Create virtual Network

Create virtual network gateway

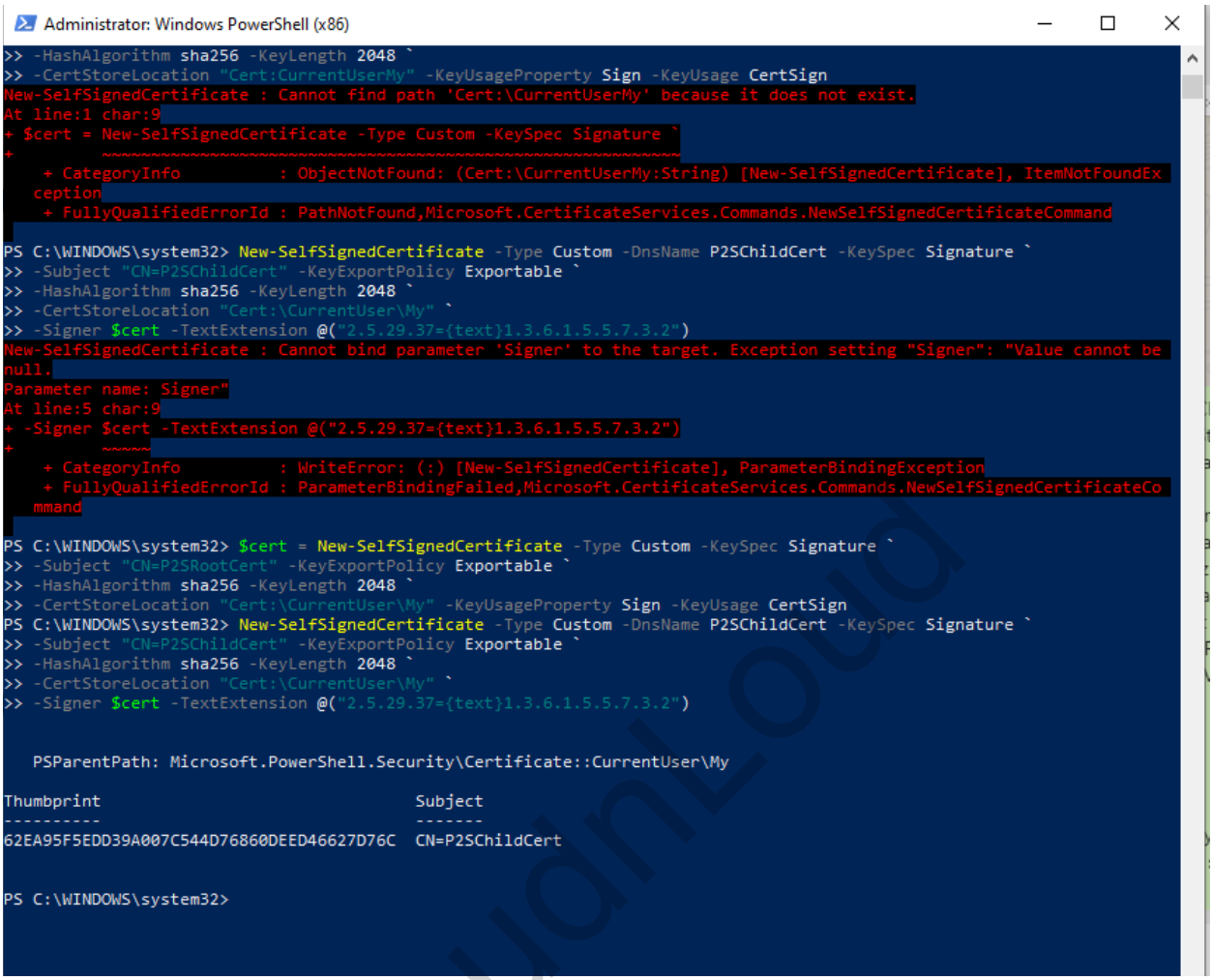
From your windows 10 laptop itself create root certificate and client certificate . (open powershell vi administrator and paste the 4 below lines together)

rootcertificate

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

Client certificate

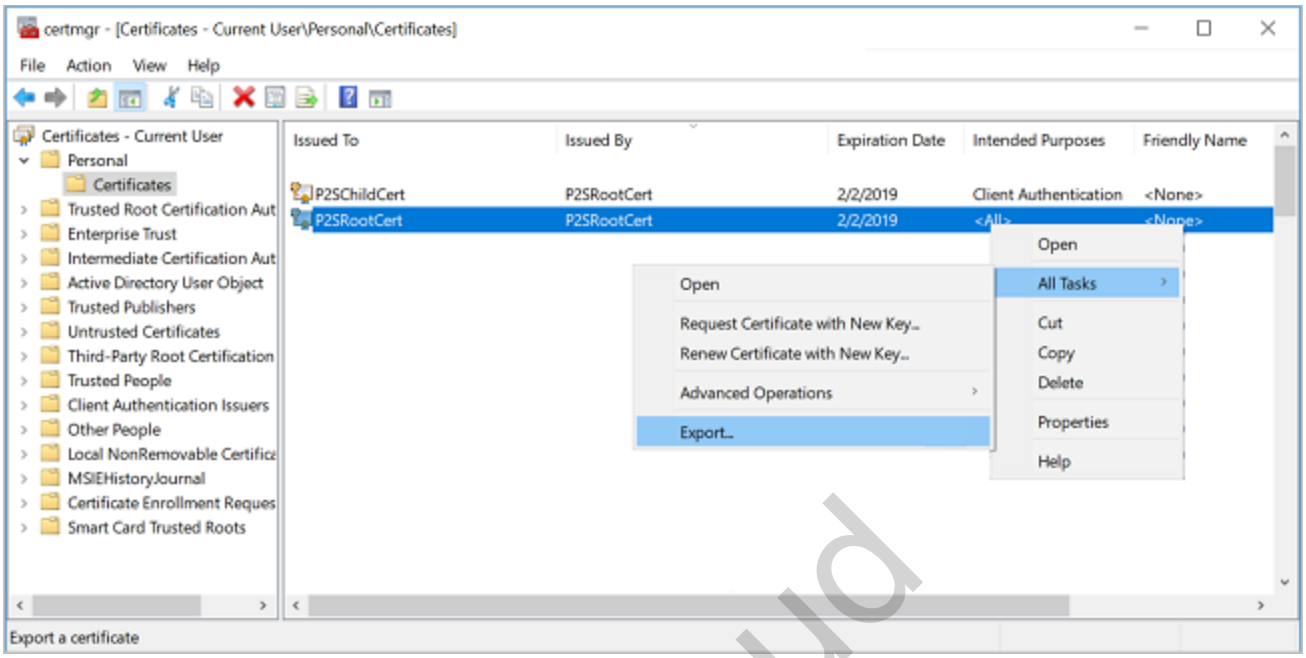
```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```



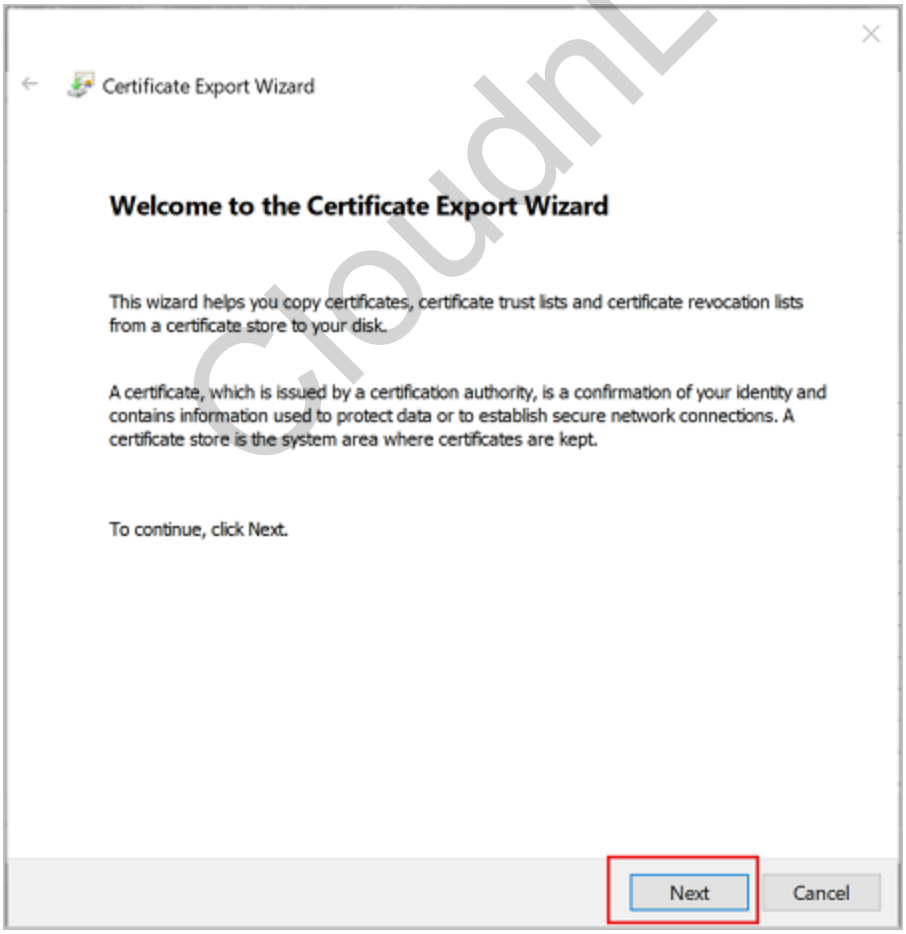
Export the root certificate public key (.cer)

After creating a self-signed root certificate, export the root certificate public key .cer file (not the private key). You will later upload this file to Azure. The following steps help you export the .cer file for your self-signed root certificate:

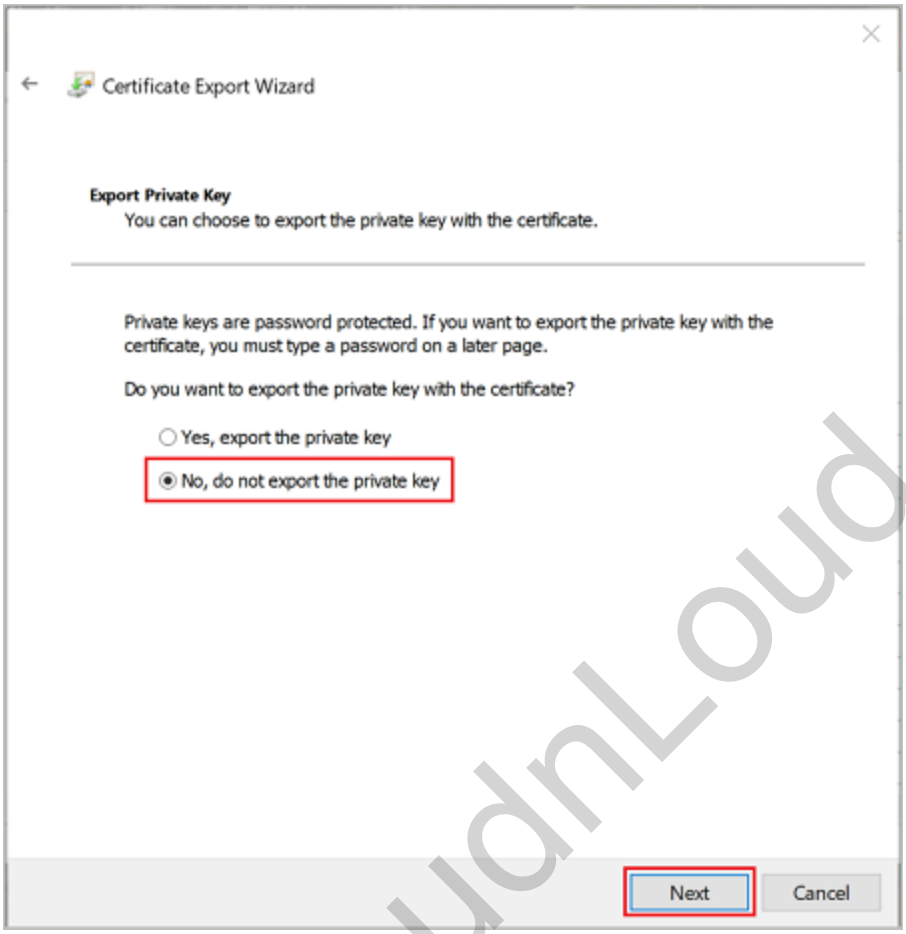
1. To obtain a .cer file from the certificate, open **Manage user certificates**. Locate the self-signed root certificate, typically in 'Certificates - Current User\Personal\Certificates', and right-click. Click **All Tasks**, and then click **Export**. This opens the **Certificate Export Wizard**. If you can't find the certificate under Current User\Personal\Certificates, you may have accidentally opened "Certificates - Local Computer", rather than "Certificates - Current User"). If you want to open Certificate Manager in current user scope using PowerShell, you type *certmgr* in the console window.



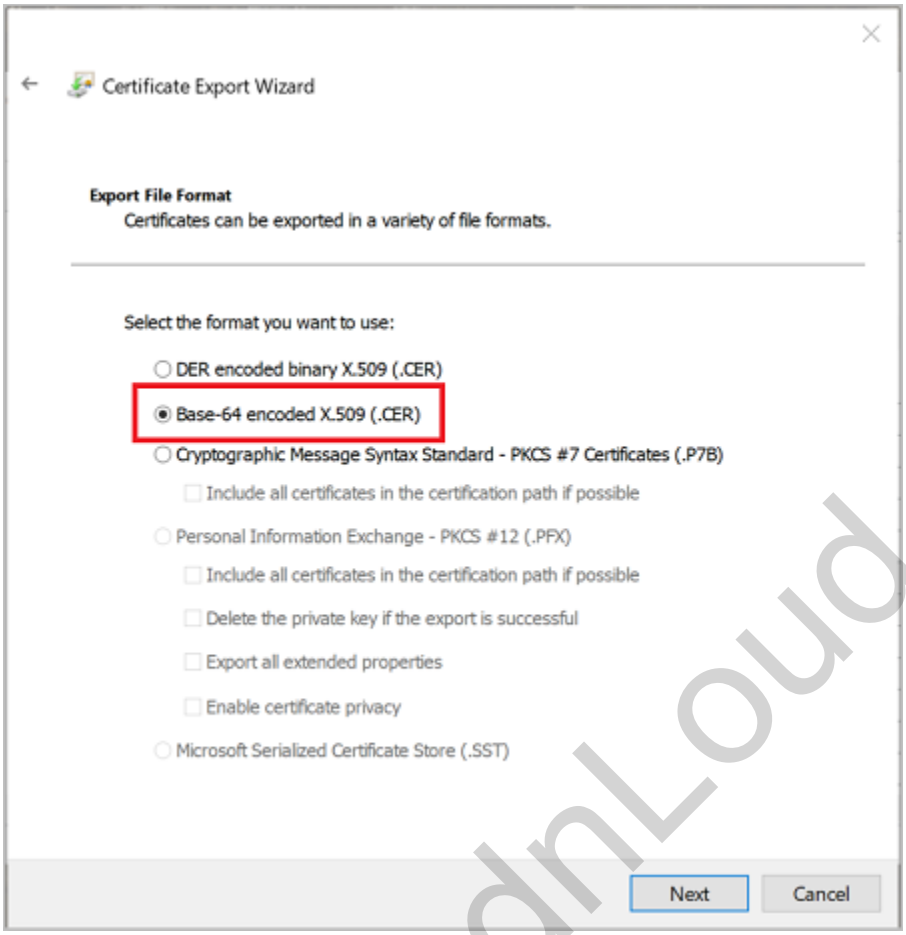
2. In the Wizard, click **Next**.



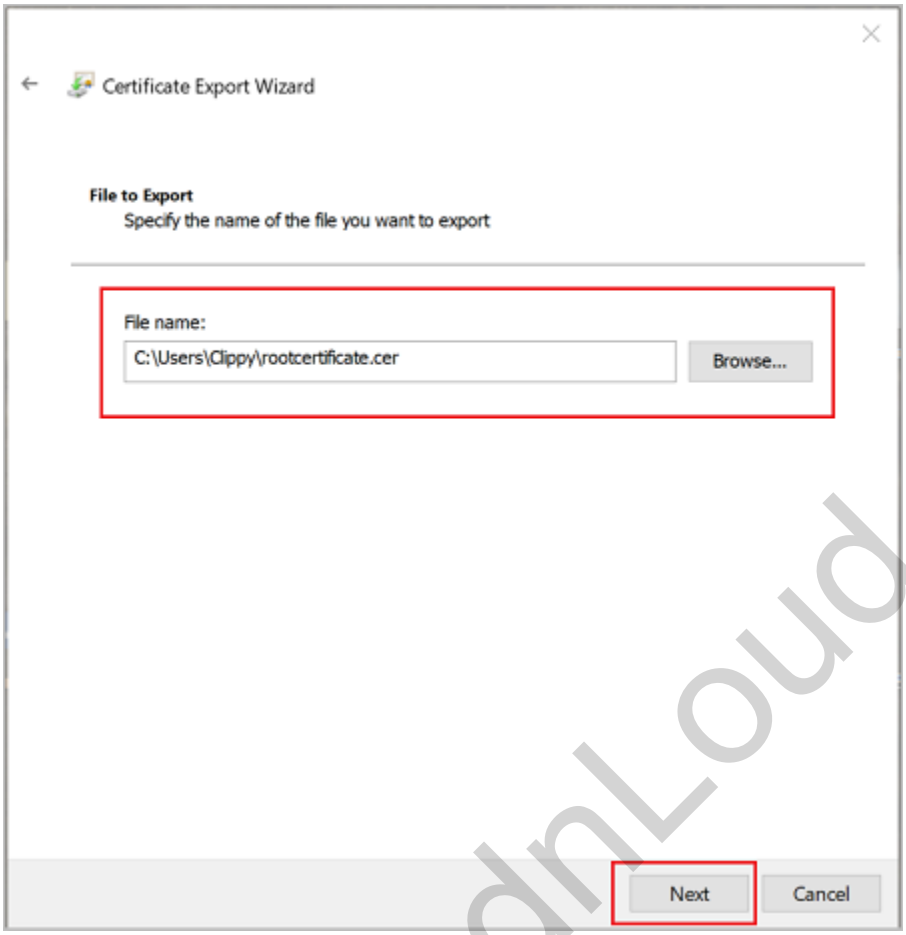
3. Select **No, do not export the private key**, and then click **Next**.



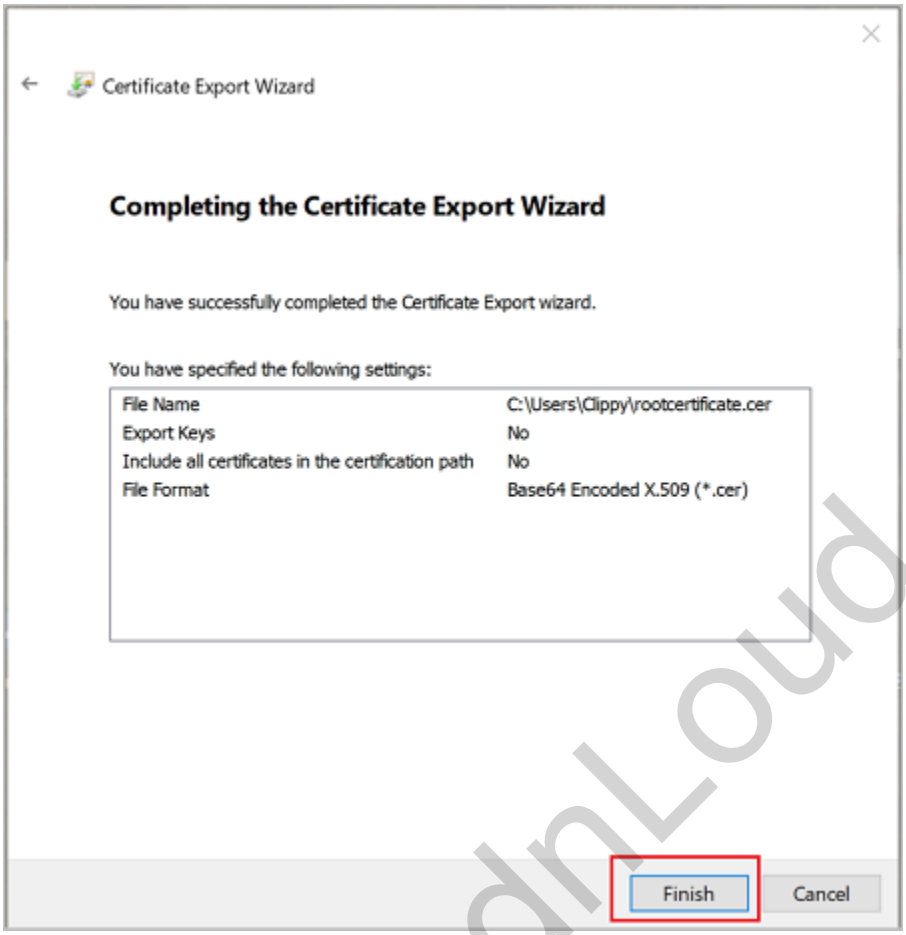
4. On the **Export File Format** page, select **Base-64 encoded X.509 (.CER).**, and then click **Next**.



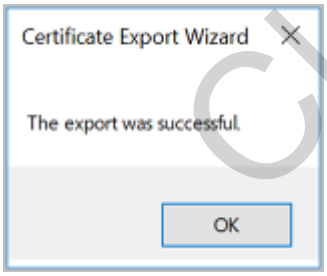
5. For **File to Export**, **Browse** to the location to which you want to export the certificate. For **File name**, name the certificate file. Then, click **Next**.



6. Click **Finish** to export the certificate.

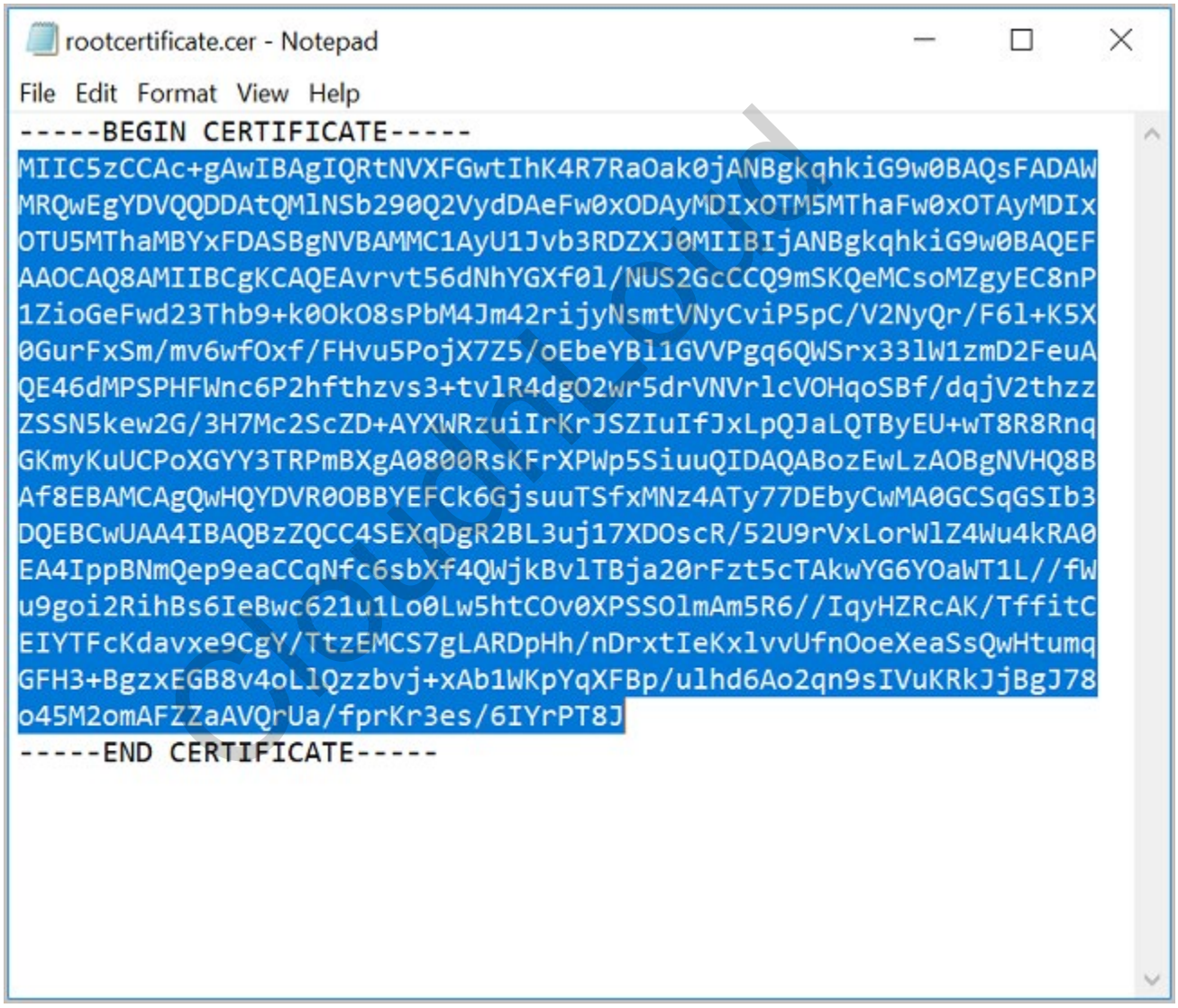


7. Your certificate is successfully exported.



8. The exported certificate looks similar to this:

9. If you open the exported certificate using Notepad, you see something similar to this example. The section in blue contains the information that is uploaded to Azure. If you open your certificate with Notepad and it does not look similar to this, typically this means you did not export it using the Base-64 encoded X.509(.CER) format. Additionally, if you want to use a different text editor, understand that some editors can introduce unintended formatting in the background. This can create problems when uploaded the text from this certificate to Azure.



Export the self-signed root certificate and private key to store it (optional)

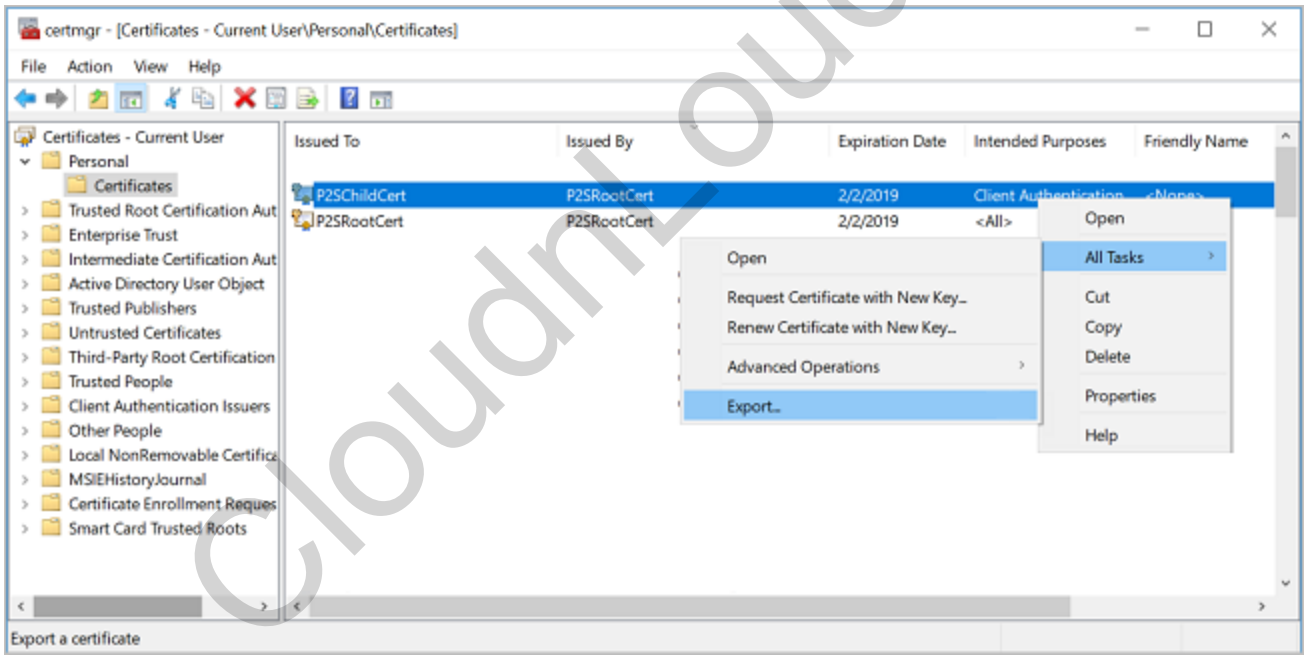
You may want to export the self-signed root certificate and store it safely as backup. If need be, you can later install it on another computer and generate more client

certificates. To export the self-signed root certificate as a .pfx, select the root certificate and use the same steps as described in Export a client certificate.

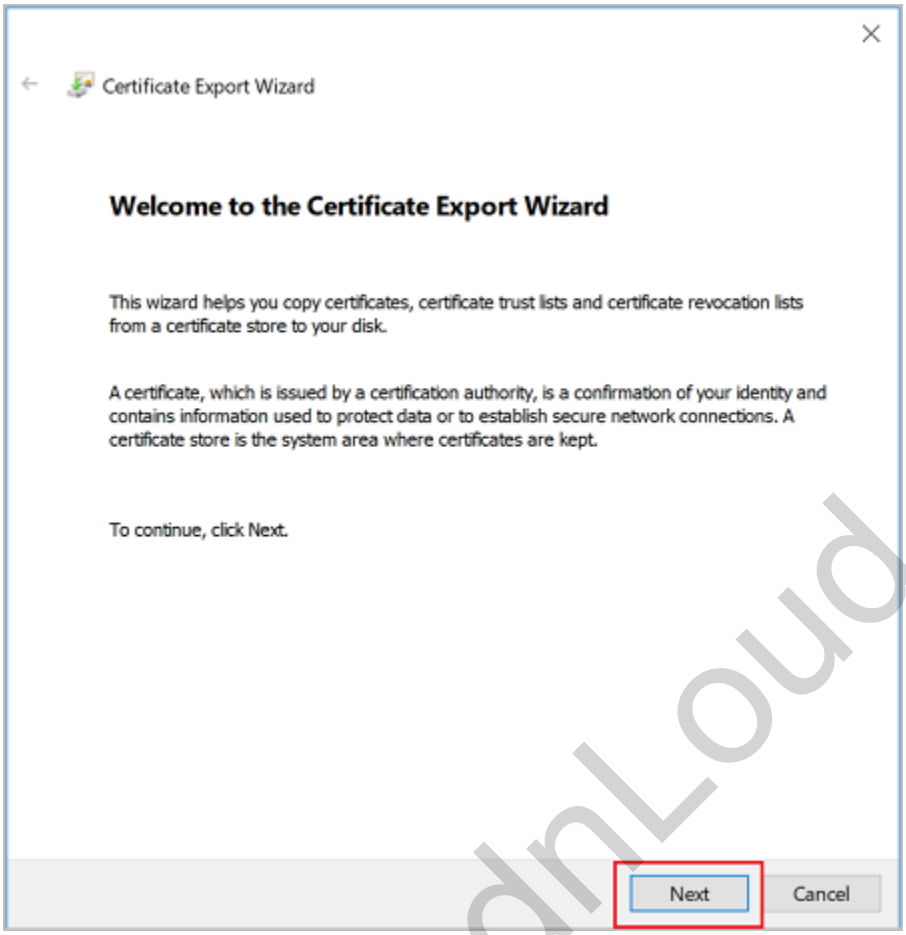
Export the client certificate

When you generate a client certificate, it's automatically installed on the computer that you used to generate it. If you want to install the client certificate on another client computer, you need to export the client certificate that you generated.

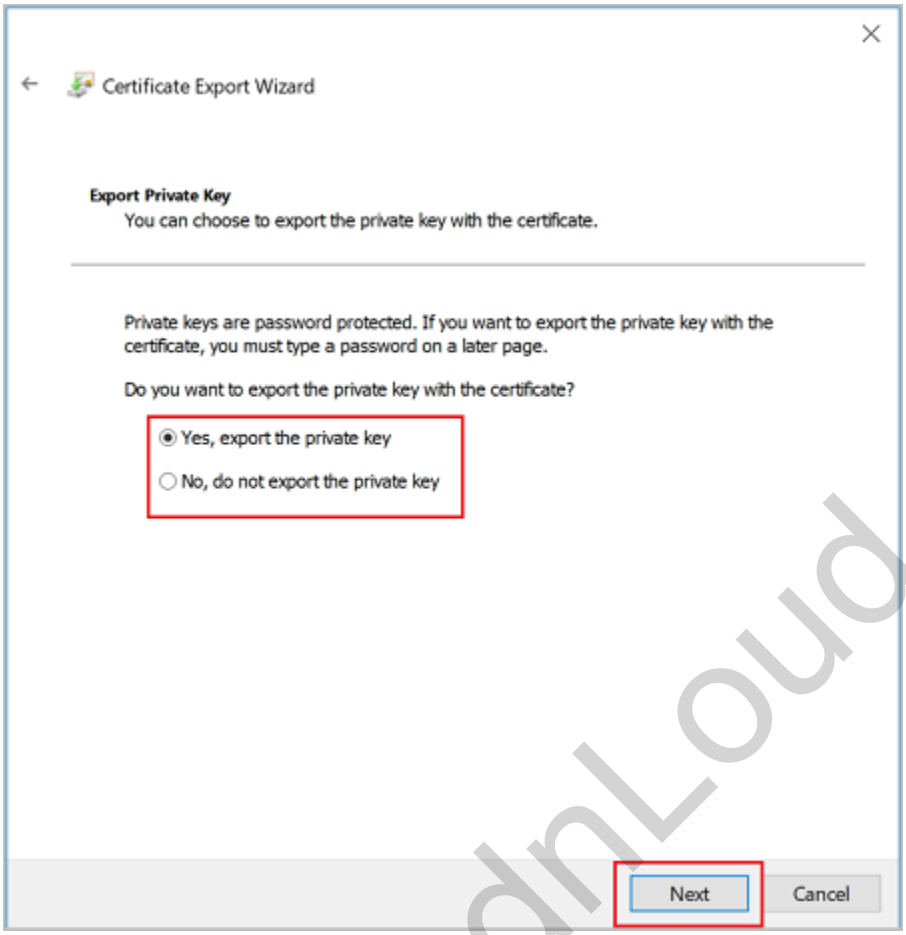
1. To export a client certificate, open **Manage user certificates**. The client certificates that you generated are, by default, located in 'Certificates - Current User\Personal\Certificates'. Right-click the client certificate that you want to export, click **all tasks**, and then click **Export** to open the **Certificate Export Wizard**.



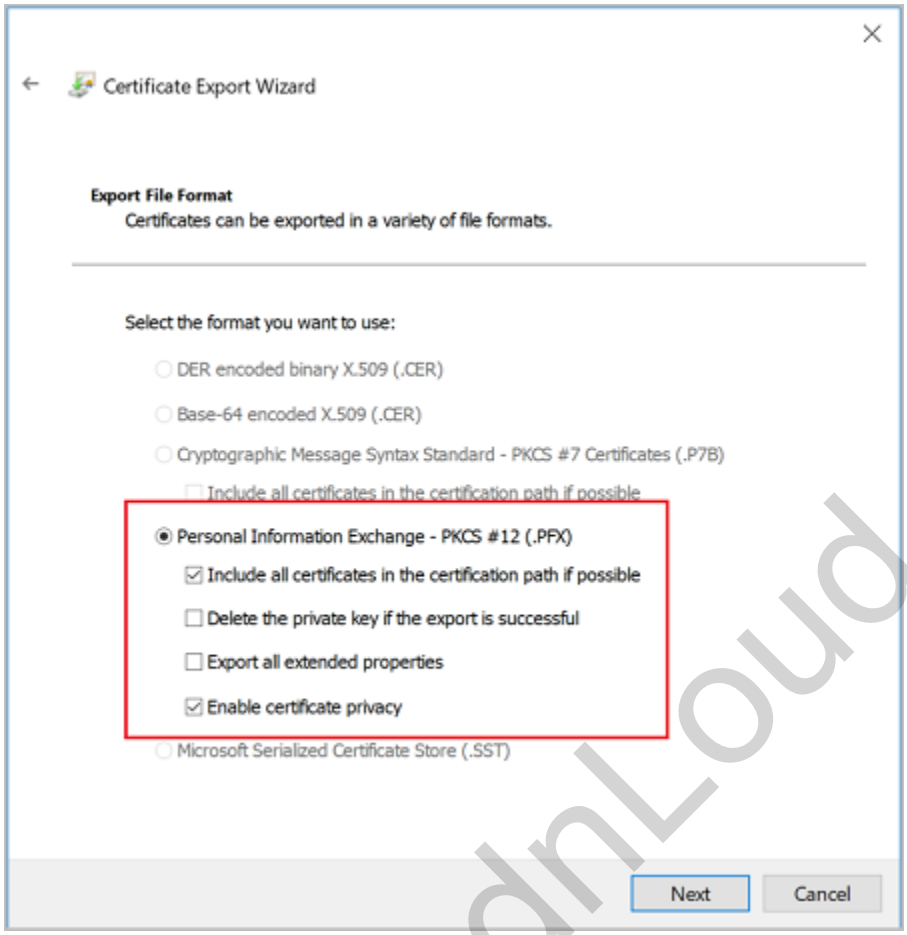
2. In the Certificate Export Wizard, click **Next** to continue.



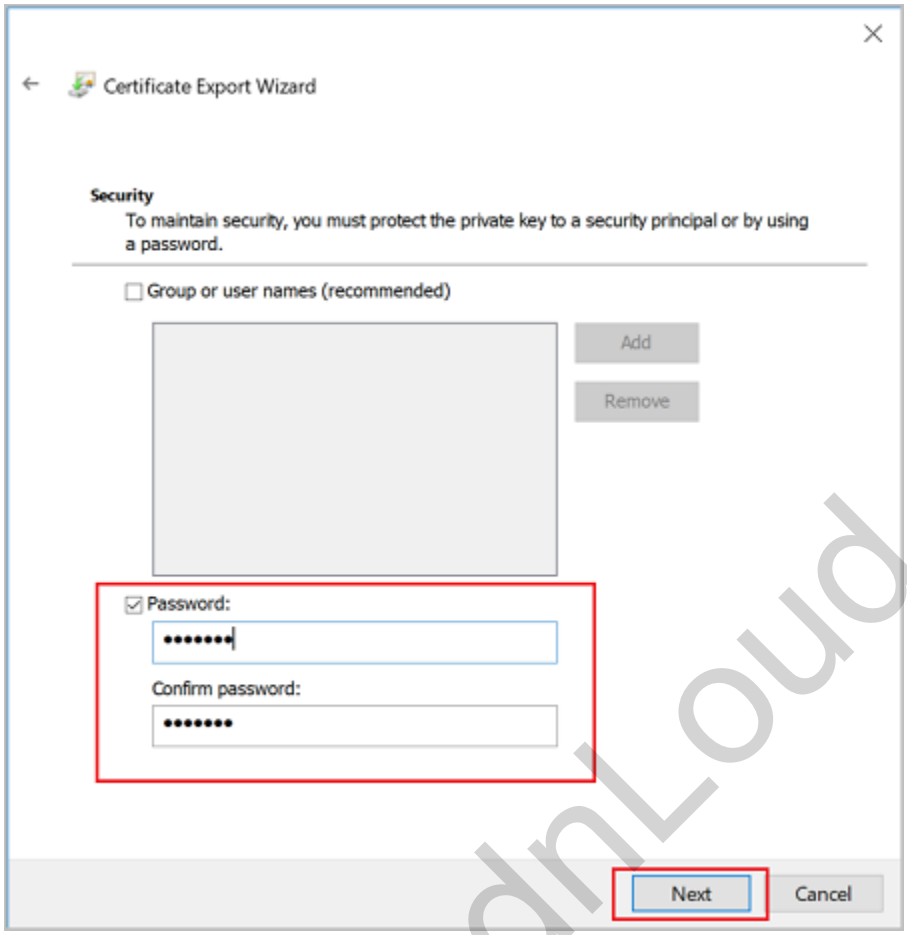
3. Select **Yes, export the private key**, and then click **Next**.



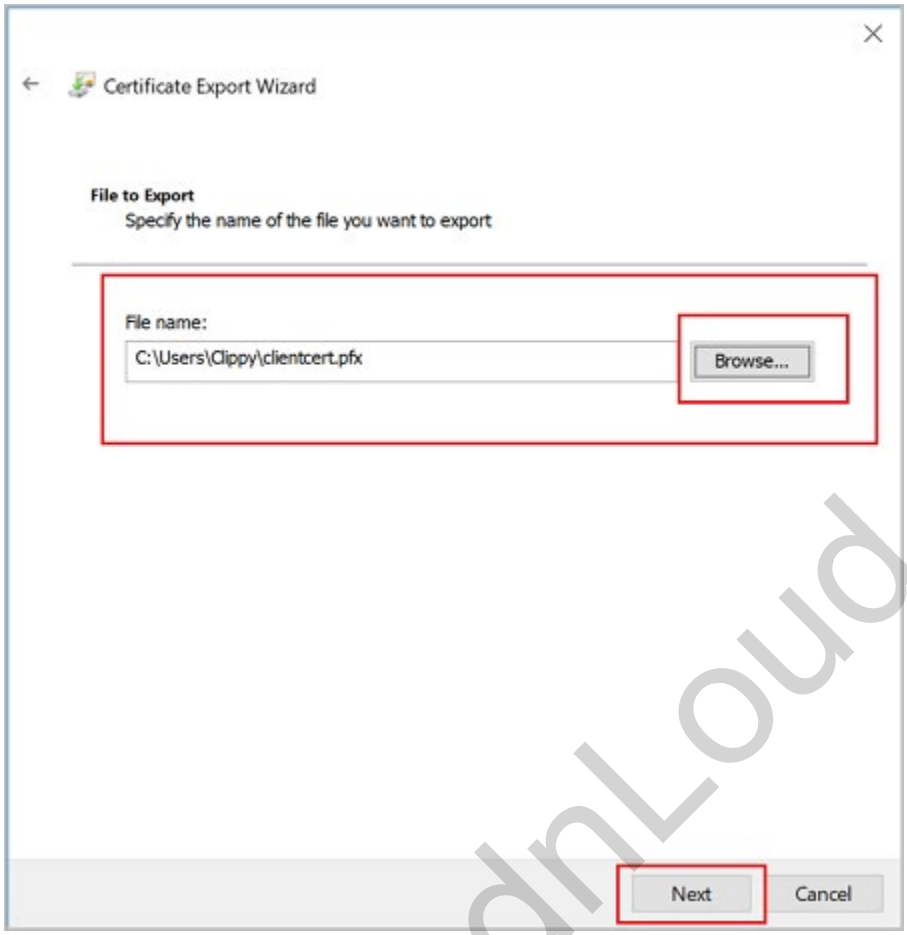
4. On the **Export File Format** page, leave the defaults selected. Make sure that **Include all certificates in the certification path if possible** is selected. This setting additionally exports the root certificate information that is required for successful client authentication. Without it, client authentication fails because the client doesn't have the trusted root certificate. Then, click **Next**.



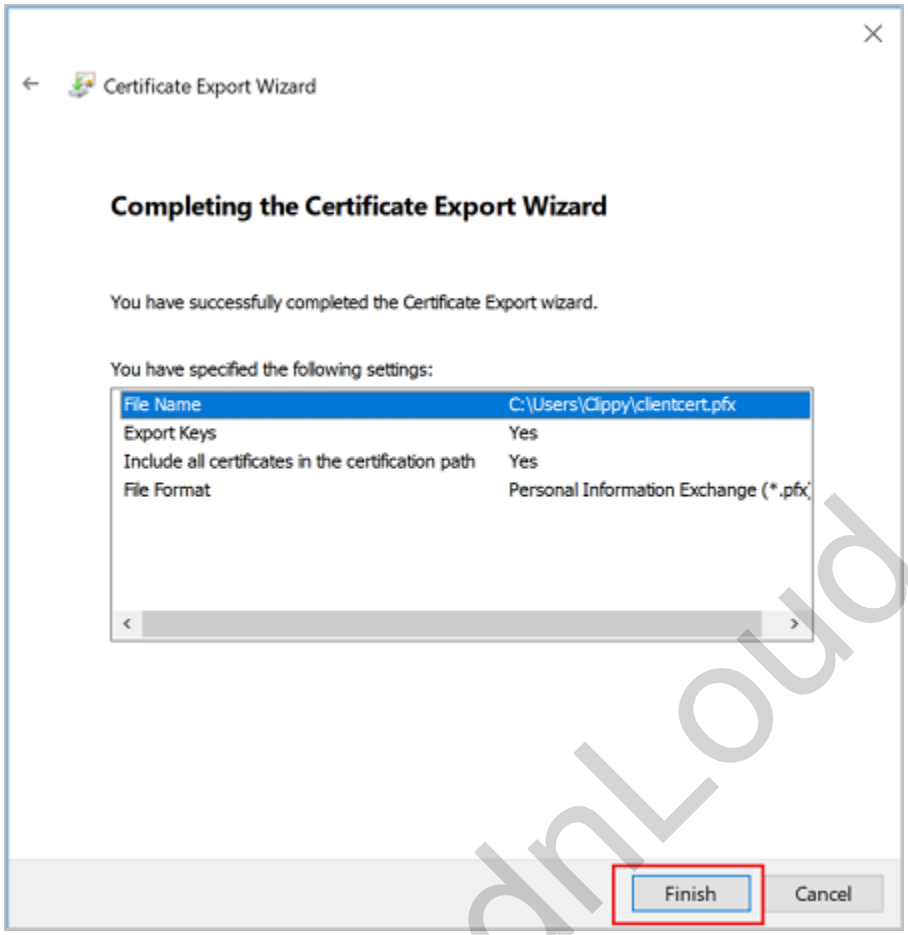
5. On the **Security** page, you must protect the private key. If you select to use a password, make sure to record or remember the password that you set for this certificate. Then, click **Next**.

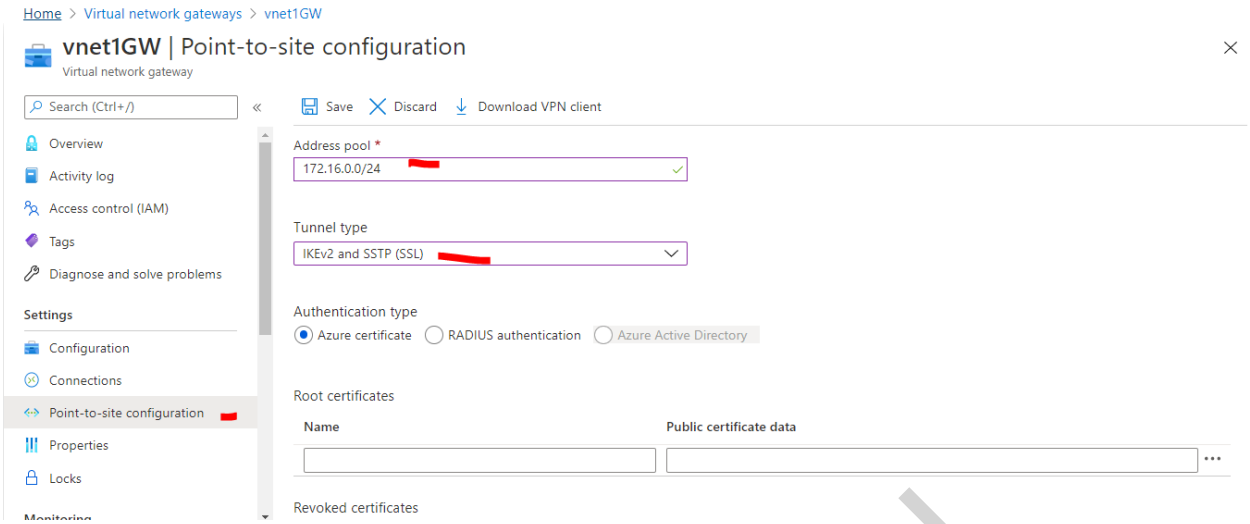


6. On the **File to Export**, **Browse** to the location to which you want to export the certificate. For **File name**, name the certificate file. Then, click **Next**.



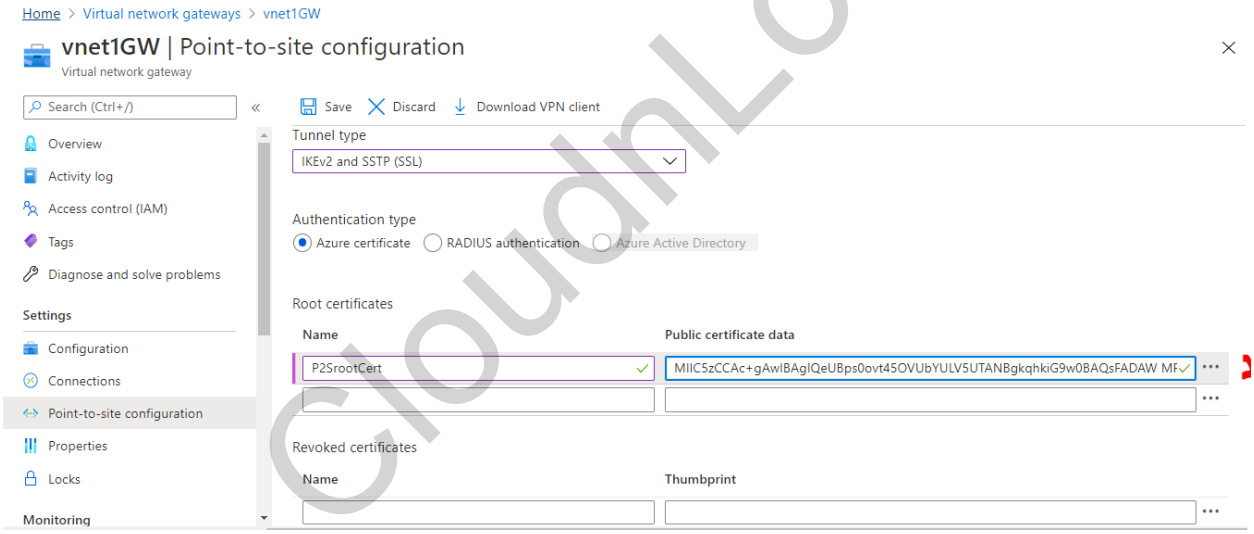
7. Click **Finish** to export the certificate.


Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name
C:\Users\Clippy\clientcert.pfx
Export Keys
Yes
Include all certificates in the certification path
Yes
File Format
Personal Information Exchange (*.pfx)
Finish
Cancel

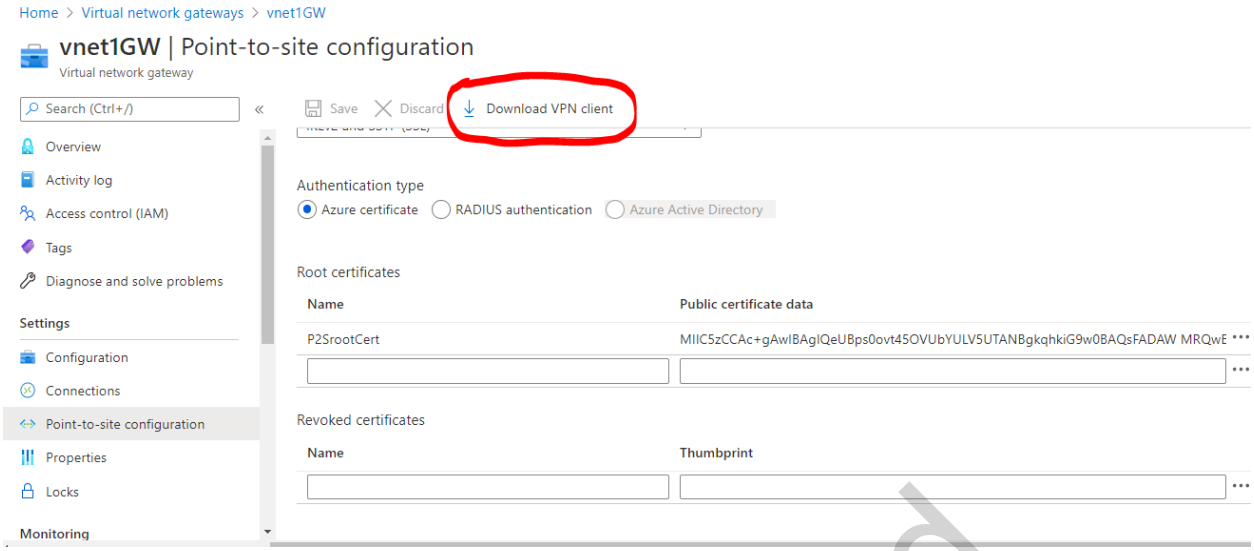


Open rootcertificate.cer file and copy the marked content

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIQeUBps0ovt45OVUbYULV5UTANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDAtQMlNSb290Q2VydDAeFw0yMDEwMDkxNzAzMDJaFw0yMTEwMDkx
NzIzMDJaMBYxFDASBgNVBAMMC1AyUlJvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA32nhGyE4Z/UlXDpoCZu2Tn8QHb1ecb0adwmzHGu/Dqmx
2hl5sac3zcnIJykuDrKXiOOl2r00BJCeaFkg7+/1TB1Y3Ar1RPi0JRA+T390ybu9
trOxtgR35na/1hhqjfVr2MBcvQI2InC+gOiN9AyvP00a3qRI/EAGZbFdkFLM+vBc
RAk/qz2fILA7jOE2LHPgDXDQAcmEUf7r0MYh+gsKJ+y/zrt9fApEFkgIcu67s3ks
bou0vEEMxyHbEfDp3o4PoRClI8WrrB3yrbTY7afxa41UNeUngbQg77ilqcVxvlfi
d9gmKDiZrKMAy5hymH6YIzEJ+L4/J67BMR66Vp37nQIDAQABozEwLzAOBgNVHQ8B
Af8EBAMCAgQwHQYDVR0OBBYEFEaOfs2e/DSmP053dXwXiULrckrMA0GCSqGSIb3
DQEBCwUAA4IBAQDT3oS0p6e5x1CbD479oJ3WOiiIe5GzKhtR6C60rWhQAJSLqASy
nYYZQ1bOdDOOIotmImv+sbtUvwtg5lcqpSfN7a8brSTq22Rewwvnh6FlQnMfIszo
XqELS6eyWXmHyF+5qYGHbW0kKcFFloLuA9Xwx/2vzrYoKooNfIc5wFdsq0IVvOW1
xM+E/a9QM1jiUWC6F/wzEkEqBhJVM+CkwOiS7yQWaRFzgEBMcRH7kPaWf0nVUqBT
9liMBVJ/XJiudhpeRo/Uu5EtQ1vCRP+hRv1/gSQYcY6s2kmKqJBV9B6tbCkG00Ub
7dWCy1NSJkMmWSuwHUzCGclQIgkOciNRXiJs
-----END CERTIFICATE-----
```

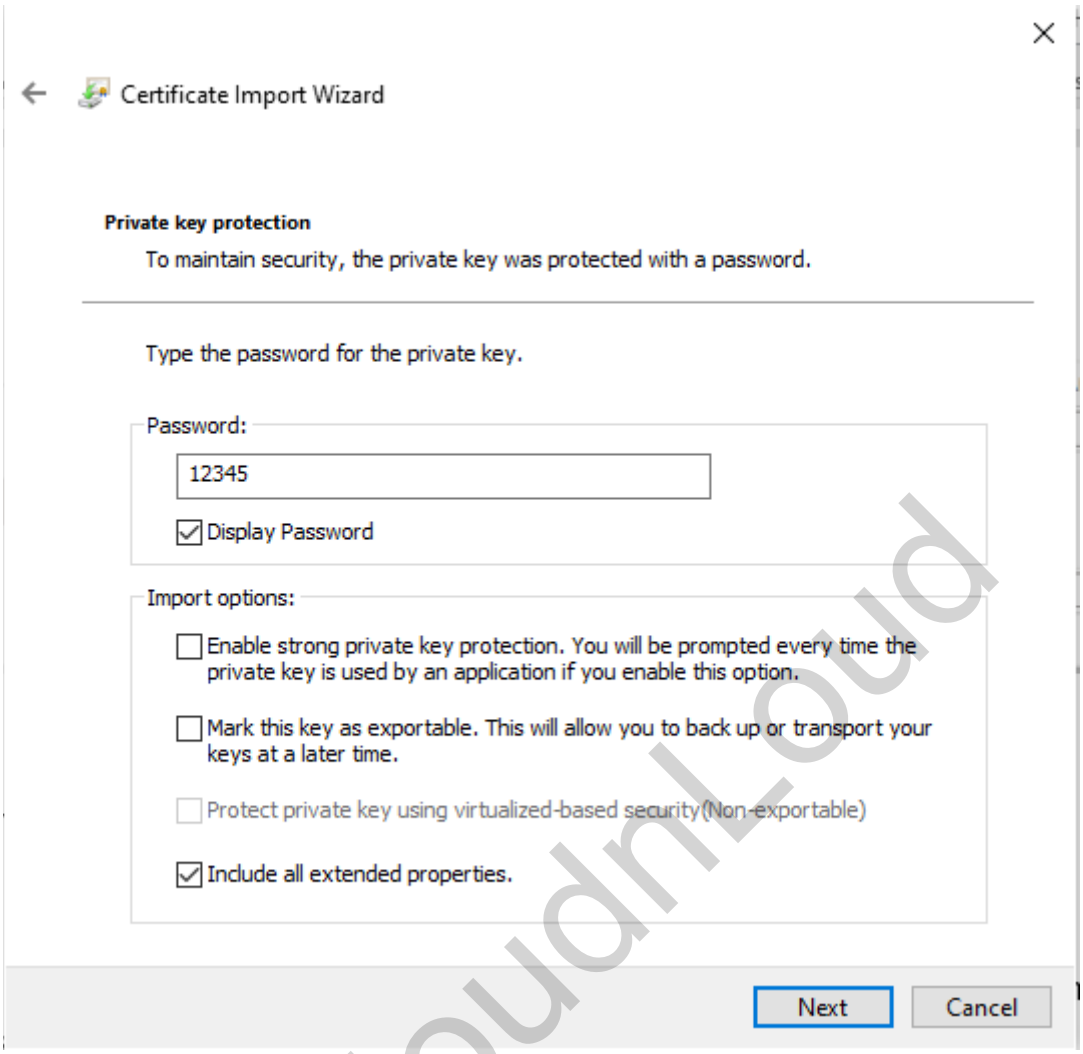


Save it

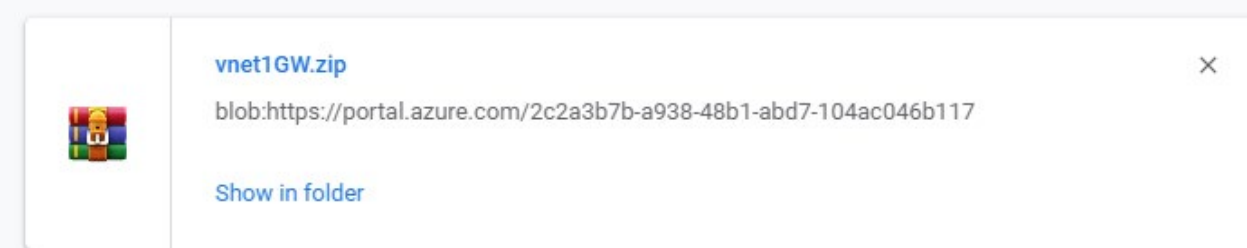


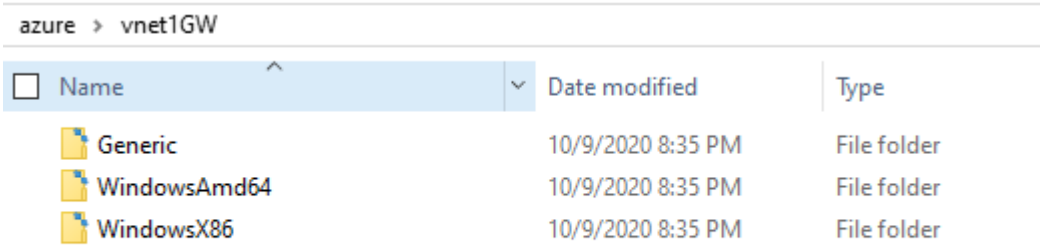
Download VPN client

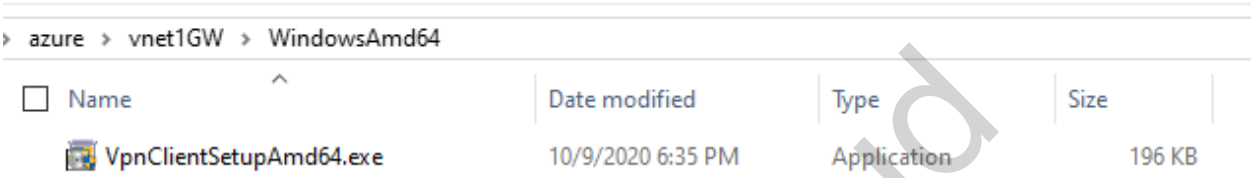
clientcertificate.pfx → from which machine you need to access azure,in that client machine you need to install client certificate.



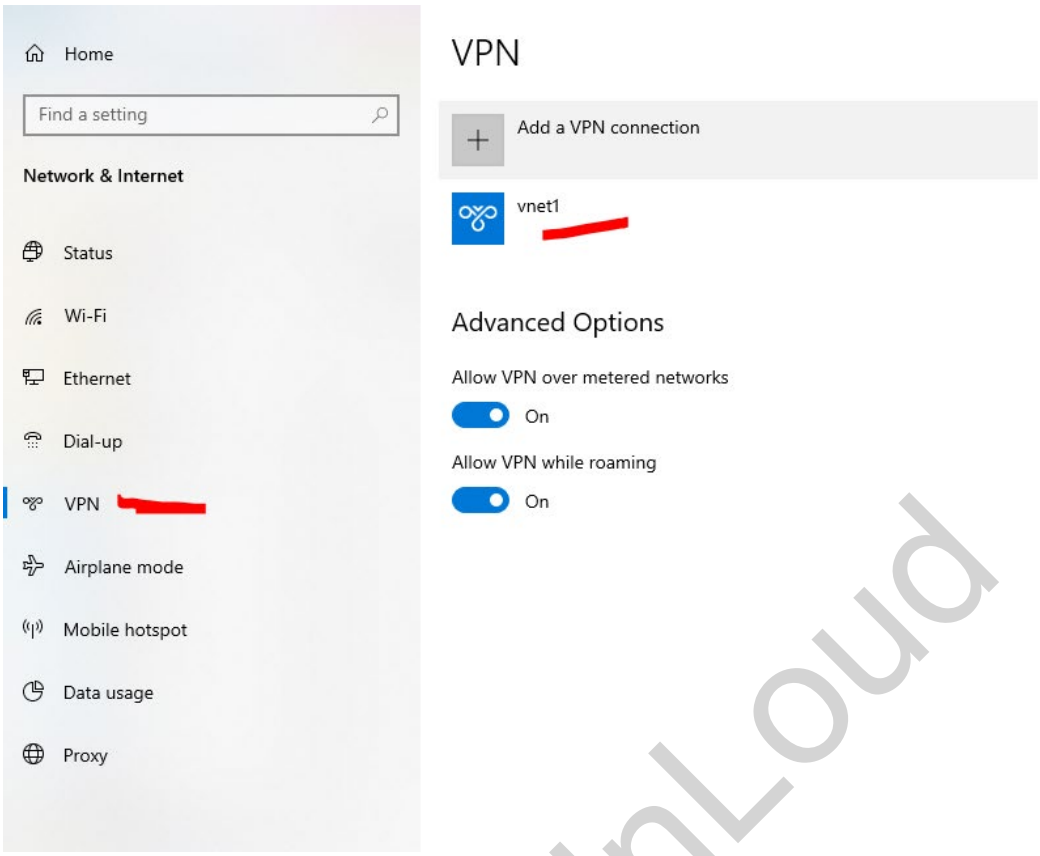
Download VPN client from the laptop

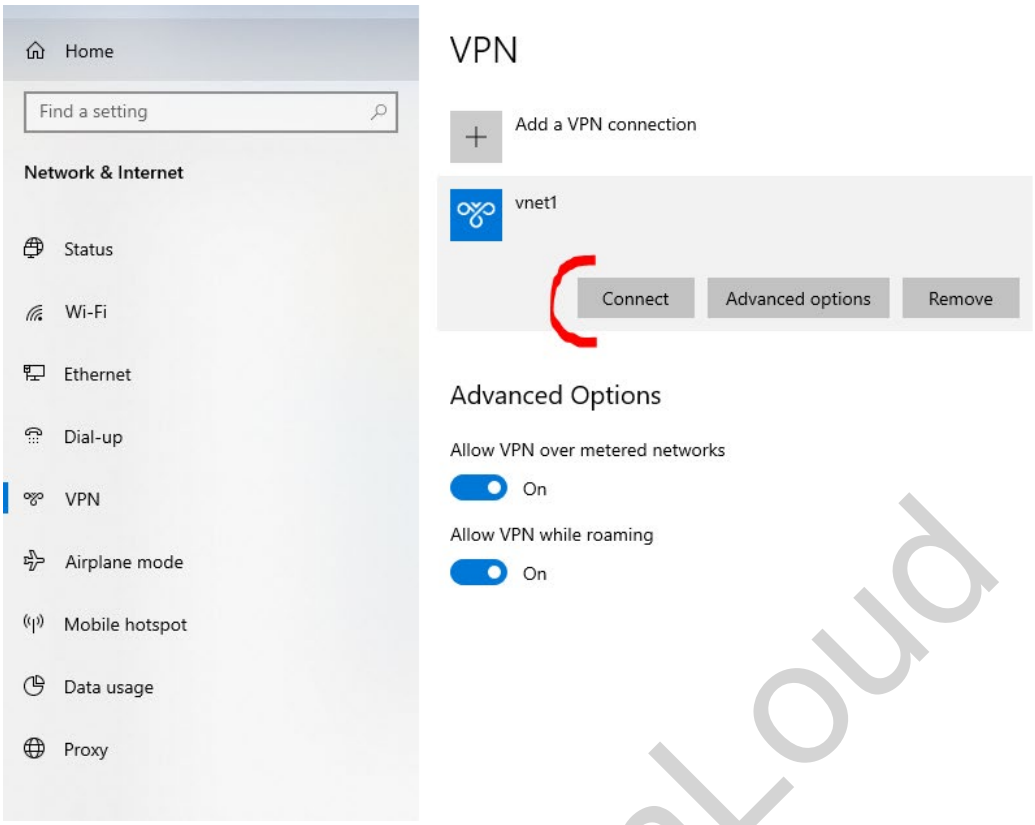


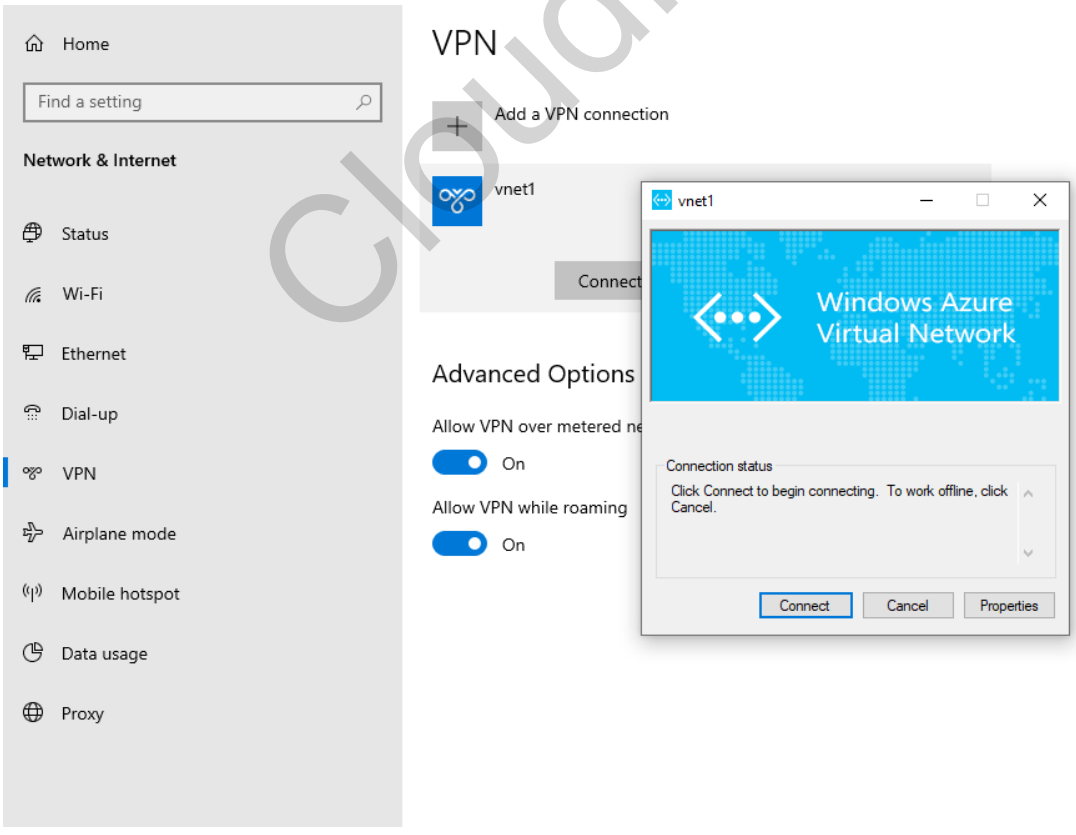


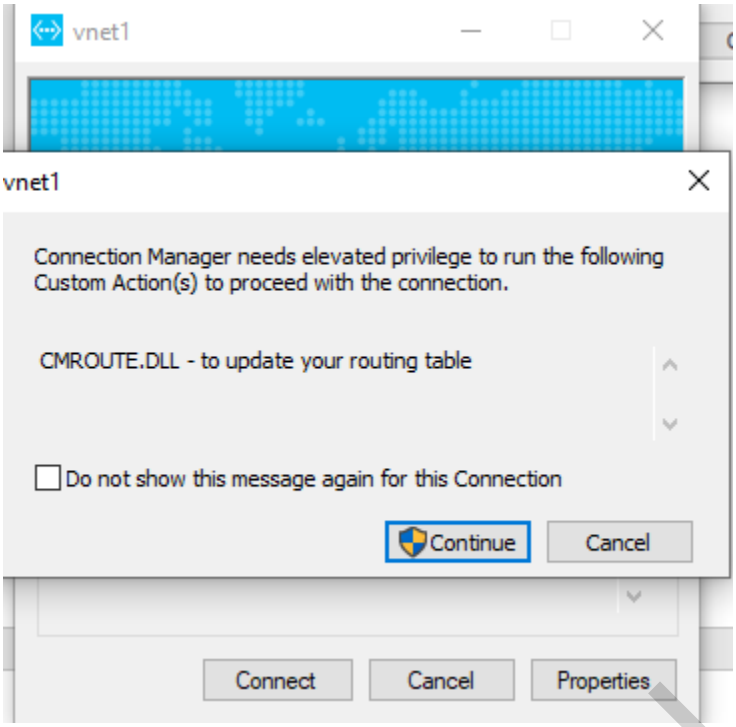


Install the VPN client software


Home
Find a setting
Network & Internet
Status
Wi-Fi
Ethernet
Dial-up
VPN
Airplane mode
Mobile hotspot
Data usage
Proxy
VPN
Add a VPN connection
vnet1
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On

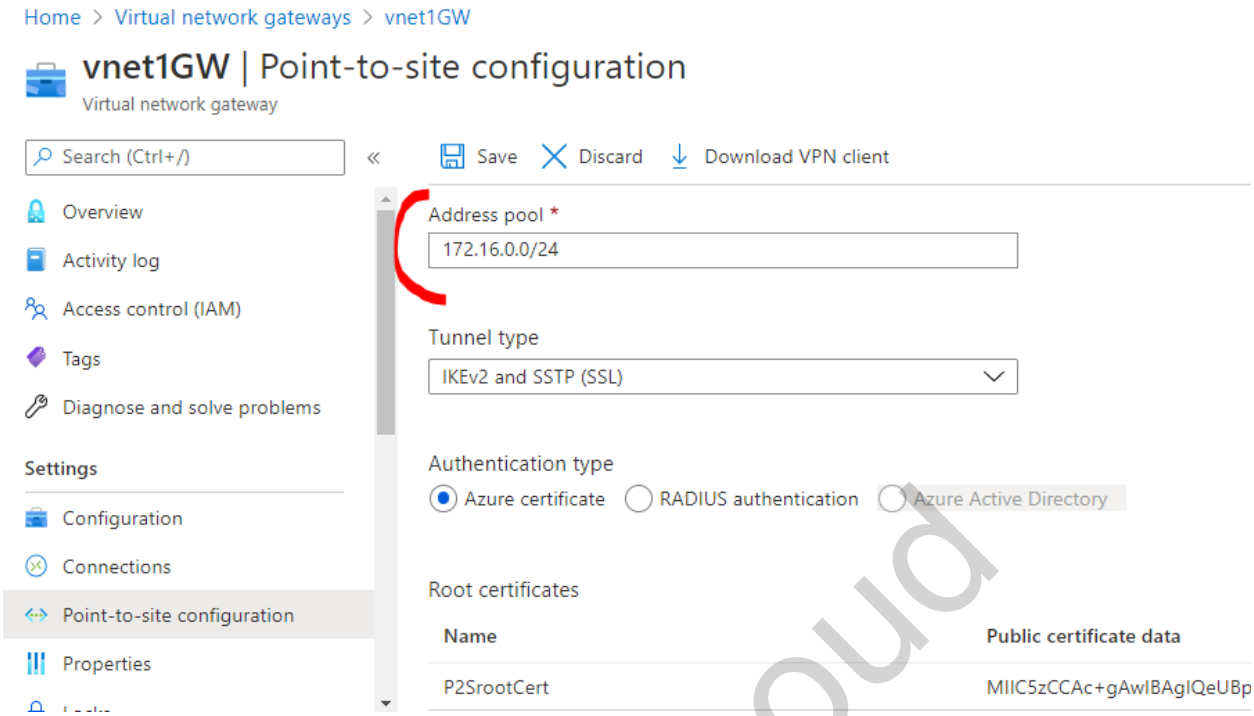

Home
Find a setting
Network & Internet
Status
Wi-Fi
Ethernet
Dial-up
VPN
Airplane mode
Mobile hotspot
Data usage
Proxy
VPN
Add a VPN connection
vnet1
Connect
Advanced options
Remove
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On


Home
Find a setting
Network & Internet
Status
Wi-Fi
Ethernet
Dial-up
VPN
Airplane mode
Mobile hotspot
Data usage
Proxy
VPN
Add a VPN connection
vnet1
Connect
Advanced Options
On
On
vnet1
Windows Azure Virtual Network
Connection status
Click Connect to begin connecting. To work offline, click Cancel.
Connect
Cancel
Properties



Now connected

See the network range



172.16.0.0/24

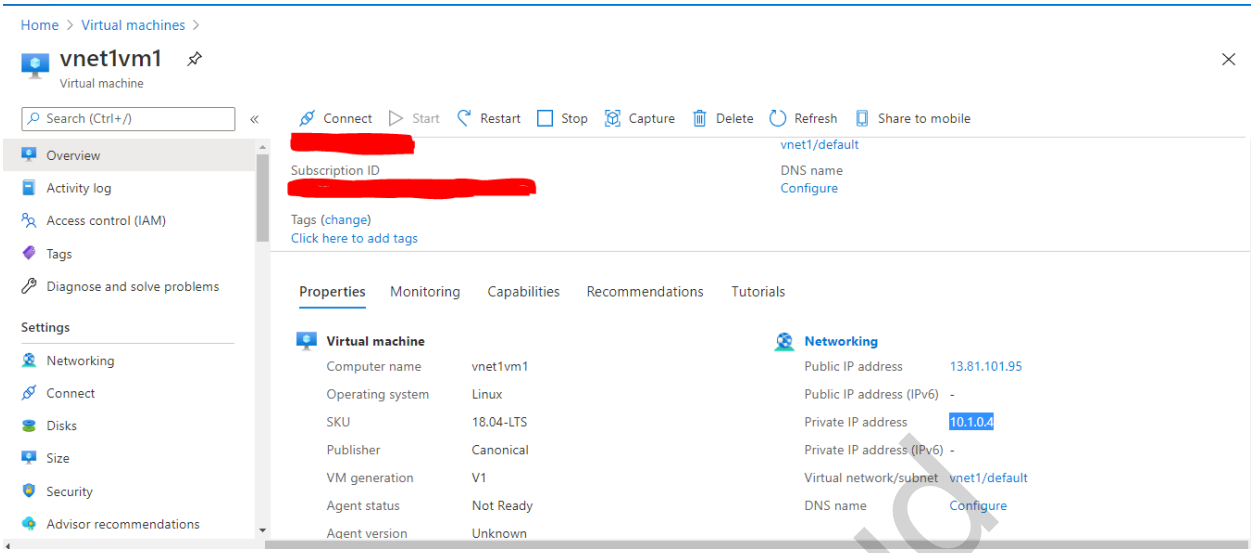
Now from your laptop

Ipconfig/all

```
PPP adapter vnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vnet1
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.16.0.130(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Create VM in the virtual network



Now the newly created VM ip address is 10.1.0.2→ internal IP address

Now you can access machine which is in the azure cloud just using its private IP address from your laptop itself.