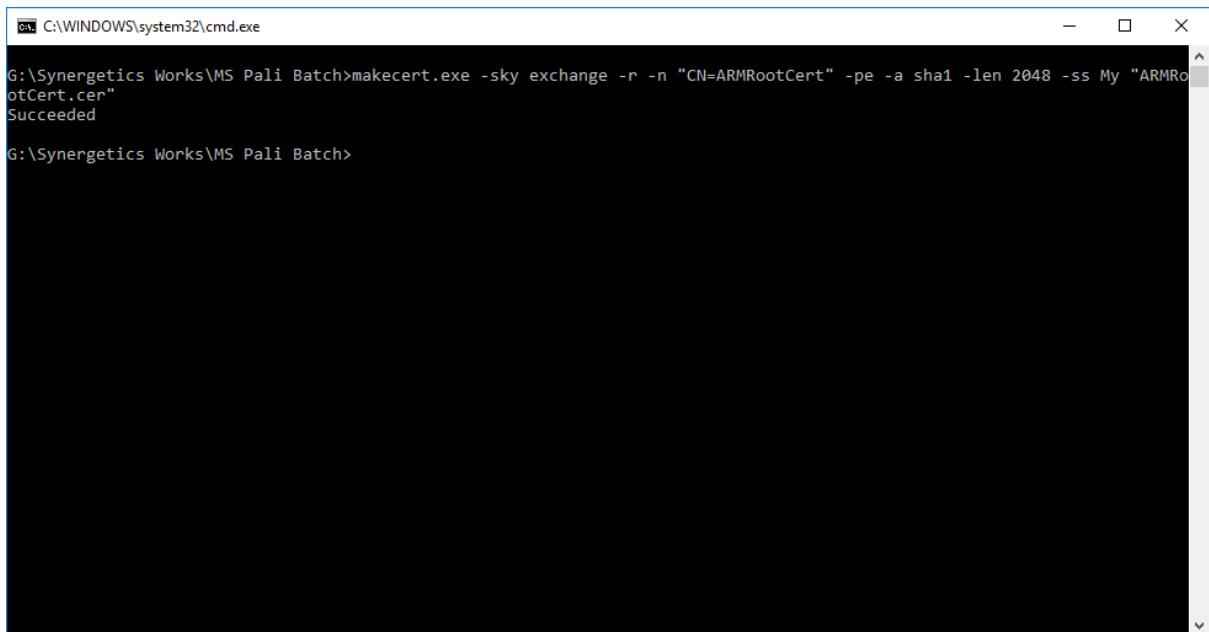


## Point to Site Demo

-----

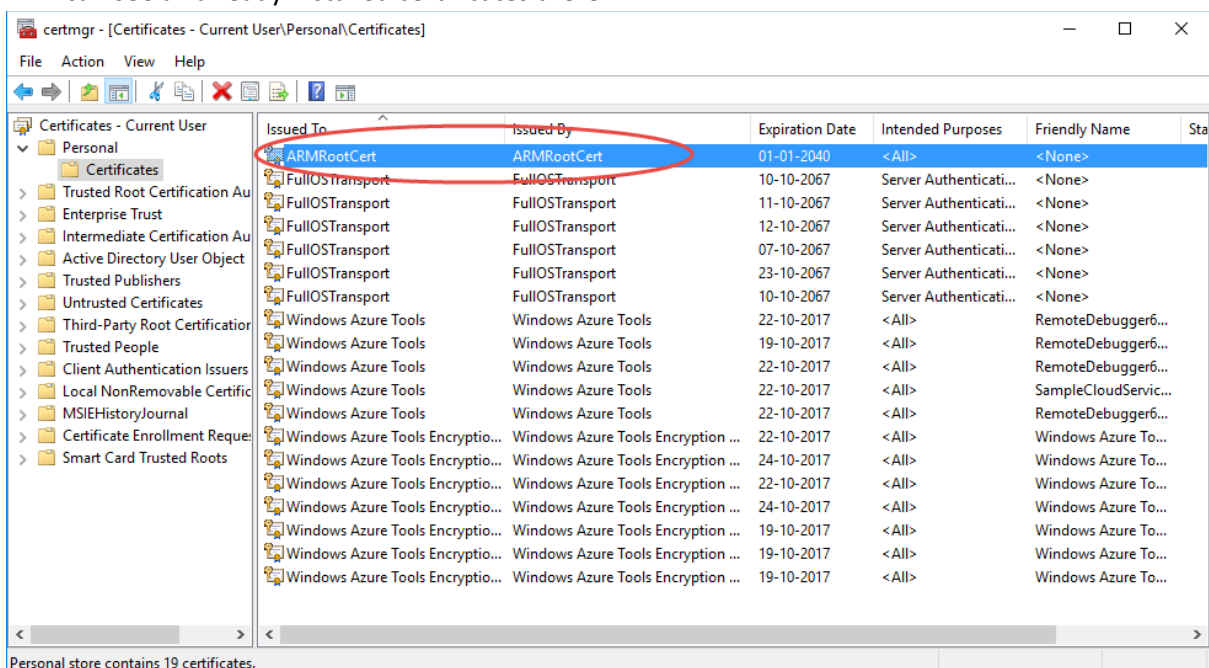
- 1) Open local machine and navigate to the folder where makecert.exe is located
- 2) Execute the following command in command window to create a root certificate

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

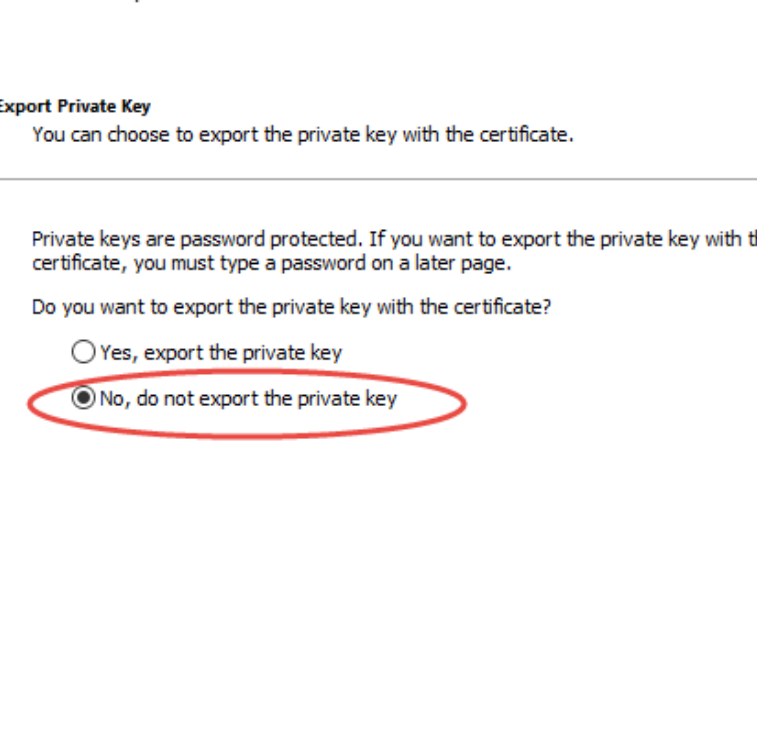



The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The command entered is: `G:\Synergetics Works\MS Pali Batch>makecert.exe -sky exchange -r -n "CN=ARMRootCert" -pe -a sha1 -len 2048 -ss My "ARMRootCert.cer"`. The output shows "Succeeded" and the prompt returns to `G:\Synergetics Works\MS Pali Batch>`.

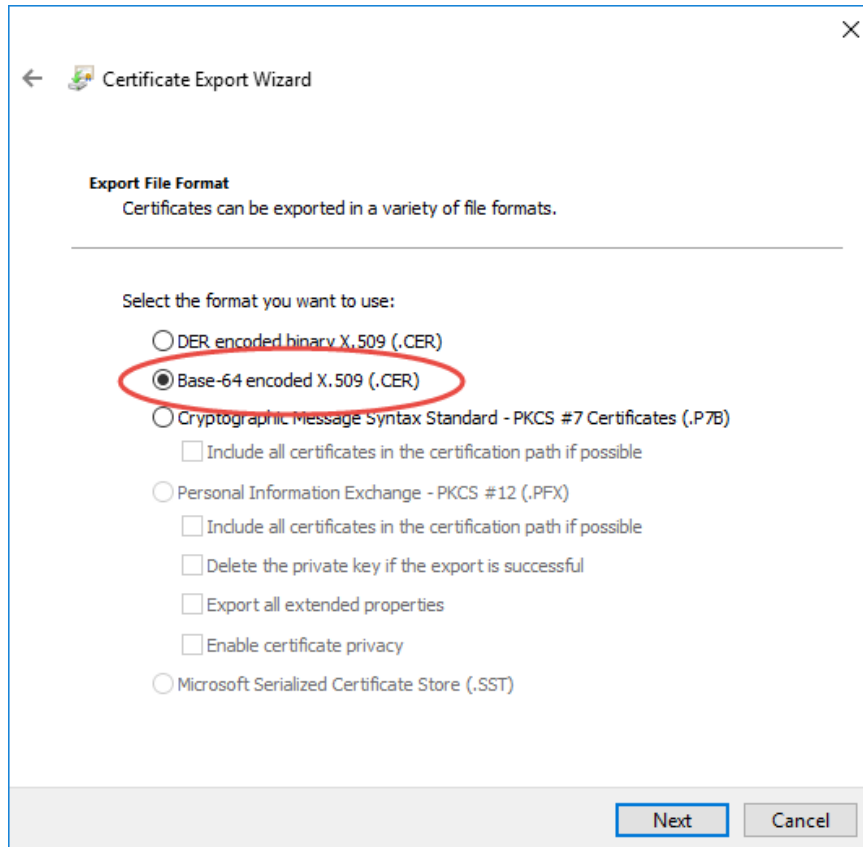
- 3) Execute the following command to open certificate manager
- 4) Certificate manager window will be opened, Navigate to Personal>Certificates folder. You can see all already installed certificates there



- 
- certmgr - [Certificates - Current User\Personal\Certificates]
- File Action View Help
- Certificates - Current User
- Personal
    - Certificates
      - Trusted Root Certification Authorities
      - Enterprise Trust
      - Intermediate Certification Authorities
      - Active Directory User Objects
      - Trusted Publishers
      - Untrusted Certificates
      - Third-Party Root Certificates
      - Trusted People
      - Client Authentication Issuers
      - Local NonRemovable Certificates
      - MSIEHistoryJournal
      - Certificate Enrollment Requests
      - Smart Card Trusted Roots
- | Issued To                         | Issued By                          | Expiration Date | Intended Purposes        | Friendly Name        |
|-----------------------------------|------------------------------------|-----------------|--------------------------|----------------------|
| ARMRootCert                       | ARMRootCert                        | 01-01-2040      | <All>                    | <None>               |
| FullOS                            | FullOSTransport                    | 10-10-2067      | Server Authentication... | <None>               |
| FullOS                            |                                    |                 | Server Authentication... | <None>               |
| FullOS                            |                                    |                 | Server Authentication... | <None>               |
| FullOS                            |                                    |                 | Server Authentication... | <None>               |
| FullOS                            |                                    |                 | Server Authentication... | <None>               |
| FullOS                            |                                    |                 | Server Authentication... | <None>               |
| Windows Azure Tools               | Windows Azure Tools                | 22-10-2017      | <All>                    | RemoteDebugger6...   |
| Windows Azure Tools               | Windows Azure Tools                | 22-10-2017      | <All>                    | RemoteDebugger6...   |
| Windows Azure Tools               | Windows Azure Tools                | 22-10-2017      | <All>                    | SampleCloudServic... |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 22-10-2017      | <All>                    | RemoteDebugger6...   |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 24-10-2017      | <All>                    | Windows Azure To...  |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 22-10-2017      | <All>                    | Windows Azure To...  |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 24-10-2017      | <All>                    | Windows Azure To...  |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 19-10-2017      | <All>                    | Windows Azure To...  |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 19-10-2017      | <All>                    | Windows Azure To...  |
| Windows Azure Tools Encryption... | Windows Azure Tools Encryption ... | 19-10-2017      | <All>                    | Windows Azure To...  |
- Export a certificate

- 
- ←  Certificate Export Wizard
- 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 the 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 Cancel

7) Select Base 64-encoded X.509 (.CER) from the list of export file formats. Click Next.



The screenshot shows the 'Certificate Export Wizard' window, specifically the 'Export File Format' step. The title bar reads 'Certificate Export Wizard'. Below the title bar, there is a back arrow icon and the text 'Certificate Export Wizard'. The main heading is 'Export File Format', followed by the instruction 'Certificates can be exported in a variety of file formats.' Below this, a horizontal line separates the heading from the options. The text 'Select the format you want to use:' is followed by a list of radio button options. The second option, 'Base-64 encoded X.509 (.CER)', is selected and circled in red. Other options include 'DER encoded binary X.509 (.CER)', 'Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)', 'Personal Information Exchange - PKCS #12 (.PFX)', and 'Microsoft Serialized Certificate Store (.SST)'. There are also several unchecked checkboxes for additional options like 'Include all certificates in the certification path if possible', 'Delete the private key if the export is successful', 'Export all extended properties', and 'Enable certificate privacy'. At the bottom right, there are 'Next' and 'Cancel' buttons.

← Certificate Export Wizard

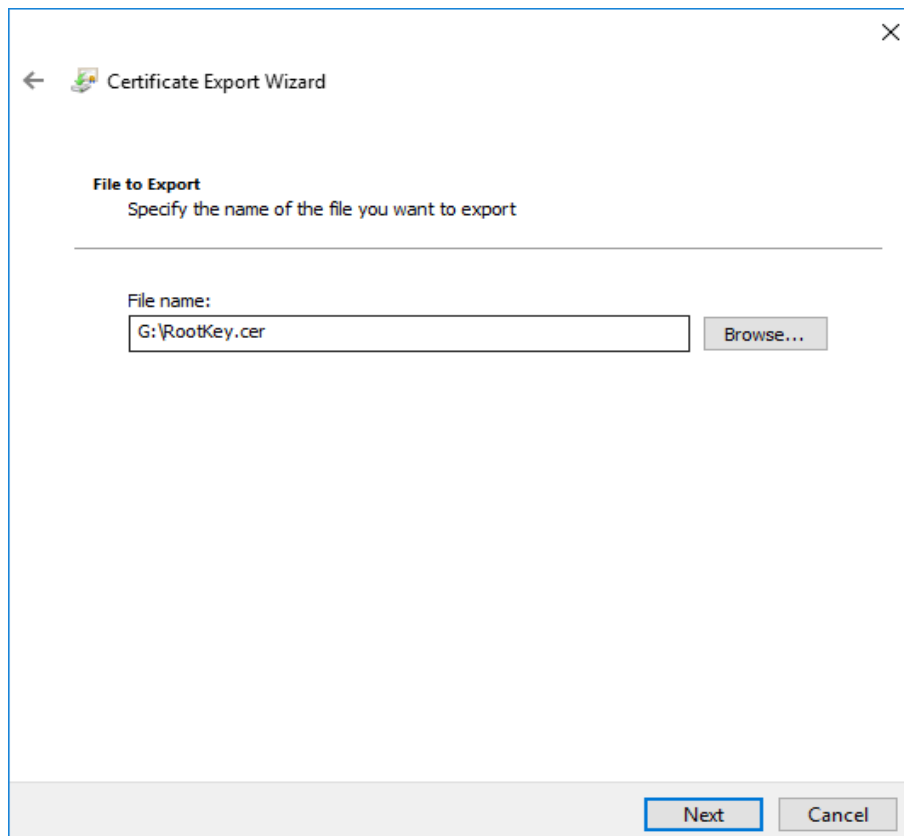
**Export File Format**  
Certificates can be exported in a variety of file formats.

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

8) Select the location and name for the file to save. Click Next



The screenshot shows the 'Certificate Export Wizard' window, specifically the 'File to Export' step. The title bar reads 'Certificate Export Wizard'. Below the title bar, there is a back arrow icon and the text 'Certificate Export Wizard'. The main heading is 'File to Export', followed by the instruction 'Specify the name of the file you want to export'. Below this, a horizontal line separates the heading from the input field. The text 'File name:' is followed by a text box containing 'G:\RootKey.cer' and a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

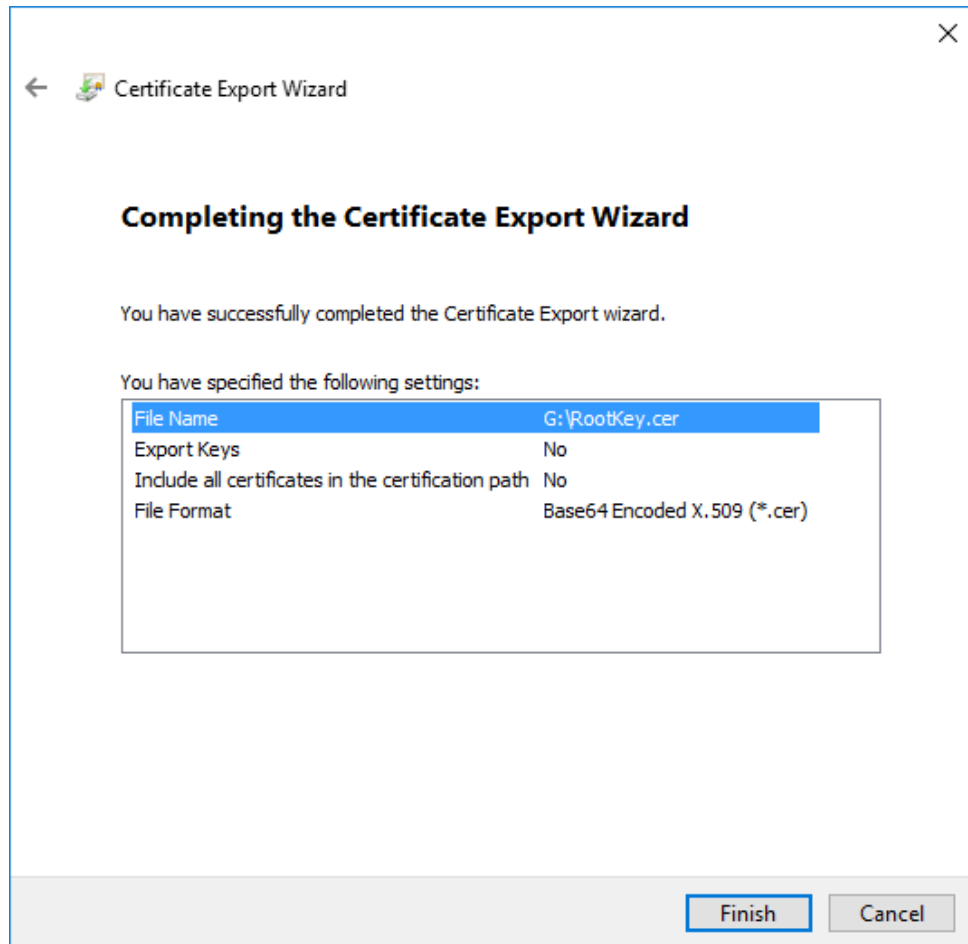
← Certificate Export Wizard

**File to Export**  
Specify the name of the file you want to export

File name:  
G:\RootKey.cer Browse...

Next Cancel

- 9) Click Finish in the Final Wizard.

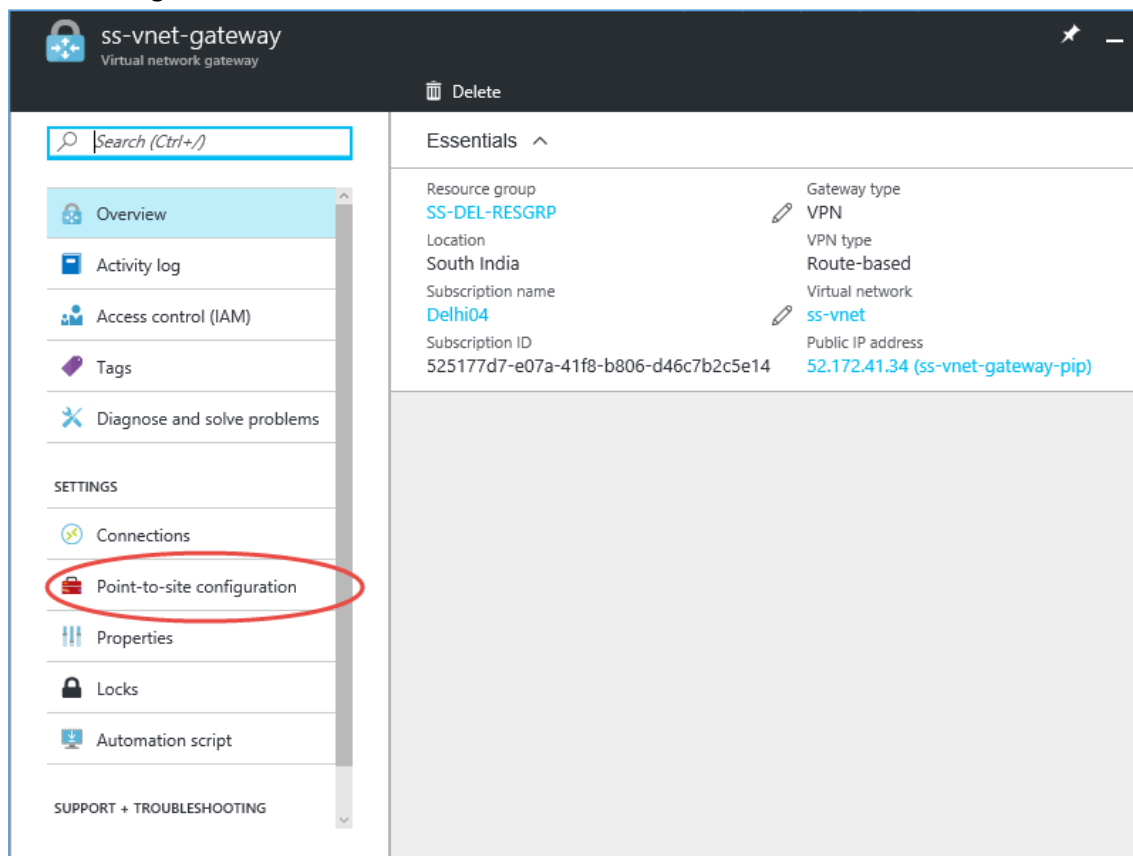


- 10) Open the Keyfile which you have saved in note pad. You can see the certificate Key similar to the below one. Select and copy the key which come in between ---BEGIN CERTIFICATE---- and ---END CERTIFICATE-----

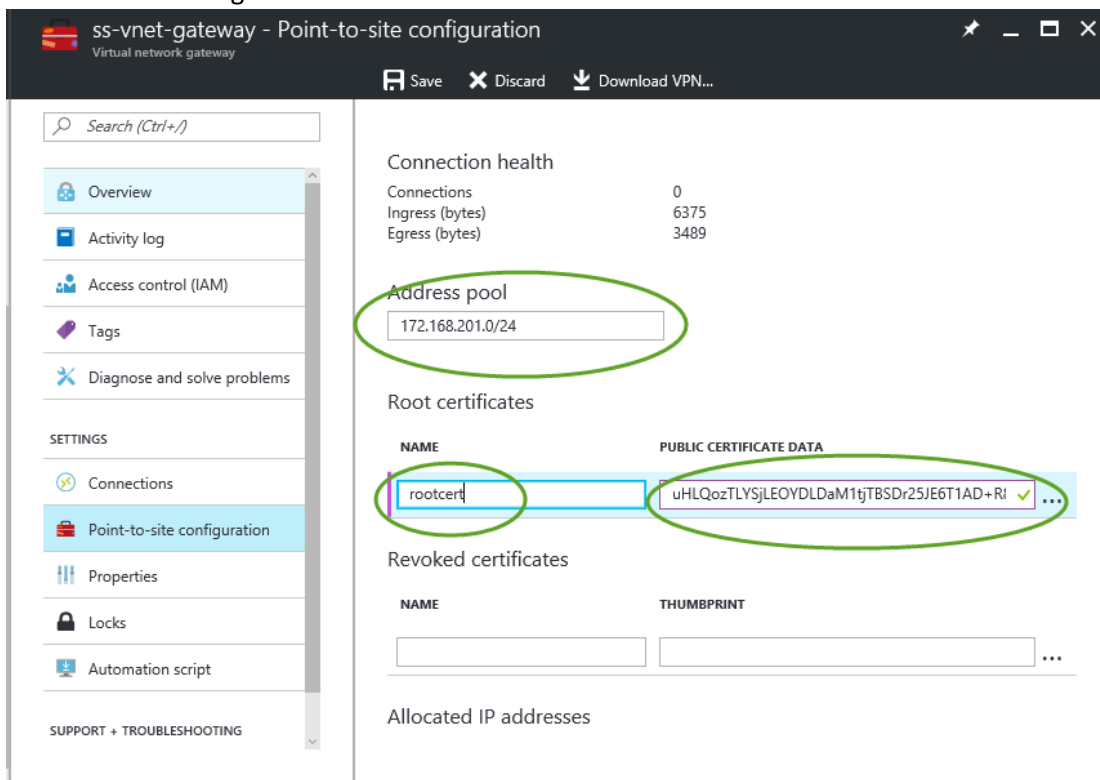
```
1 -----BEGIN CERTIFICATE-----
2 MIIC+TCCAeWgAwIBAgIQL3eydPBpKaZK36WffKSI3TAJBgUrDgMCHQUAMBYxFDAS
3 BgNVBAMTC0FSTVJvb3RDZXJ0MB4XDTE2MTEwODA3MAZmloXDTM5MTIzNTk1
4 OVowFjEUMBIGA1UEAxMLQVJNUm9vdENlcnQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
5 DwAwggEKAoIBAQCqmqC64VDKI43NsKvd3pFext1Xp+E38INRbyoCRw12Aeruee40
6 nn/2Ac5FqeSIDIdw1EfFGEcvA2RLNr4JdFl82tw98ERPlh7TaH1FP64Qk2AJb6+b
7 oLwoJC2Dwfb+Mka108ACKM4l+TQIdbvmACKGk1kmEwHMAeyktHe/Ua1UVxMymE4V
8 4ORsvv4stCzPEEK4vKIIdVbcZQPPiqKZwPntokWKJtVWdtYWIq8OMlWayZX50nT7L
9 PptUyIRWClpqMqmgBwHHIj6nqY1GsZDIfrJOv4tWDrQXjCC/3dVmsI5HKQx9S8n
10 E3U5JL4K9C9TYMIiXaFhJ9h4jfJkFUQ3HgFXAgMBAAgJsZBJMEcGA1UdAQRAMD6A
11 EAiRdHOHKSndSg2X9XqVWShGDAWMRQwEgYDVQQDEwtBUK1Sb290Q2VydIIQL3ey
12 dPBpKaZK36WffKSI3TAJBgUrDgMCHQUAA4IBAQCAGF06gA/6BK5k6MLfe1woXWsh
13 UfYPUZDUZY0Ka5NeCBiII5VIA85XStansQVY+r4MrJo64cf56diZRVRE9g8zqg5D
14 Ic4aKMoFdUwpKCMo6LT5cz7uqgYRXxwZuD7h9aj0lrd4zZG2yhe8GtNoLmdZhpW
15 /LDVKtK6I1PWHfwTn3mzm0+2+gyHfbubjNroY6aVRPXmkIjz1WRvWP2EI2g9LQxh
16 boLWPcWU7zAmhfdXdSeCKkM9mA4ATcoAsYuDHmfUvntMnztSJJN9bf7gSP5YDaLt
17 jsXDd2N8QqL28momn1LuHLQozTLYSjLEOYDLDaM1tjTBSDr25JE6T1AD+R8A
18 -----END CERTIFICATE-----
19
```

Normal text | length: 1,108 | lines: 19 | Ln: 18 | Col: 1 | Sel: 1,052 | 17 | Windows (CR LF) | UTF-8 | INS

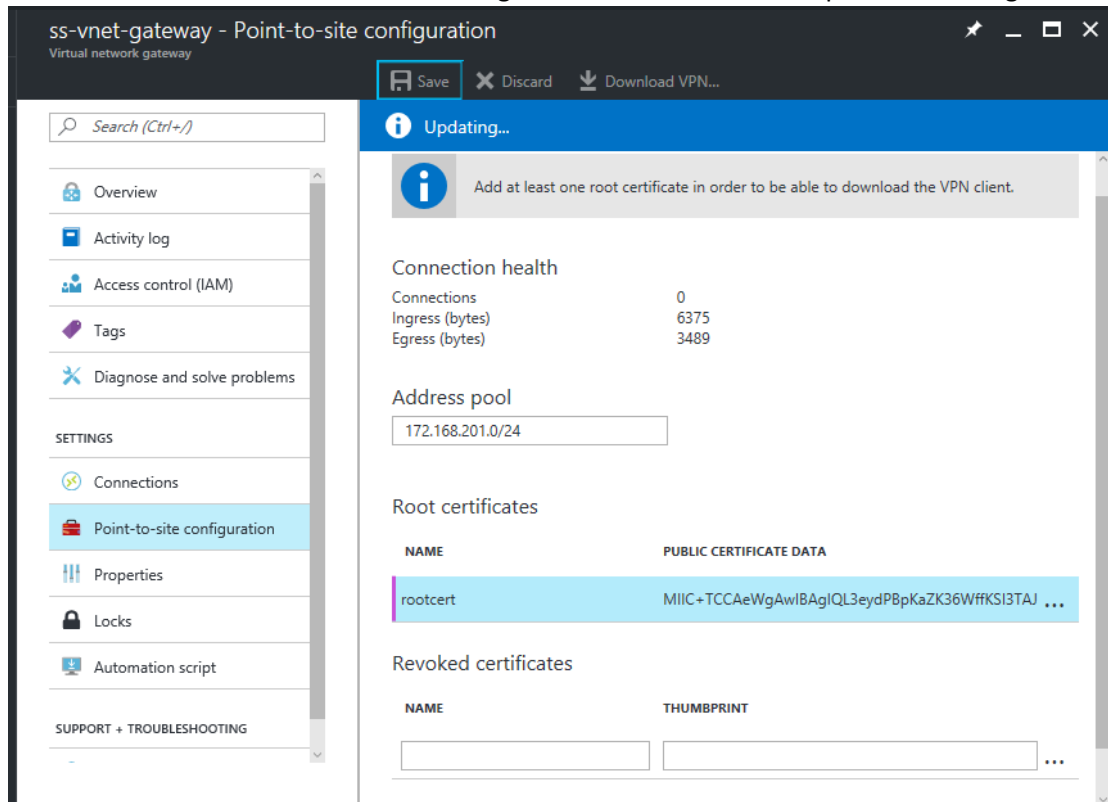
- 11) Open Azure Portal and navigate to the Virtual network gateway properties. And select Point-to-Site configuration



- 12) Specify the address pool value, and paste the copied key into the 'PUBLIC CERTIFICATE DATA' section and give a name for the certificate data.



13) Click on the save button to save the changes. It takes some time to update the changes



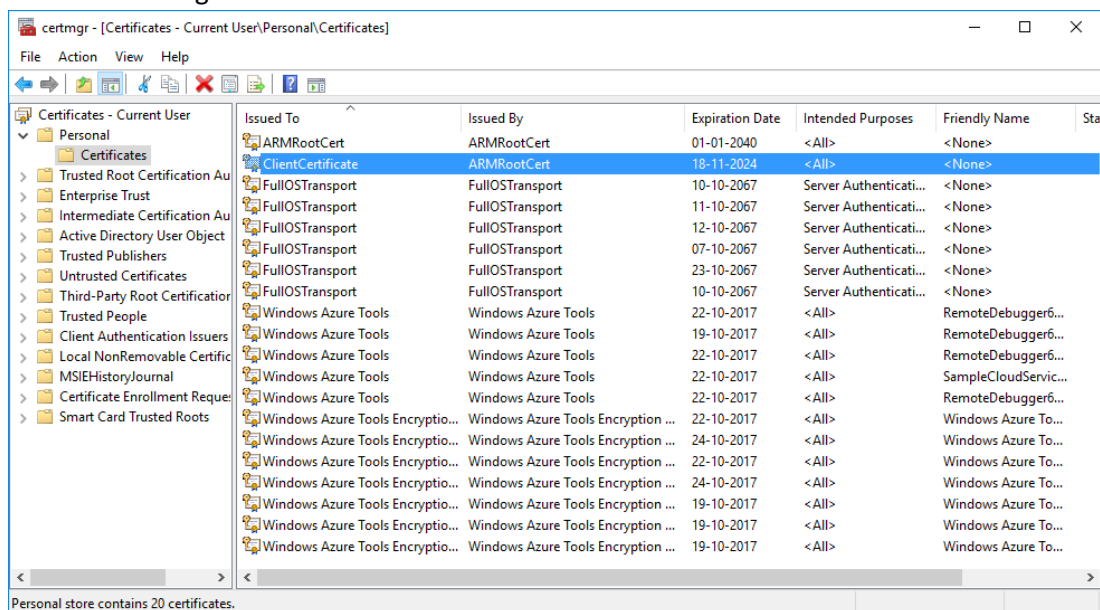
14) Now you have installed the certificate on Azure. Next you need to go and create client certificate. Open the command window and execute the following command to create a client certificate.

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

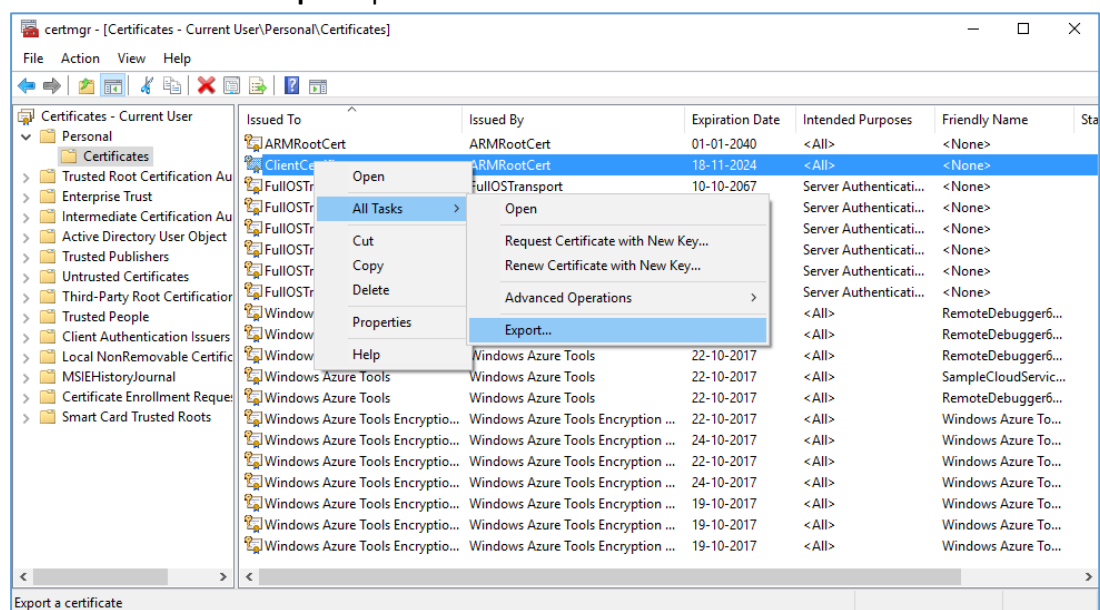
[Note: Name of the certificate can be anything it should be validating against the server certificate, So you need to specify the same name of the server certificate , eg: here it is **ARMRootCert**]



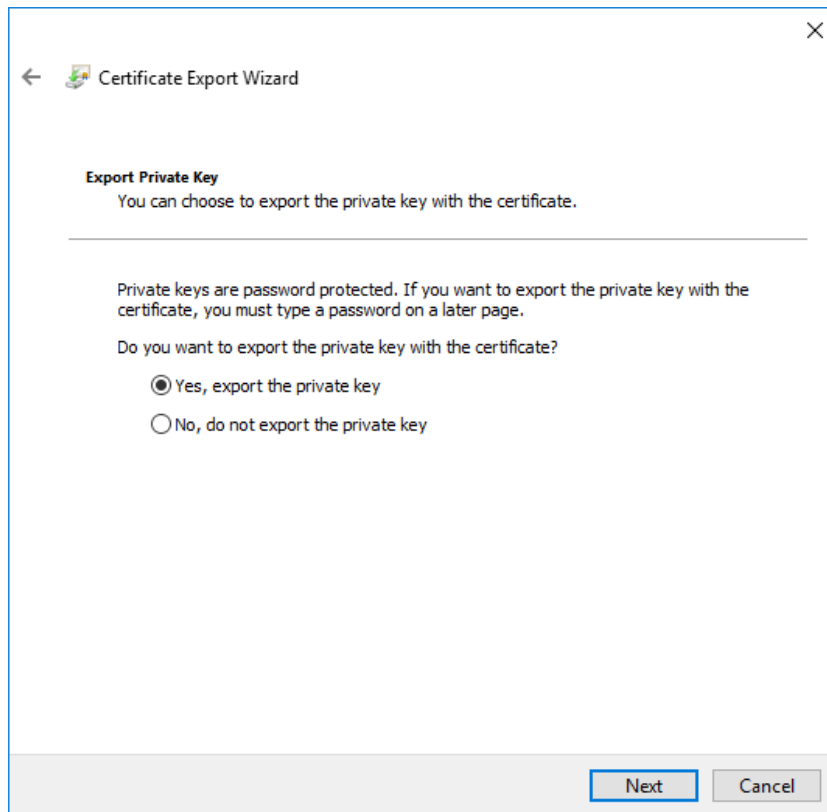
- 15) It will install a Client certificate in the computer. Open certification manager using **certmgr** command. Navigate to **Personal > Certificates**.



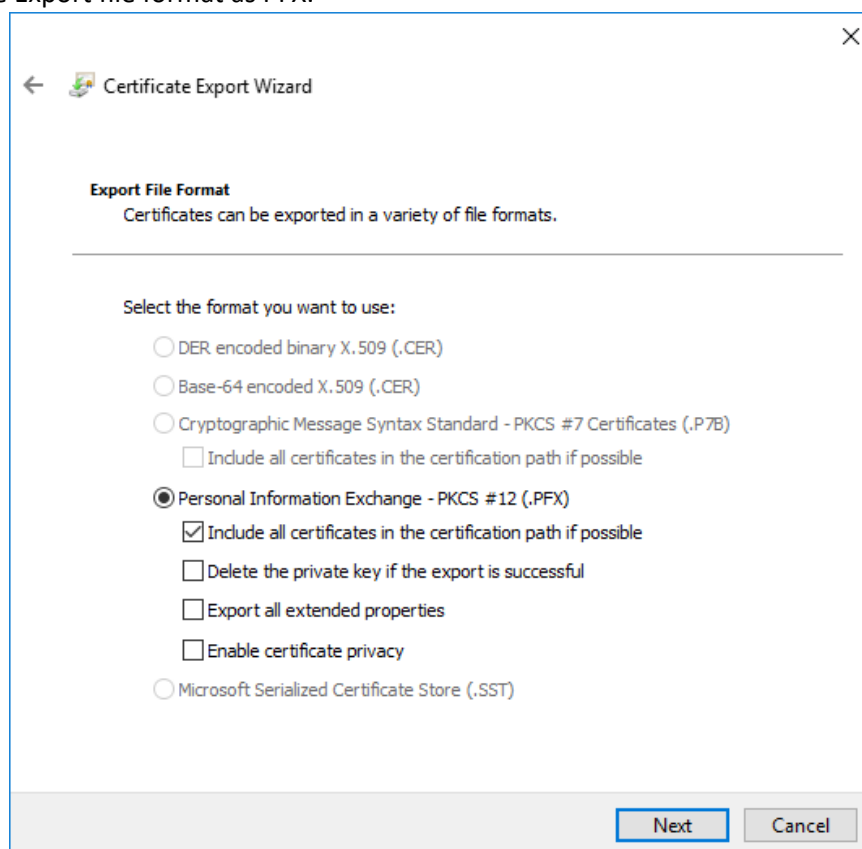
- 16) Now you can go and create the PFX file for the installed client certificate. To do so right click and select **All Tasks > Export** option.



- 17) In the certificate export wizard click Next in welcome screen, and select 'Export private key' from the wizard, Click Next

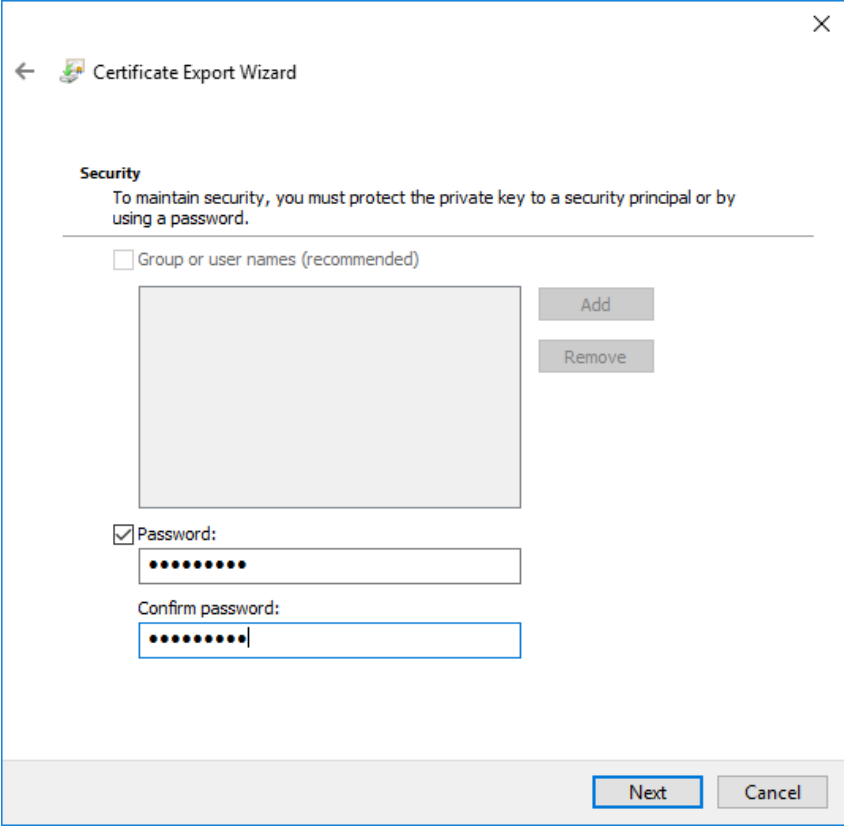


18) Select the Export file format as PFX.



19) Specify a security password for the PFX file. Click Next





← Certificate Export Wizard

**Security**  
To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

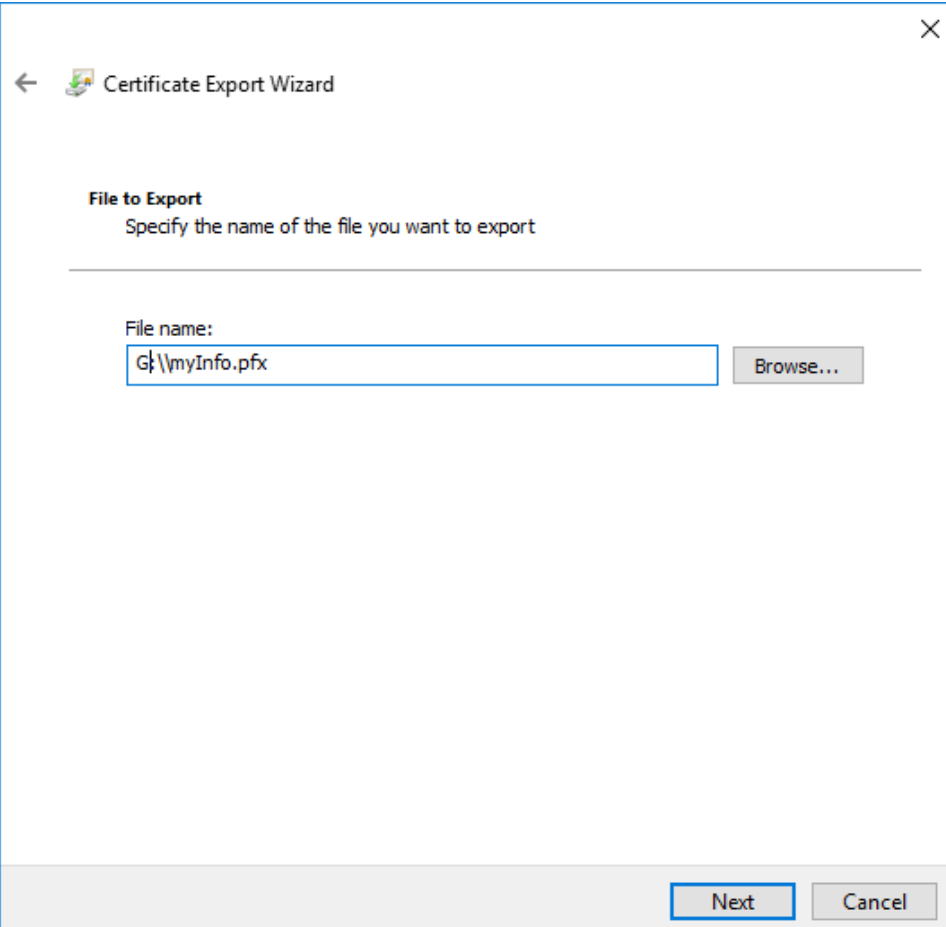
Add  
Remove

☒ Password:  
●●●●●●●●

Confirm password:  
●●●●●●●●

Next Cancel

20) Choose a location and name for the file to save. Click Next.



← Certificate Export Wizard

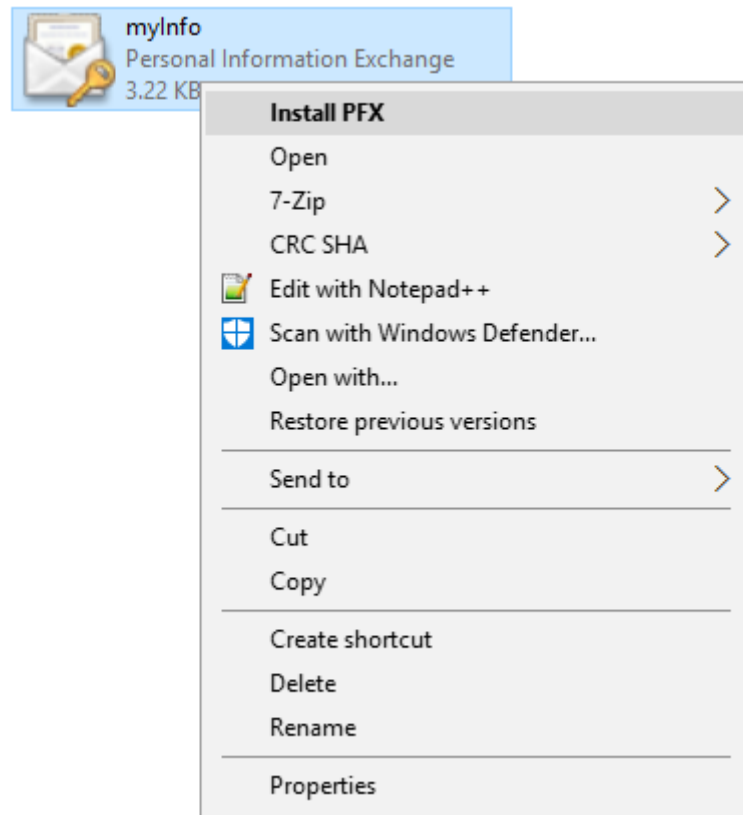
**File to Export**  
Specify the name of the file you want to export

File name:  
G:\myInfo.pfx

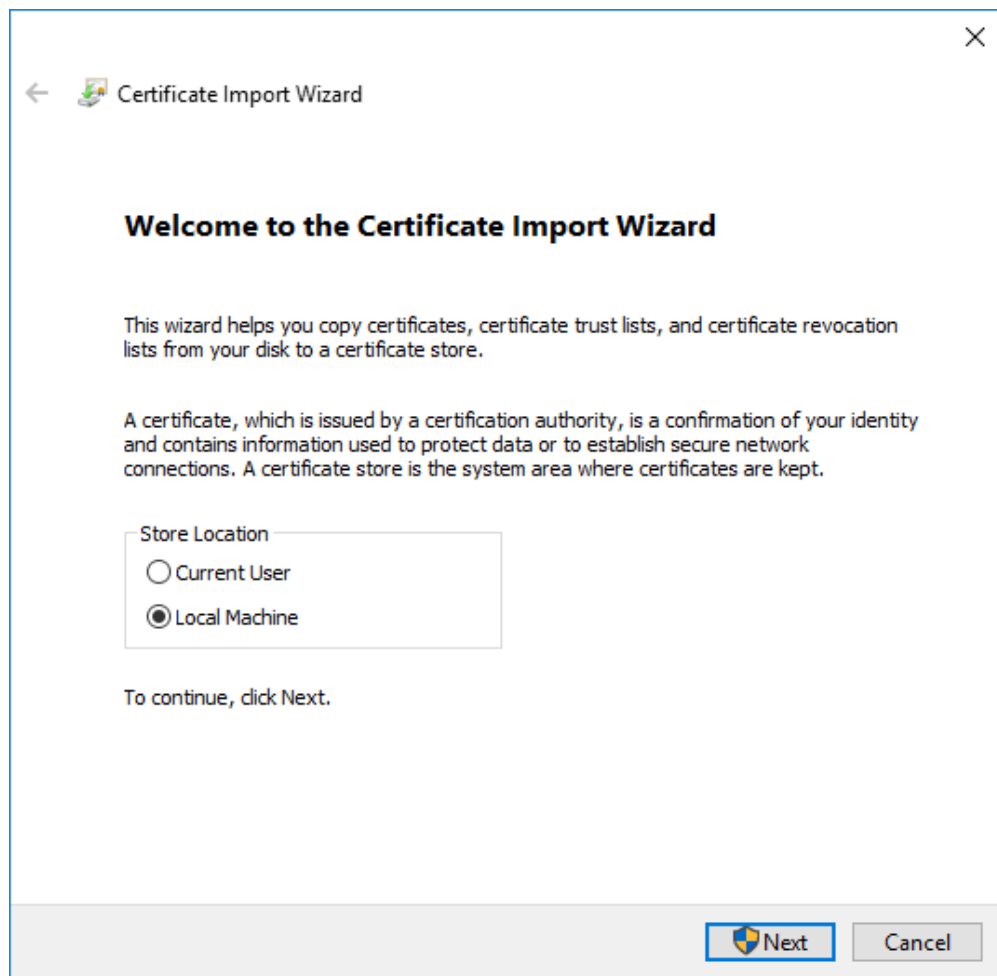
Browse...

Next Cancel

- 21) Click Finish. It creates a PFX file in the selected location.
- 22) Navigate to the location where you have created the PFX file, select and right click the file, choose **Install Pfx** option.



- 23) You will get an installation dialog box, Select **Local machine** to install.



← Certificate Import Wizard

## Welcome to the Certificate Import Wizard

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

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.

Store Location

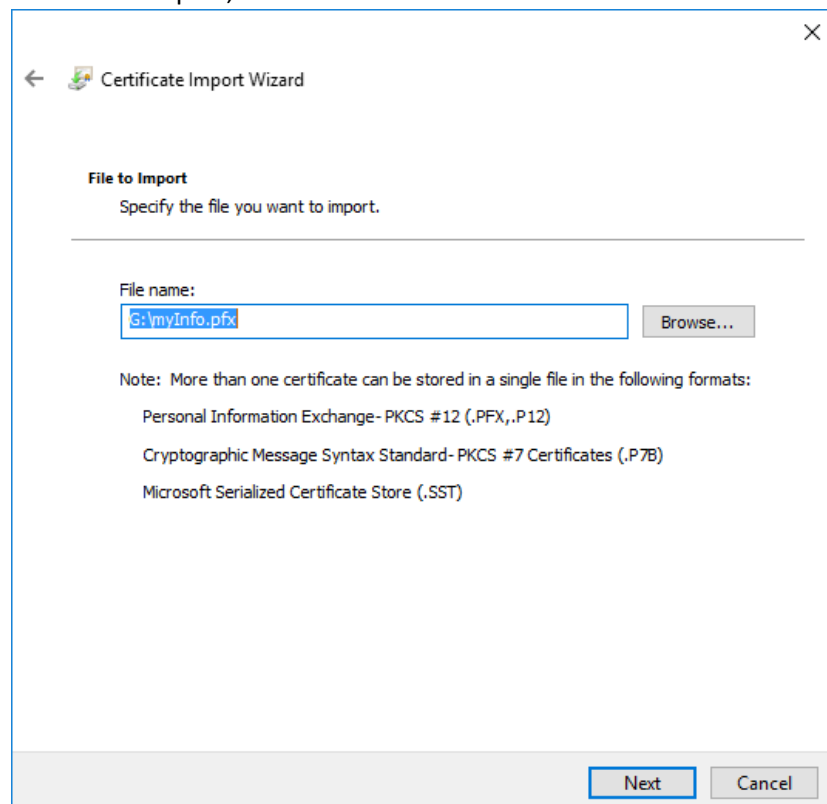
☐ Current User

☒ Local Machine

To continue, click Next.

Next Cancel

24) Confirm the PFX file to import, Click Next



← Certificate Import Wizard

### File to Import

Specify the file you want to import.

File name:

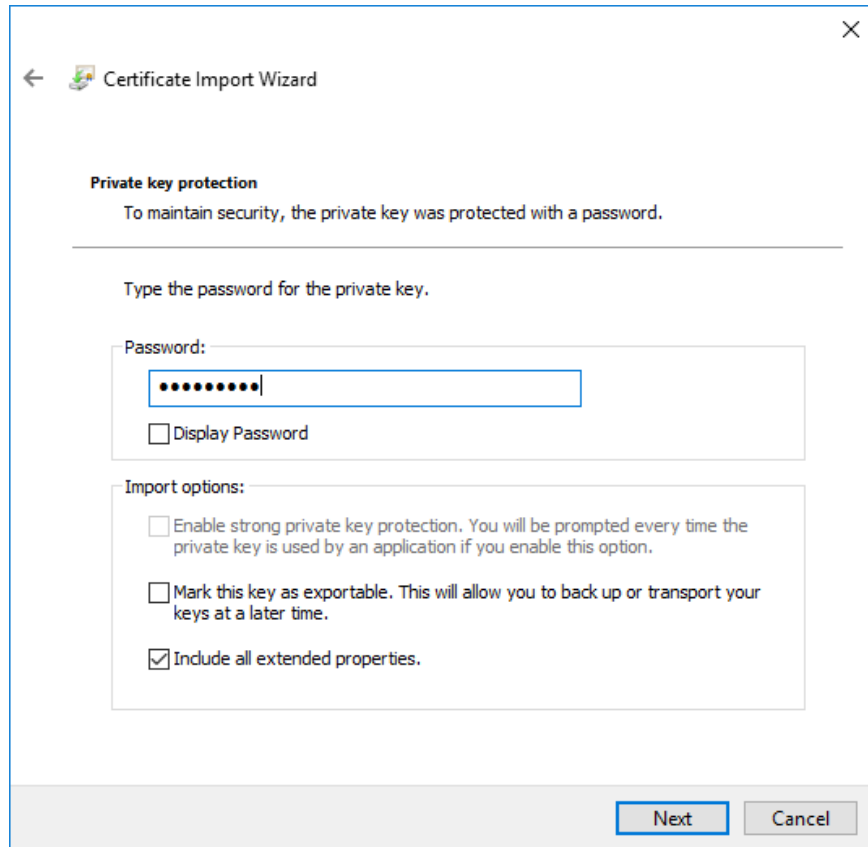
Browse...

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange - PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

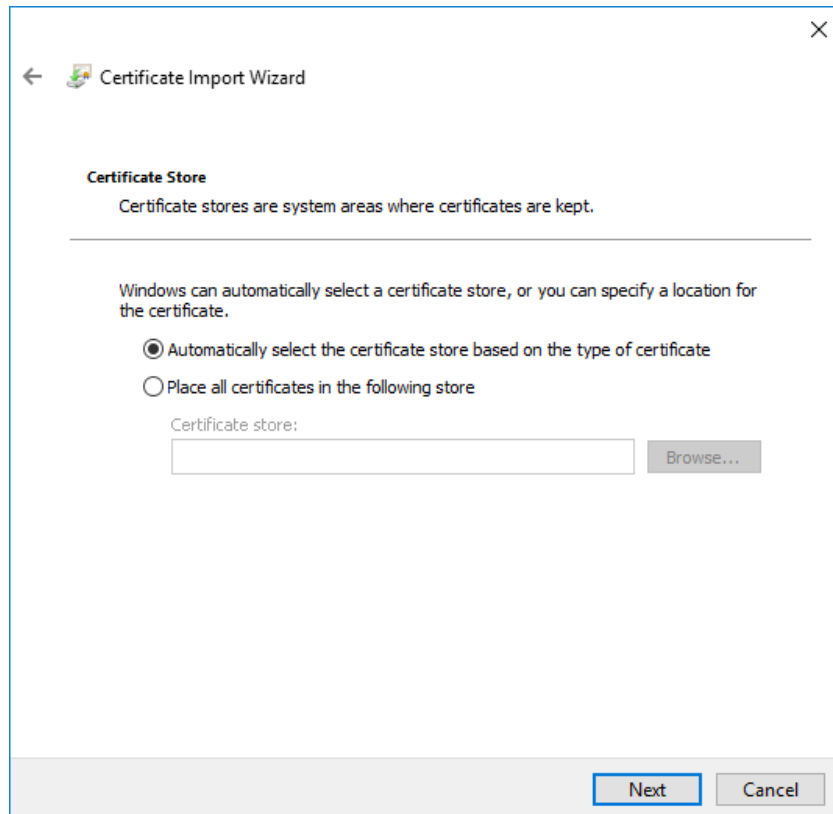
Next Cancel

25) Enter the password which you have specified while exporting file, Click Next.



The screenshot shows the 'Certificate Import Wizard' window. The title bar includes a back arrow, a certificate icon, and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the text 'To maintain security, the private key was protected with a password.' Below this is a section titled 'Type the password for the private key.' which includes a 'Password:' label, a text box containing ten dots, and a checkbox labeled 'Display Password'. Below the password section is an 'Import options:' section with three checkboxes: 'Enable strong private key protection...' (unchecked), 'Mark this key as exportable...' (unchecked), and 'Include all extended properties.' (checked). At the bottom right, there are 'Next' and 'Cancel' buttons.

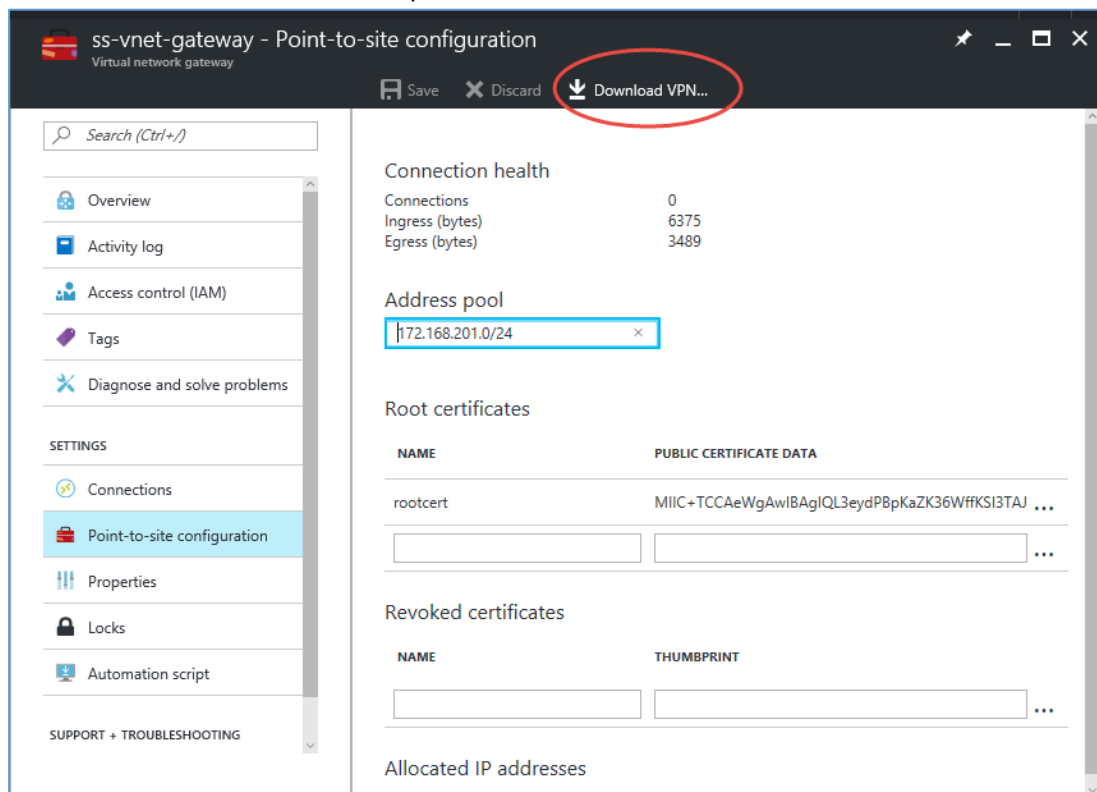
26) Select the first option from the Certificate Store wizard. It will automatically select the certificate store.



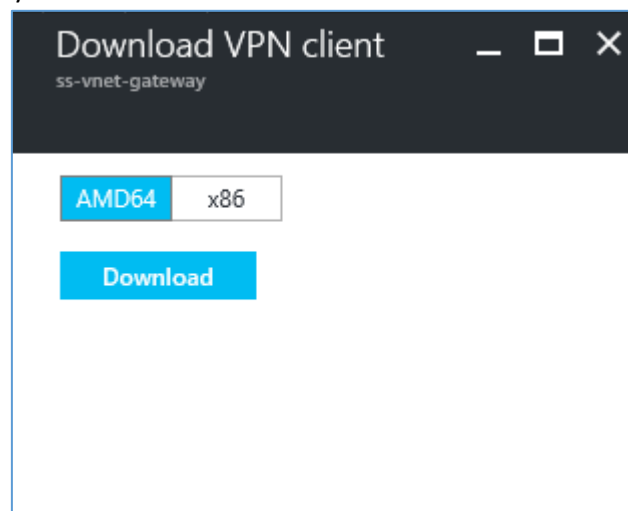
The screenshot shows the 'Certificate Import Wizard' window at the 'Certificate Store' step. The title bar is the same as the previous screen. The main content area is titled 'Certificate Store' and contains the text 'Certificate stores are system areas where certificates are kept.' Below this is a section titled 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' which includes two radio button options: 'Automatically select the certificate store based on the type of certificate' (selected) and 'Place all certificates in the following store'. Below the second option is a 'Certificate store:' label, a text box, and a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

27) Click finish to Complete the steps.

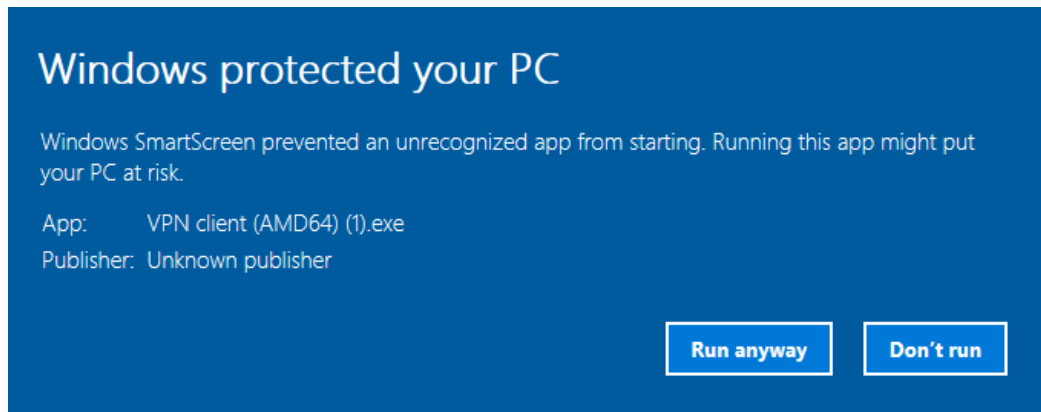
28) Once you complete the installation, you can go back to the Azure portal and navigate to the Virtual Gateway **settings** blade and select the **Point-to-Site configuration**. Click on the **Download VPN Client** from the top.



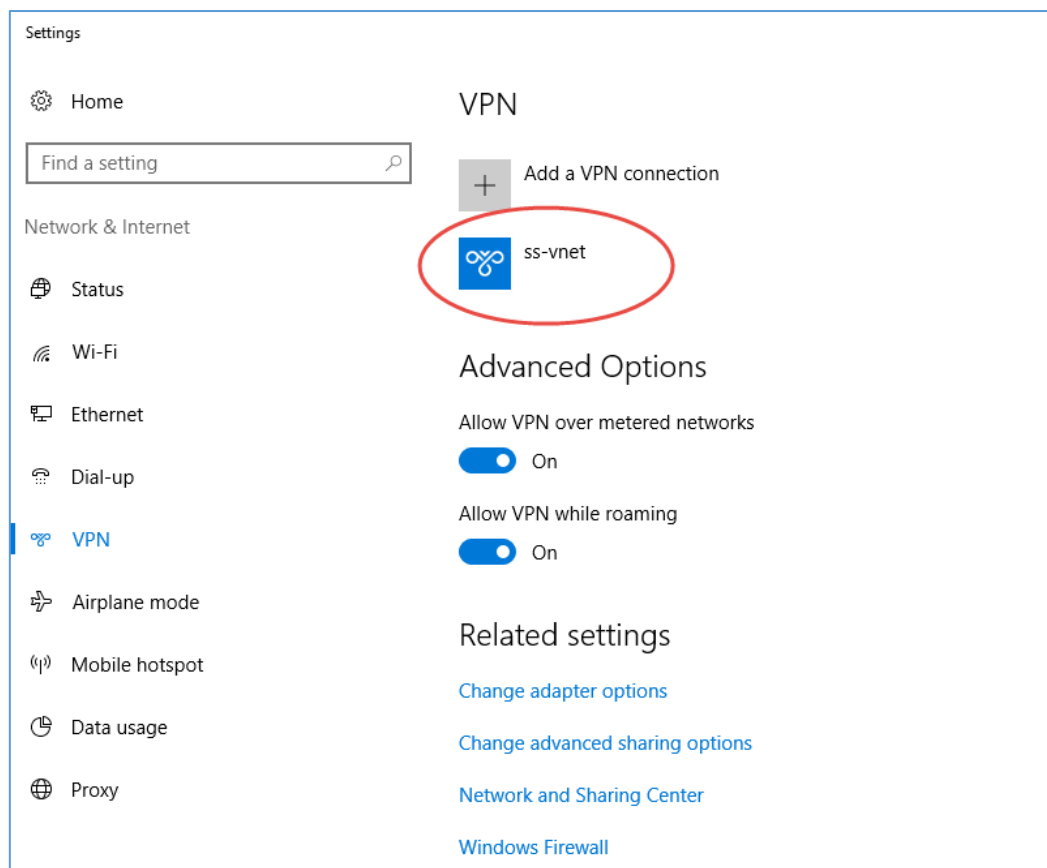
29) It opens another blade where you can select 32bit or 64bit version of the VPN client. Select appropriate one for you client machine and click download.



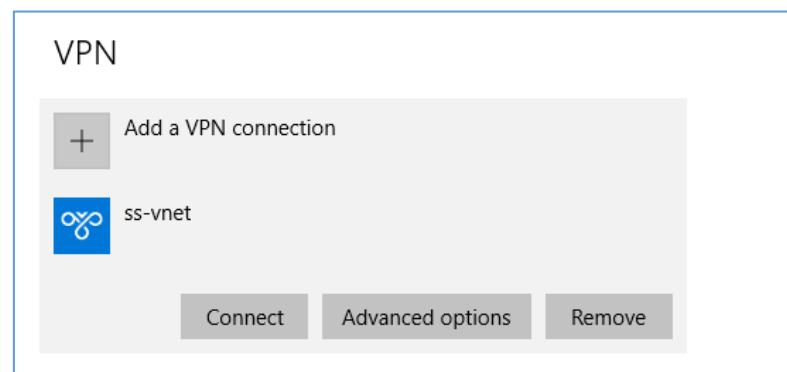
30) Install the client application as administrator, If it asks for confirmation click on 'Run anyway' (in windows8 or later clients).



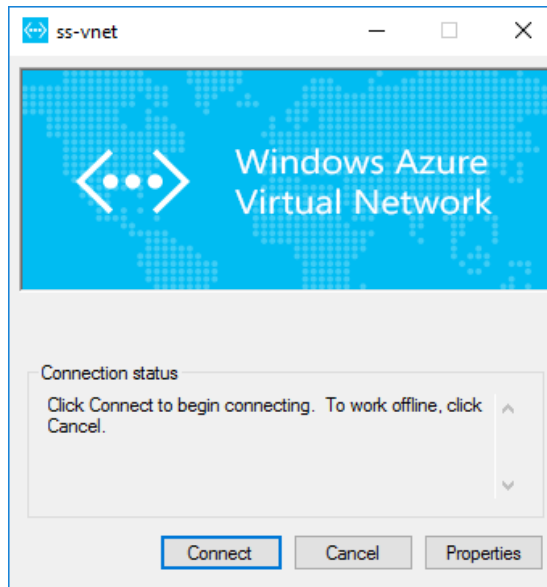
31) Once installation is completed you can go to the Network settings window and you can see the installed VPN client.



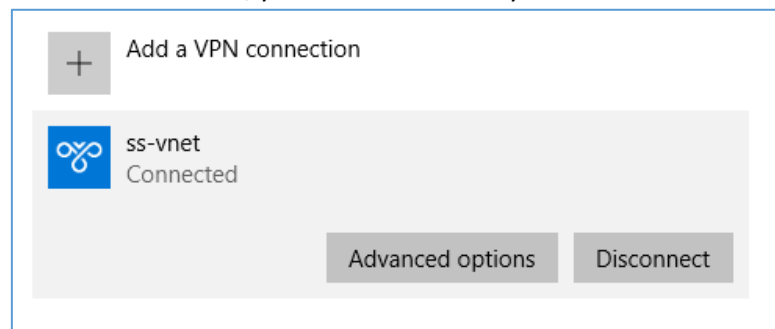
32) Click to connect to the VNET.



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



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



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

```
Command Prompt

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::2d05:c13c:9de1:be52%23
IPv4 Address. . . . . : 192.168.121.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::247c:b565:a8e2:5b90%17
IPv4 Address. . . . . : 192.168.44.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

PPP adapter ss-vnet:

Connection-specific DNS Suffix  . : 
IPv4 Address. . . . . : 172.168.201.2
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : example.com

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
```

Thank you