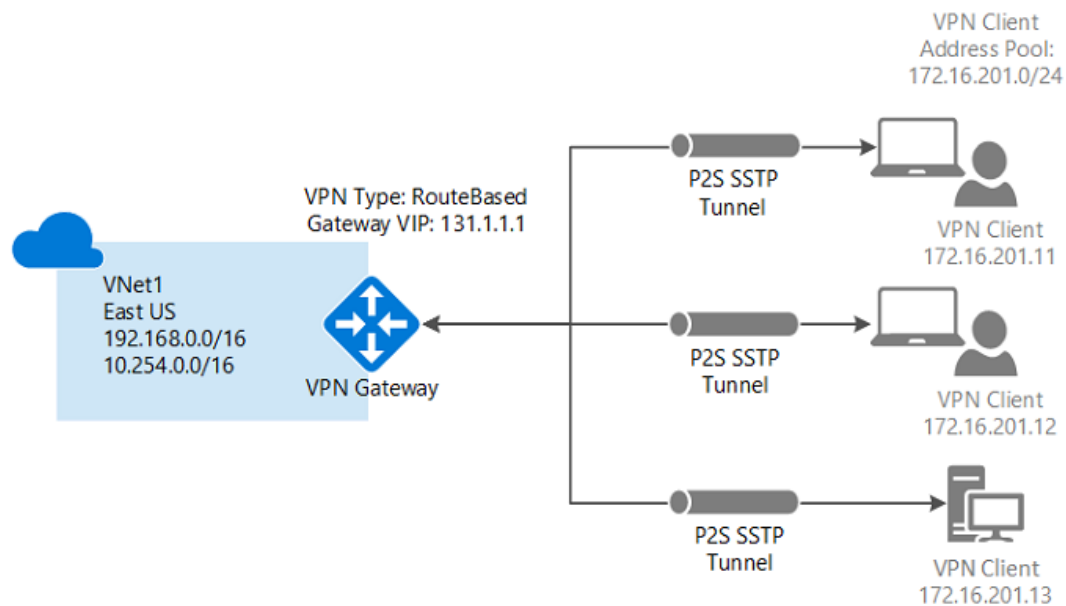



Setting up Point to Site connectivity in Azure Virtual Network




A Point-to-Site (P2S) configuration lets you create a secure connection from an individual client computer to a virtual network. P2S is a VPN connection over SSTP (Secure Socket Tunneling Protocol). Point-to-Site connections are useful when you want to connect to your VNet from a remote location, such as from home or a conference, or when you only have a few clients that need to connect to a virtual network. P2S connections do not require a VPN device or a public-facing IP address. You establish the VPN connection from the client computer.



Steps to Create Point to Site Connection

- 1) Create a new Resource group
Name: **HybridCloudResourceGroup**
Location: **SouthEast Asia**

Open Azure Portal click on the  icon. Click on the Add button to add a new resource group

+ Add Columns Refresh	
Subscriptions: Developer Program Benefit – Don't see a subscription? Switch directories	
Filter by name...	
3 items	
NAME ▾	SUBSCRIPTION ▾
 [REDACTED]	Developer Program Benefit
 [REDACTED]	Developer Program Benefit
 [REDACTED]	Developer Program Benefit

Enter the name, subscription and location and click on the create button.

Resource group

Create an empty resource group

*

Resource group name

HybridCloudResourceGroup

✓

*

Subscription

Developer Program Benefit

▾

*

Resource group location

Southeast Asia

▾

☒

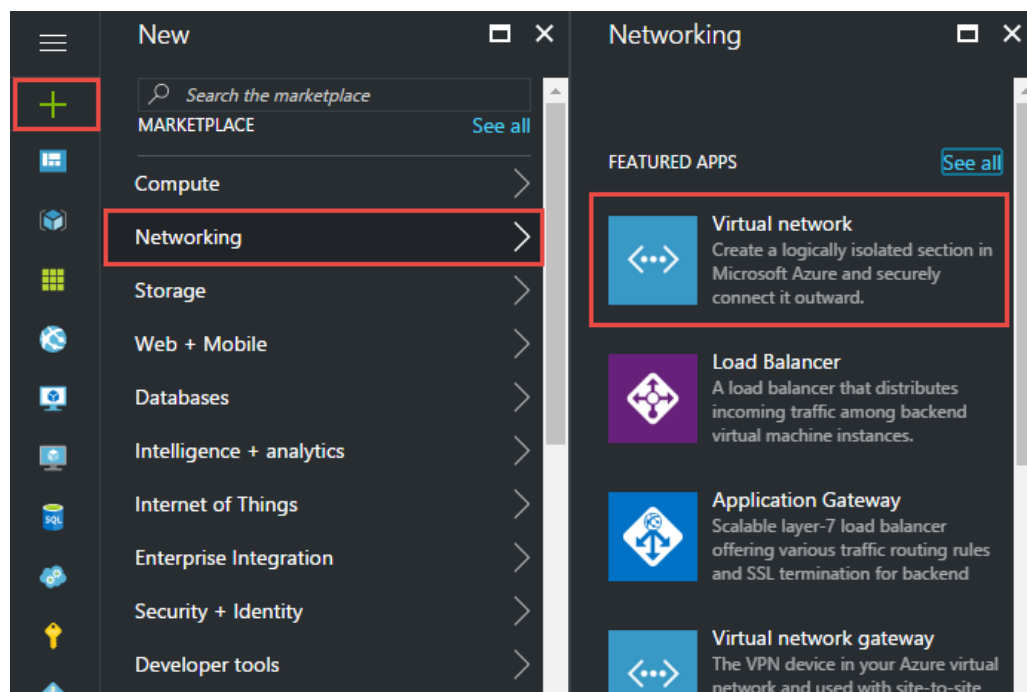
Pin to dashboard

Create

- 2) Create your first VNET in the resource group with one or more subnets, in this demo we are going to create two subnets in each Virtual network.

Virtual Network Name	AzureSite	
VNET Address space	10.11.0.0/16	
Location	SouthEast Asia	
Subnet 1	Name	FrontEnd
	Subnet address range	10.11.0.0/24
Gateway subnet	Name	Gateway subnet(default)
	Address range	10.11.2.0/27

To create the virtual network, click on the  icon and select '**Virtual network**' from the '**Networking**' services category



Specify the Virtual network name, Address space, subnet name, Subnet address range, subscription, resource group and location. Click on the 'Pin to Dashboard' check box to add the shortcut to the dashboard.

Create virtual network

* Name
AzureSite ✓

* Address space ⓘ
10.11.0.0/16 ✓
10.11.0.0 - 10.11.255.255 (65536 addresses)

* Subnet name
FrontEnd ✓

* Subnet address range ⓘ
10.11.0.0/24 ✓
10.11.0.0 - 10.11.0.255 (256 addresses)

* Subscription
Developer Program Benefit ▼

* Resource group ⓘ
☐ Create new ☒ Use existing
HybridCloudResourceGroup ▼

* Location
Southeast Asia ▼

☐ Pin to dashboard

Create [Automation options](#)

It creates your '**AzureSite**' with a subnet named '**FrontEnd**'.

- 3) You can add more subnets to the '**AzureSite**' VNET. For this demo we are using only one subnet called '**FrontEnd**'. To add more subnets, open settings blade of the **AzureSite** and select subnets. Click on the '**+Subnet**' button to add more subnets.
- 4) Now, we need to add a Gateway subnet to the VNET. To add a '**Gateway subnet**', select **subnets** from the settings blade of the '**AzureSite**' VNET. Click on the '**+ Gateway Subnet**' and specify the address range for the Gateway subnet.

Add subnet

AzureSite

*

Name

GatewaySubnet

*

Address range (CIDR block)

10.11.2.0/27

10.11.2.0 - 10.11.2.31 (32 addresses)

Route table

None

OK

5) You can now see the Gateway subnet is added to the 'AzureSite'.

+ Subnet + Gateway subnet			
Search subnets			
NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	
FrontEnd	10.11.0.0/24	251	
GatewaySubnet	10.11.2.0/27	27	

6) We need to create a **Virtual Network Gateway** to connect your client machine to the 'AzureSite' VNET.

Create virtual network gateway..

* Name
AzureSiteGateway ✓

Gateway type ⓘ
VPN ExpressRoute

VPN type ⓘ
Route-based Policy-based

* SKU ⓘ
Standard ▼

* Virtual network ⓘ
AzureSite >

* Public IP address ⓘ
(new) AzureSiteGatewayPublicIP >

* Subscription
Developer Program Benefit ▼

☐ Pin to dashboard

Create Automation options

Provisioning a virtual network gateway may take up to 45 minutes.

Configuring Certificates for Point-to-Site Connection

Certificates are used by Azure to authenticate VPN clients for Point-to-Site VPNs. After creating the root certificate, you export the public certificate data (not the private key) as a Base-64 encoded X.509 .cer file. You then upload the public certificate data from the root certificate to Azure. Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. The client certificate is generated from the root certificate and installed on each client computer. If a valid client certificate is not installed and the client tries to connect to the VNet, authentication fails.

If you are using enterprise solution you can use the existing enterprise certificate chain. But if you are not using enterprise solution, you can use a self-signed certificate to create the root certificate.

Create Root Certificates

NOTE: You can download the PowerShell scripts for creating certificates in Windows 10 machines from the following link

https://github.com/sonusathyadas/Azure-documents/blob/master/P2S_Certificates_PSScripts.zip

For Windows 10 Machines

Open PowerShell with administrative privileges. Execute the following command to generate the certificate. The certificate will be automatically installed in the '**Certificates-Current User\Personal\Certificates**' location.

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

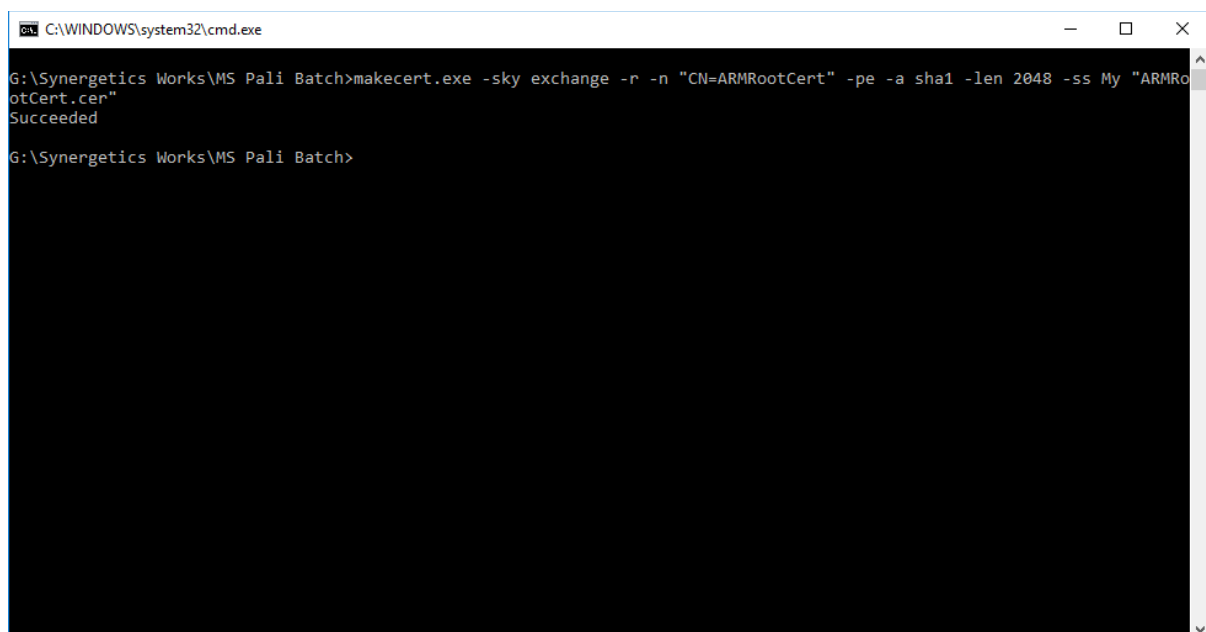
Other Windows Machines

Open local machine and navigate to the folder where makecert.exe is located

Execute the following command in command window to create a root certificate

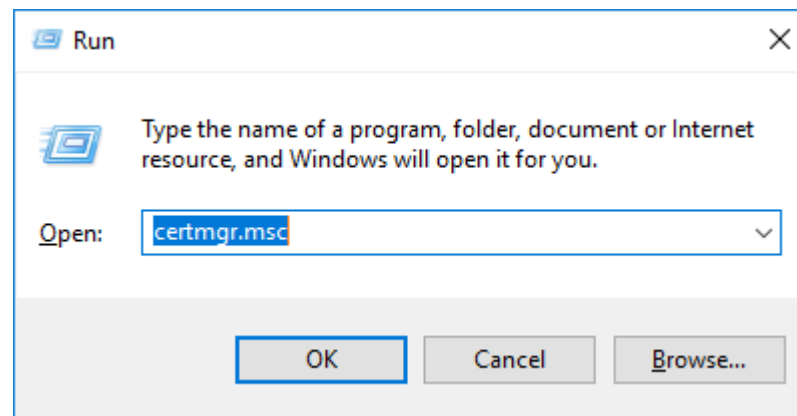
```
makecert.exe -sky exchange -r -n "CN=P2SRootCert" -pe -a sha1 -len 2048 -ss My  
"P2SRootCert.cer"
```

This will create and install a root certificate in the '**Certificates-Current User\Personal\Certificates**' location.

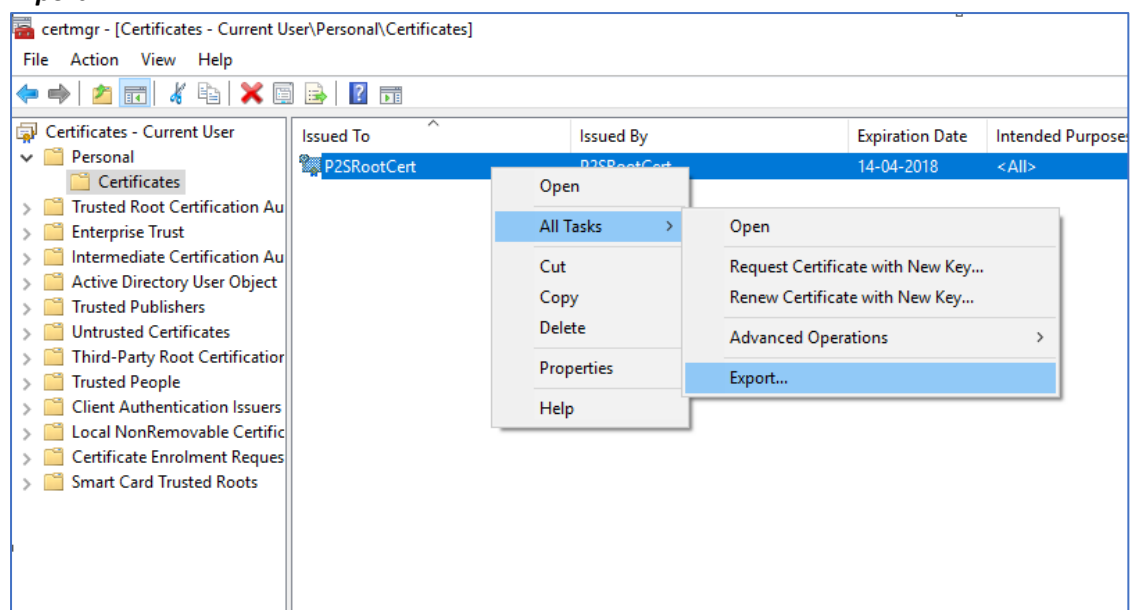


Export the Root certificate

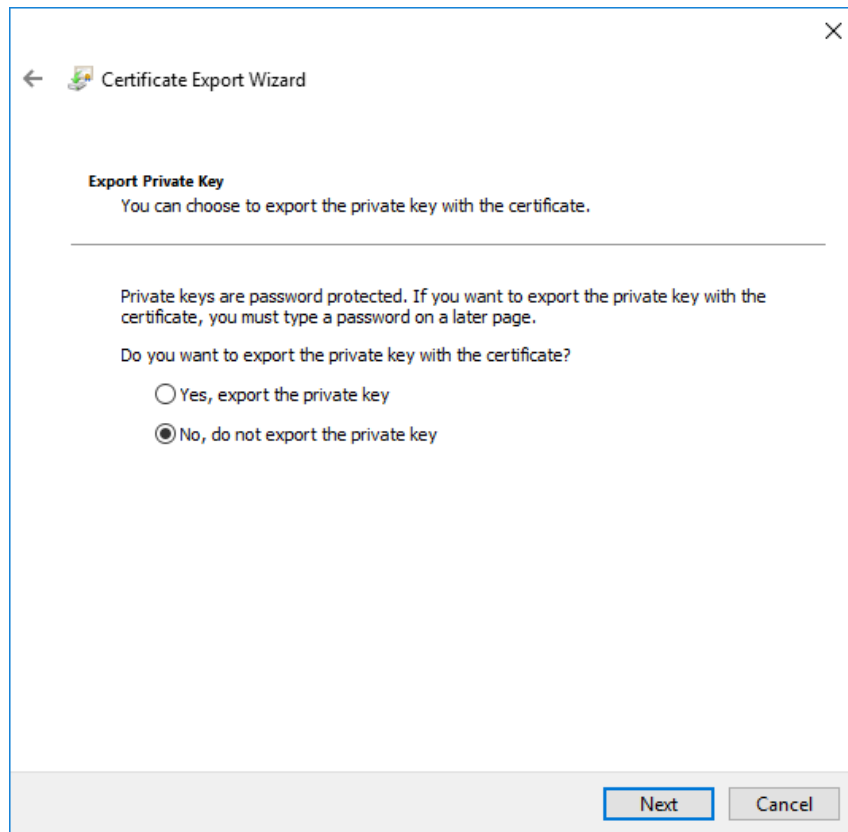
- 7) Now you need to export the public key for the root certificate. To do so open Run command and execute certmgr.msc.



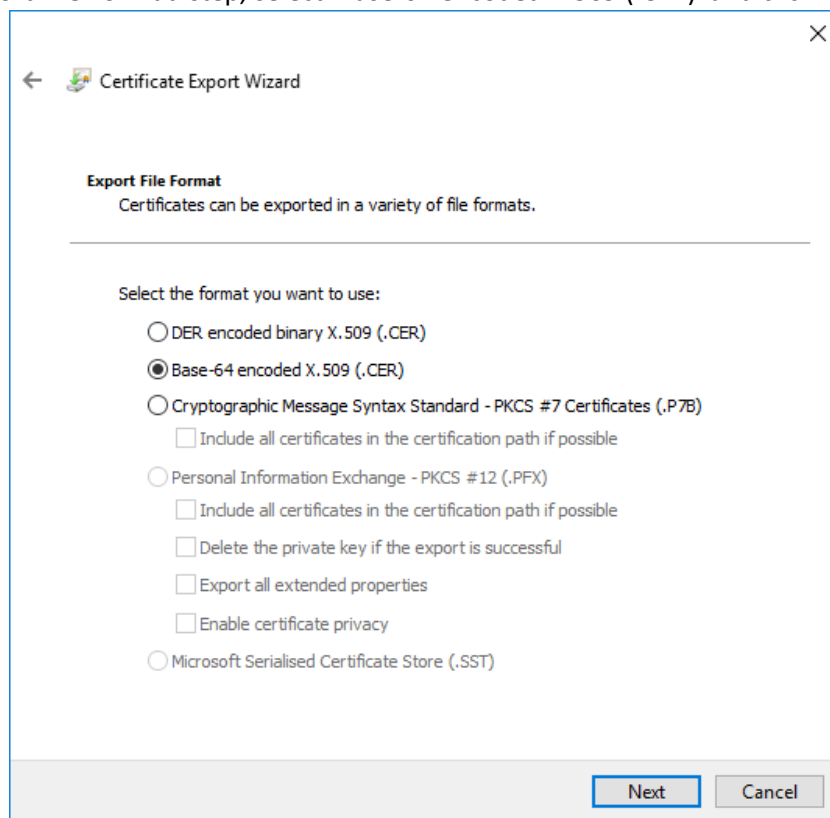
- 8) It opens the Certification Manager window. Expand **Certificates-Current User > Personal > Certificates** node. Select your certificate (**P2SRootCert**), Right click and select **All Tasks > Export**.



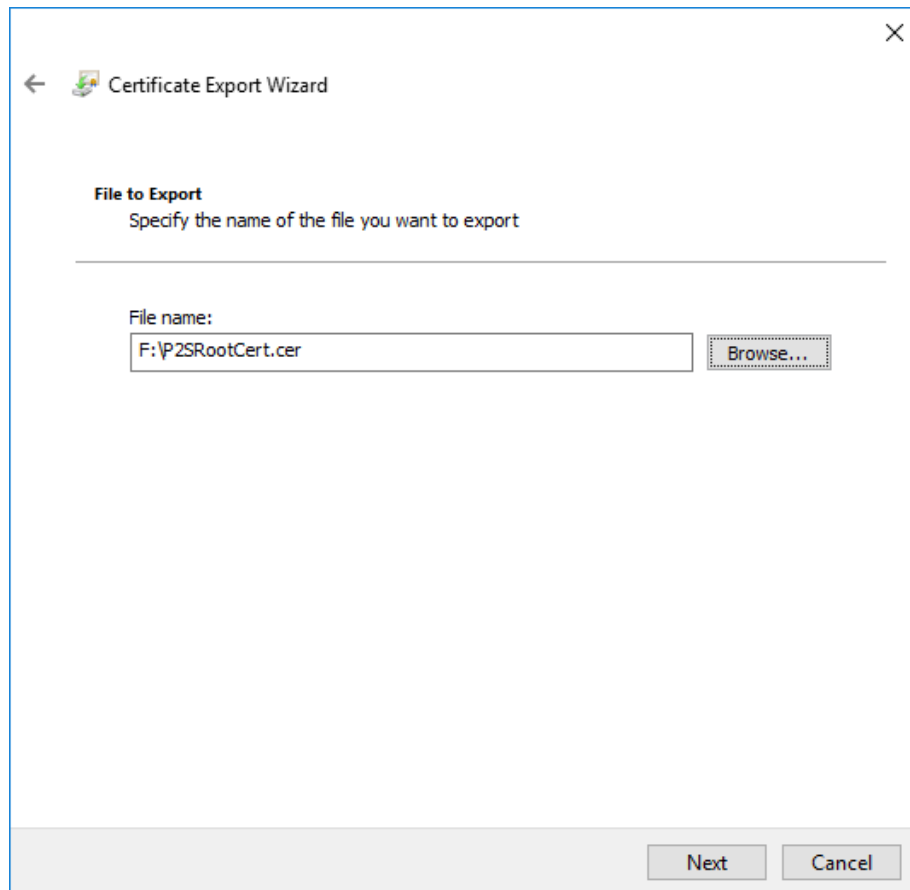
- 9) In the **Certificate Export Wizard** Window, Click Next. You will be moved to the 'Export Private Key' step. Select '**No, do not export private key**' option and click Next.



10) In the 'Export File Format' step, select 'Base-64 encoded X-509 (.CER)' and click Next.



11) In the '**File to export**' step, specify the location and name of the certificate file. You can specify the file name as '**P2SRootCert.cer**'



12) Validate and click on the Finish button to export the certificate.

Generate client certificate

Now, we need to create and install certificates for client machines. You can use unique certificates for each client, or same certificate for all clients. Unique certificate for each client is a better approach because if you want to revoke the access from the client, you can easily do it with unique certificates. But if you use same certificate for all clients, and if you need to revoke access from a client you need to remove the existing certificate and regenerate new certificate and install in all client machines.

Enterprise certificate

- If you are using an enterprise certificate solution, generate a client certificate with the common name value format 'name@yourdomain.com', rather than the 'domain name\username' format.
- Make sure the client certificate is based on the 'User' certificate template that has 'Client Authentication' as the first item in the use list, rather than Smart Card Logon, etc. You can check the certificate by double-clicking the client certificate and viewing Details > Enhanced Key Usage.

Self-signed root certificate

If you are using a self-signed root certificate you can create a self-signed certificate using PowerShell. You generate a client certificate from the self-signed root certificate, and then export

and install the client certificate. To do so open the PowerShell window with administrative privilege and execute the following command.

For Windows 10 Clients

The following Commands will work only in Windows 10, The below mentioned commands are specific to Windows 10, no PowerShell commands.

```
#List the installed certificates and its thumbprints
Get-ChildItem -Path "Cert:\CurrentUser\My"

#Get the certificate reference using the thumbprint
#$cert = Get-ChildItem -Path "Cert:\CurrentUser\My\<Cert thumbprint>"
$cert = Get-ChildItem -Path "Cert:\CurrentUser\My\<paste thumbprint
here>"

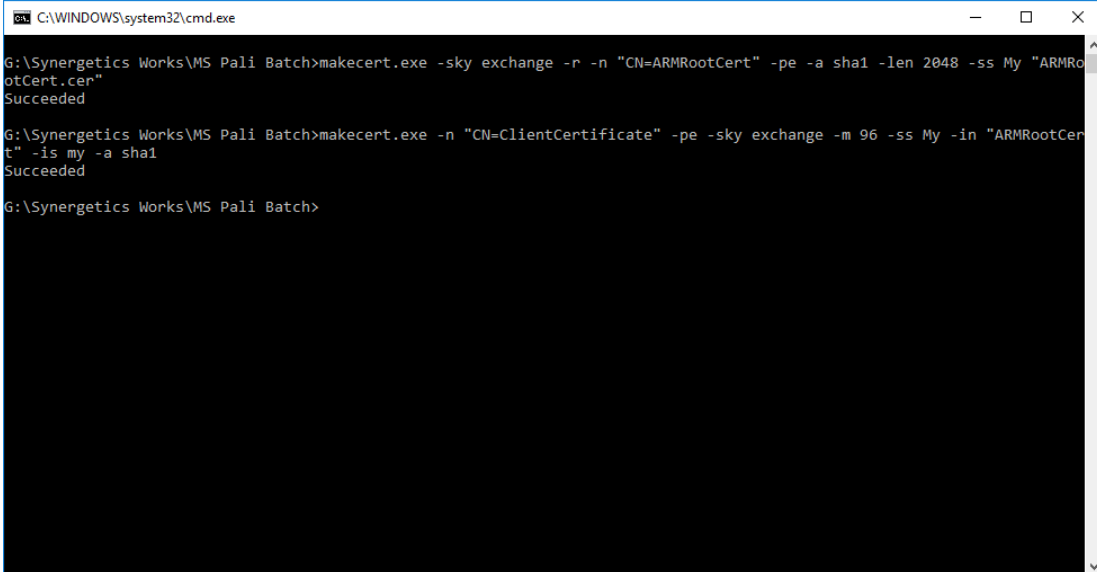
#Create and Install a child certificate
New-SelfSignedCertificate -Type Custom `
    -KeySpec Signature `
    -Subject "CN=P2SChildCert" `
    -KeyExportPolicy Exportable `
    -HashAlgorithm sha256 `
    -KeyLength 2048 `
    -CertStoreLocation "Cert:\CurrentUser\My" `
    -Signer $cert `
    -TextExtension @( "2.5.29.37={text}1.3.6.1.5.5.7.3.2" )
```

For Other Windows Clients

To create a client certificate, open the command window and execute the following command to create a client certificate.

makecert.exe -n "CN= P2SChildCert " -pe -sky exchange -m 96 -ss My -in "P2SRootCert" -is my -a sha1

[Note: Name of the certificate can be anything it should be validating against the server certificate, So you need to specify the same name of the server certificate , eg: here it is **P2SRootCert**]



```
C:\WINDOWS\system32\cmd.exe

G:\Synergetics Works\MS Pali Batch>makecert.exe -sky exchange -r -n "CN=ARMRootCert" -pe -a sha1 -len 2048 -ss My "ARMRootCert.cer"
Succeeded

G:\Synergetics Works\MS Pali Batch>makecert.exe -n "CN=ClientCertificate" -pe -sky exchange -m 96 -ss My -in "ARMRootCert.cer" -is my -a sha1
Succeeded

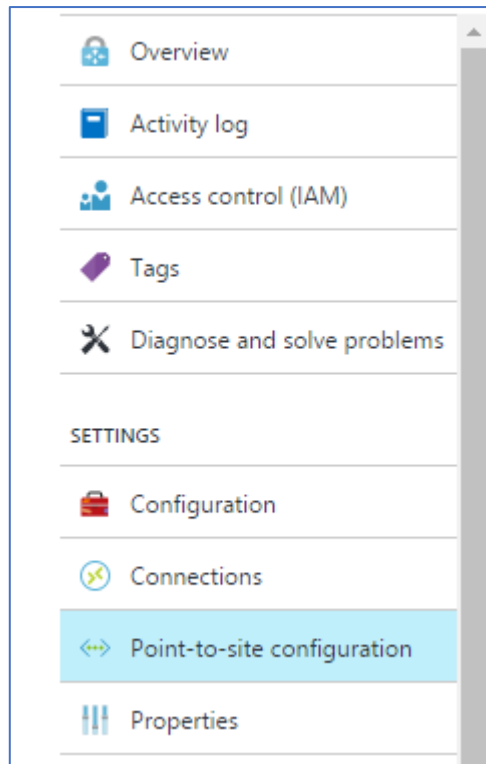
G:\Synergetics Works\MS Pali Batch>
```

Export Client certificate for other machines (optional)

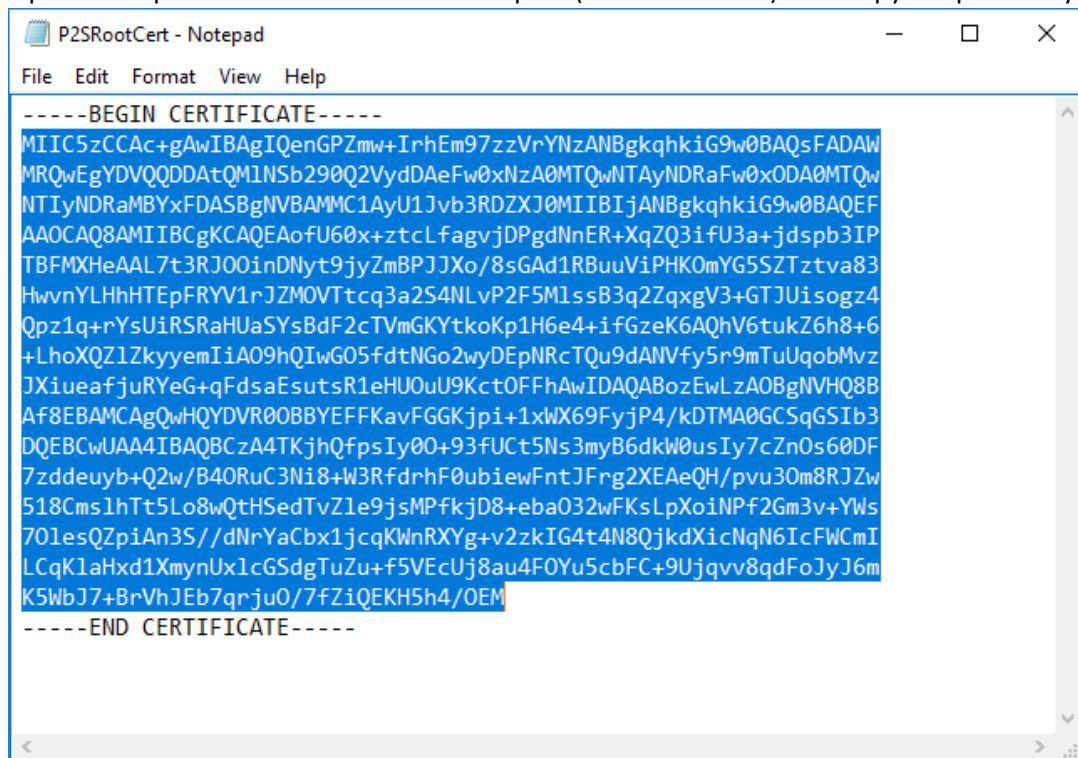
- 13) The client certificate is generated and installed in your client machine. IF you want to install the client certificate for a different machine, you need to export the certificate. For that you can follow the steps mentioned below
- To export a client certificate, open **Manage user certificates**. Right-click the client certificate that you want to export, click **all tasks**, and then click **export** to open the Certificate Export Wizard.
 - In the Wizard, click Next, then select **Yes, export the private key**, and then click Next.
 - On the Export File Format page, leave the defaults selected. Make sure **Include all certificates in the certification path if possible** is selected to also export the required root certificate information. Then, click Next.
 - On the Security page, you must protect the private key. If you select to use a password, make sure to record or remember the password that you set for this certificate. Then, click Next.
 - On the File to Export, browse to the location to which you want to export the certificate. For File name, name the certificate file. Then, click Next.
 - Click Finish to export the certificate.

Add the client to Virtual Network Gateway

- 14) To connect you client machine to the VNET, you need to add the client machine to the VNET Gateway client address pool. For that open the Virtual Network Gateway you have created. In the settings blade and select 'Point-to-Site configuration'.



- 15) Open the exported Root certificate in notepad. (P2SRootCer.cer). And copy the public key.



- 16) Enter an address pool value and paste the certificate public key in the 'Public Certificate Date' textbox and specify a valid name for the certificate. Click the Save button.

Save Discard Download VPN client

Updating...

Connection health

Connections	0
Ingress (bytes)	0
Egress (bytes)	0

Address pool

172.168.201.0/24 ✓

Root certificates

NAME	PUBLIC CERTIFICATE DATA
RootCert1	MIIC5zCCAc+gAwIBAgIQenGPZmw+lrhEm97zzVrYNzANBgkqhkiG9w0BAQwMRQwEgYDVQDD...

Revoked certificates

NAME	THUMBPRINT

Allocated IP addresses

17) Now the Download VPN client button will be enabled. Click on the button to download the VPN client.

AzureSiteGateway - Point-to-site configuration

Virtual network gateway

Search (Ctrl+/)

Save Discard Download VPN client

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Configuration

Connections

Point-to-site configuration

Properties

Locks

Connection health

Connections	0
Ingress (bytes)	0
Egress (bytes)	0

Address pool

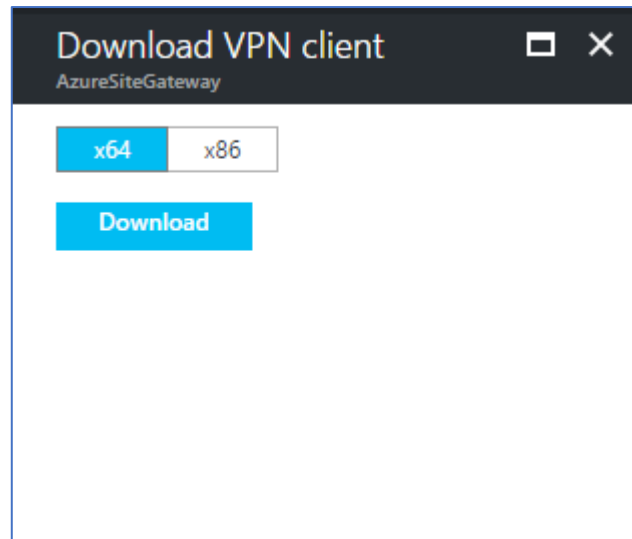
172.168.201.0/24 ✓

Root certificates

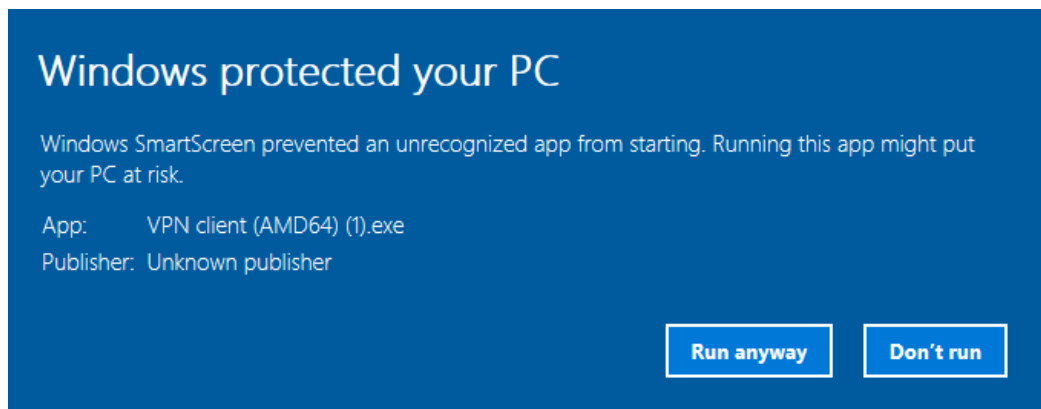
NAME	PUBLIC CERTIFICATE DATA
RootCert1	MIIC5zCCAc+gAwIBAgIQenGPZmw+lrhEm97zzVrYNzANBgkqhkiG9w0BAQwMRQwEgYDVQDD...

Revoked certificates

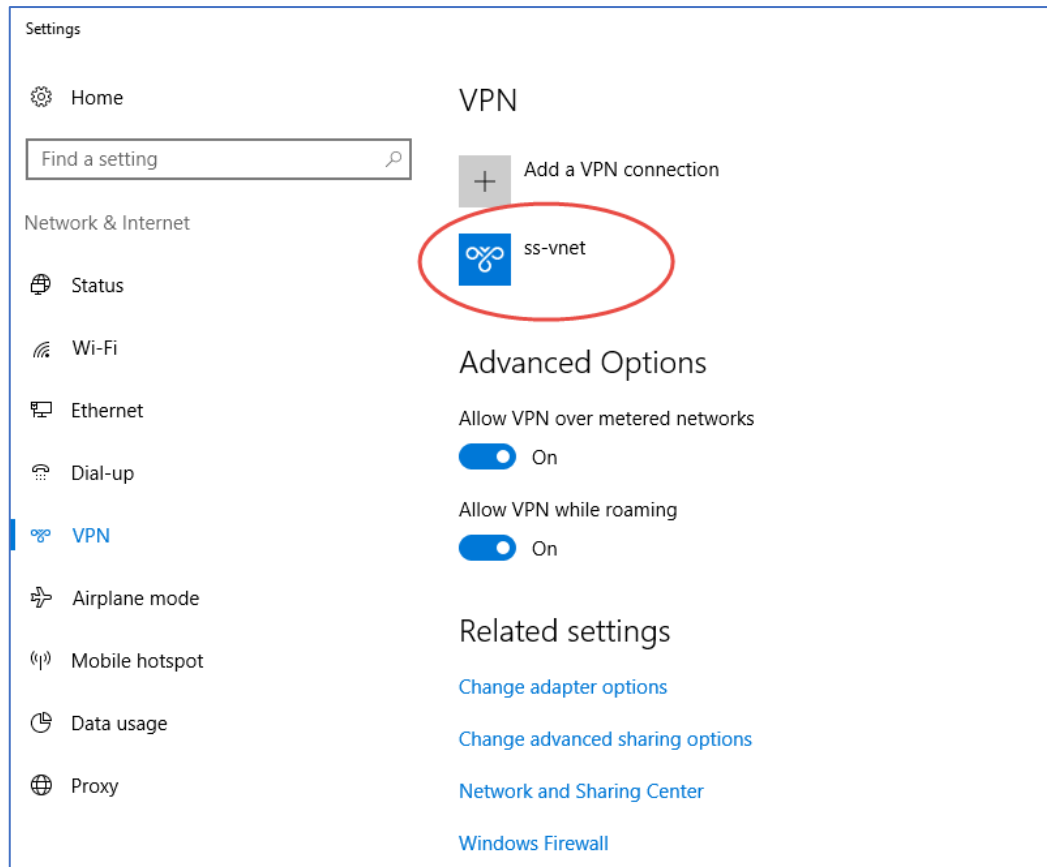
18) Click on the download button to download correct version of VPN client.



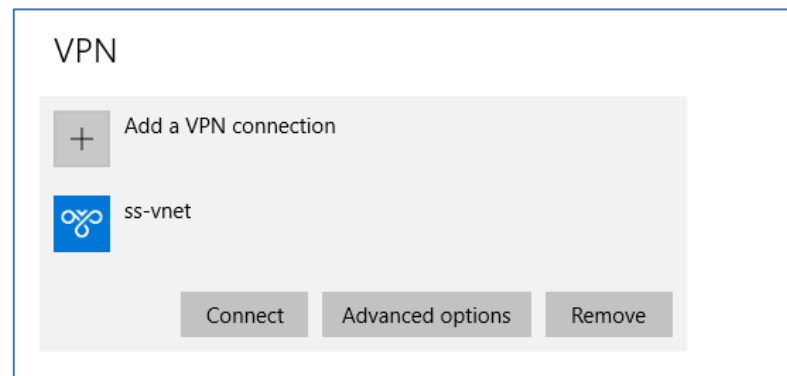
- 19) Install the client application as administrator, If it asks for confirmation click on 'Run anyway' (in windows8 or later clients).



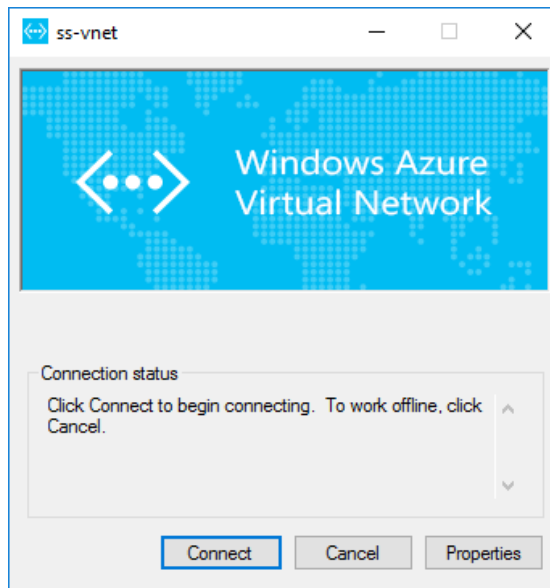
- 20) Once installation is completed you can goto the Network settings window and you can see the installed VPN client.



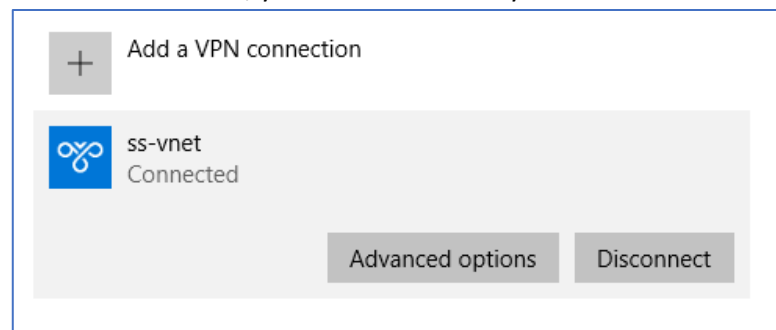
21) Click to connect to the VNET.



22) It pops up a dialog box and click on connect.



23) Once the connection is successful, you can see that the you are connected to the VNET.



24) You now goto command prompt and try **ipconfig** command to check the connectivity.

