com)

+ Create | Manage view | Refresh | Export to CSV | Open query | Assign tags

You are viewing a new version of Browse experience. Click here to access the old experience.

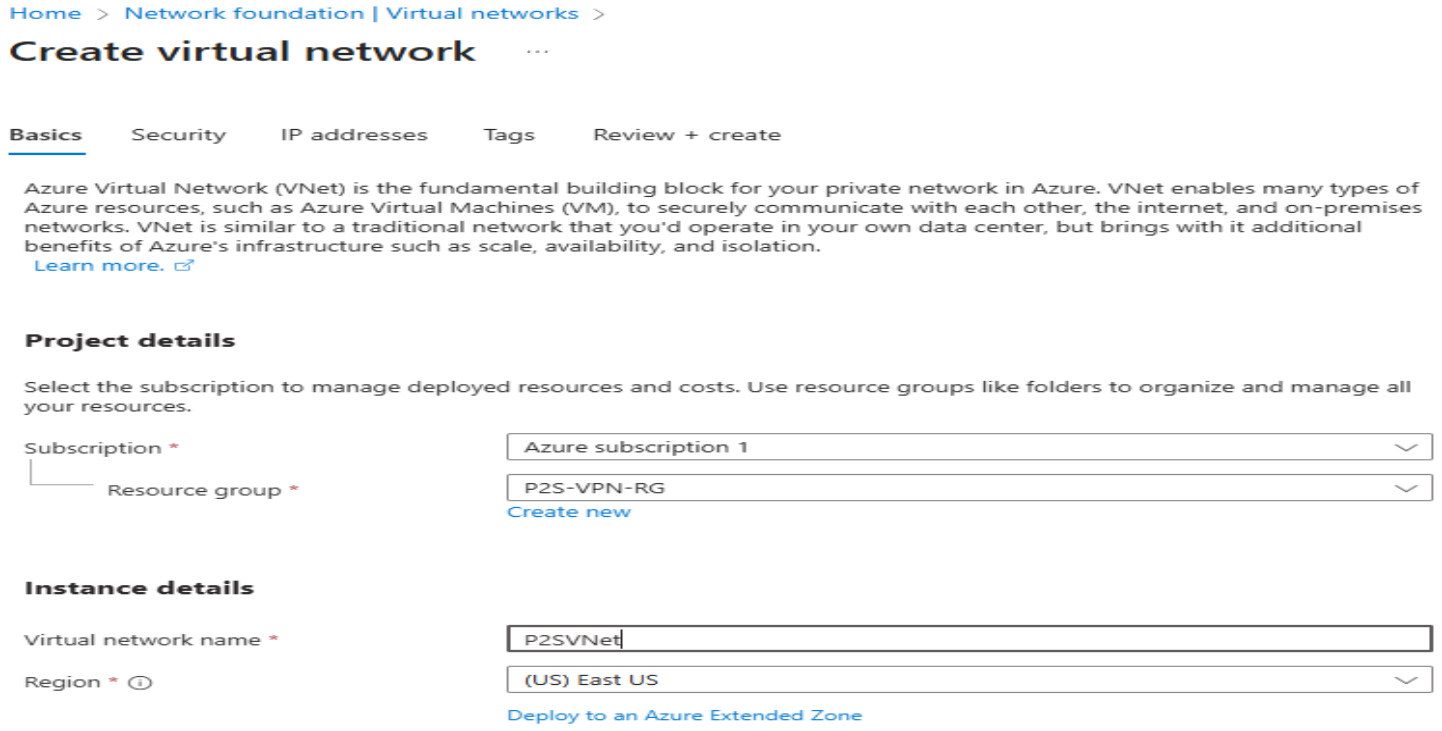
Filter for any field... | Subscription equals **all** | Location equals **all** X | + Add filter

Name ↑	Subscription	Location
P2S-VPN-RG ...	Azure subscription 1	East US

Step 2: Create a Virtual Network (VNet)

A VNet is like your private network in Azure.

1. Search for "Virtual networks"
2. Click "+ Create"
3. Fill in:
    - Resource Group: P2S-VPN-RG
    - Name: P2SVNet
    - Region: Same as Resource Group
4. Under IP Addresses:
    - IPv4 address space: 10.1.0.0/16
    - Subnet Name: default
    - Subnet range: 10.1.0.0/24
5. Leave rest default, then 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

10.0.0.0/16 Delete address space

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

Add IPv4 address space

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: Default

Name *: default2

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address *: 10.0.1.0

Size: /24 (256 addresses)

Subnet address range: 10.0.1.0 - 10.0.1.255

IPv6

Include an IPv6 address space: ☐ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

Enable private subnet (no default outbound access): ☐

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None

Create new

Add | Cancel | Give feedback

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

10.0.0.0/16 Delete address space

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
default2	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-

Add IPv4 address space

Create virtual network ...

Basics Security IP addresses Tags **Review + create**

View automation template

Basics

Subscription	Azure subscription 1
Resource Group	P2S-VPN-RG
Name	P2SVNet
Region	East US

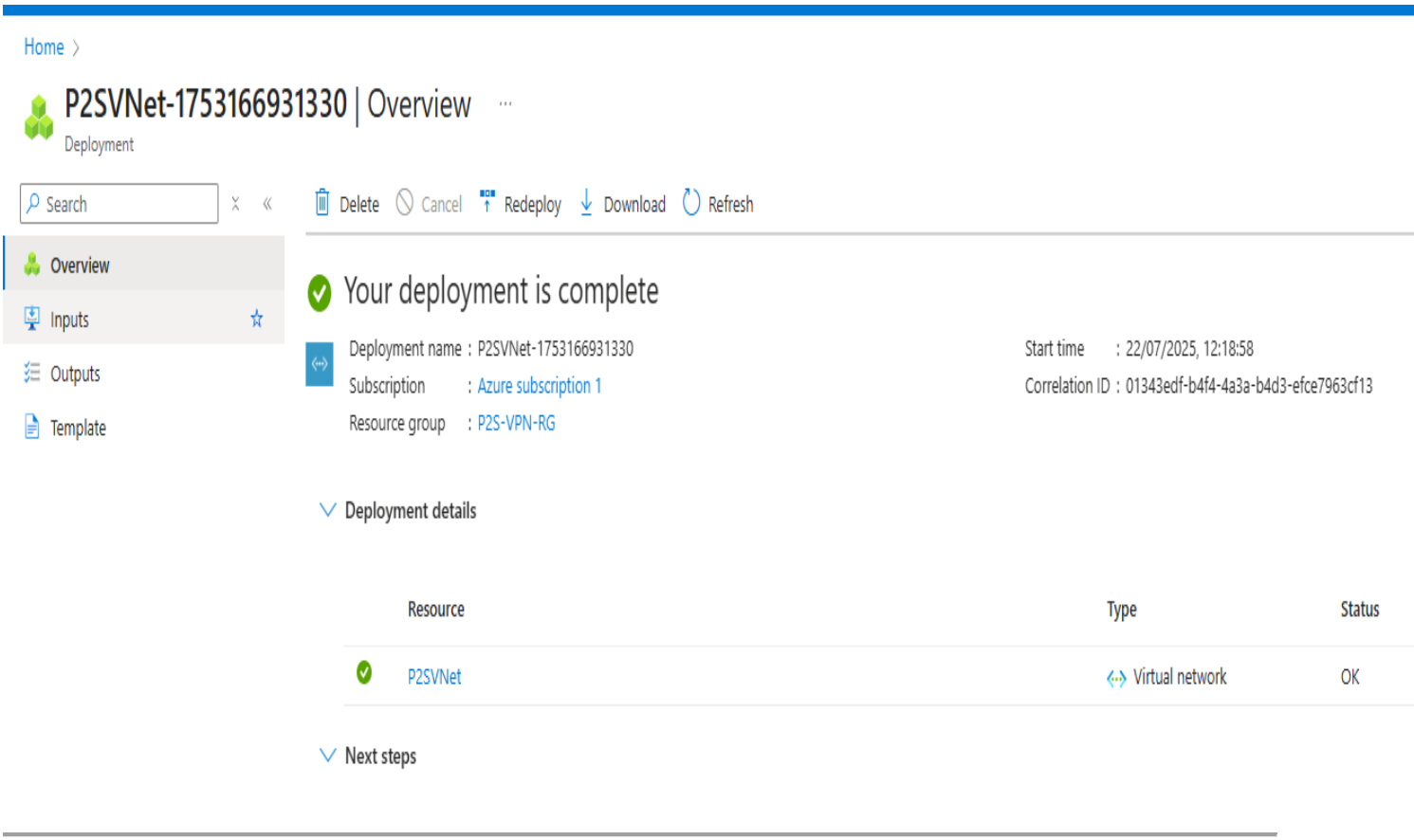
Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)
Subnet	default2 (10.0.1.0/24) (256 addresses)

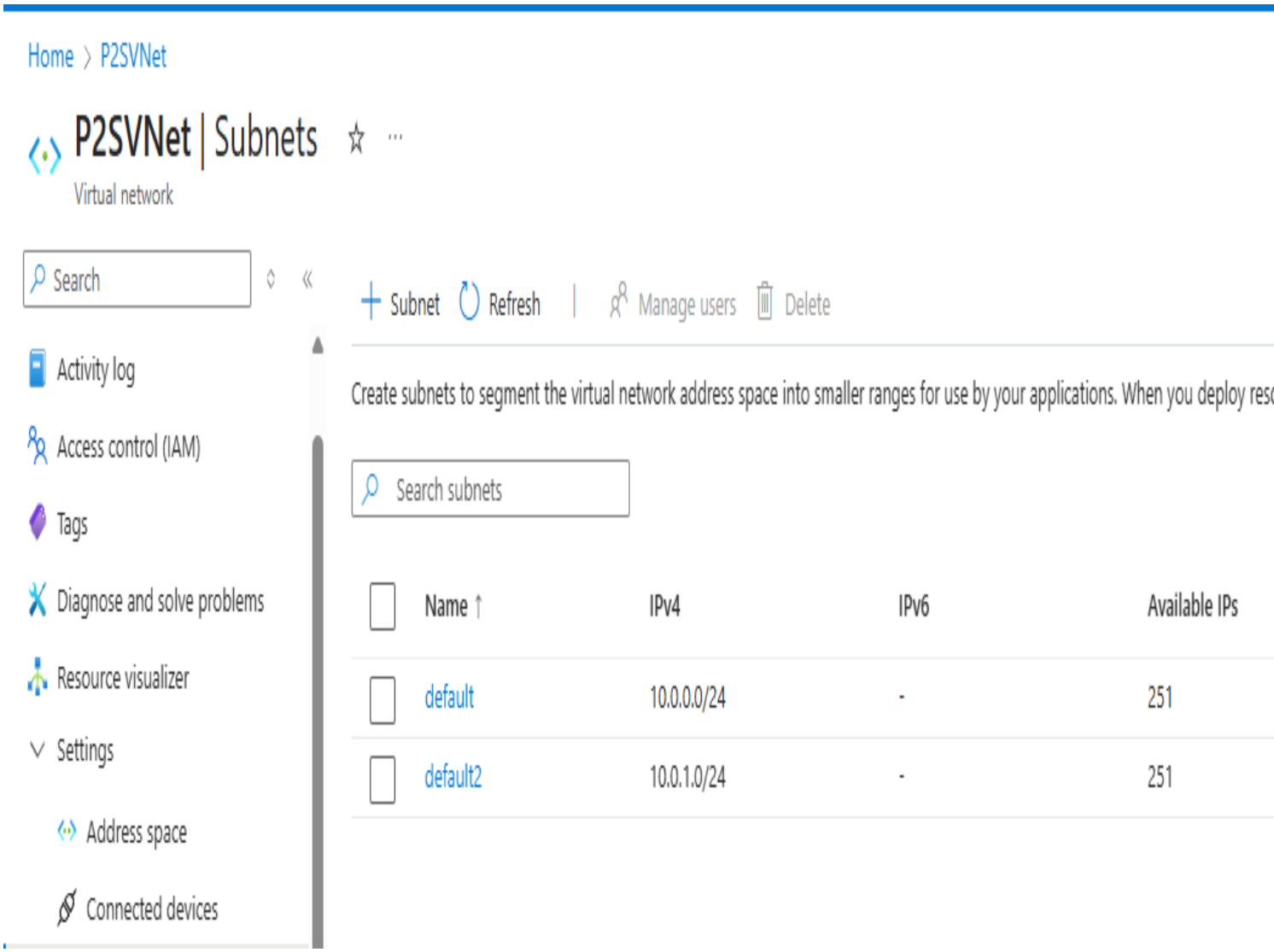
Tags



Step 3: Create Gateway Subnet

The GatewaySubnet is needed for Azure to host the VPN gateway.

1. Go to your created VNet → Subnets
2. Click + Gateway subnet
3. Name: *auto-filled as GatewaySubnet*
4. Address range: 10.1.255.0/27 (choose from unused range)
5. Click Add


Home > P2SVNet
P2SVNet | Subnets
Virtual network
Search
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnet
Refresh
Manage users
Delete
Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy reso
Search subnets
Name
IPv4
IPv6
Available IPs
default
10.0.0.0/24
-
251
default2
10.0.1.0/24
-
251

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: 10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address *: 10.0.2.0

Size: /24 (256 addresses)

Subnet address range: 10.0.2.0 - 10.0.2.255

IPv6

Include an IPv6 address space: ☐ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

Enable private subnet (no default outbound access): ☐

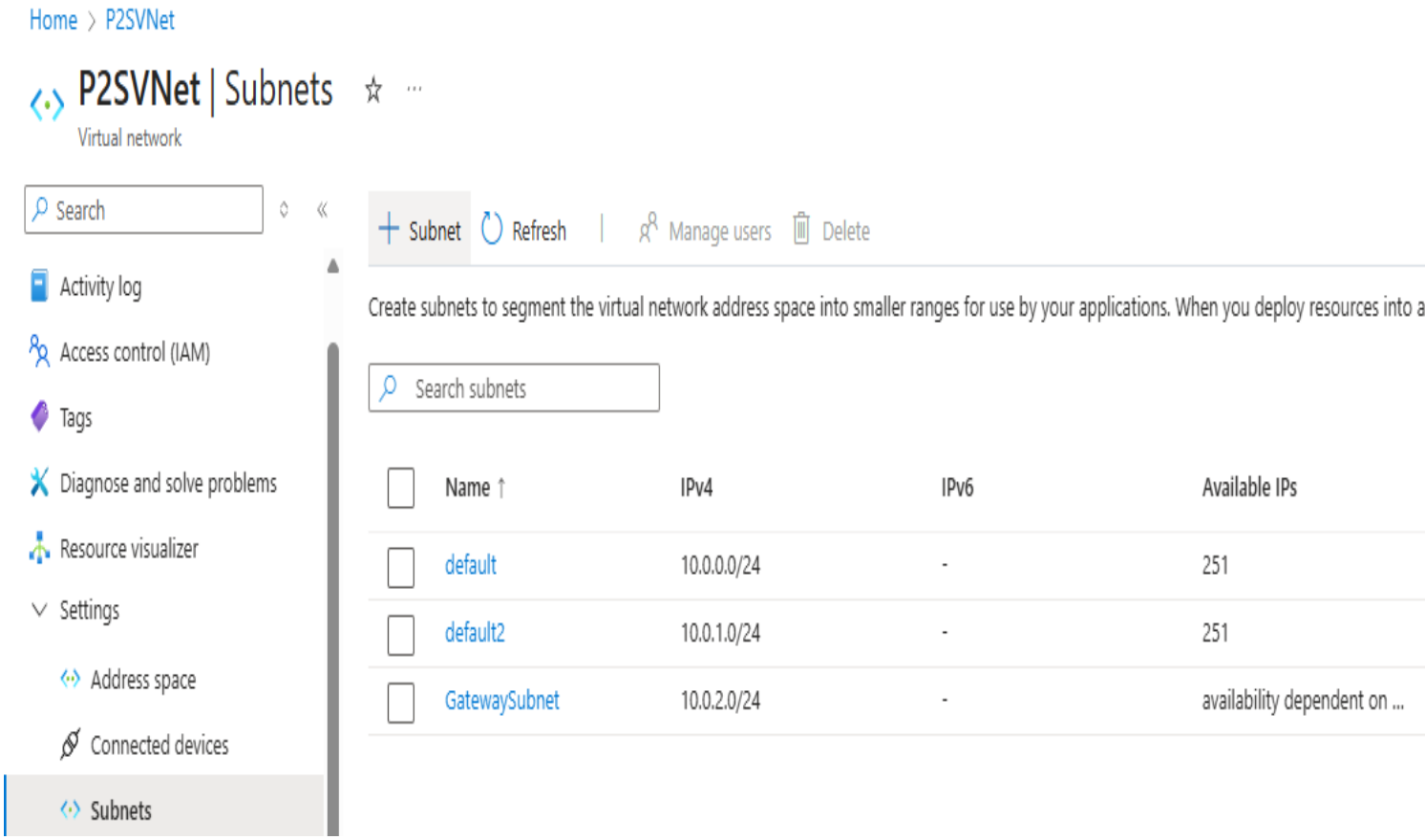
Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Add | Cancel | Give feedback



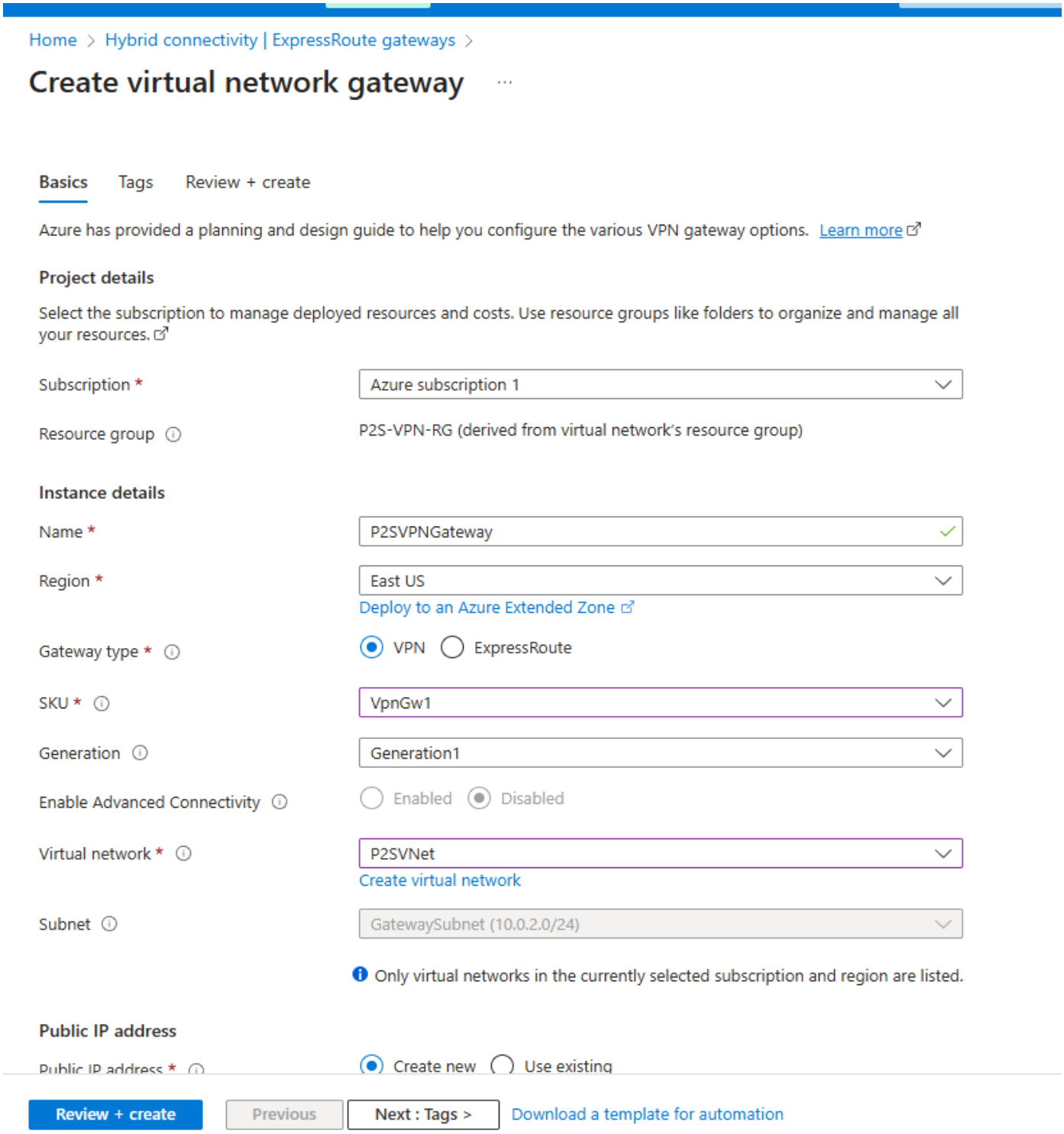
Step 4: Create a Virtual Network Gateway

This is the actual VPN device in Azure.

1. Search "Virtual network gateways" → + Create
2. Fill in:
    - Name: P2SVPNGateway
    - Region: Same as VNet
    - Gateway type: VPN
    - VPN type: Route-based
    - SKU: VpnGw1 (cheaper options available for test)
    - Virtual network: P2SVNet

- Gateway subnet: Will auto-pick the GatewaySubnet

3. Create a new Public IP: Name it P2S-Gateway-PublicIP
4. Click Review + Create, then Create.



Home > Hybrid connectivity | ExpressRoute gateways >

Create virtual network gateway ...

Virtual network * : P2SVNet

Create virtual network

Subnet : GatewaySubnet (10.0.2.0/24)

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

Public IP address

Public IP address * : Create new / Use existing

Public IP address name * : P2S-Gateway-PublicIP

Public IP address SKU : Standard

Assignment : Dynamic / Static

Enable active-active mode * : Enabled / Disabled

SECOND PUBLIC IP ADDRESS

SECOND PUBLIC IP ADDRESS * : Create new / Use existing

Public IP address name * : P2S-Gateway-PublicIP1

Public IP address SKU : Standard

Configure BGP * : Enabled / Disabled

Authentication Information (Preview)

Enable Key Vault Access : Enabled / Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

Review + create | Previous | Next : Tags > | Download a template for automation

Home > Hybrid connectivity | ExpressRoute gateways >

Create virtual network gateway ...

Validation passed

Basics Tags **Review + create**

Basics

Subscription	Azure subscription 1
Resource group	P2S-VPN-RG
Name	P2SVPNGateway
Region	East US
SKU	VpnGw1
Generation	Generation1
Virtual network	P2SVNet
Subnet	GatewaySubnet (10.0.2.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Enabled
Enable Advanced Connectivity	Disabled
Configure BGP	Disabled
Public IP address	P2S-Gateway-PublicIP
SECOND PUBLIC IP ADDRESS	P2S-Gateway-PublicIP1

Tags

None

Create Previous Next Download a template for aut

Home >

Microsoft.VirtualNetworkGateway-20250722142743 | Overview

Deployment

Search

Overview
Inputs
Outputs
Template

Delete Cancel Redeploy Download Refresh

Deployment is in progress

Deployment name : Microsoft.VirtualNetworkGateway-20250722142743
Subscription : Azure subscription 1
Resource group : P2S-VPN-RG

Start time : 22/07/2025, 14:55:37
Correlation ID : 8b28d598-15e2-435d-89f8-bdea326c0ada

Deployment details

Resource	Type	Status
P2S-Gateway-PublicIP1	Public IP address	OK
P2S-Gateway-PublicIP	Public IP address	OK

Home >

Microsoft.VirtualNetworkGateway-20250722142743 | Overview

Deployment

Search

Overview
Inputs
Outputs
Template

Delete Cancel Redeploy Download Refresh

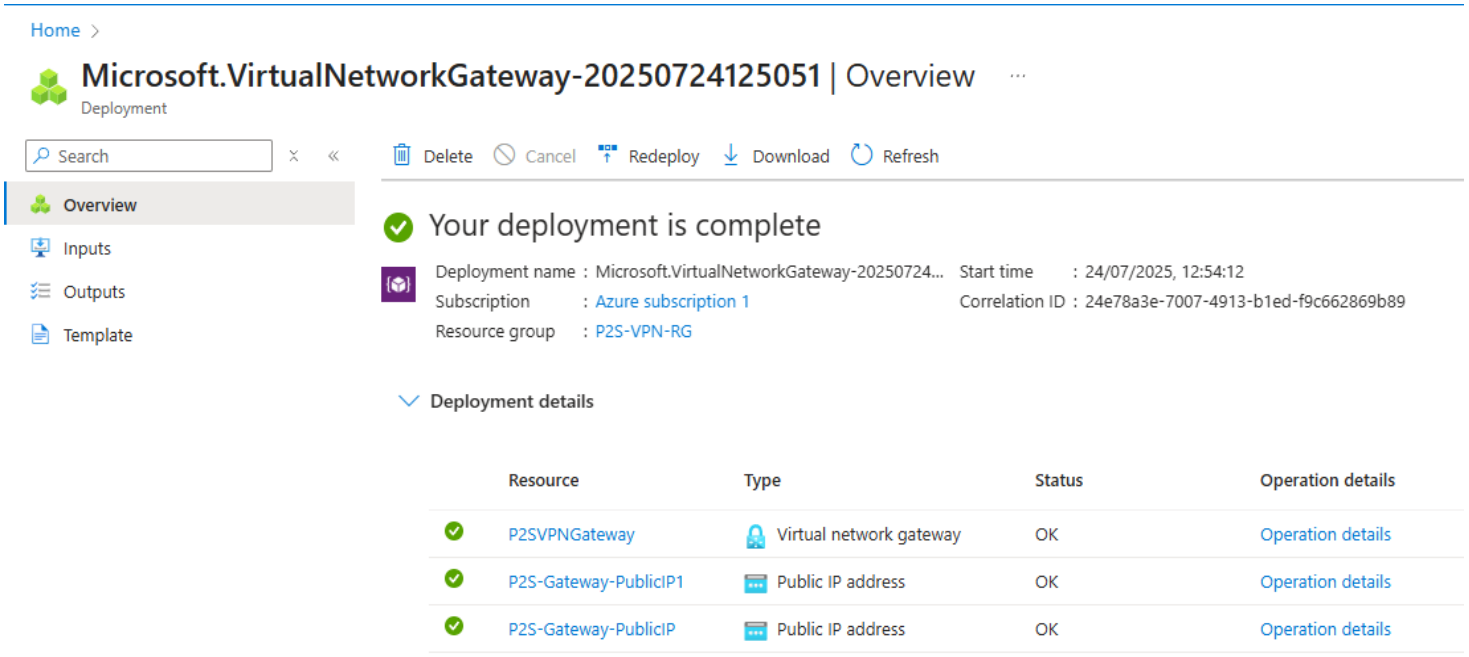
Deployment is in progress

Deployment name : Microsoft.VirtualNetworkGateway-20250722142743
Subscription : Azure subscription 1
Resource group : P2S-VPN-RG

Start time : 22/07/2025, 14:43:15
Correlation ID : 8b28d598-15e2-435d-89f8-bdea326c0ada

Deployment details

Resource	Type	Status
P2SVPNGateway	Virtual network gateway	Created
P2S-Gateway-PublicIP1	Public IP address	OK
P2S-Gateway-PublicIP	Public IP address	OK



Step 5: Generate Self-Signed Certificates

Step-by-Step: Generate Self-Signed Certificates for Point-to-Site in PowerShell

These certificates are used to **authenticate** your device when connecting to the VPN.

1: Open PowerShell as Administrator

1. Press **Windows key**
2. Type PowerShell
3. Right-click on **Windows PowerShell** > Click **Run as Administrator**

This is important. If not run as admin, certificate creation may fail.

2: Create the Root Certificate (No Output Expected)

Copy and paste the command below **into PowerShell**:

powershell

CopyEdit

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

Expected Behavior:

- PowerShell will **not show any message** unless there's an error.
- But behind the scenes, the root certificate is created in your **Current User > Personal** certificate store.

3: Verify the Root Certificate Was Created

Now run this command:

powershell

CopyEdit

```
Get-ChildItem -Path "Cert:\CurrentUser\My"
```

Expected Output:
A list of certificates will appear like this:

python-repl

CopyEdit

Thumbprint Subject

---------- -------

CB9CB46C68B7B07A2E1E70932750444E958892E0 CN=P2SRootCert

...

Look for a line where Subject is CN=P2SRootCert. That is your root certificate.

4: Store the Certificate in a Variable (IMPORTANT)

If you have multiple CN=P2SRootCert (as in your case), we'll pick **only the latest one** using [0].

powershell

CopyEdit

$rootCert = (Get-ChildItem -Path "Cert:\CurrentUser\My" | Where-Object { $_.Subject -eq "CN=P2SRootCert" })[0]

Check if the certificate is stored correctly:

powershell

CopyEdit

$rootCert

Expected: It should display info like:

diff

CopyEdit

Thumbprint Subject

---------- -------

CB9CB46C68B7B07A2E1E70932750444E958892E0 CN=P2SRootCert

STEP 5: Export the Root Certificate to .CER File

This file will later be uploaded to **Azure Virtual Network Gateway**.

powershell

CopyEdit

Export-Certificate -Cert $rootCert -FilePath "$env:USERPROFILE\Desktop\RootCert.cer"

Expected:

- A file called RootCert.cer will be saved to your **Desktop**.
- No major message; success is just the file being created.

📁 **Path:** C:\Users\<your_username>\Desktop\RootCert.cer

6: Create Client Certificate Signed by Root

Now we create a client certificate **linked to the Root**:

powershell

CopyEdit

```
$clientCert = New-SelfSignedCertificate `
 -Type Custom `
 -DnsName P2SClientCert `
 -KeySpec Signature `
 -Subject "CN=P2SClientCert" `
 -KeyExportPolicy Exportable `
 -HashAlgorithm sha256 `
```

-KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

-Signer $rootCert

Expected:

- Again, no message.
- Creates the client certificate signed by the root cert.

7: Export the Client Certificate (.PFX)

This file is used **on the client computer** to connect to the VPN.

powershell

CopyEdit

Export-PfxCertificate -Cert $clientCert `

-FilePath "$env:USERPROFILE\Desktop\ClientCert.pfx" `

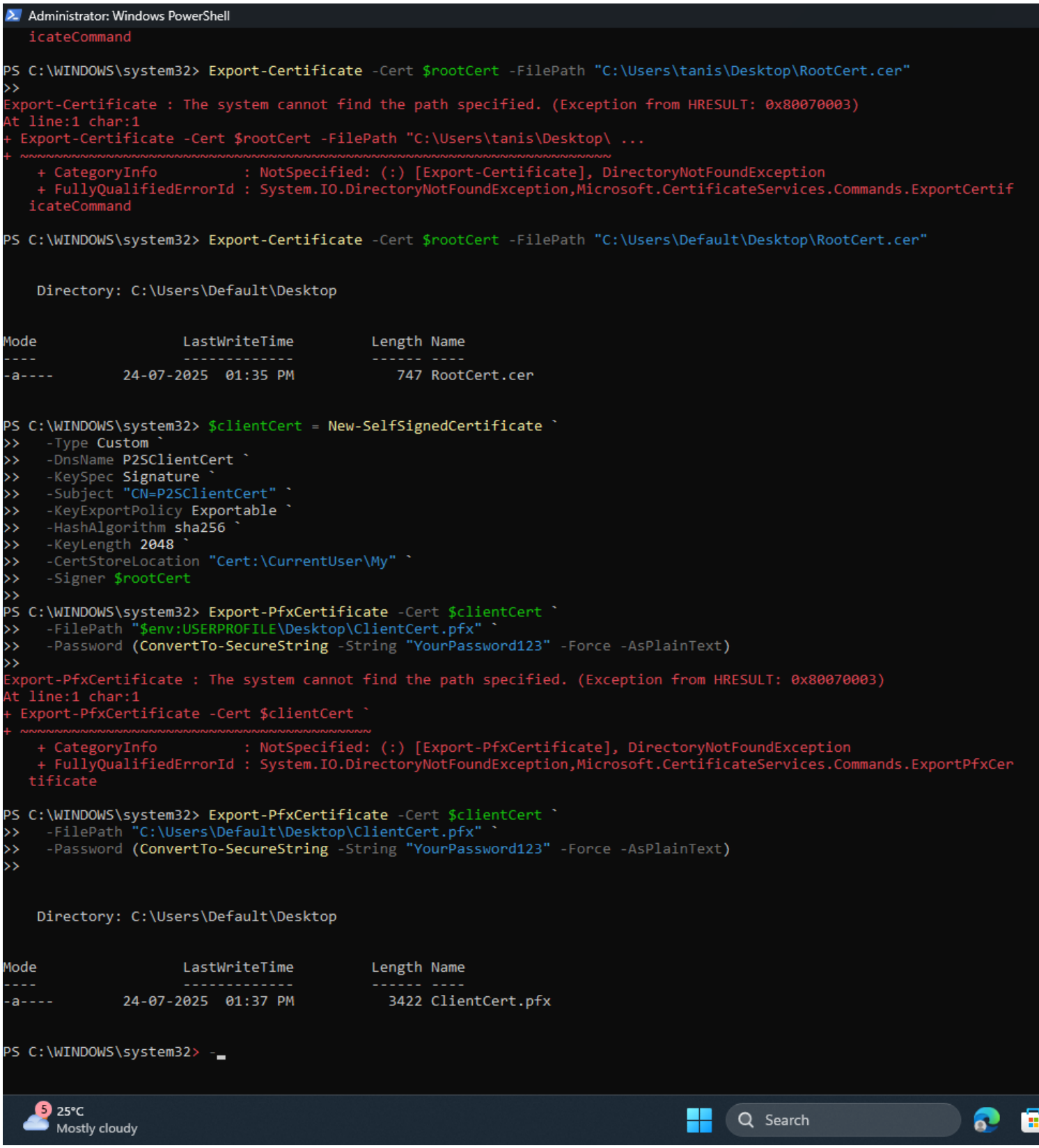
-Password (ConvertTo-SecureString -String "YourPassword123" -Force -AsPlainText)

Expected:

- File ClientCert.pfx will be created on your **Desktop**.
- This file will be **installed** on any device that needs to connect to the Azure VPN.

You'll need YourPassword123 when importing the .pfx file on another machine.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> $cert = 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> Get-ChildItem -Path "Cert:\CurrentUser\My"
>>


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
CB9CB46C68B7B07A2E1E70932750444E958892E0  CN=P2SRootCert
9F0C077E9985B2C15D14C16793AE14494D36CCD6  CN=P2SRootCert
83CB74F000B7D3AB3BC521F20CFBDDDFB93F4878  CN=P2SRootCert
7FCAC11F0875D067EAB558998A7B49A644EF7EAA  CN=P2SRootCert
72D7225D24DB419A8F1416EF2888C7BDF0AA017F  CN=P2SRootCert
6EBEF6345AF6B1EFC5D8FE72D5BF15248BC68018  CN=D71DBAE1-F02F-4E42-BF3A-4804221A01C6
6A825BDCFCC0A9ED32A9D687972C688248BF623A  CN=24daac57-140f-4013-8b28-85152735069f
5301DE55BCA656B45537E174A6BB75B117781443  CN=P2SRootCert
16D101A305CFAA640A30C715A3BBB1851A32818B  CN=P2SRootCert
0AFC6FE9961F35A9CAD6BE4B78EDC78D13AE0EE6  CN=67c0a40e-357b-4fb8-b122-2063985036cf
035A410648F0B0C52B8C0068DF1159DF7A3BAE3F  CN=trust_67c0a40e-357b-4fb8-b122-2063985036cf


PS C:\WINDOWS\system32> $rootCert = (Get-ChildItem -Path "Cert:\CurrentUser\My" | Where-Object { $_.Subject -eq "CN=P2SRootCert" })[0]
>>
PS C:\WINDOWS\system32> $rootCert
>>


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
CB9CB46C68B7B07A2E1E70932750444E958892E0  CN=P2SRootCert


PS C:\WINDOWS\system32> Export-Certificate -Cert $rootCert -FilePath "C:\Users\tanis\Desktop\RootCert.cer"
Export-Certificate : The system cannot find the path specified. (Exception from HRESULT: 0x80070003)
At line:1 char:1
+ Export-Certificate -Cert $rootCert -FilePath "C:\Users\tanis\Desktop\ ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Export-Certificate], DirectoryNotFoundException
    + FullyQualifiedErrorId : System.IO.DirectoryNotFoundException,Microsoft.CertificateServices.Commands.ExportCertif
   icateCommand

PS C:\WINDOWS\system32> Export-Certificate -Cert $rootCert -FilePath "$env:USERPROFILE\Desktop\RootCert.cer"
>>
Export-Certificate : The system cannot find the path specified. (Exception from HRESULT: 0x80070003)
At line:1 char:1
```


Administrator: Windows PowerShell
icateCommand
PS C:\WINDOWS\system32> Export-Certificate -Cert $rootCert -FilePath "C:\Users\tanis\Desktop\RootCert.cer"
>>
Export-Certificate : The system cannot find the path specified. (Exception from HRESULT: 0x80070003)
At line:1 char:1
+ Export-Certificate -Cert $rootCert -FilePath "C:\Users\tanis\Desktop\ ...
+ ~~~~~~
+ CategoryInfo : NotSpecified: (:) [Export-Certificate], DirectoryNotFoundException
+ FullyQualifiedErrorId : System.IO.DirectoryNotFoundException,Microsoft.CertificateServices.Commands.ExportCertif
icateCommand
PS C:\WINDOWS\system32> Export-Certificate -Cert $rootCert -FilePath "C:\Users\Default\Desktop\RootCert.cer"
Directory: C:\Users\Default\Desktop
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 24-07-2025 01:35 PM 747 RootCert.cer
PS C:\WINDOWS\system32> $clientCert = New-SelfSignedCertificate `
>> -Type Custom `
>> -DnsName P2SClientCert `
>> -KeySpec Signature `
>> -Subject "CN=P2SClientCert" `
>> -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 `
>> -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $rootCert
>>
PS C:\WINDOWS\system32> Export-PfxCertificate -Cert $clientCert `
>> -FilePath "$env:USERPROFILE\Desktop\ClientCert.pfx" `
>> -Password (ConvertTo-SecureString -String "YourPassword123" -Force -AsPlainText)
>>
Export-PfxCertificate : The system cannot find the path specified. (Exception from HRESULT: 0x80070003)
At line:1 char:1
+ Export-PfxCertificate -Cert $clientCert `
+ ~~~~~~
+ CategoryInfo : NotSpecified: (:) [Export-PfxCertificate], DirectoryNotFoundException
+ FullyQualifiedErrorId : System.IO.DirectoryNotFoundException,Microsoft.CertificateServices.Commands.ExportPfxCer
tificate
PS C:\WINDOWS\system32> Export-PfxCertificate -Cert $clientCert `
>> -FilePath "C:\Users\Default\Desktop\ClientCert.pfx" `
>> -Password (ConvertTo-SecureString -String "YourPassword123" -Force -AsPlainText)
>>
Directory: C:\Users\Default\Desktop
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 24-07-2025 01:37 PM 3422 ClientCert.pfx
PS C:\WINDOWS\system32> -
25°C
Mostly cloudy
Search

Step 6: Configure Point-to-Site VPN

What You're Doing:

You're setting up the P2S VPN **on the Azure Virtual Network Gateway**, so clients can connect using certificates (which you just created).

Step-by-Step Instructions

1. Navigate to Your Virtual Network Gateway

This assumes you've already created a Virtual Network Gateway (if not, I can help with that too)

- Go to the **Search bar** (top of Azure portal)
- Type: **Virtual network gateway**
- Click on your **gateway resource**

2. Click "Point-to-site configuration" in the left menu

You'll see:

- If not configured: A "Configure now" button
- If already configured: It will show current settings

Click: **Configure now**

3. Enter the Configuration Details

Field	Value	Explanation
Address Pool	172.16.0.0/24	This is a pool of private IPs that VPN clients will get when they connect. Think of it like DHCP for VPN.

Field	Value	Explanation
Tunnel Type	IKEv2 and SSTP	These are the supported VPN protocols. Choose both to support most devices (especially Windows).
Authentication Type	Azure certificate	You're using certificates for authentication (instead of username/password).

4. Upload the Public Root Certificate

You'll see a section like:

➕ Root certificates
Name | Public Certificate Data

Do the following:

A. Name:

nginx

CopyEdit

P2SRootCert

(you can name it anything, but this matches the cert you generated)

B. Public Certificate Data:

1. Go to your **Desktop**
2. **Right-click** on the RootCert.cer file → Click **Open With** → **Notepad**
3. You'll see something like:

css

CopyEdit

-----BEGIN CERTIFICATE-----

MIIDdjCCAl6gAwIBAgIUb9Z4c8g2R4f...

...

-----END CERTIFICATE-----

4. **Copy the entire contents** including:

css

CopyEdit

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

5. **Paste** it into the **Public certificate data** field in the Azure portal

5. Click Save

Wait for a few seconds. Azure will configure the VPN gateway with your settings.

Once it's saved:

- Your P2S configuration is ready
- You'll be able to download the **VPN client** in the next step

What Happens Next?

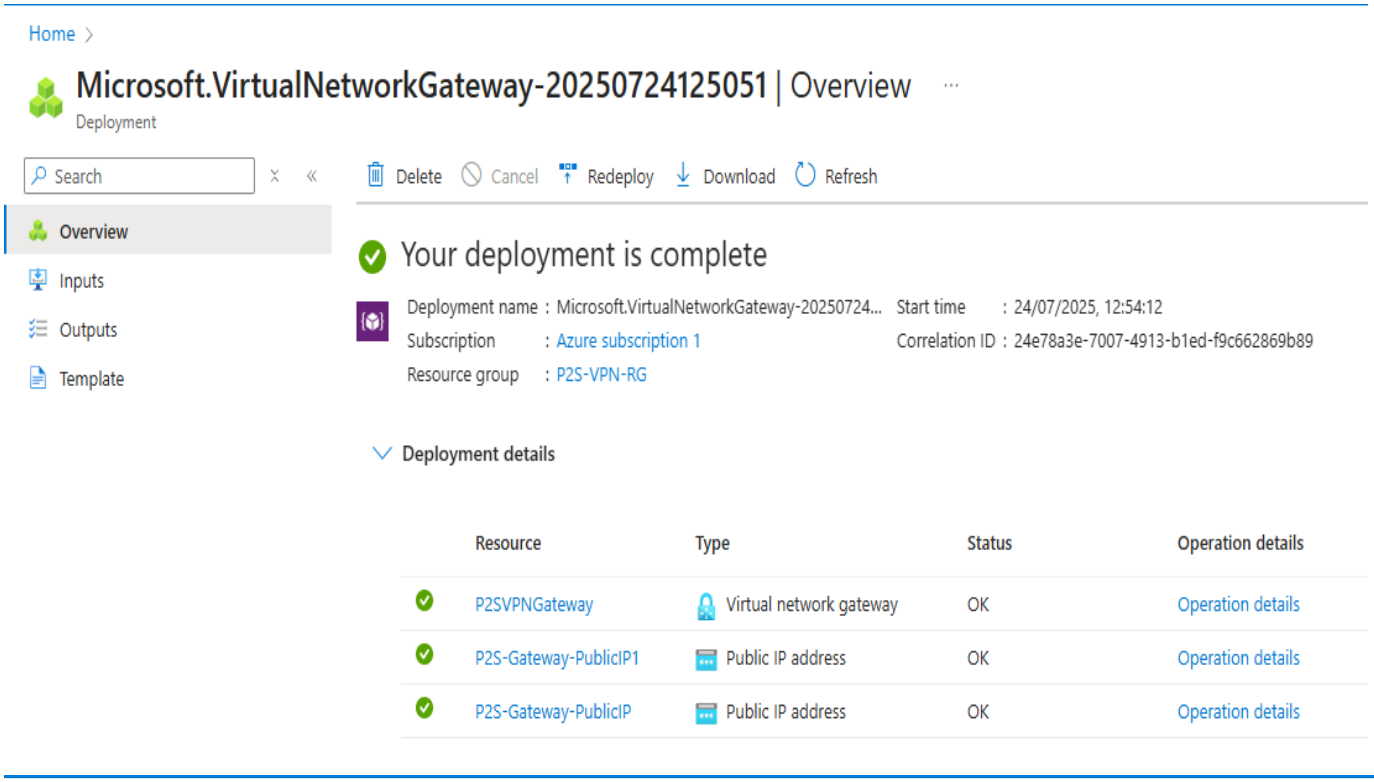
Once saved:

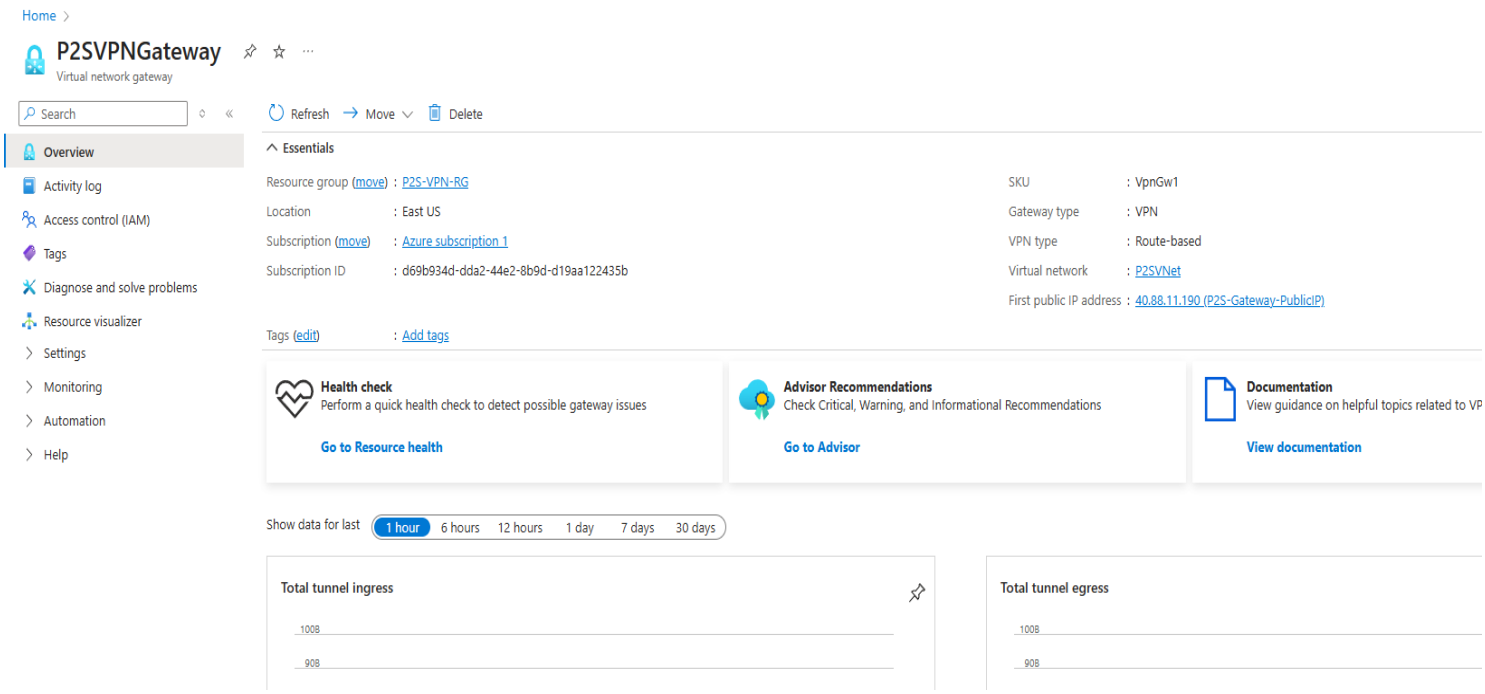
- Azure uses the root certificate you uploaded to validate any **client certificate** signed by it.
- That's how it allows your laptop (with client cert installed) to connect securely.

Why This Is Important:

This setup ensures:

- Only authorized users (with the client certificate) can connect
- All traffic is encrypted using VPN tunneling





Home › P2SVPNGateway

P2SVPNGateway | Point-to-site configuration

Virtual network gateway

point

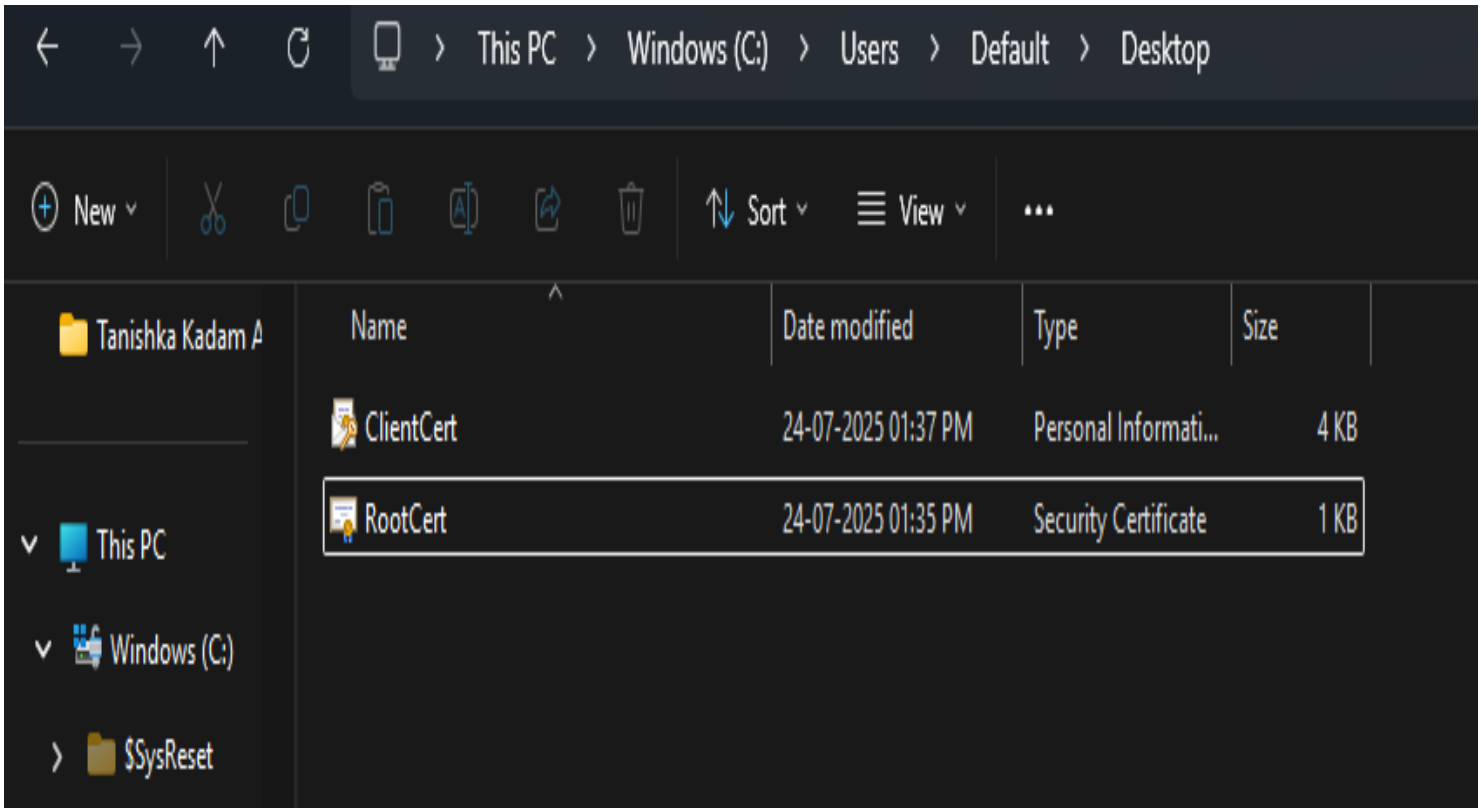
Save Discard Delete Download VPN client

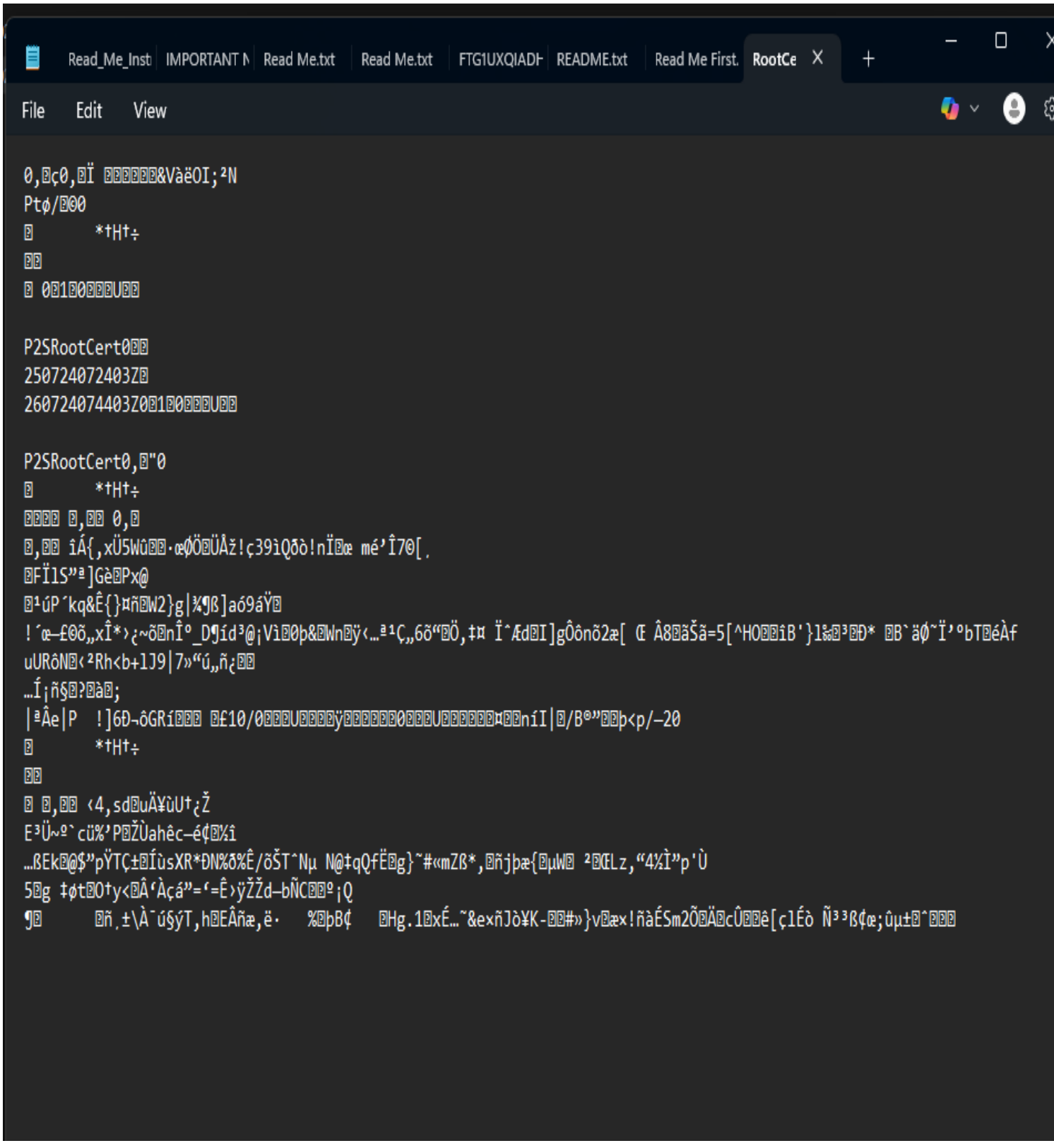
Settings

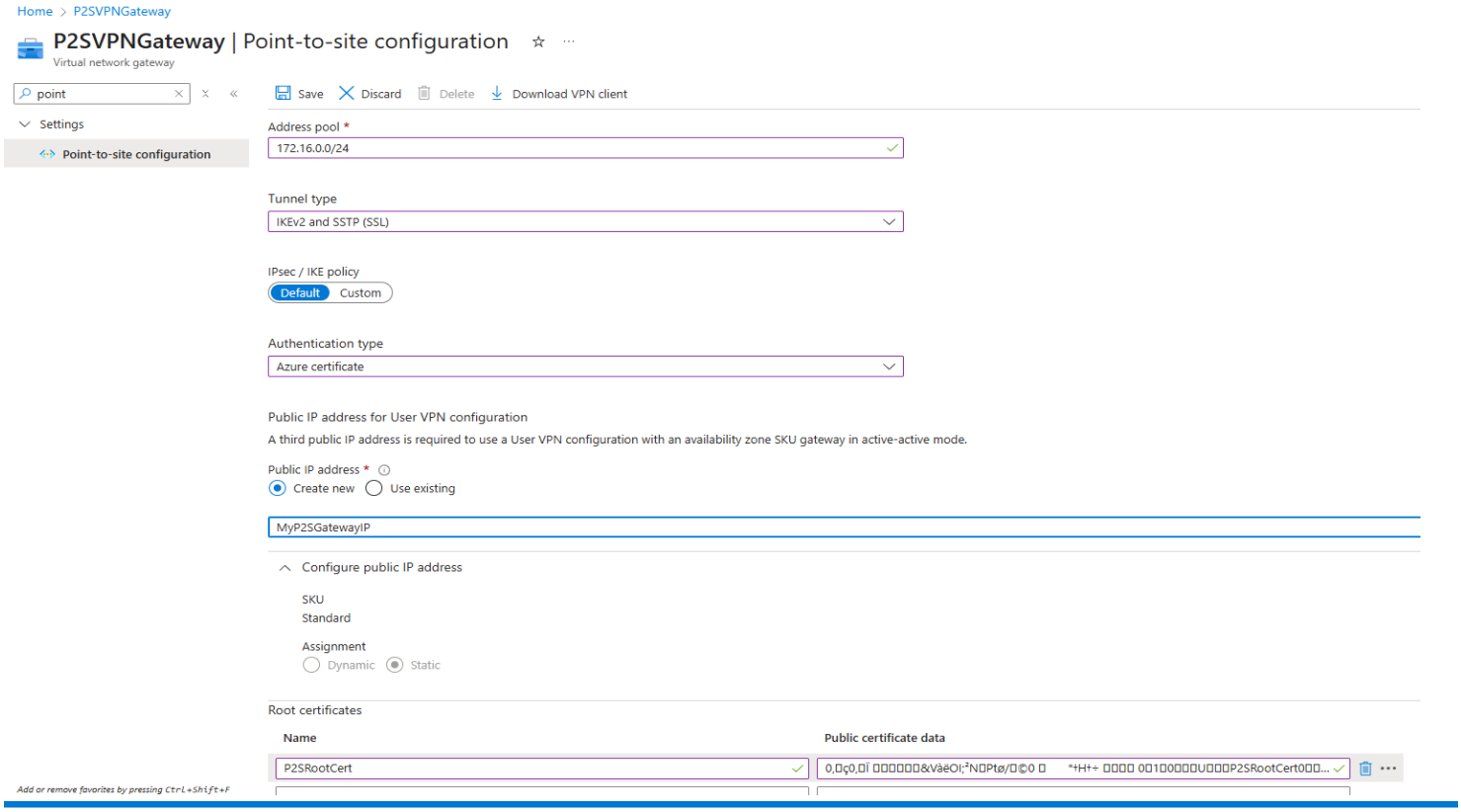
Point-to-site configuration

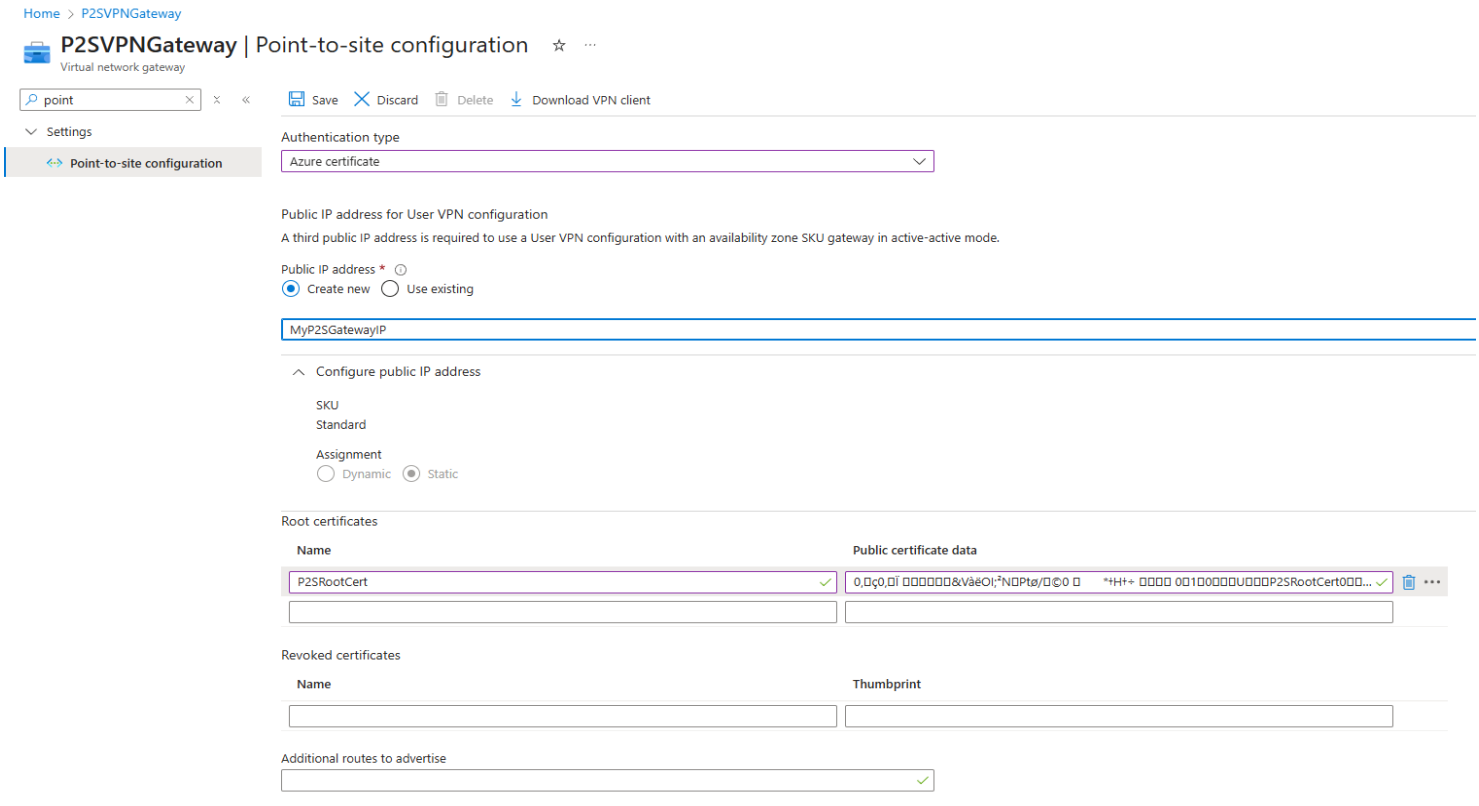
Point-to-site is not configured

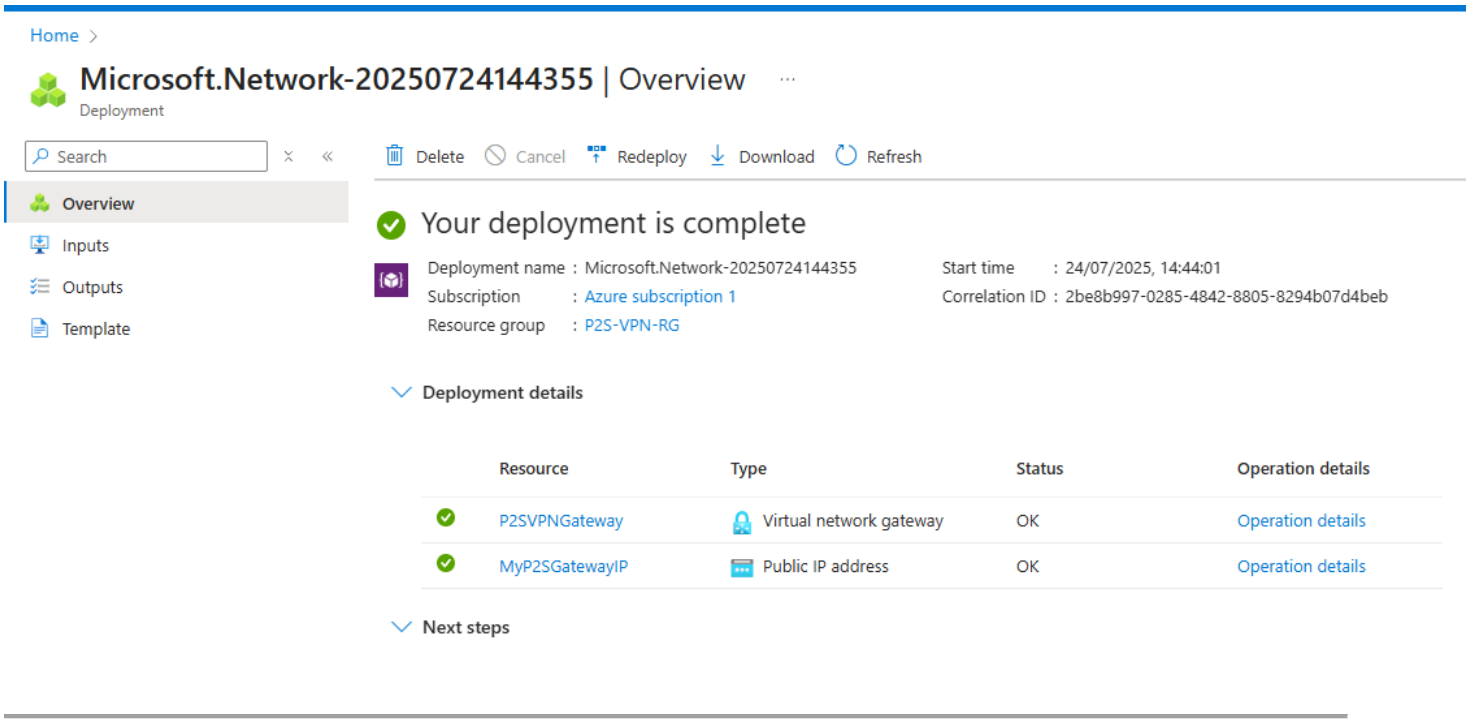
Configure now




Read_Me_Inst
IMPORTANT N
Read Me.txt
Read Me.txt
FTG1UXQIADH
README.txt
Read Me First.
RootCe
File
Edit
View
0,□ç0,□Ï □□□□□□&VàëOI;²N
Ptø/□00
□ *†H†÷
□□
□ 0□1□0□□□U□□
P2SRootCert0□□
2507240724037□
2607240744037Z0□1□0□□□U□□
P2SRootCert0,□"0
□ *†H†÷
□□□□ □,□□ 0,□
□,□□ îÁ{,xÜ5Wû□□·œØÖ□ÜÅž!ç39ìQðò!nÏ□œ mé'Î7©[.
□FÏlS"ª]Gè□Px@
□¹úP´kq&Ê{}¤ñ□W2}g|¾¶ß]aó9áŸ□
!´œ–£0õ„xÎ*›¿~õ□nÎº_D¶íd³@¡Vi□0þ&□Wn□ÿ‹…ª¹Ç„6õ"□Ö,‡¤ Ï^Æd□I]gÔônõ2æ[Œ Â8□ãŠã=5[^HO□□îB'}l‰□³□Ð* □B`äØ˜Ï'ºbT□éÀf
uURôN□‹²Rh<b+lJ9|7»"ú„ñ¿□□
…Í¡ñ§□?□à□;
|ªÂe|P !]6Ð¬ôGRí□□□ □£10/0□□□U□□□□ÿ□□□□□□0□□□U□□□□□□¤□□níI|□/B℗"□□þ<p/–20
□ *†H†÷
□□
□ □,□□ ‹4,sd□uÄ¥ùU†¿Ž
E³Ü~º`cü%'P□ŽÙahêc–é¢□½î
…ßEk□@$"pŸTÇ±□ÍùsXR*ÐN%ð%Ê/õŠT^Nµ N@‡qQfË□g}˜#«mZß*,□ñjþæ{□µW□ ²□Œ‹Lz,"4½Ì"p'Ù
5□g ‡øt□Oty‹□Â'Àçá"='=Ê›ÿŽŽd–bÑC□□º¡Q
¶□ □ñ¸±\À¯ú§ýT,h□EÂñæ,ë· %□þB¢ □Hg.1□xÉ…˜&e×ñJò¥K-□□#»}v□æ×!ñàÉSm2Õ□Ä□cÛ□□ê[çlÉò Ñ³³ß¢œ;ûµ±□^□□□


Home > P2SVPNGateway
P2SVPNGateway | Point-to-site configuration
Virtual network gateway
point
Settings
Point-to-site configuration
Save
Discard
Delete
Download VPN client
Address pool *
172.16.0.0/24
Tunnel type
IKEv2 and SSTP (SSL)
IPsec / IKE policy
Default
Custom
Authentication type
Azure certificate
Public IP address for User VPN configuration
A third public IP address is required to use a User VPN configuration with an availability zone SKU gateway in active-active mode.
Public IP address *
Create new
Use existing
MyP2SGatewayIP
Configure public IP address
SKU
Standard
Assignment
Dynamic
Static
Root certificates
Name
Public certificate data
P2SRootCert
Add or remove favorites by pressing Ctrl+Shift+F


Home > P2SVPNGateway
P2SVPNGateway | Point-to-site configuration
Virtual network gateway
point
Settings
Point-to-site configuration
Save
Discard
Delete
Download VPN client
Authentication type
Azure certificate
Public IP address for User VPN configuration
A third public IP address is required to use a User VPN configuration with an availability zone SKU gateway in active-active mode.
Public IP address *
Create new
Use existing
MyP2SGatewayIP
Configure public IP address
SKU
Standard
Assignment
Dynamic
Static
Root certificates
Name
Public certificate data
P2SRootCert
Revoked certificates
Name
Thumbprint
Additional routes to advertise



Step 7: Download VPN Client

1. In the same Point-to-site config page, click Download VPN Client
2. It will download a zip file
3. Extract and run the installer specific to your OS (Windows, macOS, etc.)

Click to go back, hold to see history

Upgrade

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

Copilot

Home > P2SVPNGateway

P2SVPNGateway | Point-to-site configuration

Virtual network gateway

point

Save Discard Delete Download VPN client

- Settings
  - Point-to-site configuration
- Monitoring
  - Point-to-site Sessions

Tunnel type

IKEv2 and SSTP (SSL)

IPsec / IKE policy

Default Custom

Authentication type

Azure certificate

Public IP address for User VPN configuration

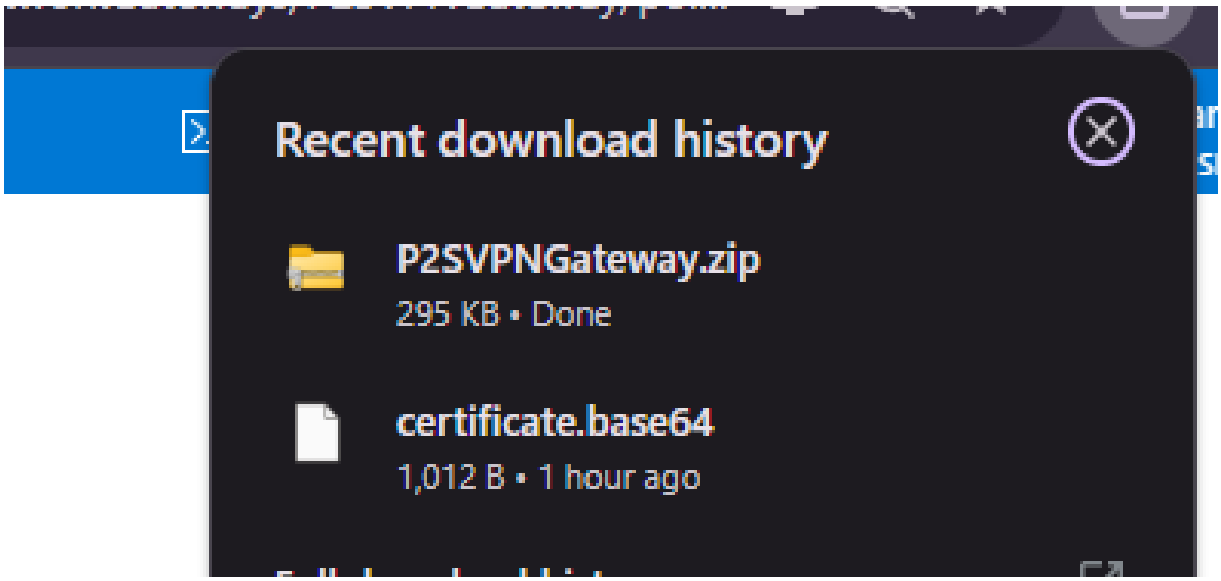
A third public IP address is required to use a User VPN configuration with an availability zone SKU gateway in active-active mode.

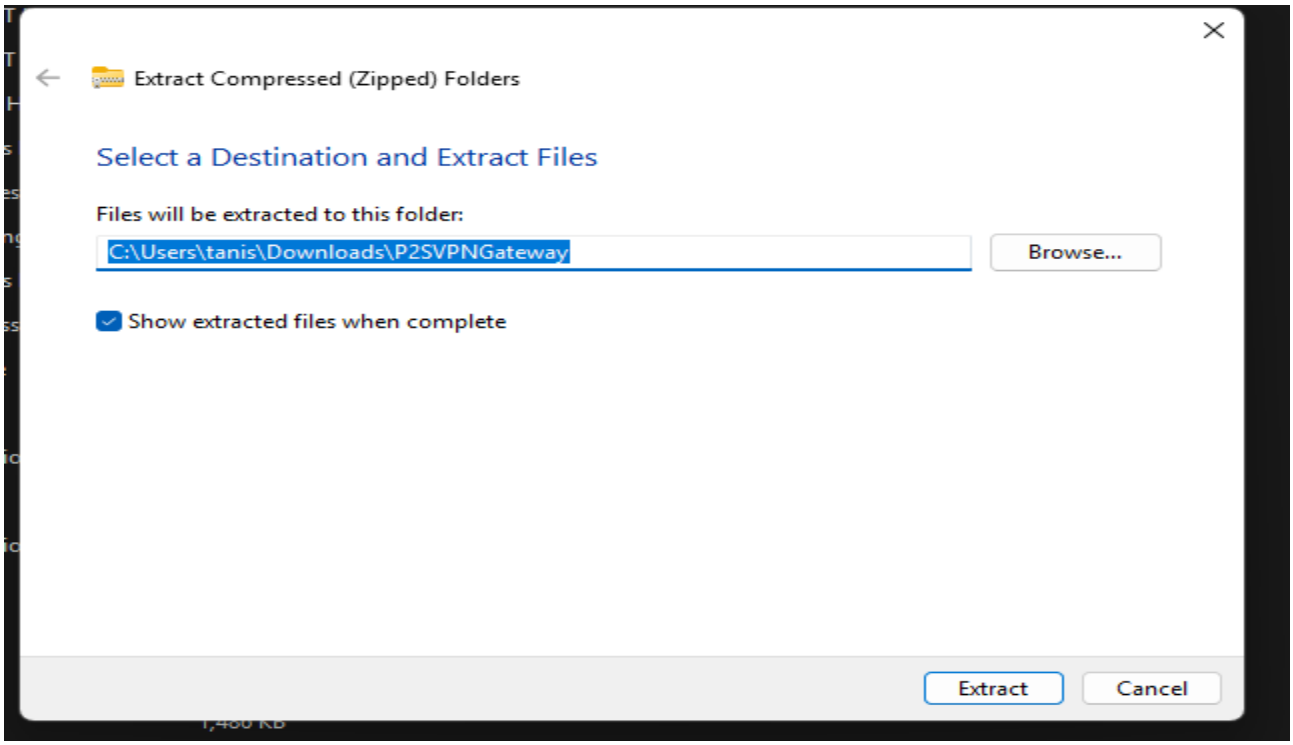
MyP2SGatewayIP

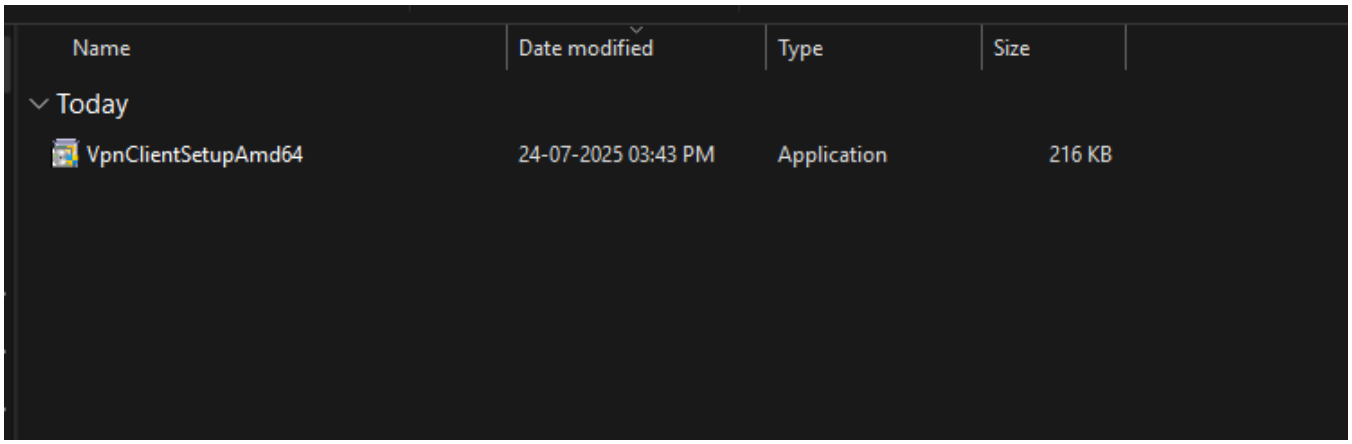
Root certificates

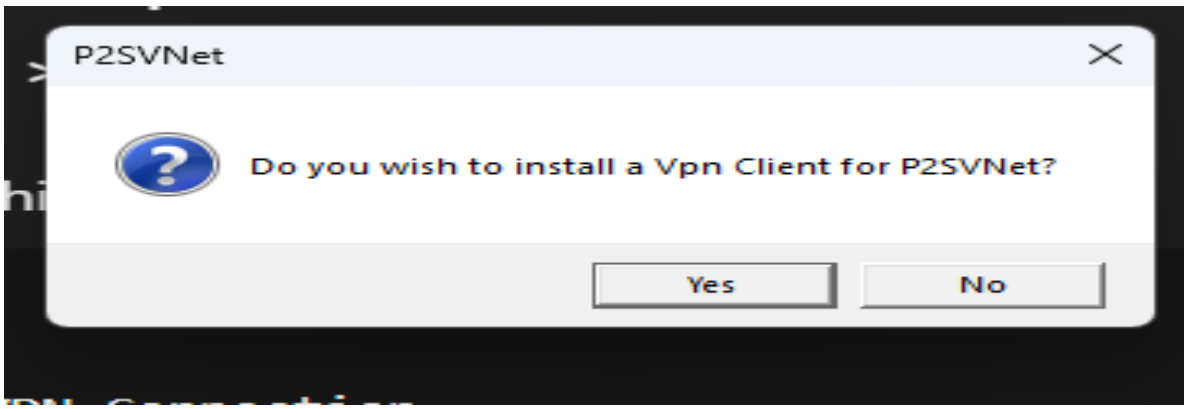
Name	Public certificate data
certificate.base64	MIIC5zCCAc+gAwIBAgIQJlbg609JO7JOC1B0+C8EqTANBgkqhkiG9w0BAQsFADA

Revoked certificates




Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\tanis\Downloads\P2SVPNGateway
Browse...
Show extracted files when complete
Extract
Cancel


Name
Date modified
Type
Size
Today
VpnClientSetupAmd64
24-07-2025 03:43 PM
Application
216 KB


P2SVNet
Do you wish to install a Vpn Client for P2SVNet?
Yes
No

Step 8: Connect from Your Computer

1. After installing the VPN client, find it under Windows > Network settings
2. Click Connect
3. You're now connected to Azure VNet!

You can now:

- Ping Azure VMs (if created)
- Access internal services hosted in your Azure network

Test Connectivity

- Deploy a VM inside the VNet
- Use Remote Desktop (RDP) to access the VM using its private IP
- Ping internal services if configured

Resource	Name	Notes
Resource Group	P2S-VPN-RG	Container for all Azure resources
Virtual Network	P2SVNet	10.1.0.0/16 range
Gateway Subnet	GatewaySubnet	10.1.255.0/27
Virtual Network Gateway	P2SVPNGateway	Hosts the VPN endpoint
Public IP	P2S-Gateway-PublicIP	Connects your device to Azure
Certificate	P2SRootCert / P2SClientCert	Authenticates users