

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")
```

.....

```
Administrator: Windows PowerShell (x86)
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:CurrentUserMy" -KeyUsageProperty Sign -KeyUsage CertSign
New-SelfSignedCertificate : Cannot find path 'Cert:\CurrentUserMy' because it does not exist.
At line:1 char:9
+ $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Cert:\CurrentUserMy:String) [New-SelfSignedCertificate], ItemNotFoundEx
ception
+ FullyQualifiedErrorId : PathNotFound,Microsoft.CertificateServices.Commands.NewSelfSignedCertificateCommand

PS C:\WINDOWS\system32> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUserMy" `
>> -Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"
New-SelfSignedCertificate : Cannot bind parameter 'Signer' to the target. Exception setting "Signer": Value cannot be
null.
Parameter name: Signer
At line:5 char:9
+ -Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"
+ ~~~~~
+ CategoryInfo          : WriteError: (:) [New-SelfSignedCertificate], ParameterBindingException
+ FullyQualifiedErrorId : ParameterBindingFailed,Microsoft.CertificateServices.Commands.NewSelfSignedCertificateCo
mmand

PS C:\WINDOWS\system32> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUserMy" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\WINDOWS\system32> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUserMy" `
>> -Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUserMy

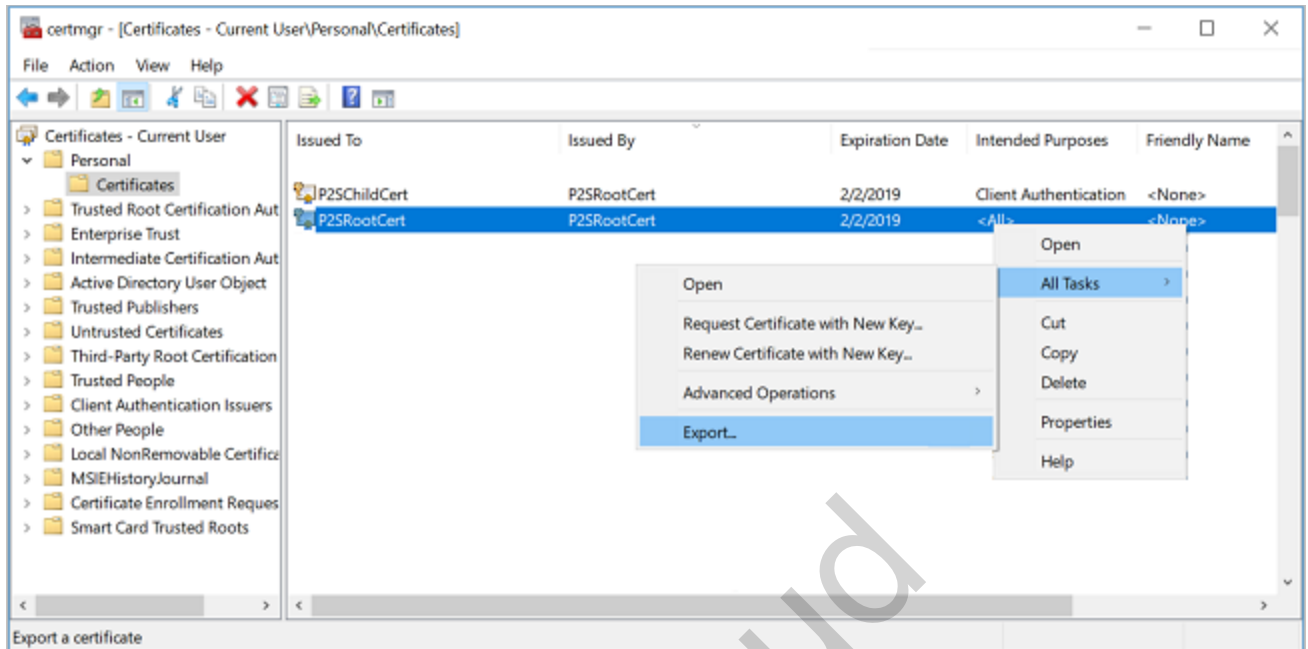
Thumbprint                               Subject
-----
62EA95F5EDD39A007C544D76860DEED46627D76C CN=P2SChildCert

PS C:\WINDOWS\system32>
```

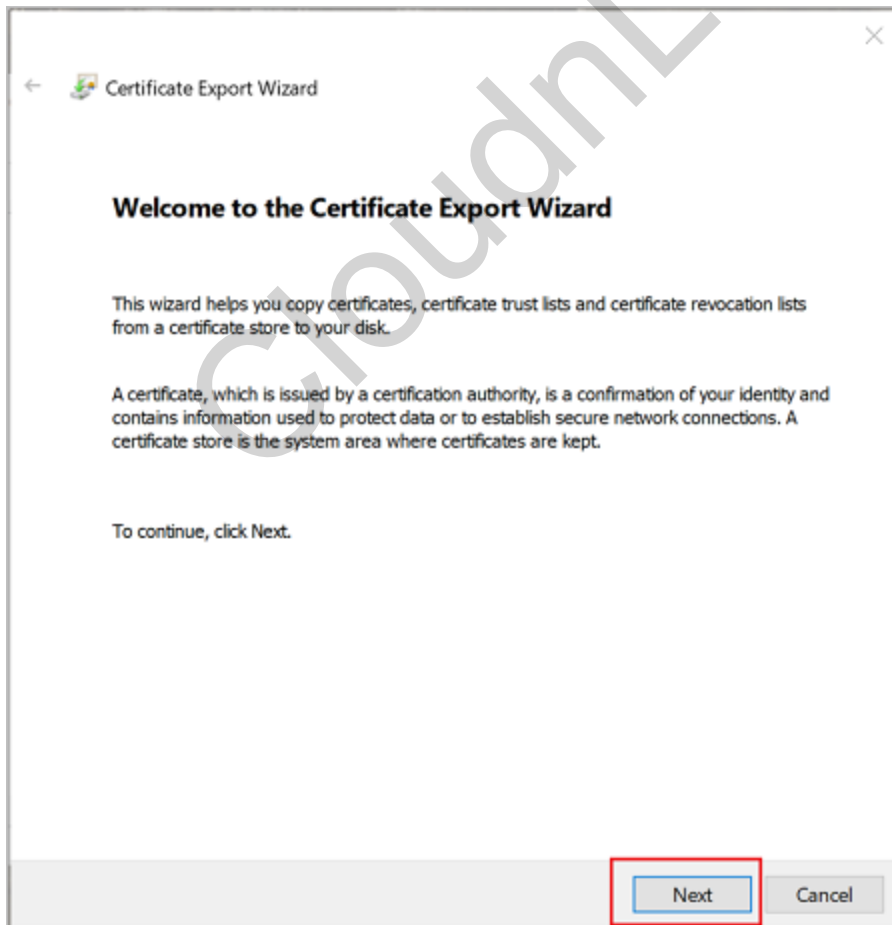
Export the root certificate public key (.cer)

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:

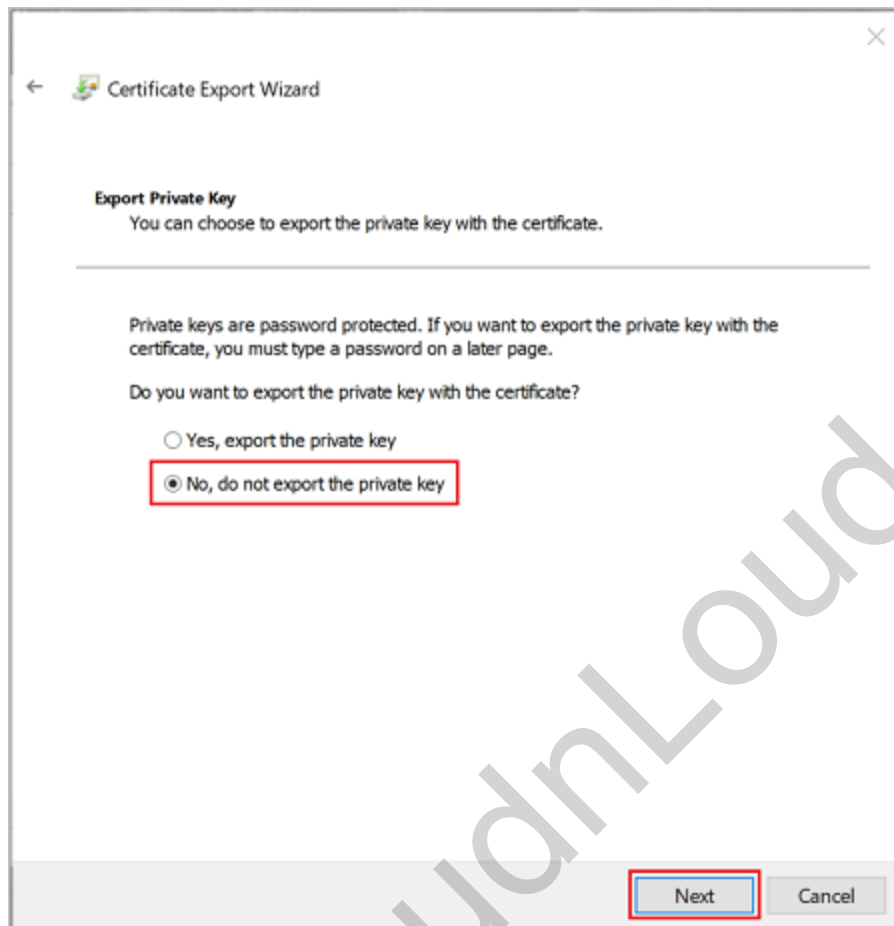
1. To obtain a .cer file from the certificate, open **Manage user certificates**. Locate the self-signed root certificate, typically in 'Certificates - Current User\Personal\Certificates', and right-click. Click **All Tasks**, and then click **Export**. This opens the **Certificate Export Wizard**. If 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.



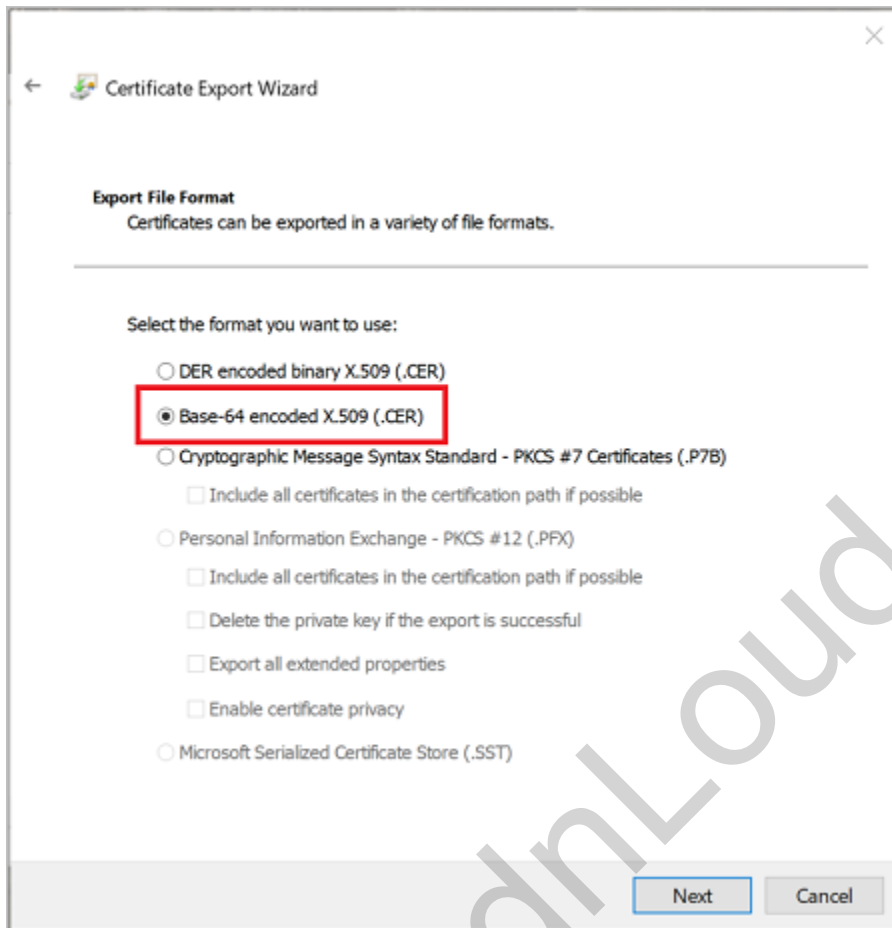
2. In the Wizard, click **Next**.



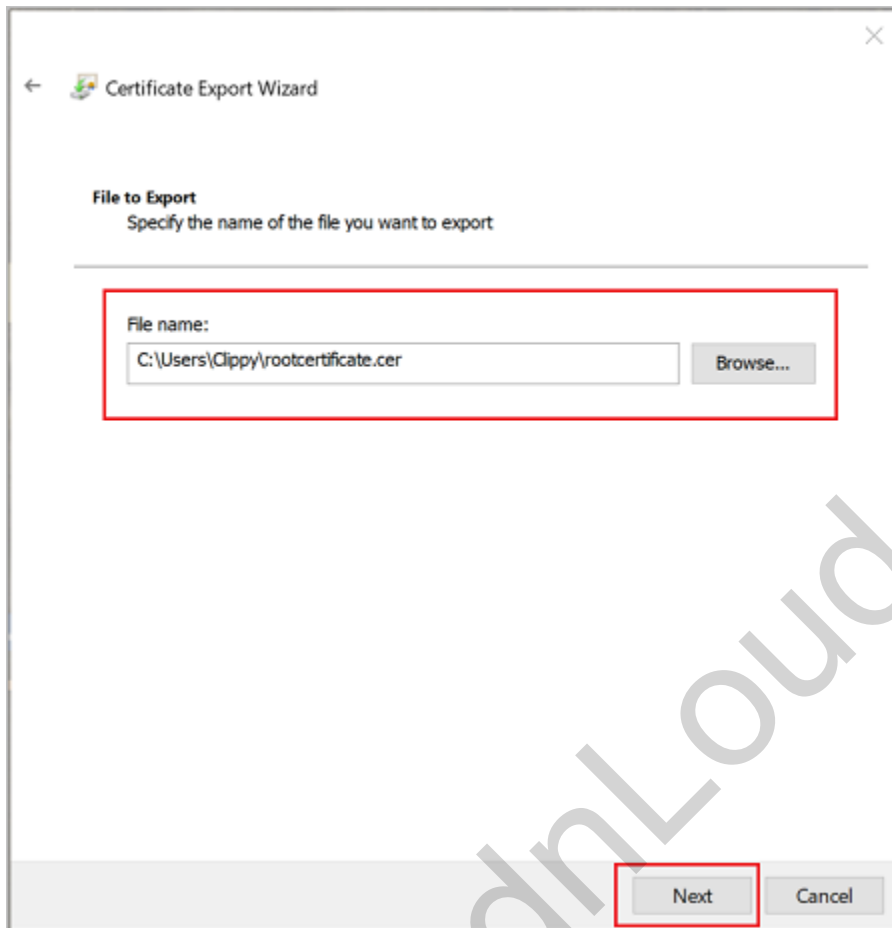
3. Select **No, do not export the private key**, and then click **Next**.



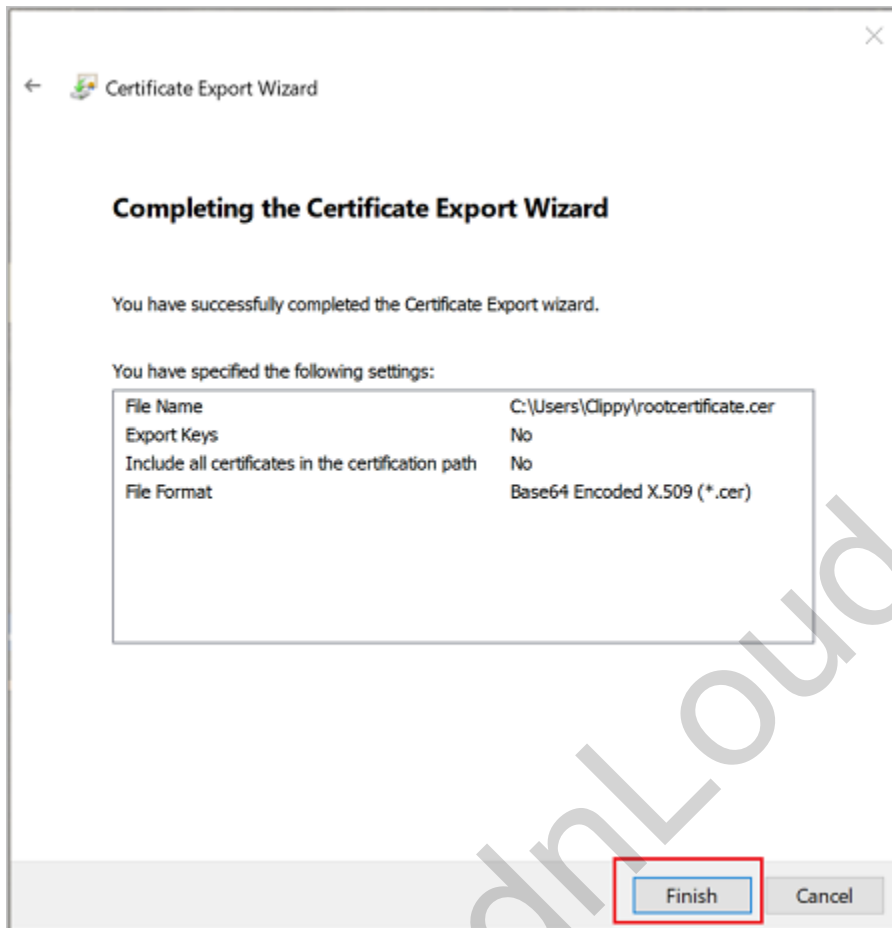
4. On the **Export File Format** page, select **Base-64 encoded X.509 (.CER)**., and then click **Next**.



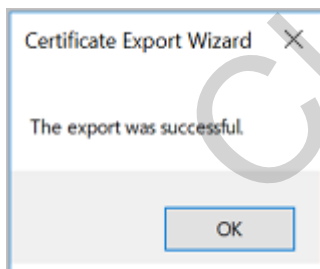
5. For **File to Export**, **Browse** to the location to which you want to export the certificate. For **File name**, name the certificate file. Then, click **Next**.



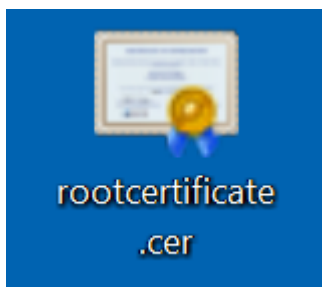
6. Click **Finish** to export the certificate.



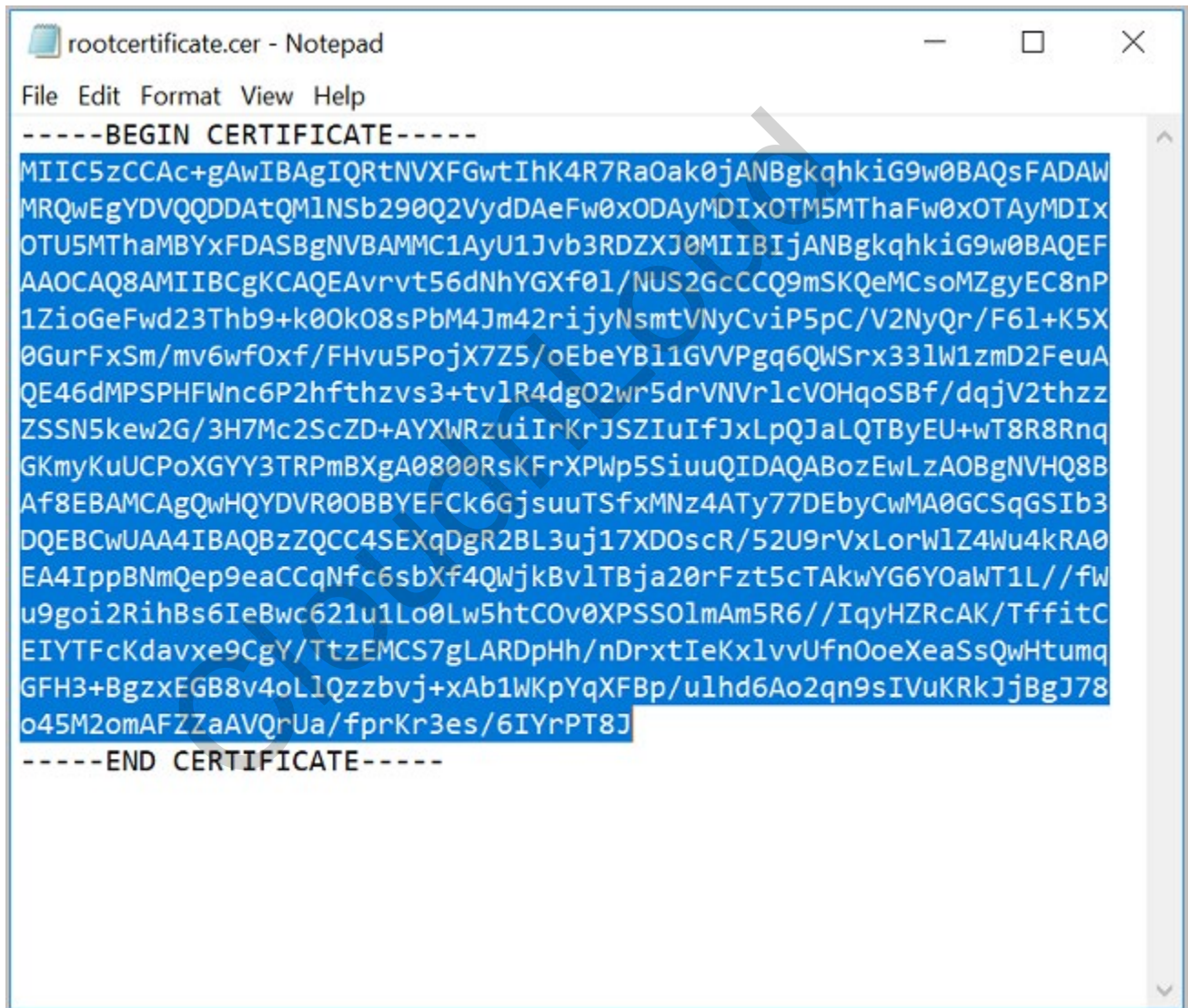
7. Your certificate is successfully exported.



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.



```
-----BEGIN CERTIFICATE-----
MIIC5zCCAC+gAwIBAgIQRtNVXFGwtIhK4R7RaOak0jANBgkqhkiG9w0BAQsFADAw
MRQwEgYDVQQDDAtQMlNSb290Q2VydAeFw0xODAyMDIxOTM5MThaFw0xOTAyMDIx
OTU5MThaMBYxFDASBgNVBAMMC1AyU1Jvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAavrvt56dNhYGXf0l/NUS2GcCCQ9mSKQeMCsoMZgyEC8nP
1ZioGeFwd23Thb9+k0Ok08sPbM4Jm42rijyNsmtVNyCviP5pC/V2NyQr/F6l+K5X
0GurFxSm/mv6wf0xf/FHvu5PoJX7Z5/oEbeYB11GVVPgq6QWSrx33lW1zmD2FeuA
QE46dMPSPHFWnc6P2hfthzvs3+tv1R4dg02wr5drVNVr1cVOHqoSBf/dqjV2thzz
ZSSN5kew2G/3H7Mc2ScZD+AYXWRzuiIrKrJSZIUfJxLpQJaLQTBByEU+wT8R8Rnq
GKmyKuUCPoXGYY3TRPmBXgA0800RsKFrXPWp5SiuuQIDAQABozEwLzA0BgNVHQ8B
Af8EBAMCAgQwHQYDVR00BBYEFck6GjsuuTSfxMNz4ATy77DEbyCwMA0GCSqGSIb3
DQEBCwUAA4IBAQBzZQCC4SEXqDgR2BL3uj17XD0scR/52U9rVxLorWlZ4Wu4kRA0
EA4IppBNmQep9eaCCqNfc6sbXf4QWjkBv1TBja20rFzt5cTAKwYG6Y0aWT1L//fW
u9goi2RihBs6IeBwc621u1Lo0Lw5htCOv0XPSS0lmAm5R6//IqyHZRcAK/TffitC
EIYTFcKdavaxe9CgY/TtzEMCS7gLARDpHh/nDrxtIeKxlvvUfnOoeXeaSsQwHtumq
GFH3+BgzxEGB8v4oLlQzzbvj+xAblWKpYqXFBp/ulhd6Ao2qn9sIVuKrkJjBgJ78
o45M2omAFZZaAVQrUa/fprKr3es/6IYrPT8J
-----END CERTIFICATE-----
```

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

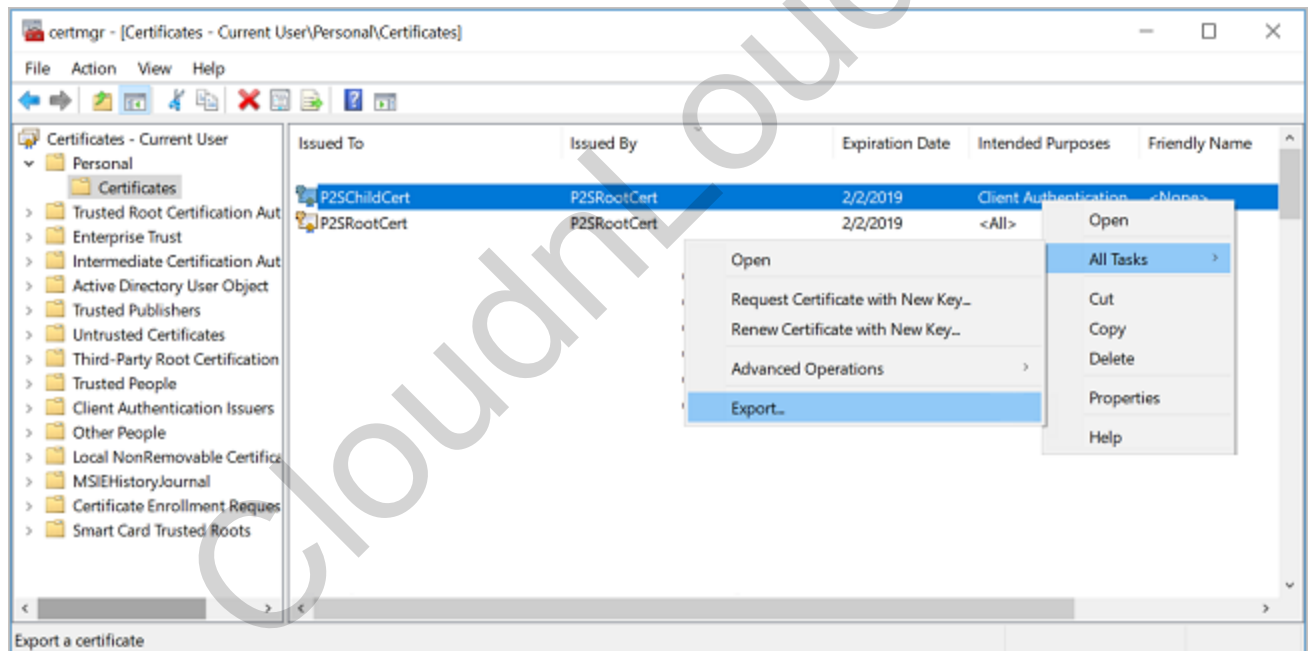
You may want to export the self-signed root certificate and store it safely as backup. If need be, you can later install it on another computer and generate more client

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](#).

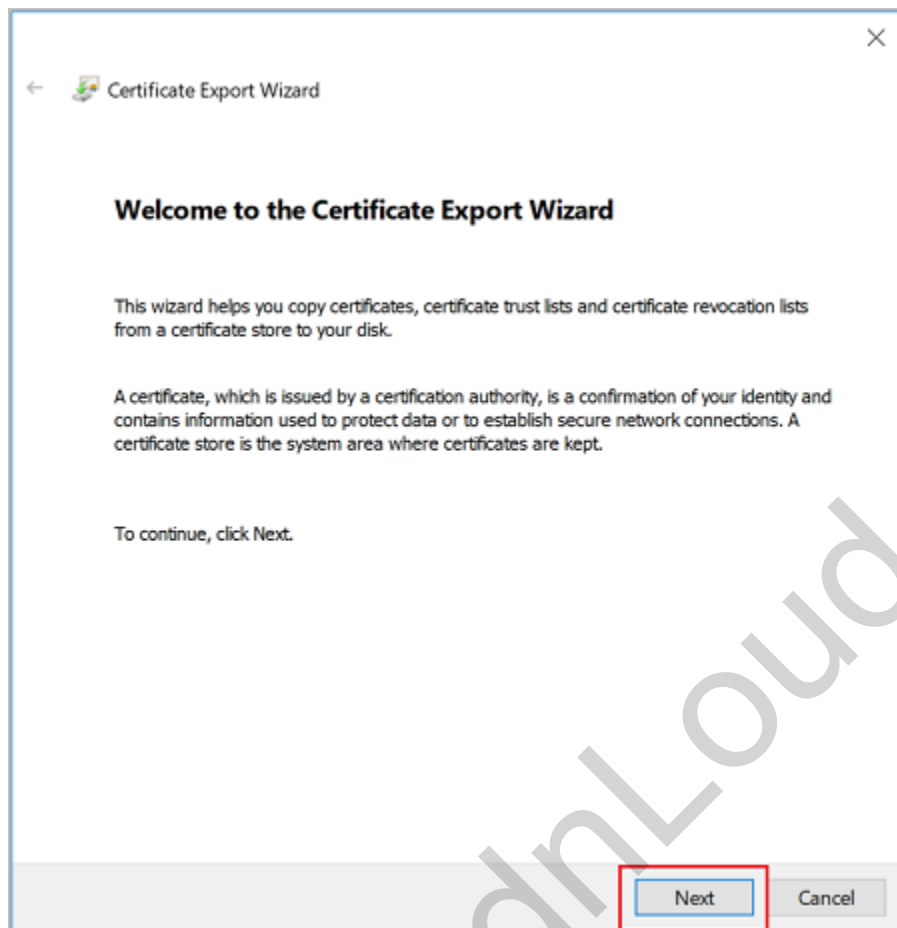
Export the client certificate

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.

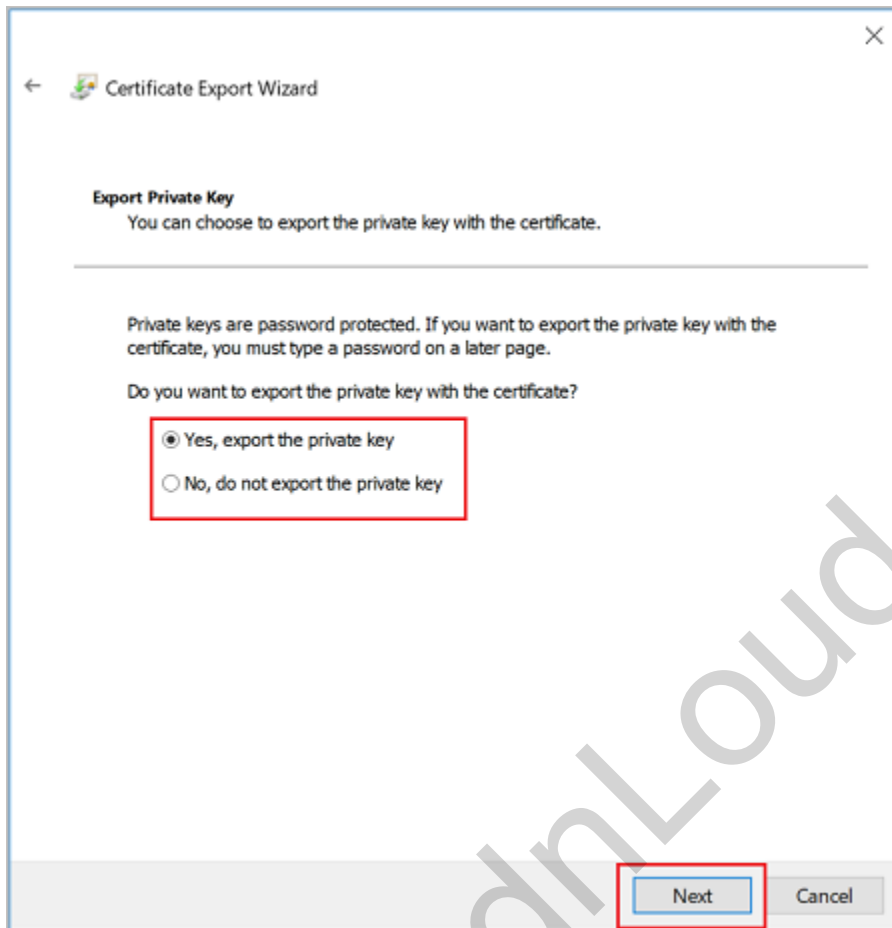
1. To export a client certificate, open **Manage user certificates**. The client certificates that you generated are, by default, located in 'Certificates - Current User\Personal\Certificates'. Right-click the client certificate that you want to export, click **all tasks**, and then click **Export**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



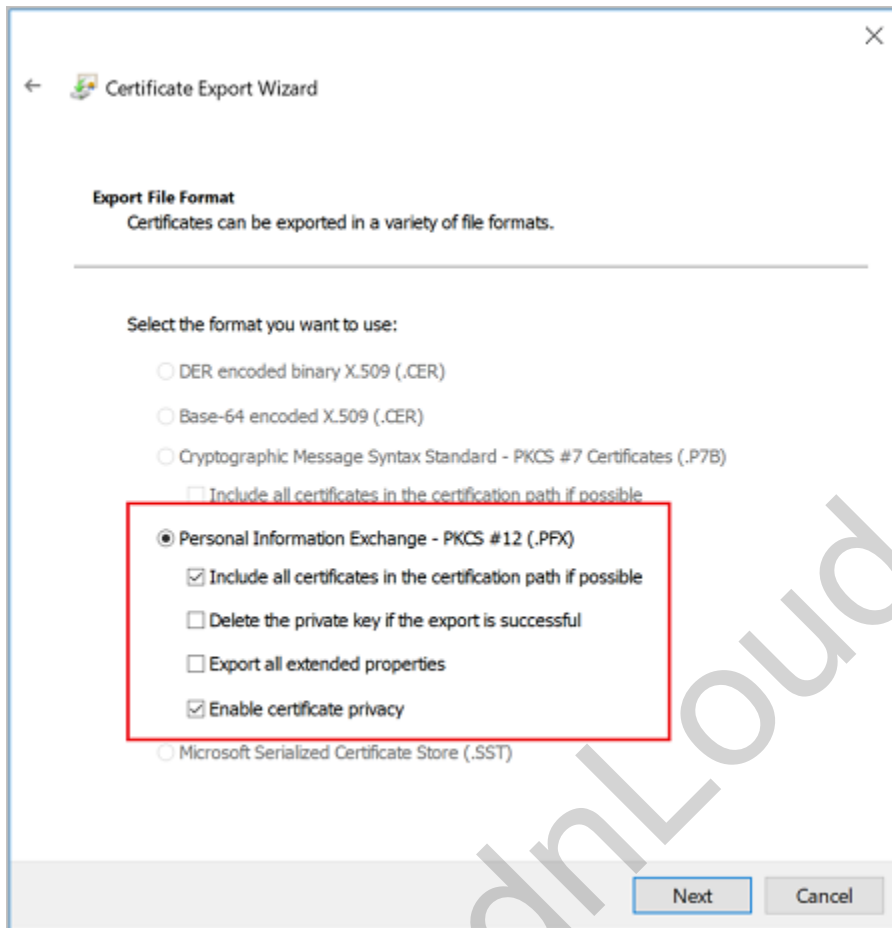
2. In the Certificate Export Wizard, click **Next** to continue.



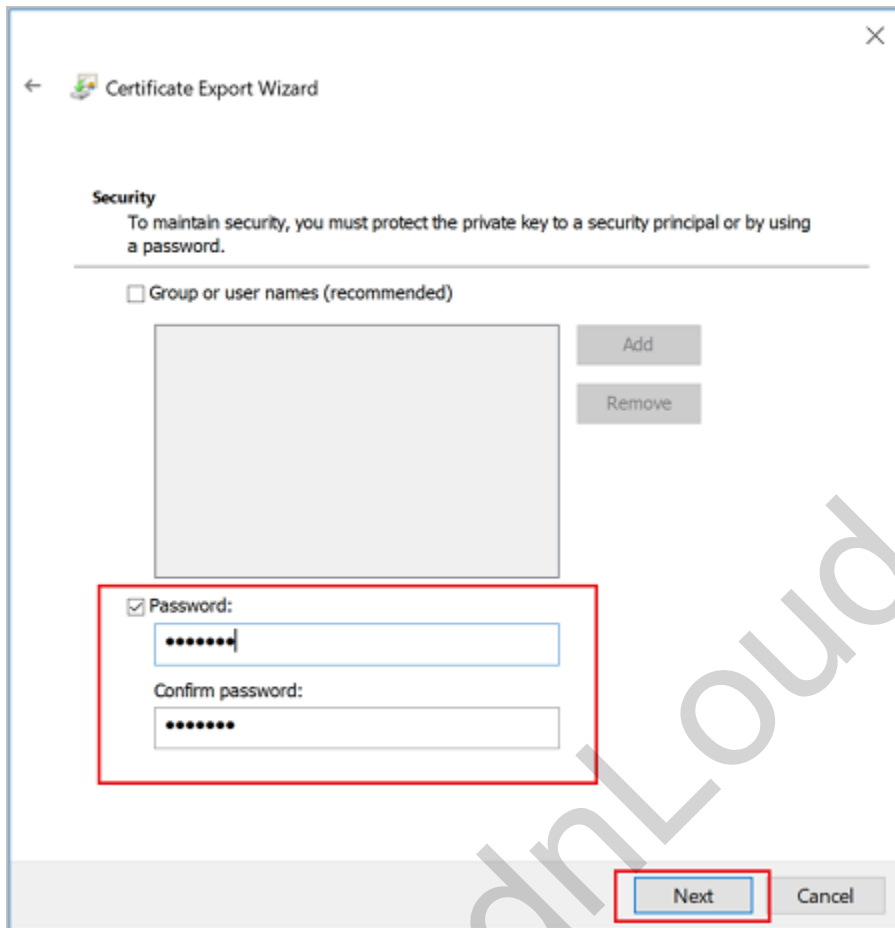
3. Select **Yes, export the private key**, and then click **Next**.



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**.



The image shows the 'Certificate Export Wizard' window, specifically the 'Security' step. The window title is 'Certificate Export Wizard'. Below the title bar, there is a back arrow and the text 'Certificate Export Wizard'. The main heading is 'Security', followed by the instruction: 'To maintain security, you must protect the private key to a security principal or by using a password.' There are two options: 'Group or user names (recommended)' with an unchecked checkbox, and 'Password' with a checked checkbox. The 'Password' option is highlighted with a red rectangle. It includes two text boxes: 'Password:' and 'Confirm password:', both containing masked characters (dots). To the right of the 'Group or user names' list is a large empty box and two buttons: 'Add' and 'Remove'. At the bottom right, there are 'Next' and 'Cancel' buttons. The 'Next' button is highlighted with a red rectangle. A large, diagonal watermark 'CloudnLoud' is visible across the center of the image.

← 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)

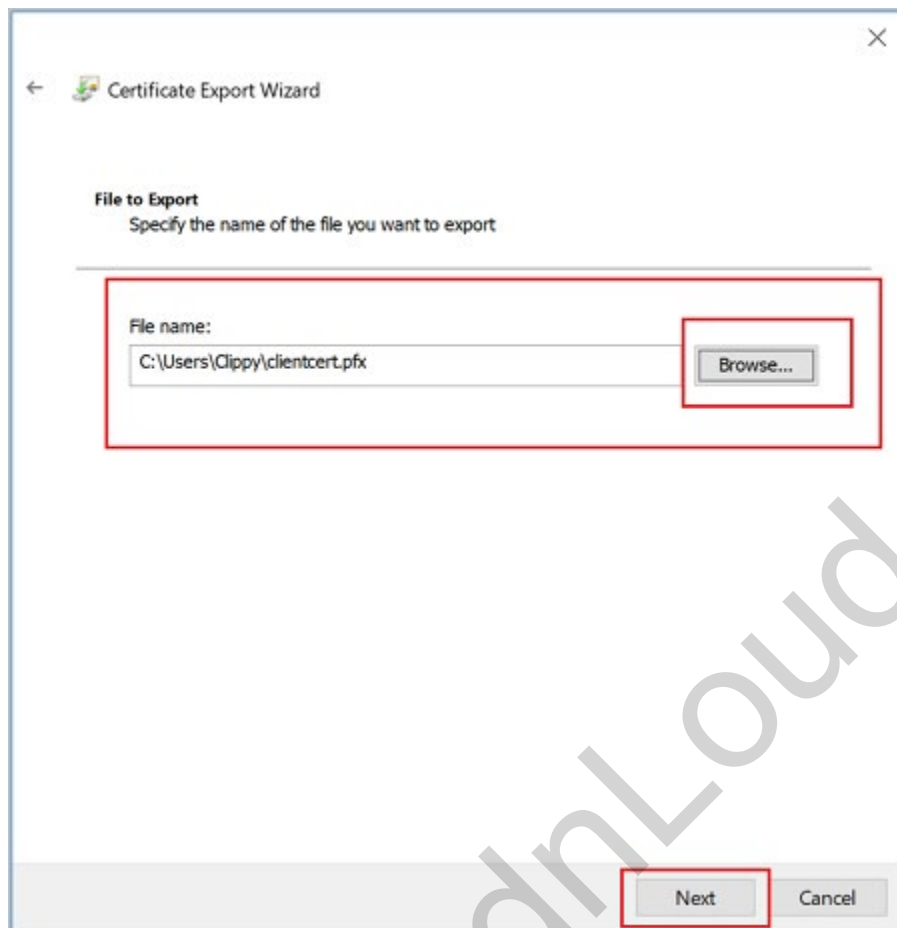
☒ Password:

Confirm password:

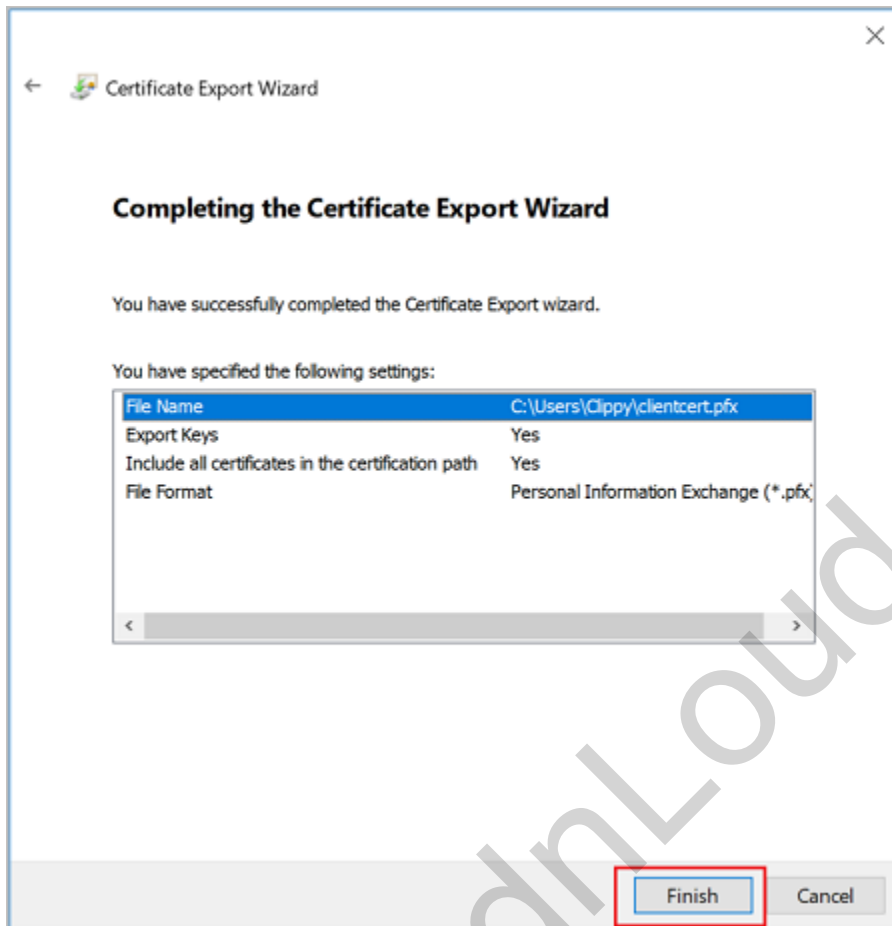
Add
Remove

Next Cancel

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.



Home > Virtual network gateways > vnet1GW

vnet1GW | 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

Monitoring

Address pool *

172.16.0.0/24

Tunnel type

IKEv2 and SSTP (SSL)

Authentication type

☒ Azure certificate ☐ RADIUS authentication ☐ Azure Active Directory

Root certificates

Name	Public certificate data

Revoked certificates

Open rootcertificate.cer file and copy the marked content

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIQeUBps0ovt45OVUbYULV5UTANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDATQm1NSb290Q2VydDAeFw0yMDEwMDkxNzAzMDJaFw0yMTEwMDkx
NzIzMDJhMBYxZDASBgNVBAMMC1AyU1Jvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA32nhGyE4Z/U1XDpocZu2Tn8QHblecb0adwmzHGu/Dqmx
2hl5sac3zcnIJykuDrKXi0012r00BJCeaFkg7+/1TB1Y3Ar1RPi0JRA+T390ybu9
trOxtgR35na/1hhqjfvR2MBcvQI2InC+gOiN9AyvP00a3qRI/EAGZbFdkFLM+vBc
RAk/qz2fILa7jOE2LHPgDXDQAcmeUf7r0MYh+gsKJ+y/zrt9fApEFkgIcu67s3ks
bou0vEEMxyHbEfDp3o4PoRClI8WrrB3yrbTY7afxa4lUNeUngbQg77ilqcVxvlfid
9gmKDiZrKMay5hymH6YIzEJ+L4/J67BMR66Vp37nQIDAQABoZEWLzAOBgNVHQ8B
Af8EBAMCAgQwHQYDVR0OBBYEFFEaOfs2e/DSmP053dXwXiULrckrMA0GCSqGSIb3
DQEBcwUAA4IBAQDT3oS0p6e5x1CbD479oJ3WoiIe5GzKhtR6C60rWhQAJSLqASy
nYYZQ1bOdDOOIotmImv+sbtUvwtg51cqpSfN7a8brSTq22Rwwvnh6F1QnMfIszo
XqELS6eyWXmHyF+5qYGHbW0kKcFFloLuA9Xwx/2vzrYoKooNfIc5wFdsq0IVvOW1
xM+E/a9QM1jiUWC6F/wzEkEqBhJVM+CkwOiS7yQWArFzgEBMcRH7kPaWf0nVUqBT
9liMBVJ/XJiudhpeRo/Uu5EtQ1vCRP+hRv1/gSQYcy6s2kmKqJBV9B6tbCkG00Ub
7dWCylNSJkMmWSuWHUzCGclQIgkOciNRXiJs
-----END CERTIFICATE-----
```



```
P2SRootCert.cer - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIC6zCCAdOgAwI8AgIQUVU0/H9T3qJGmbd6rc9zCTANBgkqhkiG9w0BAQsFADAY
MRYwFAYDQQDDA1QM1NSb290Q2VyDEwMB4XDTE3MDgwNzIxNTg0N1oXDTE4MDgw
NzIyMTg0N1owGDEwMBQGA1UEAwNUODJUm9vdEN1cnQxMDCCASIwOQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANW4PjxpJKPnYHbToxn4+YEi7BcP8HzIsZqvzqvw
UVgov0hQ2wQnxweUI27arHaZF9fjaJ9ACOUgT/XKC2gnq3mDej42CdDPzG7HGpfe
mVZZuAUDaEUh1D9nqnXpsVCuCrRIuhHYoT9Kyh9zwRYDHQa12/taTJb3fP7cXPJ1
XSpvdvms5esZpwyPpNVBN3KAHuWGW4eVCX2kS9FRGte3iR9RjGo/Ueqj/I/pVmUN
bIETe4AJEKmmjD8Lg6rdqd+hleWY9u3fxZTPCwoqTE4TZL69JZmDzUiP1LyV8qSL
hXbmLQPUXaMkNGjIvZ6Tk14xqc5+0z8pRq0jIwmZK03N10ECAwEAAAMxMC8wOgYD
VR0PAQH/BAQDAgIEMB0GA1UdDgQwBBREyrqXyzhdULzGCfgna3QbPoKSSTANBgkq
hkiG9w0BAQsFAAOCAQEAF1qxexz5x+EU24p0rPYq899QyfyfJHAZ3n3kawIxtHTQ
+hu6tDoemScv9u+aYRRj8j2CRkDec6SeuD3Daptw+PvTUWew7MQpiHVpyX1iWpHL
FpyoUCqhK7X31zYwazIAfp90/+CNsOWZI8b1RgagY7x4pYIghwhCvJvHTtB0fczX
pCX2jppjehHBecJ8Kfhd1NwXByJEFXkf/vAihuiqOKgPGVO3L2IoNVGLywG7xb6b
lkQokTCRTvHYA9wd9vCER5mhH8C5jboaQJ0T1m7jgSecilC1lKyMC7LRZQkc0NyB
HSPkthQa3ky0KEb3DG7Rdzgdr3Ic0Zuj6E1D1EJhpg==
-----END CERTIFICATE-----
```

Home > Virtual network gateways > vnet1GW

vnet1GW | Point-to-site configuration

Virtual network gateway

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Connections

Point-to-site configuration

Properties

Locks

Monitoring

Save Discard Download VPN client

Tunnel type

IKEv2 and SSTP (SSL)

Authentication type

☒ Azure certificate ☐ RADIUS authentication ☐ Azure Active Directory

Root certificates

Name	Public certificate data
P2SrootCert	MIIC5zCCAc+gAwIBAgIQeUBps0ovt45OVUubYULVSUTANBgkqhkiG9w0BAQsFADAW Mf...

Revoked certificates

Name	Thumbprint

Save it

Home > Virtual network gateways > vnet1GW

vnet1GW | Point-to-site configuration

Virtual network gateway

Search (Ctrl+/) << Save Discard **Download VPN client**

Authentication type

☒ Azure certificate ☐ RADIUS authentication ☐ Azure Active Directory

Root certificates


Name	Public certificate data
P2SrootCert	MIIC5zCCAc+gAwIBAgIQeUBps0ovt45OVUbYULV5UTANBgkqhkiG9w0BAQsFADAW MRQwE ***

Revoked certificates

Name	Thumbprint

Download VPN client

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

←  Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

12345

☒ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

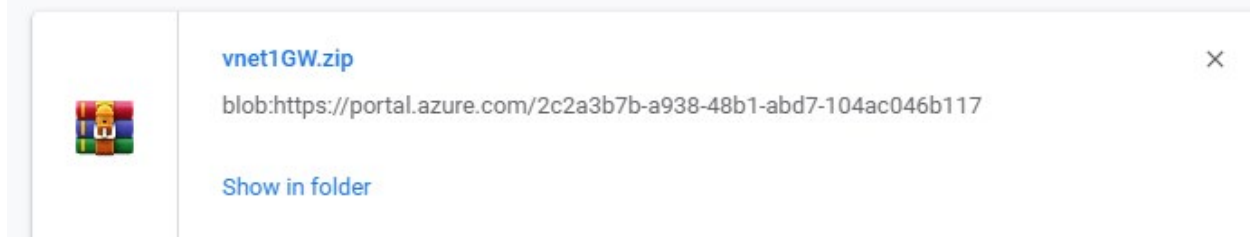
☐ Protect private key using virtualized-based security (Non-exportable)




☒ Include all extended properties.


Next

Cancel

Download VPN client from the laptop



azure > vnet1GW		
<input type="checkbox"/> Name	Date modified	Type
 Generic	10/9/2020 8:35 PM	File folder
 WindowsAmd64	10/9/2020 8:35 PM	File folder
 WindowsX86	10/9/2020 8:35 PM	File folder

> azure > vnet1GW > WindowsAmd64			
<input type="checkbox"/> Name	Date modified	Type	Size
 VpnClientSetupAmd64.exe	10/9/2020 6:35 PM	Application	196 KB

Install the VPN client software

Home

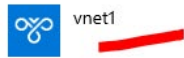
Find a setting

Network & Internet

- Status
- Wi-Fi
- Ethernet
- Dial-up
- VPN**
- Airplane mode
- Mobile hotspot
- Data usage
- Proxy

VPN

+ Add a VPN connection



Advanced Options

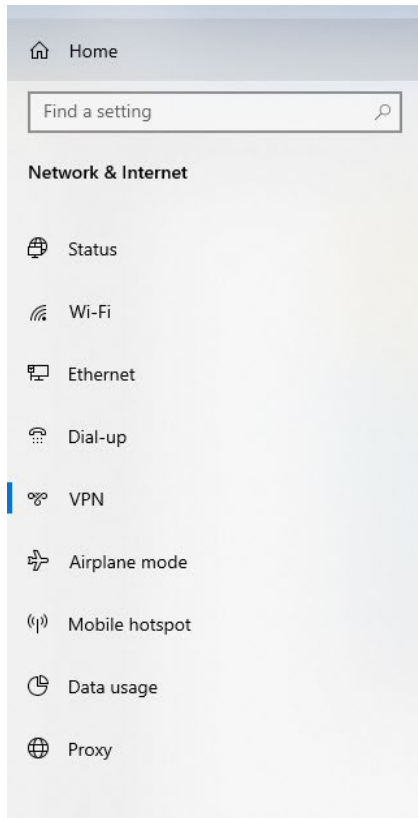
Allow VPN over metered networks



Allow VPN while roaming



CloudnLoud



VPN

+ Add a VPN connection



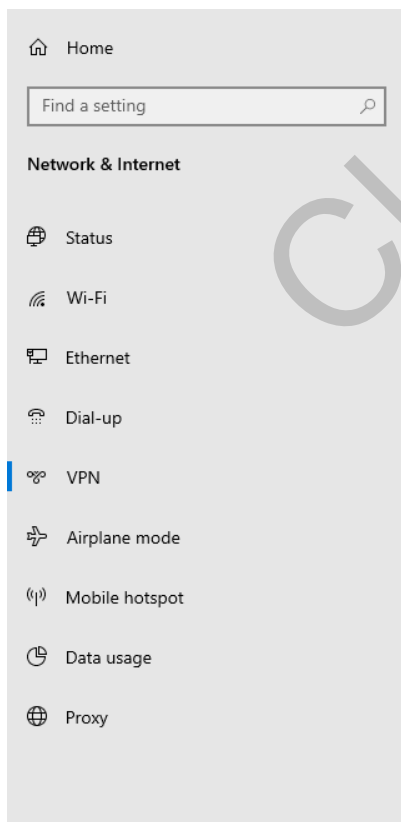
Advanced Options

Allow VPN over metered networks

☒ On

Allow VPN while roaming

☒ On



VPN

+ Add a VPN connection



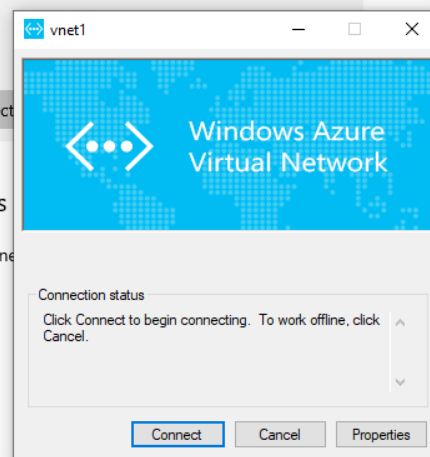
Advanced Options

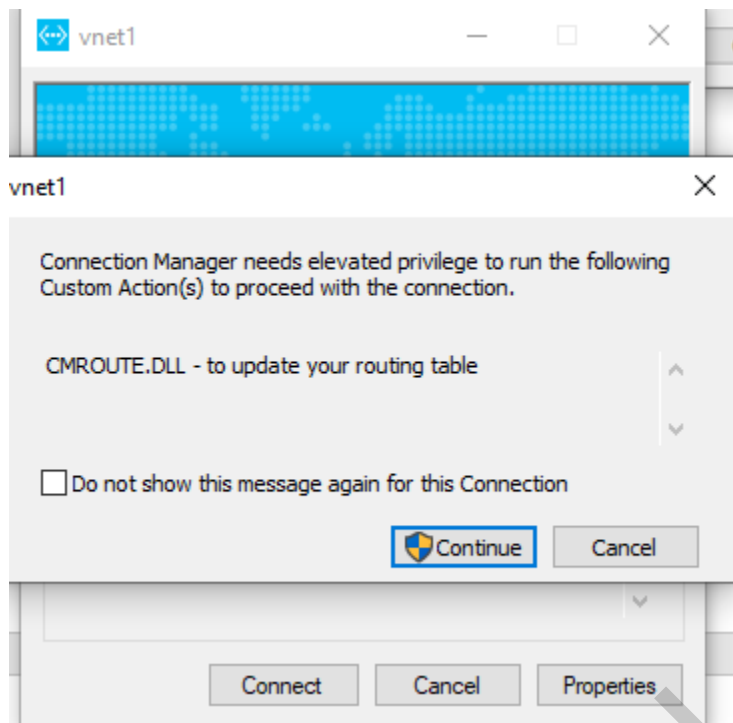
Allow VPN over metered networks

☒ On

Allow VPN while roaming

☒ On





Now connected

See the network range

Home > Virtual network gateways > vnet1GW

vnet1GW | 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

Address pool *

172.16.0.0/24

Tunnel type

IKEv2 and SSTP (SSL)

Authentication type

☒ Azure certificate ☐ RADIUS authentication ☐ Azure Active Directory

Root certificates

Name	Public certificate data
P2SrootCert	MIIC5zCCAc+gAwIBAgIQeUBp

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

Home > Virtual machines >

vnet1vm1
Virtual machine

Search (Ctrl+/) << Connect Start Restart Stop Capture Delete Refresh Share to mobile

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations

Subscription ID
vnet1/default
DNS name
Configure

Tags (change)
Click here to add tags

Properties Monitoring Capabilities Recommendations Tutorials

Virtual machine

Computer name	vnet1vm1
Operating system	Linux
SKU	18.04-LTS
Publisher	Canonical
VM generation	V1
Agent status	Not Ready
Agent version	Unknown

Networking

Public IP address	13.81.101.95
Public IP address (IPv6)	-
Private IP address	10.1.0.4
Private IP address (IPv6)	-
Virtual network/subnet	vnet1/default
DNS name	Configure

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.

```
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\pappu>ping 10.1.0.4

Pinging 10.1.0.4 with 32 bytes of data:
Reply from 10.1.0.4: bytes=32 time=75ms TTL=64
Reply from 10.1.0.4: bytes=32 time=25ms TTL=64

Ping statistics for 10.1.0.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 75ms, Average = 50ms
Control-C
^C
C:\Users\pappu>
```