

## Step-by-Step Setup: Configuring a Point-to-Site (P2S) VPN Connection from Your PC to Azure

A **Point-to-Site (P2S) Virtual Private Network (VPN)** is a secure connection that allows an individual device (like a laptop or PC) to connect to a remote cloud network, such as an Azure Virtual Network (VNet), over the internet. Unlike a Site-to-Site (S2S) VPN, which connects entire networks, a P2S VPN connects individual devices to the network. This makes it ideal for remote workers or anyone needing secure access to resources in a cloud environment like Azure. It offers key features like **secure remote access**, **cost efficiency**, **scalability**, and **enhanced security** for connecting individual devices to cloud resources.

### Step 1: Create a Subscription

- 1.1 Log in to Azure portal ([portal.azure.com](https://portal.azure.com))
- 1.2 Navigate to *Subscription*
- 1.3 Click on *Create* to create a new subscription and provide the name of the subscription
- 1.4 Follow on-screen instructions to set up the subscription

### Step 2: Create a Resource group

- 2.1 Navigate to *Resource group*
- 2.2 Click on *Create* and provide the name of the resource group
- 2.3 Select the subscription you have created earlier
- 2.4 Select the region for the resource group
- 2.5 Click on *Review + create* and then *Create* for the completion

The screenshot shows the 'Create a resource group' page in the Azure portal. The page has a breadcrumb 'Home >' and a title 'Create a resource group'. Below the title are tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is selected. A description of a resource group is provided. The form is divided into 'Project details' and 'Resource details'. Under 'Project details', there are two dropdown menus: 'Subscription' with 'Azure For Learning' selected, and 'Resource group' with 'ResourceLearning' selected. Under 'Resource details', there is a dropdown menu for 'Region' with '(US) East US' selected. At the bottom, there are three buttons: 'Review + create' (highlighted with a blue border), '< Previous', and 'Next: Tags >'.

### Step 3: Create a Virtual Network

- 3.1 Navigate to *Virtual network* in azure portal
- 3.2 Click *Create* to create a new virtual network
- 3.3 Select the subscription
- 3.4 Select resource group and location for virtual network
- 3.4 Provide a name for the virtual
- 3.5 Define the IP address space for the virtual network
- 3.6 Edit the default subnet, modify its IP range, name the subnet and save
- 3.7 Click *Review + create* and then *Create* to create the virtual network

Home > Virtual networks >

## Create virtual network

Basics Security IP addresses Tags Review + create

### Project details

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

Subscription \*

Resource group \*  [Create new](#)

### Instance details

Virtual network name \*

Region \*  [Deploy to an Azure Extended Zone](#)

[Previous](#) [Next](#) [Review + create](#)

---

Home > Virtual networks >

## Create virtual network

Basics Security IP addresses Tags Review + create

assigns the resource an IP address from the subnet. [Learn more](#)

[+ Add a subnet](#)

192.168.0.0/16

### You can modify or leave this IP range as default

/16  
192.168.0.0 - 192.168.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	

### Edit this default subnet as show on right side of the screen

[Previous](#) [Next](#) [Review + create](#)

### Edit subnet

Subnet purpose

Name \*

IPv4

Include an IPv4 address space ☒

IPv4 address range \*

Starting address \*  /24 (256 addresses)

Subnet address range

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 machines in the subnet. [Learn more](#)

[Save](#) [Cancel](#)

## Step 4: Create the gateway subnet

- 4.1 Navigate to the setting of Virtual network (e.g., MyLAN)
- 4.2 Click on [+ Gateway subnet](#)
- 4.3 You can name it or leave as default (e.g., GatewaySubnet)
- 4.4 Define the IP range within the IP range of Virtual Network
- 4.5 Click on [Add](#) to save the gateway subnet

Home > Virtual networks > MyLAN

## Virtual networks

University of Toledo (rocketstudies@com.microsoft...)

[+ Create](#) [Manage view](#)

Filter for any field...

Name \*

[MyLAN](#)

[MyNetwork](#)

[Subnets](#)

[Subnets](#)

[+ Subnet](#) [+ Gateway subnet](#)

### 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](#)

Search subnets

Name \*

Subnet purpose

IPv4

Include an IPv4 address space ☒

IPv4 address range \*

Starting address \*  /24 (256 addresses)

Size

Subnet address range

IPv6

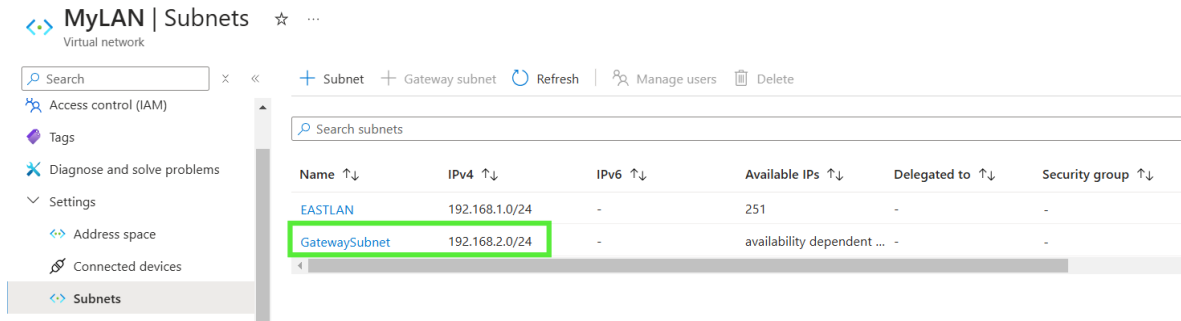
Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

**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 machines in the subnet. [Learn more](#)

[Add](#) [Cancel](#)

[Give feedback](#)



## Step 5: Create a Virtual Network Gateway

- 5.1 Navigate *Virtual network gateway* in Azure portal
- 5.2 Click *Create* to add a new virtual network gateway
- 5.3 Provide necessary details such as subscription, resource group, etc.
- 5.4 Select VPN type, SKU, and virtual network as shown below
- 5.5 Select the same resource group as created earlier
- 5.6 Click *Review + create* and wait for the deployment to be completed

[Home](#) > [Virtual network gateways](#) >

### Create virtual network gateway

[Basics](#) [Tags](#) [Review + create](#)

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [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 For Learning**

Resource group ⓘ ResourceLearning (derived from virtual network's resource group)

**Instance details**

Name \* ▼ **P2S-VirtualNetworkGateway**

Region \* ▼ **East US**  
[Deploy to an Azure Extended Zone](#)

Gateway type \* ⓘ ☒ **VPN** ☐ ExpressRoute

SKU \* ⓘ ▼ **VpnGw2AZ** **Leave as default**

Generation ⓘ ▼ **Generation2** **Leave as default**

Virtual network \* ⓘ ▼ **MyLAN**  
[Create virtual network](#)

Subnet ⓘ ▼ **GatewaySubnet (192.168.2.0/24)**

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-VirtualNetworkGateway-IP**

Public IP address SKU ▼ **Standard**

Assignment ☐ Dynamic ☒ **Static**

Availability zone \* ▼ **Zone-redundant**

Enable active-active mode \* ⓘ ☐ Enabled ☒ **Disabled**

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](#)

## Step 6: Create a self-signed root certificate

6.1 Click on this link for all details: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

6.2 Open PowerShell in your PC or laptop

6.3 Copy the commands from the link above and run for root and client certificates

6.4 Run the command *certmgr* in PowerShell to open the Manage user certificates window

6.5 Export the root certificate to download folder in your PC follow the screenshots shown below

### Root certificate command

```
1 $params = @{
2     Type = 'Custom'
3     Subject = 'CN=P2SRootCert'
4     KeySpec = 'Signature'
5     KeyExportPolicy = 'Exportable'
6     KeyUsage = 'CertSign'
7     KeyUsageProperty = 'Sign'
8     KeyLength = 2048
9     HashAlgorithm = 'sha256'
10    CertStoreLocation = 'Cert:\CurrentUser\My'
11 }
12 $cert = New-SelfSignedCertificate @params
```

### client certificate command

```
1 $params = @{
2     Type = 'Custom'
3     Subject = 'CN=P2SChildCert'
4     DnsName = 'P2SChildCert'
5     KeySpec = 'Signature'
6     KeyExportPolicy = 'Exportable'
7     KeyLength = 2048
8     HashAlgorithm = 'sha256'
9     CertStoreLocation = 'Cert:\CurrentUser\My'
10    Signer = $cert
11    TextExtension = @(
12        '2.5.29.37={text}1.3.6.1.5.5.7.3.2')
13    }
14    New-SelfSignedCertificate @params
```

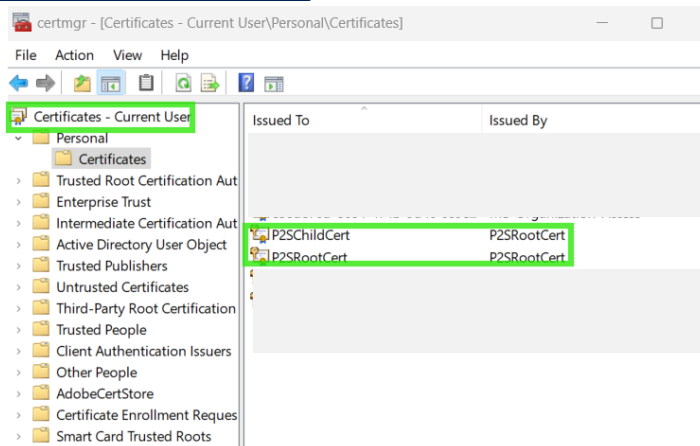
```
PS C:\Windows\system32> $params = @{
    Type = 'Custom'
    Subject = 'CN=P2SRootCert'
    KeySpec = 'Signature'
    KeyExportPolicy = 'Exportable'
    KeyUsage = 'CertSign'
    KeyUsageProperty = 'Sign'
    KeyLength = 2048
    HashAlgorithm = 'sha256'
    CertStoreLocation = 'Cert:\CurrentUser\My'
}
$cert = New-SelfSignedCertificate @params
PS C:\Windows\system32>
```

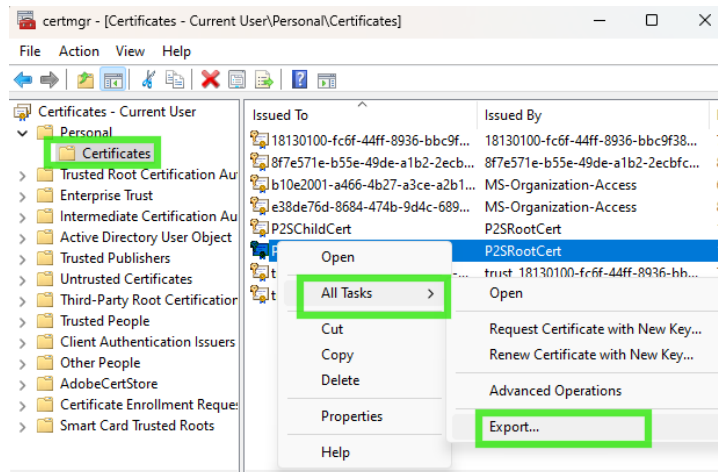
```
KeySpec = 'Signature'
KeyExportPolicy = 'Exportable'
KeyLength = 2048
HashAlgorithm = 'sha256'
CertStoreLocation = 'Cert:\CurrentUser\My'
Signer = $cert
TextExtension = @(
    '2.5.29.37={text}1.3.6.1.5.5.7.3.2')
}
New-SelfSignedCertificate @params

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

Thumbprint Subject
DAACCBED5925558387B7D38956694E0D344EBE7E CN=P2SChildCert

PS C:\Windows\system32> |
```





### Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next Cancel

#### Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

- ☐ Yes, export the private key  
☒ No, do not export the private key

Next

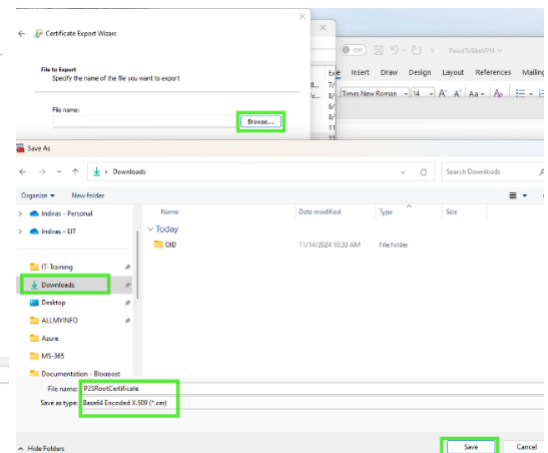
#### Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ☐ DER encoded binary X.509 (.CER)  
☒ Base-64 encoded X.509 (.CER)  
☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)  
☐ Include all certificates in the certification path if possible  
☐ Personal Information Exchange - PKCS #12 (.PFX)  
☐ Include all certificates in the certification path if possible  
☐ Delete the private key if the export is successful  
☐ Export all extended properties  
☐ Enable certificate privacy  
☐ Microsoft Serialized Certificate Store (.SST)

Next Cancel



Save Cancel

#### File to Export

Specify the name of the file you want to export

File name:  
 C:\Users\khatr\Downloads\P2SRootCertificate.cer

Next

Cancel

### Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\khatr\Downloads\P2SRootCertificate.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

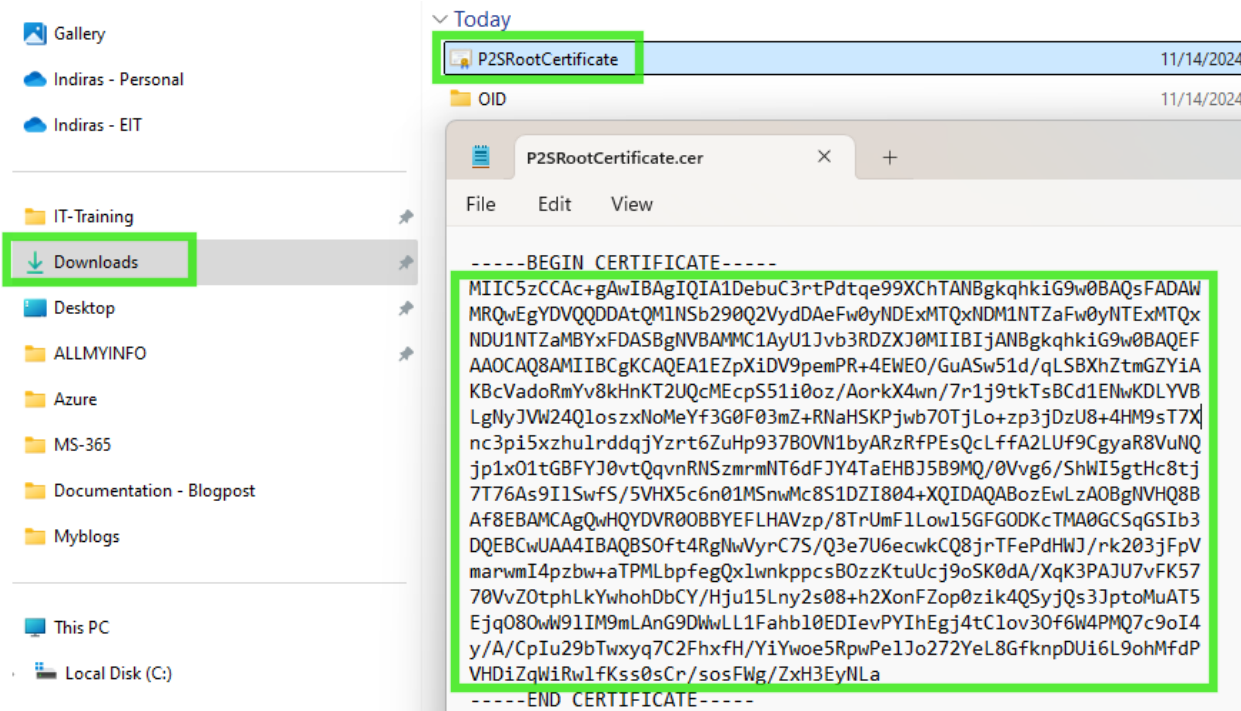
Finish

### Certificate Export Wizard

The export was successful.

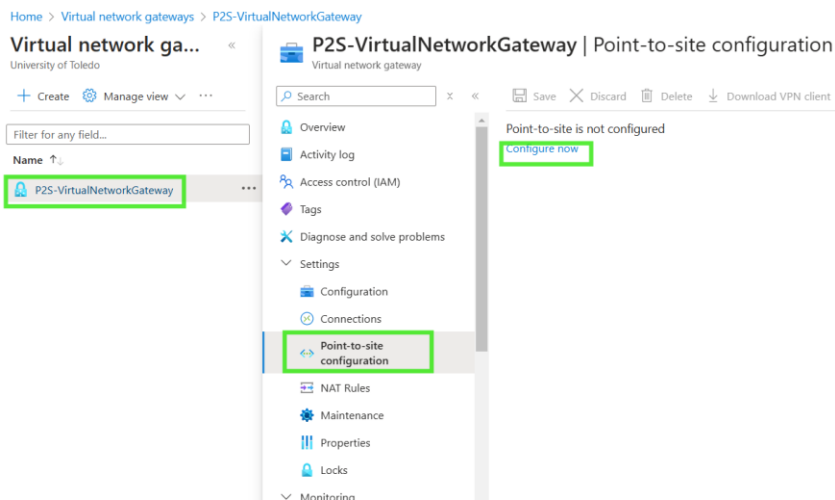
OK

## 6.6 Open the file P2SRootCertificate from downloads folder and copy it



## Step 7: Configuration of Virtual Network Gateway

- 7.1 After the deployment completion go to the virtual network gateway configuration page
- 7.2 Click on previously created virtual network gateway (e.g., P2S-VirtualNetworkGateway)
- 7.3 In setting click on Point-to-site configuration and then click on *Configure now*
- 7.4 Assign non-overlapping address pool with virtual network IP (client will get IP from this)
- 7.5 Select all requirements such as tunnel, Authentication type, etc.
- 7.6 Copy the content of root certificate (shown in step 6) to public certificate data and save
- 7.7 After saving the configuration, download from *Download VPN client*



Home &gt; Virtual network gateways &gt; P2S-VirtualNetworkGateway

## P2S-VirtualNetworkGateway | 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  
Settings  
Configuration  
Connections  
Point-to-site configuration  
NAT Rules  
Maintenance  
Properties  
Locks

Address pool \*

172.168.1.0/24

Tunnel type

IKEv2 and SSTP (SSL)

IPsec / IKE policy

Default Custom

Authentication type

Azure certificate

Root certificates

Name	Public certificate data
P2SRootCertificate	MIIC5zCCAc+gAwIBAgIQIA1D...

After saving download from here

Copy the content here

7.8 Run the file *VpnClientSetupAmd64* from the downloaded folder and install it

Downloads > P2S-VirtualNetworkGateway > WindowsAmd64

VpnClientSetupAmd64

Double click

Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: VpnClientSetupAmd64.exe  
Publisher: Unknown publisher

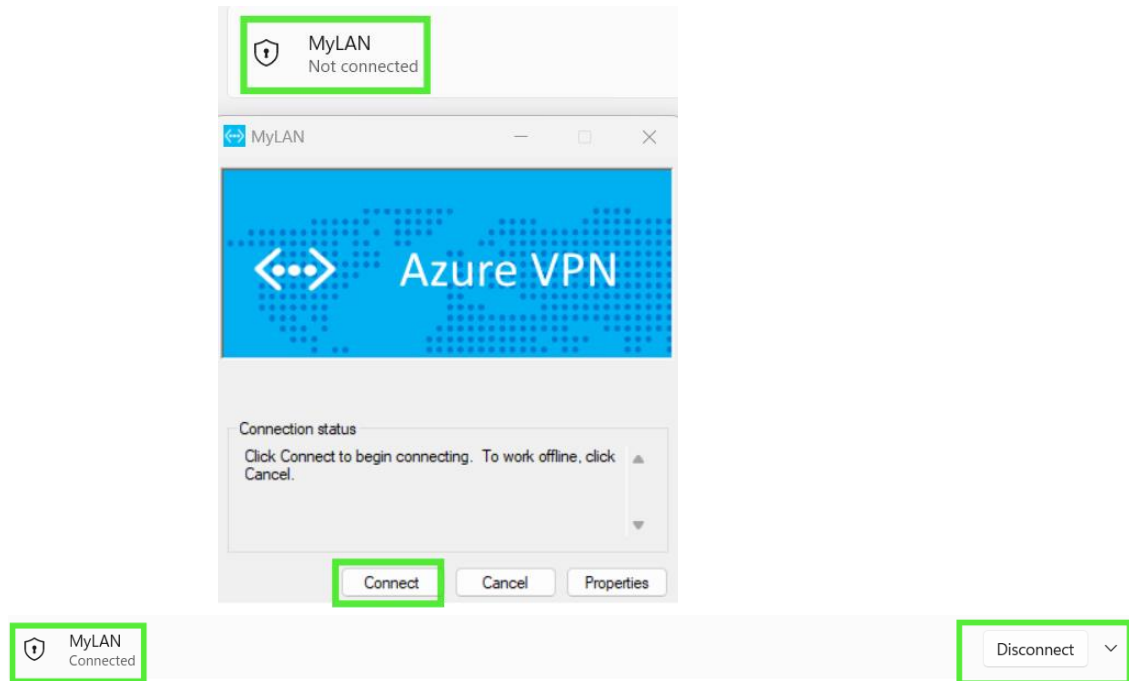
Run anyway Don't run

MyLAN

Do you wish to install a Vpn Client for MyLAN?

Yes No

7.9 After the installation connect to the VPN (e.g., MyLAN)



## Step 8: Create a Virtual Machine

8.1 Navigate to *Virtual machines* and click on *Create* to add a virtual machine

8.2 Fill out all the required details (e.g., Window Server 2022, etc.)

8.3 Click *Review + create* to create a new virtual machine

[Home](#) > [Virtual machines](#) >

### Create a virtual machine ...

[Help me create a low cost VM](#) [Help me create a VM optimized for high availability](#) [Help me choose the right VM size for my workload](#)

**Basics** | [Disks](#) | [Networking](#) | [Management](#) | [Monitoring](#) | [Advanced](#) | [Tags](#) | [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**i** This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

#### 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 For Learning ▼  
 Resource group \* ⓘ ResourceLearning ▼  
[Create new](#)

#### Instance details

Virtual machine name \* ⓘ DC ✓  
 Region \* ⓘ (US) East US ▼



Availability options ⓘ No infrastructure redundancy required ✓

Security type ⓘ Trusted launch virtual machines ✓  
[Configure security features](#)

Image \* ⓘ Windows Server 2022 Datacenter: Azure Edition Hotpatch - x64 Gen2 (free) ✓  
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ  
☐ Arm64  
☒ x64  
ⓘ Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ ☐

ⓘ You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription.  
[Learn more](#)

Size \* ⓘ Standard\_DC1s\_v3 - 1 vcpu, 8 GiB memory (\$103.66/month) ✓

Enable Hibernation ⓘ ☐  
ⓘ Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

### Administrator account

Username \* ⓘ ikhatri ✓

Password \* ..... ✓

Confirm password \* ..... ✓

### Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ⓘ ☐ None  
☒ Allow selected ports

Select inbound ports \* RDP (3389) ✓

ⓘ All traffic from the internet will be blocked by default. You will be able to

[< Previous](#) [Next : Disks >](#) [Review + create](#)

**OS disk**

OS disk size ⓘ	<div>Image default (127 GiB) ▼</div>
OS disk type * ⓘ	<div>Premium SSD (locally-redundant storage) ▼</div>
Delete with VM ⓘ	<input checked="" type="checkbox"/>
Key management ⓘ	<div>Platform-managed key ▼</div>
Enable Ultra Disk compatibility ⓘ	<div><input type="checkbox"/> Ultra disk is supported in Availability Zone(s) 2 for the selected VM size Standard_DC1s_v3.</div>

**Data disks for DC**

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM ⓘ
<div><a href="#">Create and attach a new disk</a> <a href="#">Attach an existing disk</a></div>					

▼ **Advanced**

[< Previous](#) [Next : Networking >](#) [Review + create](#)

Basics   Disks   **Networking**   Management   Monitoring   Advanced   Tags   Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#) ↗

**Network interface**

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ	<div>MyLAN ▼</div> <a href="#">Create new</a>
Subnet * ⓘ	<div>Virginia (192.168.5.0/24) ▼</div> <a href="#">Manage subnet configuration</a>
Public IP ⓘ	<div>(new) DC-ip ▼</div> <a href="#">Create new</a>
NIC network security group ⓘ	<div><input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced</div>

Public inbound ports \* ⓘ ☐ None ☒ Allow selected ports

Select inbound ports \*

**⚠ This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted ⓘ ☐

Enable accelerated networking ⓘ ☒

**Load balancing**

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options ⓘ ☒ None ☐ Azure load balancer  
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.

[< Previous](#) [Next : Management >](#) [Review + create](#)

**Virtual machines** ⓘ ...

University of Toledo

+ Create ▾ Switch to classic ⓘ Reservations ▾ Manage view ▾ Refresh ⬇ Export to CSV 🔗 Open query ⓘ Assign tags ▶ Start ⌂ Restart ☐ Stop ⓘ

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

Showing 1 to 1 of 1 records.

☐ Name ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	Status ↑↓	Operating system ↑↓	Size ↑↓
☐ DC	Azure For Learning	RESOURCELEARNING	East US	Running	Windows	Standard_DC1s_v3

## 8.4 Change the private IP address from dynamic to static by clicking *ipconfig 1*

Home > DC

**DC | Network settings** ☆ ...

Virtual machine

Search

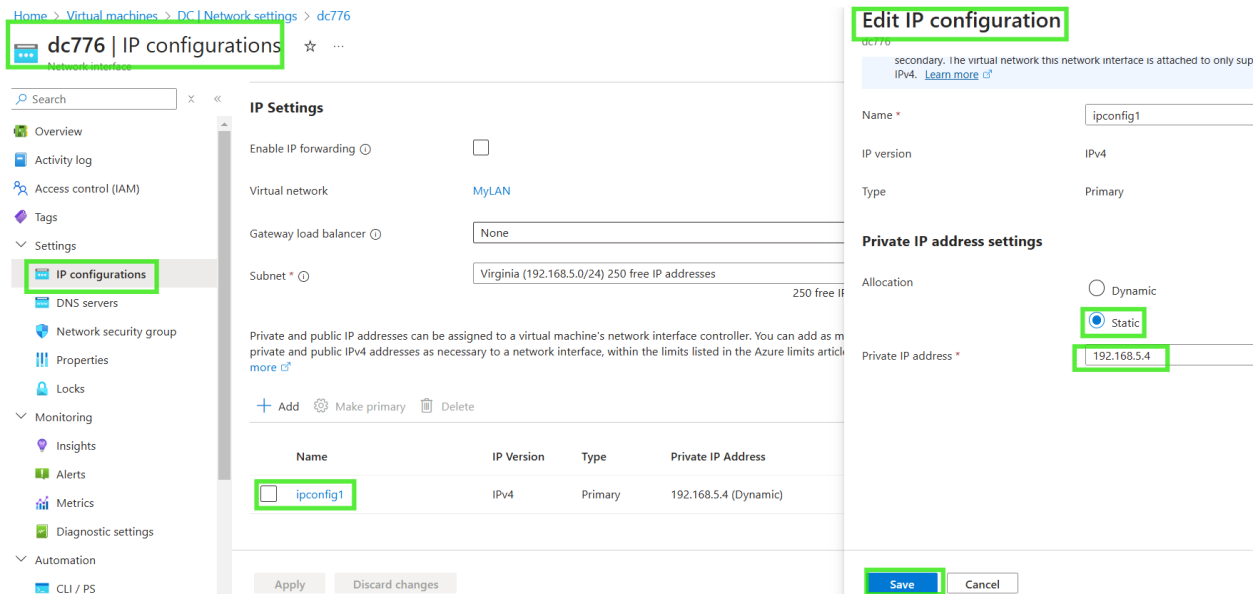
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
  - Connect
  - Bastion
  - Windows Admin Center
- Networking**
  - Network settings**

This is a new experience. [Please provide feedback](#)

List all my network interfaces for DC. What are the requirements?

Attach network interface Detach network interface

Network interface / IP configuration  
**dc776 (primary) / ipconfig1 (primary)**



## Step 9: Testing the connection

9.1 Open the command prompt in your PC and ping to private IP address of VM

```
C:\Users\khatr>ping 192.168.5.4

Pinging 192.168.5.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

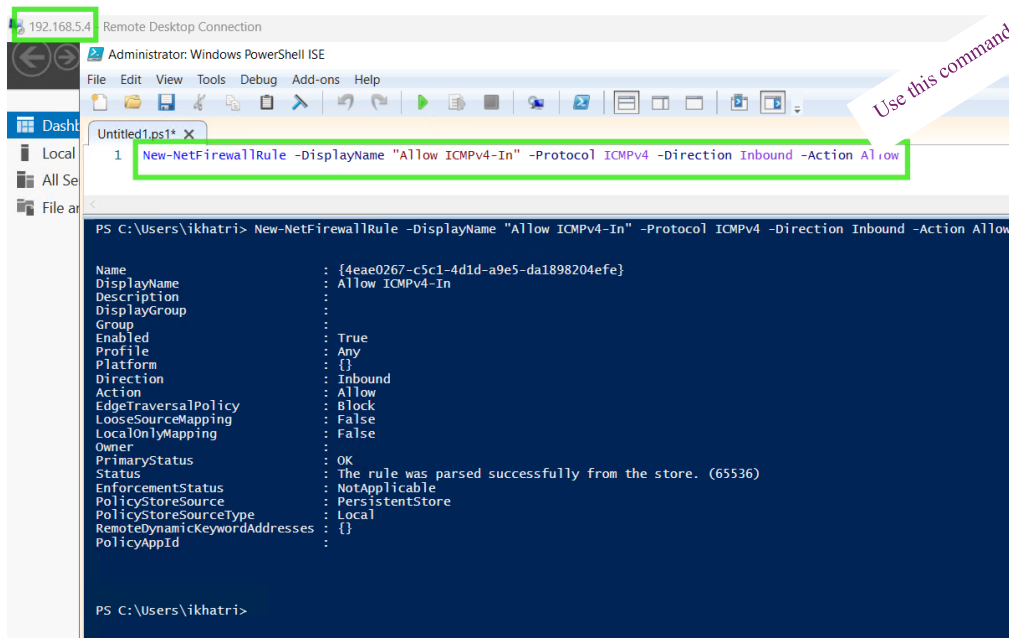
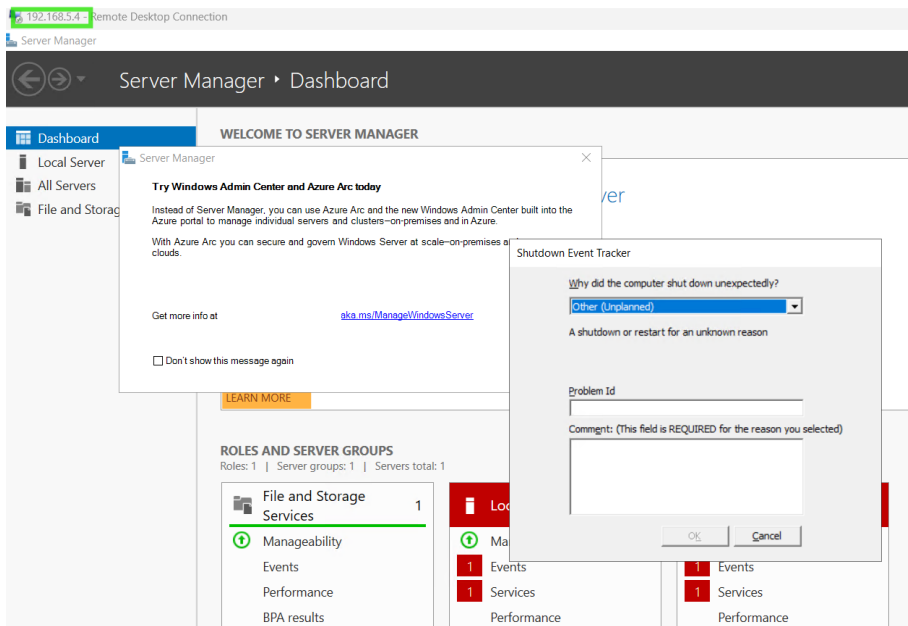
Ping statistics for 192.168.5.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\khatr>
```

9.2 Create the inbound firewall rule in VM using following steps and command

9.3 Establish a Remote Desktop Connection from your PC to the VM

9.4 Execute the following command in PowerShell on the VM to create firewall rule

9.5 Open the command prompt on your PC again and ping the private IP address of VM



```
C:\Users\khatri> ping 192.168.5.4
```

```
Pinging 192.168.5.4 with 32 bytes of data:
Reply from 192.168.5.4: bytes=32 time=11ms TTL=128
Reply from 192.168.5.4: bytes=32 time=14ms TTL=128
Reply from 192.168.5.4: bytes=32 time=19ms TTL=128
Reply from 192.168.5.4: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.5.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 19ms, Average = 15ms
```

## Conclusions

A Point-to-Site VPN connection to Azure provides secure, remote access for individual devices to an Azure Virtual Network, enabling users to connect to cloud resources as if they were on a local network. It's a simple, cost-effective solution for remote workers or small teams needing secure access to Azure resources.

### Note

1. For optimal results, it's usually best to keep your VM and VPN gateway in the same region, reducing latency and avoiding cross-region data transfer fees.
2. Proper configuration of address spaces, security rules, and firewall settings will ensure a seamless and secure remote connection to your Azure environment.

Thank you for reading. I hope it was useful

Author: Indiras Khatri

\*\*\*\*\*