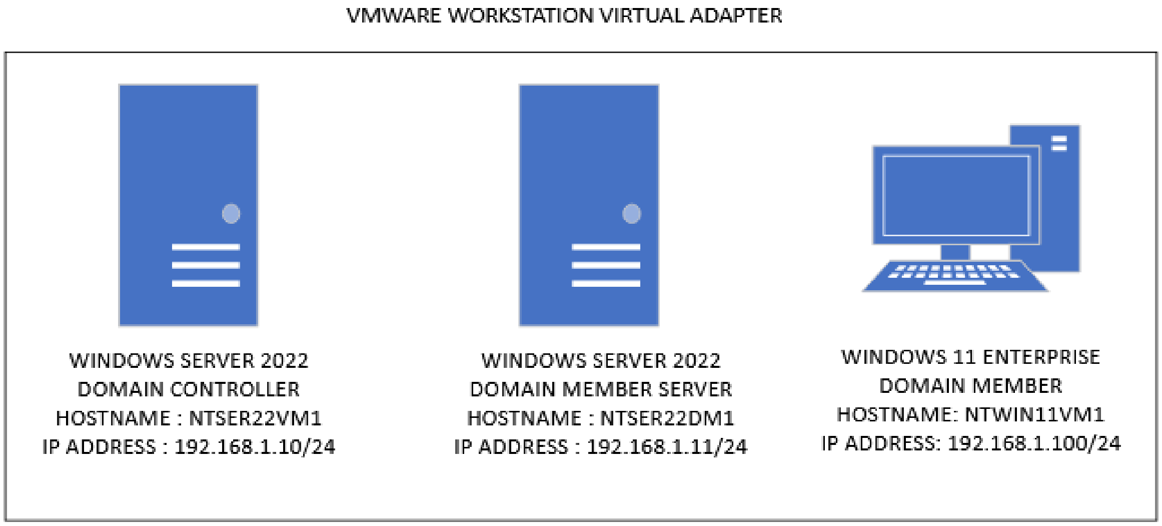
Exercise 1 - Configure Certificate Revocation Lists (CRLs)

When an administrator revokes a user certificate for any reason, the Certificate Server logs the cancellation in order to prevent a user from reusing a revoked certificate. The revocation of the certificate in a broad network must be replicated to other computers. CA servers block the use of revoked certificates to access network resources.

In this exercise:

- Request User Certificates
- Verify Issued Certificate
- Configure a New Path for CRLs
- Add Certificate Managers

Topology



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

NTSER22DM1 = Windows Server 2022 – Domain Member Server

NTWIN11VM1 = Windows 11 – Domain Member

Prerequisite

- *VMware Workstation 16 Pro*
  - When making this tutorial, we used the "Windows Server 2019" VM Template and "Windows 10 & later" VM Template. Since VMware didn't have the updated templates.

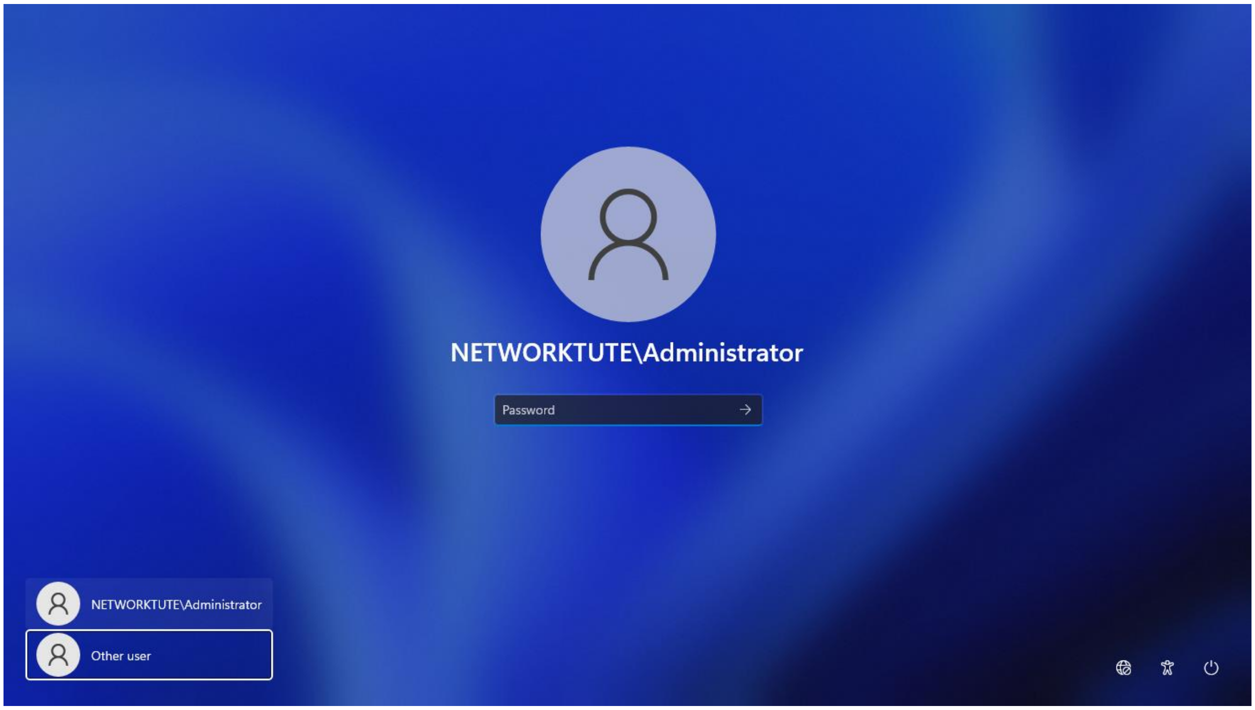
- *Microsoft Windows Server 2022*
- *Microsoft Windows 11*

Task 1: Request User Certificates

After you've set up the CA servers, you'll need to request a certificate as an Active Directory user. Follow the steps below to request a user certificate in Windows 10:

Step 1:

Connect to **NTWIN11VM1**

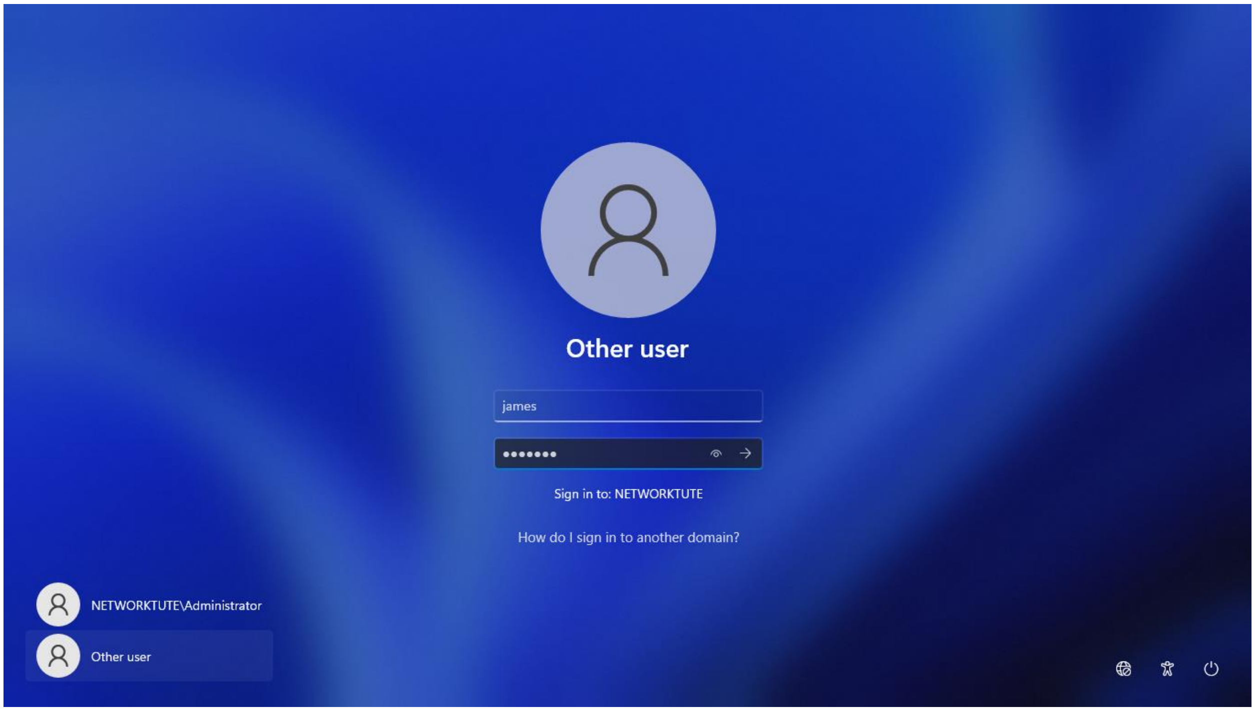


Step 2:

On the windows login screen, click **"Other user"**.

Sign in with the following credentials and then press **Enter**: ***james***

Type the **Password**: ***networktute@1***

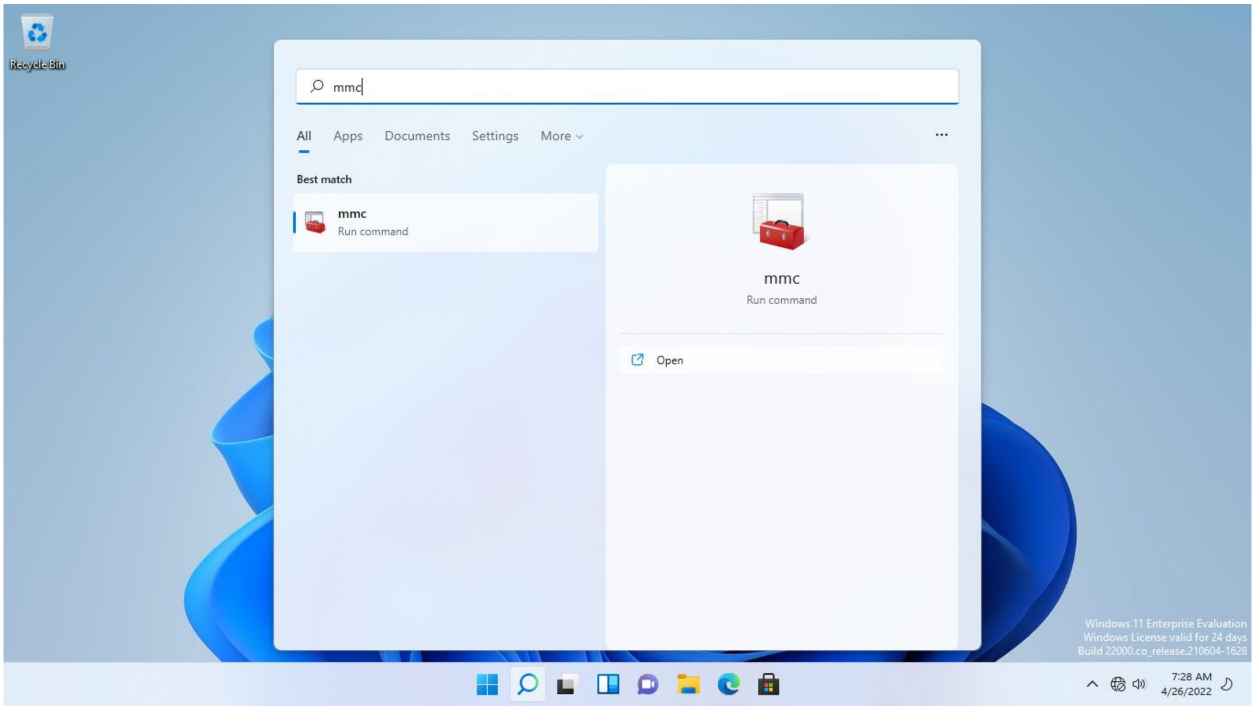


Other user
james
•••••••
Sign in to: NETWORKTUTE
How do I sign in to another domain?
NETWORKTUTE\Administrator
Other user

Step 3:

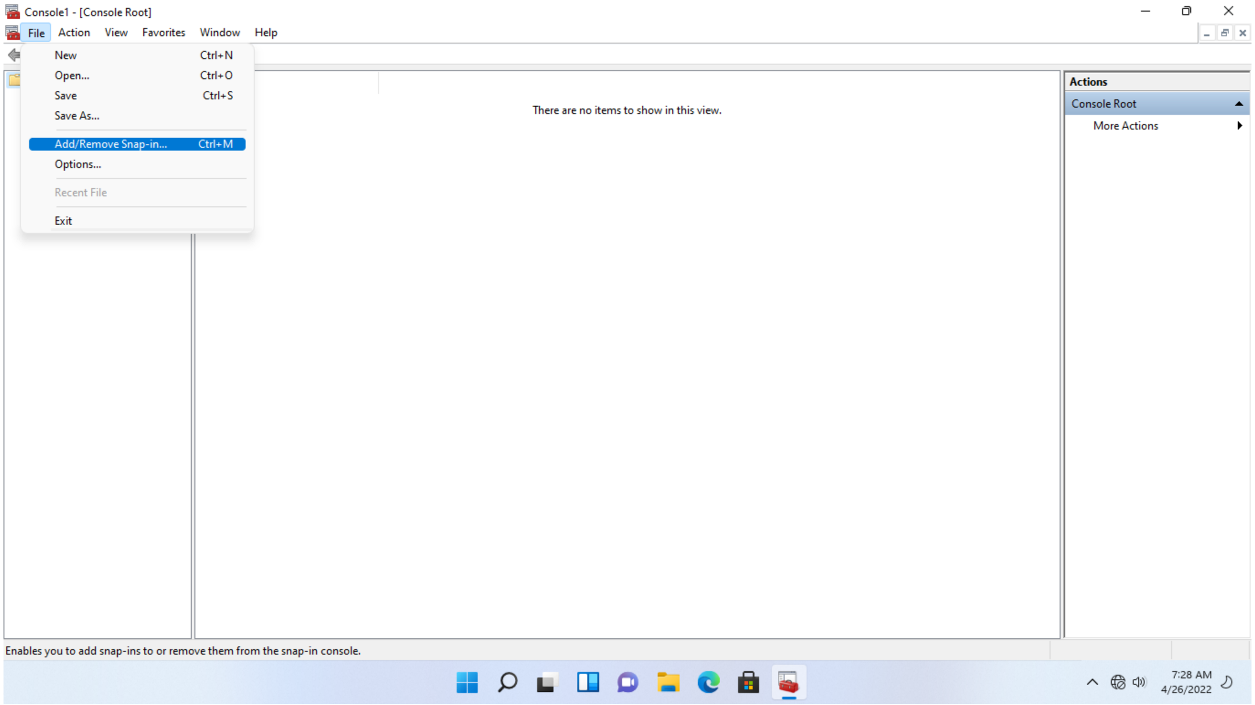
In the **Type here to search** textbox, type the following text: ***mmc***

Select **mmc** from the **Best match** menu.



Step 4:

In **Console1**, click **File** and select **Add/Remove Snap-in**.

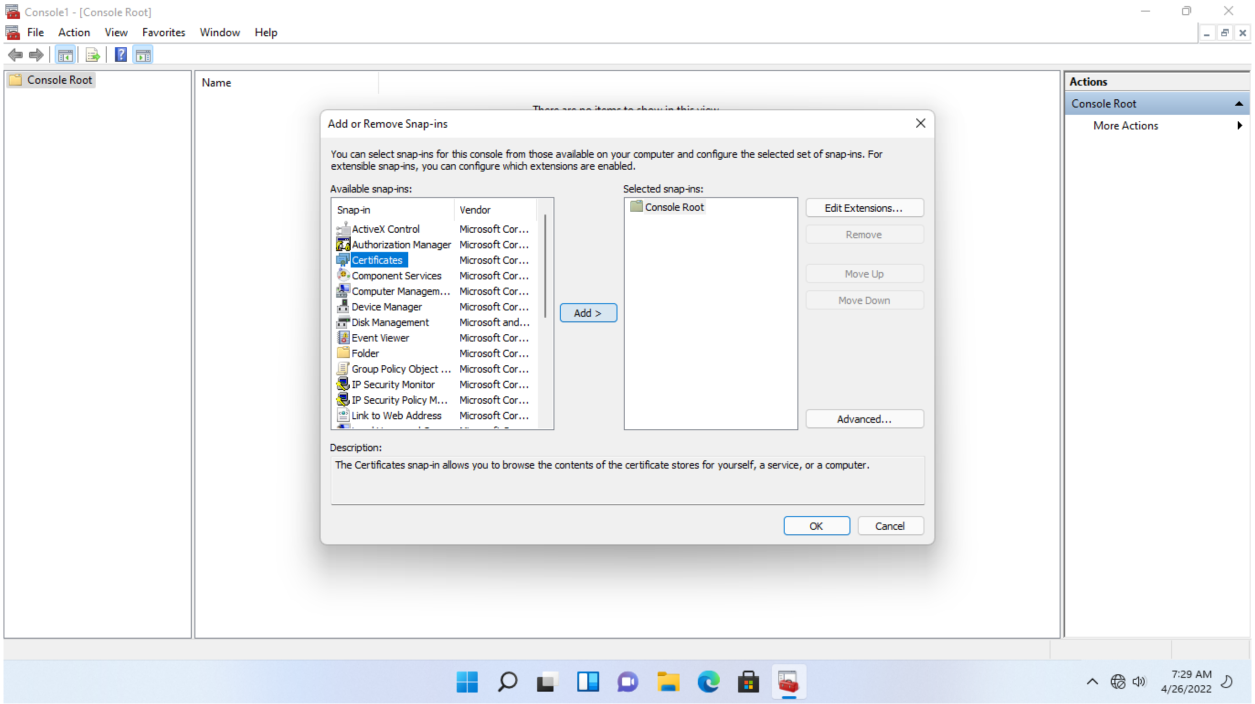


There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

Step 5:

In the **Add or Remove Snap-ins** dialog box, select **Certificates** from the left pane and click **Add**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

Console Root

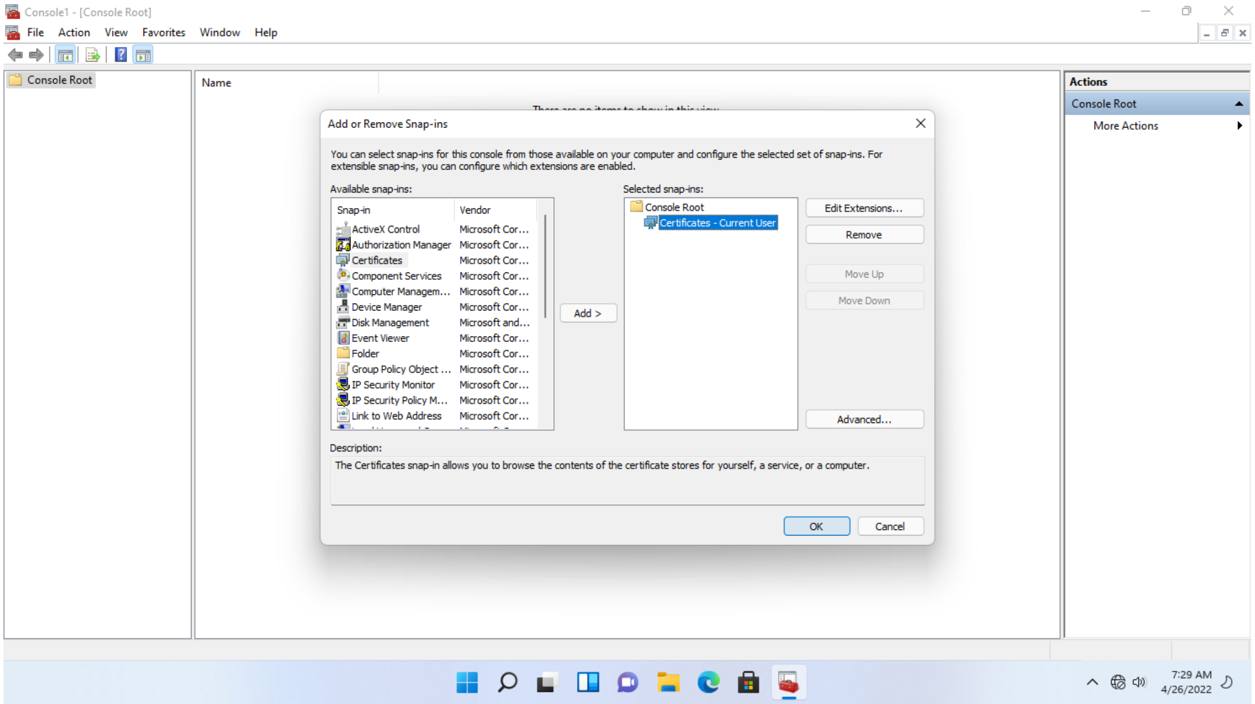
Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Step 6:

Certificates - **Current User** is now added in the right pane.

Click **OK** to close the **Add or Remove Snap-in** dialog box.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

Console Root
Certificates - Current User

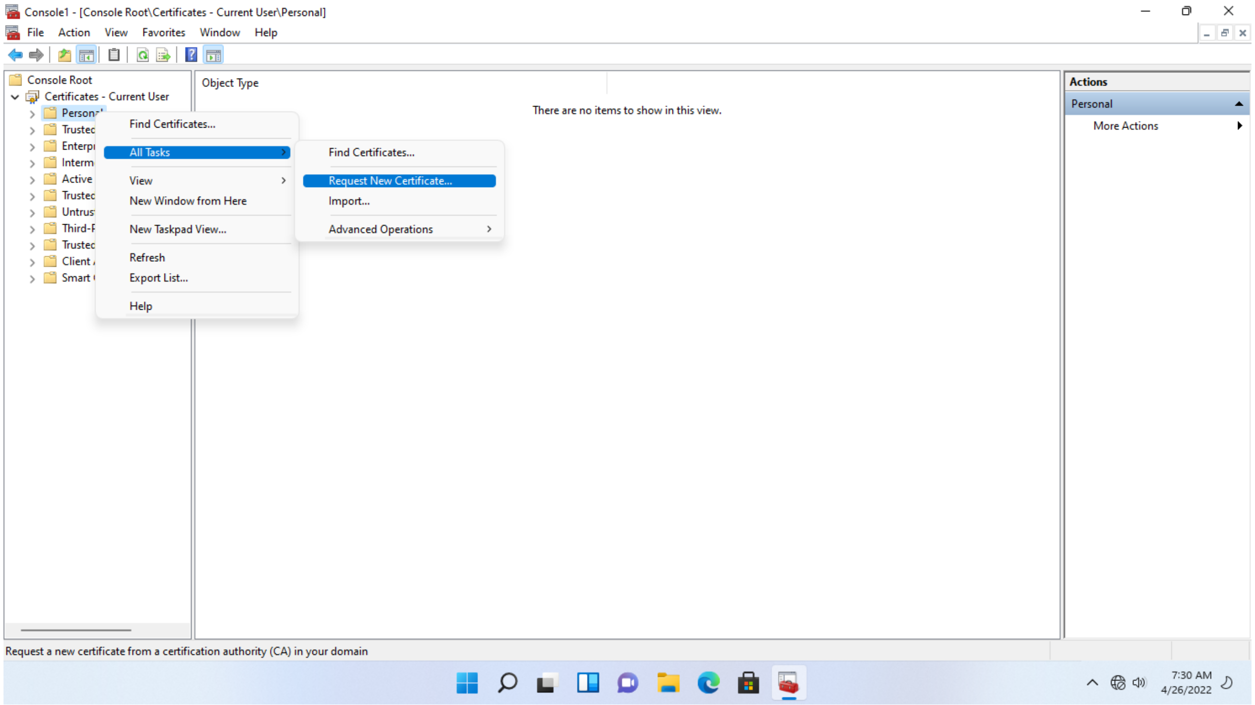
Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Step 7:

From **Console1**, expand **Certificates-Current User** and then select **Personal**.

Right-click **Personal** and select **All Tasks**, then select **Request New Certificate**.

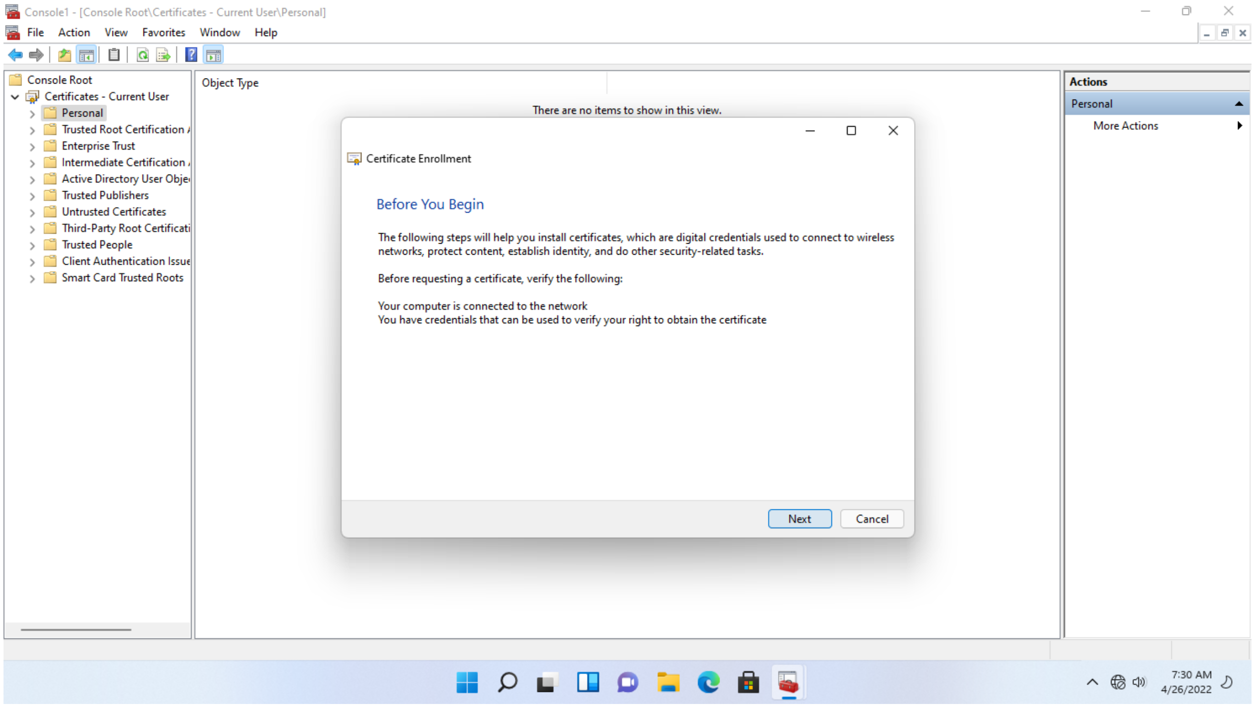


There are no items to show in this view.

Request a new certificate from a certification authority (CA) in your domain

Step 8:

On the **Before you Begin** page of the **Certificate Enrollment** wizard, click **Next**.


Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Smart Card Trusted Roots
Object Type
Actions
Personal
More Actions
Certificate Enrollment
Next
Cancel
7:30 AM
4/26/2022

There are no items to show in this view.

Before You Begin

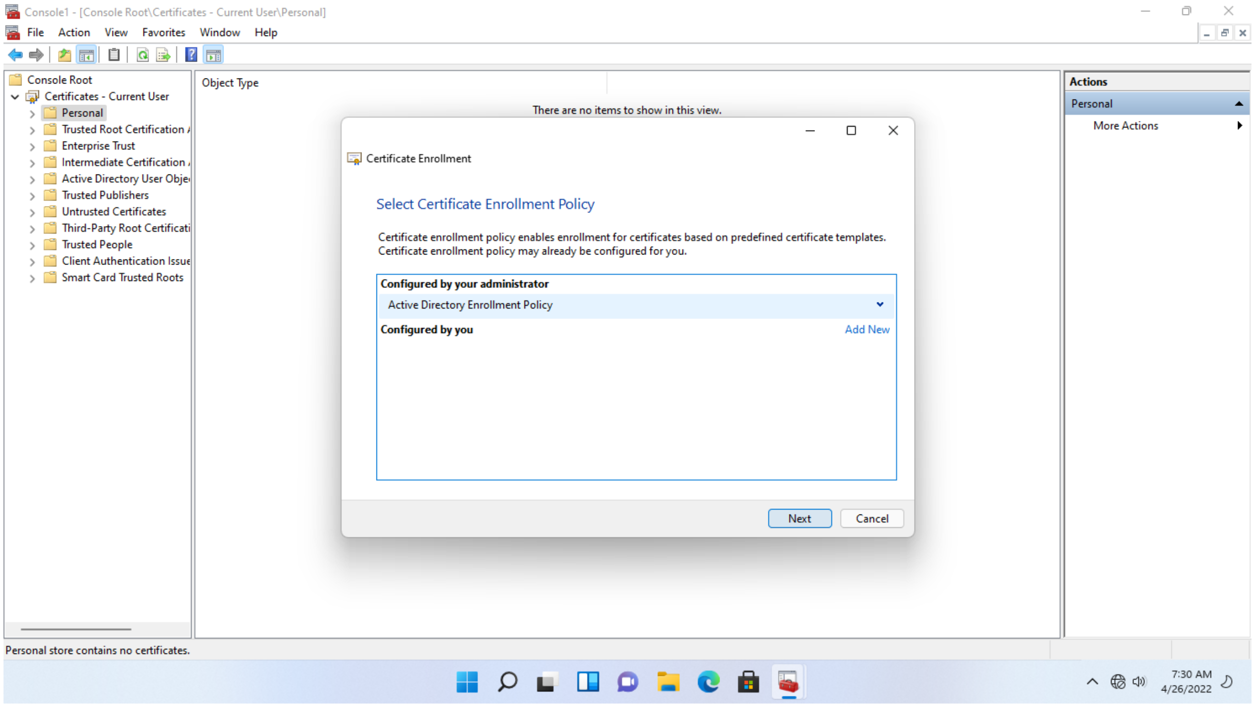
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Step 9:

On the **Select Certificate Enrollment Policy** page, ensure **Active Directory Enrollment Policy** is selected and click **Next**



Console1 - [Console Root\Certificates - Current User\Personal]

There are no items to show in this view.

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

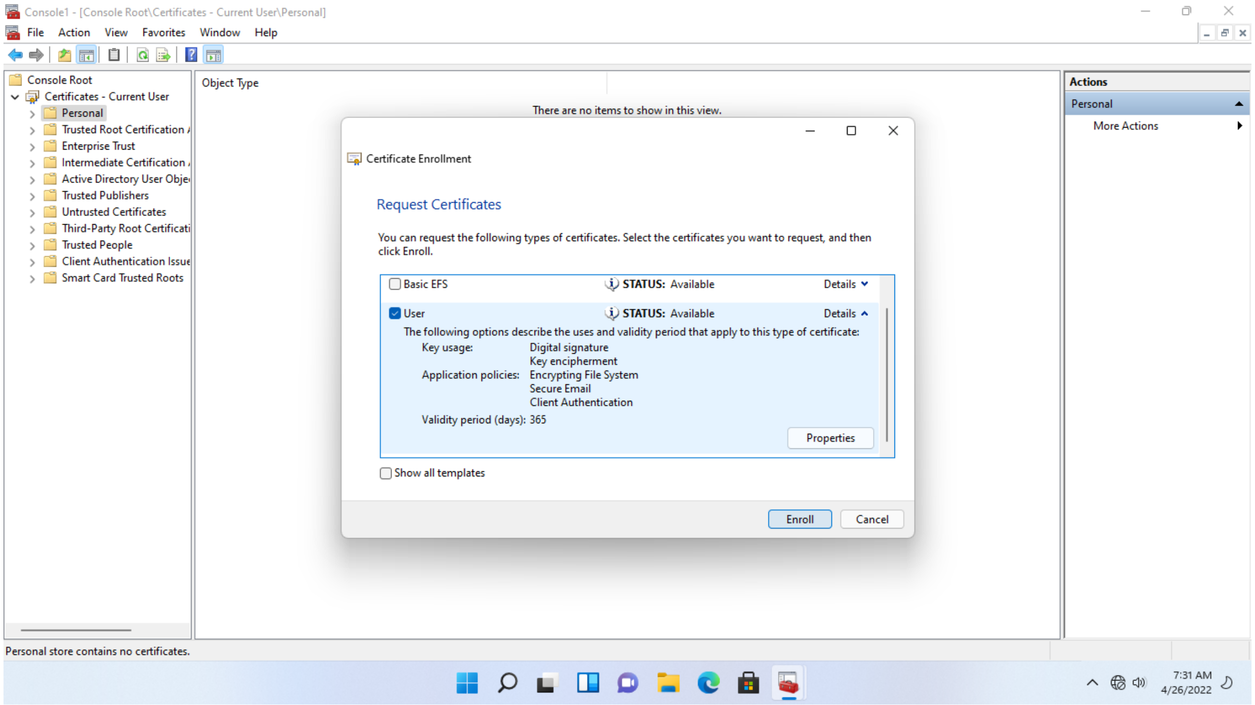
Configured by you

Personal store contains no certificates.

Step 10:

In **Request Certificates**, click the **User** checkbox and click the **Details** down arrow button.

If there are no certificates listed, • open a Command prompt as administrator • run: gpupdate /force • Re-attempt from step 7 again


Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Smart Card Trusted Roots
Object Type
There are no items to show in this view.
Actions
Personal
More Actions
7:31 AM
4/26/2022

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

☐ Basic EFS — STATUS: Available — Details

☑ User — STATUS: Available — Details

The following options describe the uses and validity period that apply to this type of certificate:

Key usage: Digital signature
Key encipherment

Application policies: Encrypting File System
Secure Email
Client Authentication

Validity period (days): 365

Properties

☐ Show all templates

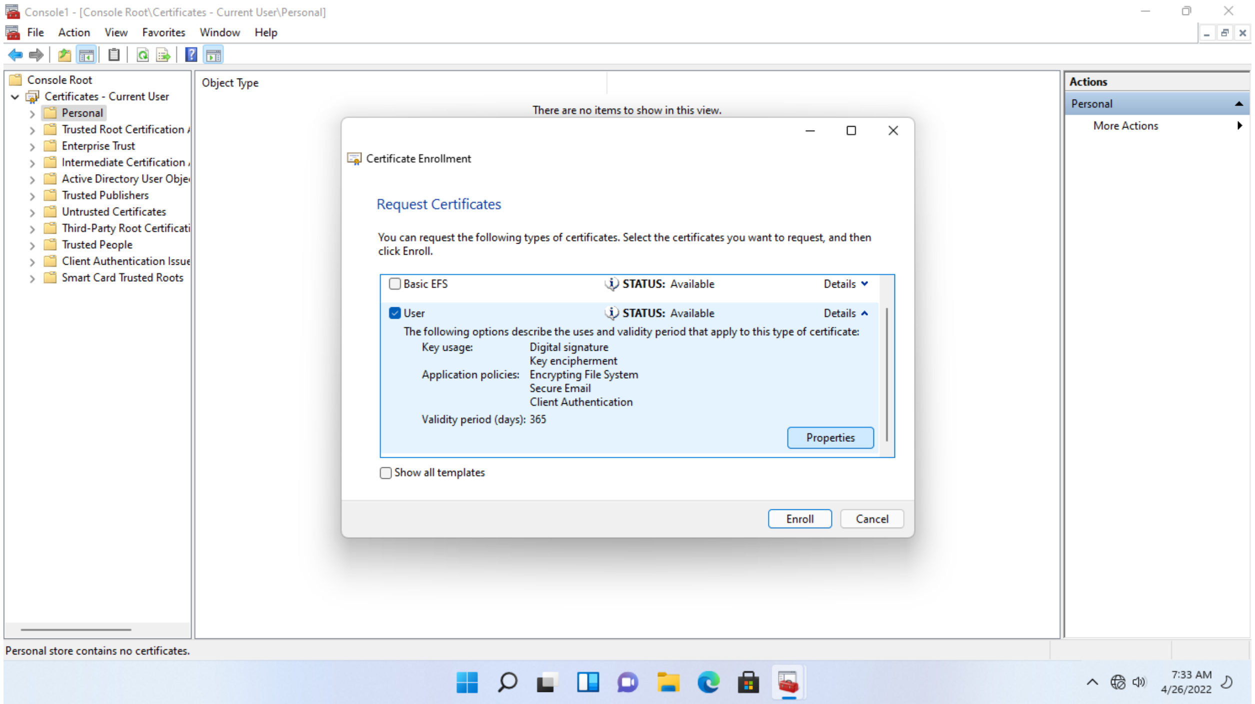
Enroll Cancel

Personal store contains no certificates.

Step 11:

The details now display additional information about this certificate.

Click **Properties**.


Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Smart Card Trusted Roots
Object Type
There are no items to show in this view.
Actions
Personal
More Actions
7:33 AM
4/26/2022

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

☐ Basic EFS — STATUS: Available — Details

☑ User — STATUS: Available — Details

The following options describe the uses and validity period that apply to this type of certificate:

Key usage: Digital signature
Key encipherment

Application policies: Encrypting File System
Secure Email
Client Authentication

Validity period (days): 365

Properties

☐ Show all templates

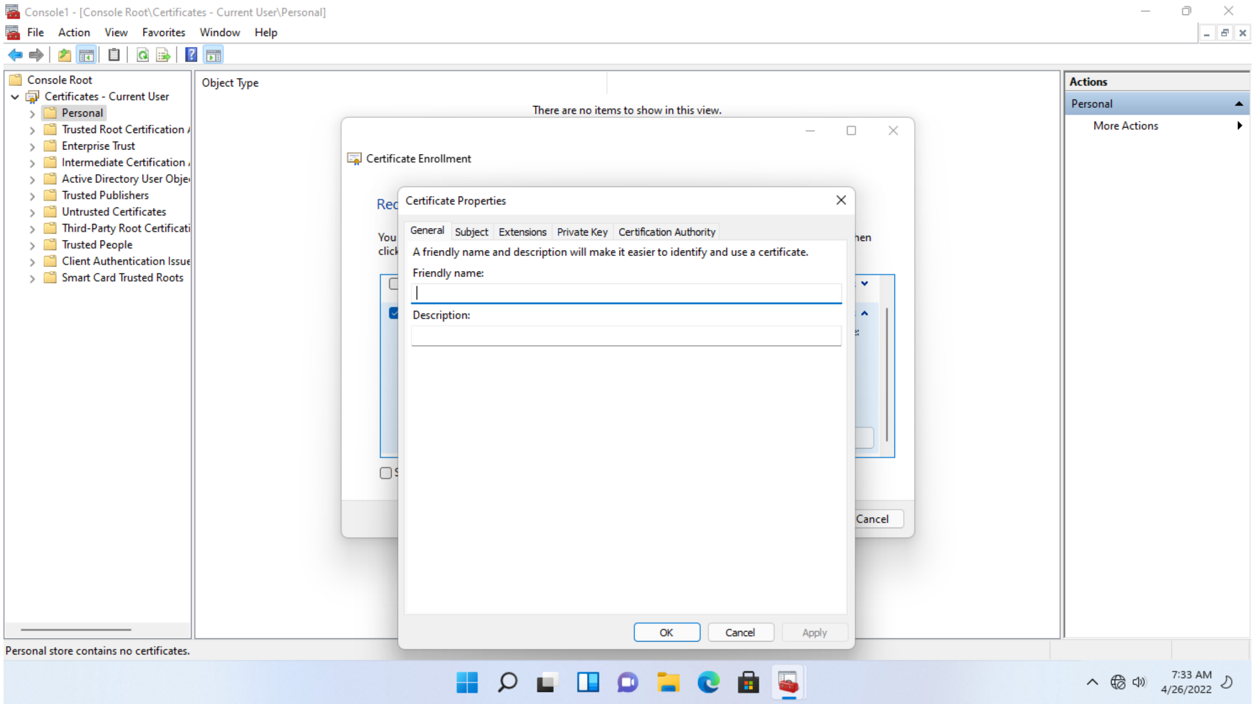
Enroll Cancel

Personal store contains no certificates.

Step 12:

The **Certificate Properties** dialog box is displayed.

Click the **Certification Authority** tab.



Console1 - [Console Root\Certificates - Current User\Personal]

There are no items to show in this view.

Certificate Properties

A friendly name and description will make it easier to identify and use a certificate.

Friendly name:

Description:

Personal store contains no certificates.

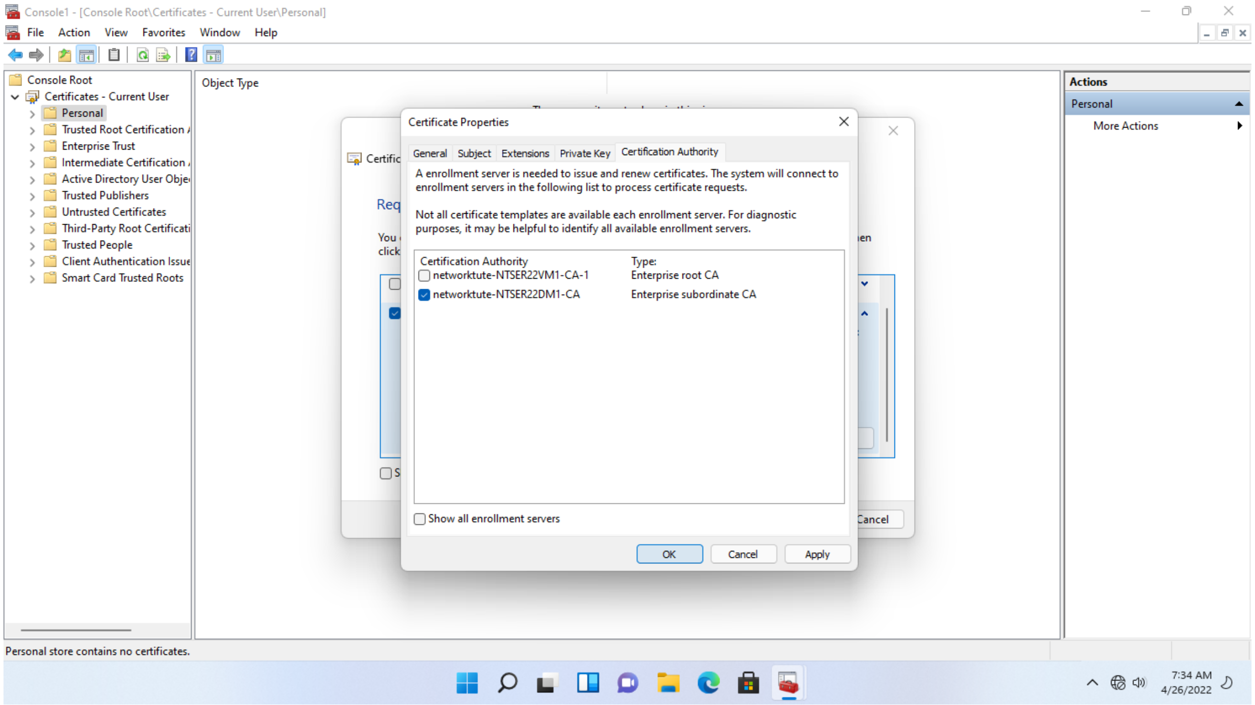
Step 13:

On the Certification Authority tab, you will find the servers that can issue certificates to the user.

Deselect the **networktute-NTSER22VM1-CA-1** checkbox.

Leave the **networktute-NTSER22DM1-CA** checkbox selected.

Click **OK**.


Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Smart Card Trusted Roots
Object Type
Actions
Personal
More Actions
Certificate Properties
General Subject Extensions Private Key Certification Authority
OK Cancel Apply
7:34 AM
4/26/2022

A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests.

Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers.

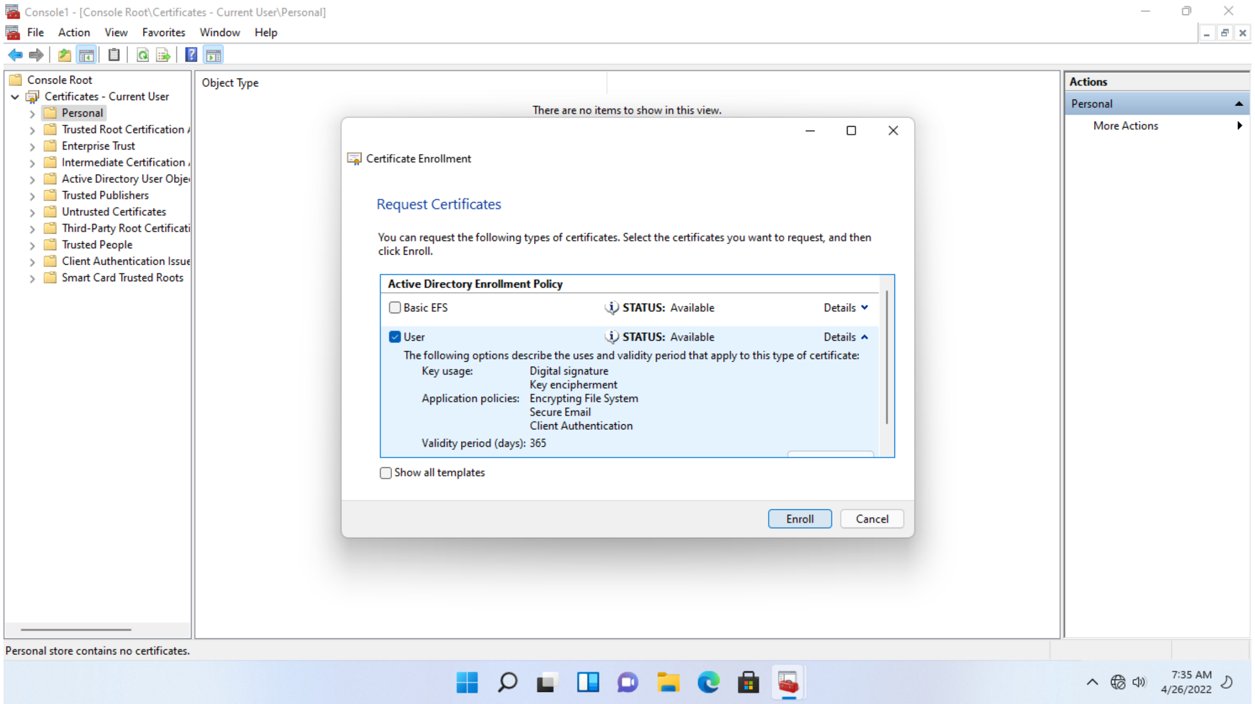
Certification Authority	Type:
□ networktute-NTSER22VM1-CA-1	Enterprise root CA
☑ networktute-NTSER22DM1-CA	Enterprise subordinate CA

□ Show all enrollment servers

Personal store contains no certificates.

Step 14:

Back in the **Request Certificates** dialog box, click **Enroll**.


Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Smart Card Trusted Roots
Object Type
Actions
Personal
More Actions
Certificate Enrollment
Enroll Cancel
7:35 AM
4/26/2022

There are no items to show in this view.

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Basic EFS — STATUS: Available — Details

☑ User — STATUS: Available — Details

The following options describe the uses and validity period that apply to this type of certificate:

Key usage:	Digital signature Key encipherment
Application policies:	Encrypting File System Secure Email Client Authentication
Validity period (days):	365

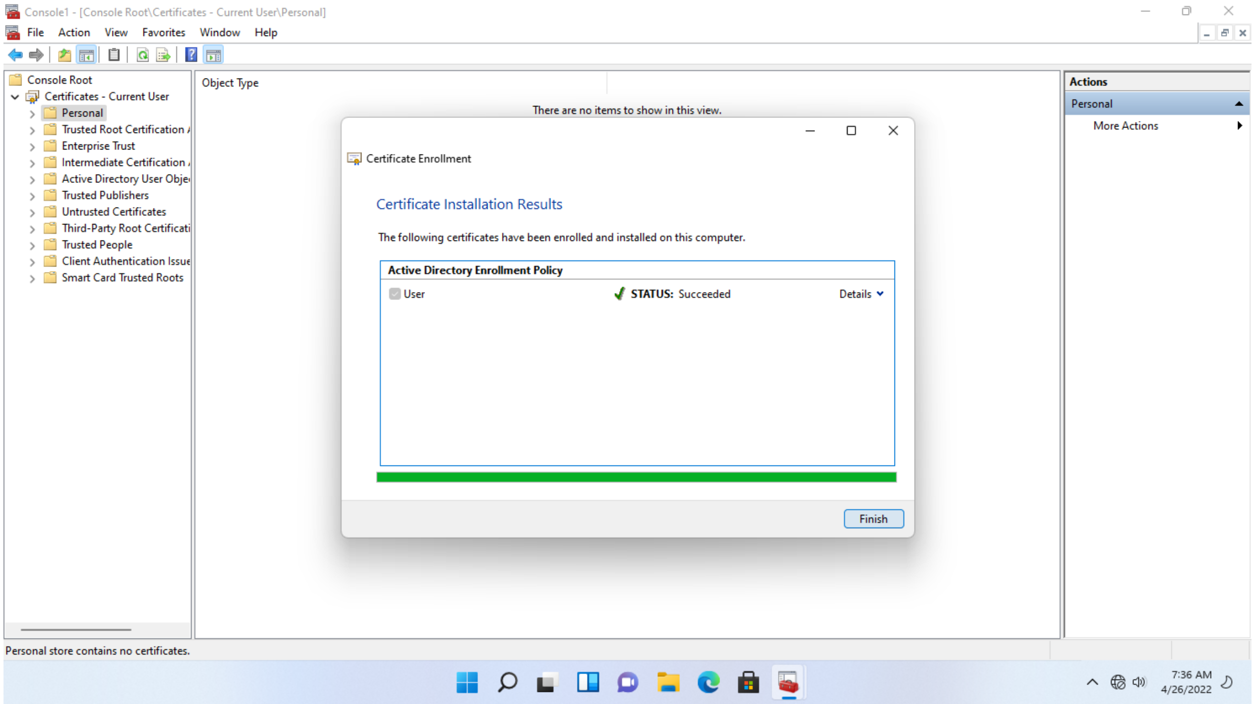
□ Show all templates

Personal store contains no certificates.

Step 15:

Wait for the enrolment to be completed.

Then click **Finish** when **STATUS**: **Succeeded** is displayed.



Console1 - [Console Root\Certificates - Current User\Personal]

There are no items to show in this view.

Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

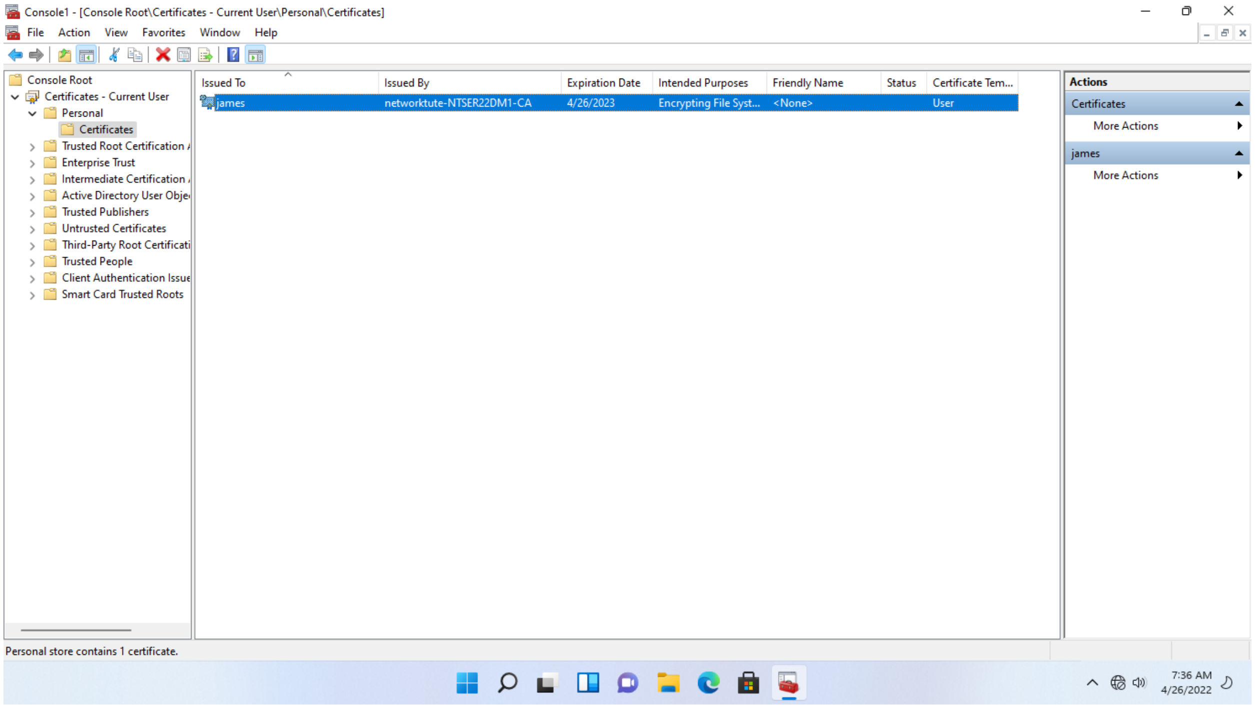
User ✓ STATUS: Succeeded Details

Personal store contains no certificates.

Step 16:

Expand **Personal** and then click the **Certificates** folder.

A user certificate has now been issued to **James**.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Smart Card Trusted Roots
Actions
Certificates
More Actions
james
More Actions
7:36 AM
4/26/2022

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
james	networktute-NTSER22DM1-CA	4/26/2023	Encrypting File Syst...	<None>		User

Personal store contains 1 certificate.

Task 2: Verify Issued Certificate

Remember that you configured the **NTWIN11VM1** machine to enroll with the **NTSER22DM1** server during the certificate enrollment.

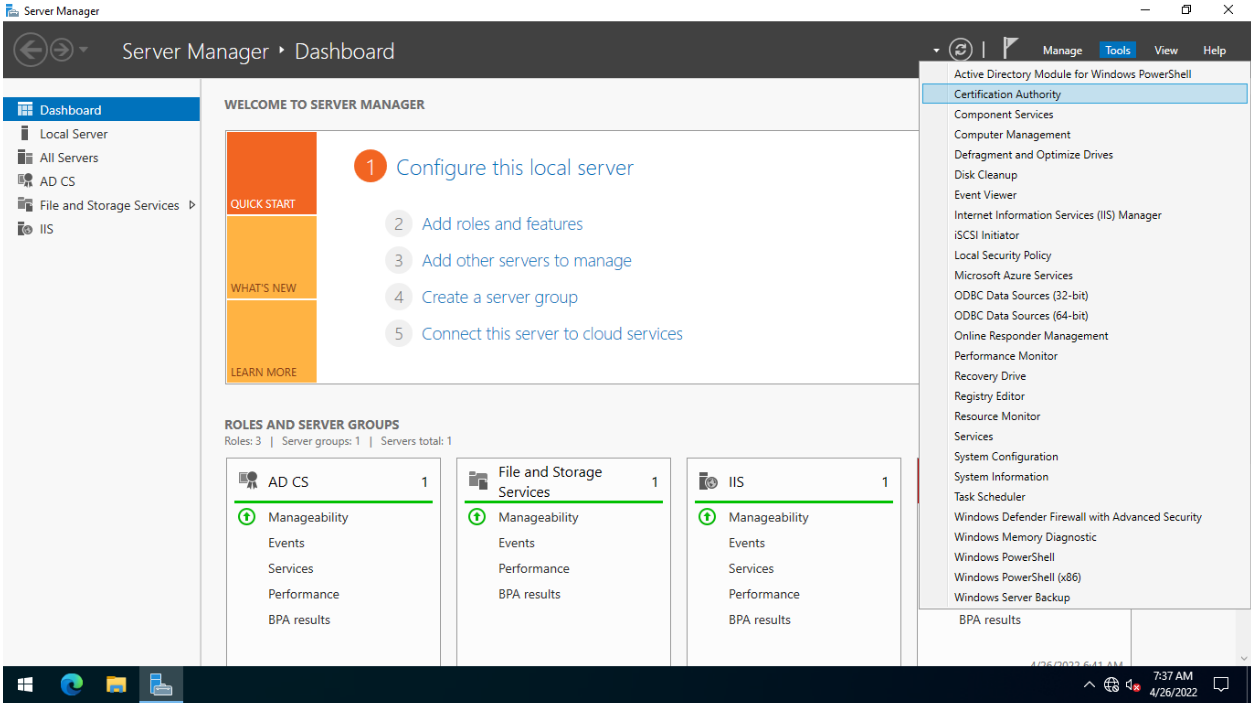
Now let’s, verify the certificate issued to User.

Step 1:

Toggle over to the **NTSER22DM1** device. If the system is locked, use the **Administrator** account to log in.

Ensure that the **Server Manager** is open.

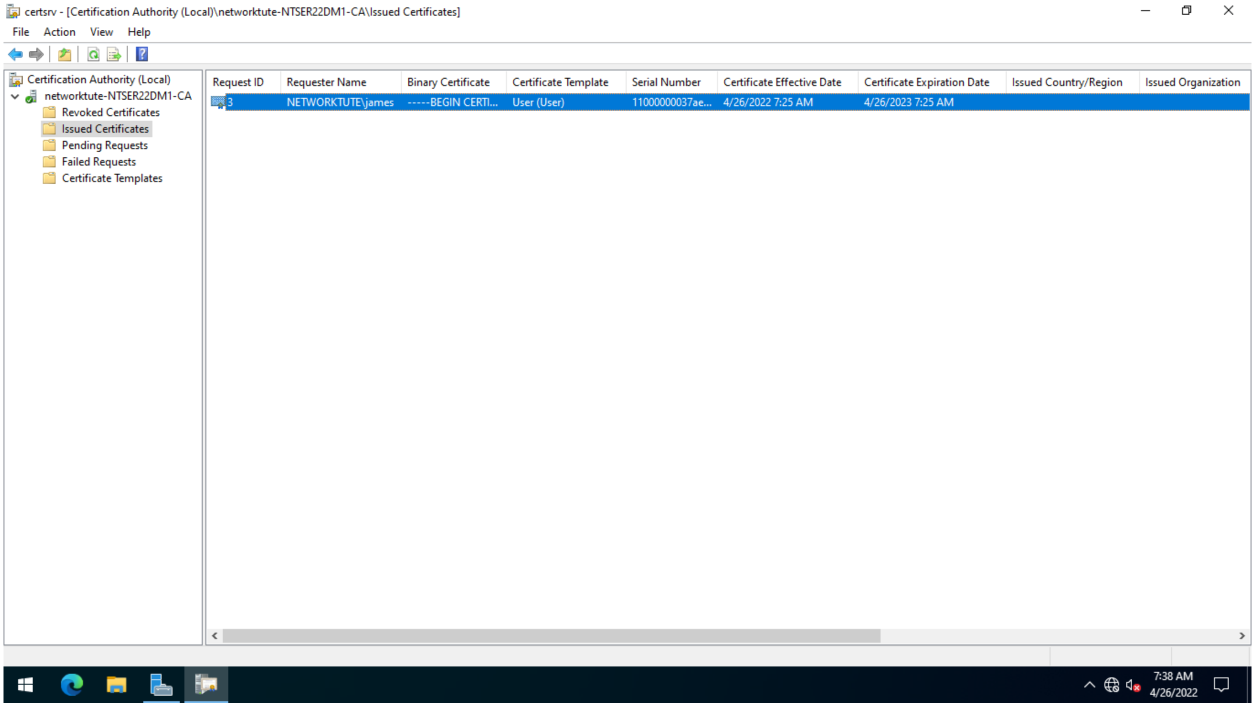
Click **Tools** and then select **Certification Authority.**



Step 2:

Certification Authority (**Local**) window opens.

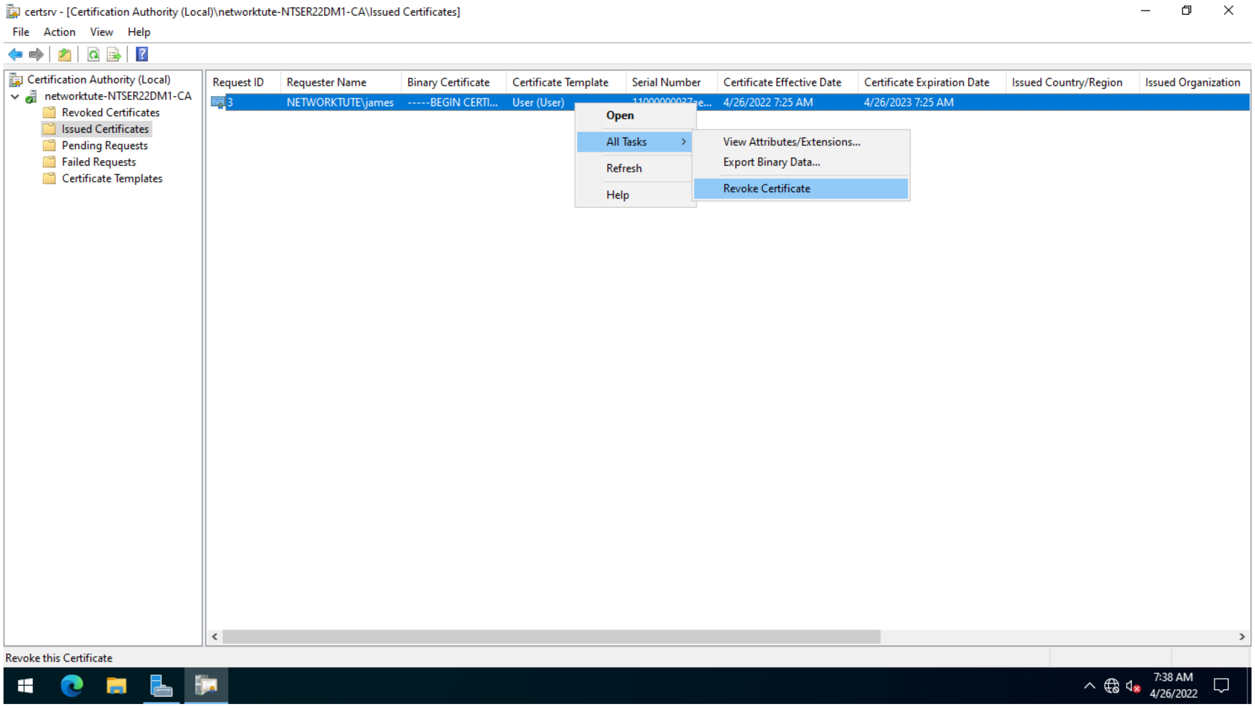
Expand **networktute-NTSER22DM1-CA** and select the **Issued Certificates** folder. Notice that a certificate is issued to **James**


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Issued Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
7:38 AM
4/26/2022

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date	Issued Country/Region	Issued Organization
3	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26/2023 7:25 AM		

Step 3:

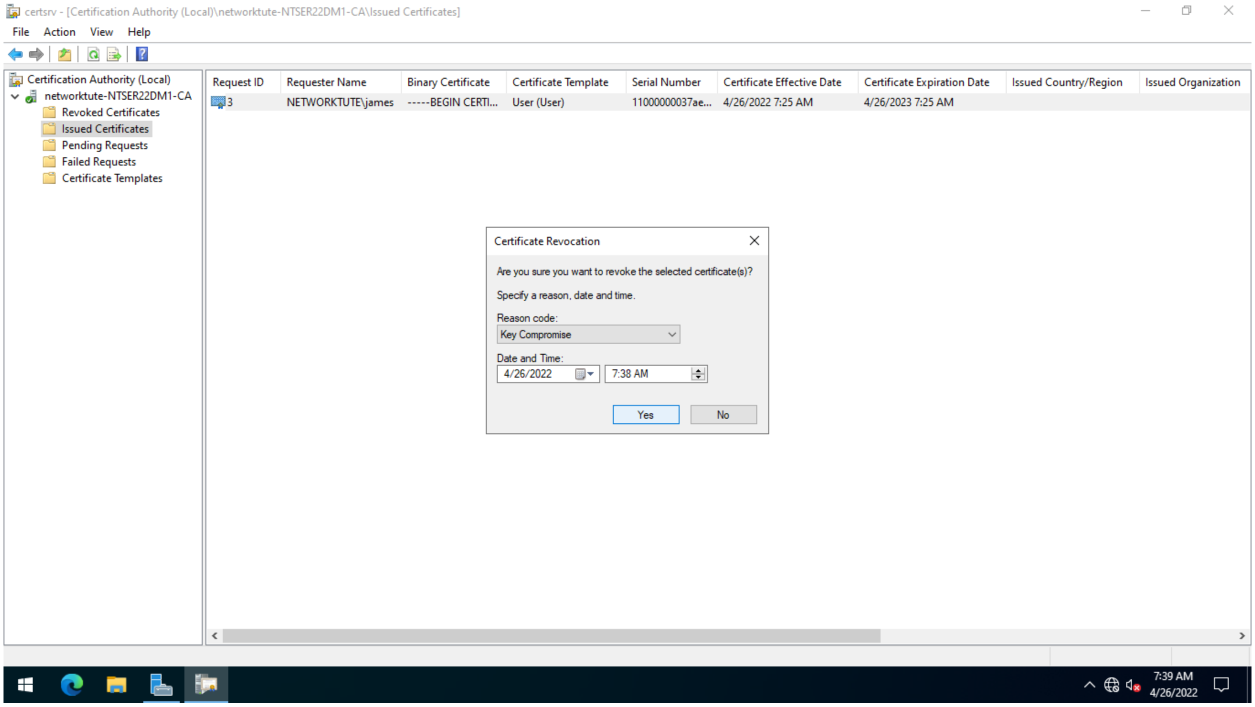
Right-click the **NETWORKTUTE\james** certificate, select **All Tasks** and then select **Revoke Certificate**



Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date	Issued Country/Region	Issued Organization
3	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26/2023 7:25 AM		

Step 4:

On the **Certificate Revocation** dialog box, select **Key Compromise** and then click **Yes**.


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Issued Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Yes
No
7:39 AM
4/26/2022

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date	Issued Country/Region	Issued Organization
3	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26/2023 7:25 AM		

Certificate Revocation

Are you sure you want to revoke the selected certificate(s)?

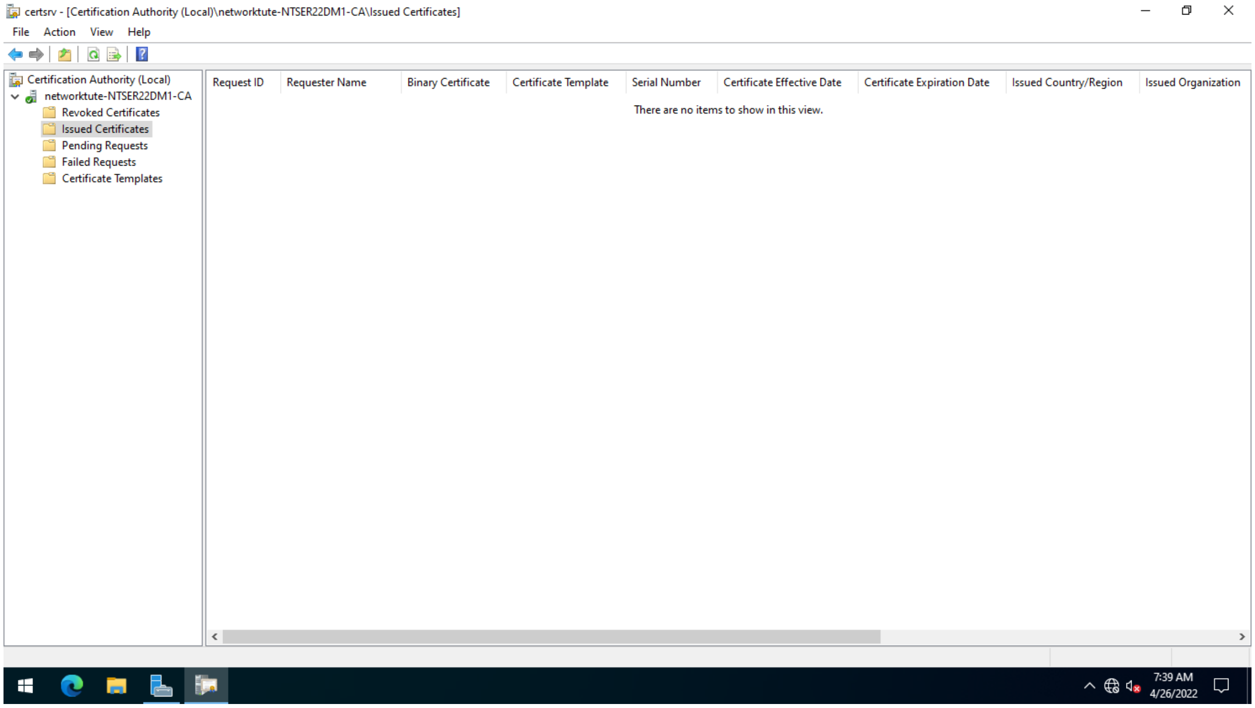
Specify a reason, date and time.

Reason code: Key Compromise

Date and Time: 4/26/2022 7:38 AM

Step 5:

The **james** certificate disappears from the **Issued Certificates** folder.

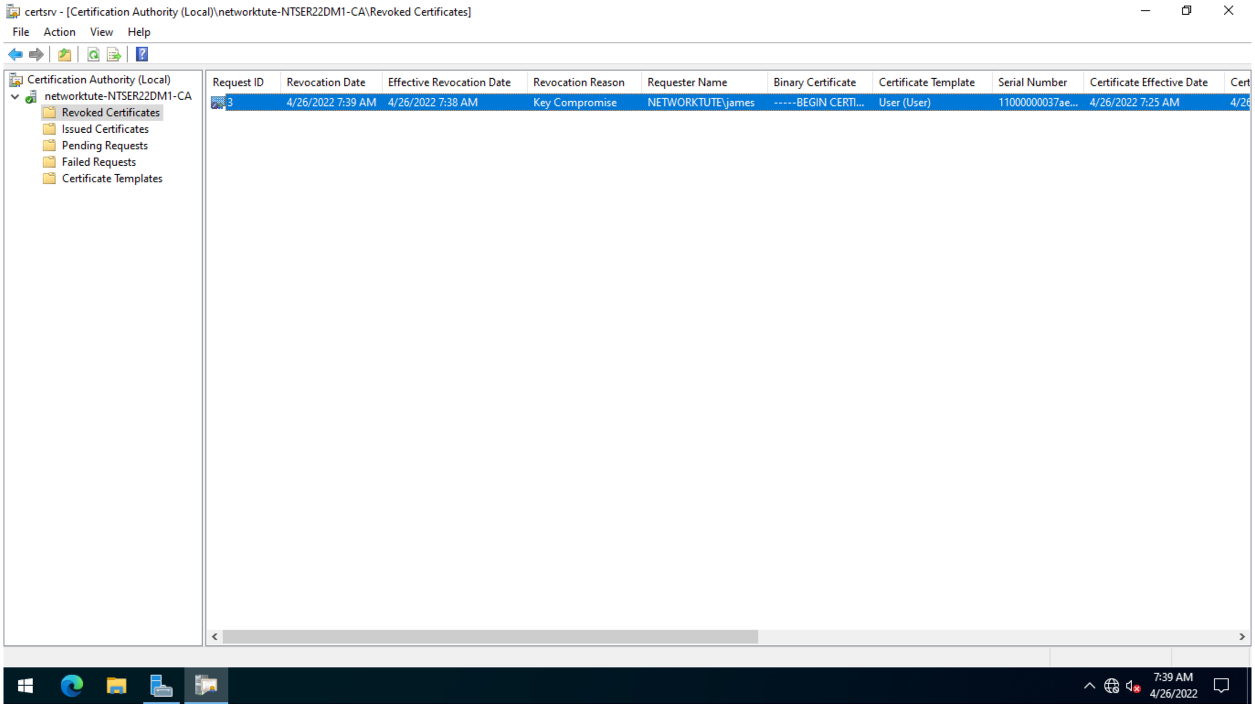


There are no items to show in this view.

Step 6:

Click the **Revoked Certificates** folder.

The **Revoked Certificates** folder now displays the revoked certificate of user James

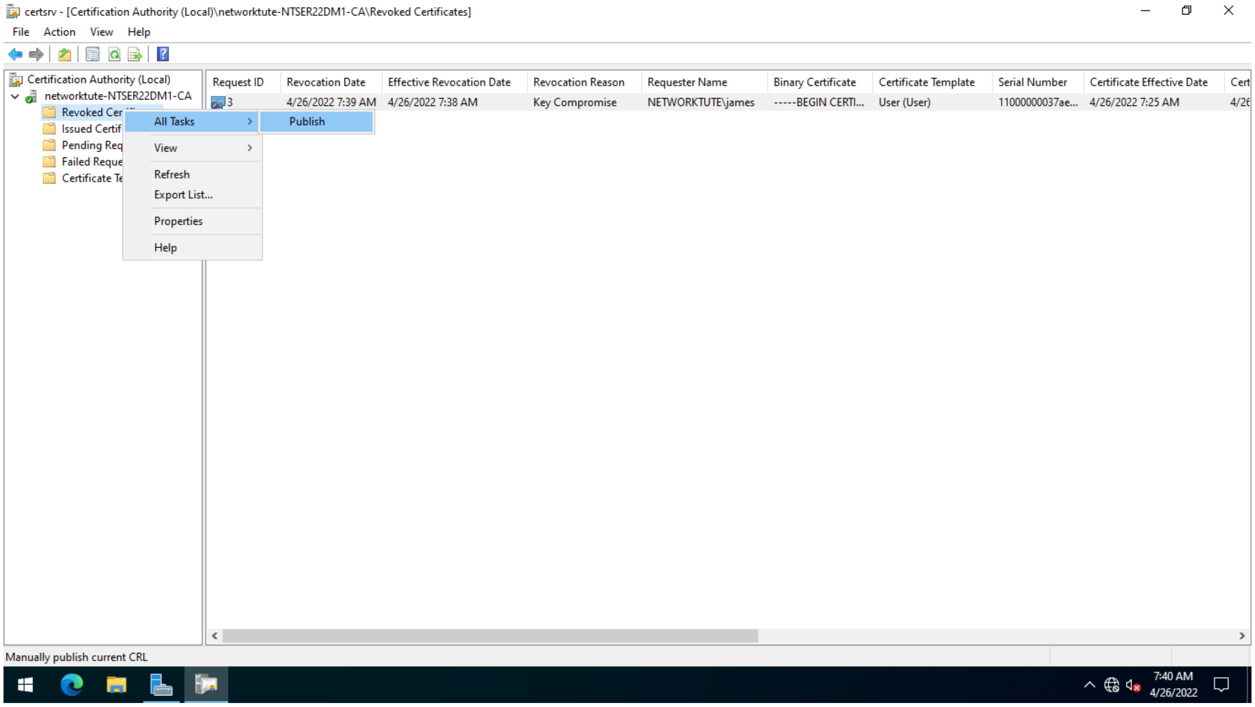

certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
7:39 AM
4/26/2022

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/2

Step 7:

You now need to publish the revoked certificates to other CA servers.

Right-click the **Revoked Certificates** folder and select **All Tasks** and then select **Publish**



Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/2

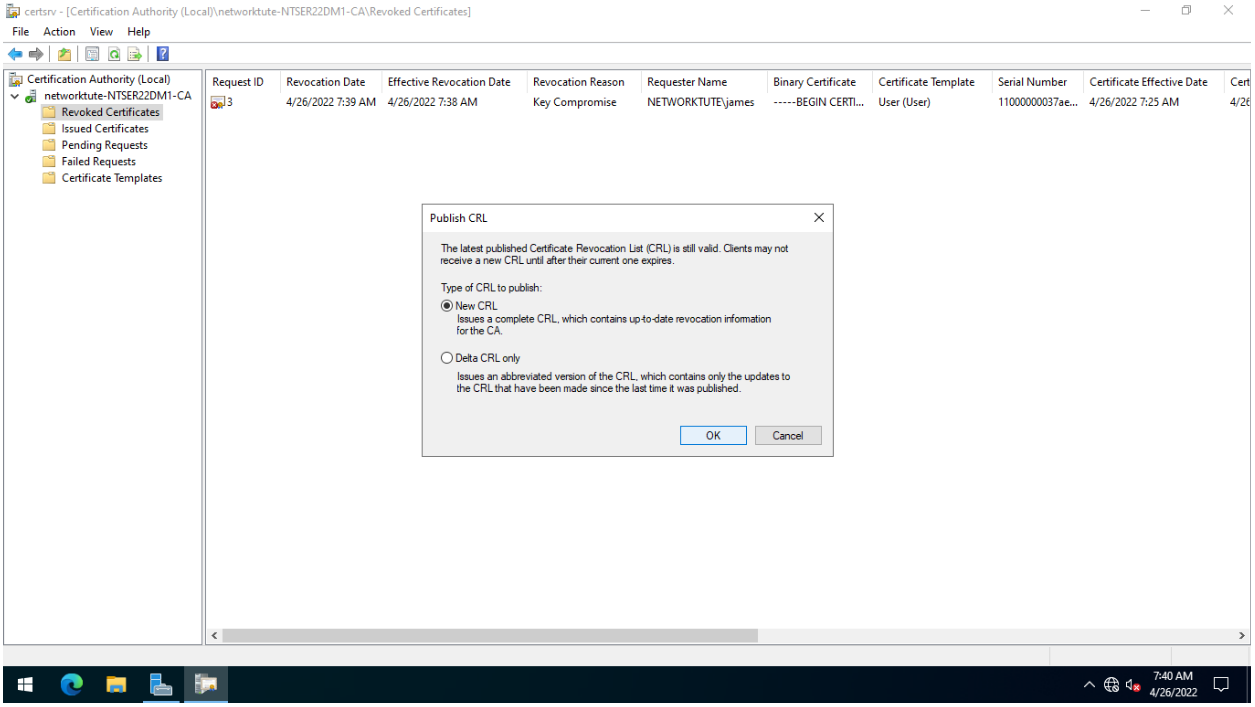
Manually publish current CRL

Step 8:

In the **Publish CRL** dialog box, ensure **New CR**L is selected.

Click **OK**

.



certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
7:40 AM
4/26/2022

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Publish CRL

The latest published Certificate Revocation List (CRL) is still valid. Clients may not receive a new CRL until after their current one expires.

Type of CRL to publish:

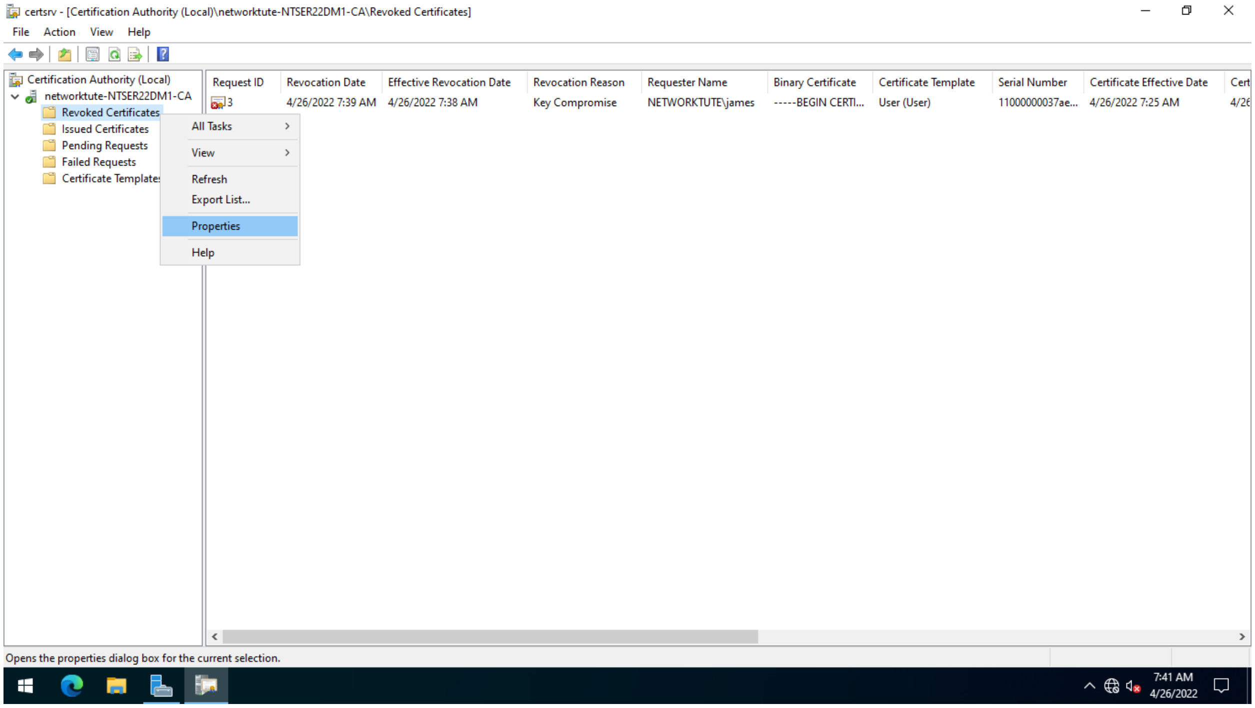
● New CRL
Issues a complete CRL, which contains up-to-date revocation information for the CA.

○ Delta CRL only
Issues an abbreviated version of the CRL, which contains only the updates to the CRL that have been made since the last time it was published.

OK Cancel

Step 9:

Right-click the **Revoked Certificates** folder and select **Properties**.

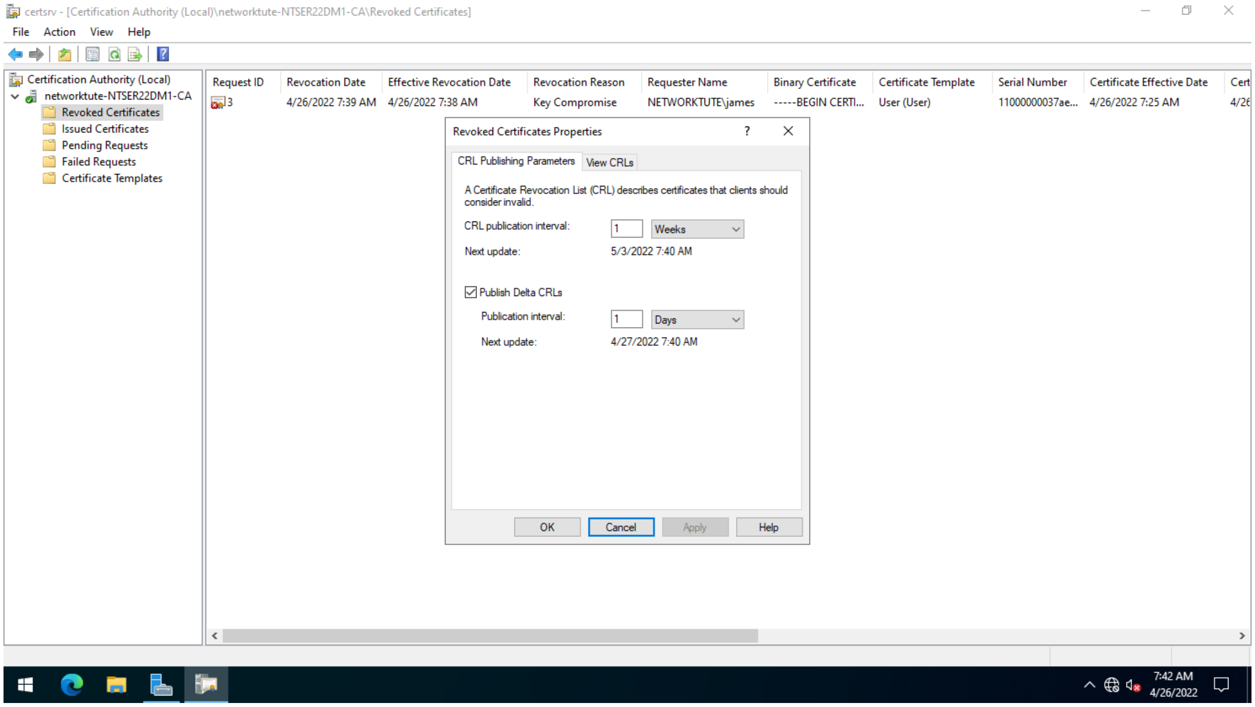


Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Opens the properties dialog box for the current selection.

Step 10:

The **CRL Publishing Parameters** tab in the **Revoked Certificates Properties** dialog box shows the publication interval for **New CRL** and **Delta CRLs** (recent updates of revoked certificates).


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Revoked Certificates Properties
CRL Publishing Parameters
View CRLs
OK
Cancel
Apply
Help
7:42 AM
4/26/2022

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

A Certificate Revocation List (CRL) describes certificates that clients should consider invalid.

CRL publication interval: 1 Weeks

Next update: 5/3/2022 7:40 AM

☑ Publish Delta CRLs

Publication interval: 1 Days

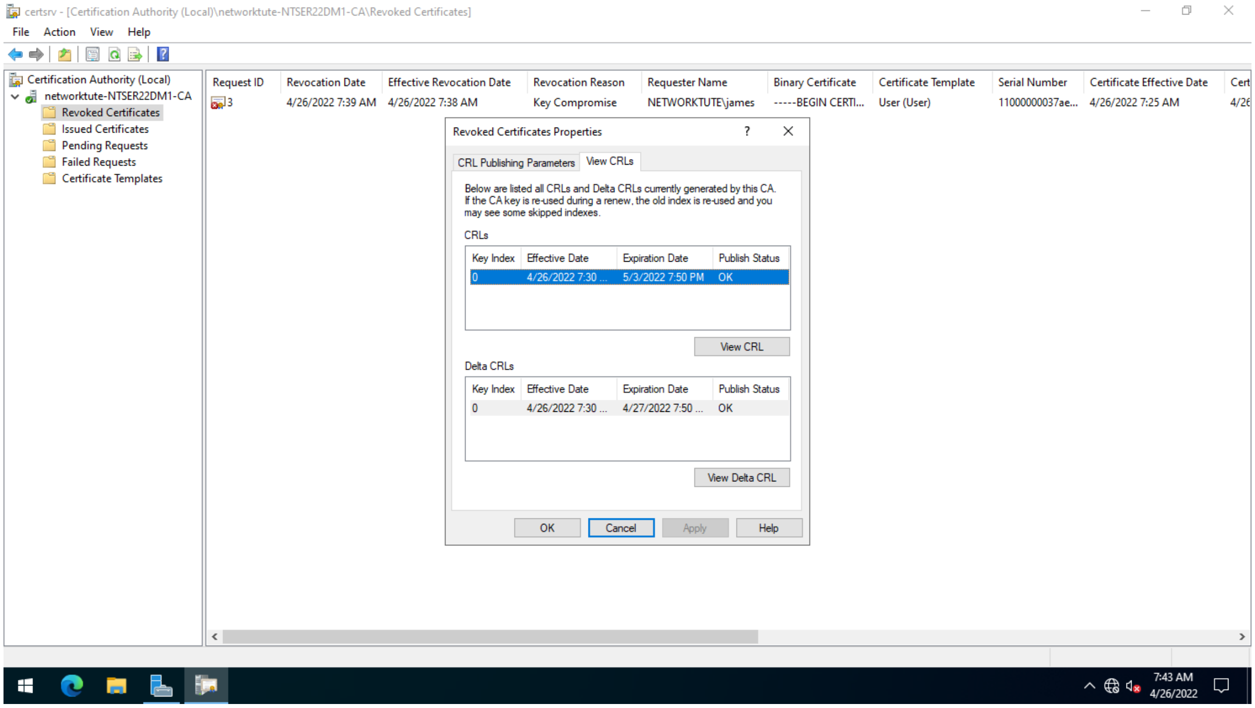
Next update: 4/27/2022 7:40 AM

Step 11:

Click the **View CRLs** tab.

The **View CRLs** tab displays the publication status of CRLs.

Click **OK**.



certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Revoked Certificates Properties
CRL Publishing Parameters
View CRLs

Below are listed all CRLs and Delta CRLs currently generated by this CA. If the CA key is re-used during a renew, the old index is re-used and you may see some skipped indexes.

CRLs

Key Index	Effective Date	Expiration Date	Publish Status
0	4/26/2022 7:30 ...	5/3/2022 7:50 PM	OK

Delta CRLs

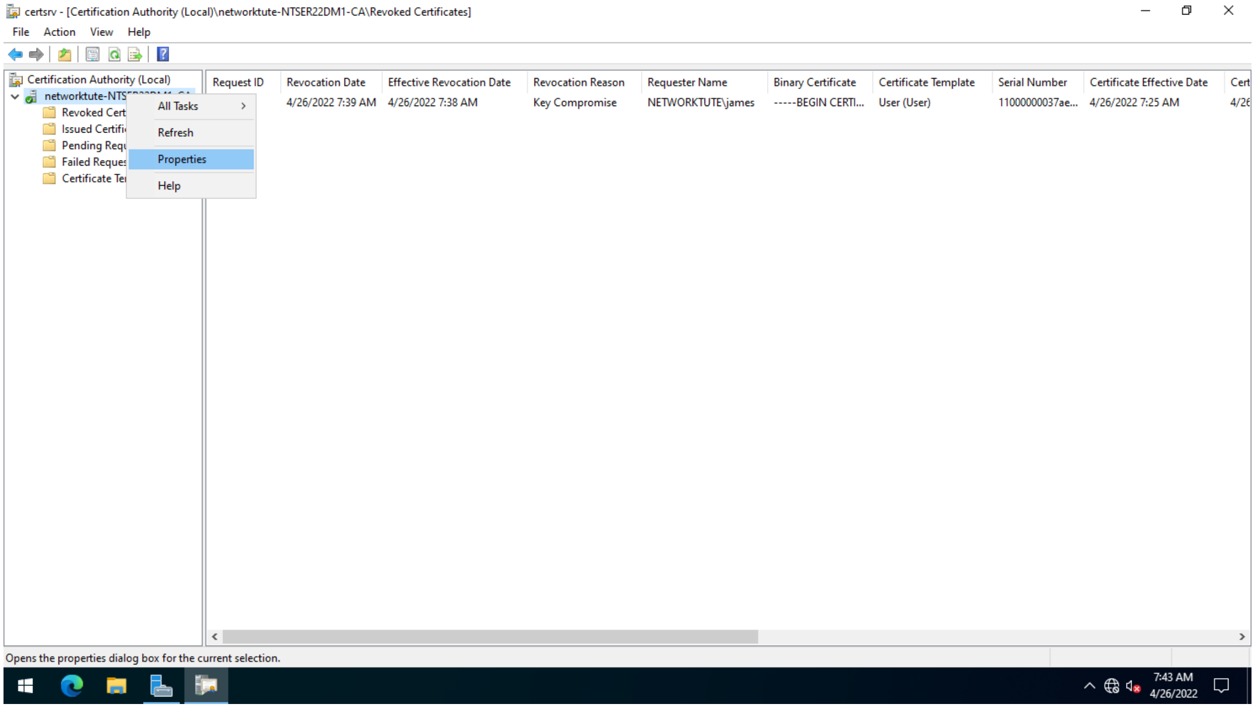
Key Index	Effective Date	Expiration Date	Publish Status
0	4/26/2022 7:30 ...	4/27/2022 7:50 ...	OK

Task 3: Configure a New Path for CRLs

It is also possible to configure a new path for the CRLs.

Step 1:

On the **NTSER22DM1** server, right-click **networktute-NTSER22DM1-CA** and select **Properties**

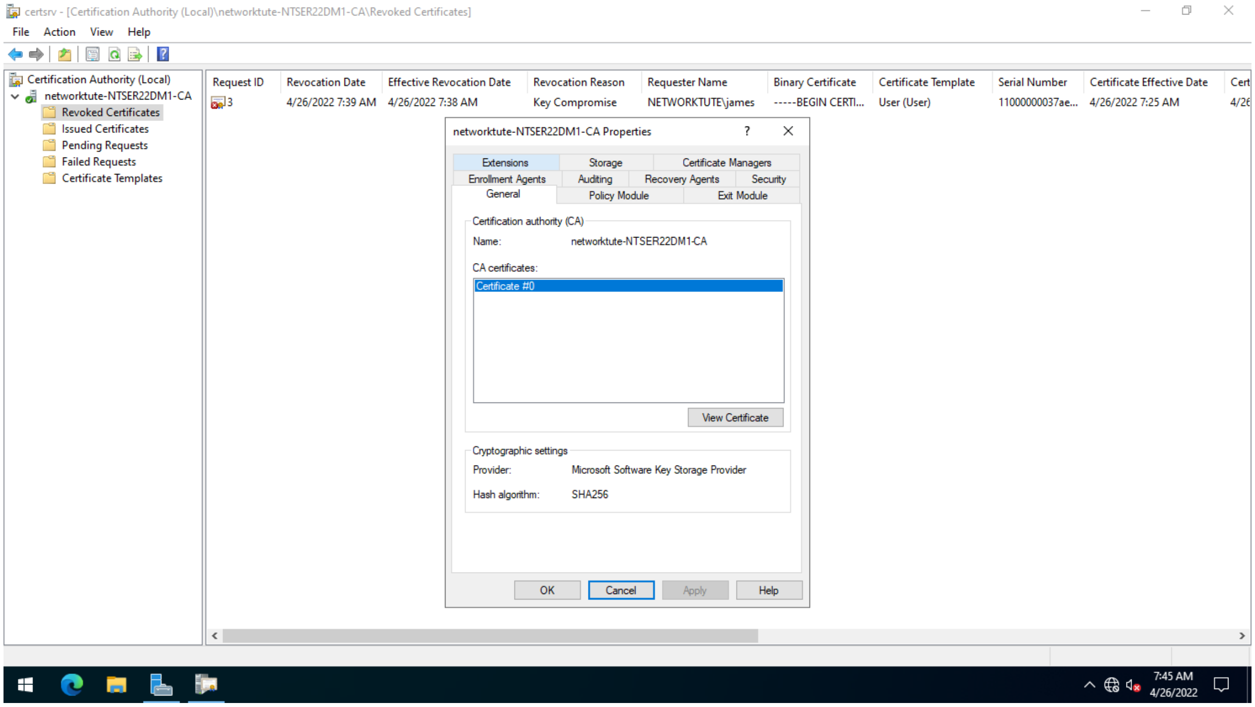

certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Opens the properties dialog box for the current selection.

Step 2:

In the **networktute-NTSER22DM1-CA** Properties dialog box, click the **Extensions** tab.


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

networktute-NTSER22DM1-CA Properties

Certification authority (CA)

Name: networktute-NTSER22DM1-CA

CA certificates:

Certificate #0

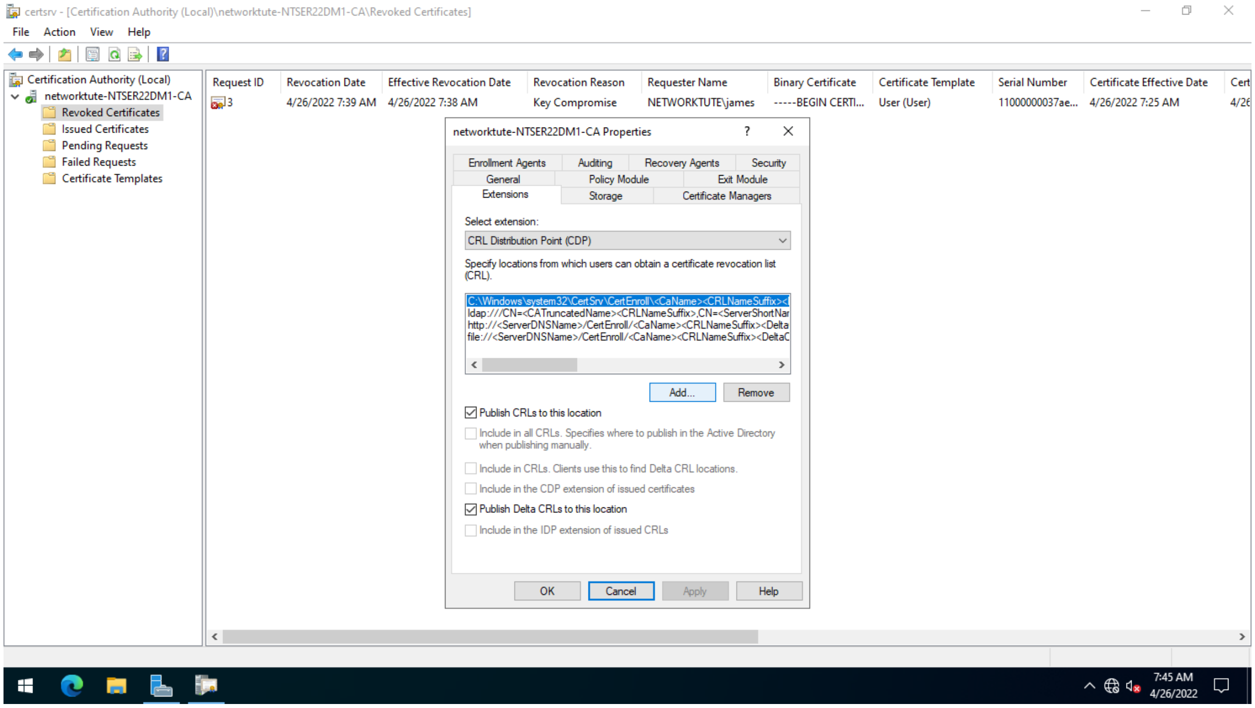
Cryptographic settings

Provider: Microsoft Software Key Storage Provider

Hash algorithm: SHA256

Step 3:

Under the **Extensions** tab, click **Add**.



Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Select extension: CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC
```

☑ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

□ Include in CRLs. Clients use this to find Delta CRL locations.

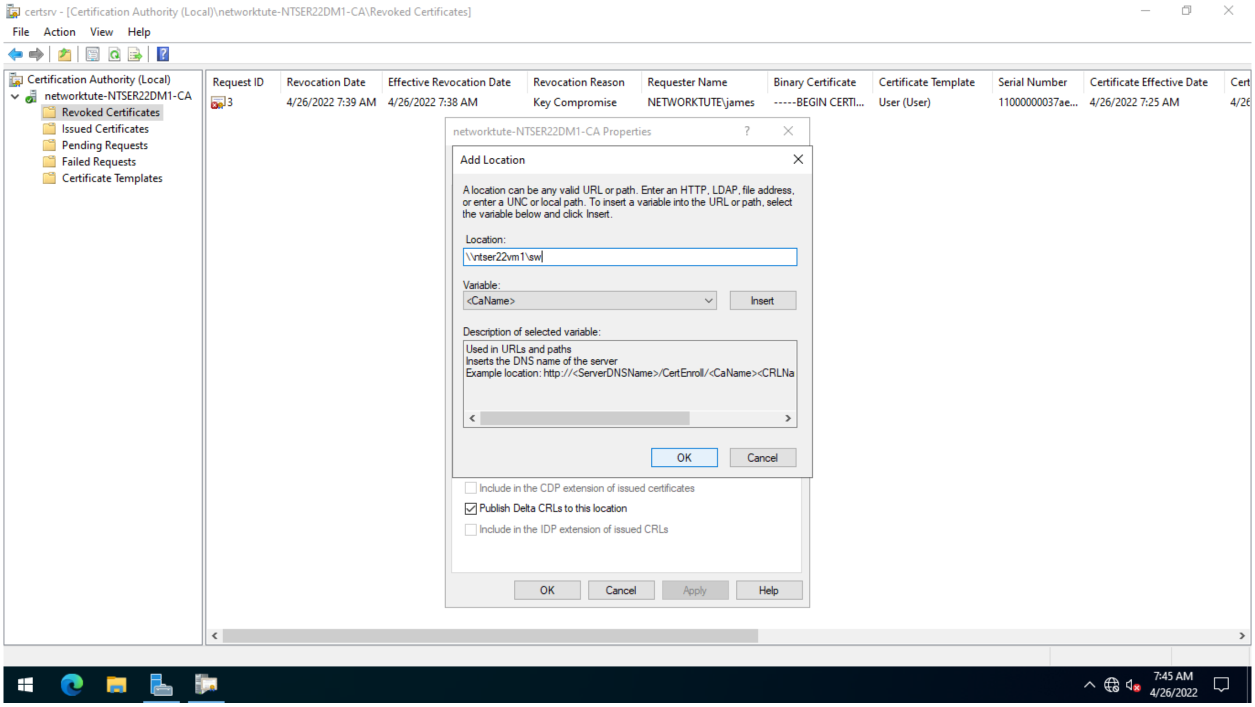
□ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

□ Include in the IDP extension of issued CRLs

Step 4:

In the **Add Location** dialog box, in the **Location** text box, type: ***\\ntser22vm1\sw***


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
networktute-NTSER22DM1-CA Properties
Add Location
Insert
OK
Cancel
OK
Cancel
Apply
Help
7:45 AM
4/26/2022

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location: \\ntser22vm1\sw

Variable: <CaName>

Description of selected variable:

Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

□ Include in the CDP extension of issued certificates

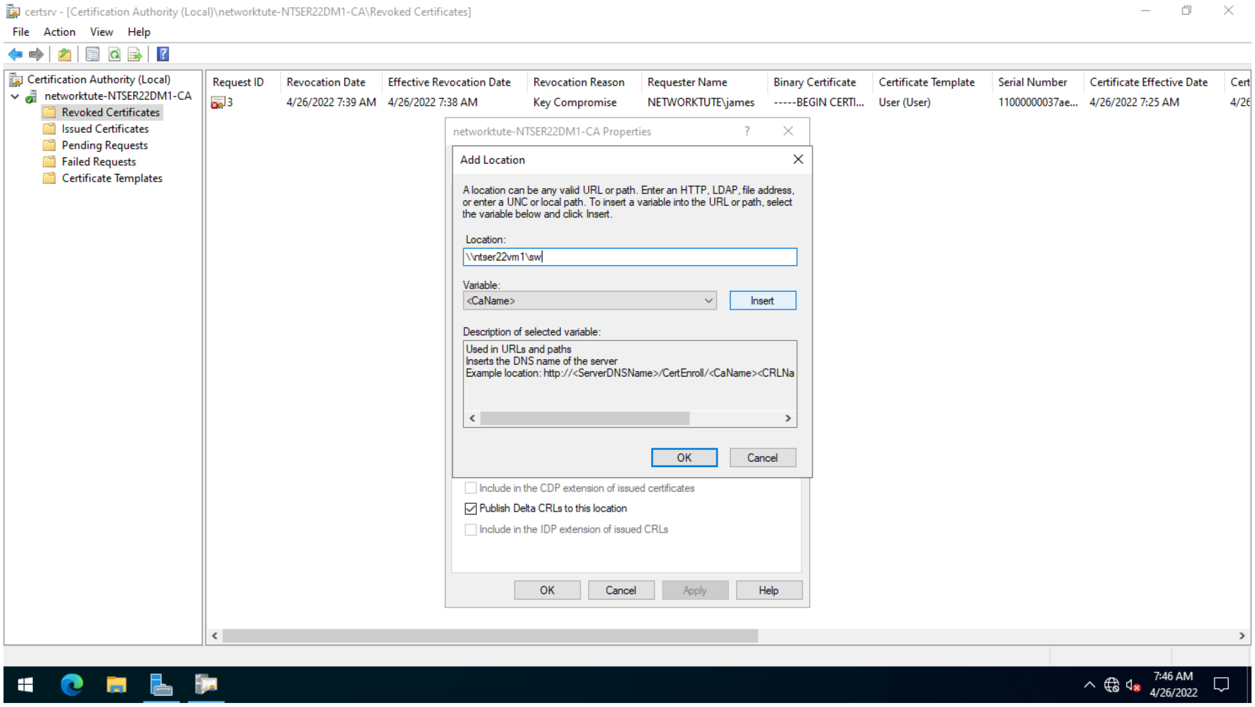
☑ Publish Delta CRLs to this location

□ Include in the IDP extension of issued CRLs

Step 5:

From the **Add Location** dialog box, after adding the network path, put the cursor at the end of the network path location.

Click **Insert**


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
7:46 AM
4/26/2022

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

networktute-NTSER22DM1-CA Properties

Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location: \\ntser22vm1\sw

Variable: <CaName> Insert

Description of selected variable:

```
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa
```

OK Cancel

□ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

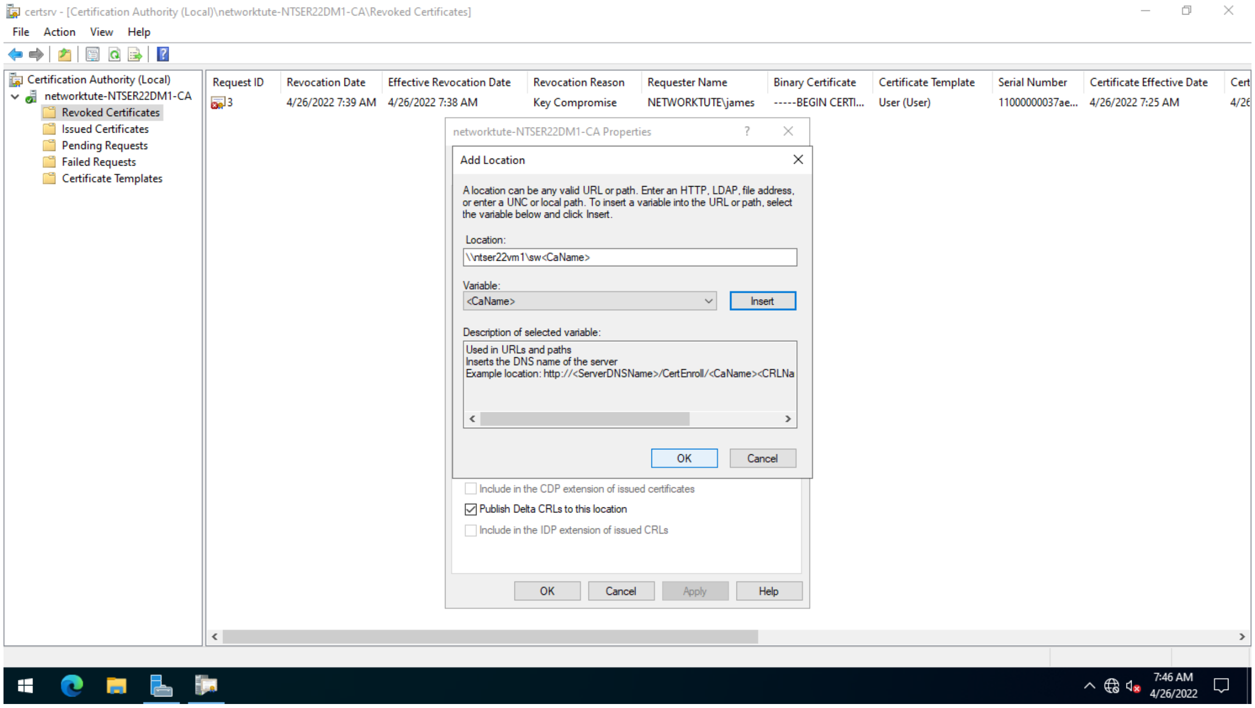
□ Include in the IDP extension of issued CRLs

OK Cancel Apply Help

Step 6:

You’ll see that <**CaName**> has appended at the end of network path \\ ntser22vm1\sw.

Click **OK**.


certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (Local)
networktute-NTSER22DM1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
networktute-NTSER22DM1-CA Properties
OK
Cancel
Apply
Help
7:46 AM
4/26/2022

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:
\\ntser22vm1\sw<CaName>

Variable:
<CaName> Insert

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

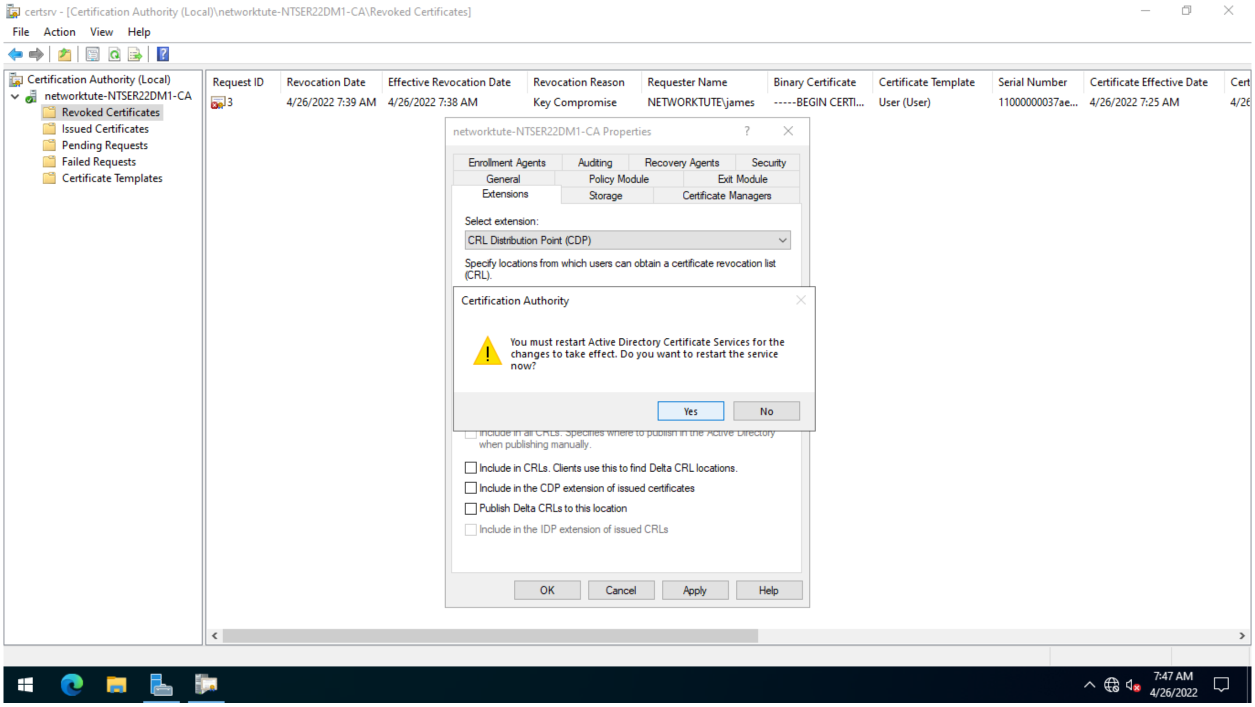
OK Cancel

□ Include in the CDP extension of issued certificates
☑ Publish Delta CRLs to this location
□ Include in the IDP extension of issued CRLs

Step 7:

Click **Apply** to save changes in the **Extensions** tab.

When prompted to restart in the **Certification Authority** dialog box, click **Yes**.



Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

Select extension:
CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

Certification Authority

You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?

Yes No

Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

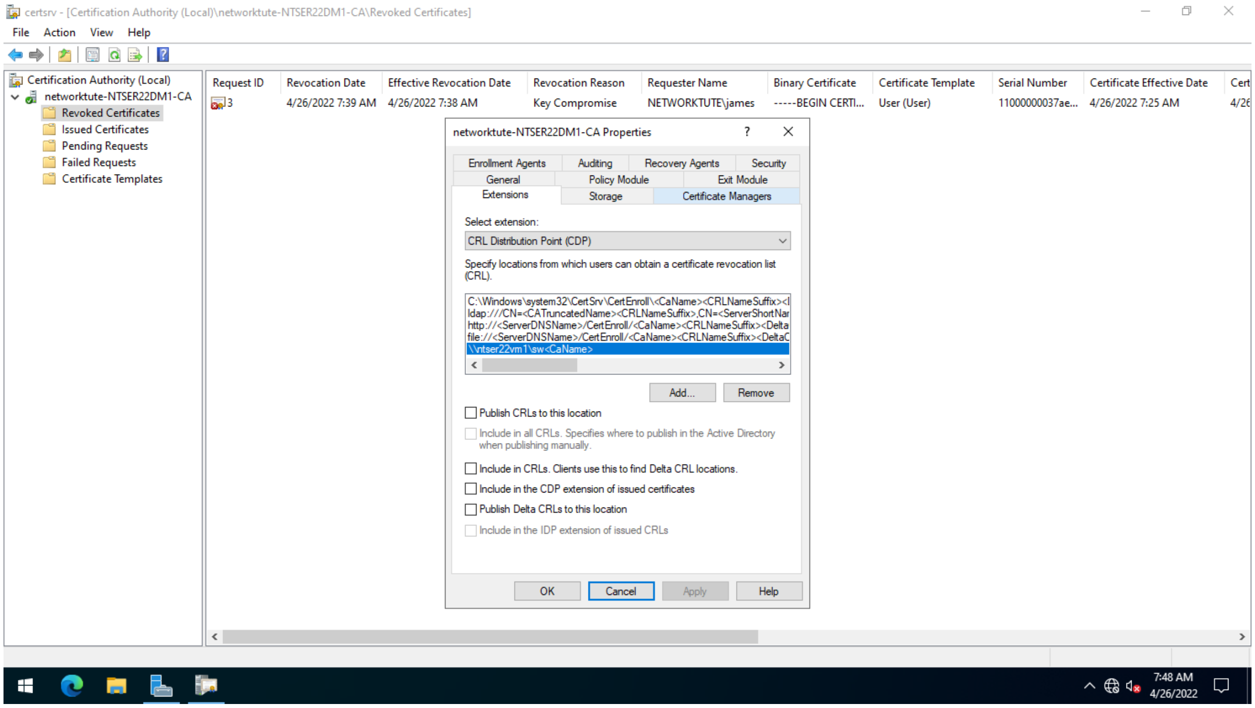
□ Include in CRLs. Clients use this to find Delta CRL locations.
□ Include in the CDP extension of issued certificates
□ Publish Delta CRLs to this location
□ Include in the IDP extension of issued CRLs

Task 4: Add Certificate Managers

You can limit administrative permissions to certain users in the CA properties. In the Active Directory environment, for example, you can limit permissions to Enterprise Admins. You can even appoint someone as a Certificate Manager.

Step 1:

Still on the **NTSER22DM1** server, click the **Certificate Managers** tab.



certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

networktute-NTSER22DM1-CA Properties

Select extension: CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><I
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC
\\ntser22vm1\sw<CaName>
```

☐ Publish CRLs to this location

☐ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

☐ Include in CRLs. Clients use this to find Delta CRL locations.

☐ Include in the CDP extension of issued certificates

☐ Publish Delta CRLs to this location

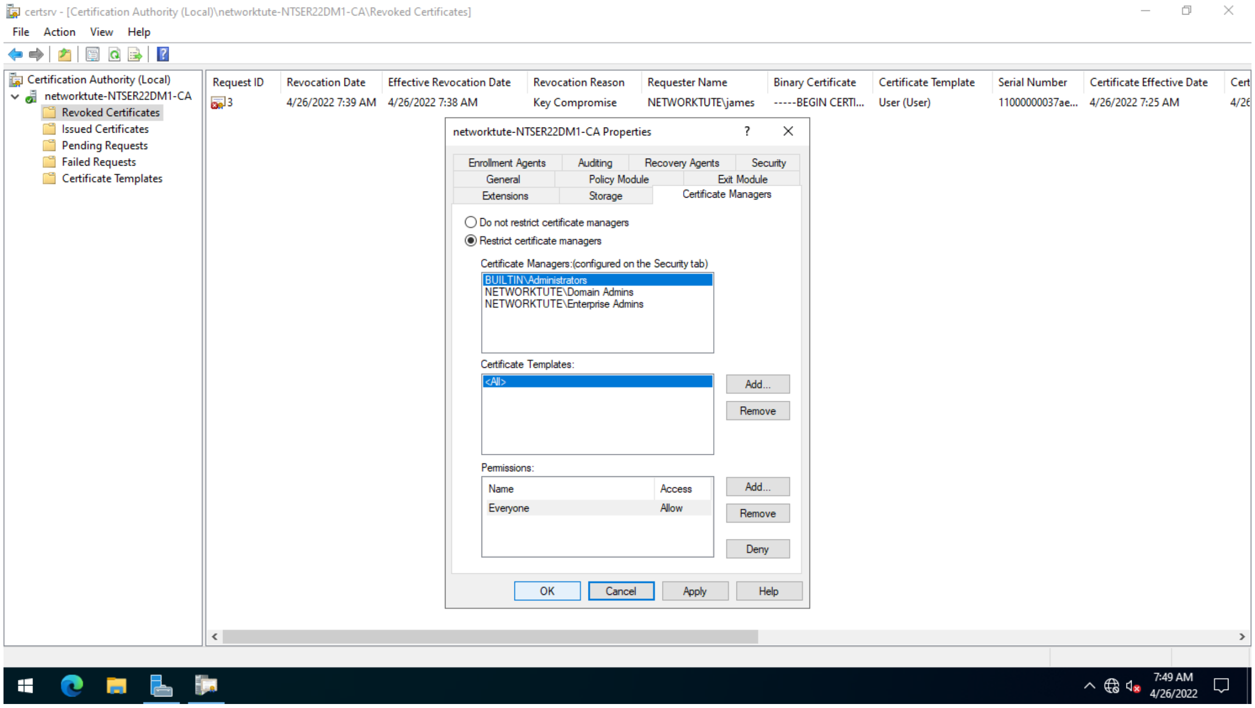
☐ Include in the IDP extension of issued CRLs

Step 2:

On the **Certificate Managers** tab, select the **Restrict certificate managers** option.

NOTE: You'll be limiting portions of AD Certificate Services administration to the Domain Admins and Enterprise Admins groups in this domain if you choose this option.

Click **OK**.



certsrv - [Certification Authority (Local)\networktute-NTSER22DM1-CA\Revoked Certificates]

Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Cert
3	4/26/2022 7:39 AM	4/26/2022 7:38 AM	Key Compromise	NETWORKTUTE\james	-----BEGIN CERTI...	User (User)	11000000037ae...	4/26/2022 7:25 AM	4/26

networktute-NTSER22DM1-CA Properties

○ Do not restrict certificate managers

● Restrict certificate managers

Certificate Managers:(configured on the Security tab)

BUILTIN\Administrators
NETWORKTUTE\Domain Admins
NETWORKTUTE\Enterprise Admins

Certificate Templates:

<All>

Permissions:

Name	Access
Everyone	Allow